Unclassified **NEA/CSNI/R(2002)1/VOL1**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

10-Jun-2002

English - Or. English

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/CSNI/R(2002)1/VOL1
Unclassified

CNRA/CSNI WORKSHOP ON LICENSING AND OPERATING EXPERIENCE OF COMPUTER-BASED I&C SYSTEMS

WORKSHOP PROCEEDINGS

Hluboka nad Vltavou, Czech Republic
25th-27th September, 2001

English - Or. English

JT00127842

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Co-operation and Development (OECD) shall promote policies designed:

- to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;
- to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and
- to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The original Member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996), Korea (12th December 1996) and the Slovak Republic (14th December 2000). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full Member. NEA membership today consists of 27 OECD Member countries: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, Republic of Korea, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities also takes part in the work of the Agency.

The mission of the NEA is:

- to assist its Member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as
- to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include safety and regulation of nuclear activities, radioactive waste management, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.

In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has a Co-operation Agreement, as well as with other international organisations in the nuclear field.

© OECD 2002
Permission to reproduce a portion of this work for non-commercial purposes or classroom use should be obtained through the Centre français d'exploitation du droit de copie (CCF), 20, rue des Grands-Augustins, 75006 Paris, France, Tel. (33-1) 44 07 47 70, Fax (33-1) 46 34 67 19, for every country except the United States. In the United States permission should be obtained through the Copyright Clearance Center, Customer Service, (508)750-8400, 222 Rosewood Drive, Danvers, MA 01923, USA, or CCC Online: http://www.copyright.com/. All other applications for permission to reproduce or translate all or part of this book should be made to OECD Publications, 2, rue André-Pascal, 75775 Paris Cedex 16, France.

COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES

The Committee on Nuclear Regulatory Activities (CNRA) of the OECD Nuclear Energy Agency (NEA) is an international committee made up primarily of senior nuclear regulators. It was set up in 1989 as a forum for the exchange of information and experience among regulatory organisations and for the review of developments which could affect regulatory requirements.

The Committee is responsible for the programme of the NEA, concerning the regulation, licensing and inspection of nuclear installations. The Committee reviews developments which could affect regulatory requirements with the objective of providing members with an understanding of the motivation for new regulatory requirements under consideration and an opportunity to offer suggestions that might improve them or avoid disparities among Member Countries. In particular, the Committee reviews current practices and operating experience.

The Committee focuses primarily on power reactors and other nuclear installations currently being built and operated. It also may consider the regulatory implications of new designs of power reactors and other types of nuclear installations.

In implementing its programme, CNRA establishes co-operative mechanisms with NEA's Committee on the Safety of Nuclear Installations (CSNI), responsible for co-ordinating the activities of the Agency concerning the technical aspects of design, construction and operation of nuclear installations insofar as they affect the safety of such installations. It also co-operates with NEA's Committee on Radiation Protection and Public Health (CRPPH) and NEA's Radioactive Waste Management Committee (RWMC) on matters of common interest.

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The NEA Committee on the Safety of Nuclear Installations (CSNI) is an international committee made up of scientists and engineers. It was set up in 1973 to develop and co-ordinate the activities of the Nuclear Energy Agency concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international co-operation in nuclear safety amongst the OECD Member countries.

CSNI constitutes a forum for the exchange of technical information and for collaboration between organisations which can contribute, from their respective backgrounds in research, development, engineering or regulation, to these activities and to the definition of its programme of work. It also reviews the state of knowledge on selected topics of nuclear safety technology and safety assessment, including operating experience. It initiates and conducts programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach international consensus in different projects and International Standard Problems, and assists in the feedback of the results to participating organisations. Full use is also made of traditional methods of co-operation, such as information exchanges, establishment of working groups and organisation of conferences and specialist meeting.

The greater part of CSNI's current programme of work is concerned with safety technology of water reactors. The principal areas covered are operating experience and the human factor, reactor coolant system behaviour, various aspects of reactor component integrity, the phenomenology of radioactive releases in reactor accidents and their confinement, containment performance, risk assessment and severe accidents. The Committee also studies the safety of the fuel cycle, conducts periodic surveys of reactor safety research programmes and operates an international mechanism for exchanging reports on nuclear power plant incidents.

In implementing its programme, CSNI establishes co-operative mechanisms with NEA's Committee on Nuclear Regulatory Activities (CNRA), responsible for the activities of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. It also co-operates with NEA's Committee on Radiation Protection and Public Health and NEA's Radioactive Waste Management Committee on matters of common interest.

CNRA/CSNI WORKSHOP ON
LICENSING AND OPERATING EXPERIENCE OF COMPUTER-BASED I&C SYSTEMS
Hluboká nad Vltavou, Czech Republic

25th-27th September, 2001

A Contents

B Summary and Conclusions

C Programme

D Papers

E Participants

A TABLE OF CONTENTS

Page

Volume I

B Summary and Conclusions 11

C Programme 37

D Papers 45

OPENING SESSION:
ADVANCES MADE IN THE USE AND PLANNING OF COMPUTER-BASED I&C SYSTEMS
Chairmen: M. Chiramal - P. Krs

Electricité de France Experience of Computer-based I&C Systems 47
François Poizat, Edf, France

The Evaluation on Applying the Digital Safety System to Existing PWR Plants in Japan 55
Yoichi Mito, the Kansai EP Co., Inc.
Masafumi Utsumi, Mitsusbishi HI Ltd., Japan

Independent Assessment of the Temelin Software Safety System 63
Petr Zavodsky, CEZ a.s., Czech Republic

Regulatory Review of the Digital Plant Protection System for Korea Next Generation Reactor 75
D.I. Kim, B.R. Kim and S.H. Oh, Korea Institute of Nuclear Safety, Korea

Decision Support for Approval of Safety Critical Programmable Systems 83
Gustav Dahll, Bjørn Axel Gran, OECD Halden Reactor Project, Norway
Bo Liwång, Swedish Nuclear Power Inspectorate, Sweden

TECHNICAL SESSION 1:
NATIONAL AND INTERNATIONAL COMPUTER-BASED STANDARDS AND GUIDES FOR SAFETY SYSTEMS 95
Chairmen: J.P. Bouard, Z. Ogiso

International Standardisation in Nuclear I&C Engineering 97
Jean-Paul Bouard, EdF, France

Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety 109
Gary Johnson, Lawrence Livermore National Laboratory, USA

The New IAEA Safety guide and the Common Position of European Regulators on Software for Systems Important to Safety 117
Pierre-Jacques Courtois, Association Vinçotte Nuclear, Brussels, Belgium

Approach to the Application of the State Regulatory Requirements, Legislation and Standards in Modernization of I&C Systems, Concerning Especially the Digital Computer-Based Systems **129**
J. Zatloukal, P. Krakora, NRI Rez, Czech Republic

Standard Base for Regulatory Activity in NPP I&C Systems Area **139**
V. Goldrin, M. Yastrebenetsky, Yu. Rozen, S. Vinogradskaya
State Scientific Technical Center on Nuclear and Radiation Safety, Ukraine

TECHNICAL SESSION 2: REGULATORY ASPECTS **147**
Chairmen: K. Hamar, A. Lindner,

EMI/RFI and Power Surge Withstand Guidance for the U.S. Nuclear Power Industry
Christina Antonescu, USNRC, **149**
Paul D. Ewing, Richard T. Wood, Oak Ridge National Laboratory, USA

Pre-Qualification of Digital Platform - U.S. NRC Regulatory Review of the Common Q Platform **159**
W.K. Mortensen, M. Chiramal

Survey and Evaluation of Digital I & C Licensing Experience **165**
Swu Yih, Chin-Feng Fan, Chan-Fu Chuang

Collecting Data from Operational Experience of Computer-Based I&C Systems - A Regulatory Perspective on Goals and Tasks **177**
G. Schnürer, ISTec, Garching, F. Seide, BfS, Salzgiter, Germany

Digital Projects in the Near Past and their Consequences in Safety Regulations in Hungary **187**
K. Hamar, HAEC, Hungary

Volume II

TECHNICAL SESSION 3
ANALYSIS AND ASSESSMENT OF DIGITAL I&C SYSTEMS **11**
Chairmen: M. L. Järvinen, M. Kersken

Preliminary Evaluation of Computerized Procedures from Safety Viewpoints **16**
Yun H. Chung, Sung N. Choi, Bok R. Kim, Korea Institute of Nuclear Safety, Korea

Modernization of the I&C System for ANP Dukovany by the Use of Computer-based Equipment **21**
F. Dalik, K. Wagner, M. Ris, SKODA, Czech Republic
Jean-Pierre Burel, Schneider Electric, Jean-Paul Mauduit, Framatome-ANP, France

FMEA Performed on the SPINLINE3 Operational System Software as Part of the TIHANGE1 NIS Refurbishment Safety Case **37**
L. Ristord, C. Esmenjaud, Schneider Electric Industries, France

Qualification of Pre-Developed Software for Safety-Critical I&C Application in NPPs **51**
M. Kersken, ISTec, Garching, Germany

A Bayesian Approach to Risk Informed Performance Based Regulation for Digital I&C QA Programs **69**
Swu Yih, Sun-Li Chyou, Li-Sing Wang, AEC INER
Chin-Feng Fan, Yuan-Ze University, Chinese Taipei

TECHNICAL SESSION 4
SOFTWARE LIFE CYCLE ACTIVITIES **81**
Chairmen: G. Dahll, F. Krizek

Implementation of Software Independent Verification Distributed Control and Information Systems and Validation for Lungmen **83**
Jiin-Ming Lin, Jeen-Yee Lee, Taiwan Power Company, Chinese Taipei

Static Analysis of the Software Used in Safety Critical System of the NPP Temelin **91**
Z. Piroutek, S. Roubal, J. Rubek, I & C Energo, a.s., Czech Republic

Assessment Methodology of the Temelin NPP Control System Performance and Quality **99**
Ivan Petruzela, Karel Bednarik, I & C Energo, a.s., Czech Republic

Methodology of NPP I&C System Algorithms and Software Expert Analysis **109**
V.S. Kharchenko, L.M. Lyubchik, M.A. Yastrebenetsky, State Scientific Technical Center on Nuclear and Radiation Safety, Ukraine

TECHNICAL SESSION 5
EXPERIENCE WITH APPLICATIONS SYSTEM ASPECTS, POTENTIAL LIMITS AND FUTURE TRENDS AND NEEDS **119**
Chairmen: B. Liwång - M. Hrehor

Operating Experience of Digital Safety-Related System of Kashiwazaki-Kariwa Unit No. 6 and 7 **121**
Makino Shigenori, Tokyo Electric Power Company, Japan

Technical Requirements on Maintenance of Digital I&C Systems Important to Safety **131**
G. Schnürer, ISTec, Garching, F. Seidel, BfS, Salzgitter, Germany

Requirements Management of I & C System Refurbishment of NPP Dukovany **141**
Jiri Pliska, I & C Energo, a.s., Czech Republic

Licensing Process of the Digital Computer-based I&C Systems to be Implemented Within the NPP Dukovany I & C Refurbishment Project **151**
Ceslav Karpeta, Scientech Inc., Josef Rosol, CEZ, a.s., Czech Republic

Temelin Nuclear Power Plant Westinghouse - I&C Change Process (Paper not available)
Dennis M. Popp, John L. Duryea, USA

E List of Participants **169**

CNRA/CSNI WORKSHOP ON
LICENSING AND OPERATING EXPERIENCE OF
COMPUTER-BASED I&C SYSTEMS
Hluboká nad Vltavou, Czech Republic

25th-27th September, 2001

B. Summary and Conclusions

CNRA/CSNI WORKSHOP ON
LICENSING AND OPERATING EXPERIENCE OF
COMPUTER-BASED I&C SYSTEMS

EXECUTIVE SUMMARY

The OECD Workshop on Licensing and Operating Experience of Computer-Based I&C Systems, was held from 25th to 27th September, 2001, in Hluboká nad Vltavou, Czech Republic, sponsored by both the Committee on Nuclear Regulatory Activities (CNRA) and the Committee on the Safety of Nuclear Installations (CSNI) of the OECD Nuclear Energy Agency (NEA). It was organised in collaboration with the Czech State Office for Nuclear Safety (SÚJB), the Czech Power Board CEZ a.s., I&C Energo a.s. and the Nuclear Research Institute, Rez near Prague.

The objectives of the Workshop were to exchange the experience gained by both the regulators and the industry in different countries in the licensing and operation of computer-based I&C systems, to discuss the existing differences in their licensing approaches in various countries, to consider the safety aspects of their practical use, and to discuss the ways of promoting future international co-operation in the given area.

The scope of the Workshop included:

- review of the progress made since the CNRA/CSNI workshop which was held in 1996
- current and future regulatory needs and/or requirements for the computer-based I&C systems
- progress made in software life cycle activities, including verification and validation, and safety/hazards analysis
- benefits of applying the computer-based I&C systems to improve plant performance and safety.

The Technical Sessions and Discussion Sessions covered the following topics:

Opening Session: Advances made in the use and planning of computer-based I&C systems
Topic 1: National and international standards and guides for computer-based safety systems
Topic 2: Regulatory aspects
Topic 3: Analysis and assessment of digital I&C systems
Topic 4: Software life cycle activities
Topic 4: Experience with applications, system aspects, potential limits and future trends and needs
Final Session: Workshop summary.

The workshop provided a unique opportunity for people with experience in licensing, developing, manufacturing, implementing, maintaining or researching computer-based systems important to safety to get together and to discuss their insights learned from their actual activities. The Workshop was successful in this point. It was attended by 65 people from 15 countries and by 2 international organizations.

Progress since the previous workshop

At the first workshop the basic concern was whether it is possible to safely implement and operate software-based systems in nuclear power plants. During the 5 years following the first OECD workshop, computer-based I&C systems have been installed and operated in both safety and non-safety systems in a number of nuclear plants all over the world. These countries have developed the systems in their own manner and universal measures to implement computer-based safety systems have not yet been obtained. This status has not changed since the previous Workshop. In parallel, the nuclear industry (consisting of the utilities, vendors, designers, and constructors) and the regulators have universally reached a somewhat stable state in addressing the issues and concerns which were identified during that first workshop. This state was achieved by accepting, in principle, that a computer-based safety system designed, implemented and reviewed based on a structured life-cycle process would provide an acceptable safety system.

The life cycle processes adopted by most of the countries are based on the requirements of national or international standards which have similar structures and methodologies. The process consists of a series of hardware- and software- related activities including design, review, tests, verification and validation, configuration management, safety analyses, and associated documentation.

In comparison with the last meeting, it is evident that great progress has been made in the application of digital computer-based I&C systems. At the same time, it was reported in several papers that new problems had emerged during these five years, for example, COTS, certification of software, obsolescence of digital spare parts, re-classification of some computer-based systems (for example, overall plant computer that controls main control panels or consoles), regulatory efficiency and effectiveness on computer-based systems important to safety, etc. Future problems from the regulatory point of view refer to both the adoption of the established qualification methods for software-based I&C systems to new developments in software technology and to the improvement of the licensing procedures.

As the progress of digital technology is very rapid from day to day, there is a need to continue following the progress of digital technology and surveying the measures for application with accumulating operating experience of previous installations. Collecting and evaluating operational experience of computer-based systems as initiated by the CSNI Task Force on Computer-Based Control Systems Important to Safety (COMPSIS) will be essential for the evaluation of reliability characteristics of such systems and devices.

Findings and Recommendations

The purpose of this Workshop was to recognize the progress of technology concerning the items that the previous Workshop and the CNRA Special Issue Meeting had indicated.

In this context, the insight from this Workshop can be summarized as follows:

Complexity: The complexity of functions required of the modern computer systems and its basic elements (cpu, graphic tools, compilers, etc.,) is increasing with technological advances. As a consequence, there are two diverging trends which need to be addressed - added functionality and capability of the system versus verifying that adequate safety is maintained. Methodologies for demonstrating software safety, including the issue of verification and validation are still controversial.

Reliability: Many papers indicated that simplicity was most important to assure the reliability of computer-based systems important to safety, but did not indicate "how simple is simple enough for safety application". At the same time, some analytical approaches were introduced but did not succeed in showing quantitative values. This status has been left unchanged since the previous Workshop. International co-operation should help in obtaining the analytical measures.

Diversity: The functional diversity is considered in most of the applications which were presented at this Workshop, while some indicated other digital diverse systems.

Digital technology evolution**:** The rapid pace of the digital technology evolution has identified the need for addressing obsolescence of components, equipment, and tools; consideration of spare parts, human resources and expertise for operating and maintaining NPP digital systems for the life of the systems. Suggestions made at the workshop, such as sharing resources and knowledge base through some vehicles like Owner's Groups, are worthy of consideration.

International and national standards: Considerable progress has been achieved on this issue. Many international standards and guides covering software lifecycle were developed and revised during these five years, while many countries have developed their own standards or guides.
Some people felt that there are too many standards that are often complex, inconsistent, and misleading. As stated in the papers at this workshop, the various standards committees are aware of these shortcomings and co-ordination activities between the various national and international standards organizations have been initiated. Such efforts should be encouraged so that the fundamental requirements and acceptance criteria for all computer system life-cycle activities in both national and international standards are clear and consistent.

Independent V&V: All of the presentations related to this issue indicated that they followed the similar style of V&V as the ones endorsed in IEC 880 and also reported that it cost too much time and human resources, with a large amount of documentation. Meanwhile, many approaches on independent V&V were reported but the insights on the degree of independence were divided. It seems difficult to reach a general consensus on the degree of independence. In particular, the independent V&V performed in NPP Temelin gave the impression that "independence" is a very costly and time-consuming activity. It seems that we stand at a turning point, that is, which way should we adopt. One way is to produce a complex system and to perform cost-ineffective independent V&V on it. The other is to pursue simplicity that does not need to perform independent V&V. For some systems, such as French SPIN/SPINELINE3, German Teleperm-XS, Japanese POL, and American Eagle it was shown that they have been already verified and moved to the stage of design certification or product certification for reuse in safety application. The

approach "Independent V&V for first application and certification of design or product for second use" is expected.

***Maintaining human competencies*:** An area of concern expressed during the workshop was that the human resources and competencies necessary to maintain the current computer-based safety and non-safety systems is not likely be available in the near future. Most of the participants agreed that addressing the problem on human resources is essentially important as well as the development of safety critical digital systems. Methods and policies for retaining the knowledge, expertise and competencies should be initiated in the industry and regulatory bodies.

COTS, PDS, PES: The use of commercial off-the-shelf (COTS) products, previously developed software (PDS), and previously existing software (PES) and other legacy systems in safety system applications is an issue that was identified as an immediate concern. Standards addressing the requirements and acceptance criteria and detailed guidance on how to implement them in a manner that is internationally applicable are needed immediately.

Conclusion

As a general conclusion, the Workshop can be considered representative of the progress made towards reaching the targets set at the Munich workshop almost five years ago. The Munich workshop had identified areas where further development and specific improvements were needed. The Hluboka workshop has reviewed the development achieved since then. Based on the papers presented at this workshop and on the discussions by the workshop participants, it is evident that the details of the life-cycle activities and the associated acceptance criteria are still in flux and have yet to be universally acceptable. The basic trends from Munich still hold and are reaffirmed in the frame of evolving regulatory and commercial environments.

Future international co-operation should strive to reach universally acceptable positions in the above areas.

OECD/CSNI WORKSHOP ON
LICENSING AND OPERATING EXPERIENCE OF
COMPUTER-BASED I&C SYSTEMS

MEETING SUMMARY

Sponsorship

The OECD Workshop on **Licensing and Operating Experience of Computer-Based I&C Systems,** was held from 25h to 27th September, 2001, in Hluboká nad Vltavou, Czech Republic, it was sponsored by both the Committee on Nuclear Regulatory Activities (CNRA) and the Committee on the Safety of Nuclear Installations (CSNI) of the OECD Nuclear Energy Agency (NEA). It was organised in collaboration with the Czech State Office for Nuclear Safety (SÚJB), the Czech Power Board CEZ a.s., and I&C Energo a.s.

2. Background:

In March 1996 the CNRA and CSNI organised a Workshop on Technical Support for Licensing Issues of Computer-Based Systems Important to Safety. The workshop was hosted by GRS/ISTec in Munich, Germany. The main purpose of the Workshop was to provide a forum for the exchange of information on the technical issues of computer-based systems important to safety. In June 1996 there was a joint CNRA/CSNI Special Issue meeting to discuss the technical support required for licensing issues of computer-based systems important to safety, utilising the results of the workshop. Follow-up activities were discussed at the December 1996 annual meetings of the CNRA and CSNI. Both meetings confirmed the general recommendations of the workshop, such as:

- Digital systems can be used in safety systems provided that they meet local regulatory requirements
- A wide spectrum of licensing approaches exists
- Further co-operation between the regulatory bodies is necessary to understand the regulatory basis for differences
- It is important to collect information on actual experience in utilising software systems.

In response to the CSNI and CNRA annual meetings in 1996, a Task Group on Computer-Based Systems Important to Safety was established under the CSNI Working Group on Operating Experience. The Task Group has developed a database (COMPSIS) on operational experience related to computer-based systems and follows up on the state of knowledge on the issues. Also, a guideline document, NEA/CSNI/R(99)14 "COMPSIS, Computer-based Systems Important to Safety, Reporting Guidelines", was issued in 1999. The data collection has already been initiated by the Task Group under a trial experiment.

The use of digital systems in NPPs is expanding rapidly. As this technology improves, more and more of these systems are being installed at existing and new plants. The most extensive applications of digital I&C systems have been made at the Darlington NPP in Canada, Sizewell B NPP in the UK, Chooz B1 (France), Kashiwazaki-Kariva 6,7 in Japan, Wolsong 2,3,4 (Korea) and Temelin NPP in the Czech

Republic. Recently, partial refurbishment of the obsolete I&C systems at some VVERs, e.g. Bohunice 1,2 (Slovakia) or Paksh 1,2 (Hungary) by digital ones was done, as well.

At the present time, there is generally a greater experience with computer-based I&C systems on both sides, the industry and among regulators, than there was five years ago. Progress has also been made in developing international regulatory guides and recommendations related to the digital I&C systems.

Based on the progress made in the development of digital I&C systems in recent years and their practical applications in many NPPs in NEA member states, the two committees, CNRA and CSNI, decided to organise a joint CNRA/CSNI Workshop in the second half of 2001 on "Licensing and Operating Experience of Computer-Based Systems Important to Safety", as a follow-up to the one which was held in 1996. The purpose was to exchange the experience gained by both the regulators and the industry in different countries in the licensing and operation of computer-based I&C systems, to discuss the existing differences in their licensing approaches in various countries, to consider the safety aspects of their practical use and to discuss the ways of future international co-operation in the given area.

3. Scope and Technical Content of the Workshop

The scope of the Workshop included:

- review of the progress made since the CNRA/CSNI workshop in 1996
- current and future regulatory needs and/or requirements for the computer-based I&C systems
- progress made in software life cycle activities, including verification and validation, and safety/hazards analysis
- benefits of applying the computer-based I&C systems to improve plant performance and safety.

The Technical Content of the Workshop included:

Opening Session: Advances made in the use and planning of computer-based I&C systems
Topic 1: National and international standards and guides for computer-based safety systems
Topic 2: Regulatory aspects
Topic 3: Analysis and assessment of digital I&C systems
Topic 4: Software life cycle activities
Topic 5: Experience with applications, system aspects, potential limits and future trends and needs
Final Session: Workshop summary.

In general terms, the Workshop attempted to give answers to questions in the following areas:

- What are the benefits of using computer-based I&C systems?
- What national and international standards and guidance could be universally acceptable from the safety perspective?
- What are the regulatory requirements for the current and future generations of digital I&C systems?
- What are the major technical issues and challenges associated with applications of digital technology in I&C systems?

4. Programme Committee of the Workshop

For the preparation of the workshop, its agenda and all the other organisational aspects, the existing CSNI Task Force on Computer-Based Control Systems Important to Safety (COMPSIS) set up the core of the workshop Programme Committee (PC). It was the responsibility of the Programme Committee to evaluate the abstracts of the proposed papers, select the papers for presentation, organise the Sessions, develop the final programme of the workshop, appoint the Session Chairmen, etc. The members of the Programme Committee were:

Mr. Jean-Paul BOUARD, EdF, France
Mr. Matthew CHIRAMAL, NRC, USA ,(COMPSIS Chairman)
Mr. Pierre J. COURTOIS, AVN, Belgium
Mr. Gustav DAHLL, OECD Halden Project
Mr. Karoly HAMAR , HAEC, Hungary
Mr. Hartmuth HEINSOHN, GRS, Germany
Dr. Marja-Leena JÄRVINEN, STUK, Finland
Mr. Karel KRIZEK, CEZ a.s., Czech Republic
Mr. Petr KRS, SÚJB, Czech Republic (PC Chairman)
Dr. Arndt LINDNER, ISTec, Germany
Mr. Bo LIWÅNG , SKI, Sweden
Mr. Zen-ichi OGISO, NUPEC, Japan
Mme. Brigitte SOUBIES , DSIN, France
Prof. Björn WAHLSTRÖM, VTT, Finland
Mr. Bob Yates, NII, United Kingdom
Mr. Miroslav Hrehor, OECD/NEA, (Scientific Secretary).

On the occasion of the Workshop there was an opportunity for participants to visit NPP Temelin with its VVER-1000 reactors equipped with the Westinghouse's digital I&C system.

OPENING SESSION : ADVANCES MADE IN THE USE AND PLANNING OF COMPUTER-BASED I&C SYSTEMS

Session Chairmen: M. Chiramal, P. Krs

Electricité de France Experience of computer-based I&C systems

Poizat Francois, EdF , France

The presentation focused on the experience gained by EdF in the transition from the electro-magnetic relay-based analog I&C systems in the 34 900 Mwe NPP units (commissioned during 1977 to 1983) to the first digital integrated protection system (SPIN) based on Motorola 6800 microprocessors in the 20 1300 Mwe P4 ad P'4 units (1984 - 1991) to the fully computerized I&C system in the 4 1450 Mwe N4 units (1997) in which the protection system (SPIN), control systems (Contronic E and uREC), control room (KIC) including plant operating procedures are computerized.
To revamping/refurbishment of the steam generator level control system, and the nuclear instrumentation system at the oldest 900 Mwe units during 1998 -99.

The presentation traced these changes, discussed the problems encountered, and the lessons learned. As NPPs trend towards more computerization and reliance on digital components, consideration should be given to the short life cycles of these products and difficult-to-maintain software skills. The presentation concluded that the trend towards the use of COTS to develop NPP I&C systems is a viable solution, provided that safety requirements are met in a cost-effective manner.

The Evaluation on Applying the Digital Safety System to Existing PWR Plants in Japan

Yoichi Mito, The Kansai EP Co., Inc.
Masafumi Utsumi, Mitsubishi HI Ltd., Japan

The presentation addressed the problem now facing the Japanese nuclear power plants of aging, obsolescence, and the high cost of maintenance of conventional analog I&C system components and equipment. The industry is studying and developing long-range plans for systematic maintenance and replacement of the analog I&C components and equipment. The latest generation of NPPs in Japan are designed with digital safety and non-safety I&C systems. The study considers the differences between the existing plants and the new plants in the area of system safety functions, redundant architecture, interfaces. Included in the study is the consideration of upgrading the main control room boards with advanced computer-based Human-machine Interface systems.

Independent Assessment of the Temelín Safety System Software

Petr Závodský, CEZ a.s., Czech Republic

The presentation covered the activities carried out by Data System and Solutions LLC (DSAS), under contract to the utility CEZ , for the independent assessment (IA) of the Temelin Plant's safety I&C system software.

The I&C system for the Temelin Nuclear Power Plant was designed and implemented by Westinghouse Electric Co. Westinghouse had performed independent verification and validation of the safety I&C system software in accordance with the requirements of standards IEC-880/1986, IEEE Std. 7-4.3.2/1993, ANSI NQA-2a/1990 Part 2.7. In addition, to provide confidence in the integrity of the safey system software, SUJB required that independent assessment be performed on the safety system software that

included independent verification and confirmation that the software design met the requirements of the standards, and an independent review and evaluation of the system software.The presentation included accounts of the following tasks performed by DSAS and its sub-contractors, and the lessons learned from these activities:

Independent audit of the software development process
Assessment of system software tools
Verification of system and software requirements
Verification of software design
Static analysis of source code
Dynamic testing
Assessment of system common mode
Verification and validation of configuration and calibration data

Based on the IA program it was concluded that there were no findings to undermine the confidence in the quality of the software design implementation process and the system software, and that the processes used by Westinghouse were generally in compliance with the requirements of the reference standards.

Regulatory Review of the Digital Plant Protection System for Korea Next Generation Reactor
D. I. Kim, B. R. Kim and S. H. Oh,
Korea Institute of Nuclear Safety

The presentation provided the regulatory review approach and results of an interim evaluation by the KINS staff with regard to the review of the standard safety analysis report of the Korea Next Generation Reactor (KNGR -AP1400).
The review raised new issues related to the system architecture of the KNGR digital plant protection system (DPPS) regarding the integration of the DPPS bistable processor and the local coincidence logic processor in each of the redundant protection channels. Another item of concern identified is the use of soft controllers in the plant digital engineered safety features actuation system (DESFAS) and the classification and qualification of such controls. The presentation also provided details the of defense-in-depth and diversity analysis for the postulated common mode/cause failure of software, and of the design of the diverse manual controls for DPPS and DESFAS.

Decision Support for Approval of Safety Critical Programmable Systems
Gustav Dahll, Bjørn Axel Gran, OECD Halden Reactor Project
Bo Liwång, Swedish Nuclear Power Inspectorate

The subject of the presentation was the application practices of the three principles of licensing and regulatory requirements - rule-based, consensus-based, and risk-based - as they pertain to software-based NPP I&C systems. The Swedish nuclear regulatory body is drafting a new inspection handbook, where these principles are applied to the lifecycle activities of the software-based system. The presentation provided a methodology for systematically combining the three principles using Bayesian Belief Nets. An experimental study that used the BBN method in combination with a software safety standard was applied to a safety critical software-based system - a computerized system for aiding helicopter landing in various locations during rescue operation. The project consisting of several tasks was discussed during the presentation.

TECHNICAL SESSION 1: NATIONAL AND INTERNATIONAL STANDARDS FOR COMPUTER-BASED SAFETY SYSTEMS AND GUIDES

Session Chairmen: J.P. Bouard, Z. Ogiso

International Standardisation in Nuclear I&C Engineering

Bouard Jean-Paul, EdF, France

The presentation on international standardisation in nuclear I&C, first introduced the global context and the international and regional relationships developed by the International Electrotechnical Commission (IEC), which, together with the International Standards Organisation (ISO) are responsible for the preparation and maintenance of many of the world's International Standards. Then it focuses on standardisation in the nuclear instrumentation and control sector and highlights the work currently being done within IEC SC45A (Instrumentation reactor). More particularly, on projects dealing with software for computer in the safety systems of NPP, classification, the sector translation of the generic standards for the nuclear domain.

Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety

Gary Johnson, Lawrence Livermore National Laboratory, USA

The presentation comparing IEC and IEEE (Institute of Electrical and Electronics Engineers) standards, recognises that, if in the past the IEC and IEEE developed two sets of standards for I&C used in NPP, today, due to the shrinking of the market, the nuclear business is a global one and thus in this environment the harmonisation of the activities of these two bodies is vital. The contents of the two sets of standards are surveyed and opportunities to improve consistency between the two sets are identified.

The New IAEA Safety Guide and the Common Position of European Regulators on Software for Systems Important to Safety

Courtois Pierre-Jacques, Association Vinçotte Nuclear, Belgium

The presentation introducing the new IAEA safety guide on software important to safety and the European report on the common position of European regulators on the same subject gave an overview of some of the distinctive aspects of those two international documents which provide guidance on the design and licensing of computer based systems. It focused on their coherence and complementarities, on their strong and original points and on the issues left open.

Approach to the Application of the State Requirements, Legislation and Standards in Modernization of I&C Systems, Concerning Especially the Digital Computer-Based Systems
J. Zatloukal, P. Krakora, NRI Rez, Czech Republic

The licensing base for computer-based systems important to safety in NPP Temelin and NPP Dukovany was introduced in this presentation. The regulatory requirements for NPP Temelin were based on the US standards related to computer-based safety systems. The adoption of US standards came from the fact that Czech standards were addressed only to analog systems and not to the digital systems at the time when digital safety systems in NPP Temelin were decided to be adopted and subsequently US standards were introduced with the adopted digital system. Meanwhile, the regulatory requirements for NPP Dukovany were based on the Czech standards namely, "Set of USJB Positions" which was developed as the licensing base for implementation of digital safety systems. The licensing stage for digital safety systems in NPP Dukovany is still under way.

Standard Base for Regulatory Activity in NPP I&C Systems Area
M. Yastrebenetsky, V. Goldrin, Yu. Rozen, S. Vinogradskaya
State Scientific Technical Center on Nuclear and Radiation Safety, Ukraine

The standard base for regulation on digital I&C systems in Ukraine NPP was introduced, together with some samples of digital systems. The Ukraine standards are basically based on 3 dominant documents but these were harmonized with international standards and some foreign national standards. The criteria for digital application in I&C systems and the main features of the assessment methods for compliance with the criteria were also introduced.

During the **panel session** some important points were brought up:

First, the ***complexity of modern basic components*** (micro processors, compilers, graphic tools etc.) and the power of the tools used for safety demonstration of computer based systems (CBS) are increasing. Those two antagonist trends maintain the situation of balanced nuclear safety when introducing CBS in NPP. Today, as always, the absolute demonstration of safety of software is out of reach, the V&V of CBS is still an open and controversial question. Over the past ten years, CBS have been introduced in many NPPs in numerous countries without any major problems. This introduction was done using basic design rules (determinism proven by design, restricted use of component, rigorous QA…) to use generic component and it appears that this sound approach can be used and trusted to face the accelerating evolution of IT.

Secondly, the ***international context of standardisation*** is deemed to be complex, misleading and even disconcerting. Co-ordination between the different bodies would be valuable. In a first step the inconsistencies should be identified, a roadmap proposing the way to deal with them could be drawn. The responsibilities and relationships between the different bodies should be clearly defined.

Finally the problem of ***maintaining human competencies*** was raised. It appeared during the debate that there was no general consensus to answer that question and to guarantee that the skills necessary for the maintenance, the licensing activities related to the modifications concerning the CBS currently in operation will be there in the future. Nevertheless, some examples of measures taken by industrial companies are given based on defining long term contract to address the problem or in recruiting staff in different domain, automation for example and training them to IT.

TECHNICAL SESSION 2 REGULATORY ASPECTS

Session Chairmen: A. Lindner, K. Hamar

In the Technical Session 2 “Regulatory Aspects” four papers were presented. They dealt with the different aspects of regulations for digital safety I&C. The first paper describes the activities and the status of the generic pre-qualification of a digital platform, the second one includes an approach to investigate several licensing procedures and to derive from this investigation improved licensing procedures, the third paper deals with the collection of data from the operational experience of computer-based I&C systems and the last one describes digital projects in Hungary and their consequences with respect to safety regulation.

PRE-QUALIFICATION OF DIGITAL PLATFORM – U.S. NRC REGULATORY REVIEW OF THE COMMON Q PLATFORM

W. K. MORTENSEN, M. CHIRAMAL

The Common Q platform is a computer system consisting of a set of commercial-grade hardware and previously developed software components dedicated and qualified for use in nuclear power plants. The Common Q platform is to be loaded with plant-specific application software to implement various nuclear plant safety system applications. The basis of pre-qualification is compliance with the NRC-approved EPRI Topical Report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications". The NRC staff reviewed the basic operation of the system, life cycle process and documentation associated with the Common Q hardware and software. The procedure was introduced by the lecturer as a type testing procedure, where the outcome also declares legal statements about the compliance with key requirements in the US, 10CFR50 appendix “B”, about quality assurance. The staff has completed the review of the qualification of nearly all of the Common Q platform components and the staff’s evaluation of the completed activities has been documented in the safety evaluation report (SER) issued on August 11, 2000.

Survey and Evaluation of Digital I&C Licensing Experience

Swu Yih, Chin-Feng Fan, Chan-Fu Chuang

This paper describes the licensing experiences of digital I&C systems based on USNRC regulations for Taiwan’s fourth NPP (Lungmen Project). The contents consist of three parts. In the first part, it is described how the licensing process was conducted, how the licensing strategy was adopted, and how the manufacturers, utility, consultant companies and regulators interact. Some statistics of licensing- related activities and events listed in chronological order are also presented to help understand the scope and complexity of this licensing. In the second part, the paper describes an in-depth analysis of USNRC digital I&C regulations. The internal logical structure, strengths and weaknesses of those regulatory codes, guides, and standards are investigated to identify the efficiency shaping factors. In the third part, modifications are proposed for the current regulation structure and regulation practice. These modifications may improve the current digital I&C licensing efficiency and effectiveness. There was a presentation of a licensing process model which can be used to evaluate the effectiveness of different licensing approaches. The original USNRC regulations and proposed modifications are then evaluated under this model to show the improvement of efficiency.

Collecting Data from Operational Experience of Computer-Based I&C Systems – A Regulatory Perspective on Goals and Tasks
G. Schnürer, F. Seidel

The paper deals with the methods and goals of the collection of data from computer-based I&C systems which are developed, qualified and maintained using a unique platform. The main goal of the data collection is to contribute to the further qualification of these systems by the evaluation and optimization of the qualification procedure, demonstration of the achieved systems' dependability and utilizing the experience of the system applications of lower safety significance within the licensing procedure for computer-based systems important to safety. The content of the records and the evaluation methods for operational experience should have been agreed by the involved experts of the licensees, manufacturers, technical support organizations and regulatory bodies. Not only the failures and the reported events are of interest, but also periods of operation without significant failures. As a long-term goal of the collection of operational experience, the achieved performance of the system might be estimated in quantitative terms. To calculate the reliability, it is crucial to establish an evaluation model in order to identify the necessary parameters as early as possible and to collect them continuously during the operation.

Digital Projects In The Near Past And Their Consequences In Safety Regulations In Hungary
K. Hamar

The paper describes from the regulatory point of view the operational experiences with digital I&C systems in Hungary. There are systems with different importance to safety used like reactor protection systems, core monitoring systems, process computers and others. Errors and problems of the digital systems and related components are listed. The lecturer emphasises the great importance of type testing for the successful licensing of the Teleperm XS system as a reactor protection system for the NPP Paks. From the ongoing licensing processes it can been seen that qualification of class "B" (following IEC 61226) may be more difficult, because of more complex static and dynamic system properties of class "B" systems. As the most important system property, the deterministic behaviour is identified. The existing experiences will be addressed in the new Hungarian safety regulations.

DISCUSSIONS AND CONCLUSIONS, SESSION 2:

During the discussion of the papers, questions regarding some of the details of the presentations were dealt with. In particular, several aspects of the model for the licensing process, presented in the second paper, were discussed. Establishing a model of the licensing process seems to be an interesting approach, but further work is necessary.

Compared to the last meeting in 1996 in Munich the great progress in the application of digital computer-based I&C systems was evident. Future problems from the regulatory point of view refer to both the adoption of the established qualification methods for software-based I&C systems to new developments in software technology and to the improvement of the licensing procedures. Collecting and evaluation of operational experience of computer-based systems will be helpful for the evaluation of reliability characteristics of such systems and devices.

The following conclusions could be drawn:

1. Type testing is an important and desired institution in licensing, beneficial for licensees, and regulatory bodies, and hopefully for developers and manufacturers, too.

2. The efficiency of the licensing process may promote or suppress the utilization of digital technology.

3. The regulator behaves as a transformer between the ”evidence” and the “confidence”.

4. The conservative approach is still present in the licensing, and the licensees and the developers are not satisfied with it. They are waiting for relaxation, and searching for the feasible techniques to support it.

5. Safety is manifest in a set of system properties, like deterministic behaviour, constant system load, simplicity, transparency, etc. At the same time, these are the “easy to license” system properties. The simplicity is in contradiction with nearly all of the another system characteristics: functionality, testability, diversity.

6. The SW reliability data collection suffers that loss, if the reported events and error cases are dependent on the licensee event reporting systems. If reporting criteria do not meet, the result is that the statistically valuable cases remain hidden.

7. From the aspect of data collection efficiency, the comparable operational profile and the unique platforms are desired.

TECHNICAL SESSION 3 ANALYSIS AND ASSESSMENT OF DIGITAL I&C SYSTEMS

Session Chairmen: M.L. Järvinen, M. Kersken

The following five papers were presented:

Preliminary Evaluation of computerized procedure from safety viewpoints

Yun H. Chung, Sung N. Choi, Bok R. Kim, KINS

The paper presents the preliminary safety assessment made to the Computerized Procedure Systems (CPS) to be implemented at the Korean Next Generation Reactor, which is planned to start commercial operation in 2010. The computer-based procedures are being used at various nuclear power plants. This change can support and enhance the operators' performance and safety. However there are safety issues which should be discussed when implementing these systems such as the impact on operators and shift performance, situation assessment and response planning, handling of complex situations particularly in failures of the CPS and change over to paper-based procedures, design for navigation and communication and software quality. The paper presents the preliminary assessment results.

MODERNIZATION OF THE I&C SYSTEM FOR ANP DUKOVANY BY THE USE OF COMPUTER-BASED EQUIPMENT

Jean Pierre Burel, Schneider El., F. Dalik, K. Wagner, M. Říš, ŠKODA
Jean-Paul Mauduit, Framatome-ANP

The paper describes the replacement of existing systems important to safety (category A and B) by computer based systems which are realized by SPINELINE 3 technology. Special parts of the system are units executing functions connected directly with the VVER reactor technology; these are developed by means of an industrial microcomputer-based system as used by Skoda. The features of SPINLINE 3 and Skoda technology are described with emphasis on their contribution to safety.

FMEA performed on the SPINLINE 3 operational system software as part of the Tihange 1 NIS refurbishment safety case

L. Ristord, C.Esmenjaud, Schneider El. Industries

The paper presents the FMEA analysis made for the new Tihange 1 Nuclear Instrumentation System which became operational in March 2001. The choice of the software based technology raised the issue of the risk of a CCF due to the use of the same software in redundant independent units. In addition to the demonstration of the application of the safety requirements for the software in safety systems, a FMEA oriented towards the significant CCF risk was required as part of the safety case. The paper presents the FMEA experience, including the adaptation of the principles of FMEA to the analyses of the software, an approach to identify the components to be analyzed, definitions of the software failure modes associated with the components, examples of the analyses performed on the operational system software and feedback of the experience. Performing the FMEA has proven to be a good way to discuss in depth safety aspects of software based systems.

Qualification of pre-developed software for safety-critical I&C application in NPP's
M. Kersken, ISTec Garching

Implementation of I&C functions important to safety in nuclear power plants are increasingly realized with computer-based systems, i.e. by its software. These so called equipment families are often used to develop these I&C functions. Extensive research work has been made, mainly during last ten years, to tackle the problem of qualifying pre-developed software to be included in the systems important to safety. Due to the great variety of software types and differences in the applications, no unique solution has yet been developed. The objective of the paper is to provide a set of staggered criteria for the qualification of pre-developed software to be used in different categories for the safety critical I&C. An attempt is made to demonstrate an exemplary procedure as to how the different approaches can be brought together, to form a useable set of staggered criteria for the acceptance of the pre-developed software. The first examples show that there will be no principal difficulty for a unified approach, because there are no major contradictions in the requirements or recommendations of the analyzed documents. The acceptance of such a unified procedure, however, needs the involvement of a broad international group of experts.

A Bayesian approach to risk informed performance based regulation for digital I&C QA programs
Swu Yih, Sun-Li Chyou, Li-Sing Wang, AEC INER,
Chin-Feng Fan, Yuan-Ze University

A proposal for a systematic way to reduce unnecessary conservatism in regulatory processes is given. Bayesian Belief Networks BBN are applied as a modelling technique to describe the assessment processes as e.g. independent V&V.
The method first enumerates major influence factors, and constructs the BBN for system risk; an event tree based on same influence factors is then generated. Tree trimming is performed to delete the impossible branches and thus control the exponentially explosive problem in the event tree construction. The numbers of occurrences of final outcomes of the tree are then counted to draw the risk profile graph. The graph can help in identifying the potential areas of unnecessary conservatism. It can also help in determining whether the resulting outcomes of proposed QA program changes are acceptable or not.

CONCLUSIONS FROM SESSION 3

As can be seen from these topics, the session comprised a quite large variety of analysis techniques which can be applied to computer-based systems in I&C important to safety. These reached from review and evaluation of computerized operating procedures for future reactors (Korea) to constructive and analytical techniques which are applied at the moment during the replacement of systems important to safety in an actual plant (Czech Republic). The application of FMEA to computer based technology (Belgium), especially to software, is quite innovative, and has been used in a safety demonstration to show low risk of common cause failure due to software.

A practical systematic approach for an acceptance procedure for pre-developed software was proposed. This approach was based on widely discussed international documents concerning this topic. Another proposal which dealt with the assessment of the effectiveness of regulation procedures based on modeling via Bayesian Belief Networks is highly interesting, because this may be a sound basis for directing the limited resources which can be spent during the development and safety demonstration of computer-based systems important to safety into the most effective combination of techniques which should be applied.

The session did not focus so much on an independent verification and validation IV&V. Discussions after this and other sessions showed, however, that IV&V has an important role in the safety demonstration, but the focus and methods can still be further developed. The application of different tools and methods - as against those which are used in V&V during development – can bring additional assurance to the safety

demonstration. The use of pre-qualified software and the associated IV&V can be one of the ways of reducing the costs of the safety demonstrations. Also in this area future work is needed in the international community.

With respect to this variety of techniques which were presented in the session and their actual or envisaged application in the near future, the session reflects an image of the whole workshop. In most of the sessions there were possibilities to exchange experience of applying well known constructive and analytical techniques to actual implementations of computer based technology. Other contributions, however, were more directed towards opening the door for new applications by providing proposals for their assessment. This mixture of direct application-oriented presentations on the one hand and others oriented towards the near future on the other side, made the workshop very valuable for the experts working in the field of I&C important to safety.

The information also provided new guides and standards for computer-based technology important to safety, which was very helpful, because this gives a better feeling of the internationally agreed principal regulatory requirements.

TECHNICAL SESSION 4: SOFTWARE LIFE CYCLE ACTIVITIES

Session Chairmen: G. Dahl , F. Krizek

The overall theme of the session was the description of the V&V methods used in the licensing process for NPPs. This includes both the methods which have been used and methods planned to be used in NPPs in Taiwan, the Czech Republic and Ukraine. Four papers were presented:

Implementation of Software Independent Verification and Validation for Lungmen Distributed Control and Information Systems
Jiin-Ming Lin, Jeen-Yee Lee, Taiwan Power Company

Static Analysis of the Software Used in Safety Critical System of the NPP Temelin
Piroutek Z., Roubal S., Rubek J., I&C Energo a.s., Czech republic

Assessment Methodology of the Temelin NPPControl System Performance and Quality
Ivan Petruzela, Karel Bednarík, CEZ a.s.,, Czech republic

Methodology of NPP I&C System Algorithms and Software Expert Analysis
V.S. Kharchenko, L.M. Lyubchik, M.A., Yastrebenetsky State Scientific Technical Center on Nuclear and Radiation Safety, Ukraine

The first paper, presented by Jeen-Yee Lee from Taiwan Power Company (TPC), dealt with the implementation of the software independent verification and validation (IV&V) for the Distributed Control & Information Systems of the Lungmen NPP. It covered the codes and standards as applicable, the scope of the software IV&V and the documents reviewed, the organisational structure and activities for performing the IV&V work. Teams from GE and TPC performed software V&V for the Lungmen project, based on the USNRC Standard Review Plan Chapter 7, BTP-14 and USNRC Regulatory Guide 1.168 respectively. Two recommendations for performing future software IV&V activities can be made on the basis of the experiences so far. One is to fully understand the regulatory requirements on software IV&V before an IV&V project gets started. The other is to establish a tracking system for IV&V activities in IV&V project to facilitate control and monitoring of the issues identified.

The next two papers described the methods used in the evaluation of safety critical software at the Temelin NPP. The first paper, presented by J. Rubek from I & C Energo s.r.o, gave an overview over the static analysis methods used in this process. The method used was influenced by the one used for the licensing of the Sizewell B protection system, although it is not a direct copy. For the analysis they used the tool MALPAS for analysis of control flow, data use, information flow and semantic compliance. The approach used was cost consuming, but made it possible to discover software anomalies which could be not found in manual check.

In the other Temelin paper, presented by I. Petruzela, also from I & C Energo, described assessment methodology of the control system performance and quality. A methodology has been developed in I&C Energo for the test assessment of the control process quality. This is based on the evaluation of the

behaviour of the main controlled quantities in the course of transients of the test. A set of criteria is defined which serve to check the performance of the Temelín NPP unit control against the design. They determine the borders of the area in which the numeric values of the assessed parameters should vary if the work is made in compliance with the design. The fulfillment of the criteria makes it possible to determine the achieved quality of the NPP Temelín unit major controllers after the completed test.

The fourth paper, presented by V. Kharchenko from the State Scientific and Technical Center on Nuclear and Radiation Safety in Ukraine, described a methodology for verification and validation and expert analysis of algorithms and software in I&C systems. The method was approved for application in Ukrainian NPP, and was in particular applied during the evaluation of the computer-based control system ASUT-1000M for Zaporozhey NPP.

These papers gave a valuable contribution to the workshop as they presented methods actually applied in the licensing of safety critical I&C systems in different NPPs, and that they cover complementary aspects of the licensing process, from general principles to more detailed techniques.

TECHNICAL SESSION 5 EXPERIENCE WITH APPLICATIONS, ASPECTS, POTENTIAL SYSTEM LIMITS AND FUTURE TRENDS AND NEEDS

Session Chairmen: B. Liwång, M. Hrehor

Operating Experience of Digital Safety-Related System of Kashiwazaki-Kariwa Unit No. 6 and 7

Makino Shigenori, Tokyo Electric Power Company

The paper presented the development of digital safety systems for the Kashiwazaki-Kariwa Unit 6 & 7. Digital control and network systems has been applied to the I&C systems of Japanese BWR's since the 1980s. The introduction has been stepwise and the scope of the application has been widened gradually. Based on the experience almost all of the I&C systems, including the safety-related systems, were finally digitised in K-6/7. The system consists of 4 divisions with a 2 out of 4 logic. As for the consideration for common mode failures, some hard-wired back-up countermeasures were installed.

In the paper the development process and the different activities for the V&V were presented. In the validation process, the semi-dynamic simulation tests were also performed additionally to investigate the integrity for system requirement.

The NUREG/CR-6430 introduced several techniques for the hazard analysis. TEPCO performed the hazard analysis utilising the FTA methodology.

For the top hazard two events was defined; failure to initiate trip signal on request and unnecessary (erroneous) trip signal without request. For each of these the underlying structures were developed step by step until the bottom hazard elements were identified. Each of the identified bottom elements were examined against their verification process.

The conclusions from the experience from the performed development, installation and operation is that the following policies should be applied to digital safety systems:

- utilisation of digital systems with good performance and operating experience
- simple software architecture
- static memory allocation, avoidance of external interrupts etc.
- use of graphical language in order to keep transparency and traceability
- modularization of the software for its reuse and effective V&V
- considerations for common mode failures and suitable backup measures

Technical Requirements on Maintenance of Digital I&C Systems Important to Safety
G. Schnürer, ISTec, Garching
F. Seidel, BfS, Salzgitter, Germany

The paper presents work which has already started in Germany.

The paper deals with the necessity of requirements on maintenance and upgrading of safety relevant digital I&C systems as a basis for the elaboration of proper maintenance and upgrade guidelines. Requirements which are treated and discussed are technical solution-oriented versus guidelines so as to have an overall general character. The adoption of existing rules and guidelines is also taken into account for the definition of these additional requirements for safety relevant I&C.

The goal of the paper is the introduction of possible safety relevant requirements with respect to
- maintenance of digital safety relevant and safety I&C
- tracing and route cause analysis of incidents caused by I&C maintenance
- support the regulatory body as well as technical experts concerning state of the art

In the paper it is shown that the international standard IEC 60880 contains the necessary elements for an acceptable modification process and discussed some areas of special interest for handling modification requests, including the configuration management system.

As a summary the following aspects are to be considered:

- Completeness and applicability of the existing requirements concerning maintenance and upgrading of digital safety systems.

- Software maintenance requirements for systems of lower safety categories.

- Maintenance requirements concerning automatically generated software.

Requirements Management of I&C System Refurbishment of NPP Dukovany
Jiri Pliska, I&C Energo a.s., Czech republic

Using an example of the Requirements Management System as implemented in the project "I&C System Refurbishment for NPP Dukovany" the paper presented the system analysis methods and the corresponding tools – generally designed CASE systems as a necessary preconditions for the organisation, management, co-ordination, inspection and evaluation of the extensive project, both from the viewpoint of the contractor and customer, as well as from the viewpoint of the national regulatory body. It is a tool for systematic identification, requirement structuring, communication, control, monitoring and verification of user requirements.

The system is based on a list of individual requirements. The user requirements are organised within a hierarchical structure which observes the structure of the application area. Individual requirements are mutually interrelated in various ways. Each requirement is expressed in the form of a written description. Some significant features of the requirements are clearly and simply expressed with a set of assigned attributes. The practical experience has proven that a good CASE system provides many more options for solutions in Requirements Management Systems than common specialised tools.

The entire system of requirements is in the HTML format represented with 14 000 files with the total size of 50 MB. Any evaluation or sorting takes from several seconds to several minutes. The most time-consuming is fulltext search, taking less than 10 minutes in the whole system. When limiting conditions are used, the search is significantly faster.

Licensing Process of the Digital Computer-based I&C Systems to be Implemented within the NPP Dukovany I&C Refurbishment Project
Ceslav Karpeta, Scientech Inc. - CR, Josef Rosol, CEZ a.s., Czech republic

The paper provided a brief outline of the NPP Dukovany I&C system refurbishment project with a particular focus on specific regulatory requirements related to the digital I&C systems and ways which the utility has adopted in order to ensure that these requirements are met. The licensing process applied to the refurbishment of the Dukovany NPP I&C system is structured to the several stages with the final objective of obtaining the regulatory permission for permanent operation of the refurbished unit. Also, an overall quality assurance programme was established in line with the regulatory requirements covering processes, activites, products, organizations, personnel, etc. The utility intends to perform various audits in order to ensure that the installed equipment will operate as intended, and to provide information needed to support the licensing process. An Audits Plan has been developed to provide the basis for those activities.

Temelin Nuclear Power Plant Westinghouse -I&C Change Process
Dennis M. Popp, John. L. Duryea, USA

During the course of the I&C Systems upgrade at Temelin NPP numerous engineering changes were incorporated in the design and then implemented onsite. From the early stages of installation, Westinghouse has implemented a controlled process to manage these changes. Since the onset of commissioning, Westinghouse has adapted a flexible approach to managing this change process so as to be responsive, during various upgrade efforts, to the needs of the Czech design organizations, as well as those of the start up team. The paper provided an outline of the development of this process.

Under the change process, all modifications to the various digital systems are reviewed to ensure that correct system functionality is maintained and integrated with other plant systems, regulatory requirements, commitments and software configuration controls.

C PROGRAMME

CNRA/CSNI WORKSHOP ON

LICENSING AND OPERATING EXPERIENCE OF COMPUTER-BASED I&C SYSTEMS

Hluboká nad Vltavou, Czech Republic
25-27 September, 2001

Tuesday, 25 September 2001

08:00 - 09:00	**Registration and Coffee**	
09:00 - 09:10	**Welcome**	**P. Krs** **SUJB, Deputy Chairman** **Mr. Krizek - CEZ a.s.**
09:10 - 09:20	**Introductory Remarks**	**M. Hrehor -OECD/ NEA**
	OPENING SESSION: **ADVANCES MADE IN THE USE AND PLANNING OF COMPUTER-BASED I&C SYSTEMS**	**Chairmen:** **M. Chiramal** **P. Krs**
09:20 - 09:50	**Electricité de France Experience of computer-based I&C systems** Poizat Francois, EdF	**FRANCE**
09:50 - 10:20	**The Evaluation on Applying the Digital Safety System to Existing PWR Plants in Japan** J Masafumi Utsumi, Mitsubishi HI Ltd Yoichi Mito, Kansai Electric Power	**JAPAN**
10:20-10:40	**Coffee Break**	
10:40 - 11:10	**Independent Assessment of the Temelín Software Safety System** Petr Závodský, CEZ a.s.,	**CZECH REPUBLIC**
11:10 - 11.40	**Regulatory Review of the Digital Plant Protection System for Korea Next Generation Reactor** D. I. Kim, B. R. Kim and S. H. Oh Korea Institute of Nuclear Safety	**REP. OF KOREA**

11.40 - 12.10	**Decision Support for Approval of Safety Critical Programmable Systems** Gustav Dahll, Bjørn Axel Gran OECD Halden Reactor Project Bo Liwång, Swedish Nuclear Power Inspectorate	**OECD/HALDEN/SWEDEN**

TECHNICAL SESSION 1

	NATIONAL AND INTERNATIONAL COMPUTER-BASED STANDARDS AND GUIDES FOR SAFETY SYSTEMS	**Chairmen:** **J.P. Bouard** **Z. Ogiso**
14:00 - 14:30	**International Standardisation in Nuclear I&C Engineering** Bouard Jean-Paul, EdF	**FRANCE**
14:30 - 15:00	**Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety** Gary Johnson, Lawrence Livermore National Laboratory	**USA**
15:00 - 15:30	**The New IAEA Safety Guide and the Common Position of European Regulators on Software for Systems Important to Safety** Courtois Pierre-Jacques, Association Vincotte Nuclear, Brussels	**BELGIUM**
15:30-15:50	**Coffee Break**	
15:50 - 16:20	**Approach to the Application of the State Regulatory Requirements, Legislation and Standards in Modernization of I&C systems, Concerning Especially the Digital Computer-Based Systems** J. Zatloukal, P. Krakora, NRI Rez	**CZECH REPUBLIC**
16:20 - 16.50	**Standard Base for Regulatory Activity in NPP I&C Systems Area** V. Goldrin, M. Yastrebenetsky Yu. Rozen, S. Vinogradskaya State Scientific Technical Center on Nuclear and Radiation Safety	**UKRAINE**
16:50 - 18:00	**Discussion Opening Session & Session 1**	

Wednesday, 26 September 2001

TECHNICAL SESSION 2 — **REGULATORY ASPECTS** — **Chairmen: K. Hamar, A. Lindner**

09:00 - 09:30	**EMI/RFI and Power Surge Withstand Guidance for the U.S. Nuclear Power Industry** Christina Antonescu, U.S. NRC Paul D. Ewing, Richard T. Wood Oak Ridge National Laboratory	**USA**
09:30 - 10:00	**Pre-Qualification of Digital Platform - U.S. NRC Regulatory Review of the Common Q Platform** W. K.Mortensen, M. Chiramal**,** US NRC	**USA**
10:00 - 10:30	**Survey and Evaluation of Digital I&C Licensing Experiences** Swu Yih, INER, AEC Chin-Feng Fan,Yuan-Ze University Chan-Fu Chuang,, Nuclear Regulation Division, AEC	**CHINESE TAIPEI**
10:30-10:50	**Coffee Break**	
10:50 - 11:20	**Collecting Data from Operational Experience of Computer-Based I&C Systems- A Regulatory Perspective on Goals and Tasks** G. Schnürer, ISTec, Garching F. Seidel, BfS), Salzgitter	**GERMANY**

11:20 - 11:50	**Digital Projects in the Near Past and their Consequences in Safety Regulations in Hungary** K.Hamar, HAEC	**HUNGARY**
TECHNICAL SESSION 3	**ANALYSIS AND ASSESSMENT OF DIGITAL I&C SYSTEMS**	**Chairmen:** **M.L. Järvinen** **M. Kersken**
13:30 - 14:00	**Preliminary Evaluation of Computerized Procedures From Safety Viewpoints** Yun H. Chung, Sung N. Choi, Bok R. Kim, KINS	**REP. OF KOREA**
14:00 - 14:30	**Modernization of the I&C System for ANP Dukovany by the Use of Computer-based Equipment** Jean Pierre Burel, Schneider El., F. Dalik, K. Wagner, M. Říš, ŠKODA Jean-Paul Mauduit, Framatome-ANP	**CZECH REPUBLIC/ FRANCE**
14:30 - 15:00	**FMEA Performed on the SPINLINE3 Operational System Software as Part of the TIHANGE 1 NIS Refurbishment Safety Case** L. Ristord, C.Esmenjaud, Schneider El. Industries	**FRANCE**
15:00-15:20	**Coffee Break**	
15:20 - 15:50	**Qualification of Pre-Developed Software for Safety-Critical I & C Application in NPP's** M. Kersken, ISTec Garching	**GERMANY**
15:50 - 16:20	**A Bayesian Approach to Risk Informed Performance Based Regulation for Digital I&C QA Programs** Swu Yih, Sun-Li Chyou Li-Sing Wang, AEC INER, Chin-Feng Fan, Yuan-Ze University	**CHINESE TAIPEI**
16:20 - 17.30	**Technical Discussion Sessions 2& 3**	

Thursday, 27 September 2001

TECHNICAL SESSION 4	**SOFTWARE LIFE CYCLE ACTIVITIES**	**Chairmen:** **G. Dahl** **F. Krizek**
09:00 - 09:30	**Implementation of Software Independent Verification Distributed Control and Information Systems and Validation for Lungmen** Jiin-Ming Lin, Jeen-Yee Lee, Taiwan Power Company	**CHINESE TAIPEI**
09:30 - 10:00	**Static Analysis of the Software Used in Safety Critical System of the NPP Temelin** Piroutek Z., Roubal S., Rubek J. I &C Energo a.s.,	**CZECH REPUBLIC**
10:00 - 10:30	**Assessment Methodology of the Temelin NPP Control System Performance and Quality** Ivan Petruzela, Karel Bednarík I &C Energo a.s.,	**CZECH REPUBLIC**
10:30-10:50	**Coffee Break**	
10:50 - 11:20	**Methodology of NPP I&C System Algorithms and Software Expert Analysis** V.S. Kharchenko, L.M. Lyubchik M.A., Yastrebenetsky State Scientific Technical Center on Nuclear and Radiation Safety	**UKRAINE**

TECHNICAL SESSION 5	**EXPERIENCE WITH APPLICATIONS SYSTEM ASPECTS, POTENTIAL LIMITS AND FUTURE TRENDS AND NEEDS**	**Chairmen: B. Liwång M. Hrehor**
11:20 - 11:50	**Operating Experience of Digital Safety-Related System of Kashiwazaki-Kariwa Unit No. 6 and 7** Makino Shigenori Tokyo Electric Power Company,	**JAPAN**
11:50 - 12:20	**Technical Requirements on Maintenance of Digital I&C Systems Important to Safety** G. Schnürer, ISTec, Garching F. Seidel, BfS, Salzgitter	**GERMANY**
13:30 - 14:00	**Requirements Management of I & C System Refurbishment of NPP Dukovany** Jiri Pliska, I&C Energo a.s.,	**CZECH REPUBLIC**
14:00 - 14:30	**Licensing Process of the Digital Computer-based I&C Systems to be Implemented within the NPP Dukovany I&C Refurbishment Project,** Ceslav Karpeta, Scientech Inc. - CR Josef Rosol, CEZ a.s	**CZECH REPUBLIC**
14:30 - 15:00	**Temelin Nuclear Power Plant Westinghouse -I&C Change Process** Dennis M. Popp, John. L. Duryea	**USA**
15:00 - 16:00	**Technical Discussion Sessions 4 & 5**	
16.00 - 16.20	**Coffee Break**	

16:20 –17:20	**FINAL PLENARY SESSION/ Workshop Summary**	**Chairman: M. Chiramal**
	Conclusions by Session Chairmen	
17:20 - 17:30	**Concluding Remarks & Adjourn**	**P. Krs (SÚJB)**

19:00 - 21:00 **Meeting of the Session Chairmen to summarize conclusions and recommendations**

Friday, 28 September 2001

09:00 - 12:00 **Visit of NPP Temelin**

OPENING SESSION:
ADVANCES MADE IN THE USE AND PLANNING OF COMPUTER-BASED I & C SYSTEMS
Chairmen: M. Chiramal, P. Krs

EDF experience in computerized instrumentation/control

F. POIZAT, EDF Industry/Basic Design Department,
12-14 avenue Dutrievoz, 69628 Villeurbanne Cedex, France
Tel.: +33 4 72 82 74 79, Fax: +33 4 72 82 77 04, e-mail/francois.poizat@edf.fr

Summary

EDF gradually swapped from electromagnetic relay based I&C systems, used on the 900Mwe NPP series (exclusive use, if we put aside the operator and maintenance aids), to fully computerised and integrated I&C systems, on the new French 1450MWe NPP series (including all the protection systems, control systems and MMI systems).

This change, directly induced by the pervasive growing use of computerised systems in all the domains, raises new problems for their use in nuclear industry : Verification and Validation, as well as timelessness. For those matters, end 1999, a new Basic Safety Rule dedicated to the use of software in NPP safety classified systems was published by the French Safety Authorities.

Our presentation will trace back those changes, considering the problems faced, some of them having been unveiled during the recent refurbishment of the Fessenheim 900MWe plant Nuclear Instrumentation System based on the SPINLINE 3 product line, developed by Schneider Electric and Framatome.

It's now clear that the current trend to use COTS to develop NPP safety systems shall take into account in a cost effective way the absolute safety requirement, not to degrade the dependability of systems aimed at assuring the NPP safety.

Introduction

The second half of the century which just ended was marked, on the scientific and industrial fronts, by the coming to maturity of two new technologies: nuclear energy and information technology (IT). The nuclear power industry was obviously closely affected by the fantastic technological development represented by the post-war advent of the first computers and, afterwards, by the proliferation of digital systems in all human activities: plant design, equipment production, automatic controls and safety features for industrial processes, communications, project management and plant operation. Nothing is done today without IT.

Seventies: from Fessenheim 1 to Chinon B4 (900 MW CP0, CP1 and CP2 plant series [1])

All the same, the first nuclear power plants did not adopt digital technology from the outset. EDF, it should be said, had a few unhappy experiences, particularly the attempt to install static relay circuitry in the fossil-fired power plant of Montereau in the sixties, or the many innovations (probably premature) at the solar power plant of Targasone in the seventies [2].
Accordingly, the first French PWR units were not computerized, at least for the control of the physical process (fission and conversion into electricity) provided by levels 0 to 2 [3]. As a result:

- The process instrumentation ("level 0") uses standard-technology sensors (measurements and monitoring) and actuators (pumps and solenoids) ;
- "Level 1" is divided between automatic control by On-Off actions (and, first of all, the reactor protection circuits and the Turbine Generator Set), on the one hand, and the reactor control systems and the turbine (to ensure power output matches grid power demand) on the other: automatic control is provided by the electromagnetic relay circuitry, while the control cabinets feature ANAlog technology (Control-Bailey modules 8720 or 9020, Alsthom REC 70 in particular);
- the control room ("level 2") makes available to the operators strip recorders and galvanometric indicators for tracking, flashing windows and horns for alarms, selector keys, pushbuttons (the well-known backlighted pushbutton switches) and potentiometers (Auto-Manual Control Stations, Setpoint Stations) for controls, all on standard consoles.

The only breakthrough, the former "status recorder", an indispensable tool for retroactive analysis of any operating incident, made its control room appearance in the computerized and improved form[4] of centralized data processing (CDP). Supplied by software service companies specializing in the energy field, this CDP only participates in real-time plant control by differentiating between the alarms grouped in the same window. As it consists of a plant control aid, it is on the boundary with "level 3" [5].

[1] The 900 MW **C**ontract **P**rogramme was made up of three plant series:

- the 6 units of **CP0**: Fessenheim 1-2 and Bugey 2-5 ;
- the 18 units of **CP1** : Tricastin 1-4, Gravelines 1-6, Dampierre 1-4, and Blayais 1-4 ;
- and the 10 units of **CP2** : St Laurent B1-2, Chinon B1-4 and Cruas 1-4.

For the 1300 MW power plants, a distinction is made between two PWR **4**-loop plant series:

- the 8 units of **P4** : Paluel 1-4, St Alban 1-2 and Flamanville 1-2 ;
- and the 12 units of **P'4**: Cattenom 1-4, Belleville 1-2, Nogent 1-2, Penly 1-2 and Golfech 1-2.

The 1450 MW series (or N4, as in **N**ew **4**-loop) is made up of Chooz B1-2 and Civaux 1-2.

[2] But the "UNGG" units (Natural Uranium, Graphite and Gas) were nevertheless given plant control computers ...

[3] Bear in mind that the Westinghouse PWR license originally left only a small share for automatic controls.

[4] The histories, diagrams etc did not exist in the status recorders.

[5] As a result, some classify it as level 2.

The latter level[6], which groups together "constraint time" data processing systems, is not subject to the operating and safety requirements which govern real time. This is probably why these systems were favorable for computerization experiments (Tagging System, Event Counting, grid follow, environmental monitoring, ...) from the very first 900 MW units.

Emergence of programmable controllers in the process: SPIN, Controbloc, ... , KIC/N4

The flexibility offered by IT soon attracted the attention of French I/C system designers (including CEA and Framatome), for two reasons:

- the need to improve knowledge of physical parameters, and therefore the operating conditions (particularly for increasing reactor operation margins). This led to the development, by Merlin-Gerin (the future Schneider-Electric), of the first Digital Integrated Protection System (SPIN), based on Motorola 6800 microprocessors. However, emphasis should be laid on the boldness of the manufacturers, who gradually developed by themselves the whole array of digital I/C systems required by their processes, both for the logic of the so-called auxiliary systems (CGEE-Alsthom created the range of Controbloc programmable controllers for this purpose) and for the control channels (Micro-Z and µREC in the 1300 MW plant series).
- the Three Mile Island accident, which highlighted the safety and human factor aspects, was the catalyst for the program baptised S3C (Control Room and I/C combined with simulator) leading to the N4 concept: its total computerization, including plant control procedures, makes Chooz B and Civaux the flagships of the computerized units.

The attached table briefly summarizes and illustrates this trend, from two "time-based" standpoints: history (plant series) and data processing speed (corresponding to the I/C levels).

[6] A field which must be distinguished from the huge field of office automation: there are several hundred applications, most local, but all disconnected from the process ("level 4" ?).

Plant series:	**CP0 / CP1 / CP2**	**P4**	**P'4**	**N4**
Levels :	34 **900 MW** units	20 **1300 MW** units		4 **1450 MW** units
Level 0: instrumentation	Standard technology	Standard technology		Standard technology
Level 1:				
Automatic controls	Electromagnetic relays	Controbloc (CGEE-Alsthom)		Contronic-E (Hartmann & Braun)
Reactor protection circuits	Electromagnetic relays	SPIN (Merlin-Gerin)		SPIN (Schneider-Electric)
Reactor control systems	Analog electronics	Analog elect.	Micro-Z	Contronic-E (Hartmann & Braun)
Turbine protection/control	REC-70 (Alsthom)	REC-70	µREC	µREC (Alsthom)
Level 2:	Standard control room	Standard control room		"KIC" (Sema-Group) :
Tracking	recorders/indicators/windows	recorders/indicators/windows		Screen images
Controls	keys, backlighted pushbutton, auto-manual control station ...	keys, backlighted pushbutton, auto-manual control station		Interactive images
Procedures	manual	manual		computerized
Level 3:				*Functionalities incorporated*
Status recorder	"KIT-KPS" (Sema-Group)	"TCI" (Sema-Group)		*in KIC above*
Other systems	Many digital monitoring, maintenance, management applications ...			

Current trends

Revamping

The first I/C revamping operations are all aimed at computerization, at least partial. Such projects abound, right across the world. Some systems which have become obsolescent have to be replaced by digital systems. As a result, this topic is giving rise to intense standard-related activity (followed up by the IAEA and the International Electrotechnical Commission).
In France, two projects focussed thinking on possible I/C revamping of units prior to N4:

- The project baptised R2C and centering on the second ten-year inspection programs (VD2) of the 900 MW units (from 1998-1999) only led to two modifications, limited to the oldest units of Fessenheim and Bugey (CP0). It involves the steam generator level control (revamp based on Alstom's P320), and the flux measurement and nuclear protection system (RPN system), which inaugurated Schneider-Electric's new product line SPINLINE 3. It can be seen that technical and economic caution has, until now (the first units of the CP0 and CP1 plant series have just experienced their VD2), won out over innovation as long as the durability of the "old" relay-based systems is not threatened.
- The ACCORD program, aimed at the VD2 of 1300 MW plants, did not lead to spectacular decisions either. At the most, consideration is being given, on the eve of the second ten-year inspection program, to identifying spare (or repair) solutions for a given board thought fragile in Controbloc, or replacing the CDP, whose maintenance is becoming costly, by a commercially available supervision system.

EDF's comparative caution towards large-scale revamping is due in particular to its specific situation as sole operator of a pool of 58 units, characterized by a strong plant series effect (similarities and even absolute identities between units). Owing to its specific position, it very early (the R2C delivered its first verdict in 1995) reviewed equipment and system ageing and obsolescence issues and deduced coherent, industrial-scale action programs. Regarding I/C, the main focus is on the building of strategic storage areas, the contracting of durability agreements with the main suppliers of critical, difficult-to-interchange systems, the developing of any necessary repair methods as necessary and the setting-up of an I/C Ageing Observatory (recently reactivated with a view to making a new status report to prepare the future VD3s (third ten year outage program: the first will take place around 2008-2009).

Keeping in operational conditions

Other changes are nevertheless perceptible, which may be difficult to dodge for utilities like EDF. Most of the equipment items are now provided, from the outset, with digital components whose functionalities benefit other customers. This is especially the case with smart sensors, for which a supplement is paid to equip them with a 4-20 mA analog output [7]. This is already true for circuit breaker cells or switchboard contactors, likewise recorders, indicators, etc. Mass-market computing is also continuing to expand and threatening the preserve of top-of-the-range computers like workstations under UNIX : the result is that computing applications (will) rely increasingly on commercial "black boxes", the well-known *COTS* (*commercial off-the-shelf*) of the Anglo-Saxons.

[7] It is clear that the electronic component era is coming to a close, while that of relays (needed for power amplification and galvanic isolation) is not threatened in the short term: it can be observed that, despite the massive computerization of N4, there are more relays in a 1450 MW unit than in a 900 MW unit!

Moreover, the evidence shows that the more a plant is computerized, the more it relies on digital components whose industrial life cycles are short and on difficult-to-maintain software skills. As a result, this type of I/C is threatened with fast obsolescence. This general observation is backed up by our experience in both 1300 MW and N4 plants. This is only one (tempting) step away from the reverse proposition ("to ensure long unit life, keep standard technology"), which is worth debating.

The search for profitability ...

... from which nuclear cannot escape forces EDF to look for non-specific solutions. This option is irreversible. But it conceals a formidable, near-structural contradiction: as IT is by far the most opaque and the least durable industry, how, with the products on the market, can safety requirements (and therefore dependability demonstration, which means free access to all documentation) and lifetime (which is the basis for return on investment but assumes the retention of skills, particularly in software) be reconciled? These two requirements are inherent in the nuclear process and therefore in its associated instrumentation/control.
The forthcoming major choices will depend on the resolution of this contradiction, as it is difficult to imagine fitting a new unit (for example EPR) with instrumentation/control of a technology which is not in the industrial mainstream.

French PWR units

giving :

- **the breakdown by plant series ...**
- **and the connection dates of the first unit of each site.**

900 MW *			1300 MW ***		1450 MW
CP0 *	**CP1 ****	**CP2 ****	**P4**	**P'4**	**N4**
6 units	**18 units**	**10 units**	**8 units**	**12 units**	**4 units**
Fessenheim 1-2 Apr. 77	Tricastin 1-4 May 80	St Laurent B1-2 Jan. 81	Paluel 1-4 June 84	Cattenom 1-4 Nov. 86	Chooz B1-2 Apr. 77
Bugey 2-5 May 78	Gravelines 1-6 March 80	Chinon B1-4 Nov. 82	St Alban 1-2 Aug 85	Belleville 1-2 Oct. 87	Civaux 1-2 Apr. 77
	Dampierre 1-4 March 80	Cruas 1-4 Apr. 83	Flamanville 1-2 Dec. 85	Nogent 1-2 Oct. 87	
	Blayais 1-4 June 81			Penly 1-2 May 90	
				Golfech 1-2 June 90	

* The 6 units of Fessenheim and Bugey do not form a true plant series

** The nuclear islands of CP1 and CP2 are strictly identical. Only the turbine halls are different (respectively "transverse" and "radial").

*** P'4 is a "slimmed-down" of P4 (civil works and layout savings).

The Evaluation on Applying the Digital Safety System to Existing PWR Plants in Japan

Yoichi Mito [1], Masafumi Utsumi [2.]

[1] *The Kansai Electric Power Co., Inc. Nuclear Power Division*
3-3-22, Nakanoshima Kita-ku OSAKA 530-8270 Japan
Tel.: +81-70-5938-2709, Fax: +81-6-6444-6279, e-mail: K576277@kepco.co.jp.

[2] *Mitsubishi Heavy Industries Ltd. Nuclear Energy Systems Engineering Center*
1-1-1, Wadasaki Hyogo-ku KOBE 652-8585 Japan
Tel.: +81-78-672-3305, Fax: +81-78-672-3268, e-mail: utsumi@atom.hq.mhi.co.jp

Summary

To resolve the aging and obsolescence issues for instrumentation and control (I&C) systems at nuclear power plants, it is necessary to form a long-range maintenance and replacement plan for them systematically. To plan to replace the non-safety I&C system, the digital I&C system would be the most powerful choice from the view of maintainability and reliability because it has already been applied to our latest PWR plants. For the safety I&C system, even though digital safety system has already developed for the next PWR plants, it has never yet been applied to our plants. Therefore, how to apply digital safety systems to existing plants has been carefully studied. At first, the differences on safety functions, redundant architecture, and system interface between the next PWR plants and the existing plants have been studied. Then, the best replacement plan for safety I&C systems has been studied to obtain as much benefits as possible that are expected for the next plants, such as high reliability, availability, operability, maintainability and cost reduction.

1. Introduction

Aging and obsolescence issue of I&C system in Japanese PWR plants has become a potential major problem, though the system has been showing excellent operating results for many years. Also, conventional non-digital I&C system contains a lot of components which need to be adjusted and maintained. So, many man-hours have been consumed for testing and maintenance during plant shutdown.

In addition, the nuclear power plants are required safety operation and higher availabilities, I&C system upgrading program from the conventional system to the latest digital system will contribute to improve system reliability, testability, and maintainability.

To upgrade I&C system in the near future also contribute to conduce plant life extension, short maintenance outage, and periodical safety review.

To apply the digital technology into the safety system, it should meet various licensing requirements. So, a joint study with utilities and venders was started to establish digital upgrading program for the safety system of the operating plants.

This upgrading program will be applied commonly to various plants that have different numbers of primary loops or different historical design backgrounds. Therefore, it is important to standardize the planning process, the applicable system architecture, and the upgrading procedure in order to ensure successful design and modification activities, and simplify operation and maintenance. In this standardization, some options will remain such as the type of the main control board (conventional type or fully computerized type) to satisfy various needs of utilities.

This paper reports status of the on going joint study to establish the most suitable system architecture and upgrading procedure to upgrade the safety system of operating plants with the digital system. The major points of this paper are;

- Selection of the model cases of system architecture
- Evaluation for each model case.

2. Digital application at Japanese PWR plants

There are sufficient successful experiences in the digital application to various non-safety control and monitoring systems. From the historical view, digital system was applied to the Radiation Waste Processing System at first. For the latest plants, digital technology was applied to all non-safety systems such as reactor/turbine control system and plant monitoring system.

Application of the digital technology into the non-safety systems is one of the steps of the plant wide digitalization plan. So, the platform hardware and software has been developed and verified in view of further their application to the safety system. For the next plants currently under licensing stage, digital system will be applied all I&C systems including safety system.

For the next plants, the operabilities and maintainabilities of digital I&C systems are improved based on various operating experiences and state of the art digital technology. And, its development and verification has finished.

3. Applicability of the system for the next plants to operating plants

To replace the safety system of operating plant with digital system, the first option will be applying the next plant system. But, it is difficult to apply the next plant system directly to operating plants because of some differences in system configuration and interfaces.(Fig.1) The issues are as follows.

(a) Difference in redundancy
Redundancy of the safety system in operating plants basically consists of three channels and two trains. On the other hand, the redundancy of the next plant consists of four channels and four trains.

(b) Difference in system interfaces
For operating plants, safety system interface with many dedicated controls, indicators and instrumentation modules via metal cables. On the other hand, for the next plant, communication network system is used as interface means between systems.

According to above differences, system architecture of the digital safety system for operating plants should be carefully examined from various points of views. Not only the differences in redundancy and system interface, but also items shown in the next section should be considered in the case study of the digital safety system for operating plants.

4. Case study of the digital safety system architecture for operating plants

Approach to establishing the suitable system architecture of the digital safety system for operating plants is going on based on evaluation of model cases.(Fig.2) In this section, preconditions to establish model cases and evaluation points for these model cases are described.

4.1 Preconditions to establish model cases

(1) Conformance to the latest licensing requirements

Some of the licensing requirements have been changed since it was issued for the current operating plants. These changes has been enforced plant safety and has clarified the design basis requirement. These latest licensing requirement updates are fully considered to develop model cases for digital upgrading for the safety system in operating plants.

(2) Functionality of the safety system

There are differences by plant in functional design and redundancy of the safety systems in operating plants. All these designs satisfy safety acceptance criteria through the safety evaluation in licensing process. But there are some points to be modified from the point of plant availability and operability improvement. For example, in the latest plants, four-channel system configuration and elimination of steam generator flow mismatch reactor trip improved plant operability. In the next plant, variable setpoint for the delta-T reactor trip will also improve plant operability.

To introduce these design into operating plant, safety re-evaluation is needed and additional equipment installation should be considered. Therefore, economical analisys have to be done to decide the re-modification on the safety system.

(3) Scope of digital application

It is important to study which system or function should be digitalized in the actual system architecture. In the next plant design, digital technology will be applied to all the safety system. On the other hand, for the operating plant upgrading, we are studying which system or function should be replaced by the digital system from the point of the interface with other systems. In this study, we are considering to include solid state logic circuit to the renewed safety system.

To examine the scope of digital application, reliability, testability and maintainability are also considered. Furthermore, countermeasures for common mode failure in the digital safety system will be included.

(4) Type of the main control board

Type of the control board is one of the major concerns to examine plant wide digital upgrading program. Conventional type control board of the operating plant is consists of dedicated instrumentation modules and controls. Instead, new type control board will be applied to next plants that is fully computerized with soft controls.

Basically, two types are considered. One is the replacement to the conventional type control board with individual indicators and controls such as used in the latest plants. The other one is the replacement to the fully software based control board for the next plants. Therefore, digital safety system must be fit to both of them.

Major Difference in interface between the safety system and the control board is the use of individual cables and communication network. Especially, component of control circuit configuration is quite different between the analog system and the digital system. In analog system, each electrical contact of controls at the control board, magnetic relays in controllers, and local switchgears are connected by individual cables to form control logic. On the other hand, in the digital system, all these data is put into the digital system to form control logic.

4.2 Evaluation points

Comparison on possible model cases based on above-mentioned preconditions are going on from many points of view including reliability, availability, test and maintenance, installation work and economy. Special considerations to be evaluated are summarized bellow from the point of upgrading of the existing system.

(1) Cabinet layout

In the planning about the layout of the cabinet, spatial separation requirements and required space due to the change of system architecture should be considered. Design basis about spatial separation in some old operating plants could be quite different from the latest design. So it will be possible to reconfigure cabinet layout referenced to the latest design at the same time with the replacement work of the cabinets.

On the other hand, due to the difference of system architecture between newly introduced digital safety system and the existing system, it may be difficult to install new cabinets in the same area of corresponding existing cabinet.

So it is important to examine possible layout changes including modification of the layout space considering spatial separation criteria for the safety system and the supporting system design such as heating and ventilation system. It might be needed to prepare new instrumentation rack room other than the existing room with some rearrangement of the layout within the building.

(2) Reuse of existing cables

Network interface between digital systems will be able to widely introduce instead of the existing interface using huge amount of cables. Especially, in the interface with the main control room and the plant computers, many cables and individual interface components such as isolation amplifier will be able to be eliminated. But, there will still remain many individual cable interfaces between non-digital equipment such as local cabinets and sensors. So it is important to reuse existing cables to minimize amount of replacement work.

Because it is difficult to extend existing cables, possible termination layout design within each cabinet and installation of some additional termination cabinets are considered in our examination. If it will needed, new termination cabinets may be installed in the cabling room under the instrumentation rack room, and some multi conductor cables may connect the new termination cabinets and the digital safety cabinets. These concerns are depend on the system architecture design and cabinet configuration of the digital safety system.

In addition to these planning, detailed investigation of the existing cables will be needed to identify each cable and to confirm route of cables and spare space in cable tray in the implementation design phases.

(3) Testing and maintenance procedure

Digital system will be able to improve testability and maintenability by many features such as elimination of components tend to drift, automatic test, automatic calibration, and self diagnostics depend on the platform and system design. These new features will change items and processes of the test and maintenance work drastically compared with conventional system. To effectively apply these features, test and maintenance procedure during plant refueling outage should be reviewed and revised. Also, equipment test requirements such as technical specification will be reviewed to achieve appropriate test procedure and interval.

(4) Effect on supporting systems

Introduction of the digital system into the safety I&C system may cause increase of power consumption and non-linear load effect on the vital instrumentation power supply system. In some cases, additional batteries or replacement to more large inverter will be needed.

Also increase of the heat source depend on the system architecture should be evaluated from the point of the heating and ventilation system design.

These examination about effects on the supporting systems should include adequate margin from the point of plant wide long-term I&C upgrading.

5. Approach to realization of digital safety system

The optimum facility compositions for the operating plant is due to be determined from the evaluation points. It is necessary to continue the following examination, in order to actually apply them to the existing I&C system.

(1) Determination of suitable upgrading time in I&C system

First of all, the facility renewal is necessary because of the deterioration of the apparatus and unavailability of electronic parts. Considering the life of the plant, I&C system needs to be replaced at the most optimum time.

(2) Consistency with plant wide I&C upgrading program

As stated at the beginning of this paper, digital upgrading of the safety system should be planned in accordance with the renewal of whole I&C system. And to realize the plan, the future design of the whole I&C system is indispensable. This future plan must include the upgrading of the main control board.

Therefore, in parallel to this examination, the future design of the main control board is being considered.

(3) Upgrading procedure of I&C system

In a case of realizing the future design of the whole I&C system, it is not so practical to replace all the I&C system at the same time because it will require too much long-term plant shutdown. So, it is feasible to perform replacement work by each through some plant refueling outages. In this situation, not only the examination on the plant wide final system architecture, but also the examination on the feasibility of the temporary system configuration is important.

As the digital systems already replaced and the conventional systems mixed in the temporary configuration, interface between systems will change along with the upgrading schedule. Though this situation itself is an inevitable process, it is important to establish the upgrading program that minimizes the changes in design of the interface portions of already replaced system.

From this point of view, the order of the system replacement is under examination to minimize the cost and to realize easier work process aiming at plant wide long-term upgrading program.

6. Conclusion

Systematic examination on plant wide I&C digital upgrading program into the Japanese operating PWR plants has been started. Especially, utility and vender joint study about the safety system upgrading is going on considering various items including licensing issue. Coupled with the examination about the type of main control board, an standardized upgrading program for operating plants will be established that include the system architecture and the order of implementation.

Fig.1 Operating Plants – Next Plants System Configuration

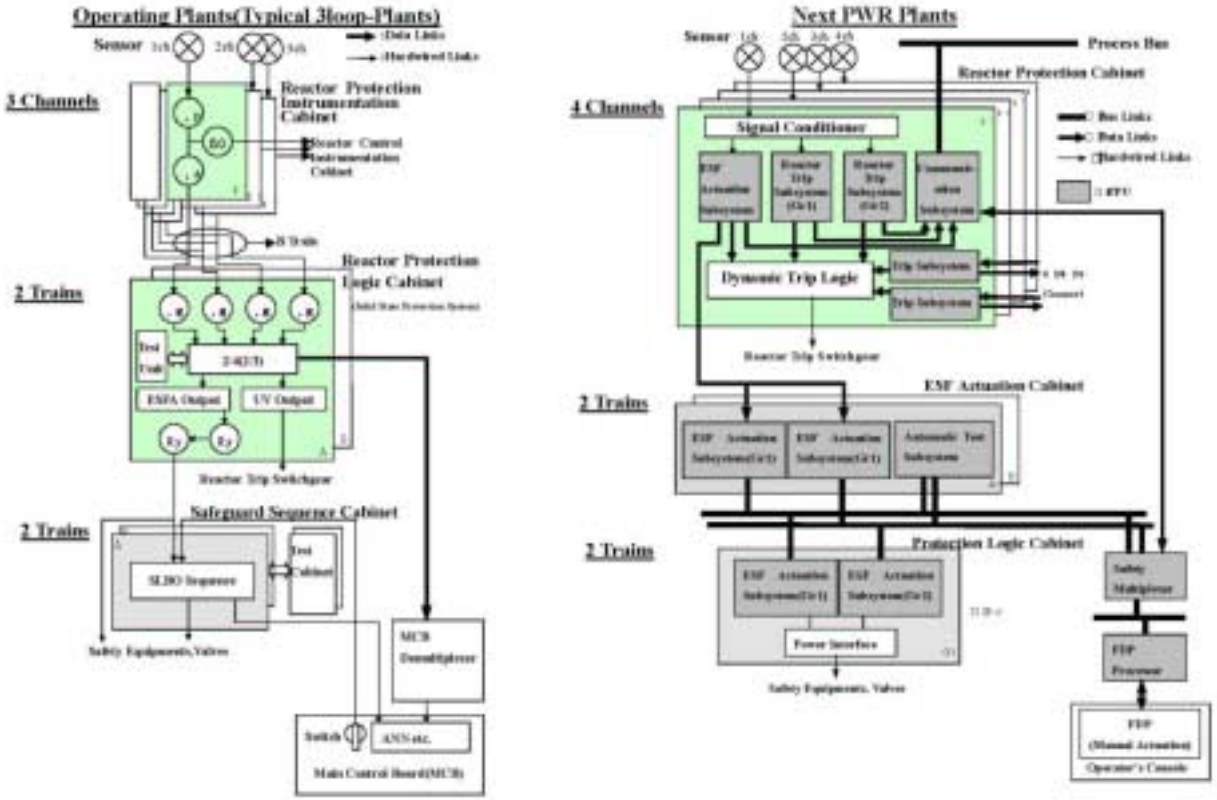
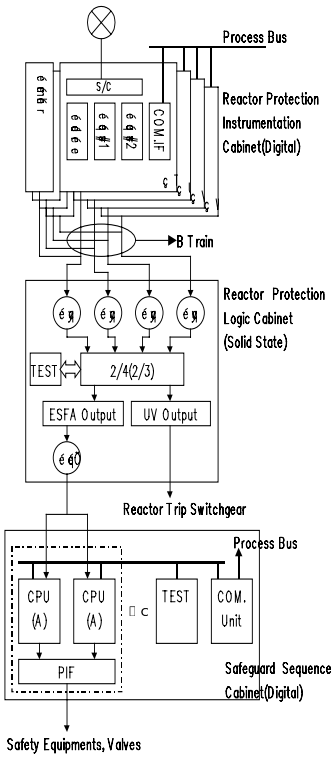
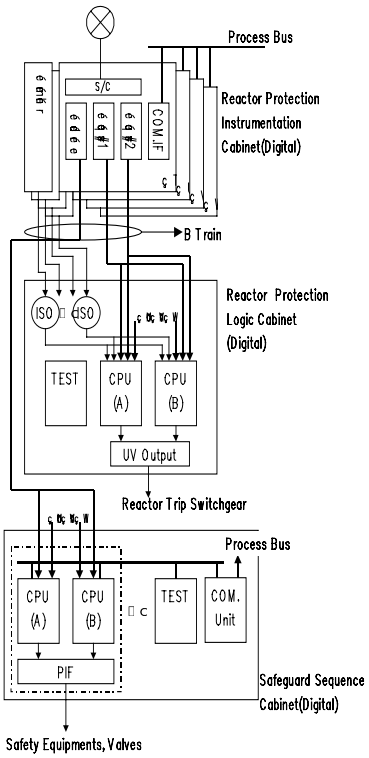
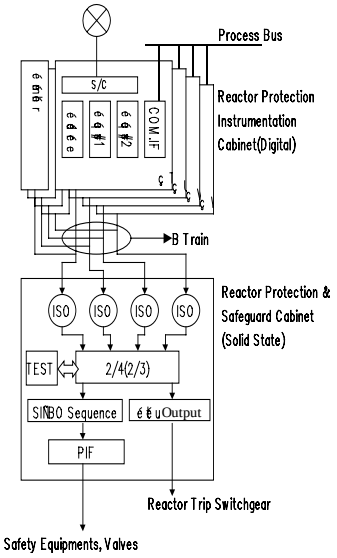


Fig.2 Typical Case of Safety System Composition (Application of the Digital System)

CASE1	CASE2	CASE3
		
Applying digital system to the reactor protection instrumentation cabinet and the safeguard sequence cabinet	Applying digital system to the reactor protection instrumentation cabinet, the reactor protection logic cabinet and the safeguard sequence cabinet	1. Applying digital system to the reactor protection instrumentation cabinet 2. Integrating the safeguard cabinet into the reactor protection cabinet

Independent Assessment of the Temelín Safety System Software

Petr Závodský
ČEZ, a. s., Division of Construction of NPP Temelín
Tel: +420 334 78 2151, Fax: +420 334 78 3815, E-mail: Zavodsky_Petr@mail.cez.cz

Summary

The Instrumentation and Control (I&C) System for the Temelín Nuclear Power Plant has been designed and supplied by Westinghouse Electric Company under contract to ČEZ and Škoda Praha. Under this contract, Westinghouse have performed independent verification and validation of the software for the safety related portion of the I&C system. In addition, a programme of Independent Assessment (IA) has been carried out to provide additional confidence in the integrity of the safety system software.

Data Systems and Solutions LLC (DSAS) have carried out the IA activities under contract to ČEZ. These activities were independent of Westinghouse. They were designed to confirm that the software production processes complied with the specified standards and to assess the software for each system. These activities were designed to be diverse from the V&V activities of Westinghouse. The scope of the IA activities was originally defined by the Czech Regulator SÚJB.

Introduction

ČEZ, a. s. Nuclear Power Plant Temelín is currently in the process of start up, commissioning and constructing two nuclear power units, based on the VVER 1000 Russian designed reactors. The Instrumentation and Control (I&C) system is being upgraded by a modern Westinghouse supplied I&C system, which meets requirements imposed on current NPP designs.

Safety Systems and Their Safety Roles

There are four safety systems of which two are automatic protection systems and two are reactor monitoring systems.

- PRPS and DPS are diverse automatic protection systems.
- PAMS and DMS are diverse reactor monitoring systems.

The automatic protection systems contribute most to plant safety as these perform automatic actions to maintain the plant in a safe state. The monitoring systems perform a significant but smaller safety role as they provide the operator with post-accident information on the reactor.

Primary Reactor Protection System

The Primary Reactor Protection System (PRPS) measures key plant parameters and performs automatic actions to maintain the reactor in a safe state including reactor trip and initiation of plant to maintain the reactor in a safe state after trip. The functions of the PRPS are:

- To provide an automatic reactor trip in all credible reactor faults that require reactor trip as part of the reactor protection requirements;
- To actuate engineered safety features (ESF) to maintain reactor safety, including post-trip cooling and containment isolation, in all credible reactor faults.

The PRPS is divided into three redundant Divisions that each comprise safety grade field sensors, Nuclear Instrumentation System (NIS) ex-core flux monitoring detectors and equipment, Integrated Protection Cabinets (IPC) and associated Reactor Trip Switchgear, and ESF actuation logic cabinets. A reactor trip condition in one Division is communicated to the other two Divisions where voting takes place which, if satisfied, results in initiation of reactor trip. Similarly, ESF actuation demands are communicated to other Divisions where voting takes place which, if satisfied, initiates the appropriate ESF plant systems depending on the initiating conditions.

The PRPS uses Westinghouse Eagle family hardware, utilising Intel 80X86 microprocessors. Each subsystem incorporates a 'host' processor board, in combination with a number of slave processor boards that provide input, output and communications functions. This general architecture is identical to that used on the Sizewell 'B' Primary Protection System (PPS), but some upgrades to the technology have been made in the Temelín PRPS. The PRPS software is mostly written in PL/M 86 but contains some modules that are written in ASM86 assembly language.

Diverse Protection System

The Diverse Protection System (DPS) is a secondary means of achieving reactor trip and initiation of post-trip cooling and provides automatic protection against all frequent reactor faults. The functions of the DPS are:

- To provide an automatic reactor trip in all frequent reactor faults that require reactor trip as part of the reactor protection requirements;
- To actuate engineered safety features (ESF) to maintain reactor safety, including post-trip cooling and containment isolation, in all frequent reactor faults.

The system therefore provides diverse reactor protection against reactor faults. As with the PRPS, the DPS comprises three redundant reactor trip and ESF actuation Divisions (Divisions I, II and III). DPS uses a different hardware platform (Motorola-based) and software language (Ada, with some 68000 assembler) to that of the PRPS. The DPS software is split into two main layers – Platform code and Application code. The Platform code provides the generic operating environment whilst the application code performs the safety tasks. As with the PRPS, the DPS uses configuration and calibration data to configure the application and provide tuneable constants.

Post Accident Monitoring System

The Post Accident Monitoring System (PAMS) is the primary means of acquiring and displaying reactor plant parameter indications to the operator that are important for accident mitigation. The functions of the PAMS are:

- Post-accident data acquisition;
- The display of plant variables important to accident mitigation.

The PAMS uses the same type of hardware, the same programming languages and the same software structure as the PRPS. The PAMS comprises two redundant divisions, each of which displays the post-accident information required by the operator, including redundant and diverse channels. The redundancy assures that loss of one power division along with the affected Post Accident Monitoring System division and input channels, is accommodated by the remaining Post-Accident Monitoring System division, without loss of required information and without creating information ambiguity.

Diverse Monitoring System

The Diverse Monitoring System (DMS) is a secondary and largely diverse means of acquiring and displaying all reactor plant parameter indications to the control rooms that are important for accident mitigation. The functions of the DMS are:

- Post-accident data acquisition;
- The display of plant variables important to accident mitigation.

The DMS uses the same type of hardware and the same programming languages as the DPS. The DMS can be considered to be an extension of the DPS that performs functions associated with displaying plant information to the operator. There are two divisions of DMS – one for the Main Control Room (MDMS) and one for the Emergency Control Room (EDMS).

Software Development Processes at Westinghouse

Implementation diversity between PRPS/PAMS and DPS/DMS is maintained by using different development teams, development processes, development platforms and tools for the two sets of systems. Associated with each of the development teams (Design Groups) is a management-independent group responsible for software V&V (V&V Group). The Design Groups are responsible for system and software specification, design and implementation. Members of the design team also perform review activities such as Design Review and second party review. A separate team within each Design Group is also responsible for subsystem and system level factory testing. The V&V Groups are responsible for verifying the software against its specifications through review, static analysis and module test activities. For DPS the V&V Group also performs V&V of higher level system documentation.

Acceptance Criteria

In 1994 SÚJB set up a clear licensing requirements, which are being used for evaluation and acceptance of the safety systems software. The acceptance criteria have been set as follows:

- The SW manufacturing including its verification at the manufacturer's factory (FAT) as well as on site (SAT) and check of the accepted SW (so called pre-existing SW) is in accordance with currently recognised recommended procedures for attainment of high quality end product (IEC-880/1986, ASME NQA-2a/1990 part 2.7, IEEE 7-4.3.2/1993),
- Independent verification and confirmation that the mentioned procedures have been really met,
- A positive outcome (meaning that no substantial deficiency has been detected which might endanger meeting the requirements of the corresponding safety function) of a Independent review of the SW end product which involved:
  - Check of system requirements and of the from them derived requirements on SW;
  - Static analyses of selected SW parts /related to PRPS and DPS/;
  - Dynamic tests of the SW as a system /related to PRPS only/.

Programme of Independent Assessment

The fulfilment of item 1) under acceptance criteria falls in responsibility of the I&C Supplier Westinghouse. To fulfil the items 2) & 3) a separate Independent Assessment (IA) programme was prepared and conducted. It must be noted that Westinghouse's program of Testing and Verification and Validation of software satisfies the requirements of standards on Testing and V&V. The IA program was in addition to the requirements in the standards. Similar program was conducted on the software of the safety system at Sizewell B. These activities were independent and diverse from the V&V activities of Westinghouse and they were designed to confirm that the software production processes complied with the specified standards and to assess the software for each system.

Organisation

The Independent Assessment of the Temelín safety system software was contracted by ČEZ, to the prime contractor Data Systems & Solutions (DSAS). The Independent Assessment team consisted of DSAS and two major subcontractors, British Energy (BE) and Fluor Global Services (FGS) formerly known as TA Group (TAG). BE and FGS had additional subcontractors to assist in the work. ČEZ have had the responsibility for communication with SÚJB as well as ensuring provision and/or access to the information and documents from the supplier, Westinghouse.

The IA comprised the following tasks and was allocated among the particular sub-suppliers as given in brackets (see Figure 4 for IA tasks example):

- Independent audit of software development processes (conducted by DSAS);
- System Software Assessment (conducted by BE);
- System and Software Requirements Verification (conducted by DSAS);
- Software Design Verification (conducted by DSAS);
- Static Source Code Verification (conducted by FGS);
- Dynamic Testing (conducted by DSAS with assistance of BE);
- Common Mode Failure Assessment (conducted by DSAS);
- Data Verification and Validation (conducted by BE).

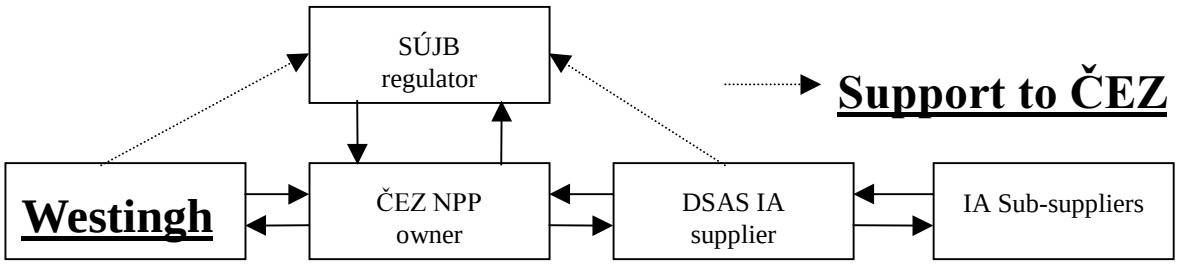


Figure 1 – Organisation of the Project

Independent Audit

Independent audits were performed on the Westinghouse software development processes for compliance with the following international standards:

- IEC 880
- IEEE 7-4.3.2
- ASME NQA – 2a, Part 2.7

The audits covered all (four) safety systems and were targeted at particular aspects of the development cycle. The audits also included an appraisal of the software development processes against certain good software development practices documented in the first supplement to IEC 880. Guidance given in NUREG/CR-6101 & NUREG/CR-6421 was used in the audit process, where appropriate.

The five audits were to audit the development processes against requirements and guidance that relates to plans and procedures and design implementation; the qualification of tools used in the development of software against requirements and guidance relating to the use of tools; the incorporation of features such as self-supervision, surveillance testing and return to service in PRPS and PAMS against requirements and guidance. Also appraised the development process against relevant industry good practice.

System Software (Tools) Assessment

System software was the term used to embrace the development system software tools that are used to develop the software of the safety systems. It includes compilers, linkers, locators, data table generation and other software tools. Some were commercial software tools and others were software tools produced by or for Westinghouse.

The overall objective of the system software assessment was to generate sufficient evidence to provide confidence in the integrity of the software tools used to produce the software. Particular attention was paid to those tools that perform complex transformations, such as compilers, which transform source code to object code. These tools have the greatest influence on the final executable code. The system software tasks set out to:

- Provide evidence that the system software has been developed in accordance with recognised good software development processes;
- Provide valid and objective evidence of operating experience of the system software;
- Provide evidence that the system software has been adequately verified, either through analysis or extensive testing for use in safety systems;
- Provide, where evidence is missing or is inadequate especially for commercially available products, further evidence that the tool performs correctly either through analysis, extensive testing (DPS) or by reverse engineering (PRPS source/code comparison) of a sample of the code.

System and Software Requirements Verification

The system and software requirements verification tasks cover the functional, performance, safety and integrity requirements. The purpose of these tasks was to confirm that:

- The system requirements satisfied all applicable codes, standards and regulatory requirements;
- The system requirements were a complete, consistent, unambiguous and accurate representation of the reactor protection functions;
- The high-level I&C system design was a complete and accurate representation of the system requirements with no unintended design elements;
- The software requirements were correctly derived from the system requirements;
- The software requirements were a complete, correct, accurate, clear, consistent and unambiguous representation of the software portion of the system requirements and design.

The scope of the task included all functionality except for subsystems not directly involved in performing the protection function such as the autotester, maintenance consoles and communication systems. To facilitate the verification of system and software requirements and to promote consistency, a traceability tool was used. The tool selected was DOORS.

Software Design Verification

This task took as its input the software requirements list generated by the System and Software Requirements Verification task. The task covered functional, performance, safety and integrity requirements in the software requirements. The purpose of the task was to confirm that the software design requirements had been correctly derived from the software requirements. The task comprised three sub-tasks:

- A software design traceability analysis that identified all software design elements from the Westinghouse documentation, which were then recorded in a software design elements list. The analysis traced the software design elements forwards and backwards to confirm that they are correctly derived from the software requirements list. It identified software requirements that are not adequately addressed in the software design, and software design elements not derived from the software requirements;
- A software design review that evaluated the software design for accuracy, completeness, consistency and correctness;
- A software design interface analysis that determined whether all external interfaces to the software and internal interfaces within the software are complete and that they are consistent with the software requirements. Each data flow item was evaluated for correctness by verifying that the name, format, content and syntax is correctly defined in all locations in the design and that each item is specified both as an input and output of interfacing modules.

For the PRPS, the scope of the task included all functionality covered in the software requirements task except for communications subsystems. For the DPS the scope was limited to the functions within the defined vertical slice.

Static Source Code Verification

Static source code verification was performed on all safety critical parts of the PRPS (defined by the PRPS hazard analysis task). Static source code verification was performed on a sample of the safety critical software for the DPS. The safety critical software was defined by the DPS hazard analysis task. The scope of the DPS sample was defined by the DPS software vertical slice analysis. This task was not performed on PAMS and DMS.

The task was a rigorous static analysis, involving a high degree of formality, to show conformance between source code and the software design. The analysis involved a tool-supported verification of the semantics of the code against the definition of the required operation of the code. It showed whether each source module implemented its corresponding module design specification and gave a high degree of confidence that the operation of each software subsystem met its requirements. This static analysis generally conformed to the requirements of IEC 880. The static analysis was carried out using software tool that was different from that used by Westinghouse. The source code was analysed using a suite of static program analysis tools known collectively as MALPAS. Static analysis comprises a set of techniques for examining the structure and the likely behaviour of the software without execution. The MALPAS analysis enabled the assessment to complete the analysis loop between the specification and the source code.

Data Verification and Validation

Data verification was achieved through verification of the data against the software specification documentation and the protection system requirements. The task included the configuration and calibration data for both the PRPS and the DPS but was limited to the safety critical sub-systems as defined for the Static Analysis task. The evidence provided by the task provides the main support for the assertions in the safety case regarding adequate data integrity.

Configuration data was verified as follows:

- Data used to configure the common functions employed by the application was checked for consistency with the Westinghouse standard template;
- Data used to configure local databases and the hardware interface used by the application was checked for compliance with the rules for the relevant data structure;
- Data was checked for correct cross-references, indexing, pointers to tables and correct buffer layout;

All data that determines functionality and architecture was checked for completeness against system requirements and functional requirements.

Calibration data was verified as follows:

- Functions that manipulate and use calibration data were checked to ensure that adequate range checking and error reporting exists;
- Data was checked to ensure the presence of all calibration data required by each function described in software documentation;
- Each calibration data item required by each function was checked to ensure that its value is in accordance with the system requirements.

Common Mode Failure Analysis

The objective of this task was to confirm that adequate defences against common mode failures exist in the design and implementation of the PRPS and DPS software and similarly, for the PAMS and DMS software. The CMF analysis task consisted of a number of activities including a review of Westinghouse documentation for CMF potential, discussions with Westinghouse personnel to determine the degree of independence between the primary and backup systems and analysis of inputs from the other IA tasks.

The analysis was performed in the following manner:

- Identification of potential CMF mechanisms through:
  - Review and comparison of development processes;
  - Comparison of development tools utilised and documented;
  - Review of identified sources in Section 4.1 of the First Supplement to IEC 880;

- Discussions with IA team members performing other tasks and review of products of other IA tasks as applicable.
- Documentation of CMF Issues - a CMF Issue was declared where any potential CMF mechanism was found to exist.
- Evaluation of each CMF Issue to determine the relative probability of occurrence - CMF Issues that were not determined to have a sufficiently low probability of occurrence were raised as Findings.

Dynamic Testing

The Dynamic Testing task was performed for the PRPS only. It was based on the same concept as the dynamic testing performed on the Sizewell B PPS. The scope of the testing was designed to maximise the coverage of the PRPS software safety functionality, therefore non-safety functions were excluded from the test coverage. The basis for exclusions from the testing was justified in a test boundary definition document.

The testing consisted of 5000 individual tests based on 10 selected accident scenarios. For each of the 10 scenarios, 500 unique combinations of PRPS input values were generated from reactor transient analysis. The tests were applied automatically to the Test Division and also to the Logical Model. The Test Division was a replica of PRPS Division 1 with simulated interactions with Divisions 2 and 3. The Logical Model was a software simulation of the PRPS requirements. Test results were recorded automatically and then compared to identify discrepancies between the predicted results from the Logical Model and the actual results from the Test Division. Discrepancies were recorded and resolved, with unresolved discrepancies being submitted as task findings.

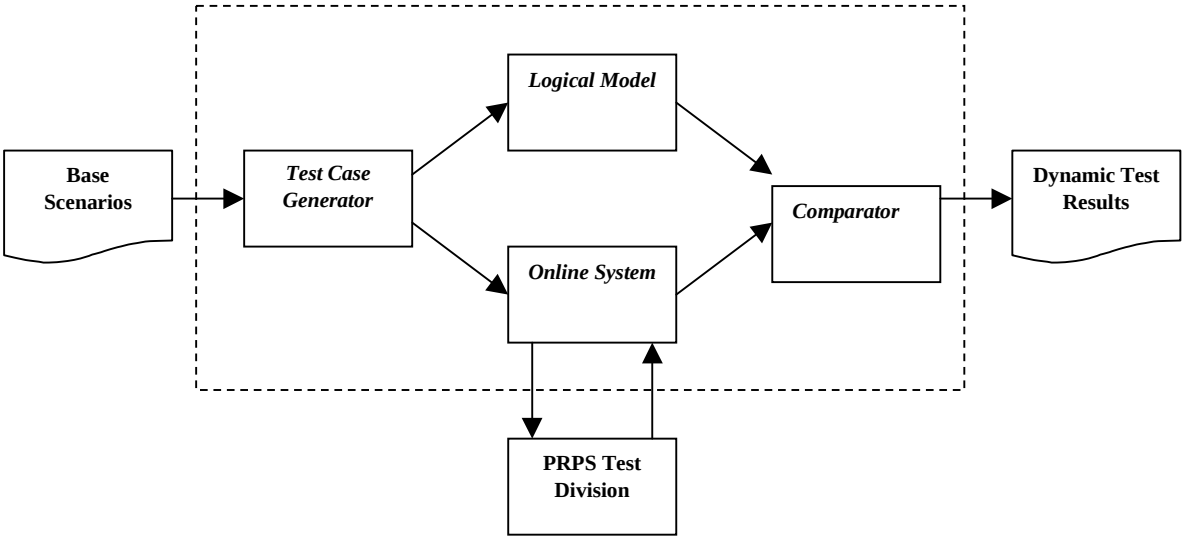


Figure 2 – Dynamic Testing Process Overview

CONCLUSION

Resolution of Findings

Each IA task had the potential to identify anomalies in the Westinghouse software processes, software and documentation. These anomalies were raised as Findings, in compliance with the Project Procedure "IA Findings Reporting and Resolution". This procedure defined the process that was used for generating, reviewing, sentencing to resolution and subsequent closure of Findings that had arisen. This process is represented in a simplified form in Figure 3.

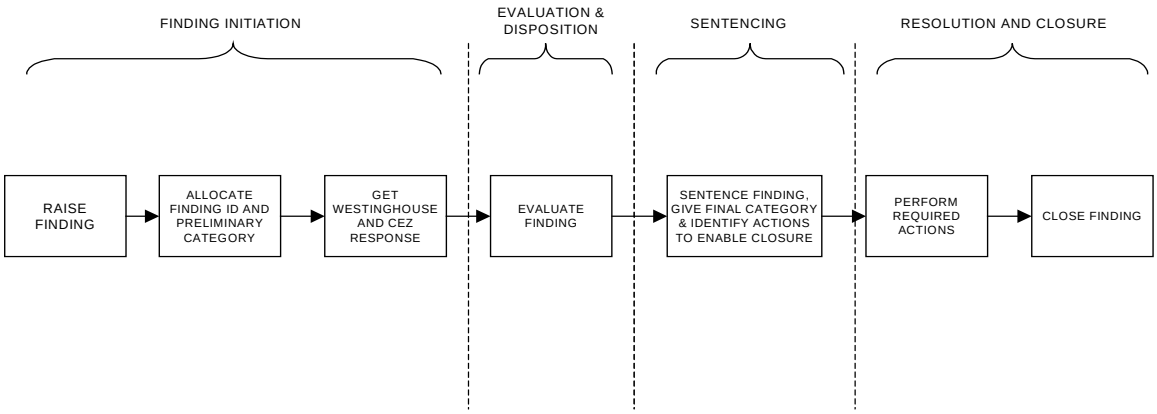


Figure 3 – Process of Resolution of Findings

Findings were sentenced by the sentencing team to agree on a final categorisation and resolution for each Finding, including the corrective action and corrective timescale categories. The sentencing team comprised a minimum of one member from the DSAS Project Management Team, one member from the organisation, which raised the Finding, a representative of ČEZ and a representative of Westinghouse. A category was assigned to each finding.

Severity/Safety Significance

Category 1: Impacts safety.
Category 2: No safety impact but is significant to the software development process or plant operation (e.g., could affect plant operation, provide misinformation to the operator or another system, or affect system testing).
Category 3: No safety impact, affects documentation, software, software development process, or conformance to defined requirements only.
Category 4: No safety impact, no effect on operations and no requirement to change documentation or software development process.
Other categories were Category 5: Invalid, Category 6: Duplicate and Category 7: Document baseline mismatch.

Corrective Actions

Category A: Design Change it is intended to align with Westinghouse's own Request for Engineering Change (REC) process.
Category B: Executable Code Change (does not include change to a code comment).
Category C: Design Document Change.
Category D: Development Process Impact.
Category E: Process Document Change.
Category F: No Action Required.
Category G: Complete the Development Process.
Category H: Provide Additional Evidence.
Category J: Add to "fix file" for consideration at the next revision of the item.
Category K: Confirm existence in "fix file" from Sizewell application.
Category L: Flag as operational issue.
Category M: Already addressed in later revision.

Statistic of Findings from IA program is following:

1	Impacts Safety	0.0%
2	Significant	0.5%
3	Not Significant	45.4%
4	No Effect	34.4%
5	Invalid	14.6%
6	Duplicate	1.3%
7	Baseline mismatch	3.8%

A	Design Change	0.0%
B	Executable Code Change	2.1%
C	Design Document Change	11.3%
D	Development Process Impact	1.2%
E	Process Document Change	1.8%
F	No Action	52.9%
G	Complete Development Process	1.3%
H	Provide Additional Evidence	0.2%
J	Add to Fix file	15.7%
K	Confirm in SXB Fix File	5.4%
L	Flag as Operational Issue	0.1%
M	Already addressed in later Rev	8.0%

Lessons Learned

Successful IA depends upon:

- Development process amenable to IA;
- Timing of work in relation to development phase;
- Adequate documentation;
- Cooperation of developers, assessors & customer.

Benefit of IA tasks can be maximised by timely and scope performance:

- Early tasks, focussed on development process;
  - Audits of development processes, to include some requirements IA;
  - Assessment of development tools.
- Later tasks focussed on verified products;
  - Static Analysis;
  - Dynamic Testing;
  - Data verification.
- Sample-based approach is acceptable, where justified;
- Consider relevancy of best practices from modern standards.

Lessons learned from particular tasks:

- Static analysis:
  - Need to define SA requirements early;
  - Make development process amenable to Static Analysis;
  - Need to match analysis to documentation quality;
  - Address code integrity and functionality separately;
  - Opportunity for significant automation.
- CMF task - Need for, and scope of, diversity between systems needs to be clearly defined prior to design activities;
- Dynamic Testing - It is the only IA task to validate end to end functionality;
- Source Code Comparison
  - Sample approach for SCC was deemed to be acceptable;
  - The SCC task should be started early to allow early tool development and to minimise the impact of findings
  - Feedback from tools suppliers is limited and difficult to obtain - effectiveness of this part of the task limited
- Audits:
  - They are effective, particularly when the audit scope is appropriate to the current lifecycle stage.
  - Elements of requirements IA tasks can be incorporated in the scope of audits.
- Data verification was effective in identifying a number of significant findings.
- Early involvement with the designers could help to automate the process and make it more effective.

Conclusions from IA program are following:

- Nothing was found that undermines confidence in the quality of either the software production processes or the software for the systems.
- The Westinghouse processes were shown to be generally compliant with the requirements of the relevant standards.

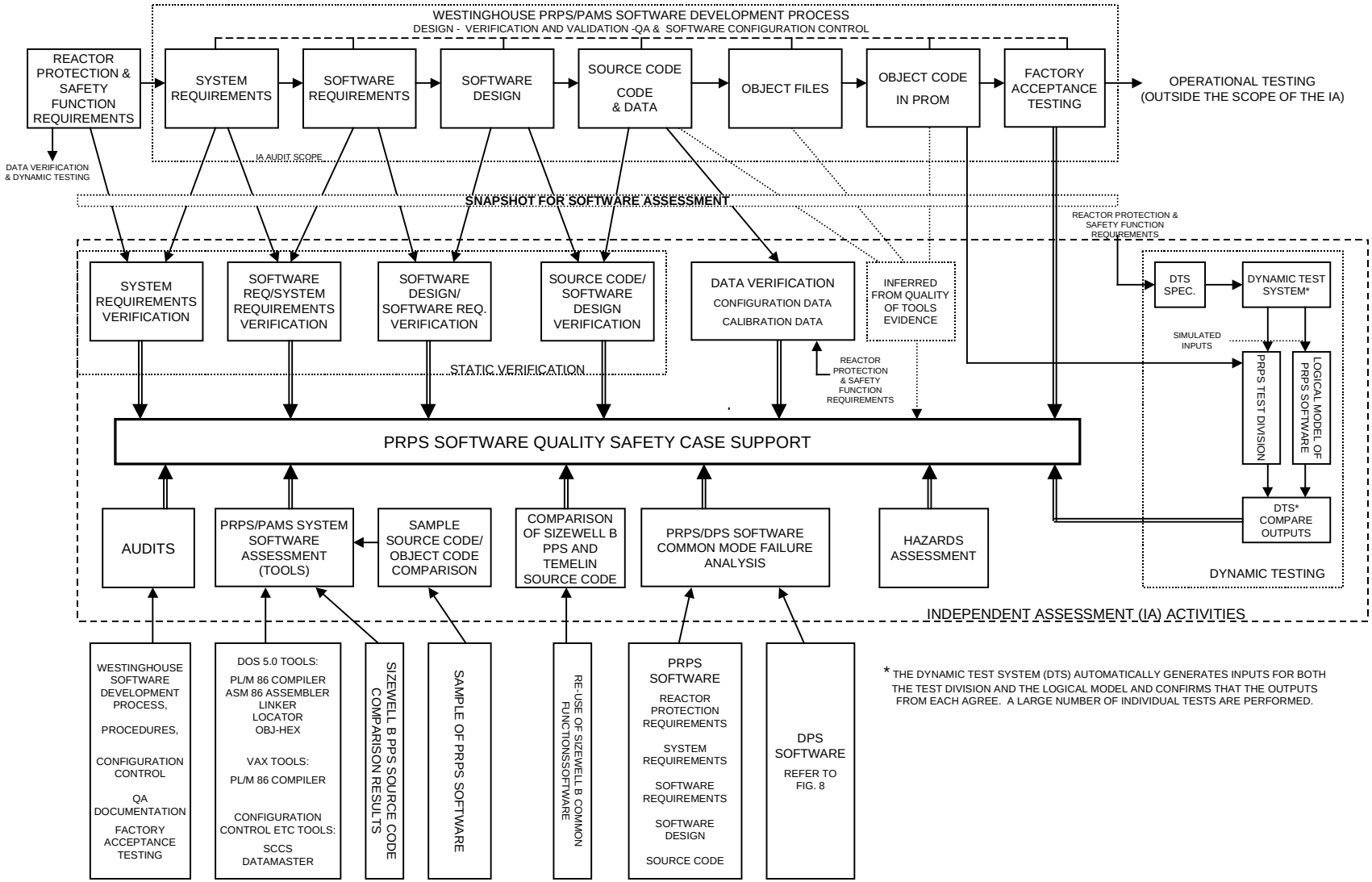


Figure 4 - IA Tasks for PRPS

Regulatory Review of the Digital Plant Protection System for Korea Next Generation Reactor

DAI. I. Kim[1], B. R. Kim[1] and S. H. Oh[1]

[1] *Dept. of Instrumentation and Control, Korea Institute of Nuclear Safety,*
Ku Sung Dong 19, Yusung Ku, Daejeon City, 305-600, South Korea
Tel: +82-42-868-0246, Fax:+82-42-861-2535, Email:dikim@kins.re.kr

Summary

This paper presents the interim evaluation result and the regulatory approach of digital plant protection system (DPPS) for Korea Next Generation Reactor (KNGR: APR-1400). Firstly, we discuss the issue associated with the integration of bistable processor (BP) and local coincidence logic processor (LCLP) as one of design changes over digital plant protection system. Secondly, regulatory approach is presented on the safety classification and the independence of the soft controller to be installed in digital engineered safety features actuation system (DESFAS). Finally, hardwired back up systems against common mode failure of a digital system are described.

I. Introduction

In Korea, sixteen (16) nuclear power plants are being currently operated and four (4) units are under construction. The instrumentation and control (I&C) system of nuclear power plant has been partially upgraded or designed by a digital based system at the operating plant [1],[2]. However, recently, it is being designed as a totally computerized digital system in the instrumentation and control system important to safety. Whilst digital technology has the capability to improve both operational performance and safety, there might be some difficulties to evaluate it on the safety sense because evaluation methodologies have not been established systematically for a digital system and some portions of digital system can not but to apply implicit requirements applicable to an analog system.

This paper describes regulatory activities associated with the review of standard safety analysis report (SSAR) on Korea Next Generation Reactor (KNGR: APR-1400) submitted to the Korean regulatory body to attain the Design Certification (DC). The purpose of this paper is to present the regulatory approach for the safety assessment of a digital plant protection system (DPPS) of KNGR which has evolutionary design features and may result in key issues in regulatory review, thereby improving the safety of the plants and reducing unnecessary regulation burden.

The issues raised during the safety review are especially the system structure of DPPS related to bistable processor (BP) and local coincidence logic processor (LCLP), the safety classification of soft controller applied newly in the DPPS, and the defense-in-depth (DID) against common mode failure.

Firstly, we discuss the issue associated with the integration of BP and LCLP as one of design changes over previous digital plant protection system. Basically, these processors are separated physically since they have inherent functions to generate a trip signal and coincidence logic signal, respectively. However, licensee proposed the structure integrated bistable function with coincidence logic one to be controlled by a single processor. This integrated structure may cause the side-effects in the reliability of software due to the complexity of software, the functional diversity by the integration of processor, and the design consistency with analog protection system, even though the proposed structure is more reliable than the

separated one in view of simplicity of hardware. Therefore, it is required that bistable and local coincidence logic processors to have a distinctive function be separated to preserve the functional distribution and to accomplish software validation/verification (V/V) facilely.

Secondly, we discuss issues about the safety classification and the independence of the soft controller to be installed in DESFAS. The I&C systems of KNGR are designed using digital technologies like multiplexer/demultiplexer in safety systems to process data efficiently and to design optimum, compact and efficient system, whereby a huge number of manual switches dedicated spatially are replaced with soft controller which is mediated by software. This drastic design change makes it more difficult to ensure the independence between safety and non-safety signals and to perform software V/V [3].

Pursuant to requirements of codes and standards, manual switches used to control the safety-related components are classified into safety system. Therefore, the regulatory position is that soft controller functionally equivalent to manual switches shall be also classified into safety system including both software and hardware. In addition, the electrical isolation and physical separation among channels shall be maintained. Finally, regulatory approach is presented on the hardwired backup system against common mode failure for the DPPS in Section IV.

II. The integration of bistable and LCL processor

1. Background

The function of BP generates a command signal to actuate a reactor trip or an ESFAS when underlying process variable exceeds a trip setpoint comparing process variable with a trip setpoint. The LCLP performs the 2/4 logic function for every trip parameter to prevent spurious reactor trip signal. The BP and LCLP are inherent functions to accomplish the function of reactor protection. As shown in Table 1, it is designed such that the function of BP is independent upon that of LCLP in DPPS. However, the function of BP and LCLP of KNGR is controlled by one processor. We describe the regulatory approach on the structure of processor in the following subsections.

Table 1: Comparison of the number of processor in Digital Plant Protection System.

Processor	Wolsong (PDC)	Ulchin 5&6	ABB-CE System 80+	WH AP-600	KNGR
Bistable Processor (BP)	2/Ch -PDC1 -PDC2	2/Ch with forward and reverse direction	2/Ch (Assignment by diversity)	2/Ch (Rx trip) 2/Ch (ESFAS)	Unification of BP/LCLP 1/Ch
Local Coincidence Logic Processor (LCLP)	Relay 2/3 Logic	4/Ch forward(2) reverse (2)	2/Ch (Assignment by diversity	2/Ch (Rx trip) 2/Ch (ESFAS)	
Comm. between BP/LCLP	Hardwired	CCC-Hi-speed Serial Link	CCC-Processors (3/Ch)	Parallel I/O Comm. Processor	CCC-Processors (3/Ch)

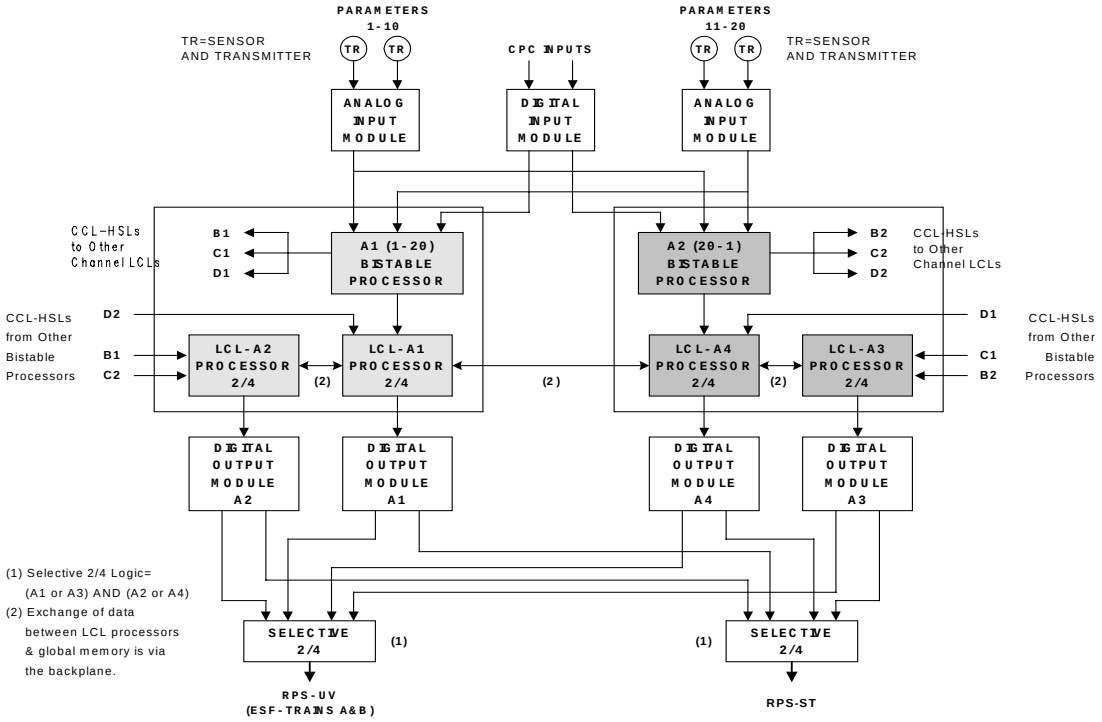


Figure 1 : Channel Block Diagram of DPPS (Ulchin units 5&6)

2. Diversity

In general, the design of digital system is distributing its function to accomplish the simplicity and to enhance the reliability due to the simplicity of software V/V. It is a current trend to design digital systems based on functional diversity. The protection system of Wolsung has two plant digital computers (PDCs) assigned by different trip parameters, therefore, even though one of PDC fails, the other PDC assigned as different trip parameters performs safety function. The protection of System 80+ is designed by principle of diversity similar to that of Wolsong plant. In case of Ulchin units 5&6, Korea, there are two BPs and four LCLPs per channel, they operate in reverse direction each other to implement the functional diversity. AP-600 system of Westinghouse has four BPs and four LCLPs, two BPs is for reactor trip and the other is for ESF. Different trip parameters are also assigned to two BPs and two LCLPs to implement the diversity. In this context, it is required that the DPPS of KNGR should be designed according to the principle of diversity.

3. Time Response and Performance

The distribution of function of BP and LCLP over the integration of them simplifies the design and enhances the system response time which may be used as a measurement of system performance. The integrated system controlled by one processor may increase the system response time and make more complex software compared with the separated processor (see Figure 1). Besides, even though the integrated system meets required response time, it may not be flexible to modify and expand its function because there is no sufficient margin after commercial operating. In general, it is practice to be designed with 40 % margin for the worst case. Multitasking and interrupting issues to design software may be also caused as opposed for deterministic processing.

4. Reliability of Software

Distribution of function of BP and LCLP may enhance the reliability by simplification of software and testability. As shown in Table 1, the functions of BP and LCLP are separated except that of KNGR. Besides, the distribution of function of BP and LCLP is to make software V/V easily and to minimize the fault of software. V/V effort needs a prohibitive amount of resource if design is too complex. Therefore, it is required that the design of software shall be simplified if possible.

III. Regulatory Approach of Soft Controller

1. Background

In the design of main control room (MCR) or remote shutdown panel (RSP), existing manual switches are replaced with soft controller on the flat panel display[5]. Soft controller controls safety related components as well as non-safety components as shown in Figure 2. As shown in Figure 2, the manual switches replaced with soft controller using a multiplexer can cut down the cost and optimize the operational sense. However, the safety classification of soft controller should be considered carefully since it controls directly components related to safety systems during and following the design bases events (DBEs). We describe the regulatory approach on the soft controller in the following subsections.

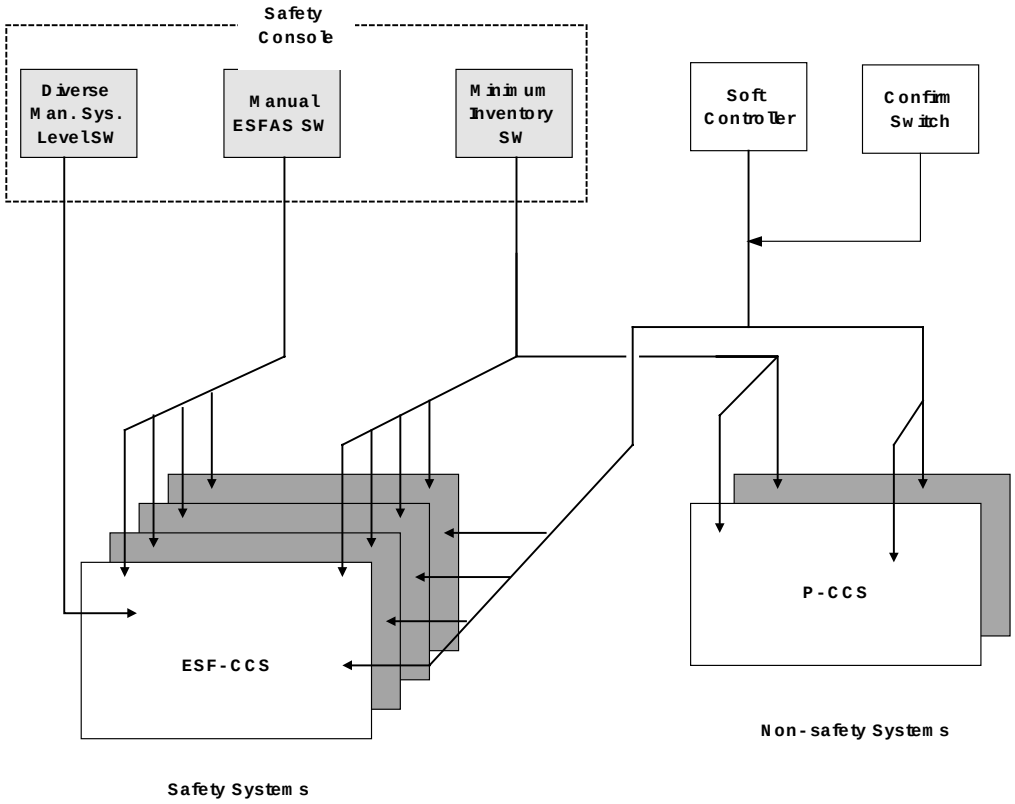


Figure 2: Soft Controller

2. Safety Classification of Soft Controller

As shown in Figure 2, diverse manual switches/controls for system level and minimum inventory switches classified into safety class are provided in safety console against the common mode failure of DPPS and DESFAS. Manual control switches on safety console are designed on the purpose of controlling safety-related systems during and following the design bases events (DBEs) using the hardwire-based control.

In accordance with requirement of IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Sections 6.2, and 7.2, "Manual Control" [3],[4] , soft controller shall be designed as a safety system because soft controller is utilized to perform the safety functions and corresponding protective actions of the execute features for each design basis event. However, only if the safety function can be completed using the manual controllers on the safety console such as manual ESFAS switch and minimum inventory switches excluding the soft controller, in the end, plant condition is capable of reaching at cold shutdown during and following the DBEs, soft controller may be classified into non-safety system.

As shown in Figure 2, soft controller is used in controlling both safety system and non-safety system. In relation with this, the existing regulations, regulatory guidelines and industrial standards require that equipment and circuit used in all of both safety and non-safety systems shall be classified into safety class and designed such that they meet requirements comparable with safety system.

Regarding capability of manual control by soft controller, the issues of man machine interface may be caused because soft controller is means replacing conventional control switches. Thereby, the performance of soft controller should be verified through dynamic simulation if it can assist the behavior of operator timely and appropriately under all anticipated situation.

3. Independence of Soft Controller

The control of component of conventional ESFAS is designed by dedicated control using the individual hand switches designed as a safety system and the physical separation among channels is maintained. Independence among channels is maintained in the view point of signal transmission by conform switch even though they are not separated physically. However, the design of soft controller in KNGR may not meet the channel independence and physical separation by using a multiplexer. Therefore, channel separation shall be maintained in accordance with relevant requirements.

IV. Regulatory Approach on the Defense-in-Depth and Diversity (D-in-D&D)

All protection systems of KNGR including a reactor trip system, ESFAS, and the plant control system (PCS) are designed on the basis of digital technology. Therefore, the postulated common mode failure of DPPS and DESFAS designed as a software-based digital system may have an adverse effect on the function of PPS and ESFAS. Diverse manual controls (e.g., backup systems) to comply with requirements on defense-in-depth and diversity (D-in-D&D) are implemented in the KNGR [1], [6]. These diverse controls are to be independent and diverse from the safety computer system, and to be located in the main control room (MCR) for manual system level actuation of critical safety functions.

The system-level circuitry is diverse from the component-level one under the assumption of different technologies and vendors. Therefore, we are able to assume that there is no chance of occurring common mode failures between these two levels. However, two kinds of backup panels have to be installed at the Main Control Room (MCR) or at the vicinity of MCR against common mode failures of each level. Firstly, the backup system at the system-level are added against loss of the DPPS due to common mode failures

and are totally diverse from the DPPS and the Alternative Protection System (APS) provided against ATWS events as shown in Figure 3. Thus, there are three layers of defense-in-depth at the system-level which are independent and diverse from among them. Secondly, the backup panel at the component-level is independent, diverse from that of the system-level and the PCS, so there are two layers of defense-in-depth. As described above, the regulatory approach for the hardwired backup systems provided against common mode failure of digitalized protection system is the same as those of Ulchin units 5&6 preceded by KNGR.

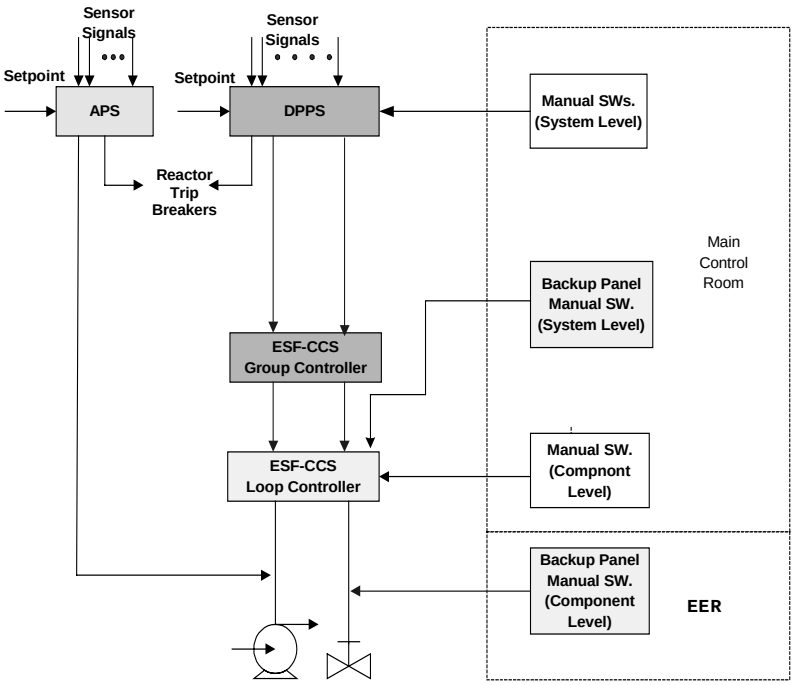


Figure 3: Backup Systems for DPPS

V. Conclusions

We have presented critical issues raised during reviewing the SSAR of KNGR (APR-1400), i.e., the integration of function of BP and LCLP, safety classification of soft controller and hardwired backup system against the common mode failure of digital system. Firstly, regarding the integration of BP and LCLP, we required utility to separate them to preserve their inherent functions to generate a trip signal and coincidence logic signal, respectively and the consistency with an analog system. Secondly, it was required that the safety classification of soft controller shall be classified into safety system in accordance with relevant requirements. Regarding the hardwired backup system, we required utility that two kinds of backup panels have to be installed at the MCR or at the vicinity of MCR, i.e., Electrical and Equipment Room (EER) against common mode failures of each level.

VI. References

[1] KINS/AR-622, “Preliminary Evaluation Report for Ulchin Nuclear Power Plant units 5 and 6,” Korea Institute of Nuclear Safety, March, 1999.
[2] B. R. KIM, “Current Status and Licensing Experience of Digital Instrumentation and Control Systems Important to Safety in Korean Power Plants,” IAEA Consultancy Meeting, Mar 13-16, 2001, Vienna.
[3] NUREG-0800, “Standard Review Plan,” Revision 4, Office of Nuclear Reactor Regulation, U.S. NRC, June 1997.
[4] P. J. Hughes and et al., “Instrumentation and Control Systems Important to Safety: A new IAEA Safety Guide,” Int. Topical Meeting on Nuclear Plant I&C, NPIC&HMIT 2000, WA. DC Nov, 2000
[5] John M. O’Hara and W. F. Stubler, “Soft Controls: Designing for Error Tolerance,” Int. Topical Meeting on Nuclear Plant I&C, NPIC&HMIT 2000, WA. DC Nov, 2000
[6] SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced-Light-Water (ALWR) Designs,” April 2, 1993

Decision Support for Approval of Safety Critical Programmable Systems.

Gustav Dahll[1], *Bjørn Axel Gran*[1] *and Bo Liwång*[2]

[1]*OECD Halden Reactor Project, P.O.Box 173, N-1751 Halden, Norway,*
Tel: +47 69 21 22 00, Fax: +47 69 21 24 40, E-mail (dahll,bjornag)@hrp.no
[2] *Swedish Nuclear Power Inspectorate,S-106 58 Stockholm, Sweden,*
Tel: +46 (0)8 698 84 92, Fax: +46 (0)8 661 90 86, E-mail bo.liwang@ski.se

Summary

One can distinguish between three principles for licensing: rule based, consensus based, and risk based. The paper discusses these three principles, and how they in practice are applied to software based systems. The Swedish nuclear regulatory body is drafting a new Inspection Handbook, where these principles are used in a lifecycle oriented framework. A methodology to combine these three principles in a systematic way, viz. Bayesian Belief Nets (BBNs) is described. An experimental study was performed to investigate the possibility to combine the BBN method with a software safety standard for safety assessment of software based systems. This was done by applying the approach on a real safety related program system.

Introduction

Due to the increasing use of programmable digital equipment in safety critical systems, the regulating bodies (in the nuclear power area as well as many others) faces the problem of licensing of such systems, in particular of the embedded software. There is therefore a clear need for methods and tools for assisting the licensing of safety critical programmable systems.

One can distinguish between three principles for licensing: *rule based, risk based and consensus based on expert judgement*. These three principles are discussed in section 2 with emphasis on how different information sources influence the decision for approval of safety critical software based systems.

The introduction in Sweden of programmable equipment in safety systems of nuclear power plants has been done successively. Along with this there has been a gradual development of the principles applied by the nuclear regulatory body in Sweden, SKI, for the approval of such systems. Section 3 describes the background and the preparation of a draft Inspection Handbook. This handbook is lifecycle oriented, i.e. the regulatory review should be made during the whole development of the system, and for each lifecycle phase it will be based on a combination of disparate evidences. A systematic way to combine such evidences is to use Bayesian Belief Nets (BBNs). This principle is discussed in section 4.

An experiment was made to investigate the possibility to combine the BBN method with a software safety standard for safety assessment of software based systems, by applying the method, on a test case, a real, safety related program system. This is described in section 5.

Principles for System Safety Assessment

Rule Based Safety Assessment

Rule based (also called deterministic) safety assessment means that the system must fulfill a certain set of rules to be approved for safety critical applications. The rules are easy to follow for the developer and easy to check for the assessor. On the other side, this method easily gets very rigid and inadequate to handle new technology.

Furthermore, the rules must be based on certain principles. Such principles may be based on laws of physics, be of probabilistic nature, or they can be of general nature, as e.g. the 'single failure criterion'. It is, however, difficult to establish such simple principles for software based systems. The rules for safe software are therefore rather based on consensus among experts of what is required for safety critical software. This is expressed through standards and guidelines.

Risk Based Assessment

There is a certain trend to change from rule based to risk based principles for licensing. This means to identify potential hazards from implementing a system in e.g. a nuclear power plant, and demonstrate that the probabilities of these hazards are kept under a certain safety integrity level. Probabilistic Safety Assessment (PSA) is therefore often required by the authorities, at least in the nuclear power area. The purpose of using PSA in nuclear power plants is to give an overall view on plant safety by identifying the initiating events of accidents, describe the event sequences, beginning from initiating events and leading to various plant damage states and radioactive releases. Further, PSA evaluates the plant risk quantitatively in probabilistic terms.

The PSA methodology comprises a variety of techniques which are partly complementary and partly overlapping. This means that in an actual analysis one will use a selection of PSA techniques. These techniques can be divided into two main categories: qualitative analysis and quantitative risk estimation. Qualitative analysis aims at identifying potential risks and their possible causes, and include methods like Fault Tree Analysis (FTA), Failure Mode, Effect and Criticality Analysis (FMECA), and Hazard and Operability (HazOp) analysis (IEC-812). The quantitative methods aim at giving probabilistic estimates of quantities related to risk, as e.g. probability of major accident, expected number of lost lives, etc. The results from the qualitative analysis are combined with probability figures associated with the different potential causes. These probabilities may be found by statistical analysis of actual events, or on the basis of engineering judgement or belief.

The PSA techniques has been applied in many decades, and was developed before programmable systems were used for safety related purposes. They are therefore best suited for conventional systems, and problems arise when programmable systems shall be analyzed, primarily due to their embedded software. There have, however, during the recent years been made several proposals to apply PSA techniques also to software systems, although they are not widely used in real safety cases.

Consensus on Safety Based on Expert Judgement

In practice, however, licensing authorities are often faced with the problem of approving systems for which there are no clear rules, and for which it is difficult to apply probabilistic methods. This is particularly a problem in software based systems. The rules given in standards and guidelines are often imprecise, or they are not directly applicable for an actual system. The practice seems to have been based on the opinion

of experts in various fields, including process knowledge, reliability engineering, human factors etc. The combined judgement of the different evidences about the system and its environment constitutes the basis for approval or not.

The acceptance process of a programmable safety critical system is based on a combination of disparate sources of information. This is illustrated in Figure 1 in the form of an 'influence net' where each node represents an aspect in the total assessment process. The top nodes in the graph represent the basic information sources which are used in the acceptance process. This information is penetrated through the net down to the bottom node, which represents the final acceptance of the system.

The latter is mainly influenced by the safety assessment of the system, although there may also be other acceptance criteria. The safety assessment is influenced by a reliability assessment of the system, as well as by an evaluation of whether a failure in the system will jeopardize safety. The latter can be achieved through a hazard analysis of potential risks to plant and environment. Safety defenses (both against hardware and software failures) may be implemented as additional barriers against consequences of failures. A commonly used principle in this respect is diversity, i.e. to obtain the same functional goal through different means.

The reliability of the system can be seen as an expression of the confidence one can have that the system contains no faults. There is also a possibility to make a reliability estimate based on test data and experience data using statistical models (e.g. reliability growth models). The confidence in fault freeness is based upon how well the system is made to avoid faults in the system, how the internal structure of the system makes it vulnerable to programming errors, and how complete the testing and other validation activities are performed. The basic information sources are:

Information about producer. The 'producer' in this context comprises both the company which develops the actual system which shall be approved for safety-related application, and vendors of COTS (Commercial Off The Shell software) modules which are applied. This information includes reputation and experience of the producer, quality assurance procedures, quality of staff, etc.

Information about production. A high production quality enhances this confidence in a system. This implies that the system is developed according to guidelines for good software engineering, that all phases are well documented, and that the documentation shows that the system at all development phases possesses desirable quality attributes as completeness, consistency, traceability etc.

Information about previous usage. The producers of COTS often use 'proven design' as an argument for high reliability. This means that the system has been used by a wide range of users over a long period, with no, or few, reported faults. The idea behind the claim of proven design is that long user experience should reveal all inherent faults, if they exist. So if no faults have been reported over a long period, this should be a strong indication on error freeness. It is questionable, however, whether this is sufficient. A COTS based system has often a quite general purpose, and may consist of many standard modules, each of which has many modes of operation. To claim general high reliability of the system based on user experience, it is necessary to show the experience with all modes of operation of all software modules. This requires information about all installations of the system.

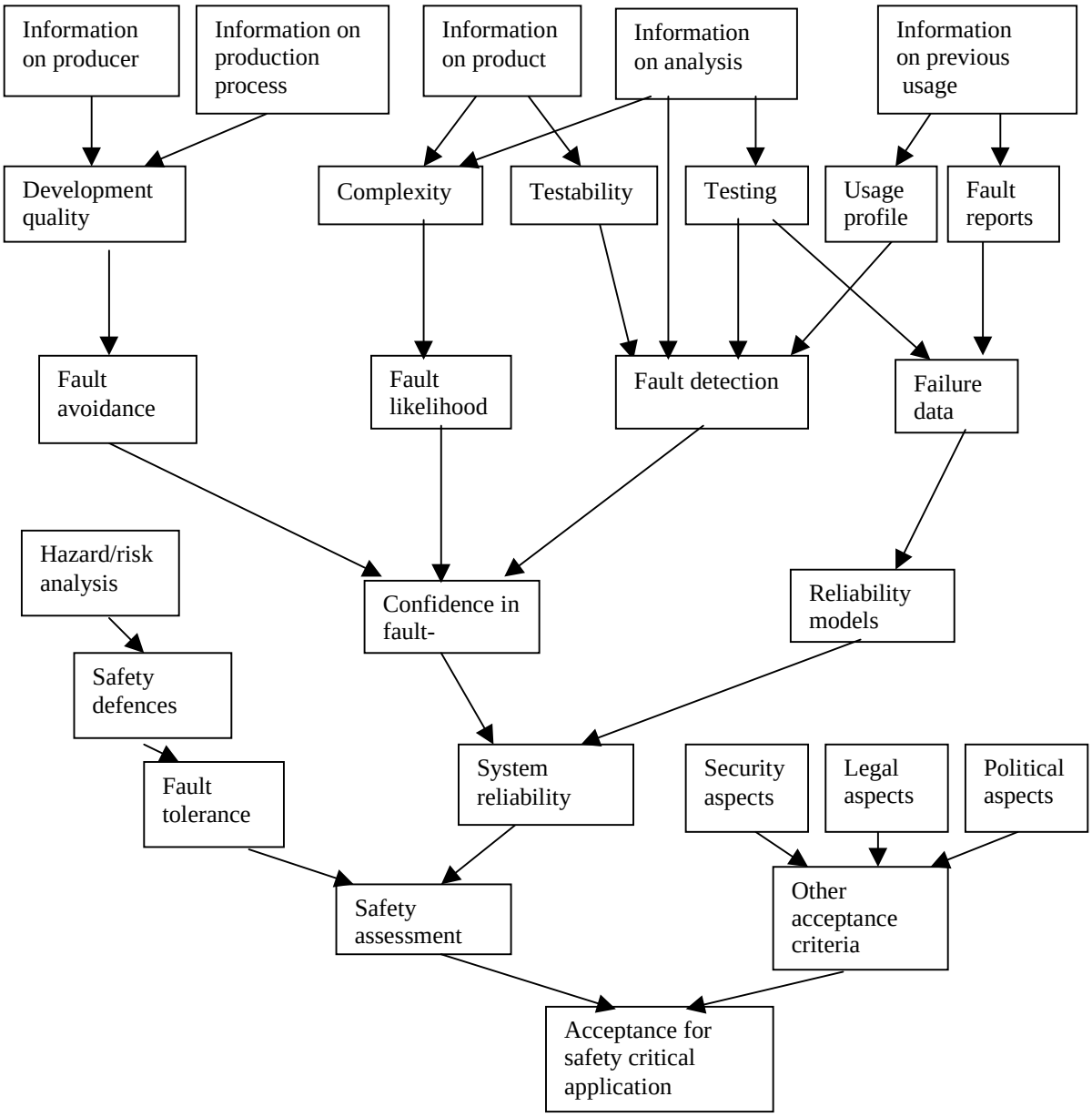


Figure 1 Influence graph of a safety acceptance and acceptance process

Information about the product. Even if a high quality production process presumably leads to a high quality product, there are certain quality attributes the final product should have, as reliability, simplicity, verifiability etc. This yields both the application software and COTS components. However, there is often a limited amount of available information about COTS at code level, so alternative information sources must be used. A main source of information about a software module is found in the specification. A complete, consistent, formal etc. specification is not always available for COTS module, but a functional specification should at least be deducible from the user manual.

Information about the analysis. This includes all activities performed to verify the correctness of the system. The analysis should be performed at the module level, and on the program as a whole. Ideally this activity should be made during all stages of the system development, as e.g. model checking of the

specifications, inspections and walkthroughs of the documentation, static analysis of code and testing of the system.

Development of ”draft Inspection Handbook” at SKI.

The nuclear regulatory body in Sweden, SKI, has not the possibility to perform a detailed technical review of a proposed new digital safety system; it has not the manpower or detailed technical expertise to do that. According to the legislation in Sweden the utility has the full responsibility for the safety of the NPP. SKI shall review that the licensee takes this responsibility in a proper way.

From 1995 SKI participates in ”Task force on safety critical software” within the EC. The purpose is to present a consensus view and recommended practices for selected issues. Both generic issues and life cycle phase licensing issues are selected. Reports has been released in 1998 and in 2000 (EC, 2000).

In Sweden a strategy for the regulatory work has been developed where an ”Inspection Handbook” is one of the tools. The strategy is to perform a review of the different types of information in the design process at the utility in what is called a Safety Demonstration and a Safety Plan. In the EC document EUR 19265 (EC, 2000) it is stated:

”Evidence to support the safety demonstration of a computer based digital system is produced throughout the system life cycle, and evolves in nature and substance with the project. A number of distinguishable types of evidence exist on which the demonstration can be constructed. The task force has adopted the view that three basic independent types of evidence can and must be produced:

- evidence related to the quality of the development process;
- evidence related to the adequacy of the product;
- evidence of the competence and qualifications of the staff involved in all of the system life cycle phases.

In addition, convincing operating experience may be needed to support the safety demonstration of pre-existing software.”

The report gives also a definition of the Safety Plan: ”A safety plan shall be agreed upon at the beginning of the project between the licensor and the licensee. This plan shall identify how the safety demonstration will be achieved. More precisely, the plan shall identify the types of evidence that will be used, and how and when this evidence shall be produced.”

As seen it is the utility that has the responsibility to give the evidence that all safety aspects has been taken care of, but the regulatory body must also know, based on the safety importance of the system, what aspects that is needed to review.

The Framework.

As the Safety Demonstration and the Safety Plan covers the total lifecycle of a project from the first concept to decommissioning, it is necessary to get knowledge of what impact on safety the different activities in the development process has. Several of the issues of interest are not directly observable, for example the quality in the design process.

To get a better structure of the review work at SKI, discussions started with IFE/Halden to develop a theoretical framework on the safety impact from different activities, or ”how to get information on issues

that are not directly observable" (Dahll and Liwång 1999). As a model of the different steps in a development process the structure in the IEC 61508 "Functional safety of electrical/ electronic/ programmable electronic safety-related systems" was used. For each of the phases in the model the framework associates a corresponding set of milestones. At each milestone there should be a check that the intended safety goal is preserved. This check could be rule based but this may become a rigid procedure. Instead an alternative was used where these checks are made on a measure of combined evidences from different information sources available about the system at the milestone. The set of milestones and corresponding milestone goals are shown in table 1.

Milestone	**Milestone goal**
Concept	Preparedness
Overall requirements	Completeness
Hazard and risk Analysis	Safety of concept
Requirement specifications	Dependable specifications
Project planning	Quality of plans
Overall System Design	Dependable design methodology
System realisation (Detailed design, programming and system integration)	Dependable system
System validation	Validated system
System installation	A safe system put in operation
Maintenance and modification procedures	Safety preserved during operation.

Table 1. The set of milestones and corresponding milestone goals.

For each of the milestones and corresponding goal there is a discussion of the set of evidence that influence the goal. As the intention is that it shall be easy to follow and understand during the development process, each milestone is illustrated with a graphical influence net model. This shows the observation and corresponding documentation, which are of importance, and how they influence the attainment of the safety goal at each milestone.

To facilitate the practical use in the regulatory review process a set of questions, with comments, are developed which reflects the structure of the influence net for each milestone. An example of the influence net for milestone goal "preparedness" in the milestone Concept can be seen in figure 2.

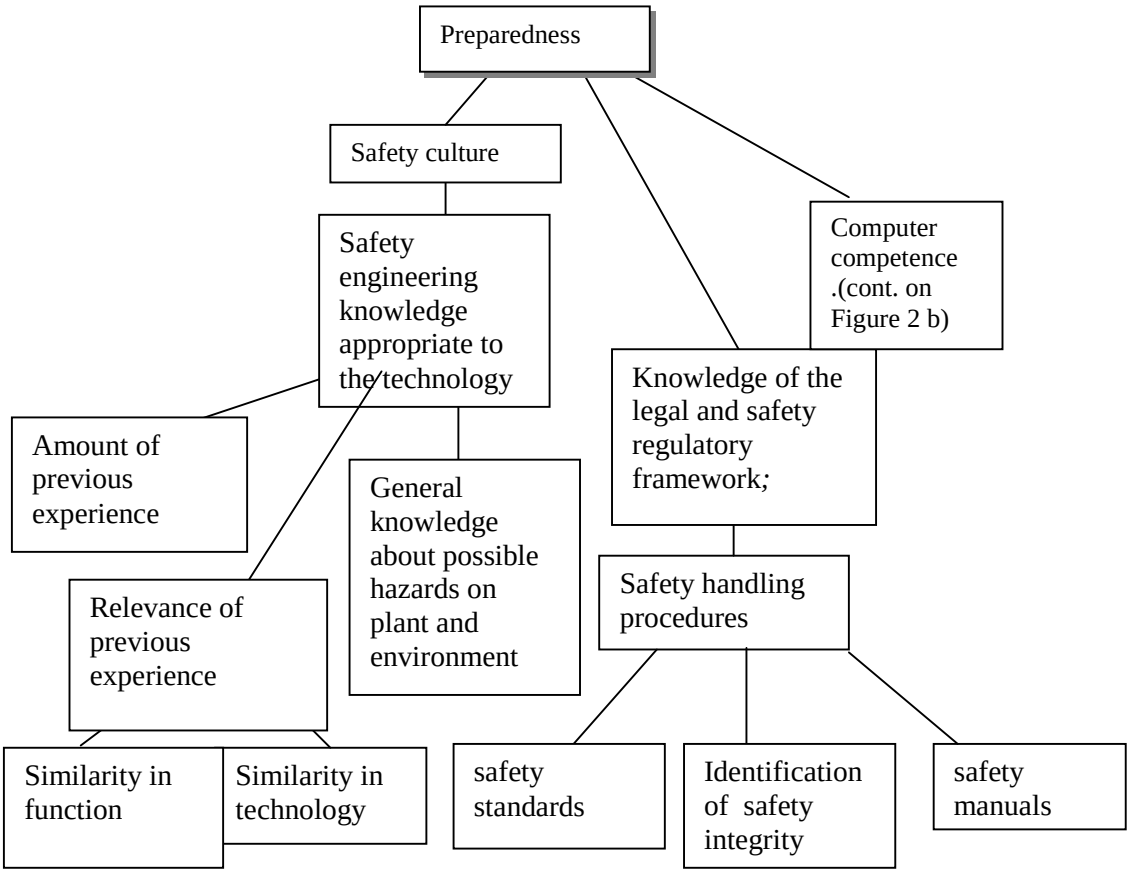


Figure 2a Influence net for milestone *Concept*

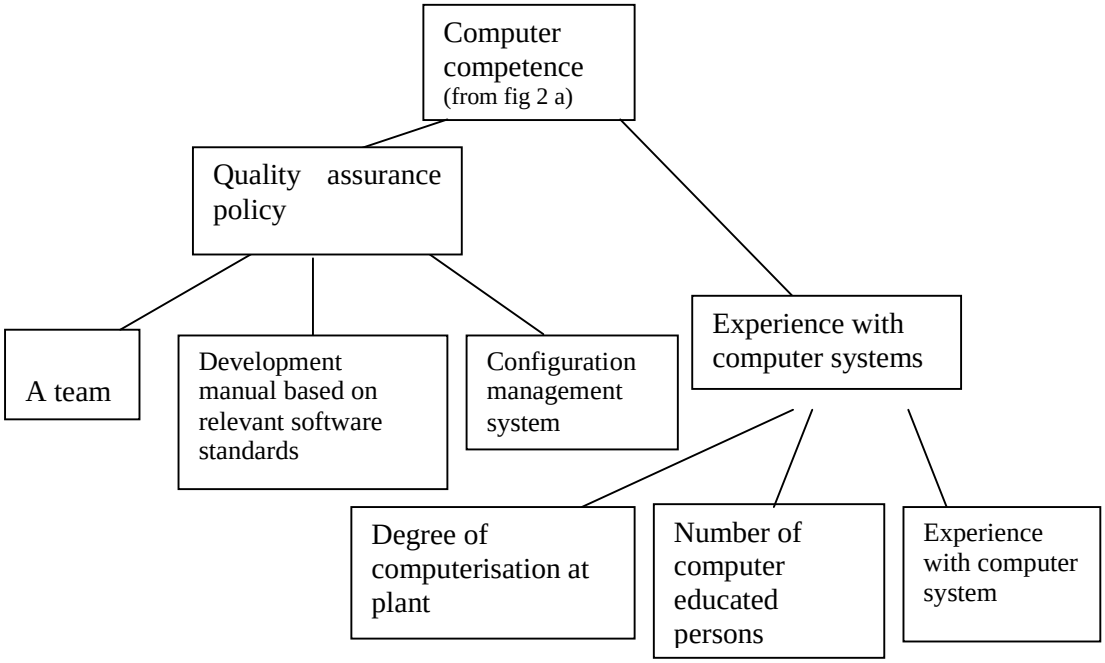


Figure 2b Influence net for milestone Concept (cont.)

The Handbook

The last step in the development of the ”Regulatory Inspection Handbook” is integration of information, criteria and issues from other activities into the influence net framework from the IFE/Halden work. This work was performed by Norman Wainwright, a former NII inspector, in Cupertino with SKI (Wainwright 2000). Most additional material comes from the EC document EUR 19265, presented above, and guides from International Atomic Energy Agency but also from relevant IEC guides.

The structure, milestones and influence net was unchanged from the previous framework but the questions and in particular the corresponding discussion and comments were expanded. The purpose is not to present exact criteria, more to be a background information for an overall safety evaluation and an evaluation of the presented evidence in the safety demonstration.

As a further development the draft inspection handbook will be used and evaluated in the review process for the new safety I&C system for Oskarshamn 1. A handbook like this is not a one time activity, it is a ongoing process to evaluate the technical development and research results to take necessary decisions on modification of regulatory review strategies and the supporting documents.

Bayesian Belief Nets

The use of Bayesian Belief Nets (BBN) has been proposed to combine evidences from different information sources in quantitative assessment of the confidence in a software based system. This methodology has mainly been developed and applied in the AI society. More recently, however, it has also been applied to software safety assessment. Work in this area has been performed in two ESPRIT projects: SERENE (SERENE 1999) and DeVa, and at the Centre for Software Reliability at City University in London (Fenton et. al. 1998) and at the Halden Project (Dahll and Gran 2000).

A Bayesian Belief Net is a directed graph consisting of a set of nodes connected by a set of edges. Both events and singular propositions are associated to each node, where the uncertainty is expressed by a probability density. The probability density expresses our belief about (or confidence to) the various variables. This probability depends conditionally on the status of other nodes at the incoming edges to the node. Some nodes are denoted as ‘observables’, and they represent the different observable properties about the software system and its development. The network edges model relations between adjacent nodes. The strength of these relations is represented as conditional probability distributions. The computation of our belief about a specific node (target node) is based on the rules for probability calculations using Bayes’ formula.

Application of the BBN method consists of three tasks:

Construction of BBN topology: This is made by combining the target node(s) with the observable nodes and the intermediate nodes. The aim is to combine all available relevant information into the net. One way to do this is to start from a target node and draw edges to nodes influencing this. Then from these nodes one can draw edges to new nodes, and in this way gradually build up a large BBN. One problem, however, is to decide when to stop, i.e. how much details one wants to have in the BBN. The practical procedure is to start with constructing a BBN, containing nodes representing high level information. The diagram in Figure 1 is not itself a BBN, but quite similar, so it is fairly straight forward to construct a high level BBN for safety assessment based on this.

Elicitation of probabilities to nodes and edges: The next step is the elicitation of probability distribution functions (pdfs) to the nodes and edges. To begin with one gives prior pdfs to variables to the top nodes (and optionally some others), and conditional pdfs for the influences represented by the edges. These pdfs may be either continuous functions or they may be in the form of conditional probability tables. The latter means that the ranges of the variables are divided into finite numbers of states.

Making computations: The computation method is to insert observations in the observable nodes, and then use the rules for probability calculation backward and forward along the edges, from the observable nodes, through the intermediate nodes to the target node (which again can be an intermediate node in a BBN at a higher level). To make computations with BBNs of a certain size and complexity computer tools are necessary. One description of a computational method is given in (Jensen 1993) with reference to the associated tool HUGIN (Aldenryd et al. 1993).

Combining BBN with the Rules of a Standard.

As a way to combine rule-, risk- and judgement based methods in licensing, an attempt has been made to combine the BBN technology with the rules of a standard for safety critical software. This was done in an experimental project carried out by a consortium composed of the OECD Halden Reactor Project, Kongsberg Defence & Aerospace AS and Det Norske Veritas. This project emphasizes the practical evaluation of the proposed methodology by trying it out on a realistic test case: a computerized system for geographical localization of helicopters. The main purpose of this system is to aid in a rescue operation if the helicopter has made an emergency landing on the sea. A correct localisation is necessary for a successful rescue operation, and the system is therefore safety critical. The system had to be approved by the Norwegian Civil Aviation Authority, and the standard for safety critical software in civil aviation, DO-178B (RTCA/DO-178B, 1992), was applied.

The project consisted of several tasks. The first was to construct BBNs on the basis of DO-178B. Even if this standard is branch specific, conclusions from this project will be of general value, since the different standards for safety critical software have similar structures. The BBN was constructed in two levels. The higher level (see Figure 3) shows how nodes representing four quality aspects, viz. *quality of the producer, quality of the production process, quality of the product*, and *quality of the analysis*, are combined with other nodes in the net, and lead to nodes representing the reliability and safety of the system.

The lower level BBNs were constructed by identifying the quality aspects with top-nodes in four BBNs. Each top node is linked to intermediate nodes representing the 10 lifecycle processes represented by the tables A1 to A10 of DO-178B. Each of these nodes was again linked to other intermediate nodes, representing the objectives of the tables (see Figure 4).

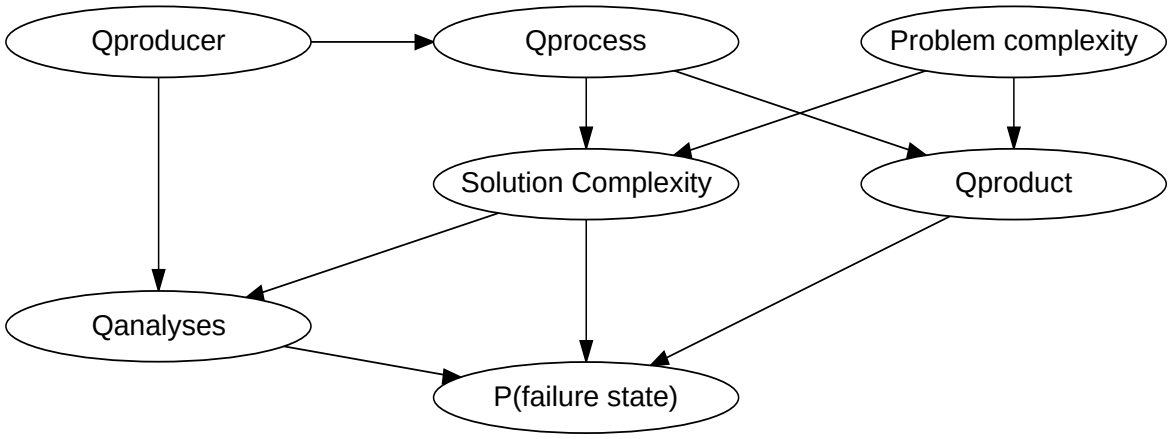


Figure 3. The BBN for the higher level

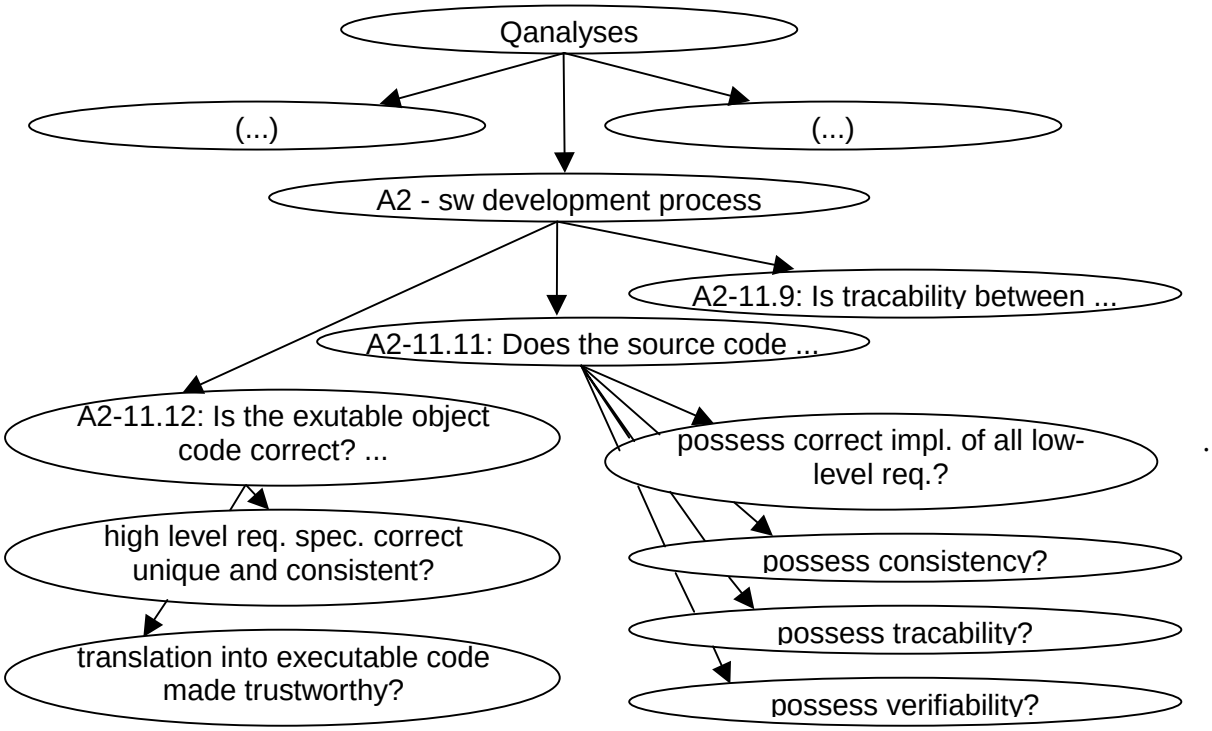


Figure 4. A part of the BBN for the '*Quality of the analysis*'

The further step was to identify a list of questions to each objective. These questions are based of the understanding of the text in the main part of DO-178B, and they are in general formulated so that the answer can be given by a 'yes' or a 'no', or a number between 0 and 1 as an expression of the strength in the belief that the answer is 'yes' (1) or 'no' (0). These questions were answered by the developer of the software, based on their experience from the system development. The elicitation of pdfs to the nodes and edges, in terms of conditional probability tables, was done as a 'brain storming' exercise by all project participants, based on general knowledge and experience in software development and evaluation. Finally

all this information was fed into the HUGIN and SERENE tools, to make a variety of computations, with the aim to investigate different aspects of the methodology (Gran 2000):

- What is the effect of observations during only one lifecycle process?
- How does the result change by subsequent inclusion of observations from the lifecycle processes?
- How sensitive is the result to changes in individual observations?

Summary and Conclusions.

The objective of this paper has been to describe ways to decision support for approval of safety critical software. Such decisions are made by rule- and risk- as well as consensus based principles combining, information from a variety of disparate evidences. The approval process should not only be made on the basis of the completed system, but should closely follow the development process. This is reflected in the draft Inspection Handbook prepared by SKI.

Software safety standards typically contain a variety of recommendations or requirements to be fulfilled during the development and validation of a system. The degree to which each of these is fulfilled constitutes a set of evidences, and these form the basis for the decision on approval. Bayesian Belief Nets has been proposed as a systematic way of combining disparate evidences.

A methodology to combine this with expert judgements and observations related to the rules/recommendations of a software safety standard was experimentally applied on a real safety related system. The experiences from this experiment led to the conclusion that the BBN methodology offers a systematic way to combine quantitative and qualitative evidences of relevance for the safety assessment of programmable systems. The most difficult activity was to perform the expert judgement, in particular in the assignment of values to the conditional pdfs. The establishment of the BBNs and prior pdfs was rather time consuming. However, the process of building up the network, e.g. by making questionnaires, and the elicitation of the prior pdfs were related to DO-178B, and not to the actual system. This implies that these have a general nature, and can be reused in many applications

Acknowledgement

The project team that performed the referred experimental project was, in addition to the authors Dahll and Gran, Siegfried Eisinger from Det Norske Veritas, and Eivind J. Lund, Jan Gerhard Norstrøm, Peter Strocka, and Britt J. Ystanes from Kongsberg Defence & Aerospace AS.

References

Aldenryd S.H., Jensen K.B., Nielsen L.B., 1993. "Hugin Runtime for MS-Windows". Tool made by Hugin Expert a/s, Aalborg.

Dahll, G. and Gran, B.A., 2000. "The Use of Bayesian Belief Nets in Safety Assessment of Software Based Systems." *Int. J. General Systems*, 29 (2), 205-229.

Dahll, G and Liwång, B, 1999 "Lifecycle model oriented safety assessment of programmable systems." Presented at OECD Halden Reactor Project EHPG Meeting, Loen, Norway, 24-29 May, 1999

EC, 2000 "Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors". EC – Nuclear safety and the environment, May 2000, EUR 19265 EN

Fenton N., Littlewood B., Neil M., Strigini L., Sutcliffe A. and Wright D., 1998. "Assessing Dependability of Safety Critical Systems Using Diverse Evidence." *IEEE Proc. on Software Engineering*, 145 (1), 35-39.

Gran. B.A. et. al., 2000. "Estimating Dependability of Programmable Systems Using BBNs." SAFECOMP'2000, Rotterdam, Oct.25th. – 27th.

IEC-publication 812, "Analysis Techniques for Systems Reliability - Procedures for Failure Mode and Effects (FMEA)." 1985.

Jensen F., 1993. *An introduction to Bayesian Networks.* UCL Press, University College London.

RTCA/DO-178B. "Software Considerations in Airborne Systems and Equipment Certifications." , 1992

SERENE, 1999. The SERENE Project. http://www.hugin.dk/serene/.

Wainwright, N., 2000 Guidelines for the assessment and approval of software based safety systems Final draft for SKI (unpublished) July 2000.

TECHNICAL SESSION 1:
NATIONAL AND INTERNATIONAL COMPUTER-BASED STANDARDS AND GUIDES FOR SAFETY SYSTEMS
Chairmen: J.-P. Bouard, Z. Ogiso

International Standardisation in Nuclear I&C Engineering

Jean-Paul BOUARD

IEC Sub-Committee 45A Secretary

SYNOPSIS There is a temptation to treat standards work as boring, tedious and not value-added! As explained in this paper, however, standardisation usually leads to economic development and increased sales. This and other reasons for international standardisation are presented, together with a brief outline of the history and operation of the International Electrotechnical Commission (IEC), which, together with the International Standards Organisation (ISO) is responsible for the preparation and maintenance of many of the world's International Standards. The paper then focuses on standardisation in the nuclear instrumentation and control sector and highlights current work being done within IEC Technical Committee TC45, and more particularly SC45A.

1 INTRODUCTION

Standardisation has been important since the industrial revolution and is normally driven by demands for:

- The interchangeability of products and
- Standard methods of measuring and assessing quality and performance.

Looking back over the decades, the most common result of national and international standardisation has been increased trade, although of course, some products are squeezed out of the market by standardisation; the story of the Betamax video recorder is the best known example of this. It may not be surprising to learn therefore, that one of the primary objectives of both the ISO and IEC is to foster trade and commerce.

Standardisation in nuclear engineering is important for the same reasons, but in addition there are other more specialised but equally valid justifications for standardisation. Most stem from the capital intensive nature of the work and from the need to promote safety on a world wide scale. In such respects there are analogies with the aircraft industry. Some other factors are worth noting here since nuclear engineering is by definition a specialised business employing a unique combination of engineering disciplines and skills.

- Firstly the need to share experience. Different countries are at different stages of nuclear development and, in some cases at least, progress and safety depend on the availability of appropriate codes of practice. Documents such as the IAEA Safety Guides are very useful in this regard but they tend to concentrate on principles whilst guidance is also needed on practical design matters. Although many countries have their own National Standards, the trend towards the adoption and use of International Standards is supported by many Nations, and one could argue that international standards represent the best codification of good practice.

- Secondly, standardisation also helps to promote a common technical language together with strong, technical infrastructures on which economies and indeed, safety depend. This is a feature of nuclear power development which has been emphasised by the IAEA.

- Thirdly there is the issue of continuity of both skills and the supporting industrial base. In many countries nuclear programmes are stagnating and fundamental and background development work is being curtailed. Such restrictions reduce the training of future generations and one way of minimising the impact of this - admittedly not the best - is by standardisation.

- Finally, then, in the nuclear industry, standardisation is a route to improved safety. This is particularly important in an environment in which the perception by the public of nuclear power is poor and based predominantly upon non-scientific judgements.

This paper describes some of the work which is being done to meet these needs through the International Electrotechnical Commission (IEC). The purpose of this paper is to remind readers of the existence of this well integrated, international standard organisation; to demonstrate its experience and to indicate how people and organisations can use it to help standardise needs. It also concentrates on IEC Technical Committee 45 (Nuclear Instrumentation) and the Sub-Committee 45A because of their relevance.

2 THE STRUCTURE AND PARTNERS OF THE IEC

The IEC was founded in 1906 and is the oldest independent International Standards organisation. The membership consists of more than 50 participating countries, including all the world's major trading nations and a growing number of industrializing countries. Together they represent more than 80% of the world's population and produce more that 95% of the world's electrical energy. A survey several years ago indicated that around 50% of the world's trade is with goods which complied with international standards.

2.1 Partners

International Partners

ISO and ITU

The IEC works closely with its international standardization partners, the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU), other regional standardization organizations and international organizations, including the World Health Organization (WHO), the International Labour Office (ILO) and the United Nations Economic Commission for Europe (UNECE). An initial agreement was signed with ISO in 1976 and ten years later the two bodies established Joint Technical Committee 1 (JTC 1) to cover the vast and expanding field of information technology.

Governmental Agencies

One of the IEC's principal partners is the World Trade Organization (WTO), whose 100-plus central government members explicitly recognize, through their Agreement on Technical Barriers to Trade (TBT), that international standards play a critical role in improving industrial efficiency

and developing world trade. These relations at government level are of particular importance in heavily regulated areas like safety, health and the environment.The number of standardization bodies which have accepted the Code of Good Practice for the Preparation, Adoption and Application of Standards presented in Annex 3 to the WTO's Agreement on Technical Barriers to Trade underlines the global importance and reach of this accord.

The IEC encourages industrializing nations to share in the benefits of joining in its work and liaises closely with the International Monetary Fund (IMF), the European Bank for Reconstruction and Development (EBRD), the World Bank, and the United Nations Development Programme (UNDP).

Regional Partners

At the regional level, the IEC works to achieve harmonization of standards among regional standardization organizations, such as CANENA, CENELEC, COPANT, EASC, ETSI and PASC. A joint working agreement exists with the European Committee for Electrotechnical Standardization (CENELEC), comprising some 20 IEC National Committees. In addition, the IEC has agreements with COPANT, EASC and ETSI (IEC/ETSI agreement), based on the exchange of information.

Co-operation between the IEC and CANENA

The co-operation agreement between the IEC and CANENA (Council for Harmonization of Electrotechnical Standards of the Nations of the Americas) signed in September 2000 relates to:

- promoting the use of IEC standards with CANENA members and
- enhancing technical cooperation in standards development.

This agreement is expected to be instrumental in ensuring a rational use of available resources in standardization activities and transparency of the standards process, thus facilitating world trade. It will also accelerate the standardization process and promote the development and implementation of IEC standards in response to market demand.

Co-operation between the IEC and CENELEC

The co-operation agreement between the IEC and CENELEC (European Committee for Electrotechnical Standardization) ratified in September 1996, and commonly known as the Dresden Agreement, relates to:

- common planning of new work
- parallel IEC/CENELEC voting

The object of this agreement is to avoid duplication of efforts, speed up the preparation of standards and to ensure the best use of the resources available and particularly of experts' time. If the results of parallel voting are positive in both the IEC and CENELEC, the IEC will publish the international standard, while the CENELEC Technical Board will ratify the European standard.

2.2 IEC Structure

The IEC carries out its business in three official languages - English, French and Russian. Almost all of the working meetings are conducted in English but the Standards are published as bilingual documents in French as well as English. They are also translated into Russian.

Each member country interfaces with the IEC through its own, internal, national committee and the IEC is, in effect, governed by these national committees through a Council and a Committee of Action to which a number of Advisory Committees report. These bodies control the work of more than 100 Technical Committees (normally abbreviated to TC's) and more than 80 technical Sub-Committees (SC's) each of which is responsible for a precise, technical field. Also, there are also 10 technical specialist committees such as those associated with the International Special Committee on Radio Interference (CISPR).

Sub-Committees can be established by any technical committee, although not all TC's chose to do so. It depends primarily upon the workload and the availability of expertise. However, both types of committee operate in much the same way. The Technical Committees, of course, have to report to the Committee of Action.

The work can be classified under five main headings:

- The development of common means of expression, vocabulary, graphical symbols, units (plus their associated letter symbols).

- The generation of standard methods of test or of declaring equipment performance. Such methods permit the ready comparison of claims regarding quality or performance. These tests are not specified as the minimum mandatory requirements although purchasers and suppliers often agree to interpret them as such.

- Agreeing levels of quality or performance arrived at by such standard test methods.

- The agreement of design features, either mechanical or electrical, which enhance interchangeability and encourage common usage throughout the world.

- Increasing safety to personnel, something which is very pertinent to the nuclear community.

All of these, even the first, are important to the nuclear industry. It is sometimes argued that communication is not a serious problem in science based technologies because of the widespread use of mathematics and of only one or two languages. However, those active in the international field quickly learn that there as many concepts of, say, English as there are people to speak them and that misunderstandings easily occur. Vocabulary, often thought of as a Cinderella subject, is therefore much more important than might be perceived.

Based on these five headings, the working scope of every Technical Committee falls into one of two distinct classes; those concerned with the enabling technologies and those writing detailed Standards on applications within specific industrial sectors. This means that Technical Committees exist which are devoted to, for example,

- terminology and related matters;

- materials and basic technology;

- electronic components such as lamps, fuses, cables etc;

And on the other hand, there are Committees devoted to:

- power generation, or

- the performance, safety and/or reliability of electrical systems and equipment in different industrial sectors (telecommunications, nuclear, aerospace).

TC45 is responsible for International Standards in the field of Nuclear Instrumentation, with Sub-Committee 45A covering Reactor Instrumentation and Sub-Committee 45B looking after Radiation Protection Instrumentation.

The IEC Council and the Committee of Action control the way in which Committees work by means of Directives (1) and Administrative Circulars. These seldom, if ever, mention detailed technical subjects. They are much more concerned with the programme and progress of the work, the interfaces with other Technical Committees and the working process since the technical content is the prerogative of national committees. Naturally, the Committee of Action is concerned with the coordination and the prevention of overlap and actively encourages liaison between the TC's. For this reason each Technical Committee is obliged to prepare a "Strategic Policy Statement" clarifying its domain, the current work and the predicted future trends.

In a body which has been active for nearly 90 years one might expect a degree of ossification but this is not so and the directives evolve continually. For example, a matter of recent concern has been the time taken for some documents to emerge and the latest edition of the Directives specifies a 3 year target duration for the issue of a new International Standard. Another important change in recent years has been the harmonisation of the IEC and ISO directives into the same document.

3 THE ROLE OF NATIONAL COMMITTEES

The main work of the TC's and SC's is carried out by working groups, comprising of experts from member Nations who do the detailed drafting of Standards. A national committee which wishes to participate in a particular field or piece of work nominates national delegates to the relevant TC or SC and may also send experts to the associated working groups. In most cases, of course, the same individuals are involved but they operate, or should operate, in different ways in the two environments. In the working group experts discuss drafts as individuals with, it is hoped, no insuperable national bias. They may generate any number of drafts (within the time limit) but their work remains amongst themselves and is sometimes the subject of very frank discussion! When they are satisfied, the resultant document is submitted to the parent committee for distribution to the National Committees who then express a considered national view.

This structure can be confusing but it also has the great advantage of permitting any individual in any member country to propose and more importantly, to contribute personally to the work. If anybody wishes to participate in this work, he can offer his services to the appropriate committee. At the very least, since draft documents are published for public comment, anyone can write to the secretary of the specialist committee.

4 THE METHOD OF WORKING WITHIN A TECHNICAL COMMITTEE OR SUB-COMMITTEE

The secretariat of each TC and SC is held on a voluntary basis by one of the national committees. This national committee is appointed by the Committee of Action and is in turn responsible for appointing a secretary. He (or she) must always act in an international way, divesting himself of any national point of view. The Chairman is nominated by the national committee holding the secretariat but is appointed directly by the Committee of Action on personal merit after views of the Nations have been sought. Thus, chairmanship is entrusted to an individual whilst national committees undertake secretariat duties and appoint a secretary. Both are supported by a relatively small Central Office organisation in Geneva.

Topics for standardisation work are decided by the national committees. Proposals for new work are set out in a formal way - preferably complete with a first draft - and circulated to the rest of the Nations by Central Office. Comments are made and majority voting decides whether the project is to go ahead. A feature of this procedure is that work does not start unless an adequate number of national committees agree to take an active part. In addition, a target completion date is agreed for the new Standard.

Working groups develop the document and in due course the TC or SC decides that the draft is good enough to be formally submitted, as a so called Committee Draft (or CD), to all national committees for written comment. As noted already, this provides an opportunity for input from a wide range of people and organisations. The resulting comments are usually resolved in the appropriate Working Group and, if necessary, further editions of the CD are circulated. The next stage is to circulate the document as a Committee Draft for Voting. The vote is to approve the issue of the document as a Final Draft International Standard (or FDIS). Further formal voting then leads, hopefully, to its being accepted, edited and published. Overall, then, there are three stages of formal voting from the first proposal for new work through to publication. The rules which control this process appear in the IEC Directives and, although apparently complex, are close to the minimum necessary to guarantee high quality standards which command international consensus and at the same time are acceptable by each nation.

5 RELATIONSHIPS BETWEEN TC45 AND THE IAEA

In 1974, the IAEA started the Nuclear Safety Standards (NUSS) programme to provide member states with internationally agreed recommendations on the safety of land based thermal neutron power reactors. This programme covers areas of governmental organisation (for the regulation of nuclear power), siting, design and operation as well as quality assurance. The Code of Practice on design sets out the basic safety principles while fourteen Guides enlarge on the more important principles. In particular, three guides are concerned with instrumentation and control:

- 50-SG-D3 on Protection and Related Features in Nuclear Power
- 50-SG-D7 on Emergency Electrical Systems at Nuclear Power Plant
- 50-SG-D8 on Safety Related Instrumentation and Control Systems in Nuclear Power Plants.

These three guides address the subject matter from the safety philosophy viewpoint and are not technical standards. They do, however, overlap the earlier IEC 231 series.

As a result of this potential for duplication and even contradiction between IAEA Documents and IEC technical standards, a formal agreement of co-operation was reached in 1981 between the IAEA and the IEC/Technical Committee 45.

The Agreement states that:

- the IAEA is responsible for the development of safety principles for instrumentation, control and electrical systems in Nuclear Power Plants,
- IEC/Technical Committee 45 is responsible for the design requirements that realise these safety principles
- TC 45 is invited to participate in the development of the relevant IAEA Safety Guides and
- the IAEA is invited to participate in TC45 Meetings.

Close co-operation has continued since then with the common goal of preparing Safety Guides and Standards for the design of instrumentation and control systems which significantly add to the safety and operability of nuclear power plants.

6 IEC/TC45 - NUCLEAR INSTRUMENTATION

TC45 is the only true nuclear technical committee of the IEC. It was set up in 1960 at the IEC General Meeting in New Delhi and the current scope is "To prepare International Standards relating to the electrical and electronic equipment and systems for instrumentation, specific to nuclear applications."

The present chairman of TC45 is Mr Richard Schomberg from France and the secretariat is currently held by the Russian Federation (Mr Youri Seldiakov).

TC45 has 6 Working Groups (WG) dealing with:

- WG 1: Classification - Terminology
- WG 3: Interchangeability
- WG 6: Electrical measuring instruments utilizing radioactive sources
- WG 9: Radiation detectors
- WG 10: Multichannel analyzers and systems based on them
- WG 14: Nuclear instrumentation for geophysical applications

There are also two Sub-Committees.

SC45A Reactor Instrumentation:

- Was formed in 1963 and is concerned with "Electronic and electrical functions and associated systems and equipment used in the instrumentation and control systems important to safety of nuclear power plants. This includes the radiation monitoring instruments used directly for plant control or safety actuation. A major consideration is the application of emerging electronic techniques to nuclear requirements, particularly computer systems and advances in information processing and control, including artificial intelligence. Part of its strategic task is to review IAEA safety codes in order to identify detail technical aspects for which standards are appropriate."

- The chairman, Mr E. Corte, is from the USA and the secretariat is held by France (Mr Jean-Paul Bouard),

- Seven Working Groups report to SC45A:

    - WG A2: Nuclear reactor measurement, control and safety instrumentation

    - WG A3: Application of digital processors to safety in nuclear power plant

    - WG A5: Special process measurements

    - WG A7: Reliability of electrical equipment in reactor safety systems

    - WG A8: Control rooms

    - WG A9: Instrumentation systems

    - WG A10: Upgrading and modernization of instrumentation and control (I&C) systems in nuclear power plants (NPP)

SC45B Radioprotection Instrumentation:

- has the current scope "To prepare standards covering all the fields of radiation protection instrumentation. That is, for the measurement under both : normal and accident conditions of external and internal individual exposure, workplace, environment (including foodstuffs)"

- The chairman is Mr I. Thompson from the UK and the secretariat is France (Mr Jean-Claude Thévenin).

- Seven Working Groups report to SC45B:

    - WG B5: Radiation protection instrumentation for environmental monitoring

    - WG B7: Equipment for the monitoring of external contamination on the body, extremities and clothing of personnel

    - WG B8: Pocket active electronic dose equivalent, and dose equivalent rate monitors

    - WG B9: Installed equipment for radiation and activity monitoring in nuclear facilities

    - WG B10: Radon and radon daughter measuring instruments

- WG B12: Instrument for radioactive contamination measurement of foodstuff
- WG B13: Revision of IEC 761 series

In total approximately 160 experts from 19 different countries contribute to the work of TC45, with most active participation from the European countries, the USA, Canada and Japan.

All three committees have been, and are very active. They have, between them, generated over 130 agreed Standards, the work covers fundamental technology as well as the specification and design and development of complete systems.

The current work programme is large, consisting of 30 items as well as the review and amendment of older Standards. As you might expect the use of software in safety systems is a major topic in one of the SC45A Working Groups and this is the salient connection with the work of TC65 Working Groups A9 and A10 which have produced IEC 61508.

I would like to focus on a few of the more significant documents being developed by the various SC45A Working Groups.

- **IEC 60880 Software for Computers Important to Safety in Nuclear Power Plants.** The original Standard, the first part, was published in 1987 and was the first International Standard to give recommendations for the use of software in nuclear safety systems. The second part, just published, provides recommendations on several key areas of using software in nuclear safety systems, namely

  - the avoidance of common cause failure
  - the selection and use of automated tools
  - the re-use of pre-existing software.

  The revision of the original 1987 IEC 60880 started in 2000 is currently going on. The new edition of the IEC 60880, taking into account the last trends of the information technology relevant for nuclear important for safety systems and corresponding to a global consistent frame should be available in 2003.

- **IEC 61226 Classification of I&C Functions.** The original Standard, published in 1993, is currently revised. It deals with the difficult and often controversial subject of classification and graded requirements for I&C functions based upon their importance to safety. The safety principles for the Standard were taken from IAEA Safety Guide D8 where three categories of importance are defined in addition to a category which has no defined safety role. The Standard establishes a method of classifying the information and control functions for nuclear power plants and the I&C systems and equipment that provide those functions. The categorisation method is based on a qualitative (i.e. a deterministic) approach.

  The new version of the IEC 61226 should be available in 2004.

- **IEC 61513 General Requirements for Computer Based Systems.** This Standard will provide requirements for the design of computer based systems which are important to nuclear safety. This is a significant document in two senses; firstly, it will be the only Standard which deals with the difficult area of designing nuclear I&C safety systems using computer based solutions. Secondly, and probably

more important, it flows down the principles, and format of IEC 61508. Consequently, this IEC Standard represents the application of IEC 61508 in the nuclear sector.

The IEC 61513 is at final vote stage and should be available mid-2001.

- **IEC 62096 Instrument and Control Systems (I&C) of interim storage and final repository of nuclear fuel and waste**. This technical report will support owners of an NPP in the decision- making process and preparation of partial or complete modernization of the I&C. For this it will deal with:
  - motivating factors for I&C modernization,
  - principal options for the elaboration of different scenarios for I&C modernization,
  - technical and economic criteria for the selection of a long term I&C strategy,
  - principal aspects to be taken into account for a detailed technical feasibility study.

  Special attention will be paid to the improvement of the reactor safety and of the human machine interface.

- **IEC 62138 Computer-based systems important for safety software aspects for I&C systems of class 2 and 3.** This International Standard will provide requirements and recommendations for the software aspects of computer-based I&C systems of safety classes 2 and 3, as defined by IEC 61513. These I&C systems may be used for category B or C FSEs (Functions, and associated Systems and Equipment), as defined by IEC 61226. Its scope can be compared to the combined scopes of IEC 60880 parts 1 and 2, the difference being that these two documents address the software aspects of I&C systems of safety class 1. It is consistent with, and complementary to, IEC 61513.

  This standard should be available in 2002

- **IEC 62235 Instrument and Control Systems (I&C) of interim storage and final repository of nuclear fuel and waste .** This Technical Report gives guidelines for the Instrument and Control Systems of interim storage and final repository of nuclear fuel and waste, regardless the origin of the stored material. This Technical Report covers storage at all types of facilities such as; fuel fabrication plants, nuclear power plants, reprocessing facilities, interim storage facilities, encapsulation facilities and final repositories for operational waste and spent nuclear fuel. The Technical Report also covers storage during transportation. All these facilities contain different nuclear materials such as new fuel, used fuel, operational waste and other miscellaneous radioactive substances and objects.

These are just a few of the 30 documents which are part of the current work programme. Although nuclear power is not a growth industry in American and European countries, there is considerable interest in other parts of the world and international standards work helps to spread competence and expertise to all nations. In the USA and Western Europe the major work is retro-fitting of modern I&C systems. In Eastern Europe the work is dominated by the pressure to bring plant design and instrumentation up to western standards. Again international standardisation has a key role to play here since they provide common ground for discussion between utilities, suppliers and Safety Authorities.

7 CONCLUSION

This paper has underlined the existence of flourishing and effective international collaboration, on standards in general, and on nuclear standards in particular. It has indicated the route by which an individual person or organisation can introduce and, subsequently, influence the work. The use of harmonised standards has to be the correct approach when set against the background of increasing international trade. Overall, therefore, it is important that each country contributes to international standardisation work otherwise their voice will not be heard. This means taking part in meetings, listening to other experts talk about their ways of working and build the international consensus.

In the field of nuclear engineering, the hope is that standardisation promotes and enhances nuclear safety. Based on some earlier research it has been estimated that about half of the countries engaged in nuclear energy do use IEC nuclear standards as they are, quoting them in purchase contracts, whilst the other half prefer national ones.

A separate, and not insignificant, benefit which helps to offset some of the effort which individuals put into this work arises from the regular meetings between practising engineers with everyday involvement in manufacturing, research, development and regulation. Formal and informal exchange of professional knowledge at a detailed level stimulates cross fertilisation of ideas and generates value far beyond immediate standardisation needs. Those who attend and participate in the working meetings learn much from each other and come to accept that other people and other countries have good reasons for having different ideas on techniques and standardisation. Examination of the technical basis of differences then brings out aspects which had not previously been fully considered by any of the parties. The greater the difference, the longer it may take to arrive at an agreed standard and occasionally progress seems very slow - particularly in harmonising techniques which have been long established, but at the end of the day, there are clear commercial benefits from participating in standards work.

REFERENCES

1. ISO/IEC Directives. Parts 1,2 & 3 Second Edition 1995 Amdt. 1997

2. Some Aspects of International Standardisation in the IEC and Related Bodies. Dr A Goodings. 1993

3 The Role of International Standards in the Design of Modern I&C Systems for Nuclear Power Plants. J M Gallagher. 1993.

4 International Standardisation in Nuclear Engineering. D.L. Curtis. 1998.

ACKNOWLEDGEMENTS

This paper is based upon three previous papers written by Mr D.L. Curtis (4), Dr A Goodings (2) and Mr J Gallagher (3). Material has been extracted from the first paper and supplemented with up to date information concerning the IEC and its committees which could be found on the IEC server (www.iec.ch). The author would like to express his thanks to Mr Curtis, Dr Goodings and Mr Gallagher for their permission to use material from their papers.

Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety

Gary Johnson[8]

Summary

Many organizations worldwide develop standards that affect nuclear instrumentation and control (I&C). Two of the primary standards organizations that affect nuclear power are US IEEE's Nuclear Power Engineering, and IEC SC45A. Today, nuclear power is very much an international industry. In this environment is vital that the activities of these standards organizations be in harmony.

The harmony between IEEE and IEC standards is currently not adequate. This paper surveys the contents of the two sets of standards. Opportunities to improve consistency between the two sets of standards will be identified. It is hoped that this paper will excite a discussion of what might practically be done to improve the harmony between IEEE and IEC standards.

1 Introduction

The collections of IEEE and IEC standards have some overlap, but in many cases cover significantly different topics. For example, IEEE standards go to great depth covering environmental qualification of many specific types of components, while IEC covers the topic only at the general level. Conversely, certain IEC standards deal with specific instrumentation and control functions, a topic area where IEEE standards are largely mute. This raises several questions. Why do two bodies that are writing standards for the same purpose arrive at such a different collection of standards? Does this diversity offer opportunities for the two bodies to build on each other's standards to efficiently improve upon the coverage of their sets of standards?

This situation poses a problem for the developers of systems for plant upgrades who must try to address both sets of standards to avail themselves of a sufficiently broad market. Additionally, the IEEE and IEC standards together form a more comprehensive set of guidance than either set alone provides. If the interfaces between the standard sets were smoother plant staff and system designers would have a better set of tools to help in the design and specification of I&C upgrades.

To understand the similarities and differences between IEC and IEEE nuclear power standards layer diagrams were developed for each set of standards.

[8] *Lawrence Livermore National Laboratory, P.O. Box 808, L-632, Livermore, CA, USA 94550. Tel: +1-925-423-8834, Fax: +1-925-422-9913, e-mail: johnson27@llnl.gov*

Layer Diagrams

Layer diagrams show the structure of a set of documents from the most general to the most specific.

Used previously in the analysis of software engineering standards (ref Jim Moore book)

Five layers: terminology, overall guidance, principles, element standards, application guides, and techniques. (Give definition from Jim Moore book) All five layers are always needed.

For nuclear power standards regulatory requirements provide the overall guidance. For IEEE this is NRC's 10CFR50. For IEC this is IAEA 50-C-D. To the extent these are different the differences will drive irreconcilable inconsistencies between the sets of standards.

Figures 1 through 4 give the layer diagrams constructed. These represent one view of the standards. Other organizations are possible - it is not possible to produce a perfect one. It is hoped that the organization here is a useful one.

3 Analysis

The standards of each set may be categorized into three groups: system standards, human machine interface standards, standards for specific functions.

The greatest overlap is in system standards. The standards in the other groups mostly cover different specific topics even though the general topics are the same.

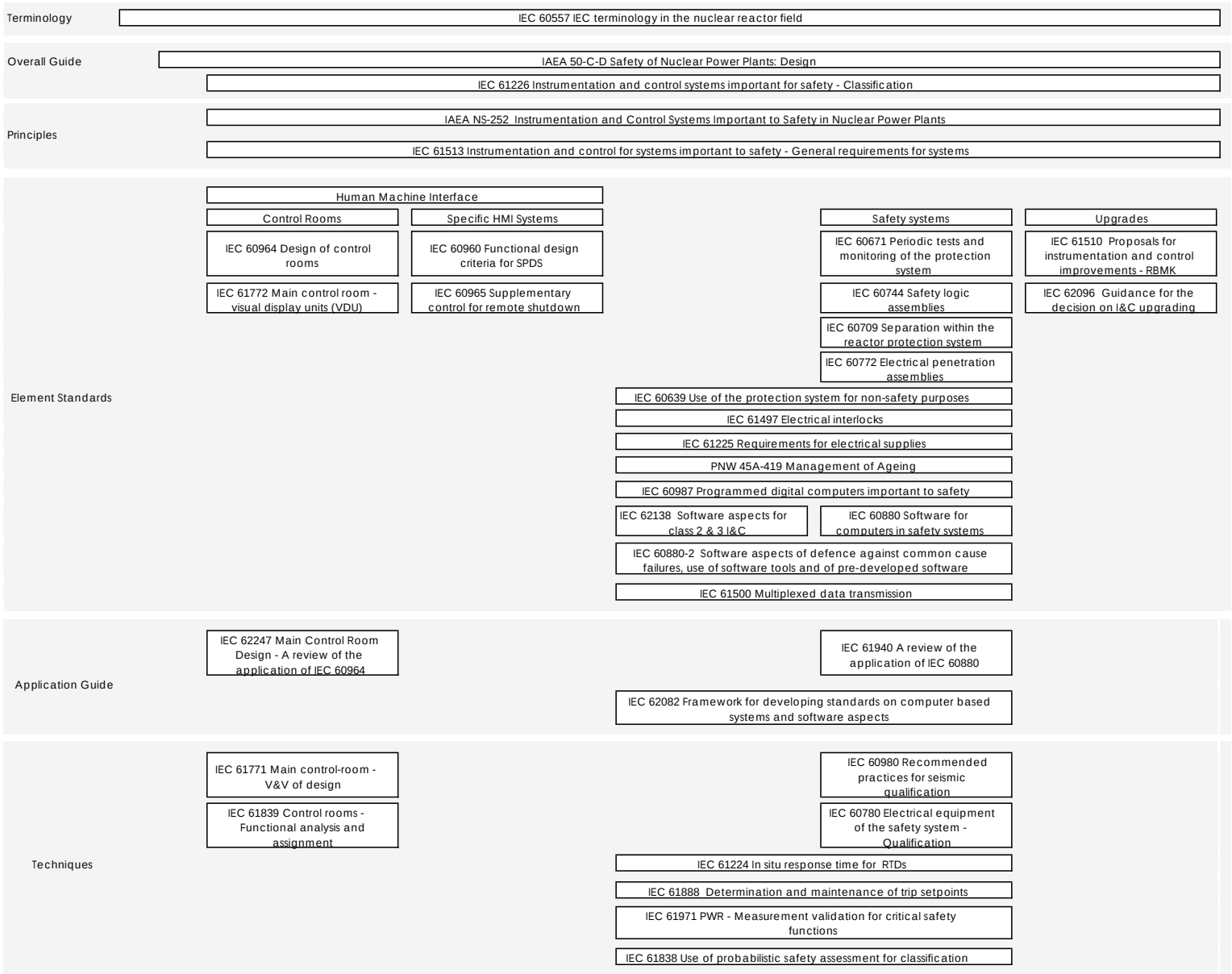
The IEEE standard set includes several general industry standards that cover relevant topics. These were explicitly included in the nuclear set by the IEEE management board, NPEC. Certain software engineering and EMI standards may be included in the set of applicable general industry standards because of their endorsement by NRC. There is no similar practice in IEC to "endorse" general industry standards for nuclear use.

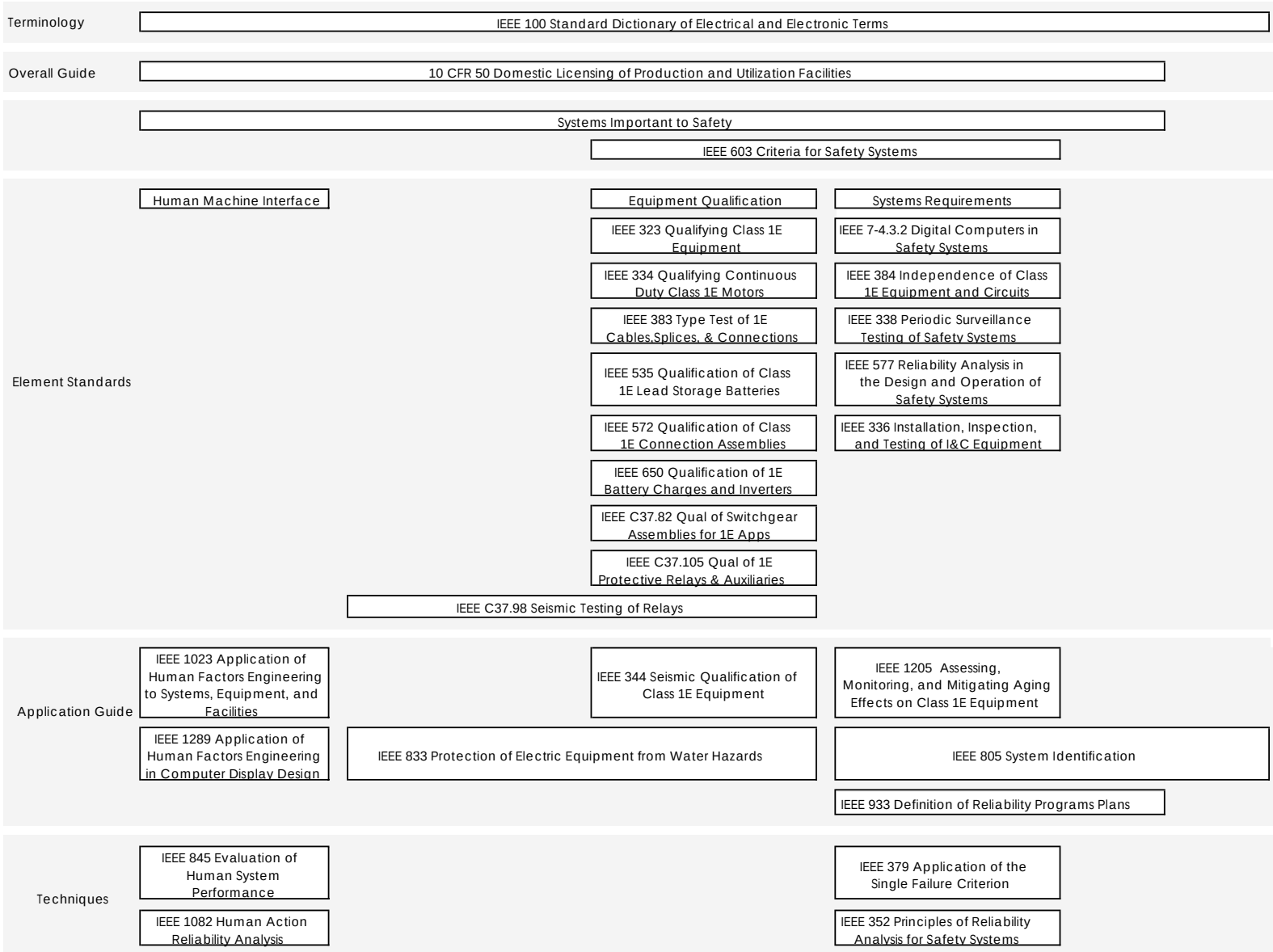
The IEC standards are considered industry specific standards under a general industry systems standard, IEC 61508. This is a relatively new development and the relationship between 61508 and the nuclear standards has not yet matured. No comparable relationship exists in the IEEE sphere.

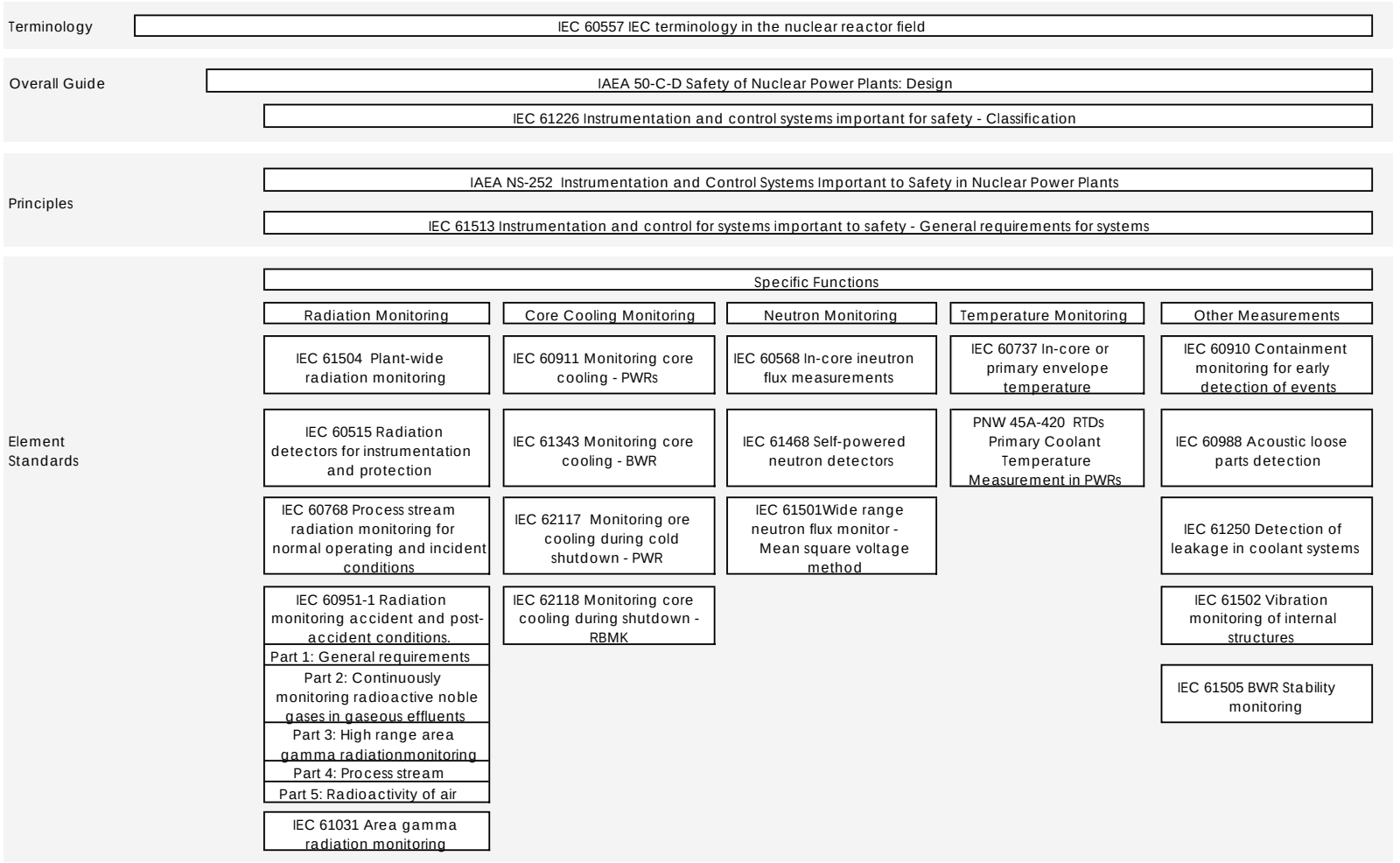
System Standards

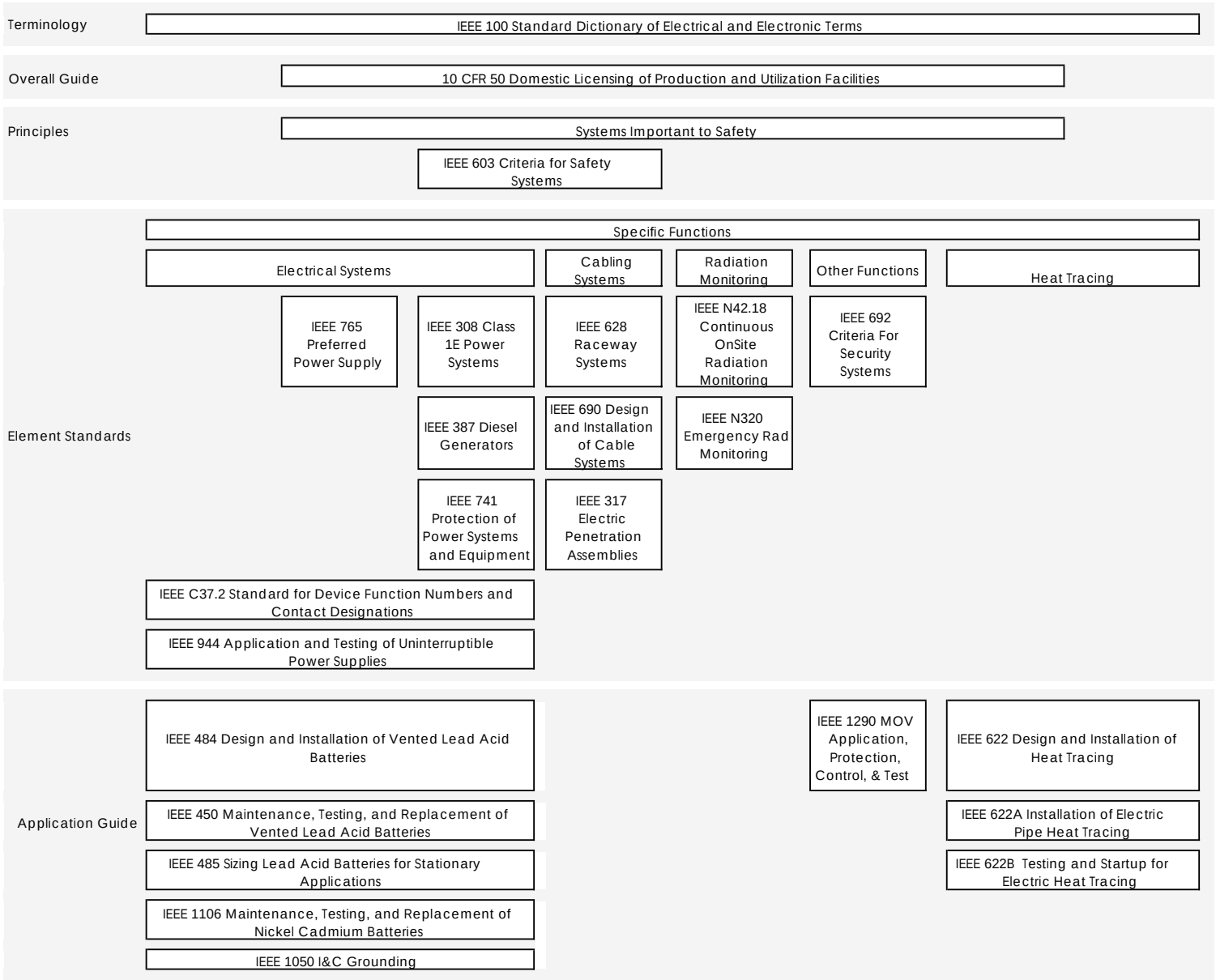
IEEE focuses on safety systems; IEC focuses on systems-important to safety. IEC gives guidance on classification. This topic is not addressed in the IEEE group. The IEC standards may offer useful tools for US risked-based regulation.

IEEE 603 overlaps with IAEA NS-252 and IEC 61513. IEEE 7-4.3.2 overlaps with IEC 60880. The highest priority should be given to working these towards harmony.


Terminology
IEC 60557 IEC terminology in the nuclear reactor field
Overall Guide
IAEA 50-C-D Safety of Nuclear Power Plants: Design
IEC 61226 Instrumentation and control systems important for safety - Classification
Principles
IAEA NS-252 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants
IEC 61513 Instrumentation and control for systems important to safety - General requirements for systems
Element Standards
Human Machine Interface
Control Rooms
Specific HMI Systems
Safety systems
Upgrades
IEC 60964 Design of control rooms
IEC 60960 Functional design criteria for SPDS
IEC 60671 Periodic tests and monitoring of the protection system
IEC 61510 Proposals for instrumentation and control improvements - RBMK
IEC 61772 Main control room - visual display units (VDU)
IEC 60965 Supplementary control for remote shutdown
IEC 60744 Safety logic assemblies
IEC 62096 Guidance for the decision on I&C upgrading
IEC 60709 Separation within the reactor protection system
IEC 60772 Electrical penetration assemblies
IEC 60639 Use of the protection system for non-safety purposes
IEC 61497 Electrical interlocks
IEC 61225 Requirements for electrical supplies
PNW 45A-419 Management of Ageing
IEC 60987 Programmed digital computers important to safety
IEC 62138 Software aspects for class 2 & 3 I&C
IEC 60880 Software for computers in safety systems
IEC 60880-2 Software aspects of defence against common cause failures, use of software tools and of pre-developed software
IEC 61500 Multiplexed data transmission
Application Guide
IEC 62247 Main Control Room Design - A review of the application of IEC 60964
IEC 61940 A review of the application of IEC 60880
IEC 62082 Framework for developing standards on computer based systems and software aspects
Techniques
IEC 61771 Main control-room - V&V of design
IEC 60980 Recommended practices for seismic qualification
IEC 61839 Control rooms - Functional analysis and assignment
IEC 60780 Electrical equipment of the safety system - Qualification
IEC 61224 In situ response time for RTDs
IEC 61888 Determination and maintenance of trip setpoints
IEC 61971 PWR - Measurement validation for critical safety functions
IEC 61838 Use of probabilistic safety assessment for classification


Terminology
IEEE 100 Standard Dictionary of Electrical and Electronic Terms
Overall Guide
10 CFR 50 Domestic Licensing of Production and Utilization Facilities
Systems Important to Safety
IEEE 603 Criteria for Safety Systems
Element Standards
Human Machine Interface
Equipment Qualification
Systems Requirements
IEEE 323 Qualifying Class 1E Equipment
IEEE 7-4.3.2 Digital Computers in Safety Systems
IEEE 334 Qualifying Continuous Duty Class 1E Motors
IEEE 384 Independence of Class 1E Equipment and Circuits
IEEE 383 Type Test of 1E Cables,Splices, & Connections
IEEE 338 Periodic Surveillance Testing of Safety Systems
IEEE 535 Qualification of Class 1E Lead Storage Batteries
IEEE 577 Reliability Analysis in the Design and Operation of Safety Systems
IEEE 572 Qualification of Class 1E Connection Assemblies
IEEE 336 Installation, Inspection, and Testing of I&C Equipment
IEEE 650 Qualification of 1E Battery Charges and Inverters
IEEE C37.82 Qual of Switchgear Assemblies for 1E Apps
IEEE C37.105 Qual of 1E Protective Relays & Auxiliaries
IEEE C37.98 Seismic Testing of Relays
Application Guide
IEEE 1023 Application of Human Factors Engineering to Systems, Equipment, and Facilities
IEEE 344 Seismic Qualification of Class 1E Equipment
IEEE 1205 Assessing, Monitoring, and Mitigating Aging Effects on Class 1E Equipment
IEEE 1289 Application of Human Factors Engineering in Computer Display Design
IEEE 833 Protection of Electric Equipment from Water Hazards
IEEE 805 System Identification
IEEE 933 Definition of Reliability Programs Plans
Techniques
IEEE 845 Evaluation of Human System Performance
IEEE 379 Application of the Single Failure Criterion
IEEE 1082 Human Action Reliability Analysis
IEEE 352 Principles of Reliability Analysis for Safety Systems


Terminology
IEC 60557 IEC terminology in the nuclear reactor field
Overall Guide
IAEA 50-C-D Safety of Nuclear Power Plants: Design
IEC 61226 Instrumentation and control systems important for safety - Classification
Principles
IAEA NS-252 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants
IEC 61513 Instrumentation and control for systems important to safety - General requirements for systems
Element Standards
Specific Functions
Radiation Monitoring
Core Cooling Monitoring
Neutron Monitoring
Temperature Monitoring
Other Measurements
IEC 61504 Plant-wide radiation monitoring
IEC 60911 Monitoring core cooling - PWRs
IEC 60568 In-core ineutron flux measurements
IEC 60737 In-core or primary envelope temperature
IEC 60910 Containment monitoring for early detection of events
IEC 60515 Radiation detectors for instrumentation and protection
IEC 61343 Monitoring core cooling - BWR
IEC 61468 Self-powered neutron detectors
PNW 45A-420 RTDs Primary Coolant Temperature Measurement in PWRs
IEC 60988 Acoustic loose parts detection
IEC 60768 Process stream radiation monitoring for normal operating and incident conditions
IEC 62117 Monitoring ore cooling during cold shutdown - PWR
IEC 61501Wide range neutron flux monitor - Mean square voltage method
IEC 61250 Detection of leakage in coolant systems
IEC 60951-1 Radiation monitoring accident and post-accident conditions.
IEC 62118 Monitoring core cooling during shutdown - RBMK
IEC 61502 Vibration monitoring of internal structures
Part 1: General requirements
Part 2: Continuously monitoring radioactive noble gases in gaseous effluents
IEC 61505 BWR Stability monitoring
Part 3: High range area gamma radiationmonitoring
Part 4: Process stream
Part 5: Radioactivity of air
IEC 61031 Area gamma radiation monitoring


Terminology
IEEE 100 Standard Dictionary of Electrical and Electronic Terms
Overall Guide
10 CFR 50 Domestic Licensing of Production and Utilization Facilities
Principles
Systems Important to Safety
IEEE 603 Criteria for Safety Systems
Element Standards
Specific Functions
Electrical Systems
Cabling Systems
Radiation Monitoring
Other Functions
Heat Tracing
IEEE 765 Preferred Power Supply
IEEE 308 Class 1E Power Systems
IEEE 628 Raceway Systems
IEEE N42.18 Continuous OnSite Radiation Monitoring
IEEE 692 Criteria For Security Systems
IEEE 387 Diesel Generators
IEEE 690 Design and Installation of Cable Systems
IEEE N320 Emergency Rad Monitoring
IEEE 741 Protection of Power Systems and Equipment
IEEE 317 Electric Penetration Assemblies
IEEE C37.2 Standard for Device Function Numbers and Contact Designations
IEEE 944 Application and Testing of Uninterruptible Power Supplies
Application Guide
IEEE 484 Design and Installation of Vented Lead Acid Batteries
IEEE 1290 MOV Application, Protection, Control, & Test
IEEE 622 Design and Installation of Heat Tracing
IEEE 450 Maintenance, Testing, and Replacement of Vented Lead Acid Batteries
IEEE 622A Installation of Electric Pipe Heat Tracing
IEEE 485 Sizing Lead Acid Batteries for Stationary Applications
IEEE 622B Testing and Startup for Electric Heat Tracing
IEEE 1106 Maintenance, Testing, and Replacement of Nickel Cadmium Batteries
IEEE 1050 I&C Grounding

IEEE 603 is supported by a suite of detailed standards on specific topics discussed in 603. With specific exceptions a similar set of daughter standards in the IEC sphere does not exist. Harmonization of the 603/7-4.3.2 and the NS-252/61513/60880 sets need to consider the influence of these detailed standards. Consideration might be given to bringing the detailed IEEE standards under the IEC umbrella.

Both IEEE and IEC have very general guidance on equipment qualification. IEEE has a set of very detailed standards describing the application of the detailed guidance to certain specific types of components. Ideally, these detailed standards would support both the IEEE and IEC general guidance.

Human-Machine Interface

IEC emphasizes HMI design for functions - main control room, SPDS, Remote shutdown. There is no equivalent in the IEEE set.

IEEE emphasizes HMI techniques. There is some overlap with IEC standards here. There should be a move towards common coverage and harmonization.

Discuss overlap in more detail - Later.

Standards for Specific I&C Functions

Both IEC and IEEE produce standards that impose requirements on specific I&C functions. Strangely, they mostly cover completely different sets of functions. The exception is radiation monitoring.

Ideally, both sets of standards could be used together. To do this they must be consistent with both the IEEE 603 and the NS252/IEC6153 sets.

Software Important to Safety:

The New IAEA Safety Guide and

The Common Position of European Nuclear Regulators

Courtois Pierre-Jacques,

Association Vincotte Nuclear (AVN), Brussels

Abstract: An overview of some distinctive aspects of two international documents which provide guidance on the design and the licensing of computer based systems important to safety prepared by a contributor to both documents. The paper takes a look at their coherence and complementarities, at their strong and original points, and at the issues they leave open.

1. Introduction

In September 2000, two documents were published simultaneously:

the International Atomic Energy Agency (IAEA) Safety Guide " *Software for Computer based Systems important to Safety in Nuclear power Plants*", Safety Guide NS-G-1.1,

and the report EUR 19265 EN of the Nuclear safety, regulation and radioactive waste management unit of the European Directorate General for the Environment[9] "Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors", categorized as a consensus document..

For practical reasons, we will refer to the first document as **SG**, and to the second as **REG**.

These two documents are important, each in its own way. **SG** is a *new* safety guide of the Agency, the first of its kind to focus specifically on software. **REG** is a first consensus document from nuclear regulators on licensing practices specifically addressing safety critical software and produced under the auspices of an international institution. Both documents have taken some innovative viewpoints, sometimes on thorny issues.

[9]This unit activities are now within the Directorate General for Energy and Transport

2. Background

Both documents have been the object of intensive work by experts and consultants, and the result of a long process of meetings and revisions.

The work on the **SG** was initiated as early as April 1991, when a group of distinguished international experts in software engineering – including Professors D.L. Parnas and N. Leveson - met in Vienna. They alerted the Agency that its current guidance did not address software issues –already considered as quite critical at the time - and they drew a list of topics for future technical reports. Their recommendations resulted in the publication, in 1994, of the technical report 367 [2]:" Software Important to safety in Nuclear power Plants" to which about fifteen experts actively contributed with papers and during lively meetings.
In April 1995, a group of four experts met again in Vienna to identify – on the basis of the technical report – the possible contents of a future safety guide. Their report advised the Agency to focus (i) on software issues, (ii) on the interface between the regulator and the licensee and (iii) on guidelines not on how to design but on what is needed to demonstrate adequacy of the design.
Then followed a series of alternate advisory group meetings, technical group and consultant meetings: October 95 and in particular November 1996, when 24 experts from 17 countries met for a week to review, comment and debate the current version of a safety guide. A fourth version of the document was submitted to the Agency Nuclear Safety Standards Advisory Committee (NUSSAC[10]) in October 1997 and accepted as a draft for a safety guide project. A subsequent version was then sent to Member States for comments. Fourteen Member States sent 465 comments which were dealt with in two consultant meetings. Two final consultant meetings took care of these comments, most very positive and constructive.
The version 7 of the guide was endorsed by the NUSSAC in its meeting of October 1999, by the Advisory Commission on Safety Standards (ACSS[11]) in December 1999, and published less than one year later.

The genesis of the **REG** document in many ways followed a similar pattern, albeit within the smaller community of the European nuclear regulators.
The 1995-2000 activity programmes of the Nuclear Regulator Working Group (NRWG) and of the Reactor Safety Working Group (RSWG) of the European Commission Directorate General XI (Environment, Nuclear safety and Civil Protection) were set up within the framework of the 1975 and 1992 resolutions of the Council of Ministers on the technological problems of nuclear safety.
In 1994, the NRWG and RSWG working groups launched a task force of experts from nuclear safety institutes with the mandate of "reaching a consensus among its members on software licensing issues having important practical aspects". From October 1994 to June 1997, the task force met three times a year. The task force selected a set of key issues, produced 64 contributions and made 7 revisions of a draft document which was eventually accepted by the NRWG/RSWG as a EC report [3] publicly available and open to comments (the report was also sent by the commission for comments to 30 prominent international experts). In March 1998, the project ARMONIA (**A**ction by **R**egulators to Har**mon**ize Digital **I**nstrumentation **A**ssessment) was launched with the mission to prepare a new version of the document which would integrate the comments received and would deal with a few software issues not yet covered. In May 1999, after 5 residential meetings of ARMONIA and 25 paper contributions, a revision 10 was submitted to the Task Force for comment and approval. Eventually, in May 2000, after two additional meetings, a revision 11 was presented

[10] now NUSSC, which stands for Nuclear Safety Standards Committee

[11] now CSS, which stands for the Commission on safety Standards

and approved by the NRWG[12], provisionally classified under the category "consensus document". It was made available through the europa server:
http://www.europa.eu.int/comm/energy/en/nuclearsafety/reports.htm - Nuclear installation safety
and published as report EUR 19265 EN in September.

3. Why this guidance is useful

SG and **REG** are guidance documents that aim to meet specific needs, not met by other standards.

The eighties left the nuclear I&C community somewhat traumatized by several modernization projects involving safety critical software that had experienced abnormal delays and costs. The lack of experience, of practical methods and of interactions between the nuclear and other industrial and software engineering communities were probably some of the causes of these problems.

Two observations emerged from these experiences.
If guidance was available to *design* software based safety systems, little or none was available to address the specific issues raised by the *licensing* of highly critical software. As far as software was concerned, regulators and licensees were abandoned to improvisation.
The second observation – somewhat antinomic but salutary – was that software is not per se safe or unsafe. Software is only one component of the system. Checking the software is (i) not sufficient and (ii) is dependent on the environment. The notions of *computer safety case* and of *computer safety demonstration* resulted from this observation and received increased attention.

The section on background already pointed out that the former of these two observations was an essential motivation for launching the **SG** and the **REG** projects.
The second observation was also instrumental. Paragraph 1.5 of the **SG** states: "*The objective of this Safety Guide is to provide guidance on the collection of evidence and preparation of documentation to be used in the safety demonstration of the software of computer based systems important to safety in nuclear power plants*." The **REG** document also has an introductory section which addresses the safety plan, the safety strategy and demonstration: "*…All the subsequent recommendations contained in this report are founded on the premise that (such) a safety plan exists and has been agreed upon by all parties involved. The intent herein is to give guidance on how to produce the evidence and the documentation for the safety demonstration and for the contents for the safety plan."*

This intent to focus on the evidence required by the safety demonstration of software - makes **SG** and **REG** documents complementary to other guidance which – like the IEC 60880 - focuses on requirements for each stage of the software design, development, and V&V processes.

To sum up, in some of its more distinctive aspects, this guidance:
- Addresses regulator and assessor concerns, potential sources of conflict in licensor/licensee negotiations, and identifies grounds for mutual agreement,
- Addresses the safety demonstration (safety case) rather than the system design,
- Emphasizes the need for documentation (**SG**) and identifies sources of evidence (**REG**).

[12]. The RSWG was discontinued in 1999. The NRWG is now made up of Nuclear Safety Authorities from the European Union countries as well as from candidate countries to the EU from Central and Eastern Europe.

4. A same Scope…

Both documents address the software of systems important to safety as the IAEA guides define them, but focus on safety systems. Both documents recognize the difficulty of defining possible relaxations on requirements for safety related software based systems. However, whenever possible, both documents explicitly specify recommendations which apply only to safety systems and thus indirectly admit possible relaxations for safety related system software:

SG: in paragraphs 1.6, 3.15, 4.17, 5.19, 5.21, 5.35, 6.7,

REG: the clauses (more than 30) that apply to safety system software only are mentioned in a specific section (section 1.10), together with specific clauses for safety related systems and examples of relaxations for new and preexisting software.

The **SG** relaxations essentially concern security requirements against the external world, the nature of the independence required from the V&V teams, requirements on the specification of functional and non-functional safety requirements, requirements for statistically valid tests commensurate with the required reliability, and the dedication of safety systems to safety functions.
Moreover, **REG** admits additional relaxations on requirements for the assessment of pre-existing software (PSW), on dependability and documentation requirements for tools, on requirements for software produced by tools, on the required safety culture, on staffing levels, on computer system design (isolation, data protection,…), on programming and coding directives, on statistical testing, on software change control and maintenance, on calibration and testing requirements in operations.

5… But Different Structures and Contents.

While the scopes of the documents are identical, their structures differ.
Their different structures reflect the fact that the **SG** is an emanation of designers, operators and regulators, while the **REG** gives a more focused regulator's common viewpoint.

The **SG** is organized in 15 sections (see appendix 1). The first four sections provide recommendations on preconditions of a software based system development project, on the management of safety, and on the planning of the project.
Sections 5 to 15 are dedicated to the individual phases of the development life cycle, up to post-delivery modifications. Each section is generally structured in the following pattern. In each section, under the heading "RECOMMENDATIONS" there is a set of recommended principles or concerns that should be addressed in this phase. Under the heading 'DOCUMENTS', there is a list of documents to be produced as an output from the phase and advice is provided concerning the contents of these documents. Also, some general recommendations are given concerning the attributes and presentation of the products of the phase. In all parts, the intent is not to provide an exhaustive description of all the material that will be needed for development purposes; instead, the intent is to summarize the principles, material and its attributes that are most important for the safety demonstration.

The **REG** document is organized around a selected set of technical issues which were considered difficult by the task force of regulators and of utmost importance to the licensing process. These issues cover a consistent set of licensing aspects right from the inception of the life cycle up to and including commissioning.
These issues were partitioned into two sets: "Generic Licensing Issues" and "Life Cycle Phase Licensing Issues". Issues in the second set are related to a specific stage of design and development process, while those of the former have more general implications and apply to several stages or to the whole system lifecycle. Each issue area is dealt with in a separate chapter of the report (see appendix 2).

Why two documents within the same scope?
The two documents have one part in common: the annex on preexisting software of the **SG** reproduces a section of the **REG**. Otherwise the contents are quite different. The **SG** is an inclusive account of all the aspects involved in the safety demonstration of a software based system, from the very initial phase before the start of a project up to and including the post-delivery modifications. The requirements and recommendations result from an agreement between experts representing different stakeholders (designers, utilities, regulators) and aim at completeness. They seek to establish an essential and comprehensive basis for the safety demonstration, assuming that more detailed requirements may need to be incorporated according to national practices, or on a case-by-case basis. In contrast, the REG focuses on a set of technical licensing issues only, for which it gives the common viewpoint of regulator's experts. The emphasis is on technical requirements, recommendations, and acceptance criteria, at a detailed level whenever necessary and possible.

6. Non - Prescriptiveness

None of these documents is of course legally binding.
Every IAEA guide foreword clearly states: *"The IAEA standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities."*

The **REG** executive summary is no less clear: " *While the Common Positions are intended to convey the unanimous views of the Task Force members on the guidance that the licensees need to follow as part of an adequate safety demonstration, it should be remembered that this guidance is non-prescriptive. Therefore, its specific application depends on each national regulatory authority. Throughout the document these common positions are expressed with the auxiliary verb "shall". The use of this verb for common positions is intended to convey the unanimous desire felt by the Task Force Members for the licensees to satisfy the requirements expressed in the clause. The Common Position requirements can be regarded as a common denominator of practices in the member states represented in the task force*."

It is the IAEA usage to use the verb "should" to express all recommendations in a safety guide, with the understanding that it is necessary to take the measures recommended or equivalent alternatives to comply with the requirements stated in the Safety Requirements publications. In the preparation of the **REG**, it was found useful to use, like the IEC standards, "shall" and "should" statements. "shall" statements are used in **REG** for expressing the common positions (as defined above), and "should" statements for *recommended practices.* Recommended practices are recommendations supported by most, but which may not be systematically implemented by all of the members states represented in the task force. In contrast, the set of requirements of a *common position* was – I believe -regarded as being "technically necessary" (the same technical necessity that would leave no choice to a railway safety guide but to require that the gates "shall" be closed before the train is on the railway crossing).

7. Some salient points

Both documents make steps forward by showing consensus on certain prevention or precaution measures to deal with software issues that either always proved difficult, or are new because they are engendered by new software practices. Below are a few examples, with no intent of being complete.

On automatic code generation
As far as licensing is concerned, there has always been much debate between proponents of systems generating code from application specifications and those more familiar with the classical development cycle. Here is the position of the **SG:**

Code can be produced from the system specifications in various ways that are essentially combinations of two distinct approaches: the classical development process through stages of specifications and design…, or the use of code generating tools which receive as input a high level language application-oriented description of the system. The choice between these two approaches depends on the tools and resources available to the parties involved in the project, and should, in particular, take into account trade-offs between design and the demonstration of the dependability of tools. The recommendations of this Section (i.e. the section on software implementation) *apply to all possible combinations of the two approaches.(9.2)*

And on software requirements for code generated by tools (**SG**):
Software requirements are the subset of the computer system requirements that will ultimately be implemented as computer programs…The verification of the software requirements against the upper level requirements is an important step in the licensing process…(7.1)
If the computer system requirements are sufficiently detailed and their documentation is sufficiently formal, and if parts of the computer system design and of the code are generated by tools, then a separate software requirement document may be unnecessary for those parts. However, those parts of such computer system requirements from which code is generated or reused should be regarded as a statement of software requirements against which subsequent code should be verified. Also any separately compiled modules that are included by the code generator should be supported by separate documents for the software requirements (7.4).

On software and code hazard analysis
The application of hazard analysis to software is still barely dealt with by international guidance. The **SG** has several recommendations, e. g.:
…the computer based system and its interfaces to the plant should be evaluated at various phases of the development for potential contribution to hazards at plant level. (possible techniques are outlined in TRS 367 - Section 8.3.9). When such potential critical behaviours are identified, they should be traced into the Computer System Design, the Software Design and the code in order to identify parts of the design and of the software that require special design features. In addition, these hazards should be traced back into the requirements and should be incorporated into the plant safety analysis as appropriate(10.27).

…A documented demonstration should be provided that the Software Design addresses the hazards identified in previous analyses and the requirements that have been identified as important to safety.(8.14)

On pre-existing software (PSW)

The **SG** addresses the use of pre-existing or COTS (Commercial-Off-The-Shelf) software for safety functions (paragraphs 1.9, 2.11, 6.1, 6.40, 10.1, and annex).
The **REG** recognizes that licensees may wish to make use of such software given that appropriate assessment has been undertaken. Two of its sections deal with the issue: a specific one also reproduced as an annex in the **SG**, and another devoted to safety related systems. For safety systems, the **REG** is clear: *For safety systems (category one), the PSW shall be subjected to the same assessment (analysis and review) of the final product (not of the production process) as new software developed for the application. If necessary, reverse engineering shall be performed to enable the full specification of the PSW to be evaluated. (1.3.3.5)*

For safety related software, the **REG** recognizes that several possible sources of evidence may be exploited: : *Simplicity is required for safety systems. Safety related systems can be more complex. For these latter systems less information may be available on the development process and on the product. In certain cases, it might be possible to compensate for this lack of information - typical for pre-existing software (PSW) of category 2 - by using evidence provided by functional testing and adequate operational feedback. (1.10.1.3)*

Another source of evidence is suggested for safety related software: *In order to evaluate the possibility of relaxing certain requirements of the safety demonstration, as a minimum, the consequences of the potential modes of failures of the computer based system shall be evaluated. For instance, a failure mode analysis may show that certain relaxations are possible, when failures of the system can be anticipated and their effects can be detected and corrected in time by other means. (1.10.3.3)*

On independent assessment

This is a difficult issue. In human societies, which draw their strength from interrelations and interdependencies, independence is somehow against nature, and often difficult to achieve. Besides, there are several types of independence, all of which are susceptible to make access to relevant information more difficult, and thereby affect assessors' competence. So, it is important to clarify what sort of independence is required and for what purpose.

The **SG** makes the following distinction**: …** *Independence includes:*

- *Technical independence: done by different people, preferably using different techniques and tools;*
- *Management independence: led and motivated by different people. The V&V team and the development team should have different management lines. Official communication between independent teams should be recorded;*
- *Financial independence: there should be a separate budget with restrictions on transfer of financial resources between development and V&V.(4.17)*

The **SG** also allows some relaxations:. *The amount and type of independent V&V should be justified with respect to the safety class of the system, e.g. financial independence may not be required for safety related systems.*

The **REG** emphasizes competence but does not go as far as strictly requiring (shall) financial independence: *The system and its safety demonstration shall be subjected to a documented review by persons who are*:

(a) Competent;

(b) Organizationally independent of the supplier(s) of the system (and of its safety demonstration), and

(c) Not responsible for or in the development, procurement and production chain of the system.(1.9.3.1)

The **REG** also suggests that for safety related systems, independent validation only might be needed, in contrast to the requirements for independent verification (section 2.5), validation (section 2.6) and assessment (section 1.9) defined for safety systems.

On formal methods

The **REG** has 9 common positions on this difficult topic and 6 recommended practices. One of the key principles on which the common positions were founded is:

No credit can be taken in a safety demonstration for the use "per se" of a formal method without due consideration being given to the specific evidence brought in by this use, and to its contribution to the safety demonstration of the system. (1.8.3.1)

On documentation

The **SG** emphasizes documentation, and has a set of requirements on the documents to be produced in each section dealing with a stage of the development process. One general requirement is: *The set of documents should ensure the traceability of design decisions… Appropriate documents should*

be produced at each step of the development process. It is essential that documentation be updated throughout the iterative development including commissioning and ongoing maintenance processes. The documents available to the regulator should be identical to those used by the designers. The designer should be informed of this requirement early in the project.(3.35)

On determinism and interrupts

Both documents are not always fully aligned, but it is difficult to catch them out in blatant incoherence. For instance, the **SG** states: *The architecture chosen should be deterministic. A design should be selected that makes the operation of the software predictable in terms of response to inputs and the time to produce a response. A fixed, repeated sequence of operations (e.g. polling) may generally be used rather than interrupts. Communication protocols should be deterministic and should not depend on the correct operation of other, external systems (8.10).*

The **REG** is somewhat less conservative**:** *…the code shall - as much as possible - run in a direct and fixed sequence pattern…Interrupts shall be avoided unless they lead to a significant simplification. Where interrupts are used, their usage and masking during time and data critical operations shall be proven correct and shall be well documented. The use of high-level synchronisation programming primitives shall preferably be used to deal with interrupts. The hardware and software shall be designed so that every interrupt is either serviced or explicitly masked. (2.4.3.3.2)*

On software reliability and demonstrable dependability

Here, both documents are more cautious than other international standards.

The **SG** emphasizes the issue of dependability, but avoids that of software reliability**:** *The system must not only be dependable, it must also be possible to demonstrate to the regulator that it is dependable. This safety guide is intended to guide licensees in how to achieve demonstrable dependability through design and qualification methods that improve traceability and through the production of adequate documents.(3.19)*

And later, in the section on software requirements, it explains why: *An overall software reliability target may be stated, but it should be understood that the achievement of such a target will be less demonstrable than the fulfillment of other types of requirements. It is extremely difficult to demonstrate that quantitative reliability requirements for software have been met. Currently available methods do not provide results in which confidence can be placed at the level required for systems of the highest importance to safety, and therefore this Safety Guide does not provide guidance on the use of software reliability models. If applicants propose the use of software reliability models for certification or commissioning, a rationale for the model should be included in the certification or commissioning plan and agreed with the regulatory authority. (7.11)*

The **REG** is clearly uncompromising. *It is recognised that the reliability of a computer-based safety system cannot be demonstrated by testing. Therefore, the demonstration of safety has to depend to some degree on the quality of the processes involved….(1.6.2.1).*

However, at the same time, it recommends that the level of reliability that would be required from the software be not left ignored: *The level of reliability required from the software should be explicitly stated, with the understanding that the achievement of a reliability level is less demonstrable than other requirements (2.3.4.1.4).* Retrospectively, one might wonder why this is a recommended practice, and not a common position (shall).

8. Recommendations for further work

Documents of this kind are never complete. Because they result from a consensus, they mark an important step forward, but need to be revised as knowledge and technology progress. When the **REG** neared completion, early in 2000, the members of the task force identified a few important areas where they agreed that more knowledge or experience was needed to establish useful guidance:

1. Diversity/Redundancy
   - Regulator positions requirements for diversity at architecture level;
   - Regulator positions on software diversity

2. Software Reliability
   - Methods to obtain quantitative estimations (numbers).
   - Regulator position to cope with situations where numbers cannot be obtained although quantitative objectives exist for plant operations.

3. Structure of Safety demonstration
   - Contents of a safety demonstration (safety case).
   - Organisation and structure (framework) for claims, sub-claims, arguments, proofs, ...

4. Criteria to rank software based systems in safety categories.
   - Criteria such as existence of redundant back-up, pure informative output or direct action, consequences of failure,..

5. Explicit requirements and acceptance criteria for distinct sorts of software:
   - Code produced by application oriented code generation tools (issues of validation).
   - Libraries,
   - Input/output drivers.
   - Run time and System software (operating systems), etc…

By way of independent confirmation, is was interesting to note a posteriori, that most of these topics were also included as research targets in the NRC proposed five year research plan for digital I&C technology, introduced by Steven Arndt at the Embedded Topical Meeting on Nuclear Instrumentation, Control and Human-Machine Interface Technologies, at the 2000 ANS/ENS International Meeting in Washington, D.C. [1]

9. Conclusions

The forceful value of the two documents lies in the consensus they achieve. Whatever the auspices are, consensus and common positions are always obtained at a given time, in a given context and on certain issues. They never dispense from adaptations and revisions. They are, however, the only way to make progress, especially in those cases where there is uncertainty or where some knowledge or operational experience is missing and a precautionary approach must be followed.

The work discussed above already proved useful in different respects:

- To share technical expertise among those who contributed,
- To support regulators in their national policies,
- To assist licensees in dealing with foreign manufacturers and suppliers
- To help designers produce systems that anticipate licensing requirements and are portable.

10. Acknowledgements

This paper gives a sketchy and personal viewpoint and is not an exegesis of the two guidance documents. As such, it does not do justice to the impressive work of the two teams of dedicated experts who produced them.
Thanks are due to J. Pachner, International Atomic Energy Agency, Vienna, J. Gomez, DG for Energy and Transports of the European Commission, Pierre Govaerts, AVN, and to Manfred Kersken, ISTec, Germany and Bob Yates, NII, UK, former members of those teams, for their useful comments on a previous version of this paper.
The European Commission Research Project "Cost Effective Modernisation of Systems Important to Safety (CEMSIS)" (project FIKS-CT-2000-00109) in part supported this work.

11. References

1. Licensing issues for advanced I&C technologies. Nuclear News, January 2001, 57-58.

2. Software Important to Safety in Nuclear Power Plants. IAEA Technical Reports Series 1994.. TRS N°367, 1994.

3. European nuclear regulators' current requirements and practices for the licensing of safety critical software for nuclear reactors. European Commission, DG Environment, Nuclear safety and Civil Protection, Report EUR18158 (revision 8), 1998.

Appendix 1: Contents of Safety guide NS-G-1.1

1. INTRODUCTION
2. TECHNICAL CONSIDERATIONS FOR COMPUTER BASED SYSTEMS
   Characteristics of computer based systems
   The development process
   Safety and reliability issues
   Organizational and legal issues
3. APPLICATION OF REQUIREMENTS FOR MANAGEMENT OF SAFETY TO COMPUTER BASED SYSTEMS
   Requirements for management of safety
   Design and development activities
   Management and quality assurance
   Documentation
4. PROJECT PLANNING
   Development plan
   Quality assurance programme
   Verification and validation plan
   Configuration management plan
   Installation and commissioning plan
5. COMPUTER SYSTEM REQUIREMENTS
   Recommendations
   Documents
6. COMPUTER SYSTEM DESIGN
   Recommendations
   Documents
7. SOFTWARE REQUIREMENTS
   Recommendations
   Documents
8. SOFTWARE DESIGN
   Recommendations
   Documents
9. SOFTWARE IMPLEMENTATION
   Recommendations
   Documents
10. VERIFICATION AND ANALYSIS
   Recommendations
   Documents
11. COMPUTER SYSTEM INTEGRATION
   Recommendations
   Documents
12. VALIDATION OF THE COMPUTER SYSTEM
   Recommendations
   Documents
13. INSTALLATION AND COMMISSIONING
   Recommendations
   Documents
14. OPERATION
   Recommendations
   Documents
15. POST-DELIVERY MODIFICATIONS
   Recommendations
   Documents

ANNEX: USE AND VALIDATION OF PRE_EXISTING SOFTWARE

Appendix 2:
Contents of Consensus Report EUR 19265 EN

Introduction
Background
Scope, Objectives and Implications
Safety Plan
Generic and Life Cycle Phase
Licensing Issues
Recommendations

Part 1: Generic Licensing Issues

1.1 **Categorisation and Classification**
Rationale
Issues Involved
Common Position
Recommended Practices

1.2 **Applicable Standards**
Rationale
Issues Involved
Common Position
Recommended Practices

1.3 **Use and validation of Pre-existing Software**
Rationale
Issues Involved
Common Position
Recommended Practices

1.4 **Tools**
Rationale
Issues Involved
Common Position
Recommended Practices

1.5 **Organisational Requirements**
Rationale
Issues Involved
Common Position
Recommended Practices

1.6 **Software Quality Assurance Programme and Plan**
Rationale
Issues Involved
Common Position
Recommended Practices

1.7 **Security**
Rationale
Issues Involved
Common Position
Recommended Practices

1.8 **Formal methods**
Rationale
Issues Involved
Common Position
Recommended Practices

1.9 **Independent Assessment**
Rationale
Issues Involved
Common Position
Recommended Practices

1.10 **Requirements for New and Pre-existing Software (PSW) of Safety Related Systems**
Rationale
Issues Involved
Common Position
Recommended Practices

Part 2: Life Cycle Phase Licensing Issues

2.1 **Computer Based System Requirements**
Rationale
Issues Involved
Common Position
Recommended Practices

2.2 **Computer System Design**
Rationale
Issues Involved
Common Position
Recommended Practices

2.3 **Software Design and Structure**
Rationale
Issues Involved
Common Position
Recommended Practices

2.4 **Coding and Programming Directives**
Rationale
Issues Involved
Common Position
Recommended Practices

2.5 **Verification**
Rationale
Issues Involved
Common Position
Recommended Practices

2.6 **Validation**
Rationale
Issues Involved
Common Position
Recommended Practices

2.7 **Change Control and Configuration Management**
Rationale
Issues Involved
Common Position
Recommended Practices

2.8 **Operational requirements**
Rationale
Issues Involved
Common Position
Recommended Practices

Approach to the Application of the State Regulatory Requirements, Legislation and Standards in Modernization of I&C systems, Concerning Especially the Digital Computer-Based Systems

Ing. Jan Zatloukal,
RNDr. Petr Krákora,
both ÚJV Rez a.s.

1. INTRODUCTION

This paper summarizes the experience with the specification and application of the licensing base for the modernization of I&C systems, especially with respect to the digital computer-based systems. It is based on the current project´s development state and licensing phase. The authors base their approach on the actual conditions and experience with suppliers, with whom they cooperate in the area of licensing (Ing. Zatloukal with Škoda, Nuclear Engineering, RNDr. Krákora with Framatome). By the date of the paper submission the phase 2 (which should be rounded off by the SÚJB approval of the upgrade according to §9 paragraph (1) letter f) of the Atomic Act) has not been yet completed and therefore the complete feedback, represented by the licensing documentation review and remarks by the state regulatory body, cannot be included into this version of the paper. The up-to-date experience will be therefore presented only at the seminar.

2. HISTORY

If we review the application of the digital computer-based protection and control systems and their compliance with requirements, it is necessary to recollect the history of the evolution of nuclear energy and simultaneously also the evolution of relevant legislation. The decisive period of the development of nuclear energy is the second half of the 1970s, when the government of Czechoslovakia decided to start construction of nuclear power plant based on licensed VVER-440 design. The design documentation was of Soviet origin and the construction, assembly and start-up were supervised by the authorized bodies of the Soviet Union. During continued construction of NPPs, the industry of the Czech Republic took over the increasing share of the technology supplies. However, the instrumentation and control system remained to be supplied by the former U.S.S.R. Together with the license was taken over also the safety approach based on Soviet standards. Czech legislation and standards in the area of the peaceful utilisation of the nuclear energy were significantly widened during the license appropriation. Among the most important legislative activities rank the approval of the **Act on the state supervision over the nuclear safety** and **decrees of the Czechoslovak Atomic Energy Commission No. 2, 4, 5 and 6. The Decree No. 2** specified requirements on the assurance of nuclear safety of nuclear power facilities during their design and construction, the **Decree No. 4** specified requirements on their siting. **Decree No. 5** specified basic requirements on the development, approval, implementation and control of the quality assurance programs and related measures and activities in planning, preparation, design, manufacture, assembly, commissioning and operation of selected nuclear power facilities from the viewpoint of nuclear safety. **The Decree No. 6** specified safety requirements on the nuclear power facilities during their commissioning and operation and determined the obligatory approach for bodies, organizations and their employees ensuring commissioning (including its preparation) and operation of such facilities. The decrees were subsequently applied even in the stage of the detailed design and during construction. According to these decrees, the

safety of the power plant was evaluated in the Final Safety Analyses Report before its start-up and the plant was commissioned.

Comparing the above mentioned decrees with current requirements, it can be stated that the Czechoslovak legislation (and in principle also then existing Soviet standards) were on very good level and covered all the areas of the today´s the nuclear safety policy and original principles and criteria are, to the large extent, identical with current ones. New regulations differ only in deeper explanation or in the concrete way of the realizing of the compliance with standards. The then created Czechoslovak legislation had also built on the experience of US NRC and took over some of its elements as the Technical Specifications and others, not used in Soviet approach. In licensed manufacture of the technology or in domestic supplies during assembly and tests the Soviet regulations and standards were modified to be in compliance with domestic ones or, if Soviet regulations and standards were not applicable or were missing, Czechoslovak regulations and standards were applied. In this way, the fully satisfactory system was created, completely ensuring requirements on nuclear safety as formulated in the document "Provisions on the application of regulations and standards in the design of Czechoslovak nuclear power plants with units VVER-440 with reactors V-213", issued by the Federal ministry of fuels and energetics of the ČSSR in 1980. In the 1980s nuclear power plants with VVER-440 reactors were successfully operated in the ČSSR and the construction of the Temelín NPP with VVER-100 reactors was being prepared. At the same time, the IAEA was developing the current standards of the nuclear safety goals and criteria. These are distinctly summarized in the report of the International Nuclear Safety Advisory Group (INSAG) Safety Series № 75-INSAG-3, "Basic Safety Principles for Nuclear Power Plants", and elaborated in detail in the IAEA Safety Guides (Safety Series №. 50-SG-xx).

3. NPP TEMELÍN

At the beginning of the 1990s, during construction, it was decided that the NPP Temelín has to comply with international nuclear safety criteria. Among others, it was decided about the replacement of the control system. Westinghouse Electric Corporation, the winner of the bid, incorporated into its design the digital computer-based systems, which up to then had not been used in the NPPs of the former Eastern bloc. These systems won the recognition for their indisputable advantages in other industries (including classical power plants).

Original legislation framework valid for construction and licensing of the NPP Temelín was determined by then valid acts of the CSSR, mainly the Act No. 28/84 Coll. and related regulations and decrees of the CSKAE and Soviet standards. Requirements on protection and control systems were on the legislation level formulated only vaguely and special regulations and technical standards took into account only the then used analog technology. SÚJB therefore accepted the principle of licensibility in the country of origin. The principles, guides and standards valid in the U.S.A. were therefore accepted for assessment of safety and reliability of the Temelín I&C system.

During the NPP Temelín construction, as a consequence of the split of Czechoslovakia and establishment of the SÚJB, so called "Atomic Act" – the Act No. 18/1997 Coll. – was developed and approved together with realization regulations, among others Regulations No. 195/97 Coll. and No.214/97 Coll. Therefore, it was necessary to prove the compliance with their requirements. The process of comparison of the new Czech legislation with the U.S. regulations was chosen as the most suitable.

The requirements on the safety important systems and components for the commercial nuclear reactors in the U.S.A. are codified in the Volume 10, Code of Federal Regulations, Section 50 (10 CFR 50), Appendix A, "General Design Criteria for Nuclear Power Plants". Guidelines, how to comply with the specified requirements, are in the Regulatory Requirements, Part 1, issued by the U.S. Nuclear Regulatory Commission (NRC). Generally, the Regulatory Guides in themselves do not provide all the details necessary to comply with individual requirements, but they refer to standards issued by the relevant

professional organizations. The Regulatory Guides provide the instructions about methods that are acceptable to the Nuclear Regulatory Commission. However, these methods are not the only ones acceptable by the Nuclear Regulatory Commission. The supplier in the Final Safety Analysis Report proved, that requirements of Regulation No. 195/1999 Coll. are identical to those of the NRC General Design Criteria (GDC) from Appendix A, 10 CFR Section 50, and therefore can be used without any limitations.

The basic U.S. standard for I&C systems is the IEEE Standard 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations". This standard specifies the minimum functional design criteria for the power supply and I&C of NPP safety systems and is used together with other standards that in more detail specify for instance the equipment requirements, criteria on separation, reliability analysis, human factors influence, etc. The list of all the used guides, standards, codes and regulations, their use and requested compliance was proved by the supplier in Chapter 7.1 of the NPP Temelín FSAR. In the review process of the submitted documentation, the SÚJB found such evidence as satisfactory.

4. NPP DUKOVANY

In the second half of the 1990´s, in compliance with requirements on the improvement of nuclear safety and operational reliability of the NPP, works have been initiated on the preparation of modernization of the NPP Dukovany I&C system. On April 9, 1999, on the request of the utility – CEZ a.s., NPP Dukovany, SÚJB issued its Decision No. 79/99, in which it summarizes the requirements that has to be complied with during the I&C modernization. In this way, SÚJB took from the very beginning the active approach in specification of legislation and standard requirements base (unlike at the NPP Temelín, where the process of specification of these requirements was in the introductory phases covered by the general principle of the licensibility in the country of origin). SÚJB employed its experience gained in the licensing process of the NPP Temelín and, taking into account the absence of more detailed Czech regulations and guides especially in the area of digital I&C systems, it decided to specify in advance the unified framework for the enforcement of the requirements of the Czech legislation and Czech and international standards by the issue of the document "Set of SÚJB Positions to Selected Aspects of the I&C Renovation of the Dukovany NPP" (further only the “Set of SÚJB Positions”). In this way it established the set of requirements, which allows to unify the evaluation of digital computer-based I&C systems of NPPs. This set is based on Czech and international legislation and standards in the following hierarchy (according to the priority of their application):

- Legislation of the CR (Act No.18/97 Coll., Regulation • 195/97 Coll., Regulation No. 214/97 Coll.)
- SÚJB Decision No. 97/99 and the "Set of SÚJB Positions" (appendix to letter No. 11987/3.2/00)
- IAEA Recommendations: Safety Series No.. 50-C-D/Rev.1, 50-C-D1/Rev.1, 50-SG-D3, 50-SG-D8; IEC and ISO standards (or their Czech equivalents), especially CSN IEC 643, 880, 987, 1226, IEC 61513; CSN EN ISO 9000-3; CSN ISO-IEC 12207.
- US NRC Codes and Regulations: 10CFR50, Appendix A; NUREG-0800/1997; selected Regulatory Guides, especially RG 1.152, 1.168 ÷ RG 1.173; IEEE standards, especially IEEE Std 603-1991, 7-4.3.2-1993, IEEE Standards Collection – Software Engineering (1994 edition).
- Other Czech technical standards

The set of requirements on the application of standards and regulations was included also in the tendering documentation for the Dukovany I&C modernization and subsequently it became a part of the contractual conditions.

The tender was won by the SKODA Nuclear Engineering with the principal supplier – consortium Framatome-ANP/Schneider Electric. Their solution is based on the integrated digital system SPINLINE 3, used also in EDF NPPs in France.

The proofs of compliance with the requirements are submitted to SÚJB in individual licensing stages in the form of documentation required by the Act No. 18/97 Coll., completed by others, more detailed technical reports. This documentation contains updates of the "SÚJB-approved" documentation (PSAR, Technical specifications, List of selected equipment and Program of operational controls), completed by Topical Reports both for the individual I&C systems and to the general aspects and requirements of the I&C system as a whole. These so-called Transverse Topical Reports are subdivided into the following thematic groups (as the "Set of SÚJB Positions"):

- I&C SYSTEMS CLASSIFICATION
- ACCEPTABILITY OF THE DIGITAL SOFTWARE I&C SYSTEMS IMPORTANT FOR NUCLEAR SAFETY
- REQUIREMENTS ON THE SOFTWARE DEVELOPMENT PROCESS OF I&C SYSTEMS IMPORTANT FOR NUCLEAR SAFETY
- REQUIREMENTS ON THE V&V OF THE SAFETY I&C SYSTEMS SOFTWARE
- REQUIREMENTS ON THE PROTECTION AGAINST CMF IN THE SAFETY I&C SYSTEMS SOFTWARE
- REQUIREMENTS ON THE COMMUNICATION BETWEEN SUBSYSTEMS OF THE SAFETY I&C SYSTEMS
- REQUIREMENTS ON THE TESTABILITY UNDER OPERATING CONDITIONS
- REQUIREMENTS ON MEETING THE SINGLE FAILURE CRITERION AND ON THE REDUNDANCY
- REQUIREMENTS ON THE EQUIPMENT QUALIFICATION AND THE ISSUE OF ITS VERIFICATION
- REQUIREMENTS ON THE RELIABILITY

The topical reports prepared by the supplier to individual topics are listed in the following table (corresponding Westinghouse reports for the NPP Temelín are given for the purpose of comparison):

ASPECT	NPP Temelín	NPP Dukovany
I&C SYSTEMS CLASSIFICATION		TTR 1 – Classification, NCD DC 13
ACCEPTABILITY OF THE DIGITAL SOFTWARE I&C SYSTEMS IMPORTANT FOR NUCLEAR SAFETY		TTR 2 – Acceptability of Digital Computer- Based I&C, NCD DC 11
REQUIREMENTS ON THE SOFTWARE DEVELOPMENT PROCESS OF I&C SYSTEMS IMPORTANT FOR NUCLEAR SAFETY		TTR 3 – Software Development, NCD DC 6; Software Quality Assurance Plan, NCD DC 8, SEI 1 208 718; Software Configuration Management Plan, NCD DC 10, SEI 1 208 720; Software Life Cycle Process, NCD DC 10; Software Life Cycle Process, NCD DC 10;
REQUIREMENTS ON THE V&V OF THE SAFETY I&C SYSTEMS SOFTWARE	TEM-I&C-LICEN-005 "Verification and Validation Topical Report"	TTR 4 – Software V&V, NCD DC 7
REQUIREMENTS ON THE PROTECTION AGAINST CMF IN THE SAFETY I&C SYSTEMS SOFTWARE		TTR 5 – Software Common Cause Failure, NCD DC 12
REQUIREMENTS ON THE COMMUNICATION BETWEEN SUBSYSTEMS OF THE SAFETY I&C SYSTEMS		TTR 6 – Communication, NCD DC 17
REQUIREMENTS ON THE TESTABILITY UNDER OPERATING CONDITIONS	TEM-DOC-PRJ-026, "Temelín Test Strategy Document	– TTR 7 – Testability, NCD DC 14
REQUIREMENTS ON MEETING THE SINGLE FAILURE CRITERION AND ON THE REDUNDANCY	TEM-I&C-LICEN-025 "Functional Block Analyses and Failure Modes and Effect Analyses	TTR 8 – Single Failure Criterion, NCD DC 4
REQUIREMENTS ON THE EQUIPMENT QUALIFICATION AND THE ISSUE OF ITS VERIFICATION	TEM-I&C-LICEN-020, "Methodology for Qualifying Westinghouse-Supplied Safety-Related Electrical Equipment for the NPP Temelín Instrumentation and Control Program	TTR 9 – Qualification, NCD DC 19
REQUIREMENTS ON THE RELIABILITY	TEM- I&C-LICEN -027 "Topical Report - I&C Reliability Analysis	TTR 10 – Reliability, NCD DC 20

At the time of writing of this paper, the upgrade of the NPP Dukovany I&C system was in the stage of preparation of the Basic Design and from the required license documentation the Topical Reports, Appendix to the PSAR, revision 2, version 1, the draft of the List of Selected Equipment, the draft of the Limits and Conditions and the draft of the Program of Operational Inspections were prepared and submitted to SÚJB for evaluation. The compliance with the above mentioned requirements was proved by the supplier – Framatome-ANP/Schneider Electric for the designed equipment in corresponding Topical Reports. The supplier accepted all SÚJB requirements without exception and adapted oneself to the required standard and legislation base.

Some key aspects of the I&C modernization are discussed in more detail in the following paragraphs.

5. CLASSIFICATION

Equipment classification follows the standard IEC 61226/1993, in compliance with the SÚJB requirement in the "Set of SÚJB Positions". According to it, the systems are classified into individual classes and according to their ranking they are subject to other requirements, e.g. on qualification or inclusion into the Limits and Conditions. The classification according to IEC 61226/1993 and the Regulation № 214/97 Coll. is very similar, the requirements on classified equipment of both the standard and the valid regulation shall be met. The List of selected equipment, whose draft was submitted within the phase 2 of the licensing process, uses consistently the classification according to the Decree № 214/97 Coll.

6. ACCEPTABILITY OF DIGITAL SOFTWARE I&C

As the replacement of the NPP Temelín I&C by the digital system was approved and this system was subsequently licensed, the digital software systems can be considered as generally acceptable. The "Set of SÚJB Positions" quotes only the basic legal documents mentioned previously (the Act № 18/1997 Coll., the SÚJB Regulations № 195/1997 Coll., № 214/1997 Coll., № 106/1998 Coll.) and the requirements on the new system for the NPP Dukovany are generally specified in the „Resolution № 79/99“ independently on the fact if the system is digital or not. The volume 7 of the FSAR Update under acceptability understands the extent and requirements of IEC 61513, which further states, that the requirements on SW of digital computer-based systems to be applied in I&C category A systems are specified for SW in standards IEC 60880 and 60880-2 and on HW in IEC 60987.

Transverse Topical Report 2 was elaborated to this topics by the supplier to be transmitted to SÚJB.

7. SOFTWARE DEVELOPMENT PROCESS, SOFTWARE V&V

For modernized digital computer-based I&C systems, classified as IEC 61226 category A, the SW development process shall be (according to the "Set of SÚJB positions" a complex process containing:

- planning activities,
- life cycle process activities, and
- some transverse activities of the SW life cycle process implementation.

An appropriate set of SW life cycle activities is provided for instance in Regulatory Guide 1.173 "Developing SW Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", which endorses IEEE Std 1074 "Standard for Developing Life Cycle Processes".

Planning activities shall result in a set of planning documents, containing

- SW Project Management Plan
- SW Quality Assurance Plan
- SW Verification & Validation Plan
- SW Configuration Management Plan
- SW Safety Plan, and
- SW Life Cycle Plan, which can be divided according to individual steps of the SW life cycle process into:
  - SW Development Plan
  - SW Integration Plan
  - SW Installation Plan
  - SW Training Plan
  - SW Operations Plan
  - SW Maintenance Plan.

In licensing process, phase 2, the supplier carried out required planning documentation as parts of Transverse Topical Reports 3 and 4 (see the table above).

The required outputs of the **life cycle process activities** are following design documents (only documents listed, worked out in phase of basic design):

- SW Requirements Specifications (SRS)
- SW Design Specifications

In the scope of basic design the supplier provided a set of documents containing input data for SW requirements specifications and several documents concerning the design specifications (functional diagrams, equipment specifications).

Other documentation (as Operation, Maintenance and Training manual) will be completed in later design phases.

Other **"transverse" activities of the SW life cycle process implementation** contain V&V (the required output is the set of V&V reports), configuration management (CM reports) and Safety analyses.
SÚJB requires for the V&V Process to meet the requirements of IEC 880, but does not insist on performing the V&V by a third independent organization assuming that the group carrying out the activities at the manufacturer's is in no way interested in the development process of the verified SW.

8. PROTECTION AGAINST COMMON MODE FAILURE, IMPLEMENTATION OF DIVERSITY AND DEFENSE IN DEPTH

The assurance of robustness against the common mode failures in performance of the safety important I&C functions and implementation of diversity is not required by the Czech legislation (there are only general requirements). The SÚJB Resolution № 79/99 specifies the requirements on diversity (items 11,B.3.a and 11,B.3.b), Czech legislation solves only separation of protection and control systems (Regulation № 195/99 Coll.).

The "Set of SÚJB positions" prefers the approach of US NRC and recommends as an example the Westinghouse document TEM-I&C-LICEN-017, which elaborates the design criteria for the diversity implementation. In relation to the Dukovany I&C modernization the document further develops the requirements on diversity.

The requirement on implementation of diverse line of protection in the U.S. legislation is on the general level stated in GDC 22 as the measure against the loss of the protective function and is specified in §50.62 of 10CFR50 for the purposes of ATWS (Anticipated Transient Without Scram). This requirement was later on extended in the US NRC Staff Requirements Memorandum on SECY 93-087 into so called four-point position, concerning the issues of the diversity and defense-in-depth implementation in safety important digital computer-based I&C systems. Good presentation of the methodology gives NUREG/CR-6303.

SÚJB requires implementation of diversity in protection against PIE solved in the safety analyses with occurrence frequencies above 10^{-3}/year (ANSI condition II, III). It is possible to limit the CMF postulation only to SW of the programmable parts of systems performing safety functions. It is also admissible not to consider the SW CMF in SW modules for which a 100% reliability will be declared (error-free SW). The diversity can be implemented as functional diversity or equipment diversity. The analysis of implemented diversity is required.

These requirements were taken into account by the supplier in the Basic Design and the topics was evaluated in the Licensing documentation: Transverse Topical Report 5 - Software Common Cause Failure, and the FSAR Update, vol. 7, rev.1, version 1). The supplier also took into account the newest IEC 60880-2 standard. Implemented CMF is based on means of functional and signal diversity. Transverse Topical Report 5 presents also the preliminary analysis of SW CMFs, the required detailed analysis will be submitted during next licensing phase.

9. single failure criterion (SFC), redundancy

SÚJB in the "Set of SÚJB positions" specifies for the case of EDU I&C modernization the definition of the single (random) failure criterion, including all operation states/conditions, during which the SFC shall be considered. SÚJB does not exclude the possibility of acceptance of extraordinary cases, in which the protection system will not be resistant against the single failure, but requires an exact specification of such conditions and their strict limitation, individual discussions and a demonstration, that the refusal of the exception would cause very significant and hardly feasible design modifications.

In the interpretation of the requirement on redundancy, at least threefold redundancy of all parts of protection systems is recommended (to express it in a simplified way). There shall be a deterministic evidence of meeting the SFC, probabilistic analysis will not be accepted.

During phase 2 of the licensing process the supplier carried out the Transverse Topical Report 8 - Single Failure Criterion, discussing the implementation of SFC and redundancy and containing also the deterministic analyses for the protection system.

10. CONCLUSIONS

The active SÚJB approach, consisting in early definition of the requirements beyond the Czech legislation and standards (especially for the digital computer-based systems), allowed CEZ to implement the specified requirements into contract documents. In this way priorities in application of legislation, guides, standards and other requirements together with their applicability status were set.

The application of the requirements, especially in several key aspects specified in the Set of SÚJB positions, express in all levels of the project: in contract provisions, design specifications (requirements on the system architecture, operational and performance requirements) as well as in design and licensing (safety) documentation.

The present state of the project (Basic Design, Licensing Phase 2) shows, that the used approach of early requirements specification serves well. Contemporary Czech legislation based on the Atomic Act and executive regulations together with clearly specified SÚJB positions establish an appropriate frame for application of other both Czech and international codes and standards without the need of further legislative codification of additional principles and requirements.

Standard Base for Regulatory Activity in NPP I&C Area

M. Yastrebenetsky, V. Goldrin, Yu. Rozen, S. Vinogradskaya

State Scientific Technical Center on Nuclear and Radiation Safety,
17 Artema str., Kharkov 61002, Ukraine

Tel.: +38 0572 471 700, Fax: +38 0572 471 700

e-mail: yastreb@reliable.kharkov.ua, rel@online.kharkiv.com

Summary

Ukrainian standard base for regulatory activity in the area of NPP I&C systems now includes 3 documents:

- *"Requirements on Nuclear and Radiation Safety to NPP I&C Systems Important to Safety" [1, 2]*
- *"Methodic of Assessment of Compliance of NPP I&C Systems to Safety Requirements" [3, 4]*
- *"Requirements to Order and Contents of Life Extension of Instruments which are included into Safety Important Systems" [5, 6]*

The methods of selection of regulatory requirements for I&C systems (status, criteria of selection, systematization of initial date, procedure of establishing, main peculiarities, etc.) were examined.

1. Introduction

Under establishment of standard base for regulatory activity in NPP instrumentation and control (I&C) systems area in Ukraine, different methods are possible in principle:

- to adopt as standard base the requirements of normative documents on safety that are currently in force in any other country (for example USA, Germany, Russia);

- to adopt as standard base the requirements of international standards and guides on safety developed by IAEA, IEC, ISO not creating own ones;

- to work out the own standard base taking into consideration home and international experience on regulation and safety evaluation as well as available scientific-technical and economical potentials for NPP safety assurance in Ukraine.

The last version was adopted, as:

- the Ukraine already has her own formed system of normative documents on nuclear safety and new documents shall fit the structure of this system.
- at Ukrainian NPP are implemented the I&C systems, designed not only by Ukraine but by great number of foreign companies (for example USA, Germany, Czech Republic, Russia), each of them uses the standard base of their own country. The Ukrainian standard base shall be unified for all these systems;
- the countries with different economic development have non-similar means to provide and confirm safety of their NPP that considerably influence the level of standard bases of these countries.

The standard base:
- applies to I&C systems important to safety and their components:
  - software-hardware complexes (SHC);
  - hardware (HW);
  - software (SW);
- not contrary to laws and basic normative documents on nuclear safety that are currently in force in Ukraine ;
- harmonized to a maximal possible extent with the requirements of international safety standards and guides [7-9, etc.] that are not included in Ukrainian normative documents;
- use the experience of safety regulation available in national standards of the leading countries.

Let us dwell on the development methods of the first of three indicated documents. These methods provide the following:
- determination of a status of developed documents (their category, rank and connections in the system of normative documents on nuclear safety that are currently in force in Ukraine;
- establishment of criteria for selection of regulatory requirements;
- systematization of initial data used for safety regulation of I&C systems and their components;
- standardization of regulation procedure (establishment of regulatory requirements)

The status of developed documents

In the system of documents on nuclear safety that are in force in Ukraine it is possible to separate out three hierarchy levels.

The upper hierarchy level is the documents of government bodies (Ukrainian legislation, decrees of Ministry Councils) determining the order of state safety regulation in the scope of nuclear power use.

Normative documents developed and/or put in force by Regulatory Body of Ukraine, containing the basic provisions on assurance of NPP safety including the fundamental regulatory requirements to their systems and components (including I&C systems) are considered as the second hierarchy level.

The third hierarchy level is represented by normative documents of Regulatory Body of Ukraine, which establish the general regulatory requirements with regard to determined tasks, system classes or kinds of NPP equipment.

The connections between these hierarchy levels provide the following:
- requirements established in documents of upper hierarchy level are detailized in documents of downstream adjacent hierarchy;
- documents of more low hierarchy level can in case of necessity establish the additional regulatory requirements;

- in documents of lower hierarchy level the requirements contradictory to requirements established in documents of any upper hierarchy level shall not be laid down.

On the grounds of stated above it is determined that documents being developed on I&C systems regulation and safety evaluation should:

- be positioned on the third hierarchy level;
- establish the general regulatory requirements with regard to I&C systems important to safety of NPP and their components that ad and/or detailize the basic requirements of normative documents of the second hierarchy level;
- be binding under elaboration of normative, project, design and other documents and carrying out of works on creation, reconstruction or modernization particular I&C systems and their components;
- be used as basis for evaluation of I&C systems safety, both acting at Ukraine NPP and new (reconstructed, modernized) ones.

Selection criteria of regulatory requirements

An important aspect of safety regulation methods is the establishment of guideline criteria for determination of composition and contents of regulatory requirements on I&C systems and their components. Such criteria were elaborated as result of analyses and summarizing of domestic and foreign normative documents, recommendations of international organizations on safety as well as other sources.

Under elaboration of normative documents the following criteria ("requirements to regulatory requirements") are used:

- ***necessity*** – criteria according to which the using of I&C systems not meeting this regulatory requirements can result in violation of limits and/or conditions of NPP safe operation;
- ***completeness*** - criteria according to which the using of I&C systems meet all qualifying standards most likely does not result in violation of limits and/or conditions of NPP safe operation;
- ***sufficiency*** – completeness criteria attributed to separate regulatory requirement;
- ***unambiguous*** - criteria according to which the least rigid requirement of possible versions meeting the sufficiency criteria are adopted as the regulatory requirements;
- ***correctness*** – correspondence of regulatory requirement with respect to similar requirements that are regulated in normative documents of the same and/or more upper hierarchy level;
- ***progressiveness*** – meeting of the regulatory requirement the achieved level of science, engineering and technology;
- ***testability*** – the possibility of evaluation of I&C systems meeting to the regulatory requirements, which are based upon the facts, test results and/or analyses results;
- ***traceability*** – testability criteria attributed to different stages of object life cycle;
- ***clarity*** – quality criteria of regulatory requirement statement providing its understanding by specialists without additional explanations;
- ***uniqueness (single meaning)*** - quality criteria of statement which makes it impossible to interpret differently the same regulatory requirement;
- ***categoricity*** - criteria according to which each I&C systems shall meet all relevant regulatory requirements.

During safety regulations the necessity, completeness and sufficiency criteria were taken into account when determining the list of the regulatory requirements; the correctness, progressiveness, testability and traceability criteria – when establishing the concept contents of each requirement; the clarity and uniqueness criteria – when stating the regulatory requirements in the developed normative document. The testability, traceability, clarity, uniqueness criteria as well as categoricity of regulatory requirements are essential from the point of view of safety evaluation.

Initial date systematization

The normative base foundation used under elaboration of regulatory requirements of I&C systems and their components is as following:

- Ukrainian Legislations concerning nuclear power use and nuclear safety;
- Norms and Rules on Nuclear Safety;
- Standards of former USSR that are currently in force in Ukraine;
- Ukrainian Standards;
- Safety Standards and Guides developed by international organizations – IAEA, IEC, ISO;
- National Standards of USA, Germany, France, Russia.

The documents of two last groups are not formally adopted in Ukraine; therefore, the requirements, norms and rules included into them cannot be regarded as per definition as regulatory requirements for Ukraine. However, they are of exclusively great importance for our county, as they reflect the international experience that «outrunning the limits of purely national bounds tends to definite harmony in practice of safety assurance at the European and even the world level" [11].

In accordance with the adopted methods, all abovementioned normative documents (ND) are structured as per two classification characteristics.

Depending on the subject of normative regulation the following classes are marked out:

- ND on NPP safety containing requirements to NPP systems and elements, that apply also to I&C systems and/or their components (class A: "NPP Safety");
- ND establishing the requirements to I&C systems and their components used in different industrial branches including NPP (class B: "Industrial systems");
- ND that are concerned directly and only to NPP I&C systems and their components (class C: "NPP I&C systems");
- ND of general technical nature establishing requirements related to NPP I&C systems (class D: "General Technical ND").

Depending on the scope of activity ND are divided into the following types:

- Ukrainian Legislations, Standards, Normative Decrees of Ukrainian Regulation Body (type 1: "Ukrainian ones");
- Norms and rules on nuclear safety and standards of former USSR that are currently in force in Ukraine (type 2: Interstate ND);
- Safety Standards and Guides of International Organization (type 3: "International ones");
- National Standards of other countries (type 4: "National ones").

Crossings of rows (classes) and columns (types) generate the groups of ND, each of which was analyzed during the development.

Procedure of establishment of regulatory requirements

Proposed procedure provides the following order of initial data analyses and establishment of regulatory requirements to I&C systems [1,2]:

- in accordance with the adopted structure of normative base for each group of ND the lists of normative documents that include the requirements to I&C systems and their components are worked out;

- the complete lists of such requirements regulated in each of analyzed normative documents are worked out;

- on the ground of necessity criteria the requirements important from the point of view of nuclear safety assurance are generated;

- for each of such requirement the essential analyses are carried out using method of comparison its statements within different normative documents, probably, with involvement of other sources (publications, reports, etc.);

- carrying out the evaluation if each requirement meets the criteria of completeness, unambiguous, correctness, progressiveness, testability and traceability;

- according to analyses results the statements of regulatory requirements are offered;

- each statement is evaluated as per clarity and completeness criteria;

- in accordance with the necessity, completeness and sufficiency criteria the complete lists of requirements to I&C systems are determined as well as the degree of their binding (depending on safety class, functional destination and other peculiarities of subject of regulation).

Table 1 – 3 present the proposed lists of the regulatory requirements to I&C systems, hardware (HW) and software (SW).

Table 1. Regulatory requirements to I&C systems

Group of requirements
Meeting single failure principle
Meeting independence principle
Meeting redundancy principle
Meeting diversity principle
Requirements to protection against common cause failures
Requirements to reliability
Requirements to accuracy
Requirements to response rate
Requirements to human-machine interface
Requirements to protection against unauthorized access
Requirements to technical diagnostics
Requirements to prevention from staff errors
Requirements to resistance against environmental impact
Requirements to resistance against changing parameters of supplied power
Requirements to quality
Requirements to testing and acceptance

Table 2. Regulatory requirements to HW

Group of requirements
Requirements to stability against the environmental impact
Requirements to stability against mechanical impacts
Requirements to stability against electrical fields
Requirements to stability against impact of special media
Requirements to stability against changing parameters of supplied power
Requirements to accuracy
Requirements to electrical insulation
Requirements to electromagnetic compatibility
Requirements to reliability
Requirements to testability
Requirements to protection against unauthorized access
Requirements to fire safety
Requirements to qualification

Table 3. Regulatory requirements to SW

Group of requirements
Requirements to structure and elements of SW
Requirements connected with diagnostics and self-inspection
Requirements connected with provision for reliability
Requirements connected with protection of data
Requirements to process of SW development
Requirements to used SW
Requirements to documenting of SW development
Requirements to procedures of SW verification
Requirements to documents on SW verification

The main peculiarities of regulation "Methodic of Assessment of Compliance of I&C systems to Safety Requirements"

- Maximum usage of existing in Ukraine types of documents. Expert review of each document is performed immediately after preparation of this document – almost in "on-line" mode. Safety Analysis Report is important but is not the only document in the complete set of documents for safety assessment. The designer and NPP can analyze the remarks of experts and make appropriate changes without long delay.

- Typical steps of I&C systems expert review:

    - expert review of NPP technical decision on modernization (with conception of modernization);

    - expert review of specification;

    - expert review of design documentation;

    - expert review of software V&V plan and report;

    - expert review of Safety Analysis Report;

    - expert review of methodic and results of site acception test.

- Safety assessment includes:

    - software and hardware analysis along with analysis of systems as a whole;

    - analysis of the interface between I&C modernized and unchanged parts;

- analysis of the system quality assurance program.

- Each expert review contains a set of expert cards. Each card contains:
    - the requirements according to standards, rules, guides;
    - brief description (summary) of this requirements realization in system documentation;
    - expert evaluation;
    - conclusion and recommendations.

Regulatory requirements was used in licensing of computer information systems, SPDS, automatic regulators, refueling machine control systems, protection systems, etc. (designers of these systems were the companies of USA, France, Germany, Czechia, Russia, Ukraine) for Ukrainian NPP. These requirements will be used under licensing process of I&C systems for new units – Rovno 4 and Khmelnitsky 2.

References

1. NP306.5.02/3.035-2000. Requirements of Nuclear and Radiation Safety to NPP I&C Systems Important to Safety on NPP/ M.A. Yastrebenetsky (ed.), Y.V. Rozen, V.S. Kharchenko et al., Nuclear Regulatory Administration of Ukraine, Kiev, 2000.

2. M. Yastrebenetsky, Y. Rozen, V. Vasilchenko, S.Vilkomir. Elaboration of common regulatory requirement on modernized NPP instrumentation and control system important to safety. Foresight and precaution. Proceedings of ESREL 2000, SARS and SRA-Europe annual conference.A.A.Balkema, Rotterdam, 2000,p.813-817.

3. NP 306.7.02/2.041-2000. Methodic of Assessment of Compliance of NPP I&C Systems to Safety Requirements/ M.A. Yastrebenetsky (ed.), S. V. Vinogradskaya, V.S. Kharchenko et al., Nuclear Regulatory Administration of Ukraine, Kiev, 2000.

4. M. Yastrebenetsky. Safety assessment of NPP instrumentation and control systems. Nuclear plant instrumentation , control and human-machine interface technologies (NPIC & HMIT 2000).American Nuclear Society. 2000. Washington, DC. ISBN : 0-89448-6446.

5. ND 306.711-96. Life extension of hardware included into safety important I&C Systems. General requirements to order and content of works/ M.A. Yastrebenetsky (ed.), V.M. Goldrin. Ukrainian Ministry of environment protection and nuclear safety. Kiev, 1996.

6. M.A. Yastrebenetsky, L.N. Garagulya, etc. Reliability analysis of VVER-1000 information and control system. The 3rd JSME/ASME Joint International Conference on Nuclear Engineering. Kyoto, Japan. 1995, Vol. 3, p. 1295-1298.

7. IAEA 50-Sg –D3. Protection System and Related Features in Nuclear Power Plants.

9. IAEA 50-Sg-D8. Safety-Related Instrumentation and Control Systems for Nuclear Power Plants.
10. IAEA Safety Standards Series. Instrumentation and Control Systems Important to Safety in Nuclear Power Plants. Draft safety guide.
11. IEC 880. Software for Computers in the Safety Systems of Nuclear Power Plants.

12. Libmann, J., Elements of Nuclear Safety, EDP, France, 1996

TECHNICAL SESSION 2
REGULATORY ASPECTS

Chairmen: K. Hamar, A. Lindner

EMI/RFI and Power Surge Withstand Guidance for the U.S. Nuclear Regulatory Commission

C. Antonescu[1], P. D. Ewing[2]

[1]U.S. NRC, Office of Nuclear Regulatory Research, ERAB, MS T-10E33, 2 White Flint North, 11545 Rockville Pike, Rockville, Maryland 20852, USA
Tel.: +011 1 301 415 6792, Fax: +011 1 301 415 5160, e-mail: cea1@nrc.gov

[2]Oak Ridge National Laboratory, P.O. Box 2008, MS 6006, Oak Ridge, Tennessee 37831 USA
Tel.: +011 1 865 576 5019, Fax:+011 1 865 576 2813, e-mail: ewingpd@ornl.gov

Summary

This paper discusses the regulatory guidance implemented by U.S. NRC for minimizing malfunctions and upsets in safety-related instrumentation and control (I&C) systems in nuclear power plants caused by electromagnetic interference (EMI), radio-frequency interference (RFI), and power surges. The engineering design, installation, and testing practices deemed acceptable to U.S. NRC are described in Regulatory Guide (RG) 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency in Safety-Related Instrumentation and Control Systems" (January 2000) and in a Safety Evaluation Report (SER) endorsing EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," (April 1996). These engineering practices provide a well-established, systematic approach for ensuring electromagnetic compatibility (EMC) and surge withstand capability (SWC).

Introduction

The typical environment in a nuclear power plant includes many sources of electromagnetic interference (EMI), radio-frequency interference (RFI), and power surges, e.g., hand-held two-way radios, arc welders, switching of large inductive loads, high fault currents, and high-energy fast transients associated with switching at the generator or transmission voltage levels. The increasing use of advanced analog- and microprocessor-based instrumentation and control (I&C) systems in reactor protection and other safety-related plant systems has introduced concerns with respect to the susceptibility of this equipment to EMI/RFI and power surges, as well as the creation of additional noise sources.

Digital technology is constantly evolving, and manufacturers of digital systems are incorporating increasingly higher clock frequencies and lower logic level voltages into their designs. However, these performance advancements may have an adverse impact on the operation of digital systems with respect to EMI/RFI and power surges because of the increased likelihood of extraneous noise being misinterpreted as legitimate logic signals and of surge potentials causing equipment/parts damage. With recent advances in analog electronics, many of the functions presently being performed by several analog circuit boards could be combined into a single analog circuit board operating at reduced voltage levels, thereby making analog circuitry more susceptible to EMI/RFI and power surges, as well. Hence, operational and functional guidance related to safety in the nuclear power plant environment is necessary to address the possibility of upsets and malfunctions in I&C systems caused by EMI/RFI and power surges.

Regulatory Guide (RG) 1.180, *Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems*, was issued in January 2000 to address EMI/RFI and power surge issues for safety-related digital I&C systems in nuclear power plants. The technical basis behind the practices in RG-1.180 is given in NUREG/CR-5941, *Technical Basis for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems*, and NUREG/CR-6431, *Recommended Electromagnetic Operating Envelopes for Safety-Related I&C Systems in Nuclear Power Plants*. Prior to the issuance of RG-1.180, NRC staff had accepted the Electric Power Research Institute (EPRI) topical report TR-102323, *Guidelines for Electromagnetic Interference Testing in Power Plants*, in a Safety Evaluation Report (SER) by letter dated April 17, 1996 as one method for addressing electromagnetic compatibility (EMC) issues in safety-related digital I&C systems. RG-1.180 complements the position set forth in the SER by improving the technical basis for evaluating EMI/RFI immunity and power surge withstand capability (SWC).

RG-1.180 and the EPRI TR-102323 SER adhere to the same overall approach and are generally in agreement. Each recommends EMI/RFI-limiting practices based on IEEE Std 1050, endorses emissions and susceptibility test criteria and test methods to evaluate safety-related I&C systems, and identifies appropriate operating envelopes for equipment and systems intended for selected locations in nuclear power plants. Each document presents acceptable means for demonstrating EMC and they are consistent in their respective approaches. The licensee has the freedom to choose the method best suited to the situation.

Design and Installation Practices

RG-1.180 endorses the design and installation practices described in IEEE Std 1050-1996, *IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations*, as suitable for limiting the generation and effects of EMI/RFI and power surges. IEEE Std 1050-1996 was developed primarily to provide guidance on the design and installation of grounding systems for I&C equipment specific to power generating stations. Further purposes of the standard are to achieve both a suitable level of protection for personnel and equipment, and suitable electrical noise immunity for signal ground references in power generating stations. IEEE Std 1050-1996 addresses grounding and noise-minimization techniques for I&C systems and recommends practices for the treatment of both analog and digital systems. The standard specifically addresses the grounding and shielding of electronic circuits on the basis of minimizing emissions and their susceptibility to EMI/RFI and power surges. The SER accepts the 1989 version of IEEE Std 1050. There are minor differences between the 1989 and 1996 versions of IEEE Std 1050, with some technical ambiguities from the 1989 version being cleared up in the 1996 version.

One exception was taken in RG-1.180 to the design and installation practices in IEEE Std 1050-1996. Section 4.3.7.4, "Radiative Coupling," of the standard maintains that the "field strength" of propagating electromagnetic waves is inversely proportional to the square of the distance from the source of radiation. This statement needs to be reevaluated because radiative coupling is a far-field effect. A distance, r, greater than the wavelength divided by 2π ($r > \lambda/2\pi$) from the source of radiation is considered to be far field, which is the region where the wave impedance is equal to the characteristic impedance of the medium. Both the electric and magnetic "field strengths" fall off as $1/r$ in the far field, not as $1/r^2$. This concept is not to be confused with the propagation of electromagnetic waves in the near field ($r < \lambda/2\pi$) where the wave impedance is determined by the characteristics of the source and the distance from the source. In the near field, if the source impedance is high ($>377\Omega$), the electric and magnetic "field strengths" attenuate at rates of $1/r^3$ and $1/r^2$, respectively. If the source impedance is low ($<377\Omega$), the rates of attenuation are reversed: the electric "field strength" will fall off at a rate of l/r^2 and the magnetic "field strength" at a rate of $1/r^3$. The significance of this exception lies in the appropriate application of the design and installation practices in IEEE Std 1050-1996. For example, the strength of magnetic fields

from a low-impedance source is typically substantially much reduced within a short distance and simply moving equipment away from strong sources of magnetic fields can prevent interference problems.

IEEE Std 1050-1996 references other standards that contain complementary and supplementary information. In particular, IEEE Std 518-1982, *IEEE Guide for the Installation of Electrical Equipment to Minimize Noise Inputs to Controllers from External Sources*, and IEEE Std 665-1995, *IEEE Guide for Generating Station Grounding*, are referenced frequently. The portions of IEEE Std 518-1982 and IEEE Std 665-1995 referenced in IEEE Std 1050-1996 are endorsed by RG-1.180 and are to be used in a manner consistent with the practices in IEEE Std 1050-1996.

EMI/RFI Testing Practices

To verify the adequacy of safety-related I&C systems and equipment design, both RG-1.180 and the SER endorse applicable EMI/RFI test criteria in the U.S. Department of Defense's Military Standard (MIL-STD) 461, *Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference*. Also endorsed are the associated test methods in MIL-STD 462, *Measurement of Electromagnetic Interference Characteristics*. EMI/RFI test criteria from both MIL-STD 461C and 461D, as well as their respective MIL-STD 462 and 462D test methods, are cited in RG-1.180 and the SER. The bases behind the selections are detailed in NUREG/CR-5941 for RG-1.180 and in EPRI TR-102323 for the SER. MIL-STDs 461 and 462 were developed as measures to ensure EMC. Applications of the MIL-STD test criteria and test methods are tailored for the intended function of the equipment and the characteristic environment (i.e., which tests and what levels are applied depend on the function to be performed and the location of operation).

The MIL-STD 461D test criteria acceptable to the U.S. NRC in RG-1.180 and the SER for susceptibility and emissions testing on safety-related I&C systems intended for nuclear power plants are listed in Table 1. These criteria cover conducted and radiated interference (emissions and susceptibility), exposure to electric and magnetic fields, and noise coupling through power and control leads. The criteria do not cover conducted interference on interconnecting signal lines because the MIL-STD test methods do not explicitly address signal line conducted susceptibility. Research covering this area is presently ongoing. MIL-STD 461D provided the latest revision of the test criteria at the time that RG-1.180 and the SER were issued, thus it represents current practice. However, guidance on the MIL-STD 461C counterparts to the MIL-STD 461D test criteria is also given to avoid placing an undue burden on the nuclear power industry by limiting the available test resources to those test laboratories with just the MIL-STD 462D test capability.

Table 1 MIL-STD 461D Test Criteria.

Criterion	Description
CE101	Conducted emissions, power leads, 30 Hz to 10 kHz
CE102	Conducted emissions, power leads, 10 kHz to 10 MHz
CS101	Conducted susceptibility, power leads, 30 Hz to 50 kHz
CS114	Conducted susceptibility, bulk cable injection, 10 kHz to 400 MHz
RE101	Radiated emissions, magnetic field, 30 Hz to 100 kHz
RE102	Radiated emissions, electric field, 10 kHz to 1 GHz
RS101	Radiated susceptibility, magnetic field, 30 Hz to 100 kHz
RS103	Radiated susceptibility, electric field, 10 kHz to 1 GHz

C = conducted, E = emissions, R = radiated, and S = susceptibility.

RG-1.180 provides two acceptable suites of EMI/RFI emissions and susceptibility criteria. It is intended that either set of test criteria be applied in its entirety, without selective application of individual criteria (i.e., no mixing and matching of test criteria). The reason for this is the avoidance of lapses in frequency coverage of the criteria, discontinuities in test phenomena coverage, miscalculations in test unit conversions, and unreasonable comparisons of operating envelope levels. The SER does allow mixing and matching, but exercising good engineering judgement in the performance of the EMI/RFI tests is recommended when doing so.

The MIL-STD 461 test criteria have associated operating envelopes that serve to establish test levels. The operating envelopes that are acceptable to the U.S. NRC are not given herein, but can be found in RG-1.180 and the SER. The operating envelopes in both documents are similar, with only minor differences. The detailed technical basis for the operating envelopes in RG-1.180 is presented in NUREG/CR-6431. The technical basis for the RG-1.180 operating envelopes begins with the MIL-STD envelopes corresponding to the electromagnetic environment for military ground facilities, which were judged to be comparable to that of nuclear power plants based on general layout and equipment type considerations. Plant emissions data measured at 14 nuclear units were used to confirm the adequacy of the operating envelopes. From the MIL-STD starting point, susceptibility envelopes were adjusted to account for the plant emissions measurement data collected at eight nuclear units in 1995 and reported in NUREG/CR-6436, *Survey of Ambient Electromagnetic and Radio-Frequency Interference Levels in Nuclear Power Plants*. In addition, emissions data collected at six nuclear units during a 1994 EPRI study were used as a basis for adjusting the susceptibility envelopes. Figure 1 illustrates the comparison of the power plant data and the operating envelope for radiated electric fields (RS103), while Figure 2 illustrates a similar comparison for radiated magnetic fields (RS101). The basis for adjustments to the equipment emissions envelopes included consideration of the primary intent of the MIL-STD envelopes and maintaining some margin with the susceptibility envelopes. Finally, when changes to the operating envelopes from the MIL-STD origin were motivated by technical considerations, consistency among the envelopes for comparable test criteria was promoted and commercial emissions limits for industrial

environments were factored into adjustments of the envelopes. The basis for the operating envelopes endorsed by the SER is detailed in EPRI TR-102323.

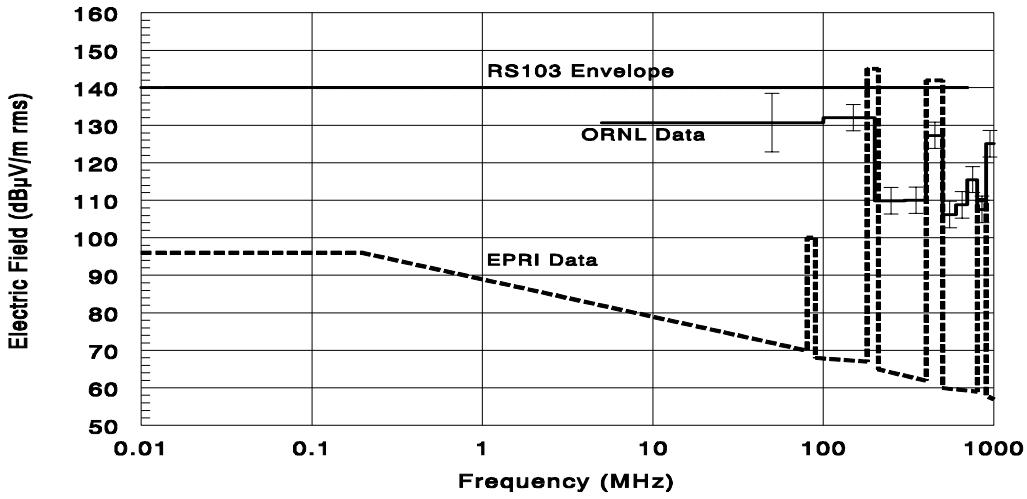


Figure 1 Plant Data vs Radiated Electric Fields Envelope

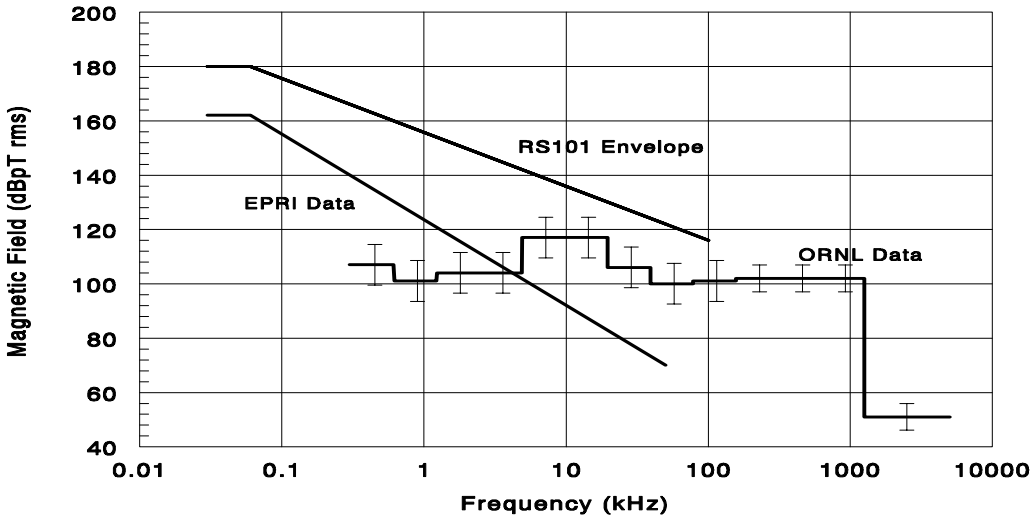


Figure 2: Plant Data vs Radiated Magnetic Fields Envelope

Surge Withstand Capability (SWC) Testing Practices

RG-1.180 endorses the SWC test criteria recommended in IEEE Std C62.41-1991, *IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits*, and the associated test methods recommended in IEEE Std C62.45-1992, *IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits*. IEEE Std C62.41-1991 provides guidance for the selection of voltage and current surge test criteria for evaluating the SWC of equipment connected to low-voltage ac power circuits. The standard defines a set of surge test waveforms that includes lightning-induced transients, oscillatory ring waves, and electrically fast transients (EFT) caused by load switching. The recommended test waveforms have manageable dimensions and represent a baseline surge environment. IEEE Std C62.45-1992 provides guidance on the test methods and equipment to be employed when performing the surge tests. The SER endorses the comparable surge testing practices in Parts 4 and 5 of the International Electrotechnical Commission (IEC) Standard 801, *Electromagnetic Compatibility for Industrial Process Measurement and Control Equipment*. IEC 801 has been superseded by IEC 61000-4, *Electromagnetic Compatibility: Part 4, Testing and Measurement Techniques.* Typical environmental conditions for surges in a nuclear power plant can be represented by the waveforms given in Table 2.

Table 2 Representative Power Surge Waveforms.

Parameter	Ring Wave	Combination Wave		EFT
Waveform	Open-circuit voltage	Open-circuit voltage	Short-circuit current	Pulses in 15-ms bursts
Rise time	0.5 µs	1.2 µs	8 µs	5 ns
Duration	100 kHz ringing	50 µs	20 µs	50 ns
Peak value	3 kV	3 kV	1.5 kA	3 kV

Withstand levels that are acceptable to the U.S. NRC are given in RG-1.180 for each surge waveform. IEEE Std C62.41-1991 describes location categories and exposure levels that define applicable amplitudes for the surge waveforms that should provide an appropriate degree of SWC. Location categories depend on the proximity of equipment to the service entrance and the associated line impedance. Exposure levels relate to the rate of surge occurrence versus the voltage level (e.g., surge crest) to which equipment is exposed. Withstand levels are presented in NUREG/CR-6431 and based on *Category B* locations and *Low to Medium Exposure* levels. *Category B* covers feeders and short branch circuits less than 10 meters from the service entrance. *Low to Medium Exposure* levels encompass systems in areas known for little load or capacitor switching and low-power surge activity to areas known for significant switching transients or medium- to high-power surge activity. Comparable IEC 801 SWC levels, also acceptable to the U.S. NRC, are given in the SER.

Regulatory Positions

Table 3 lists the specific regulatory positions in RG-1.180 that have been set forth by the U.S. NRC. This guidance complements the position set forth in the SER by improving the technical basis for evaluating EMI/RFI and power surges. The RG-1.180 guidance is applicable for all new safety-related systems or modifications to existing safety-related systems that include analog, digital, or hybrid (i.e., combined analog and digital electronics) equipment. While nonsafety-related systems are not part of the

guidance, control of EMI/RFI from these systems is deemed necessary to ensure that safety-related I&C systems continue to perform properly.

The electromagnetic conditions at the point of installation for safety-related I&C systems should be assessed to identify EMI/RFI sources that may generate local interference. The EMI/RFI sources could include mobile, portable, and fixed equipment. Steps should be taken during installation to ensure that systems are not exposed to EMI/RFI levels from sources that are greater than 8 dB below the operating envelopes. When feasible, the emissions from nonsafety-related systems should be held to the same levels as safety-related systems.

The endorsed operating envelopes are acceptable for locations where safety-related I&C systems either are or are likely to be installed and include control rooms, remote shutdown panels, cable spreading rooms, equipment rooms, auxiliary instrument rooms, relay rooms, and other areas (e.g., the turbine deck) where safety-related I&C system installations are planned. To ensure that the operating envelopes are being used properly, equipment should be tested in the same physical configuration as that specified for its actual installation in the plant. In addition, the physical configuration of the safety-related I&C system should be maintained and all changes in the configuration controlled. The design specifications that should be controlled include cable separations, shielding techniques, enclosure integrity, apertures, gasketing, grounding techniques, and EMI/RFI filters. Also, the endorsed test methods for evaluating electromagnetic emissions, EMI/RFI susceptibility, and power SWC are intended to be applied to the safety-related I&C equipment in test facilities or laboratories prior to installation.

Any modifications to the electromagnetic operating envelopes (e.g., lower site-specific envelopes) should be based on technical evidence comparable to that presented in NUREG/CR-6431. Relaxation in the operating envelopes should be based on actual measurement data collected in accordance with IEEE Std 473-1985, *IEEE Recommended Practice for an Electromagnetic Site Survey (10 kHz to 10 GHz)*.

Exclusion zones should be established through administrative controls to prohibit the activation of mobile and portable emitters in areas where safety-related I&C systems have been installed. An exclusion zone is defined as the minimum distance permitted between the point of installation and where portable emitters are allowed to be activated. The size of the exclusion zones should be site-specific and depend on the effective radiated power and antenna gain of the portable emitters. The size of exclusion zones should also depend on the allowable emission levels designated for the installation area. Additional guidance on exclusion zones is provided in NUREG/CR-6431.

Table 3 Specific Regulatory Positions for EMC Guidance.

Regulatory Position	EMC Issue	Standards	Comments
2	EMI/RFI limiting practices	IEEE Std 1050-1996	Full standard endorsed with one exception taken.
		IEEE Std 518-1982 IEEE Std 665-1995	Endorsed as referenced by IEEE Std 1050-1996.
3, 4, 5	EMI/RFI emissions and immunity testing	MIL-STD 461D MIL-STD 462D	Selected MIL-STD 461 test criteria endorsed along with MIL-STD 462 test methods.
		MIL-STD 461C MIL-STD 462	Alternative test suites.
			Operating envelopes are included in Reg. Pos. 4 and 5.
6	Surge withstand capability testing	IEEE Std C62.41-1991 IEEE Std C62.45-1992	Selected IEEE Std C62.41 surge test waveforms endorsed with IEEE Std C62.45 test methods.
			Withstand levels for nuclear power plants are included in Reg. Pos. 6.

Conclusions

The issuance of RG-1.180 and the EPRI TR-102323 SER by U.S. NRC has resulted in clear guidance on the practices necessary for a comprehensive EMC program. Both documents represent guidance that is acceptable to U.S. NRC. These practices are presently being applied to analog, digital, and hybrid (i.e., combined analog and digital electronics) safety-related I&C equipment. The concurrence within the nuclear industry is that approval cycles have been significantly reduced, EMC awareness has been heightened, and the number of EMC-related occurrences has been reduced.

Adherence to the guidance in RG-1.180 and the SER for safety-related I&C systems has contributed to the assurance that structures, systems, and components important to safety are compatible with the environmental conditions associated with nuclear power plants. Consensus standards were endorsed that cover design, installation, EMI/RFI, and SWC practices. Test methods have been provided that contribute to a well established, systematic approach for ensuring EMC. Operating envelopes that have been confirmed with actual measurement data in nuclear power plants have been recommended.

References

EPRI TR-102323, *Guidelines for Electromagnetic Interference Testing in Power Plants*, Electric Power Research Institute, April 1996.

Ewing, P.D., Korsah, K., *Technical Basis for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems*, NUREG/CR-5941, Oak Ridge National Laboratory, April 1994.

Ewing, P.D., Wood, R.T., *Recommended Electromagnetic Operating Envelopes for Safety-Related I&C Systems in Nuclear Power Plants*, NUREG/CR-6431, Oak Ridge National Laboratory, January 2000.

IEC 801, *Part 4, Fast Electrical Transient/Burst Requirements*, International Electrotechnical Commission, Technical Committee No. 65, 1988.

IEC 801, *Part 5, Surge Immunity Requirements*, International Electrotechnical Commission, Technical Committee No. 65, 1990.

IEC 61000-4-4, *Part 4, Electrical Fast Transient/Burst Immunity Test*, International Electrotechnical Commission, 1995.

IEC 61000-4-5, *Part 5, Surge Immunity Test*, International Electrotechnical Commission, 1995.

IEEE Std 473-1985 (Reaff 1991), *IEEE Recommended Practice for an Electromagnetic Site Survey (10 kHz to 10 Ghz)*, Institute of Electrical and Electronics Engineers.

IEEE Std 518-1982 (Reaff 1990), *IEEE Guide for the Installation of Electrical Equipment to Minimize Noise Inputs to Controllers from External Sources*, Institute of Electrical and Electronics Engineers.

IEEE Std 665-1995, *IEEE Guide for Generating Station Grounding*, Institute of Electrical and Electronics Engineers.

IEEE Std 1050-1996, *IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations*, Institute of Electrical and Electronics Engineers.

IEEE Std C62.41-1991 (Reaff 1995), *IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits*, Institute of Electrical and Electronics Engineers.

IEEE Std C62.45-1992, *IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits*, Institute of Electrical and Electronics Engineers.

Kercel, S.W., Moore, M.R., *Survey of Ambient Electromagnetic and Radio-Frequency Interference Levels in Nuclear Power Plants*, NUREG/CR-6436, Oak Ridge National Laboratory, November 1996.

MIL-STD 461C, *Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference*, U.S. Department of Defense, August 4, 1986.

MIL-STD 461D, *Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference*, U.S. Department of Defense, January 11, 1993.

MIL-STD 462, *Measurement of Electromagnetic Interference Characteristics*, U.S. Department of Defense, July 31, 1967.

MIL-STD 462D, *Measurement of Electromagnetic Interference Characteristics*, U.S. Department of Defense, January 11, 1993.

Regulatory Guide 1.180, *Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems*, U.S. Nuclear Regulatory Commission, January 2000.

Pre-Qualification of Digital Platform - U.S. N RC Regulatory Review of The Common Q Platform

Keith Mortensen
Matthew Chiramal
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington DC 20555
E-mail address: WKM@NRC.GOV, MXC@NRC.GOV

ABSTRACT

CE Nuclear Power (CENP)(formerly ABB Nuclear Automation, presently Westinghouse Nuclear Automation) submitted Topical Report CEN PD-396-P, Rev.1,"Common Qualified Platform" to the NRC for review. The intent of the submittal is to obtain NRC acceptance of the pre-qualification of the CENP Common Q platform. The Common Q platform is a computer system consisting of a set of commercial-grade hardware and previously developed software components dedicated and qualified for use in nuclear power plants. The Common Q platform was developed by CENP from the standard AC 160 computer system developed by ABB Automation Products, GmbH (ABB Products) of Europe. The Common Q platform is to be loaded with plant-specific application software to implement various nuclear plant safety system applications.

The basis of pre-qualification is compliance with the NRC-approved EPRI Topical report TR-106439, "Guideline o n Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications." [A copy of this document may be obtained from the NRC Public Document Room http://www.nrc.gov/NRC/PDR/pdr1.htm]. The pre-qualified Common Q would provide utilities and other users with a pre-qualified platform that could be used in future applications for upgrade or replacement of plant safety instrumentation and control (I&C) systems. The purpose of the NRC review is to determine whether the design and proposed use of equipment and other technical requirements provide reasonable assurance that the applicant or licensee will comply with the applicable regulatory requirements, and that public health and safety will be protected. The review, audit, and inspection n activities by the NRC staff are not intended to completely evaluate all aspects of the design and implementation of the digital I&C system. The review scope is sufficient to allow the reviewer to reach the conclusion of reasonable assurance described above.

To ensure that the CENP Common Q platform will perform its safety function as designed, the NRC staff reviewed the basic operation of the system, life cycle process and documentation associated with the Common Q hardware and software design implementation, the commercial grade dedication reports for the components and previously-developed software (PDS) for the ABB AC160 PLC modules and for the flat-panel display system (FPDS) and other non-AC100 support components, the programming specifications for the future development of application software, and generic design information far the systems described in the four appendices to the topical report. These activities involved the review of design implementation documentation, technical meetings with the vendor; and audits at the vendor's facilities.

The NRC staff used the guidance in NUREG 0800, the Standard Review Plan (SRP), Chapter 7, Rev.4 [http://www.nrc.gov/NRC/NUREGS/SR08OO/CH7/index.htm], in conducting the review. Based on this guidance, the NRC staff identified additional information needed by the staff to perform the safety evaluation of the Common Q platform. The staff, in its review of the CENP qualification program, focused on how the safety requirements are met according to the guidance in SRP Chapter 7, including the supporting Branch Technical Positions (BTPs) and referenced US Regulatory Guides, and in EPRI Topical Report TR-106439. The staff has completed the review of the qualification of nearly all of the AC160 PLC system components and the staff's evaluation of the completed activities has been documented in the safety

evaluation report (SER) issued on August 11, 2000. CENP has remaining qualification testing of some AC160 PLC modules and all of the qualification testing for the non-AC160 components. This testing is scheduled for August2001. The SER and this paper reflects the status of the review as completed. The SER also identifies generic open items and plant-specific action items.

INTRODUCTION

In March 1999,CEN P submitted topical report CENPD-396-P, Rev. 00, "Common Qualified Platform" and the associated software program manual, "Software Program Manual for Common Q Systems" (SPM). Later in1999, the following four appendices to the topical report were submitted

Appendix 1, "Common Qualified Platform Post-Accident Monitoring System"
Appendix 2, "Common Qualified Platform Core Protection Calculator System"
Appendix 3, "Common Qualified Platform Digital Plant Protection System"
Appendix 4. "Common Qualified Platform Integrated Solution"

In June 2000, CENP submitted Revision 1 of both the proprietary and non-proprietary versions of the topical report and the associated software program manual and the four appendices that considered the comments provided by the NR C staff o n the initial set of documents.

Revision 1 describes a nuclear safety-related instrumentation and controls (I&C) platform developed by CENP. CENP is proposing one common platform with a modular structure in which various components can be incorporated and applied to nuclear safety-related applications, including component replacements and complete system upgrades. The appendices describe design approaches for implementing the generic platform into I&C systems at nuclear power plants and provide additional information to support the review of the generic design details for the Common Q platform.

SYSTEM DESCRIPTION

The Common Q platform developed by CENP consists primarily of a set of digital hardware and software components from the standard AC 160 system, a product developed by ABB Automation Products, GmbH (ABB Products), in Europe The standard AC160 is a system of PLC products currently used for control systems in industries unrelated to nuclear power. To complete the Common Q platform, CENP combines the FPDS and other components with its set of AC160 system components The FPDS consists of the flat-panel display module, a microprocessor-based single-board computer module, and communication interfaces for communication with the AC160 and other components and systems. The display module is a color thin-film transistor flat-panel display readable under high ambient light. The display module provides a graphic-al user interface (GUI) with pull-down menus and touch-screen capability. The FPDS is the human-system interface system (HSIS) for the associated nuclear plant system.

For nuclear power plant applications, this platform consisting of a let of commercial-grade hardware and previously developed software components.is being dedicated and qualified and is to be loaded with plant-specific application software to implement various nuclear plant safety system -applications.

The hardware components of the platform are:

- Advant Controller 160(AC160) with P M646 or PM645C processor modules
- S600 input and output (S6001/O) modules
- Bus communication interface (C1631) modules

- Power supply modules
- Watchdog timer module
- Communication systems
- Flat-panel display system(FP D S)

The AC 160 software, residing on flash programmable read-only memory (PROM) in the processor module, consists of a real-time operating system, task scheduler, diagnostic functions, communication interfaces, and plant specific application programs. The application program will be created using the Asea Brown Boveri (ABB) Master Programming Language (AMPL) Control Configuration (ACC) software development environment that includes a function block library for creating specific logic for the application. The Common Q platform uses three types of data communication systems: the AF100 (Advant Field bus 100) network communication system; the high-speed link (HSL) serial communication system; and external communication systems such as Ethernet. The AF100is used for transferring process data and messages within the channel (e.g., between AC160s and the FPDS). The process data are used for monitoring and controlling a process, and the messages are used for program loading and for diagnostic purposes. The HSL is used to transmit data to other channels in a multichannel system. Fiber-optic modems and cables maintain isolation of redundant safety channels. The external communication system is used to transfer calculate data from the Common Q system to the external systems, such as the plant non-safety control system. Previously-developed software (PDS) embodies the .software that was developed to satisfy a general market need before being incorporated into the Common Q platform. PDS includes commercial software that is integral to the delivered system and software that supports the delivered system. Some PDS is used to develop the application software to implement the safety functions in the Common Q upgrades. The PDS for the Common Q platform is procured from two vendors: the vendor of the AC160 PLC system and the vendor of the FPDS operating system.

The PDS being used in the Common Q are as follows:

Operating systems
Compilers, linkers, and loaders
Database software
Communication drivers
Human-machine interface software
Display-building software

Some of the PDS resides in Common Q memory when the Common Q is performing its safety functions (i.e., at runtime). Other PDS used as development or support tools does not reside in Common Q memory at run time. That which resides in memory at run time is subjected to higher regulatory requirements. The run-time P DS for the Common Q platform include the real time operating systems, task schedulers, diagnostic functions, and communication functions, all of which reside in the PLC’s PROM. The AC160 operating system provides for the deterministic behavior of the Common Q platform.

CENP's S PM specifies the procedures for implementing a structured software life cycle process for the plant-specific software and provides guidance for configuration management of commercial-grade hardware and PDS. Since the application software has not yet been developed, the staff's evaluation does not include the review of the outputs of the life cycle process, but is limited to the evaluation of the specified process. The same is true of the FP DS software. Licensees using the Common Q platform for plant-specific applications will be required to implement the application software in accordance with CENP's SPM. The application program and its control modules in a n AC160 will coexist in PROM with the other system software programs, such as the diagnostic routines and communication interfaces.

QUALIFICATION

In evaluating the Common Q platform, the staff made several site visits to the CENP offices and inspected CENP procedures that are referenced in the topical report and audited reports of commercial-grade dedication activities. During the site visits, the staff inspected CENP procedures that are referenced in the topical report and audited reports of commercial-grade dedication activities.

CENP provided copies of selected reports of commercial-grade dedication activities for more detailed review by the staff at NRC headquarters. Based on these activities the staff requested that additional documents dealing with commercial-grade dedication activities be placed on the docket. In June 2000, CENP submitted the following six proprietary reports:

"Seismic Qualification Test Report for Common Q Applications"
"Environmental Test Report for Module Equipment Qualification for Common Q Applications"
"EMI Qualification Test Report for Module Equipment Qualification for Common Q Applications"
"Commercial Grade Dedication Report for the QNX Operating System for Common Q Applications"
"Generic Operating History Evaluation Report on Previously-Developed Software in ABB AC160, U0 Modules and Tool Software"
"Design and Life Cycle Evaluation Report on Previously-Developed Software in A BB AC160.U0 Modules and Tool Software"

Based on its review of these documentation and interaction with CENP staff, the NRC staff identified items that needed additional activities and related documents to complete its review. CENP committed to provide the needed details. The safety evaluation by the NRC staff issued on August 16, 2001, discusses these open items: Common Q input/output modules to be re-designed to meet specified performance requirements; complete dedication of power supplies: complete design and dedication of watchdog timer; complete electro-magnetic compatibility and environmental qualification activities of some hardware items; provide additional information on software module testing, independence aspects of communication buses, and human-machine interface design details

Based on its review of CENP's dedication of the commercial-grade AC 160 PLC system and FPDS GUI, the staff concluded that CENP had demonstrated in accordance with the guidance in EPRITR-106439 that the Common Q platform is acceptable as equivalent to an item designed and manufactured under a 10 CFR Part 50, Appendix B, quality assurance program.
The staff reviewed CENPs SPM, which specifies the procedures for implementing a software life cycle process for the yet-to-be-developed application software and provides guidance for configuration

management of commercial-grade hardware and previously developed software, against the guidance in SRP Branch Technical Position-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems." Based on the review of the SPM and the topical report and appendices, the staff concluded that the specified procedures for software development and software configuration management will provide a quality software life cycle process, and that these plans commit to documentation of life cycle activities that will permit the staff or others to evaluate the quality of the design features upon which the safety determination will be based. The staff, therefore, concludes that the software development plan for new plant-specific safety system application software for the Common Q platform safety systems meets the guidance of US Regulatory Guide 1.152 (http://www.nrc.gov/NRC/RG/01/01-152rl.html], and that the special characteristics of computer systems have been adequately addressed.
The design applications discussed in the four appendices of the topical report are considered by the staff as models that can be used in designing the plant-specific applications.

PLANT-SPECIFIC APPLICATION

The staff has .reviewed the commercial-grade dedication of the Common Q platform and has determined that the Common Q platform has the required quality upon the satisfactory resolution of the outstanding open items. The quality of the plant-specific Common Q system is dependent on the licensee's proper implementation of the CENP software program manual and the resolution of plant-specific items. Because this topical report is for a generic platform, licensees referencing the topical report must describe in detail how they propose to use the Common Q design in plant-specific applications and must address all plant-specific interface item s. including the following plant-specific action items:

assess and verify the compatibility of Common Q, I/O modules to plant l/O requirements HSIS review and implementation
verification of environmental qualification compatibility of generic Common Q to actual plant conditions
design implementation of plant-specific application software per the requirements of CENP's SPM
verification of plant-specific requirements of l&C systems such as accuracy and response times, functions, control of access to the system, failure modes analysis, and technical specification requirements.

CONCLUSION

CENP submitted the topical report to obtain NRC acceptance of the pre-qualification of the CENP Common Q platform. The Common Q platform is a computer system consisting of a set of commercial-grade hardware and previously developed software components dedicated and qualified for use in nuclear power plants. Based on the review of the topical report and other documents, and on the audits conducted and meetings with CENP, the NRC staff concludes that for the systems and component reviewed, the design of the Common Q platform meets the relevant NRC regulatory requirements and is acceptable for safety-related instrumentation and control (I&C) applications in nuclear power plants, subject to the satisfactory resolution of the generic and plant-specific open items.

Survey and Evaluation of Digital I&C Licensing Experiences

Swu Yih[1], Chin-Feng Fan[2] Chan-Fu Chuang[3]

[1] Institute of Nuclear Energy Research, PO Box 3-11, Lung Tang, Taiwan, ROC.
Tel: +3-4711400-6335, e-mail: syih@iner.gov.tw

[2] Dept. of Computer Science, Yuan-Ze University, Chung-Li, Taiwan, ROC
Tel:+3-4638800-360, e-mail: csfanc@saturn.yzu.edu.tw

[3] Nuclear Regulation Division, Atomic Energy Council, Taipei, Taiwan, ROC
Tel:+2-23634180-307, e-mail: chung@aec.gov.tw

Summary

Digital I&C licensing experiences showed significant performance variance among different cases, i.e., some were smooth and efficient while others were lengthy and problematic. In order to explain the causes of such variance and to develop more efficient licensing techniques, we conducted an in-depth survey and analysis of these licensing experiences. By viewing the licensing process as an evidence- confidence conversion process, a Licensing Performance Model has been developed and used as a framework to analyze the behavior characteristics of licensing activities. The model identified major factors and functions that dominate the performance of licensing process, among which the proficiency maturity and evidence profiles are the most critical factors that affect the licensing performance. During the evaluation step we were able to apply this model to explain why some previous licensing cases were successful and some were troublesome. This successful application shows the validity of the proposed model. Finally, we presented insights into the nature of licensing process gained form this study and recommended approaches for improving licensing performance .

Introduction and Motivations

This paper presents a survey and evaluation of efficiency-related issues of digital I&C licensing cases performed in the recent years. The process of digital I&C licensing in nuclear industry starts when the utility presents an I&C design and its associated quality evidence to the regulator; the regulator will then determine whether the presented I&C system meets mandatory safety requirements that prescribed in pre-issued regulations. Thus the scope of our concern covers both the applicant's preparation effort and the regulator's review effort. An inefficient licensing process may cause unnecessary delay of the commercial operation of nuclear plants. Due to the enormous investment of constructing a nuclear power plant, any delay implies huge social and economical loss. Therefore, in the nuclear industry, every stakeholder is working hard to pursue a smooth and efficient licensing process. The licensing practice in general is quite effective and smooth for most case; however, experiences showed that some digital I&C licensing cases were frustrating for each party involved. It is even not too exaggerated to claim that the licensing practice has hindered the progress of introducing digital I&C techniques to nuclear power plants. This makes the progress of I&C computerization process far behind that of the petrochemical industry, which does not have mandatory licensing requirements. Various efforts have been proposed to resolve this problem, such as developing better regulations, powerful license review tools, etc. We propose another approach to alleviating the I&C licensing problem by extracting useful lessons learned from previous experiences. The rationale is that since some licensing cases are successful and some are problematic, thus if we could conduct a comparative analysis of these cases, focusing on analyzing the reasons of their success and failure. Thus, we may identify the critical *efficiency shaping factors* affecting the licensing process efficiency, and then by managing these critical factors properly, we may be able to avoid repeating the same problems that were encountered by previous troublesome cases in the future.

Our strategy is to develop a licensing performance *evaluation framework* based on the information collected from previous digital I&C licensing experiences. This framework is then used to identify critical factors and their influence on licensing efficiency. The following part of this paper presents preliminary results of our study. Our paper consists of 5 sections, First, a brief survey of five digital I&C licensing cases will be presented. The survey focuses on licensing practice and the future trend is also revealed from these cases. We then describe an evaluation framework, which is used to investigate the cause-consequence relations among licensing efficiency shaping factors. The framework thus can be used to explain why some licensing case succeeded and others failed. Recommendations that may improve I&C licensing efficiency will then be presented, followed by conclusion and future work.

Survey of Digital I&C Licensing Experiences

Licensing process can be divided into two distinct sub-processes: evidence preparation process and evidence review process. The following discussion is presented in terms of these two categories.

Chooz B Nuclear Power Plant (Peyrouton,1993)

P20 was the major digital control system selected by EdF for its Chooz B nuclear power plant. It was designed by Cegelec Company, which is a major French I&C provider with abundant relevant I&C experiences. The system is a distributed microprocessor-based control system that resides on a redundant LAN network. A 32-bit Transputer (Guesnier,1989) is chosen as its primary microprocessor. Since Transputer is designed for parallel applications, this system basically is running as a parallel processing system.

This project was started in 1986. In 1990, the project was delayed for 2 years; it was finally given up by EdF because more delay (estimated 4-6 years) was expected. This failed project cost EdF 300 million Francs (MacLachlan, 1994a) and 4 years schedule delay (delay already made by P20 and delay by the new design). The major reason for the failure is that the software has become too complex to be verified effectively and confidently.

Contronic E is chosen by Edf to replace the failed P20 system (Appell,1992). The problem of software verification is alleviated because Contronic E has many years field experience in chemical and petrol plants. However, French regulatory agency still did not feel confident in this new design (MacLachlan,1994b), and all the safety issues were finally settled after a long negotiation between two sides.

Darlington Nuclear Power Plant (Craigen, 1994)

Darlington nuclear plant is a CANDU type nuclear power plant developed by AECL. CANDU is among the first nuclear plants to use computers to perform safety functions. The digital technique has evolved from Digital Comparators (PDCS) used in the CANDU 600 (early 1980s), to microprocessor based trip meter (Pickering Nuclear Generating Station), to the fully computerized shutdown system of Darlington SDS1 and SDS2. The latest design made improvements in increasing the functionality to support more comprehensive self testing, surveillance, diagnosis, and channeled displays to the operators.

In 1982, Ontario Hydro, with the concurrence of AECB, had decided to fully implement the decision-making logic of the shutdown system on computers. The development work began in early 1983. In early 1987, an AECB review uncovered discrepancies and raised doubts as to whether the software implemented

the requirements correctly. In mid 1987, AECB hired software safety expert Dr. David Parnas to help investigation and to recommend how to improve the software. Dr. Parnas identified the areas of concerns and proposed a formal mathematical inspection in Jan. 1989 to break the licensing impasse. The complete software requirements specifications have to be rewritten to provide the required and correct format documents for inspection. This whole process completed in Feb. 1990 when AECB finally issued a license for full power operation.

When AECB issued the license on Feb. 1990, AECB also made a statement, requesting that the software would have to be *redesigned* for long-term use (Craigen ,1994). As a consequence, Ontario Hydro, AECL, and AECB are designing a new set of software engineering standards for guiding software development (AECL,1995). The development and regulatory status for the redesign activities is reported in (Chun,2000).

Sizewell B Nuclear Power Plant (NEI,1993)

Sizewell B plant adopts a two level strategy to its reactor system, i.e., a digital primary protection system backed up with a conventional secondary protection system. PPS consists of four Eagle series redundant channels as its backbone structure; each channel consists of the digital equipment performing data acquisition, signal conditioning and conversion, signal processing, trip demand processing, and Engineering Safety Features actuation. In normal operation, trip signals come from any two of four channels will trigger the protection system.

The PPS was developed by Westinghouse as one of its Eagle 21 series product. According to the statistics (NEI,1993) published by Nuclear Electric (Owner of Sizewell B), Westinghouse invested 200 man-years for developing PPS and 50 man-years for carrying out independent verification and validation (IV&V) to assure that PPS met all related quality standards and requirements. However, due to lack of objective software quality and safety metrics, NE spent another 250 man-years to perform a comprehensive and complicated verification and validation to improve its confidence in PPS (Marshall, 1993).

On October 21 1993, Computer Weekly, a U.K. based magazine, published a short editorial message (CW,1993) saying that it had obtained a confidential NII (British nuclear regulatory agency) report consists of questions raised by NII for the reliability issues of Sizewell B PPS. The magazine will make this confidential report available to anyone who is interested in the topic; the purpose is to providing a "well informed discussion" in the subject. In early 1993, British Computer Society, an prestigious academic organization, published an open letter expressed concerns over the safety performance of Sizewell B Primary Protection System and recommended several improvements (Marshall, 1993).

Kashiwazaki-Kariwa 6 / 7 Nuclear Power Plants (Fukumoto,1998)

Kashiwazaki-Kariwa Unit 6 and unit 7 (KK6/7) is the first commercial Advanced Boiling Water Reactor (ABWR) design nuclear power plant. The basic design was jointly developed by Hitachi, Toshiba and GE Nuclear Energy. The digital I&C development process followed Japan’s regulation (JEAG 4609-Guidelines for Application of Digital Computer to Safety Protection System) which in general are less complex than USNRC regulations. The I&C design was based on Problem Oriented Language (POL) which helped to make the final system reliable and verifiable. The system validation testing was performed with the help of a PC-based automatic testing tool. This tool could carry out pre-defined validation testing procedures and generated testing reports automatically. The use of automatic testing tool effectively reduced the time and manpower required for the validation test. The validation testing covered dynamic transient tests in which simulated design base transients were generated for testing the behavior of digital I&C system. A very important feature of KK6/7 I&C project is that manufacturers have accumulated more

than 15 years experience in handling the digital I&C components for non-safety operations. Such experience paves the foundation for the success of the project.

During licensing process the regulator authority-MITI, asked Nuclear Power Engineering Corporation to perform a comprehensive qualification testing. The testing was efficient and successful; thus, the permit was issued without lengthy negotiation as that happened in most cases in the western countries. Due to its success in licensing process, KK6/7 has become a performance benchmark for other digital I&C licensing projects.

Load Sequencer of FP&L Turkey Point Plant (Kenndy,1994)

The Load Sequencer of unit 3,4 of Turkey Point Nuclear Power Plant was upgraded to digital design in late eighties. FP&L submitted application documents to USNRC for approval in June 1988. All review open items were finally closed and an approval was issued on Feb. 1992. The complete licensing process took 3 year and 8 months. During a NRC sponsored digital I&C technical workshop held in 1994, Mr. Larry Kennedy of FP&L reported this project and expressed complaints about the lengthy licensing process (Kenndy,1994).

Case Summary

Generally speaking, the above cases show that some digital I&C licensing cases suffered from high evidence preparation cost (P20, Darlington, Sizewell B), but still faced doubts about their potential safety performance (Darlington, Sizewell B); thus, these cases demonstrated poor licensing efficiency. On the other hand, KK6/7 showed quite good licensing efficiency. The remarkable point is that the result of licensing is not proportional to the invested effort. For example, KK6/7 spent relatively less quality-related effort than Sizewell B, Chooz B and Darlington, but still gained satisfactory review results from regulators. Such obvious performance difference implies the existence of techniques that can improve efficiency of current licensing practice. In the next section we will investigate what the critical efficiency shaping factors are and pursue methods that can manage these factors effectively.

Development of Evaluation Framework for Digital I&C Licensing Process

This section is to develop an evaluation framework that can investigate the underlying factors affecting the performance of licensing process.. First two subsections explain how to develop such a framework, followed by applying this framework to diagnose previous licensing experiences and propose solutions.

The Nature of Licensing Process

The purpose of licensing, according to Chapter 7 Standard Review Plan (SRP) (NRC,1997), is to "*determine whether the equipment, …process to be performed provide reasonable assurance that the licensee will comply with the regulations and public health and safety protected.*" The key word here is "*reasonable*" which apparently is quite subjective in nature, i.e., different regulators may have different acceptance standard about the quantity and quality of evidence that are considered to be "*reasonable"*. In another paragraph, SRP states that the reviewer need not to "*completely evaluate all aspects*" of the submitted documents. "*The review scope needs only to be sufficient to allow the reviewer to reach conclusion*." Here the word "*sufficient"* is also a subjective criterion. Based on these statements we can identify the mechanism of licensing process is to let the regulator to buildup a feeling of *assurance* or *confidence* based on submitted evidence. Therefore, the most important concepts in licensing process are: *sufficient evidence and assurance*. According to Webster Dictionary, assurance means: (1) something on which one can rely as a guarantee of truth. (2) Self-confidence. Now let's compare the difference before and after licensing process. Before the license process starts, it is reasonable to assume that the applicant should already have *reasonable assurance* in his mind that his design fully complies with regulations. Then after a successful licensing review process, a permit will be issued if and only if the regulator *also*

has reasonable assurance that the submitted design will comply with regulations. Therefore, the difference before and after licensing process is that, superficially, the evidence is presented to the regulator and accepted by the regulator; pragmatically, a state of *confidence* is built up in the regulator's mind based on the evidence. In other words, the major mechanism during licensing process is the conversion of the submitted evidence into the regulator's confidence. Thus, we may consider the essence of licensing process as an *evidence-confidence conversion* process.

There are many factors that can affect the efficiency of this evidence-confidence conversion process, Proper handling of these factors results in an efficient licensing process. The following sections will identify these factors and analyze their contributions to the efficiency of licensing process.

Licensing Process Evaluation Framework: An Evidence-Confidence Conversion Process

Figure 2 shows a schematic view of a licensing process based on evidence-confidence conversion perspective. The complete licensing process covers evidence preparation process and evidence-confidence conversion process.

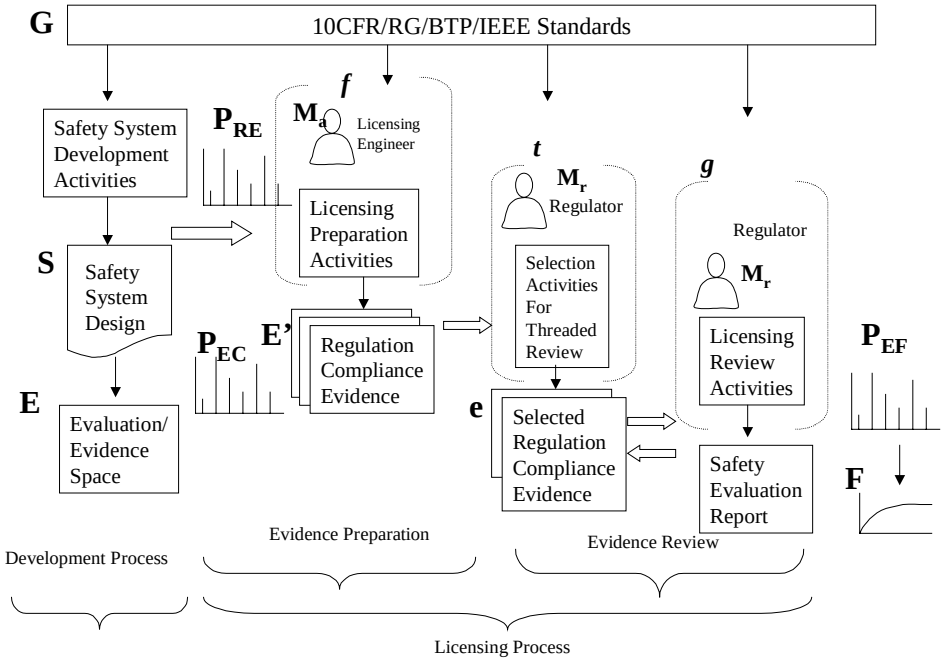


Figure 1: Licensing process model viewed as evidence-confidence conversion process

The licensing process can be defined as 9 tuples with 6 sets and 3 functions. Licensing Process $= (\mathbf{G}, \mathbf{S}, \mathbf{R}, \mathbf{E}, \mathbf{P}, \mathbf{M}, f, g, t)$

$f : \mathbf{G} \times \mathbf{S} \times \mathbf{M_A} \times \mathbf{P}_{\mathrm{RE}} \times \mathbf{P}_{\mathrm{EC}} \rightarrow \mathbf{E'}_{\mathrm{A}}$ .....Evidence preparation function

$t : (\mathbf{G} | \mathbf{S} | \mathbf{E}) \times \mathbf{M_R} \rightarrow (\mathbf{G'} | \mathbf{S'} | \mathbf{e'})$.....Thread auditing(selecting and slicing) function

$g : \mathbf{G'} \times \mathbf{S'} \times \mathbf{e'_A} \times \mathbf{P}_{\mathrm{EF}} \times \mathbf{M_R} \rightarrow \mathbf{F}_R$..... Confidence conversion fucntion

Definition of each term is explained as following:

G-Government regulations: As shown in Figure 1, they are 10CFR codes, regulatory guides, branch technical positions, technical reports, industry standards, etc.

S- I&C System design: complete I&C system design specification submitted by the applicant for licensing review.

R –Resource allocated for evidence processing effort. $\mathbf{R}_p$ represents evidence preparation effort, $\mathbf{R}_p$ represents evidence review effort.

E- Evidence space, **G** x **S** defines the state space needed to be evaluated, **E** is all the evidence needs to be generated for evaluating whether **S** complies with **G**. In reality, the applicant can only prepare a subset of **E**, i.e., **E'** and **E'** $\subseteq$**E** under a fixed **R**. The regulator can only select (thread auditing) a part of **E'**, i.e., **e**, **e**$\subseteq$**E'**, for review. Therefore, **e**$\subseteq$**E'** $\subseteq$**E.**

P- Various Profiles that shaping the performance of licensing activities.

$\mathbf{P}_{EF}$**-** Evidence-conFidence Profile: There are many different kinds of evidence and evidence owns different confidence conversion power, i.e., some evidence is more convincing than others.

$\mathbf{P}_{EC}$-Evidence Cost profile. The preparation cost for different evidence is not equal. $\mathbf{P}_{EC}$ represents the cost variance when one prepares different evidence.

$\mathbf{P}_{RE}$- Resource Evidence allocation profile. It represents how the total evidence preparation resource **R** is allocated for preparing different evidence.

M - Proficiency maturity level: it represents the degree of proficiency of staff members performing licensing activities. The proficiency can be roughly divided into three levels: novice, competent and expert. The level will affect the quality of evidence and resource consumption. $\mathbf{M}_A$ represents the applicant's and $\mathbf{M}_R$ represents the regulator's proficiency level respectively.

F – Confidence level achieved after reviewing evidence **e** during licensing process.

This model provides a framework such that further investigations can be conducted by analyzing relations among model components.

Conditions for Optimal Licensing Performance: Aligned Profiles

From the model we can define the optimal licensing performance as that achieving the maximal confidence under a fixed licensing resource. A qualitative discussion on the conditions that lead to the optimal licensing performance is given below.

1. Assume the total amount of resource for evidence preparation is **R**
2. Assume the resource allocation scheme is defined as resource allocation profile $\mathbf{P}_{RE}$ **;** then resource devoted to preparing each kind of evidence is determined.
3. The amount of evidence produced under such resource allocation scheme is decided by referring to evidence cost profile $\mathbf{P}_{EC.}$
4. When the evidence submitted to the regulator for review, the regulator's confidence will be converted from the evidence by referring to evidence-confidence profile $\mathbf{P}_{EF}$**.**

The process is shown in Figure 2. The confidence conversion process showed that conditions that lead to the optimal licensing performance are closely related to the alignment relation among three evidence profiles, i.e., $\mathbf{P}_{RA}$,$\mathbf{P}_{EC}$ and $\mathbf{P}_{EF}$**.** The exact optimal condition can be derived by mathematical techniques if the mathematical definition of each profile is known. Intuitively speaking, the more the confidence return generated by evidence, the more resources should be devoted to that evidence. Thus we may conclude that the key to an optimal licensing efficiency is the proper alignment of resource evidence profiles, Evidence-Cost Profile and Evidence-Confidence Profile. Figure 2a shows a good alignment case and Figure 2b shows a poor alignment case.

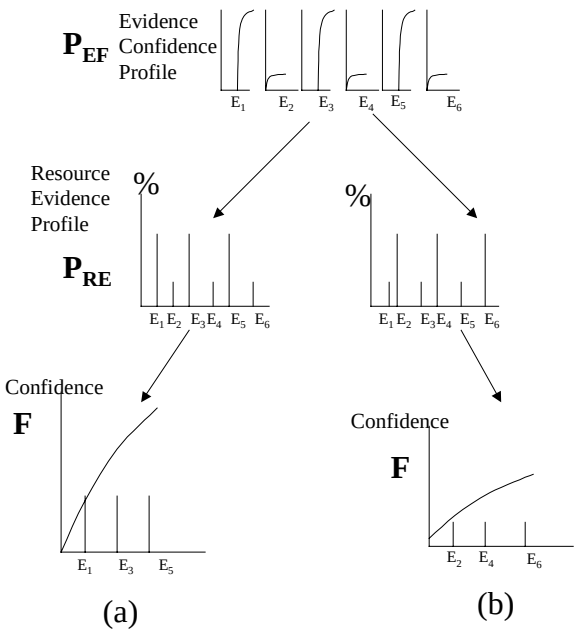


Figure 2: Licensing performance comparison for different profile alignment

Application of Licensing Process Model

The developed licensing process model represents a simplified model, but it captures essential features of real licensing practices. The advantage of having a model is that we can perform logical analysis and correlate results with real cases. Thus we can apply this model to explain previous licensing experiences and obtain insights into the characteristics of licensing process.

Diagnosis of Previous Digital I&C Licensing Cases

In this section we apply the developed model to explain those digital I&C experiences reported above. The result is also shown in Figure3.

Sizewell B: The major problem stems from the misalignment of three evidence profiles. The extra IV&V performed by EU did not contribute commensurate confidence return due to the fact that Westinghouse had already performed an effective internal V&V. The evidence-confidence return for EU IV&V effort became very low due to the saturation effect. The evidence preparation is an overkill activity due to the overlooking of the diminishing return effect of the evidence-confidence profile.

Chooz B: Chooz B's I&C project overlooked the severity of evaluation space explosion problem. The chose of Transputers as its computing platform resulted in a prohibitive workload for V&V task, i.e., the evaluation space is too huge to be evaluated. Unable to conduct complete V&V was the official statement for explaining why P20 project failed.

Darlington: Darlington Digital Shutdown System Project's problem came from the mismatch between the applicant's and the regulator's evidence-confidence profiles. Regulatory authorities adopt Dr. Parnas' position, which considered more rigid analysis as necessary evidence. The utility had to re-submit formal analysis information for review thus delayed the licensing process.

KK6/KK7: The major reason for KK6/7's success lies in the fact that KK6/KK7 I&C project adopted well-developed design that vendors have accumulated more than 10 years' experience. The cost for preparing evidence was low and knowledge was abundant and shared among stakeholders. Thus all evidence profiles were well aligned, and this resulted in an effective licensing process.

Load Sequencer/Turkey Point:

This project was performed in late eighties when both the utility and regulators were lacking of enough digital I&C experience. At beginning the evidence-confidence return was very low as showed in Figure 3. It took time for the regulator to establish a working evidence-confidence profile to support the reach of final conclusion.

Figure 3 shows the profile alignment situations for each case discussed above.

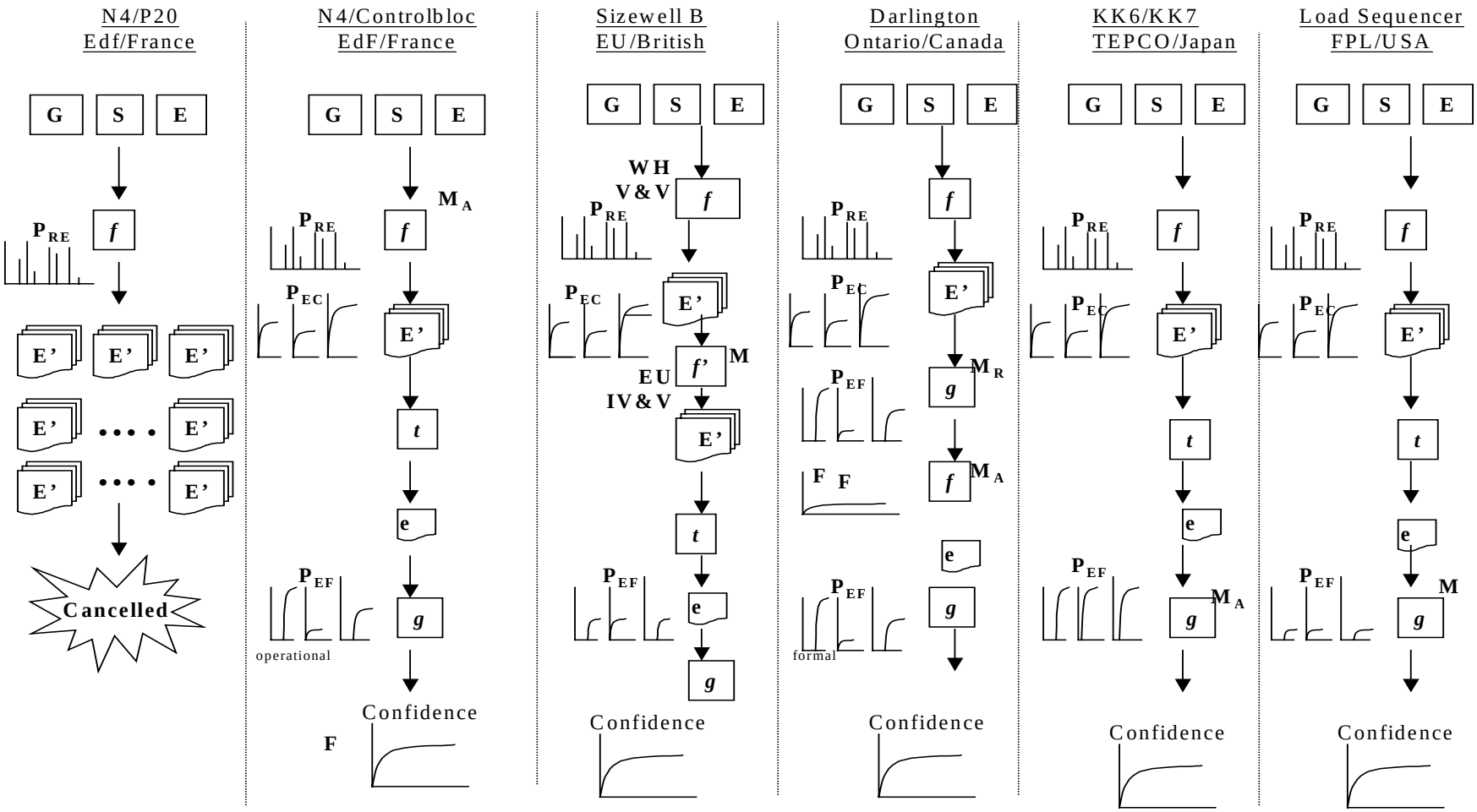


Figure 3: Diagnosis of Digital I&C Licensing Experiences

Insight Gained From Evaluation of Licensing Process Model

After applying the proposed licensing performance framework to evaluate the previous licensing experiences, we can obtain lessons learned and thus improve our understanding about the nature and limitations of licensing process.

- *Concept of Evaluation Space and Its Implications*

  Evaluation space is defined by regulations and system design, i.e., $G \times S$. This represents the scope to be worked with during licensing process. The larger and complex of the evaluation space, the more difficult the licensing will be. This feature implies that we shall choose simplified digital devices for safety systems in order to have a small and manageable evaluation space. This explains why PLC-based design is more popular than microprocessor-based design in digital I&C safety applications; a PLC-based design is much simpler than a microprocessor-based design for a same functionality. This observation coincides with Dr. Lawrence's recent research finding that promotes the use of "simple, but practical, computer-based instrumentation components for safety application." (Lawrence,2000)

- *Diminishing Return Behavior of Evidence Cost profile*:

  The evidence-confidence profile in general has a diminishing return characteristic. At beginning, the confidence level can increases as more evidence is collected. But the tendency of increment will saturate, i.e., up to a certain point, the confidence level gained will diminish even more evidence is collected. Thus, beyond the saturation point, invested resource will be wasted as what happened in Sizewell B PPS IV&V project. This feature can also be used as an argument for reducing some controversial regulations, such as independent requirements for V&V and safety analysis (NRC ,1997), as well as overwhelming documentation requirements, etc.

- *The Impacts of Human Factors in Licensing Process*

  This influence of human factors can be observed by examining the proposed model. For functions *f,g,t,* each process involves the proficiency maturity factor which is highly people-dependent and also can be highly subjective. Therefore, the performance of software licensing process is heavily affected by people's capability. This is quite different with hardware-oriented equipment licensing process. The ultimate goal of managing human factor for a licensing process is to maintain well consensus among all stakeholders. In a broader sense, consensus represents not only having similar interpretation of regulations but also having the same perception of evidence-confidence profiles. Without consensus the licensing process can be difficult and frustrating, as that happened in Sizewell B or Darlington projects. On the other hand, when all people reach consensus, then the licensing process can be smooth and efficient as that happened in KK6/7 project.

- *The Essence of Managing Licensing Process: Resource Management Under Uncertain Environment*

  The key words appeared in SRP include such as: *reasonable assurance* and *sufficient*. All of these key words heavily depend on personal judgment. The subjectivity invokes certain degree of flexibility and unpredictability for the performance of licensing process. In the model we represent such subjectivity judgment in form of evidence-confidence profile and evidence-cost profile and maturity proficiency. Figure 3 shows the typical distribution of these profiles. However, in reality, there is significant uncertainty associated with these profiles. The uncertainty comes from both stochastic nature (aleatory uncertainty) and lack of complete knowledge (epistemic uncertainty) about the behavior of evidence–confidence relation. Without accurate evidence-confidence and evidence-cost information, the managing of licensing process becomes a resource management process under highly uncertain environment.

- *Principle of Effective Digital I&C Licensing Process: Continuous Risk Management (CRM)*

  Experiences point out that within evidence-confidence conversion model two dominant performance influence factors are proficiency maturity and evidence-confidence profile. The inherent uncertainty associated with these factors makes any attempt for efficient licensing resource management very difficult. It is because our traditional regulation philosophy is founded on a deterministic environment such that safety can be assured by prescribing what the applicant must comply with. In other words, conventional compliance-based regulation is based on the assumption that the behavior of those activities or equipments under regulation is deterministic and predictable; confidence thus can be established thereafter. For digital I&C equipment, along with its related software development activities, the performance is neither stable nor predictable for most of the time. Thus, compliance-based regulation approach often results in resource waste due to the inaccurate estimation of the evidence-confidence profile and the evidence-cost profile. In principle, such an inherent uncertainty problem can be alleviated by Continuous Risk Management (CRM) technique. An accurate evidence profiles assessment is still difficult. However, the mismatched gap between various evidence profiles can be narrowed by continuously assessing and mitigating risk as the project goes on. Risk Informed Performance Based (RIPB) approach, recently promoted by USNRC, emphasizes the consideration of risk contribution of regulated equipment or activities in the decision-making process. RIPB practice can be viewed as a CRM technique. Thus, we consider RIPB practice a promising candidate for solving digital I&C licensing problems and worth further studying.

Conclusion and Future Work

In this paper we reported the preliminary result of our survey and evaluation of major digital I&C licensing experiences accumulated in the recent years. The motivation is that we noticed the performance variance among different digital I&C licensing cases, i.e., some were smooth and efficient while others were lengthy and problematic. In order to explain the causes of such variance and to develop techniques for improving the effectiveness of licensing process, we conducted an in-depth survey and analysis of these experiences. By viewing the licensing process as a confidence conversion process, a Licensing Performance Model is developed and used as a framework to analyze the behavior characteristics of licensing activities. The model identified major factors and functions that dominate the performance of licensing process, among which the proficiency maturity and evidence profiles are the most critical factors affecting the licensing process. During the evaluation step we were able to apply this model to explain why some licensing cases are successful and some are troublesome. This successful application shows the validity of the proposed model. Finally, we presented several insights into the nature of licensing process.

Our evaluation identified that inherent uncertainty associated with the various profiles dominates and limits the potential performance of licensing process. Based on our study we consider that Continuous Risk Management technique should be applied to cope with such uncertainty. Risk Informed Performance Based Regulation (RIPBR) currently promoted by US nuclear industry basically fits the definition of Continuous Risk Management technique. USNRC has issued relevant regulatory guidance for RIPBR and some of which could be applied to digital I&C licensing process. We believe that the development of a comprehensive RIPBR approach to digital I&C licensing process worth further in-depth studying.

References

(AECL,1995) Standard for Software Engineering of Safety Critical Software, (Electrical and Controls Engineering Department Standard), 982-C-H-69002-0001 Rev R0.

(Appell,1992) Appell, B., "Putting in a Replacement for Controbloc P20 at Chooz B," *Nuclear Engineering International*, July 1992, pp.45-48

(Chun,2000) Regulatory Assessment of the Darlington Shutdown System Trip Computer Software Redesign, C. Chun, L. Staples, A. J. Faya, NPIC&HMIT 2000, Washington DC, Nov. 2000.

(CW,1993) Editorial Message, *Computer Weekly*, October 21, 1993, UK.

(Fukumoto,1998) Fukumoto,A, et al**,** A verification and validation method and its application to digital safety systems in ABWR nuclear power plants, *Nuclear Engineering and Design*, V183N2, pp.117-132, July 1998.

(Craigen ,1994) Craigen, D., Gerhart, S. and T. Ralston, "Case Study: Darlington Nuclear Generating Station," *IEEE Software*, Jan. 1994, pp30-32.

(Guesnier,1989) Guesnier, G., Anglaret, M., Colling, J.M., and Raimondo, "C&I Systems for France's N4 NPPs", *Nuclear Europe*, Sept.-Oct., 1989, pp.17-18

(Hughes,1993) Hughes, G. and Boettcher, D.B., "Developments in Digital Instrumentation for Nuclear Electric's(UK) Power Plant", *Nuclear Energy*, Vol. 32, No.1, Feb. 1993, pp.41-52

(Lawrence,2000) Lawrence, J.D., "Software Qualification in Safety Applications," *Reliability Engineering and System Safety*, 70(2000)167-184.

(Kenndy,1994) Paper presented in Proceedings of Digital System Reliability and Nuclear Safety Workshop, Sept. 13-14, 1993, Rockville, Maryland, USA.

(MacLachlan,1994a) MacLachlan, A., "I&C Woes Behind It, EDF on Target for Startup of First N4 Reactor", *Nucleonics Week*, July 14, 1994, pp.3-4.

(MacLachlan,1994b) MacLachlan, A., "French Regulators 'Lost Hope' of Proving Chooz-B Digital I&C System," *Inside NRC*, May 30, 1994. pp.6-7.

(Marshall, 1993) Marshall,P and R. Silver, "Sizewell B Computer Controversy Looms Over Fuel Load Schedule," *Nucleonics Week*, Vol.34, No.42, Oct.21, 1993

(NEI,1993) "Sizewell B Reactor Protection Reliability: Nuclear Electric Presents its Case," *Nuclear Engineering International*, Mar. 1993, pp.28-33.

(NRC,1997) NUREG 0800, Chapter 7, Standard Review Plan, USNRC, Washington, DC.

(Peyrouton,1993) Peyrouton, M. and M. Pirus, "Progress on N4 I&C Architecture," *Proceedings of Topical Meeting on Nuclear Plant Instrumentation, Control and Man-machine Interface Technologies*, Apr. 18-21, 1993, Oak Tenn., pp.305-311.

Collecting Data from Operational Experience of Computer-Based I&C Systems - A Regulatory Perspective on Goals and Tasks

G. Schnürer[1], F. Seidel[2]

[1] Institute of Safety Technology (ISTec), Garching
Tel.: +49 89 32004-523, Fax: +49 89 3200-300, e-mail: sgu@grs.de

[2] Federal Office for Radiation Protection (BfS), Salzgitter
Tel.: +49 5341 885-863, Fax: +49 5341 885-865, e-mail: Fseidel@bfs.de

Abstract

Provided that the considered computer-based I&C systems are developed, qualified and maintained using an unique platform, the data from operational experience of the system's application at nuclear power plants can be collected under unified aspects. The main goal of the data collection is to contribute to the further qualification of these systems.

The following goals are of particular interest from the regulatory perspective:

- Evaluation and optimization of the qualification procedure,
- Demonstration of the achieved systems' dependability as well as
- Utilizing the experience of the system applications of lower safety significance within the licensing procedure for computer-based systems critical to safety

The content of the records and the evaluation methods for operational experience have to be identified carefully. As a good practice, the involved experts of the participants in this business, i.e., the licensees, manufacturers, technical support organizations and regulatory bodies should agree upon this identification. It should be noted, that not only the failures and the reported events are of interest, but also periods of operation without significant failures. Those should be considered as well in the frame of safety evaluation and qualification.

As a long-term goal of the collection of operational experience, the achieved performance of the system might be estimated in quantitative terms. To calculate the reliability, it is crucial to establish an evaluation model in order to identify the necessary parameters as early as possible and to collect them continuously during the operation.

Introduction

The safety-related application of software-based I&C systems is increasing also at nuclear power plants. Consequently there has been also a growing debate over the issues what data can be derived from test and operational experience.

The source of the uncertainty in software dependability is not of probabilistic nature. Rather, software failures may follow an erroneous data input or because of an inadequate requirements specification. Thus, software failures may occur in applications (distinct demand) or under environmental circumstances for which the system was not or not correctly designed; therefore in [1] the term "error-forcing context" is introduced. Because the input data configuration space as well as the configuration space of possible environmental data are very complex for real I&C systems the software behavior can not be tested completely. As an example, just consider the non-linear interaction between the hardware/software modules of a distributed I&C system during a real time application. Due to this quasi-probabilistic software failure behavior, probabilistic methods like fault and event tree analysis are applicable for quantitative reliability assessment.

Systematic approaches for quantitative software reliability assessment are still under investigation. Complementary, deterministic expressions about the software reliability can be derived from the software qualification procedure, particularly if the software and hardware of the I&C system are developed on a unique platform over the whole life cycle.

With this contribution the authors like to repeat and rearrange the facts on operational experience of computer-based I&C from the regulatory and expert's perspectives. They would like to stimulate the further collection of operational experience, particularly for software-based I&C developed on a unique platform. Especially, the principles and high-level requirements implied for platform development and qualification can be utilized to assess the operational experience.

Classification

Faults and failures

Because the possible design faults and erroneous input data will influence the software functionality in different manner, it is necessary to distinguish types of failures and faults, e.g. related to safety or reliability. The distinction between different types of software failures and faults should be consequently considered during the collection of operational experience by assessing the impact of the distinct occurrences on safety and reliability. For instance, a fault tolerant system operating in a cyclic deterministic mode will tolerate any erroneous input signal. On the other hand the system will react fail-safe if the erroneous input signal will get consolidated over some system cycles. Thus, this case is characterized by the transition from normal to abnormal but safe operation mode. Unlike, a system without fail-safe capabilities will react accidentally. Within the collection of operational experience both cases should be clearly distinguished from each other. Generally, faults and failures should be assessed and valued according to the importance to safety.

Collecting operational experience, following kinds of faults and failures should be considered:

- Hidden fault versus detected fault
- Systematic failure of the whole system versus systematic failure of only one subsystem
- Non-detected (passive) failure versus self-detected (active) failure
- System failure without fail-safe reaction versus failure after which the system is automatically transferred into a safe operating mode
- Input data error which will disturb the system's operation versus the case that the same input error is ignored or corrected by the system; i.e. the system's operating mode is robust against input errors
- Dependent versus independent failures

For instance, according to this scheme the following hypothetical scenario may have the deepest impact on safety:

- The software contains hidden faults.
- On a certain demand (by special combination of input data, or by a signal value outside the specification) a hidden fault will become active and will lead to a systematic failure of the safety I&C system.
- The I&C system will not react fail-safe, i.e. the I&C system is left in an accidental state or a plant safety system function will get activated to transfer the plant to a non-tolerable state.

Software types

Within the collection of operational experience software types should be distinguished, e.g. in the following manner:

- Application software: Non-application specific functional blocks or modules as well as function block diagrams, in which the modules are coupled to each other according to the application specific designed. The functional block diagrams may be developed on an unique platform
- Operational software: Like software for CPU operation, I/O actions, signal transmissions, exception handling, etc. Mostly this software can be treated only as black boxes. A re-qualification is useful to limit the functionality to the necessary extent.
- COTS (commercial off the shelf software): Pre-developed software, mostly developed on a platform different from the platform for the development of the application software. Normally the above mentioned operational software originally consists of COTS. Depending on the safety significance, COTS should be re-qualified to a certain extent. The assessment of operational experience – here in different application – might be helpful.
- Tool software: E.g. software used for the specification and coding of application software. This software should be qualified according to the safety significance of the target software. Particularly the software tools used for platform development and qualification are belonging to this category, in this application the software tools or distinct versions of the software are used during the whole life cycle, i.e. for specification, design, qualification (simulator and test software) and maintenance.

Collecting data of operational experience/ Goals of data collection

The most common objectives of the collection of operational experience for software-based systems are the in-depth analysis and assessment of new types of faults and failures including the recommendation of corrective actions as well as the derivation of learned lessons. Moreover to the authors understanding, the following aspects might be considered in more detail:

Demonstration that the applied I&C system meets the design principles (deterministic approach, root cause analysis)

After collection of operational experience over a certain period of time, the question should be answered from a deterministic point of view, whether the system has met the design principles and the top-level system requirements. The main design principles are e.g. deterministic cyclic behavior, functional independence of redundant system parts, diversity, fail-safe behavior, and robustness against environmental exposures. Top-level system requirements are established e.g. on the response time, signal and data flow.

As a basis for this assessment the findings of self-tests and periodical maintenance as well as all experiences where the system gave an abnormal response should be taken into account. For each of this case a certain list of design principles and system requirements should be analyzed item by item, whether this item is touched by the respective abnormal finding or not. Concerning top-level system requirements the above mentioned list might be established from the system requirements specification. The design principles can be taken from associated guidelines; e.g. [2]. In the frame of a BMU/BfS research project such principles are listed up specifically to a German I&C system [3].

This kind of systematic approach to the assessment of operational experience can be helpful to examine the I&C system requirement specification as a possible source of faults - implying also the potential to common cause failures. It will contribute to establish root cause analysis procedures to cover the high-level requirement specification.

Test coverage assessment

For concrete I&C systems a fully test coverage is practically not achievable. Nevertheless the designer and the V&V team are faced with the problem of performing and optimizing an appropriate test profile to meet the associated requirements of guidelines and standards. Therefore, it should be demonstrated that the chosen test file is appropriate or - if this cannot be achieved - this test file is to optimize. For this task the collection of operational experience can be very helpful, if the records of the I&C activities are available, unlike they are resulting in a system failure, in an abnormal system reaction or in the correct activation of the specified function. An operational profile can be derived and later compared to the test profile to demonstrate whether the profile was appropriately chosen for the qualification.

For further discussion we found two related main questions concerning the treatment of operational experience:

- Treatment for a high amount of data

The record of all occurred I&C activities may imply a great expense in the later assessment of the collected information. An appropriate record structure and schedule for condensing the recorded data might be helpful to reduce the effort. In this matter we would like to pick up proper recommendations and, if already available, the experience of the audience. The question can also be expressed as " What effort is appropriate to gain more detailed information to optimize the test strategy for further system application?" – always assuming, that the system is developed and qualified on the same platform.

- Treatment, if the data base is too low

This case concerns that during operation the number of I&C activities is too low to gain evidence for the test coverage. This case will particularly occur if the I&C system performs functions of high importance to safety with the result that the system function is very seldom activated, assuming that an appropriate defense in depth concept is applied in the I&C design. Even this case is the most interesting case from the safety point of view. Covering this, in Germany the following solution is applied:

Selected systems to perform safety-related functions like reactor power limitation and control were developed and qualified on the same platform as for safety-critical systems. That means, in comparison to safety-critical systems the same qualification requirements were applied for the qualification of the safety-related hardware and software. These systems were extensively tested, particularly during on-site operation in parallel to the original hard-wired I&C system. Due to the off-line mode chosen for parallel operation of the software-based system, additionally special test sequences were performed without affecting the plant operation. This leads to additional test experiences. After commissioning these systems now the performance of real I&C functions like reactor power control is much more frequently than any function of higher safety significance.

Of course, the concern is remaining that the safety related control functions are generally not comparable with any safety-critical function. According to the design the considered I&C systems are operating in a deterministic cyclic manner. Thus the system's operating mode is independent from any input signal. That means, from the aspect of operational experience the final purpose of signal processing and voting has no importance; again, provided that the compared systems are developed and qualified according to the same basic design and on the same platform. Therefore, the resulting higher amount of operational experience with the I&C system for reactor control and limitation may result in the first above mentioned problem. Note that the provision of the deterministic cyclic system behavior should be approved as a main postulate for this kind of collection and interpretation of operational experience. Robustness tests with any given input signals can be helpful. Within the later assessment of the collected operational experiences it should be further examined whether this postulate is met by the system. For instance, a system or component failure triggered by an input signal, gives evidence that the system does not fulfil the postulate, at least not in any case of demand.

Quantitative system reliability assessment

There are different approaches to analyze the software-based system's reliability quantitatively. Methods successfully applied in reliability analysis for hardwired I&C systems like fault tree analysis, event tree analysis, Markov analysis and failure mode and effect analysis will be analyzed to a certain extend according to their applicability to software-based systems. This paper cannot show the

state of the art of quantitative reliability assessment in detail. Recent results can be summarized as following [4-7]:

- For complex I&C systems there is no general approach, often the combination of different methods applied for certain software modules (distinguishing e.g. application specific software and COTS) will yield best results [4]
- Often there is a lack of data to feed the reliability models. In a first step the data will get conservatively estimated to estimate the lower limit of the reliability. Further investigations will show, whether more precise data can be derived from operational experience

In the case that the correct function as well as findings of the system are recorded following results can be derived:

- The systems' or sub-system's availability can be obtained with more evidence; that means under consideration of the test intervals.
- The ratio of cases in which the system reacts either abnormal or as specified can be estimated with more evidence.
- If dependent failures are occurred, their nature can be analyzed in more detail, using all the test data recorded between and after their occurrences.

Taking these facts into account, we suggest that the reliability experts should identify

- The reliability models, which are appropriate to estimate the reliability of the special I&C system, and
- All the data, which are necessary to feed these models.

The result might be discussed together with system specialists to confirm that the collection of all identified data will be feasible.

The Five-Steps-Concept – a proposal to collect and assess operational experience

In Table 1 a systematic approach following [8] is proposed for the acquisition of data to evaluate operational experience. The approach covers the following 5 steps:

1) Evaluation of data and information which have been collected by the utility and involved experts to identify and investigate distinct fault phenomena (incident reports)
2) Taking into account the related information about operational experience which the vendors gained from the operators (backward system)
3) Evaluation of the operational data which are collected by the utility covering the cases the digital system has responded on a operational or safety related demand correctly in the specified manner (experienced operational profile)
4) Consideration of the data concerning digital I&C related incidents in domestic plants
5) Consideration of the data concerning digital I&C related incidents in foreign plants.

To our present concept the first three steps are particularly directed in order to collect operational data of a equipment family which is developed and maintained on a distinct platform. So the

description of the distinct platform and the failed functionality should be of more interest than e.g. the place of application.

Complementary in the last both steps, the world-wide gained experience will be taken into account, including the information about the application of other I&C products. Therefore, to our understanding this concept represents not a different or separate program, but will be rather a special selective application of the very useful COMPSIS data library.

REGULATORY ASPECTS APPLYING THE RESULTS OF RELIABILITY ANALYSIS OR SOFTWARE-BASED SYSTEMS

Relation between quantitative and qualitative approaches

Within the German regulatory framework, qualitative reliability requirements are preferably established. Concerning the deterministic requirements, operational experience can be utilized and evaluated in order to show that the I&C design principles and top-level requirements are met during operation.

The German regulatory framework contains quantitative criteria only by relative terms. For instance, it is required that the safety I&C shall not determine (affect) the availability of the plant safety system, see KTA 3501. According to the state of the art, the availability of both, the plant safety system as well as the I&C hardware, can be estimated. However, as a new task the estimation of an upper limit for the software-based system availability is to cope with. The result might be of certain interest within the licensing procedure for a software-based system for safety-critical applications.

As a German requirement for licensing, any new system's functionality and quality should be demonstrated by operational experience. This stands of course beside the general requirement to prove the quality.

This paper refers particularly to software-based I&C systems developed on a unique platform. Such a unique platform ensures an adequate documentation. During qualification, the hardware and software modules can – at least partly - be treated as white boxes. Consequently, the platform development supports the qualitative reliability assessment. As a compliment, the quantitative assessment can be supported by operational experience which are collected from all systems qualified according to the same standard and using the same platform. This way, the platform development shows advantages also according to the quantitative reliability assessment.

Consensus between involved parties

Even the optimization might be possible, the collection of operational experience may imply a considerable effort for all participants over the long-term period of some years. The participants (licensee, vendor, regulatory body and technical support organizations) should therefore agree from beginning upon the effort (e.g. the record format, time period and the content of the data collection), as

well as upon the objectives of this collection. If quantitative reliability assessment is foreseen experts on reliability assessment should be involved to establish the record contents and format from the beginning.

Conclusion

Taking into account the effort of the operators and vendors to collect operational experience from applications of computer-based I&C, the authors see the chance that these information and data can be utilized to support in following fields:

- The demonstration of the required qualification of computer-based I&C is based on deterministic as well as probabilistic approaches. Operational experience is required to derive dependability data.

- In the case of comparable operational profiles and unique platforms operational data can be collected together within a unique data library. Consequently the derived dependability data should be applicable – case by case may be under special conditions - to other systems of the same platform and of a comparable operational profile.

- Already established qualification procedures can be additionally validated and optimized. For instance, the test procedure of systems of the next generation can be optimized on the basis of the – real experienced - operational profile of the previous generation.

- The procedure to license the safety critical application of computer-based I&C – e.g. in the case of upgrading of a hardwired safety I&C system - can be supported using the operational experience from applications of the equipment which is developed and maintained on the same (unique) platform.

Needed agreements for the treatment of operational experience:

- The parameters which are necessary to obtain dependability data after a certain period of operation should be established before the data collection is started.

- The parameter profile should be harmonized under participation of the involved parties.

- Conditions by means of familiarity and anonymity are prerequisites for the treatment and acquisition data of operational experience.

The project is supported by the German Ministry of Environment, Nature Conservation and Reactor Safety (BMU). As a first result the five step concept is now under discussion. The participation in the COMPSIS activities is important for our project which started last year.

References

[1] Garrett, Ch, Apostolakis, G., Context in the Risk Assessment of Digital Systems, Risk Analysis, Vol. 19, No. 1, 1999

[2] Instrumentation and Control Systems Important to Safety in NPPs, IAEA Safety Guide 252, Vienna,

[3] Laue, K.-D., et.al., “Werkzeuge (Tools) zur Überprüfung rechnergestützter Leittechniksysteme mit sicherheitstechnischer Bedeutung", BMU/BfS research project, excerpt is to be published

[4] NUREG/CR-6101, “Software Reliability and Safety in Nuclear Reactor Protection Systems”, Appendix “Technical Background”, June 1993, Livermore, CA

[5] Saglietti, F., “Verfahren zur quantitativen Abschätzung von Zuverlässigkeitskenngrößen für Softwareprodukte”, ISTec-A-320, Institut für Sicherheitstechnologie Garching, 1998

[6] American Nuclear Society, “Proceedings of the International Topical Meeting on Probabilistic Safety Assessment PSA ’96”, vol. III, chapter “Information and I&C Systems, p. 1453ff., October 1996, Park City, Utah

[7] American Nuclear Society, “Proceedings of the International Topical Meeting on Probabilistic Safety Assessment PSA ’99”, vol. 1, chapter “Reliability Analysis of Digital systems”, p. 499ff.; chapter “Software Reliability”, p.641 ff.; August 1999, Washington, DC

[8] Lindner, A., Makuschies, B., Hoffmann, E., “Entwicklung von Methoden zur Erfassung von Betriebserfahrung mit rechnerbasierter Sicherheitsleittechnik in Kernkraftwerken”, ISTec–A–566, Institut für Sicherheitstechnologie Garching, 2001

Tab. 1: 5 steps concept – a proposal to collect and assess operational experience

Step	Kind of operational data acquisition	Acting organizations / institutions	Area of application	Period of acquisition	Aim of the acquisition	Remarks
1	**INVESTIGATION OF ASSERTIONS WHICH DO NOT EFFECT THE FUNCTIONALITY IN A NON TOLERABLE MANNER**	**UTILITY**	Limited to the effected system	Limited period	Explanation of root causes, investigation of fault phenomenon	
2	Feedback experience of the manufacturer	Manufacturer	All specimen of a distinct type of equipment	Lifetime of the equipment	Conclusions concerning fault effects B (reliability data)	Backward system
3	Acquisition of the operational acting (correct initiation of protection e.g.)[1)]	Utility (manufacturer)	total system	Lifetime of the system	To gain confidentiality in the experienced operational profile; "positive operational experience" (reliability data)	[1)] Important because of activations are seldom
4	Acquisition of national incidents	Utility TSO manufacturer	Digital safety systems in German NPP	Lifetime of the system	Generic assessment of digital I&C systems and equipment, particularly regarding the detection of design faults	TSO: technical support organizations like TÜV and GRS/ISTec
5	Acquisition of international incidents (within the COMPSIS framework)	OECD/IAEA	Digital systems in NPP abroad	Duration of operation of nuclear power plants	Establishing an international database for generic operational experience	

Digital Projects in the Near Past and their Consequences in Safety Regulations in Hungary

K.Hamar
Hungarian Atomic Energy Authority H-1539 Budapest 114. Pob. 676 hamar@haea.gov.hu

Summary

With the licensing and operational experience, the Hungarian Authority intends to reformulate the safety regulations and guideline statements. We have to refine the design principle recommendations, and restructure the licensing from the aspect of procedural rules, in order to establish better licensing environment for the benefit of the licensees, and the regulatory staff. Experience discussed below covers first of all the cases of reactor protection system, core monitoring system and process computer. Some statistical data will be also presented.

Experience

Reactor protection system, Teleperm-XS

In 1993, evaluating a Simple Task Specification the Hungarian Atomic Energy Authority (HAEA) Nuclear Safety Directorate (NSD) formulated first time an opinion about I&C refurbishment, and has not refused the idea of installing digital system for reactor protection functions. This regulatory position resulted digital solutions for the Hungarian NPP units in the commercial bid.

In the reliability analyses about the Teleperm-XS system of the contracted Siemens Company it was assumed that, for every EP1 actuation, functional diversity is ensured by the use of two physical diverse measured initiation criteria dealt by two different computers (Ts-a and Ts-b) in each train. The list of these diverse initiation criteria were accepted by NSD in 1996.
This is the only diversity assumed in the system against common mode failures. Accordingly, the possibility that the first action initiation can be missed must therefore be considered.

From the viewpoint of software, the interesting result of the analyses was the demonstration, that the common software parts, common to both computers Ts-a and Ts-b, a reliability level of 1E-6 is achieved. The analyses take the challenge to demonstrate, these levels are guaranteed.
On the other hand, the international expert opinion assumes, such a level is impossible to demonstrate by statistical testing. While the quantified reliability gave the opportunity to go on with scientific and theoretical discussions on the subject, the practical necessity of licensing this system arose.

Fortunately, not only the probabilistic approach could prove the reliability and requirement fulfilling behavior of the T-XS system.

The regulatory approach rely very far on the institutional type testing results, which are certified by German state authority technical support organizations. Another important issue in the licensing procedure was the existence of manufacturer independent factory acceptance test. The FAT test field provides the possibilities for open loop tests. In the Hungarian project the closed loop tests were done with the full scope plant simulator on the site, with a representative RPS configuration. The role of the closed loop testing is mainly the validation of technological functions, while open loop tests are exercising the computer system functions more. The above mentioned testing targets were interpreted in the FAT Plan, as it is in the Appendix of this paper.

During the evaluation we could see, beyond the theoretical effort Siemens went into big depths citing all of the available operational experience to formulate statistical evidences. What is desirable from operational aspect, was bad from statistical aspect. However there are some hundreds of Teleperm-XS modules operated in the existing configurations, the number of modules of one or another specific type, and the number of error occurrence are not enough for a big statistical mass. According to the available figures, the theoretical error calculations on the different modules resulted much worse reliability, than the real life operation up to now. So the T-XS behaved better in operation than it was theoretically assumed in a conservative approach, for example, with that assumption, the self testing can discover only the 90% of random HW errors. This year the reactor refurbishment project is about installing the 3rd Teleperm-XS configuration in the Hungarian Paks site, between 20. July and 20. September 2001.

The loss of reactor scram actuation is a crucial potential system error, which can happen only as result of common cause failure in all of the redundant RPS trains, due to the design principles. In this case the operator has the opportunity to start manual action, at least, switching off the control rod drives electric power supply with handy push button, to drop the rods with gravity. Going further, we have to analyze the rod effects.

The consequences of control rod jam or sticking were analyzed on different ways, among them with SMARTA computer code. The calculation show, in the VVER440 reactor core the pressure and the temperature in relation with the dynamic reactivity effects are not challenging the primary circuit on dangerous level, boiling is not probable, while, of course, the safe and long term reactivity control needs the boron injection. As a comparison, unintended rod withdrawal may have worse consequences to local temperature and boiling probability, and to the fuel and control rods. In general the ATWS event group has ~1% contribution to the CDF, that is in the 10E-6/year range, while the CDF median value is in the range of 10E-5/year.

These facts are conveying that message regarding the system reliability qualification, an ALARA approach is acceptable, especially, if the most important serial element to the RPS, the control rod drives and mechanism, have a given, and in the best case constant reliability.

Another approach is a kind of cost-benefit comparison, where the assessment effort spent to exhaustive and statistical testing, should take into consideration that fact among others, the I&C and electrical systems are together contributing with 15% to the CDF value in a detailed PSA level-1 model. The resources for different assessments should be shared among the different systems.

After the above considerations about the RPS, the licensee and developer offered test strategy and extent were accepted. The number of the test cases is approximately 200, which are representing different unit transient scenarios, which result actuation of reactor protection. The tests were executed in FAT, and in simulator environment.

Because of the individual modifications in the application, these test cases were run several times in both environments, on the Unit 1 and Unit 2 configuration. The total number of the executed tests, including the closed-loop manual test performed on the simulator, is around 2000.

No failures were detected in the on-line software during these tests. Considering the 0.5/year value for the real actuation demand, we probably may have that estimation, that the time elapsing between the occurrence of two software failures, causing actuation masking, exceeds 4000 years. Taking into consideration the periodic tests of the RPS also, which are exercising the protective functions, while the unit is running with nominal load, we believe the unavailability due to SW reason, is better, than 1E-4/year. We have to keep in mind, during these tests, those input parameters which are not intentionally triggering the RPS, can de defined, random, or living, which introduce differences, even if one specific test case will be executed many times.

It can be assumed due to the fail-safe design, the residual SW errors, which hasn't been discovered yet, will initiate spurious actuation instead of actuation masking.

The total number of the test cases for the RPS and the representative configuration, connected to the plant simulator, on the four Units together, is expected to be 10 000, thus the SW reliability is hopefully growing to 1E-5, upon the completion of the Unit 4 system.

Core monitoring systems

Core monitoring system resides in IEC1226 "B" class, since it has been installed on all of the four units between 1992-1994. The system consists of two fold redundant micro-VAX, with the application named Verona 5.2 version, running in VMS environment. The application can be characterized with 50.000 line of Fortran and C source code. Data acquisition is running on 5 Motorola68000 computer cabinets, under OS9 system.
In August 2000 Authority refused operational license application due to many modifications during the implementation phase (coding, testing and pilot run) of the last version.
With the modification permit the Licensee had right to operate and test the modified system for three month. The modifications had been completed during this period aimed to correct algorithm and communication problems.
Asking the procedure, what the Licensee followed many cases, the Licensee argued with the citation of safety code paragraphs, which were formulated originally to distinguish the repair and modification regarding the mechanical components. Since the software hasn't been excluded in the paragraph text, this argumentation had a formal chance.
The SW error correction is naturally modification, deviates from the mechanic analogy, where the corrective action intends to restore the original technical conditions. The SW error correction intentionally wants to achieve new technical condition and behaviour.
The review of safety regulations in 2001 needs to handle software issues in a special manner, deviating from the presently existing general definition of error and repair. Our approach this time is that, in case of SW products, we try to define the terms of repair and modification against the functional specification, and the system specification.

Process computer re-classification due to increasing safety importance

The old system had been in "C" (IEC1226) safety class. The newly installed successor process computer system consists of four pairs of redundant Supervisory Control and Data Acquisition (SCADA) Intel platform servers, several additional computers and operator workstations. A WEB server provides information for a large number of remote users in their office computers. The application is running in Windows-NT environment.
The system has an important role to present and archive the RPS readings, and corresponding calculated values in the control room. Due to this fact, the system installation took place parallel to the Reactor protection system refurbishment.
The most significant function group comprises the implementation of a critical safety function monitoring system. This task is being carried out under the scope of a joint international agreement established by the OECD NEA. The project goal was to develop an operator support system to support the execution of new symptom-based Emergency Operating Procedures, for application in VVER reactors, with the Paks NPP as the target plant. EOP starts run in 2002.
Due to the increasing safety significance, the Regulator classified the process computer as "B" safety class system this year, but give dispensation from immediate qualification of the system, regarding the pilot project, and the good operational experience since 1999.

The system has many "commercial off the shelf" COTS software modules, that means any functional modification in the future requires qualified COTS, or qualified application. Both parties are facing problems to solve it.

Errors and problems of digital systems and related components 07.1999 – 07.2001

All of the below listed systems started their service in this period. The below data is based on licensee event reports (LER).

RPS and RPS related errors and problems were found during service time, FAT excluded. Cumulated service time in the period: 3 years. DFD is the graphic representation of the application, this is practically a data flow scheme, the symbols are I&C engineering and process control symbols. The DFD is compiled to running code.

Specification error (DFD correction needed)	**3**
Random HW error (power supplier errors: 4)	**10**
Recurrent HW error (first occurance random, DC power supplier error)	**3**
Systematic or CCF HW error	**1**
Application SW bug	**2**
High load on safety related (non safety) Ethernet bus	**1**
Measurement anomaly, no cause identified	**1**
Loss of telegram (due to assyncron behaviour)	**1**
Error log, but no cause identified	**1**
Non-recurrent phenomena, had no effect to log files	**1**
Sensor error	**17**
Human error caused value reading lead to actuation	**2**
Gateway and Service Unit (recurrent error is 1 error)	**3**

Diesel Generator Control System – Woodward PLC error during service time.
Cumulated service time in the period: 2 years.

Random HW error (power supplier error)	**1**

Uninterrupted 220VAC power supply, type Staro-Eta error during service time.
Cumulated service time in the period: 32 years

Random HW error (inverter ignition control board)	**1**

Other systems had no LERs during the same time, which doesn't mean necessarily, they had no errors. LER criteria is technical specification violation due to system unavailability.
In case of the RPS systems the above data covers only the new digital systems on the 1st and 2nd unit of Paks NPP. The old systems are not included. **Not only LERs, but all RPS error indications should be reported** due to occasional regulatory prescription in the permission of the RPS refurbishment.

Licensing

In the safety code we have only some statements about computers. These statements were formulated in 1996.

Where such a system or component is used, the reliability of which basically depends computer program, suitable techniques and standards should be used during the development and the entire lifetime of the computer program or the compliance with these techniques and standards should be set as an objective through the following:

a) during the development of the computer program, verifying the operation of the safety-related system and component, the application of ***latest design practice*** *commensurate with approved standards;*

b) quality assurance program and plan operated on the basis of ***appropriate quality assurance*** *standards****;***

c) complete and sufficiently ***diverse testing*** *of the latest validated program version by a group independent of the developer;*

d) execution of a ***wide-range and independently qualified test program****, which includes the test of all system functions and proves system reliability.*

The quality assurance played proper role in the RPS, and in the diesel controller project. The uninterrupted power supplier control function is very simple, and the PLC has mainly firmware. It is easy to report the QA worked.
In the core monitoring project, despite of the QA, the big mass of software, and the classic structured development characterized the situation. It took a big effort to finish the project.
The process computer and the object oriented SCADA has a very good reputation among the licensee staff, but the regulator had no opportunity to assess the quality and quality assurance measures, up to now.
We believe, the sufficient testing could be proved in all of the projects, but the divers testing can be mentioned surely in case of the RPS project, only. Diverse testing environment was not available in the other projects. The independently qualified test program is true from that aspect, they were independent to the developer, in every case.
We are in trouble with point a), with latest design practice. The above characterized projects followed totally different techniques in development: Complex PLC like graphic interpretation, simple conservative PLC program development, structured programming, and tendency to object oriented programming in the SCADA project.

Due to the appropriate standards the RPS introduced into the practice the most important safety requirements:

- Simplicity
- CCF protection: separation, cabling, earthquake resistance
- CMF protection: HW, SW, specification
- Fail-safe construction
- Reliability
- Testability

Since the appropriate standards could not be identified neither among the Hungarian standards, nor among the EU directives, we should like to address these system properties in the new safety code directly, in order to maintain the safety of class “A” systems. It is not possible to go into details from technical aspect, the safety code is governmental decree level document. On the other hand it is also not practical to do so, because there are many interested parties in a general legislative procedure, which can disturb technical

statements easily. The IEC and IAEA will represent the good practice, as it is intended originally, and they can be interpreted in the guideline series, however they are not obligatory.

The requirement of simplicity conflicts with almost all the other requirements, mainly the functional requirements (not representing the subject of the present article), testability and diversity.

Some other system properties should be underlined among the requirements for class "A" systems:

- Use of a strictly cyclical, controller-type program
- The input data should be processed only by the application software. The input data may have no impact on the behaviour of the operating system and the run-time environment.
- Changes in the input data do not cause interruption.
- Changes in the input data do not cause changes in the sequence of task implementation.
- The processors and the communication networks have a constant load, regardless of the status of the inputs and the equipment (HW failures).
- The status of the system does not depend on the status of the environment.
- The distribution of the system resources is static.
- The software modules and their interface are strictly defined.
- Software modules are thoroughly tested and qualified, independently to the application specific tests.
- The redundant trains operate asynchronously and do not use a synchronising mechanism, while the actual service time of the trains should be always different.

Analyzing the above projects and systems, we can see, the RPS system meets these requirements, the diesel generator controller also owns these properties, the uninterrupted power supplier control function is very simple, and the safety could be proved easily, even with no regard to the above requirements.
In case of the core monitoring, the sample readings and calculations has the cyclic and deterministic behaviour, the question is that, how it is running in the reality on a VMS system, together with the archive function. The archive is working on aperture principle, so it is event driven.
The process computer intentionally transient sensitive due to archive goals, the changing of input data may change the execution sequence, during plant transients the system load has very dynamic character.

Conclusion

That means in the reality, to give floor to the daily practice of assessment and other regulatory activities, not all of the above requirements should be followed in class "B" (class "C" is out of regulatory interest). This is beneficial to the Licensee operated existing systems, too.
But, it is interesting to see, the qualification of class "A" systems was much easier, than the cases of the "B" class core monitoring system, and, what we believe, the process computer. The reason is that, the safety is manifesting in a set of static and dynamic system properties, among them probably the most important is the deterministic behaviour. If this property is assured, the assessor has much easier job. Which is again a safety contributor. That conclusion will be surely addressed in the new safety regulations.

Appendix

A very short description of the Hungarian party executed FAT tests, excercising the Teleperm-XS system to be installed in Paks NPP for Reactor Protection System functions.

1. Identification of system components and test environment. The examination is based on the comparison to of the CRC sums in the downloaded code to the CRC of the compiled code, while some other identifiers are also taken to account. The identification of the SPACE system components running on the service unit is belong to this task also.

2. Function tests, status of readings handling. Verification of the functional behavior of the system against the functional specification. The task also combines input failures, and transient simulation is generated on the inputs. This test was done by the Siemens Co. also, finalizing the in-house tests.

3/1. Fault tolerant behavior. The system is divided into stand-alone units, while unit errors are simulated in different combinations. The testing staff is checking the impacts of the failures. Automatic system regeneration should follow the error situation.

3/2. Fail safe behaviour. Single, double and triple analog and binary signal failures are injected into the redundant inputs of the system. The effect is checked on the different data monitors and on the output to the actuators.

3/3-1. Self monitoring. The test covers basic hardware tests during start up, cyclic testing in operation, voter computer master-checker function, watchdog (time out), exception handler functions, cabinet alarm, individual signal monitoring, check back of output signals, error status and error message processing.

3/3-2. Periodic tests. This test covers the operator initiated test functions, the safety conditions of periodic test initition (only one train can be tested at the same time, etc),
returning of the tested train back to normal operation, while artificial errors still are in the data process.

3/3-3. Start–up tests. The extent and the content of these test differs from the periodic tests.
Anyway this test is due at power unit start-up after refueling and general overhaul.

3 /4. Man-machine interface. This test is exercising the human operations on the safety monitoring system, the service unit, the test machine, and the information subsystem.

3/5. Independence of the subsystems. This exercise should prove, he three redundant trains, the man-machne interface in the main and emergency control rooms, the service units and the gateway computers to the information subsystems are totally independent from each-other from physical, electrical and logical aspect. The test field is applicable only to prove the logical aspect, no information or lack of information can influence the proper operation of the subsystems. The electrical aspect is type tested, any further test can damage the system. Physical aspect is the function of on-site installation.

3/6. Deterministic behaviour. The test should provide that proof, the operation and collecting of analog and binary signals are really cyclic with the same time constant, with a given tolerance margin, in any external condition represented by values of inputs. The external conditions are simulated by redundant, nearly syncron, slowly slipping probe signals, while the safety function execution, in accordance with the momentary probe signal configuration, is expected. At the same time the availability of the data on different points of the system is checked.

3/7. Input accuracy check. This test doesn't need explanation. The test should cover all of the existing and physically different input channels and converters. The test machine is a requisite.

3/8. System reliability checks. Exercising the system with big number of negative random input sequences, which tests the potentiality of unintentional reactor trip. Success condition is the lack of reactor trip signal during any time extent.
The another test is random input test also, the input random patterns are mixed with trip combinations. Serves to test the loss of reactor trip potentiality.

3/9. Accessibility of system software. The user can assess the software on three ways: via the Service Unit on-line, via the Test Machine, and by manual actions. Authorised user is allowed to access on the Service Unit. Under defined system conditions or without administered permissions (turn key switches) the test machine operation is not allowed. If test has already started, the system should turn back to normal operation. Manual action like opening the cabinets must be indicated by alarm.

3/10. Information interface. In these tests the data connection to the gateway computers are tested. The completeness of the data tables and the cyclic refresh of the data items are verified.