Unclassified **NEA/CSNI/R(2002)1/VOL2**

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/VOL2
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

JT00127841

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.

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 TABLE OF CONTENTS

TECHNICAL SESSION 3:

ANALYSIS AND ASSESSMENT OF DIGITAL I & C SYSTEMS
Chairmen: M. L. Järvinen - M. Kersken

Preliminary Evaluation of Computerized Procedure From Safety Viewpoints

Yun H. Chung[1], Sung N. Choi[2], Bok R. Kim[3]

Korea Institute of Nuclear Safety, 19 Guseong-Dong Yusung-Gu, Taejon, 305-338, South Korea

[1]Tel: +82 42 868 0245, Fax: +82 42 861 9945, e-mail: yhchung@kins.re.kr
[2]Tel: +82 42 868 0241, Fax: +82 42 8612535, e-mail: choisen@kins.re.kr
[3]Tel: +82 42 868 0242, Fax: +82 42 861 1700, e-mail: kimbr@kins.re.kr

Summary

The KNGR is an evolutionary reactor and is under development. This paper briefly describes standard design license system and primary design features of the Computerized Procedure System (CPS) and compares the CPS of the KNGR with other computer-based procedure systems.
From a literature survey and an informal study, we firstly derive the review issues for safe plant operation – safety impact on operation personnel and shift performance, design for situation assessment and response planning, utilization during complex situations including the CPS failure, design for navigation and communication, and software quality. Then we present the preliminary evaluation results.

Introduction

Korean Next Generation Reactor(KNGR) is an evolutionary reactor, which has an official name as Advanced Power Reactor 1400 and is under development. The KNGR is now under preliminary safety review and has a plan of commercial operation in 2010.

The KNGR introduces a lot of brand-new human-machine interface (HMI) design features in nuclear industry of Korea, such as workstation-based control room; Large Display Panel which provides a bird's view of plant condition; the CPS which shows all operation procedures; Soft Controls using touch screen which can control both safety and non-safety components; advanced alarm system using prioritization and filtering.

The standard design license system for APR 1400 requires Standard Safety Analysis Report(SSAR), Standard Design Specification, Emergency Operation Procedure Writing Guidelines, and the design details of Standard Design is expected to the level of design certification documents of U.S. advanced light water reactor. The applicant of Standard Design should establish and submit a verification program to confirm that the as-built facilities of a nuclear power plant (NPP) satisfies both the design and applicable regulatory requirements, during the stage of design licensing review. And the program which is called as DCPVP(Design, Construction, and Performance Verification Program) shall be reviewed by the regulatory body and performed by an applicant to construction or operation license during the stage of construction or operation licensing review. The Certificate of Standard Design will be valid for 10 years (Lee et al., 2001). The KNGR is under the preliminary safety review.

The purpose of NPP procedure is to guide human actions when performing a task to increase the likelihood that the actions will safely achieve the task's goal. In contrast to decision aids, procedures define decisions to be made and actions to be taken (USNRC, 2000). The human factors goals of procedures do not generate an undue task overload and are easy to understand and follow (Niwa et al., 1996). That is the reason why Writer's Guide is an essential component of the Emergency Operation Procedure(EOP) Generation Packages.

Evaluation of Computerized Procedure System

Computerization of procedures in nuclear industry seems to be a design trend as shown in Table 1. Spurgin et al. (1993) described an overview of many computer-based procedure system. Now many nuclear power plants (e.g, Beznau, Chooz B, Civaux, Temelin) use various types of computer-based procedure(CBP) system. The driving forces include the limit of paper-based procedure(PBP) presentation ways, including lack of interactive capabilities between PBP and sophisticated systems, and the high volume and cost associated with paper manuals used in complex and technically demanding environments. (Wourms and Rankin, 1994)

Overview of Computerized Procedure System

The CPS is a computerized operator support system and covers all operation procedures. It provides information through workstation consoles using flowchart and tree structure and also has an automatic checking capability of step logic including continuously applied steps. The CPS however is a passive system. The CPS was developed upon the basis of Computerized Procedure Manual II (COPMA II), which was developed by the Halden Reactor Project.

Table 1. Comparison of Computer-based Procedures

System Name	KHNP CPS	EdF N4 Reactor	Westinghouse COMPRO[1]
Procedure Scope	All[2]	All	EOP
Active/Passive	Passive	Active[3]	Passive
On-line/Off-line	On-line	On-line	On-line
Operation/ Training	Both	Both	Both
User = SS or Operator	Operators with SS[4] overview	Operators with SS overview	SS
System falls?	Paper-based procedures	Paper-based procedures	Paper-based procedures
HMIs	2 CRTs Workstation	2 CRTs	2 CRTs Workstation
Basic structure of main page	Six parts[5]	Three parts[6]	Four parts[7]
Software grade	Non-safety	Non-safety	Non-safety
NPPs	APR 1400, Korea	Chooz B and Civaux, France	Beznau, Switzerland Temelin, Czech Rep.

Note:

1. COMPRO stands for Computerized Procedure
2. All means normal and abnormal procedures as well as emergency operation procedures.
3. Operator can override computerized monitoring. So the human operator must remain in final charge of plant unit operation at all times (Pirus et al., 1997).
4. SS stands for Shift Supervisor.
5. Six parts consist of Menu pane, Continuously Applied Step pane, Postponed pane, Multi-procedure Display pane, Procedure Overview pane, and Current Step pane.

6. Three parts consist of upper, middle, and lower panel. Upper part presents symbols of all the sub-procedures. Middle part presents the main parameter values and special plant system states. Lower part presents the same kind of presentation, but is reserved for support systems monitoring (Pirus and Chambon, 1997).
7. Four parts consist of Pull Down Menus, Parallel Information, Current Procedure Information, and User Prompts (Lipner and Kerch, 1996).

The CPS displays consist of a main screen and a support screen. The main screen has six panes. Those are menu pane, continuously applied step pane, postponed pane, multi-procedure display pane, procedure overview and current step pane, as shown in Figure 1. The support screen can show additional information for the current step on an adjacent screen.

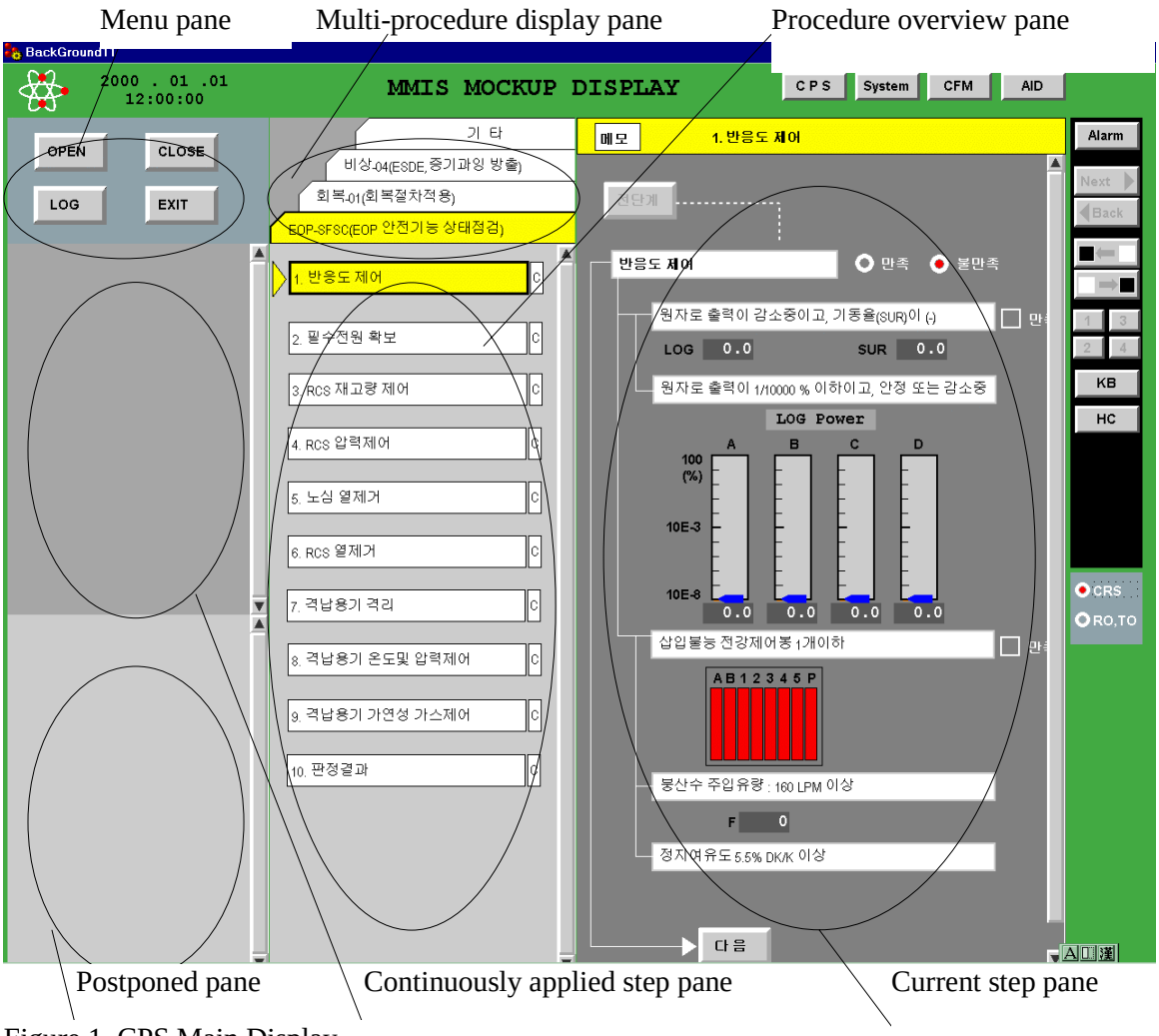


Figure 1. CPS Main Display

Operator (Reactor Operator or Turbine Operator) is able to accomplish plant operation by using only the main screen, but when he wants additional information (e.g., P-T curve, variable trends, etc) in relation to current step, he can use the support screen. The support screen is linked to the current step and appears automatically as the current step changes in the main screen.

All the process information and control components that are cross referenced in the instruction, are presented near the associated instructions so that an operator can easily evaluate the

instruction or confirm the computer's evaluation. The component symbols targets are used to call up the control components in the soft control HMI. All these process information are updated by plant data from Information Processing System. Control commands from the CPS are sent to soft control HMI to select the control component.

The entry condition of current step is evaluated by the computer based on process information. The result of evaluation is dynamically displayed on the instructions of current step pane. So the procedure is no longer static like paper procedures. Even though the CPS shows its evaluation dynamically, operator is able to override the computer's decision and change the procedure flow.

Expected impact of the CPS usage

In relation to expected impact of the CPS, Min et al. (2001) addressed one study that has examined the effect of using the CPS in 2000. One major finding was that there was a dramatic reduction in verbal communication between the supervisor and the two operators. In Korea, while executing an EOP with a PBP, the control room supervisor is supposed to read each procedure step aloud and the corresponding operator should echo the procedure step. The assumption the designers made was that the operators at the advanced MCR would follow the same guideline for verbal communication while executing the procedure with the CPS. Apparently participants did not fully abide by this guideline and the CPS seemingly eliminated inquiry-reply type of communication.

Another finding was about the scope of auto-checking features. Designers emphasized the benefit of providing auto-checking features and showed the tendency towards more auto-checking features. For example, the CPS can execute a procedure step by comparing the set point value with actual process values using the logical relationships specified in the step. This reduces the crew cognitive workload. However, although auto-checking features are a major advantage of the CPS, it creates serious concern. Roth and O'Hara(1998) reported that "on occasion the CPS could provide misleading information or direct the operators down the wrong procedural path." The supervisor put too much trust in the CPS, and called out the wrong actions suggested by the CPS without double-checking. This problem may occur with paper-based procedures, but the CPS aggravates the problem. The supervisor's passive mode of information processing may erode mental model.

Design and evaluation issues of the CBP system

Wourms and Rankin (1994) recommended the design approach from an integrated systems point-of-view which considers the combined influences of software, hardware, interface design, and available techniques on human-machine system performance, the thoughtful consideration of the relative strengths and weaknesses in human information processing, and a smooth transition from CBP to PBP during CBP failure.

Niwa et al. (1996) identified four concerns of using procedures, such as whether operators are able to use the current procedures in a sufficiently reliable way; whether the use of procedures creates additional tasks that deflect effort from main task; whether the procedure in their present form lead to damaging increases in workload; whether the specific format of the procedures constitutes a source or risk. And they suggested six aspects of procedure presentation that can have an impact on above concerns; navigation, formatting, progress in monitoring, help and explanation facilities, process linking, and procedure adaptation.

Roth and O'Hara (1999) described impacts of CBPs, such as team structure and dynamics; ability to monitor and redirect procedures. They specifically classified effect on team structure and

dynamics into the cognitive performance of individual crew members, the functioning of the crew as a team, the scope of responsibility of the different crew members, the communication pattern among crew members, the situation awareness of the different crew members.

O'Hara et al. (2000) suggested general considerations for near-term approaches to CBP systems: the pace control of the procedure and the transitions within and between procedures, support of the high-level awareness of procedure goals and the context, availability of variable levels of detail in procedure steps, automatic monitor of process variables, procedure step completion, and place keeping, careful support of step logic analysis, emphasis of training issues.

US NRC (2000) also raised several human performance issues associated with CBPs. The issues are as follows: methodological and criterion requirements for evaluating CBP effects, role of plant personnel in procedure management, team performance, situation awareness, response planning, and operator error; level of automation of procedure functions; keyhole effects and use of multiple CBP procedures; CBP failure in complex situations; hybrid procedure systems; and specific CBP design features.

From the above literature review and informal study of the CPS, we identified the review issues. Those are impact on operation personnel and shift performance, design for situation assessment and response planning, utilization during complex situations, including the CPS failure, design for navigation and communication, and software quality. The following section describes the preliminary results for each review issues respectively.

Preliminary Evaluation Results

Impact on operation personnel and shift performance

The CPS does not have a capability of automation for decision-making and manipulation to control plant according to operation procedures, but provides information for operator to handle (i.e., finish, delay, pass) each step. So responsibility of decision-making still remains to each operator. The designers took preliminary validation using some scenarios (e.g., LOCA, SGTR) during design phase. However, they did not suggest the evaluation measures for performance of operation personnel and shift. Although the CPS can make information search easy, it needs an appropriate performance measures and the evaluation results as per, which shows the acceptable impact on personal and shift performance.

Design for situation assessment and response planning

The CPS automates error-prone tasks, such as basic step logic determination; monitoring of continuously applied step and entry condition, that can minimize cognitive load on operators. The current step pane contains detailed information (e.g., variable value, component status, note and so forth) in order to accomplish each step. Basic structure for current step is flowchart and tree logic. Operator has to execute some actions to satisfy each instruction. Since the structure is very simple and intuitive, operators are able to understand it easily. It also provides additional information of plant system with Information Processing System (IPS) mimic CRT.

With the improvement of related information search, memory of plant condition, operation support information and recording of execution results, the CPS tries to support the situation assessment and response planning. In addition, the procedure overview pane displays the current step and executed steps using color coding. The design for situation assessment and response planning seems reasonable for

changing operation environment. However, the display method of automated processing, the display space and/or the large number of continuously applied steps remain as an open issue.

Utilization during complex situations, including the CPS failure

When the CPS failure takes place during its use, it does not any longer provide supporting information to operator any more. Then operator has to use the paper procedures, which looks similar to computerized procedures. Just in case, the computer system printed the executed steps when each step completed. It will give a chance to keep track of failed condition. After fast understanding with printed steps, operator can handle an unexpected situation with paper procedures. The design for smooth transition from CBP to PBP seems acceptable. However, there still exists the necessity of the usefulness validation about the design of transition.

Design for navigation and communication

In order to reduce the unnecessary navigation, the CPS has six panes and supporting screen as described before. Specifically for navigation among steps and/or procedures, it contains procedure overview pane, current step pane and multi-procedure display pane. Among these panes, the multi-procedure display pane holds the three most recent procedures which operator opened from the procedure lists. All the other procedures can be accessed by using ?Etc? button at the multi-procedure display pane. Comparing with the COMPRO of Beznau nuclear power plant, shift operators of main control room share the information of the CPS, which can provide an implicit communication tool among operators.

The design for navigation seems acceptable. As for communication issue, the very low level of communication among the crews raises serious concern in many aspects (Min et al., 2001). It may hinder crews from sharing situation awareness. In general, when a group of persons work together to accomplish a common goal, they need a common understanding for the given situation and each other's intentions and actions. In other words, a high performance team shares situation awareness so that a member may find other members error, or even prevent an error (Hutchins, 1995). The low level of communication also eliminates the chance of training on the job. Operators learn the supervisor's role by observing his action and by communicating one another. Therefore the CPS needs the more thoughtful way of communication.

Software quality

The CPS is a non-safety grade information system. That is, the software category of the CPS is "Important to Safety" among four categories (i.e., Safety Critical, Important to Safety, Important to Availability, General Purpose), and will take verification and validation process according to its grade. The "Important to Safety" software is a second grade software whose function is necessary to directly perform alternate protection system control actions or software that is relied on to monitor or test protection functions, or software that monitors plant critical safety functions. The software grade of the CPS is equivalent to that of AP-600 and N4 plants. The software grade and its corresponding V&V plan are acceptable.

Conclusion and Discussions

From the literature survey of design and evaluation documents and an informal study, we found that CBP is a design trend and can support and enhance operator performance effectively. However there exist a few open issues too. That is why the designers need to implement CBP system thoughtfully. This paper addressed five issues for the review of the CPS for safe plant operation, but we will not limit to the review issues that are listed here. This paper also described the preliminary evaluation results. That is, we are on the long way of safety review.

References

Hutchins, E. (1995), Cognition in the Wild, MIT Press, Cambridge, Massachusetts.

Lee, J., et al. (2001), Legislation of Safety Regulatory Requirements for Korean Next Generation Reactor (III-2), Korea Institute of Nuclear Safety (in Korean).

Lipner, M. and Kerch, S. (1996), Operational Benefits of an Advanced Computerized Procedures System, Westinghouse Electric Company

Min, D., Chung, Y. and Kim, B. (2001), An evaluation of computerized procedure system in nuclear power plant, Proceedings of IFAC Human-Machine Systems 2001 (in press).

Niwa, Y., Hollnagel, E. and Green, M. (1996), Guidelines for computerized presentation of emergency operating procedures, Nuclear Engineering and Design, 167, pp. 113-127

O'Hara, J., Higgins, J. and Kramer, J. (2000), Automation of emergency operating procedures: Finding the right balance, Proceedings of NPIC & HMIT 2000

Pirus, D. and Chambon Y. (1997), The Computerized Procedures for the French N4 Series, IEEE Sixth Annual Human Factors Meeting, pp. 6-3~6-9.

Requests for additional information (RAI) and Responses for Standard Safety Analysis Report of the KNGR (in Korean).

Roth, E. and O'Hara, J. (1998), Integrating Digital and Conventional Human System Interface System: Lessons Learned from a Control Room Modernization Program, BNL Report J6012-3-4-5/98, Upton, NY: Brookhaven National Laboratory.

Roth, E. and O'Hara, J. (1999), Exploring the Impact of Advanced Alarms, Displays, and Computerized Procedures on Teams, Proceedings of the Human Factors, and Ergonomics Society, 43rd Annual Meeting, pp. 158-162.

Spurgin, A. and Wachtel, J. (1993), The state of practice of computerized operating procedures in the commercial nuclear power industry, Proceedings of the Human Factors, and Ergonomics Society, 37th Annual Meeting, pp. 1014-1018.

Sung, C. and Jung, Y. (2000), Computerized Procedure System for Korean Next Generation Reactor, Proceedings of NPIC & HMIT 2000

USNRC (2000), Computer-Based Procedures Systems: Technical Basis and Human Factors Review Guidance, NUREG/CR-6634, U.S. Nuclear Regulatory Commission.

Wourms, D. and Rankin, W. (1994), Computer-based procedures, CSERIAC-RA-94-002, CSERIAC.

Modernisation of I&C system for ANP Dukovany by the use of computer-based equipment.

Author: Jean-Pierre BUREL (Schneider Electric)
Co-author: Frantisek DALIK, Karel WAGNER (Skoda-JS), Miroslav RIS (Škoda Energo), Jean-Paul MAUDUIT (Framatome-ANP)

Abstract

The original safety and control systems of Dukovany NNP will be replaced by new digital systems. For safety systems (category A according to CSN IEC 61226) the SPINLINE 3 Technology developed by Schneider Electric and Framatome ANP is used. For some systems important for safety (category B), the computer based system Škoda is used. Both technologies, already implemented on several reactors in different countries over the world, are well suited for modernisation projects and have been yet used for these ones. They give the opportunity to reach the latest safety requirements governed by international and national standards.
This paper describes these technologies, the architecture and the main features of the new I&C systems, especially safety systems. The consequences regarding safety and operability are considered.
The computer-based systems used for information systems (category C) are not mentioned in this paper.

Implementation of New Digital Safety Systems on Dukovany NPP

1. INTRODUCTION

The fundamental trend of the technology for automation has a high changing rate. The components on the market become more and more fast and complex. They allow better performances and a better efficiency in system operation. The use of computers to operate industrial plants and factories becomes general and Nuclear Power Plants have the same evolution.

Safety systems for Nuclear Power Plants are governed by strong requirements, which cannot be fulfilled by products designed for normal industrial applications. That's why in all countries, safety classified systems and non-safety classified systems for NPPs use different technologies even if the classification standards give several definitions and gradations for systems.

In co-operation with Framatome ANP, Schneider Electric has developed a technology dedicated to safety systems. This digital technology called SPINLINE 3 results from the experience obtained by Schneider Electric after more than 20 years on digital safety systems for Nuclear Reactors.

For the management of the Control Rod Drive Mechanism System for the reactors VVER-1000 operated in Czech Republic and in Ukraine, a computer-based system has been developed in Škoda and is in operation since 1996 on the South – Ukraine NPP and then in Chmelnická NPP and Temelín NPP.

The modernisation of I&C safety systems of the Dukovany NPP is based mainly on the SPINLINE 3 technology with the active participation of Czech companies like ŠKODA-JS and ŠKODA ENERGO, I&C ENERGO and •EZ. This project is now in progress. The first implementation of new safety systems is foreseen for the Unit No. 3 of the Dukovany NPP during the years 2002 - 2005.

2. CHARACTERISATION OF THE SAFETY SYSTEMS FOR NPPs

In the context of NPPs, the differences between „ Safety systems „ and „ Industrial systems " concern, for safety systems, the guaranty of operation in all circumstances, even in case of failure or after an accident like a limited fire or an earthquake.

An „ **Industrial system** " needs to be efficient in term of performances and in term of costs. The development has to be easy and the time for design and for implementation must be as short as possible. The consequences of a possible failure can be acceptable even if it is not desired.

A „ **Safety system** " has more or less the same requirements regarding performances and costs, but it has to be primarily capable to operate in any time and in any conditions. That is the fundamental difference and the main issue is to reach a reasonable proof of it. This guarantee of operation is of the highest importance. It is not acceptable to have a faulty system when a protective action is required.

3. TECHNOLOGY

3.1 SPINLINE 3 Technology

SPINLINE 3 is a digital and modular solution, which covers all safety functions and all functions important for safety, from measurement acquisition to actuator control, mainly:

- Reactor protection (reactor trip and associated engineered safety features, diesel load sequence),
- Reactor control and limitation,
- Nuclear instrumentation.

The main featuring objectives of the SPINLINE 3 technology are:

- A technology, which complies with safety requirements for NPPs (national and international standards).
- An efficient, fast and industrial development methodology
- A long term guarantee for maintenance and spare parts, more than 25 years
- Easy operation and maintenance,
- State of the art performances

The SPINLINE 3 technology can be described from a combination of three major components: The system, the hardware, and the software.

3.1.1 The System

A system built with the *SPINLINE 3* technologies is a combination of several units, which perform functions following strict safety performances. The achievement of these safety performances is obtained by following a development methodology, which includes the design of the architecture, the validation of probabilistic safety assessment, the qualification of the design with accuracy and response time.

With the *SPINLINE 3* it is possible to design small and large distributed safety systems, with an adequate redundant architecture.

A safety system has to comply with various criteria, some typical can be listed:

- Fail-safe architecture: *SPINLINE 3* assures that the outputs controls to actuators are always valid or in a safe position in case of failure.
- Fault-tolerance (including single failure criterion): *SPINLINE 3* can meet any redundancy requirements.
- Functional diversity: can be implemented to defend the system against common cause failures.
- Functional insulation: by avoiding propagation of failures between redundant divisions and individual system of different categories.
- Determinism: for all types of processing, the same inputs produce the same outputs with a guaranteed response time.
- Easiness of operation and maintenance.
- Flexibility for further evolution without any hardware modification.
- Modularity: *SPINLINE 3* can be delivered either as racks to be integrated into existing cabinets (for refurbishment purposes) or as whole cabinets.
- Scalability: *SPINLINE 3* fits various sizes of I&C systems. It can be used for highly distributed architectures such as a reactor protection system, distributed processing for acquisition, function processing and vote.

SPINLINE 3 meets international standards (IAEA, IEC) and various national standards for the design of nuclear safety I&C system.

3.1.2 The Hardware

The *SPINLINE 3* hardware is a set of modular components, designed, manufactured and qualified specifically for safety applications in nuclear reactors. These components are cabinets, racks, electronic boards or modules and cabling elements between components. They are designed, manufactured and qualified according to nuclear requirements and standards.

The wide range of I/O boards and their capacity allows *SPINLINE 3* to fit any safety nuclear application needs for control. The use of powerful CPU boards and high speed networks gives short response times even for complex functions and, above all, the response time is guaranteed by the deterministic features of the *SPINLINE 3* components.

The hardware components include:

- Cabinets and 19" 6U racks. Cabinets and racks are designed to withstand harsh conditions e.g. temperature, EMI, vibrations, earthquake as defined in relevant standards,
- A full range of input and output boards for binary and analogy data, neutron instrumentation, thermodynamic instrumentation, actuator control,
- A 25 MHz 68040 Motorola microprocessor CPU board, with 2 megabytes of secured read only flash, 2 megabytes of RAM and 64 kilobytes of non-volatile EEPROM memory. This board can provide up to 4 NERVIA interfaces,
- High speed deterministic 1E network: NERVIA is a 10 megabit/s, broadcast type, token ring network. The medium is either optical fibre or shielded cable with twisted pairs of wires. It is used for communications within the safety system or for communications with non-safety units. Both NERVIA hardware and software fully comply with class 1 E requirements,
- Actuator network: The 1E actuator network is based on a master/slave protocol and uses many of the NERVIA network components. It is dedicated to safety actuator control needed for example for the Engineered Safety Features,
- Interfaces to the PC world via the NERVIA network. *SPINLINE 3* may also interface with other analogy or digital systems using networks, serial data links or wire-to-wire links.
- The NERVIA network is the standard communication link within the safety system.
- It provides safe and efficient data exchange among units. It is based on a broadcast protocol i.e. any message sent by one unit is received simultaneously by all the other units of the network. Data is exchanged within consistency blocks and secured by CRC checksum.
- A processing unit can communicate with other units through one to ten NERVIA networks.
- One NERVIA network can link up to 30 different units.
- A PC NERVIA board, installed in PC, allows communication between 1E equipment and other equipment.
- Other data links.
- Gateways are available to Ethernet networks and can be developed to other networks if needed, either on a processing unit or on a standard PC.

Cabinets comply with the IEC 60529 standard: « Degrees of protection provided by enclosures (code IP) », protection index IP22 and are qualified under seismic stress. They receive power supply, racks, fans, input/output cabling interfaces, internal wiring and display devices.

3.1.3 The Software

The *SPINLINE 3* software of each digital unit is developed by using a set of tools and procedures dedicated to nuclear safety software developments. The software tools are based on a „ System and Software Development Environment (SSDE) “ named CLARISSE, which allows developing a complex multi-unit processing system. CLARISSE is standardised and is delivered as an independent software package. It provides the software tools a libraries needed to perform *SPINLINE 3* configuration and the application software development.

Any *SPINLINE 3* software is a combination of two parts:

- The **system software** is standard and comes as a software component to be used on the CPU boards of the processing units. It is ready for use after a simple configuration to fit the needs of the customer I&C systems. It provides basic functions like communication, data acquisition or services to be used by the application software.
- The **application software** is specific and may be developed either by Schneider Electric, by an engineering company or by the customer himself.

The **system software** is a software layer with a minimum complexity that mainly achieves the interface between the local and remote data delivered by the I/O and communication link boards and the application software.

It also tests continuously the hardware and provides services to the application software.

The system software has been developed and validated according to nuclear standards for software based 1E safety systems, mainly CSN IEC 60880, CSN IEC 60880-2.

The adaptation of the system software to the application needs is done, using the processing units and networks configuration tool of the CLARISSE System and Software Development Environment.

The **application software** performs the functions linked with the functional diagram and the operation of the system.

The main features of the application software are the following:

- *Dataflow organization*: the program is entered as a set of boxes connected by wires, flowing from the input data on the left to the outputs orders on the right. The wires convey data according to data types; the boxes transform data by means of Boolean operators, numeric operators or by means of functions. All loops in the layout are precisely controlled using the „previous„ operator.
- *Top/down design*: The application program starts with an upper level view and proceeds through refinement steps for both the functions and the data. Relevant details are added at the appropriate level (information hiding concept).
- *Single task*: the application program associated with the system software runs as a single continuous program loop. One loop execution is called a scan. Every scan, outputs are computed from a fixed image of the inputs and from relevant results of the previous scans. There is no processing done under interrupt and no multitasking. These avoid potential deadlocks, resources sharing and overload problems. It helps demonstrating the fulfilment of the response time requirements as well as the simplicity of the software design.

- *Synchronous approach*: the application program is designed to meet the synchronous hypothesis i.e. the program shall react instantaneously to input events. The hypothesis is fulfilled when the processing is always performed within the scan time allocated to the unit. The *SPINLINE 3* CPU board offers enough computing power to fit the processing needs of typical I&C protection functions in the nuclear field. Moreover, the dataflow organisation of the program makes the CPU load quite independent from the actual values of the inputs.

The development of the **application software** takes place in a classical lifecycle-based development process, starting with system requirements and ending with validation and commissioning tests.

The software design and coding phases are made easier and safer due to the use of CLARISSE SSDE.

The main *SPINLINE 3* application software development benefits:

- There is no longer software design and coding phases involving manual and error-prone activities. The software architecture comes with the product with all the properties needed for the intended type of application (i.e. safety protection I&C).
- As the SCADE language is close to automatism, process engineers can easily review the unit functional specifications and hence, they can help getting the right functional specification even at the detailed software specification level.
- In order to fulfil specific functional requirements, the development of elementary functions, using a high level programming language is possible. The development of elementary functions is performed, using a dedicated V development-cycle on the CLARISSE SSDE.

The CLARISSE System and Software Development Environment (CLARISSE SSDE) are available for the specification, design, coding, and validation of I&C systems. It runs on a UNIX based workstation (typically a Sun SPARC station under OS Solaris). The CLARISSE SSDE provides the followings functions:

- Description of the I&C architecture and processing units: This description is used to automatically configure the system software, the networks stations and the messages exchanged among the units.
- Input have the I&C functions: I&C functions are described, using The SCADE formal language. This language provides block diagram formalism with a rigorous graphical and textual syntax and a well defined semantic. It is easy to learn and to use by technical staff involved in I&C project. SCADE is user-friendly and does not require specialized programming skills: the I&C application is described in the same way as non-software based automatism. The verification and validation process does not require software skills and is therefore simpler.
- Simulation of SCADE specification: the simulation is possible since the early phases of the application design. It allows designers to check the actual behaviour of their specification. The simulation capability can also be useful during the test and validation phases, to perform additional functional tests on the final specification.
- Automated code generation: The SCADE specification is translated into understandable C code. This C code is then compiled, assembled and link-edited. The resulting binary code is either downloaded to the target CPU boards (development phases) or loaded into read-only memory components (for operation). For safety purpose, on line downloading or modification of software is not possible on the units, once in operation. The software is secured in write-protected memory with both physical and electronic identifiers. During operation, only user-defined parameters, which have been declared as modifiable, can be changed, either locally or through a NERVIA communication.

- Verification and validation of each steps of the software design using appropriates tools.
- Documentation production: Most of the documentation is automatically generated.
- Software configuration management.

3.2 The Skoda Technology

3.2.1 The System

This system is an industrial microcomputer-based system with an user program support SoFIC (Software for Industrial Controller) implementing control algorithms primarily of logical and regulation character. The use of efficient communications enables to build remote complexes ranging from middle to large control systems.

The special parts of the system are units executing functions connected directly with the VVER reactor technology.

The system technology is designed such to meet requirements for long-term reliable operation, permanent keeping all functional parameters, easy operation and maintenance.

Methodology of the system design is in compliance with normal industrial standards meeting simultaneously requirements for the safety- related systems in NPP.

3.2.2 The Hardware

The hardware components are cabinets, racks, electronics modules and cabling accessories. Cabinets and racks are designed to withstand environmental influences as defined in relevant standards (including seismic, EMC etc.). Group control level processor module is based on Intel 486 processor. The module is provided with 16 MB RAM, 512 kB Flash EPROM and 512 kB SRAM. Individual control processor modules are based on Intel 80C196 series microcontrollers. Basic system communication is the RDD (Remote Distributed Data) communication based on a RS485 serial bus with the transmission speed of 0,5 MBaud. The message transmission is based on the „flying master – token passing access„ with the synchronous SDLC message format (secured by CRC). The RDD is deterministic broadcast type communication with redundant arrangement in critical applications.

3.2.3. The Software

The basic system software integrates environment for loading, saving, initiation, debugging and operating user control algorithms. Due to its design, the system software directly supports modular programming and enables the user to utilize resident library containing functional elements, blocks and services for communications control. The operation history oriented system seems to be an advantageous instrument, which enables the storage and reviewing of selected system and user defined events.

The system basic tool of application program module development is a language PL/C (Programming Language for Controllers) having features of higher structured program language. The PL/C language describes all program and data objects at a symbolic level. The PL/C language together with the system software architecture support the following main principles:

- Transparency of programming through structuring of user control tasks to modules.
- Symbolical handling with objects by using large resident library of functional elements, blocks and services.
- Predefined names of variables and constants having global validity in a specific controller (at the RDD communication at a specific network).

- System reliability supported by a development policy of the application software, system support security and testing as well as Watchdog system for system run security.

The process of the application software development complies with requirements of relevant standards (primarily CSN IEC 60880).

4. THE SAFETY

4.1 The Safety Of SPINLINE 3 System

One of the major interests of a *SPINLINE 3* systems is the high level reached regarding the safety performances. The safety is built from several fundamental characteristics: the Deterministic behaviour, the Separation between safety parts and the fully Safety oriented design.

4.1.1 Deterministic behaviour

SPINLINE 3 deterministic behaviour is a key feature in order to meet response time requirements and to avoid overload situations.

It is based on the following characteristics:

- Software units run cyclically and sequentially

  A unit cycle (scan) is composed of the following steps:
  - Self-monitoring,
  - Cycle time management,
  - Data acquisition,
  - Application processing,
  - Data output,
  - Local terminal management.

  The steps are always executed in the same order. The scan time of each unit is fixed and monitored, and then the unit response time is bounded and guaranteed.
- Software units do not make use of interrupt driven tasks or algorithms based on dynamic memory allocation.
- NERVIA networks run cyclically and sequentially
- A network cycle (scan) consists in:
  - A token is circulated through all the network stations according to a pre-defined order,
  - A station is allowed to transmit its data on the network only when it owns the token and within a specified time window.

  The network response time is bounded and guaranteed The scan time of each network is fixed and monitored. The network stations are always scanned in the same order.

- Exchange of data among units through networks are pre-defined and systematic:
- All inter units data exchanges are configured in fixed tables.
- System response time. The maximum response time for a system is established using the max response time of each units and networks. The *SPINLINE 3* determinism guarantees that I&C outputs will always be delivered within the computed maximum response time limit.

4.1.2 Separation

The separation between redundant divisions or channels is achieved by separate locations for redundant parts of the equipment and electrical isolation for communications.

Using some specific features performs the functional separation between units regarding the communications:

- Inter-units communication through NERVIA networks, using optic fibres implements electrical separation and geographical separation within the plant.
- Asynchronous behaviour of units and networks neither at the hardware level nor at the protocol level. This avoids the risk of multiple units hangs due to the failure of a single unit or network. The operation management of redundant units is easier thanks to the fact that networks work independently of the status of the connected units and units work independently of the status of the connected networks.
- "1E units / non 1E units" are separated:
  - Non-1E units shall be clearly separated from 1E units. Nevertheless, non-1E units may have to exchange data with 1E units. *SPINLINE 3* makes it possible, thanks to the safety properties of the NERVIA network. These properties ensure that non-1E units can never prevent 1E units from performing their safety function.
  - Non-1E units may act as observers only: These units can only read the data available on the network but they cannot emit data on the network. They cannot interfere with the 1E functions.

4.1.3 Safety Oriented Design

SPINLINE 3 hardware and software components have been designed specifically to design safety I&C systems. They include appropriate features to defend (i.e. detect and act) against failures, which may occur inside the system, due to causes coming from inside or outside the system. *SPINLINE 3* safety-oriented features are given hereafter:

- Each data processed by SPINLINE 3 is associated with „validity„ information.
- Each unit monitors its related units and networks and takes appropriate actions in case of failure or error detection.
- Output controls from the system are set in a safe status in case of internal hardware failure detection, loss of power supply, or detection of IC scanning disruption,
- The CPU clock is monitored against possible frequency drift.
- The system software includes appropriate defensive programming to make sure that there are no inconsistencies in the control and data flows. The detection of any inconsistencies would result in a CPU stop.
- The application software can include consistency checks and properties assertions in order to defend against possible design or operation faults.

4.2 The Safety of Skoda Technology

The system design of the SKODA technology includes in principle the same characteristic as the SPINLINE 3 system.

The deterministic behaviour is the fundamental system characteristic and to be attained, basically the same means are used as with the system SPINLINE 3.

Though the system separation is not designed in such a range as required for safety systems, all I/O signals are galvanically separated inclusive redundant system communications. Signals representing connection links to the safety system are galvanically isolated even between each other.

Within the system design, also principles supporting achievement of maximum safety behaviour of the system in the event of detection of failure in input data or proper failures are incurred.

5. INTRODUCING THE NEW SAFETY SYSTEMS FOR DUKOVANY PROJECT

The main motivations for the replacement of safety I&C systems are the following:

- Availability of spare parts
- Improvement of safety by implementation of new functions
- Consistency with international standards
- Reduction of the costs of plant operation

The objectives of such a modernisation are the following:

- To guaranty performances in term of safety, reliability and technical performances. This implies the use of a qualified system with adequate features like redundancy and diversity.
- To reduce the number of sensors.
- To reduce the time between periodic tests.
- To minimise the costs for maintenance: powerful diagnostic functions to simplify the time to repair and a short time to perform the periodic tests.
- To be adaptable with the existing installation. It means to be compatible with the parts of the existing system, which are not modernised.

5.1 The existing systems to be modernised

The existing systems (important for safety, categories A and B) to be modernised are the following:

- EX-CORE: The Nuclear Instrumentation System corresponding to previous AKNT
- RTS: The Reactor Trip System corresponding to the HO-1
- ESFAS: The Emergency Safety Features Actuating System corresponding to the SOB
- RLS: The Reactor Limitation System corresponding to the HO-3 and ROM
- RCS: The Reactor Power Control System corresponding to the ARM
- RRCS: The Reactor Rod Control System corresponding to the control part of SORR
- ELS: The Emergency Load Shedding corresponding to the APS
- SAS: The Support Action System corresponding to the TOPG

Additionally, a new system PAMS, Post Accident Monitoring System will be introduced (as the category A) on the basis of the FRAMATOME/VME technology.

Also the systems of category C are modernised by computer – based technologies, but are not described in this paper. There are namely:

- SGPS: Steam Generating Protection System corresponding to the LOPG
- PCS: Process Computer System corresponding to the URAN
- IN-CORE: IN-CORE Measurement System corresponding to the SVRK (Hindukus)

5.2 The CONCEPT, main requirements

The design of the new system is based on fundamental requirements, which are the results of a safety analysis performed under the supervision of •EZ technical team. Some of the most important requirements are the following:

- Three divisions instead of two for the reactor trip
- Integration of trip and ESFAS
- Sharing the sensors between the different systems (RTS, ESFAS, PAMS etc.) and sharing digital outputs between the three divisions.
- Taking into account the need for diversity to reduce the risk of Common Mode Failure.
- The cabling to the actuators is kept, including the 220Vdc for control
- Installation to be executed during normal outages
- Parallel operation of new safety systems during one year
- All the safety sensors and their cables are replaced
- Limited number of modifications in control rooms and new procedures

5.3 Building the architecture of the new system

The new safety system is built by following a classic method, starting from the protection functions: These functions concern the trip and ESFAS. Two levels are considered:

- The acquisition and processing level
- The voting and actuation level

Acquisition and Processing level: Acquisition, digitalisation and processing the parameters in three independent divisions. The Digital Instrumentation System (DIS), which receives all the measurements, covers this level: The functions of the DIS are the following:

- Acquisition and digitalisation of signals from sensors: this includes:
  - Temperatures (TCs and RTDs)
  - Pressures, levels, flows
  - Neutron measurements (pulses and wide range current)
  - Binary inputs from switches
- Processing the signals to make calculations and comparison to setpoints
- Transmission and communication between the units by using NERVIA, a network designed to achieved the safety requirements in NPPs.
- Communication with external systems based on an open industrial network, typically Ethernet.

Voting Logic and Actuation level: Inside each division, equipment performs a 2oo3 voting logic and produces controls for all safety actuators and for the trip system. This level is covered by the Digital Reactor Protection System (DRPS). Actuator signals are treated with a high level of reliability by using a dual control concept to reduce the risk of spurious actuation and to allow the test during the operation.

Communication between safety units is based on three independent safety networks (NERVIA) based on a fibre optic technology, one for each division transmit the results of the comparison to the setpoints from the processing level to the actuation level. These networks are also used to send data to other systems, including to the PCS computer via two gateways: the Interface and Display Management System (IDMS).

To improve the resistance to the risk of Common Mode Failure, diversity is implemented.

- Each PIE is addressed by two parameters, each processed by two separate digital units, giving two Lines Of Protections (LOP A and LOP B). That is why inside each division, four digital units process all the parameters needed for TRIP and ESFAS.
- Each division of the DRPS is divided in two sets. Both sets control the ESFAS actuators of the division. Each set of a DRPS division controls respectively a set of TRIP breakers performing a 2oo3 voting logic from the three divisions. This structure provides a diverse protection system.

A specific NERVIA network connects the three DRPS divisions to the IDMS in order to transmit the internal parameters for diagnostics, supervision or transfer to the Process Computer System (PCS).
The role of the power supply to guarantee the ESFAS actuation is fundamental. To respect the original design, each division has an Emergency Load Shedding System (ELS) to start a diesel generator.
To limit the number of reactor trips, each division is equipped with a Digital Reactor Limitation System, separate from the DRPS but located in the same cabinets.
Two other systems are connected to the protection system: The technological protection of steam generators and its peripheral functions are included in the SAS function. The Reactor Control System (RCS) performs the regulating function to operate the reactor in a predefined diagram according the power of the reactor. This system replaces the existing ARM function.

Optimised structure of a new **Reactor Rod Control System** (RRCS) is a result of functional analysis and arrangement of the existing equipment. The RRCS is divided in two basic levels:

- The level connected with reactor drives consists of Motor control cabinets connected to motors (drives) of control rods and Position evaluation cabinets connected to LD-1 sensors. Also Position rough indication cabinets located on the main and emergency control rooms belong to the level.
- Control and information level consists of Group and individual control cabinets, Monitoring and diagnostics cabinets and equipment of Operator's console.

Cabinet arrangement and subsystems housed therein are performed in such a way that dimensions of the new cabinets comply with initial dimensions of cabinets and contain identical number of subsystems performing the same basic functions as the original systems providing, however, all advantages of the modern technology. Using this experienced approach when replacing the original system with new one provides for quick and safe implementation even during such short time as planned (only outages for refuelling).

Individual subsystems are interconnected by redundant communication links RDDCU ŠKODA (RS485 Interface). Communication system contains three independent redundant lines.

5.4 Operation of the new safety systems

The technology of **SPINLINE 3** offers various possibilities to support the operation of the system:

- **On-line diagnostics** to identify and locate all detected failures. This function allows a short time to repair the system.
- **Test without stopping the operation**: Due to the architecture of the system, the test of a unit inside a division is possible by keeping the division in operation.
- **The use of Automatic tester** gives a great advantage to reduce the costs for maintenance. The tester is based on a computer, which manages some specific interface components or modules to generate test signals, which replace the input signals of the tested unit.
- **First cause identification**, this function is important to address the time sequence of an accident for analysis. It is performed in the IDMS to select the first decision to start a protective action.

- **Display management.** The system is able to manage the displays in the Main Control Room and in the Emergency Control Room.

The **RRCS system** performs the following main functions during operations:

- **Control rods movement** (manual/automatic mode)
- **Control rods position** measurement and indication
- **Individual and group rods control**

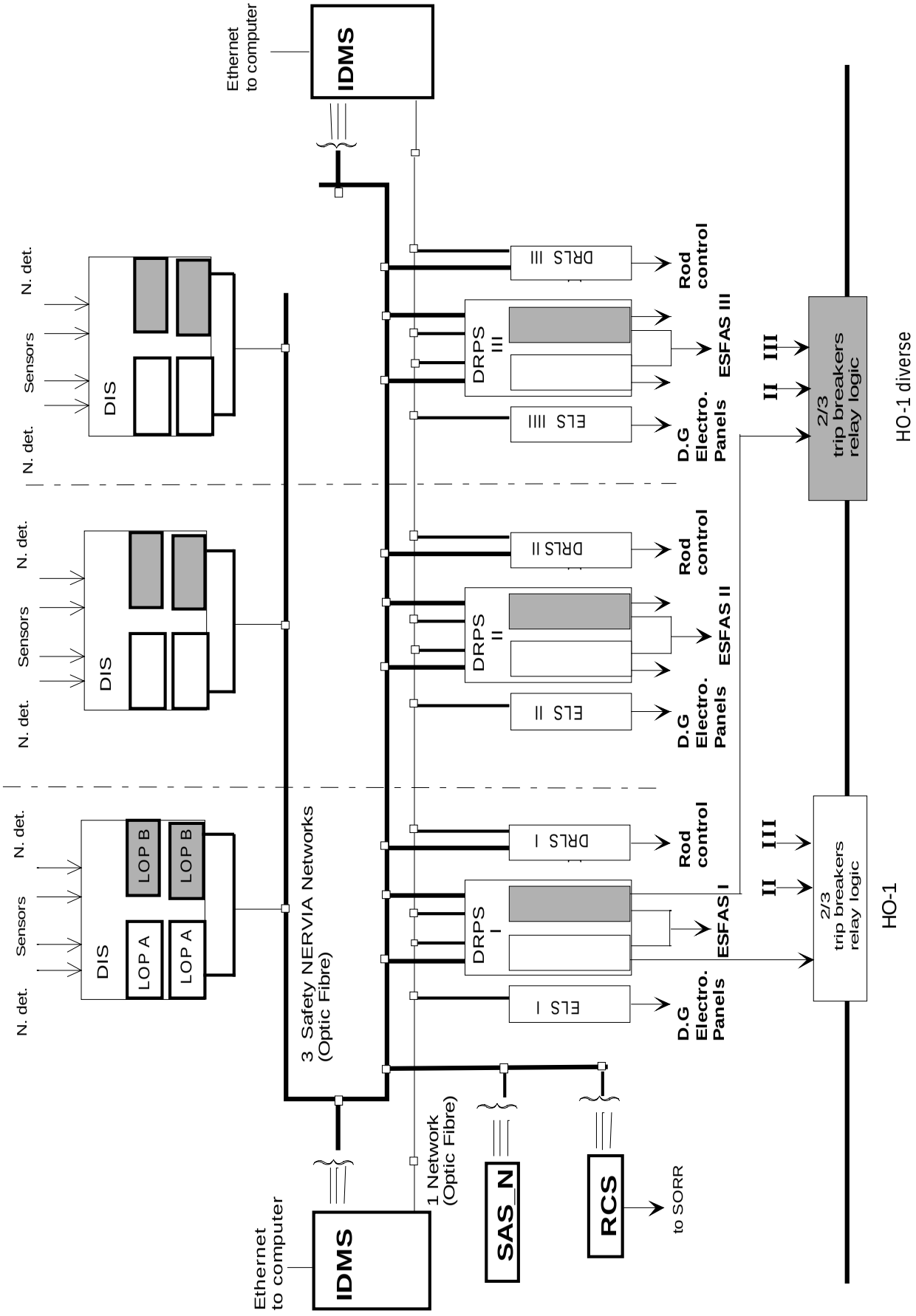
  One part of RRCS is dedicated to measure and monitor other important internal signals for diagnostic and maintenance purposes. In this case it possible to perform following additional functions:
- **Failure detection and its signalisation** occurred within the RRCS system and received either by means of binary inputs or via communication links from other parts
- **Collection, pre-processing and displaying** of measured data and control signals
- **Archiving of selected data** and failure reports
- **Display, evaluation and archiving** of important data while testing individual derives or driving groups on the reactor
- **Test report** printouts
- **Checking for functionality** of all microprocessor units of the RRCS system through data verification procedure
- **Sending failure** signals to MCR
- **Display of data tables** received from individual parts of the equipment as per operation personnel choice

6. CONCLUSION

The project of I&C modernisation in Dukovany NPP is in progress. The new safety systems are based on the latest technology developed by Schneider Electric in co-operation with Framatome ANP to produce any kind of safety systems for NNPs.

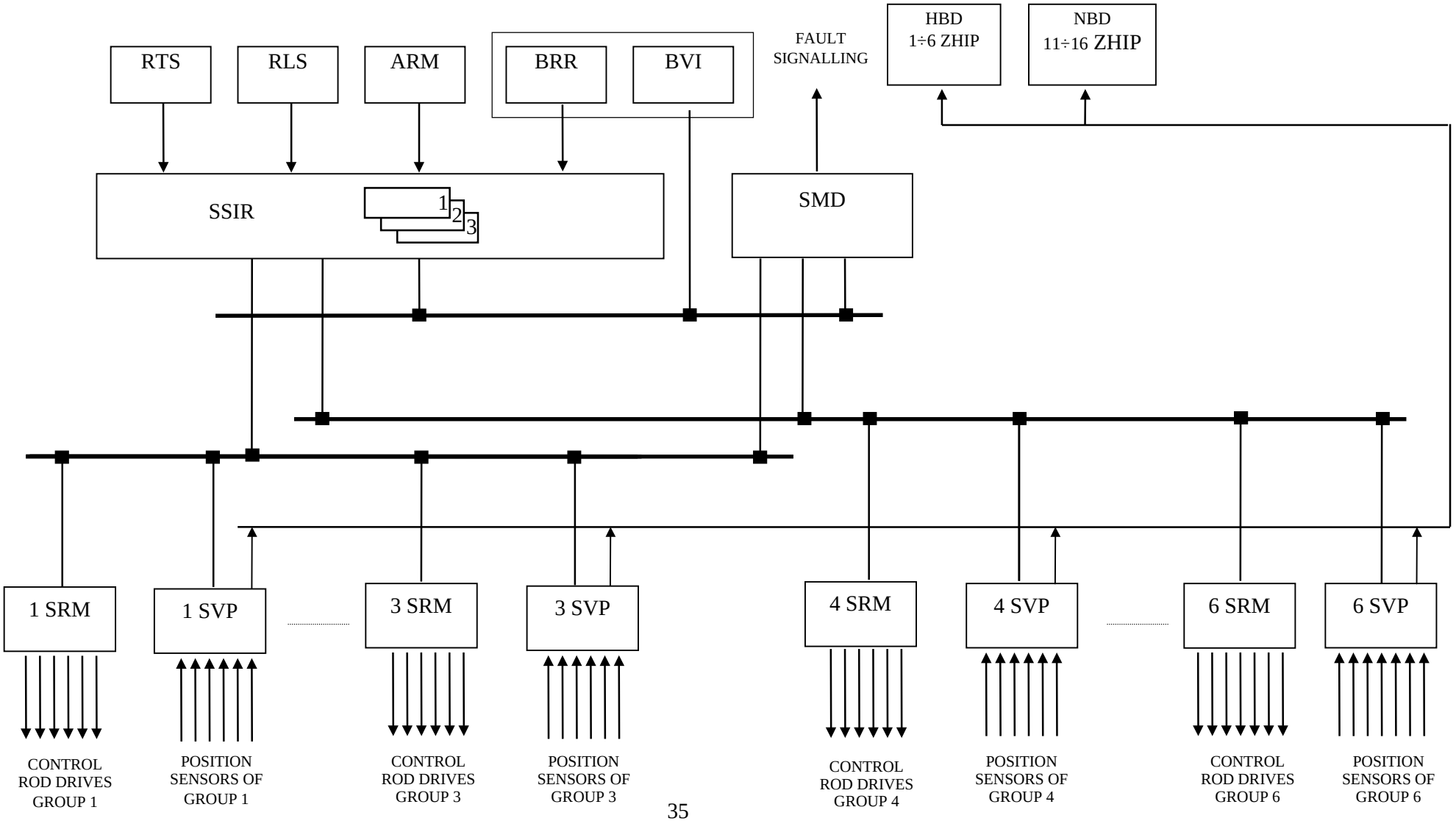
The RRCS as a system important for safety is based on the industrial state of the art system proven for five years on several Nuclear Power Plants of VVER type.

The detailed design is starting and the first system implementation on site is planned to be done in 2003.
The new system will be operated in parallel with the existing system between 2004 and 2005.
The final operation with the new system on the first unit will start in 2005.
The last unit will be modernised in 2009.



GENERAL ARCHITECTURE OF THE SPINLINE 3 SYSTEMS

GENERAL ARCHITECTURE OF RRCS system



FMEA Performed on the *SPINLINE3* Operational System Software as part of the TIHANGE 1 NIS Refurbishment Safety Case

L. Ristord [1], C. Esmenjaud [2]

[1] *Schneider Electric Industries M3 38050F Grenoble France*
Tel.: +33 476 606 827, Fax: +33 476 606 462, e-mail:laurent_ristord@mail.schneider.fr

[2] *Schneider Electric Industries M3 38050F Grenoble France*
Tel.: +33 476 605 860, Fax: +33 476 606 462, e-mail:claude_esmenjaud@mail.schneider.fr

Summary

This paper introduces the SPINLINE3 technology and TIHANGE 1 the NIS project.
It then focuses on the specificity of FMEA performed on software. It points out the benefits of this analysis and also some of the limitations and possible developments. It also gives characteristics that, if present in the software, help the analysis and the defenses.

It takes as an example the analysis performed on the Operational System Software of the Schneider Electric safety digital generic platform SPINLINE3.

Introduction

Schneider Electric has been designing and manufacturing I&C solutions dedicated to the implementation of safety and safety related functions in nuclear power plants for more than 25 years. The first solutions were non software-based. Since 1980, software-based safety solutions have been successfully developed and used.

Building on the I&C components developed for the EDF N4 1450MW PWRs, Schneider Electric and Framatome have developed a safety generic digital platform called *SPINLINE3*, dedicated to the implementation of safety I&C functions in new plants or for the refurbishment of safety equipment in existing plants. *SPINLINE3* has been available since 1997 and has been successfully used to implement category A safety functions on several projects for new reactors as QINSHAN phase II PWR plants in China and for refurbishment projects as KOZLODUY VVER plants in Bulgaria, and FESSENHEIM and BUGEY 900MW PWRs in France. *SPINLINE3* has been chosen to refurbish the TIHANGE 1 Nuclear Instrumentation System (NIS) and the safety I&Cs at the four DUKOVANY VVER 440/213 units.

The architecture of most of the safety systems implemented by Schneider Electric and Framatome includes a redundancy of identical I&C channels, i.e. using the same hardware and software design. When performing safety analyses on such architectures, software is identified as a potential source of Common Cause Failure (CCF).

Defense against CCF due to software within one system is usually based on diversity measures taken at plant or system level or on reliability of the software at system level. Where the “software reliability” argument is claimed, the demonstration shall provide sufficient evidences that the software is free of defects that could lead to CCF. The claim of “error free” software is generally not possible to demonstrate, due to impossibility of exhaustive testing and limitations within formal proof processes.

Performing a FMEA on the software is a mean to narrow the scope of the demonstration by finding out the software components that may, if faulty, lead to a CCF. It is then easier to show, either that those software components are error free or that the postulated component failure modes will be detected and will lead to a safe position. This analysis has been performed on the Operational System Software and on the Application Software for the new TIHANGE 1 Nuclear Instrumentation System (NIS).

Main features of the SPINLINE3 technology

Introduction

Nuclear safety I&C systems have to meet demanding functional and non-functional objectives. They need high reliability and quality of components as well as good properties of architectures such as deterministic behavior, fail-safe and fault tolerant features, functional diversity, and separation. Furthermore, these systems should avoid unnecessary complexity and prevent when possible, operator and maintenance errors. In addition, safety I&C systems shall meet the other customer expectations such as modularity, scalability, flexibility, ease of operation.

Th*e SPINLINE3* technology possesses the features essential to design and implement safety I&C systems fitted to the customer requirements and compliant with national and international nuclear standards and regulations.

SPINLINE3 concepts and design criteria

SPINLINE3 provides a set of mechanical, electronic and software components consistent with the following concepts and design criteria:

Deterministic behavior

SPINLINE3 architectures are designed using two kinds of basic components: Processing Units (PU) and data links. Theses basic components are combined to implement multi channel architectures with distribution of treatments and redundancy of data links where relevant in order to meet the functional and non-functional requirements. The properties of the processing units and data links ensure a deterministic system behavior with bounded response time for the functions under any load conditions.

*SPINLINE*3 architectures may be modeled as a set of synchronous (i.e. cyclic) components exchanging data through non synchronized interfaces. The European project CRISYS (CRitical Instrumentation and control SYStem) has shown that, for application functions such as those needed for reactor protection, a *SPINLINE*3 architecture has the same deterministic behavior as a single synchronous processing unit.

Failsafe and fault tolerant features

SPINLINE3 failsafe and fault-tolerant features allow the design of I&C systems compliant with the single failure criteria. Failsafe features are part of the component design. For instance, to control trip and ESFAS safety actuators, *SPINLINE3* provides actuators boards with 2oo2 votes between two processing units. Any detected failure within the board itself or in the related processing units will result in a predefined output toward the actuator. Fault tolerance features include both fault detection mechanisms within and outside the basic components, and the ability to design adequate redundancy in the system architectures.

Functional diversity

SPINLINE3 features ease the implementation of functional diversity, by allowing distribution of diverse treatments in separate processing units. The high quality of *SPINLINE3* hardware and software components makes other types of diversity non necessary, resulting in systems simpler to design, operate and maintain.

Physical and functional separation

SPINLINE3 data links are mainly implemented through safety networks: *NERVIA* networks and *ACTUATOR* networks. The use of optic fiber allows implementation of clear geographical and electrical equipment separation within one system and between systems. The *NERVIA* network can link 1E units and non-classified units implemented for instance in industrial PCs. The *NERVIA* protocol ensures that any unit on the network can read data from data areas of other units but can only write in its own data area. Therefore, a non-classified unit cannot do unintended changes in a classified one.

SPINLINE3 technology

SPINLINE3 is mainly based on microprocessor technology. The application functions are basically implemented by means of application software programs running on the microprocessors of the processing units. Microprocessor capabilities are also used within *SPINLINE3* components when relevant for acquisition and output of data, hardware self-testing, HMI and network protocols. *SPINLINE3* components include also non-microprocessor-based components like pulse and low current amplifiers for neutron detector input conditioning. It also includes a set of mechanical components such as cabinets, racks and cabling systems fitted to NPP's requirements. (See [4] for further details)

Software components

- A low complexity and standardized software component, the Operational System Software, comes with each processing unit and provides within an infinite single loop, the following functions: hardware tests, cycle time management, data acquisition, call to application software, data output, HMI management.

- The application software is dedicated to the customer needs. It is derived from the requirements and expressed as functional block diagrams, using the System and Software Development Environment. The application software may call pre-existing components from a qualified library.

System and Software Development Environment

The System and Software Development Environment (SSDE), named *CLARISSE*, include the following activities: (see [4] for a full list of features)

- description of the I&C architecture, processing units configuration, input/output with sensors and actuators, data exchanged between processing units,

- description of the I&C functions, using the *SCADE* tool. *SCADE* provides a functional block diagram language with a formally defined graphical and textual syntax and semantic. It is easy to learn and use by technical staff trained in I&C process. *SCADE* does not require specialized software programming skills and helps achieving the consistency and completeness of the descriptions,

- automated generation of the executable code. The *SCADE* diagrams are translated into high quality C code, then compiled and link-edited with relevant libraries. The resulting binary code is identified, and secured in read-only memory for operation,

Software qualification

The *SPINLINE3* software components intended to run within safety processing units or networks have all been developed and qualified according to IEC60880. They are fully documented and reviewable [5] by licensing bodies, under contractual agreement with confidentiality clauses. The re-usability of the Operational System Software component makes possible additional arguments based on feedback of experience.

The TIHANGE 1 NIS refurbishment project

Background

The non-digital TIHANGE 1 NIS I&C system has been replaced by a digital equipment which had to meet the same physical and functional requirements.

The NIS architecture

The TIHANGE 1 NIS is composed of four cabinets, one for each protection channel (See figure 1).

The Source, Intermediate and Power range functions are performed within separate processing units distributed in four physically and electrically independent cabinets.

Each cabinet hosts one power range processing unit and either a source range or an intermediate range processing unit as follow :

- cabinet L1 : Power + Source
- cabinet L2 : Power + Intermediate
- cabinet L3 : Power + Source + Reactivity unit (non 1E)
- cabinet L4 : Power + Intermediate + Monitoring unit (non 1E)

Two Nervia networks link units of cabinets 1 and 2, and units of cabinets 3 and 4 to the non 1E Reactivity and Monitoring units

A mobile automatic testing unit has been also provided. It can be plugged to only one processing unit at the same time and only for the periodic testing session of this unit.
As in the former non software-based NIS, Source range processing units, Intermediate range processing units and Power range processing units are redundant and identical.

The main benefit of this architecture is its simplicity and its low cost. A drawback is the sensitivity to software common mode failure and more generally to design common mode failure.

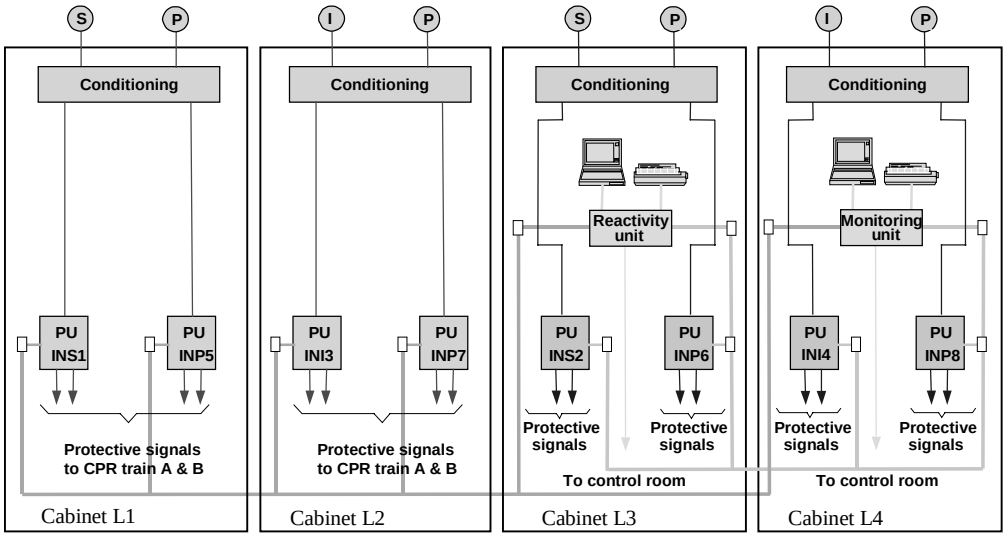


figure 1 : Tihange 1 NIS architecture

The Tihange 1 NIS software

Each 1E classified processing unit is composed of standard *SPINLINE3* hardware, the standard Operational System Software, parameterized according to the Source, Intermediate or Power Input/output requirements, and a dedicated application software.

The *SPINLINE3* Operational System Software has been developed and validated to IEC 60880 requirements previously to the Tihange 1 project. It is a standardized pre-existing software component of the *SPINLINE3* solution.

The application software for the Source, Intermediate and Power range processing units have been developed to meet the functional requirements of the Tihange 1 NPP. The requirements have been derived from the former Tihange 1 NIS and translated into Functional Block Diagrams (FBD) by Framatome. Then, the software have been developed and validated by Schneider Electric, using the CLARISSE System and Software Development Environment and the SCADE design language.

Requirement for software free from errors leading to SCCF

For the Tihange 1 project, we have been required to demonstrate that the software is free from errors which could lead to Significant Common Cause Failures (SCCF), i.e. common cause failures of the NIS that could lead to an unsafe situation of the plant.

It has been recognized that the methods and tools used for the software development and V&V, the respect of the requirements of IEC 60880, the experience of the software teams were suitable to produce software “as error free as possible”. This has been proven by the feedback of experience gained on similar projects that we have developed during the last 20 years. We have nevertheless been required to perform an additional analysis on the 1E software, using an FMEA technique, in order to identify those parts of the

software which, if faulty, could lead to SCCF and to provide additional evidences that theses parts are free from theses faults.

In the next section of this paper, we introduce the principle of the FMEA performed on the Tihange1 software and discuss some of the results found, using this technique.

Principles of the Software FMEA performed for the Tihange 1 project

Introduction

Definitions of « failure mode and effects analysis »

"The Failure Mode and Effects Analysis (FMEA) is a systematic, bottom-up method of identifying the failure modes of a system, item, function and determining the effects on the higher level. It may be performed at any level within the system (e.g., piece-part, function, blackbox, etc,). Software can also be analyzed qualitatively using a functional FMEA approach. Typically, a FMEA is used to address failure effects resulting from single failures" [1]

The Failure Mode and Effects Analysis (FMEA) is a "Qualitative method of reliability analysis which involves the study of the failure modes which can exist in every sub-item of the item and the determination of the effects of each failure mode on other sub-items of the item and on the required functions of the item." [2]

Particularities of FMEA performed on software

An FMEA may start from any level of design provided that it defines identified components with understandable failure modes. It is then possible to find the consequences of the failure of the components at system and/or plant level. It should be also possible to find out and understand the causes that may lead to these failure modes.

When performing an FMEA on mechanical, fluid or electrical system, failure modes of components such as pipes or resistors are generally understood, likely to happen and their consequences may be studied. A component is supposed to fail, due to some reason as wearing, aging or unanticipated stress. The analysis may not always be easy, but at least, the safety engineer can rely on data provided by the component manufacturer, results of tests and feedback of experience when available.

When performing an FMEA on software, very few information or support is available. The safety engineer has to apply his own knowledge of software to set up an FMEA approach, i.e.:

- to find out the appropriate starting point for the analyses,
- to set up a list of relevant failure modes,
- to understand what makes those failure modes possible or unlikely (the causes) and what are the consequences.

When Common Cause Failure is not a concern due to the use of diversity, the software failure modes can be considered at processing unit level only.

A list of five general purpose possible failure modes at this level has been given in [3] :

(a) - the operating system stops
(b) - the program stops with a clear message
(c) - the program stops without clear message
(d) - the program runs, producing obviously wrong results
(e) - the program runs, producing apparently correct but in fact wrong results

For a 1E I&C software such as the Tihange 1 software, developed with the *SPINLINE3* technology, failure modes (a), (b), (c) will lead to a safe state, whatever the causes could be, even if such failure mode should be avoided as far as possible.

Failure modes (d) and (e) may or may not lead to SCCF, depending on the cause :

- if the cause is a software fault, activated by a hardware failure, sensor failure, or human error within one channel, the failure mode is unlikely to be a CCF or a SCCF, due to the redundancy.
- if the cause is a software fault activated by an operational condition, the failure mode will be a CCF and could be a SCCF if it happens to prevent the performance of a required safety action.

Principles of software faults and software failure modes

A software component designed and coded either manually or with the help of tools may be subject to a wide variety of faults. The root cause of these faults is to be found in the specification, in the design or in the implementation. A software fault can be seen as a deviation in the content and/or in the order of instructions or data stored in memory causing the microprocessor not to behave as expected under some event or sequences of events. Trying to consider all possible faults that could affect even a simple software component is not practicable. Nevertheless, it is possible to consider the consequences of such faults, as they will lead to a few numbers of software failure modes

Differences between hardware and software FMEA

Hardware FMEA

- may be performed at functional level or part level
- applies to a system considered as free from failed components
- postulates failures of hardware components according to failure modes due to aging, wearing or stress
- analyses the consequences of theses failures at system level
- states the criticality and the measures taken to prevent or mitigate theses consequences

Software FMEA

- is only practicable at functional level
- applies to a system considered as containing software faults which may lead to failure under triggering conditions
- postulates failures of software components according to functional failure modes due to potential software faults
- analyses the consequences of theses failures at system level
- states the criticality and :
  - describes the measures taken to prevent or mitigate theses consequences,
  - or shows that a fault leading to the failure mode will be necessarily detected by the tests performed on the component,
  - or demonstrate that there is no credible cause leading to this failure mode, due to the software design and coding rules applied

Application to the Tihange1 software FMEA

SPINLINE3 software components relevant for FMEA

The *SPINLINE3* software is composed of Blocs of Instructions (BIs) executed sequentially.

- BIs are either "intermediate" – they are a sequence of smaller BIs – or "terminal" – they cannot be decomposed in smaller BIs.
- They have only one "exit" point. They produce output results from inputs and possibly memorized values. Some BIs have direct access to hardware registers.
- They have a bounded execution time (i.e. the execution time is always smaller than a fixed value).
- They exchange data through memory variables. A memory variable is most often written by only one BI and may be read by one or several BIs.

SPINLINE3 BIs do not implement dynamic resource allocation algorithms which could lead to dead-lock situations and Interrupts are not used

Figure 1 shows the first levels of decomposition of the software of a processing unit

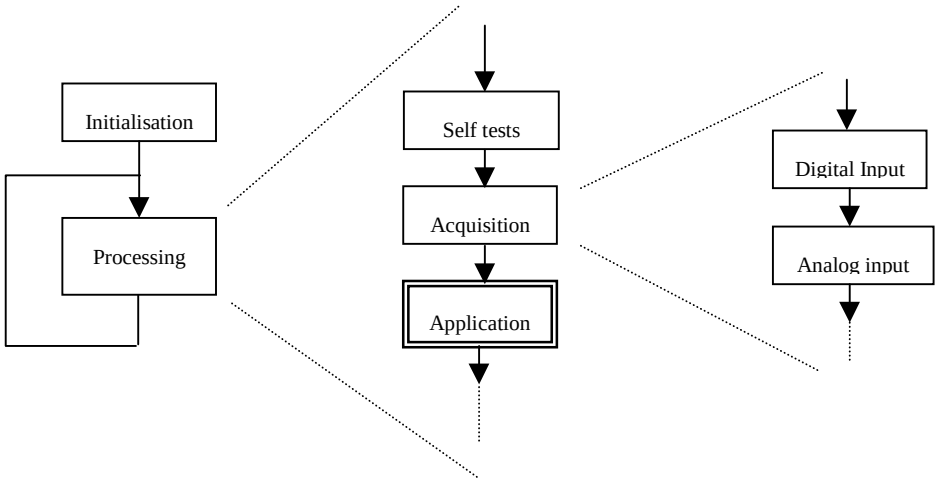


figure 1 : firsts levels of the BI decomposition of a *SPINLINE3*

The block of instruction "Application" is itself a sequence of BIs, derived from the application functional block diagrams or from the SCADE diagrams.

The other blocks of instructions belong to the *SPINLINE3* Operational System Software.

Definitions of software failure modes in the context of SPINLINE3 software

The BI is the basic component used for the software FMEA
The correct behavior of a BI is characterized by the following:

1. the BI execution ends at its "exit" point

2. the BI execution time is bounded. The execution time may be different from one execution to another, due to possible different control flow paths within the BI.

3. the BI performs the intended actions and does not perform unintended actions

   3.1 it provides the expected outputs

   3.2 it does not modify variables that it shall not modify

   3.3 it interacts as expected with I/O boards

   3.4 it interacts as expected with CPU resources

   3.5 it does not modify code memory and constants

The BI failure modes are derived from the definition of this correct behavior:

1. the BI execution does not ends through the “exit” point

2. the BI execution time does not meet time limits

3. the BI does not perform the intended actions or performs unintended actions

   3.1 it does not provide the expected outputs

   3.2 it modify variables that it shall not modify

   3.3 it does not interact as expected with I/O boards

   3.4 it does not interact as expected with CPU resources

   3.5 it modify code memory or constants

Software FMEA process

The following process has been chosen:

Generic analyses have been performed, considering software components of BI type and SPINLINE3 characteristics for all failures modes but 3.1

Dedicated analyses of the SPINLINE3 Operational System Software and of the Tihange 1 application software have been performed, at the functional level for failure modes 3.1 and some aspects of failure modes 3.3 and 3.4. The functional level has been found equivalent to the high level BI decomposition, and easier to analyze.

All failure mode found to be a CCF have been considered as potential SCCF (worst case).

Issues raised have been solved by complementary analyses, based on the detailed implementation of the software.

Examples of analysis and results obtained by the FMEA

Example 1: failure mode "bi execution does not meet time limit"

SPINLINE3 software is such that:
- output boards shall be periodically refreshed, otherwise a watchdog switches the outputs to a safe position
- the processing unit cycle time is regulated. If the associated timer is exceeded when the regulation test is executed, it causes the unit to stop and consequently, the output boards watchdogs to react.

The possible situations caused by the failure mode are :
- the execution time of the BI is "infinite" and causes the output boards watchdogs to react => safe position,
- the execution time of the BI is "infinite" and the output boards are still refreshed (i.e. there is an infinite loop involving an output module) => **potentially unsafe situation,**
- the execution time of the BI is not "infinite" and causes an overrun of the unit cycle time : the unit stops => safe position,
- the execution time of the BI is not "infinite" and does not cause an overrun of the cycle time : no consequences.

The second situation has led to a further analysis of the loops within the Operational System Software in order to show that this situation cannot happen. In addition, a list of the Technical and Quality Assurance measures taken to avoid or detect this failure mode has been established.

Example 2: failure mode 3.1."BI does not provide the expected outputs "

Introduction

The example is about the Acquisition Functional Block of the *SPINLINE3* Operational System Software.

The acquisition function accesses the input boards through hardware registers or shared memory. It delivers the values to the application software, with a validity bit set to "true" if the input values are "ok" and set to "false" if either a sensor or the input board itself is faulty

The analysis is reported in the following array

Failure Mode	Local effect	System effect	Criticality	SCCF	Prevention/comments
1	2	3	4	5	6

1. failure mode description
2. effect at first level
3. effect at NIS system level
4. criticality : C : high, CM : limited, NC : low
5. SCCF : Significant Common Cause Failure at NIS level
6. if SCCF, measures taken in order to be sure that the failure mode cannot happen (no software fault) or will be detected and lead to a safe position.

Sample of the analysis

Failure Mode	Local effect	System effect	Criticality	SCCF	Prevention/comments
1. - acquisition block provides values with invalid status when they are valid hardware is ok	correct values are transmitted to application software with invalid status	application software processes validity bit and take safe behavior	NC		
2. - acquisition block provides values with valid status when they are invalid hardware is not ok	invalid values are transmitted to application software with valid status	risk of unsafe outputs	C	no	This failure mode is activated by a random hardware failure in one unit. It is not considered as a SCCF
3. – acquisition block provides erroneous values when they are valid hardware is ok	erroneous values are transmitted to application software with valid status	risk of unsafe outputs	C	yes	Digital boards: software processing is independent from the input values. – test of each input with values 0 and 1 Analogue boards: software processing is independent from the input values. - test of each input with several values, checking that others inputs are not changed. Range checks performed by the application may detect this failure mode
4. - acquisition block provides erroneous values when they are invalid hardware is non ok	erroneous values are transmitted to application software with invalid status	application software processes validity bit and take safe behavior	NC		

figure 3 – sample of FMEA of the Acquisition Functional Bloc

Comments

The analysis is dedicated to software components. The postulated failures of these components are supposed to be caused by software faults present in the components, triggered by external conditions. In the example, the status of the input boards (hardware ok or non-ok) is one of these conditions. Other possible conditions may be sensors input values, operator interfaces, operating modes.

Comments on failure modes 1 and 3: hardware ok. The correct behavior of the acquisition function is to access the input board and to return correct data with a validity bit set to “true”. These failure modes state that the acquisition function acquires data from a non-faulty input board but because of software faults, provides erroneous output to the application software, resulting in situations 1 and 3. In situation 1 the validity bit is erroneously set to false; the application software assures the safe behavior of the unit In situation 3, the validity bit is correct but the data is erroneous. This situation is critical because the application software may behave in an unsafe way and is a SCCF because it may impact any units using this type of board, while in normal operation.

Comments on failure modes 2 and 4 : hardware non ok. The correct behavior of the acquisition function is to return a validity bit to “false”. These failure modes state that, because of software faults, the acquisition function provides an erroneous output to the application software, resulting in situations 2 and 4. Situation 2 is critical because invalid values are transmitted to the application software with valid status that may result in an unsafe behavior of the unit. It is not a SCCF because the software fault is triggered by a failure of the hardware that is unlikely to be simultaneously present on several units. Situation 4 is not critical because of the invalid status associated to the erroneous data.

Feedback of experience

Analyses oriented toward failure mode 3.1.“BI does not provide the expected outputs” performed on a software component are only functional for two main reasons: The first reason is the nature of software components, which are basically functions providing, outputs from inputs. The second reason is that all the possible functional failures shall be considered because, neither the possible failures of the underlying microprocessor and memories, nor the potential software faults can help restricting this analysis.

When the FMEA analysis is oriented toward the risk of SCCF, possible failures of the underlying hardware are taken into account by redundancies at system architecture and are not likely to cause SCCF, because of the random nature of theses failures.

Software faults may be SCCFs when the same software is used in identical redundant units in a system architecture as it is the case in the Tihange 1 NIS and when they are triggered by a condition common to all channels. For instance, a neutron flux going over a threshold limit. As we know that software faults can only be design faults, the best way – and may be the only way- to prevent software SCCF is to make sure that SCCF prone software components are “as error free as possible”.

Performing a software FMEA allows to:
- identify the SCCF prone software components in the software program
- cross-check the validation testing performed on these components. The validation tests give the assurance that known critical paths in the software are free from software faults
- find out what are the “defense in depth” measures to use in order to prevent or mitigate the consequences of a failure mode
- find out the technical and/or quality dispositions best suited to prevent the occurrence of classes of software faults which could lead to critical failure modes

The tests provided by the FMEA are not intended to be a proof that the software is free of SCCFs. They are not sufficient when testing is not exhaustive, which is the most frequent situation. They can only be used as a demonstration added to the technical and quality dispositions taken for the development and the V&V of the software.
These dispositions should be at a minimum compliant with the “shall” requirements of IEC60880 and preferably with most of the “should” clauses.

Lessons learned from the SPINLINE3 OSS software FMEA

The *SPINLINE3 OSS* is a pre-existing software component developed and validated according to IEC 60880.

The test cases given in the FMEA are a subset of the tests already performed during the validation of the OSS. No new test cases have been necessary. This is because the validation strategy and the FMEA are based on a functional approach, one consisting in a systematic testing of the functions of the software, the other consisting in finding ways to guarantee that critical failure modes of theses functions are unlikely to happen or mitigated.

Some tests cases have been done with more input values when practicable, in order to increase test coverage and confidence in the demonstration.

The FMEA has not caused significant changes in the development process and technical rules used to produce 1E software in our department. Rules for software fault prevention and mitigation were already defined in our methodology and have provided acceptable prevention for SCCF situations identified by the FMEA.

Performing the FMEA for the Tihange 1 project has proved to be a good way to discuss in depth safety aspects of software-based systems with our customer and with the licensing authority.

Conclusion

The New TIHANGE 1 Nuclear Instrumentation System successfully started operation on the beginning of Marsh 2001 after the plant outage, as planned at the beginning of the project. The choice of a software-based technology has raised the issue of the risk of CCF due to the same software being used in redundant independent units. Implementing functional diversity or equipment diversity has been considered but found either not practicable or of little value within this context.

The safety characteristics of the *SPINLINE3* solution and the stringent and proven safety software development process applied by the Nuclear department of the Schneider Electric company have made acceptable the principle of a design based on redundant identical processing units for this project. In addition, because of the possible consequences in case of the NIS not performing its protection function on demand, the licensing authority has required an FMEA oriented toward the SCCF risk as part of the safety case.

This FMEA has been performed on :
- the NIS architecture
- the *SPINLINE3* Operational System Software
- the three Tihange 1 application software (i.e. source, intermediate and power range)

The process used and the results have been elaborated by Schneider Electric and reviewed by the customer and the licensing authority all along the project development until final acceptance. Issues have been raised and answers and/or complementary analyses provided, some of them making direct references to the code itself.

In this paper, we have presented this software FMEA experience including:
- adaptation of the principles of FMEA to analyze a software program
- choice of a “block of instruction” (BI) approach to identify the components to analyze
- definition of the software failure modes associated with the BIs
- examples of the analyses performed on the *SPINLINE3* Operational System Software
- feedback of experience

References

[1] – ARP4761 – Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment – 1996 –§ 4.2 and annex G

[2] – IEC 60812, Ed. 2: Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)

[3] – A. Villemeur. - Sûreté de fonctionnement des systèmes industriels, Eyrolles, 1988

[4] – C.Esmenjaud, M.Prunier A.Parry - Use of the *SPINLINE3* generic safety digital I&C platform for the refurbishment of the French 900MW Nuclear Instrumentation System, NPIC&HMIT, Washington, DC, November 2000.

[5] - C.Esmenjaud, Reviewability guidelines for computer-based safety systems OECD/NEA – Munich 1996.

Qualification of Pre-Developed Software for Safety-Critical I&C Application in NPP's

M. Kersken[1]

[1] Institute for Safety Technology (ISTec), Garching
Tel.: +49 89 32004-546, Fax: +49 89 32004-300, e-mail: ker@grs.de

Summary

Implementations of I&C functions important to safety in nuclear power plants are increasingly realized with computer based systems, i.e. by its software. Often so called equipment families are used to develop these I&C functions. Besides a hardware platform, these equipment families provide pre-developed software in the form of basic components from which I&C functions can be composed by configuration and parameterization; but also larger components which have been developed by conventional software engineering, as e.g. operating systems, I/O drivers, self-supervision software, etc. are included. Outside the equipment families, it may be desirable to introduce also other types of pre-developed software, e.g. for simulation and for analysis purposes.

The assessment and qualification of software for computer based systems important to safety requires (as e.g. in IEC 60880) a set of detailed documents according to the development steps of the software life cycle. For pre-developed software the amount of documentation available and its detail will not be sufficient in most cases. On the other hand, the pre-developed software may have been operating in many applications, and it should be possible to evaluate this operating experience to demonstrate dependability.

The objective of this paper is to provide (as an example) a set of staggered criteria for the qualification of pre-developed software to be used in different categories for safety critical I&C. These qualification criteria appear in the form of requirements for the application of methods and measures in the different safety categories. The three safety categories are those from IEC 61226.

Besides the safety categories, there are also usage categories which denote whether the pre-developed software is executed directly online, or is used to directly generate online executed software, or is used to support the generation of online executed software.

Introduction

Pre-developed software which is used in I&C systems important to safety may range from small software elements up to large and complex software products. Small software consists e.g. of the elements of a function block library (of an equipment family) which are configured and provided with parameters to implement an I&C function, or part of it. Large and complex software may be e.g. operating systems, communication drivers, software for computer self-supervision or simulation packages. General purpose pre-developed software may be commercially available (commercial-off-the-shelf, COTS) or may have been developed for a similar application as the envisaged one. In the latter case this may be a non-nuclear application important to safety or a development in the nuclear context for a different plant and/or within a different safety category.

In any of these cases, before the inclusion of a piece of pre-developed software into a new system, there must be a demonstration that the pre-developed software is suited for the envisaged purpose, is reliable, and is of sufficient quality. This demonstration is denoted here as “qualification”.

Different research projects have been investigating into the problem of qualification of pre-developed software for applications with high risk potential and their results are already incorporated in summarizing reports or documents which seek for consensus concerning such a qualification. Also standards can be considered as a kind of summarizing document, because they are developed with an involvement of the different parties engaged in the development, procurement, qualification, operation and licensing of such systems. All these summarizing documents are, however, dependent on geographical differences, i.e. emphasis is put on different aspects of the qualification process. The objective of this paper is to give a more unified approach to the qualification of pre-developed software.

One of the basic summarizing documents which is used here is the report [7] which has been obviously discussed widely in the U.S. between NRC and LLNL and in a pre-review conducted by Mitre Corporation. The IEC standard [1] was heavily discussed for almost ten years on an international basis. In Europe a kernel of technical support organizations discussed for five years some of the most important and practical issue areas raised by the licensing of software important to safety [3], among them the issue of use and validation of pre-existing software. This chapter is also contained as an annex in the IAEA safety guide on software /12/. These three documents form the basis for the proposal of a qualification process for pre-developed software in this paper.

Grading of requirements

In order to spend the effort for qualification effectively, criteria are needed which can be used to focus on functions and systems which are most important to safety and deserve the highest qualification effort, and those of lower importance to safety with (in general) lower associated qualification effort.

In the nuclear field grading is tied to the consequences of the failure of a system in most of the national and international categorization/classification models[1]. An attempt to develop a standard where the probability of occurrence of a failure is also included, i.e. a risk based categorization, was made in IEC. This resulted, however, not in a standard but in a report [10] which contains four examples for a categorization using probabilistic safety analysis PSA.

[1] Functions important to safety are put into categories in IEC 61513 [6], whereas systems important to safety are put into classes.

The following refers to the categorization/classification of IEC 61226 [2] because this standard is

- internationally agreed in the nuclear field by vote,
- introduced in Germany by DIN (German Standards Institute),
- very similar to other German guidelines [4].

Assignment criteria for the three categories A, B and C according to [2] are:

Category A

An I&C function and the associated systems and equipment FSE shall be assigned to category A if it meets any of the following criteria:

a) It is required to mitigate the consequences of a postulated initiating event(PIE) to prevent it from leading to a significant sequence;

b) its failure when required to operate in response to a PIE could result in a significant sequence of events;

c) a fault or failure in the FSE would not be mitigated by another category A FSE, and would lead directly to a significant sequence of events;

d) it is required to provide information or control capabilities that allow specified manual actions to be taken to mitigate the consequences of a PIE to prevent it from leading to a significant sequence of events.

In reference to point d), factors such as the availability of redundant information sources, sufficient time for operator evaluation of alternative sources of information, and whether the manual actions are the only sources of mitigation of the sequence of events shall be considered in categorizing FSE. If manual action is required to preserve NPP safety, the I&C FSE that enables this action shall be assigned to category A.

Category B

An I&C FSE shall be assigned to category B if it meets any of the following criteria and is not otherwise assigned to category A:

a) it controls the plant so that process variables are maintained within the limits assumed in the safety analysis;

b) a requirement for operation of a category A FSE in order to avoid a significant sequence would result from faults or failures of the (category B) FSE;

c) it is used to prevent or mitigate a minor radioactive release, or minor degradation of fuel, within the NPP design basis, but of less importance than a significant sequence of events[2];

d) it is provided to alert control room staff to failures in category A FSE;

e) it is provided to monitor continuously the availability of category A FSE to accomplish their safety duties;

f) it is used to reduce considerably the frequency of a PIE as claimed in the safety analysis.

Category C

An I&C FSE shall be assigned to category C if it meets any of the following criteria and is not otherwise assigned to category A or category B:

a) it is used to reduce the expected frequency of a PIE;

b) it is used to reduce the demands on, or to enhance the performance of, a category A FSE;

c) it is used for the surveillance or recording of conditions of FSE, to determine their safety status (fit for operation, operating, failed or inoperative), especially those whose malfunction could cause a PIE;

d) it is used to monitor and take mitigating action following internal hazards within the NPP design basis (e.g. fire, flood);

e) it is used to ensure personnel safety during or following events that involve or result in release of radioactivity in the NPP, or risk of radiation exposure;

f) it is used to warn personnel of a significant release of radioactivity in the NPP or of a risk of radiation exposure;

g) it is used to monitor and take mitigating action following natural events (e.g. seismic disturbance, extreme wind);

h) it is the NPP internal access control.

After the assignment of I&C functions to safety categories it is necessary to find criteria for the implementation of these functions. Criteria for the implementation of functions of category A via computer-based systems and newly developed software for the specific purpose of such functions are given in [9], for pre-developed software of the same category A guidance is given in [1]. For categories B and C, there is an evolving standard [5] in IEC at the moment, which is meant to become valid for new as well as for pre-developed software.

[2] The definition of a minor radioactive release or minor degradation of the fuel shall be according to national practice. A minor radioactive release might be that due to a release of coolant without additional fuel damage. Minor degradation of the fuel might involve damage to a small amount of fuel cladding without release of coolant or loss of ability to cool the core satisfactorily.

Usage categories of pre-developed software

The categorization of software also depends on the characteristics of its usage. If the piece of software under consideration is directly executed in the application, then it is classified according to IEC 61226 as the function which it is implementing. Category A software implements a function of category A; the same holds for B and C.

However, if the piece of software under consideration is used to produce – more or less directly – the application software, and there are means to check the output of the software under consideration, then it might be possible to chose a lower category as a qualification goal. The proposal made in this paper is to keep software that produces directly application software (denoted as “indirect 1” here) in the same category as the latter, if no other means for the thorough verification of the application software exists. If such a possibility exists, then the software that produces directly application software can be put into the next lower category. An example for software that directly produces application software is an automatic code generator which receives as input a syntactical and semantical fully defined specification and delivers either source code or executable code at its output. This kind of specification and automatic code generation is a widespread technique in I&C equipment families for process automation. Of course there is always the possibility to perform tests with the output of software of usage category “indirect 1”. This is, however, not regarded as sufficient (see also chapter 2.2 of [11]). The reason for this is, that by automatic code generation one or more design steps are skipped, respectively are not visible for the purpose of qualification. If there is such a gap, the analyst performing the qualification should at least have access to a “good” representation of the software at the beginning and at the end of this gap. Good means in this context, that the representation is understandable for the analyst. At the front end of the gap this may be easily given by e.g. a graphical representation of the I&C specification by standardized symbols. The “low end” may be source code representation of a high-level language. In addition it would be desirable, that at the “low end” of the gap, which is the code, the representation of the software is accessible by a tool, e.g. a static analyzer, which can support the software analyst in understanding, finding of faults and inconsistencies, and also in the specification of test cases, if this is wanted.

Software, that produces indirectly application software is denoted as “indirect 2” here. These are tools which support the development of software by a structured approach (CASE tools). Examples for such a structured approach are methods like SA (Structured Analyses), SD (Structured Design), SADT (Structured Analysis and Design Technique), etc. The tools based on approaches like this establish a framework within which the application software can be interactively developed.

With software of usage category “indirect 2” code can be produced that is understandable by humans and accessible by tools as e.g. static analyzers and debuggers. Moreover such tools deliver documented information on development levels of the application software, thus providing input to a human-centered analysis of the application software. As the development part and the analysis part for application software produced by software of category “indirect 2” is strongly human-centered, the probability that a fault in the tool results in a fault in the application software is much lower than with category “indirect 1”. Therefore this type of software is treated as non-classified NC. Also the verification and validation tools which are used by the analyst, like static analyzers and debuggers are categorized as NC. Their application is primarily human driven, and a tool fault is not likely to introduce a fault in the application software. This is in line with IEC 60880, which requires in clause 8: “Hardware and software tools used for computer system validation need no special verification. They should, however, be shown to be suited to their purpose.”

In the following the usage categories and their relationship to the categories of IEC 61226 are summarized.

Usage category	Characteristics of the software	IEC 61226 category
DIRECT	**DIRECTLY EXECUTED IN AN APPLICATION OF CATEGORY A OR B OR C**	A or B or C
indirect 1	generates automatically code (source code or executable code) for	
	- category A	A or B[1]
	- category B	B or C[1]
	- category C	C or NC[1]
indirect 2	supports the development of code for category A or B or C (CASE-Tool)	NC

[1] The next lower category of IEC 61226 may be chosen, if the output of the code generator is understandable and can be verified by a human by means in addition to testing and/or an independent tool is available for verification.

Table 1: Usage categories of software and their relationship to categories of IEC 61226

Qualification criteria for pre-developed software

The ideal situation for pre-developed software would be that it has been developed for an exactly identical function as the envisaged one, according to the quality requirements of the safety category of this function. Usually, however, this is not the case, and one or more of the following issues must be tackled with:

- missing elements in the production process,
- product documentation missing or of insufficient quality,
- operational profile in the past very different from the envisaged one,
- only a (small) part of the pre-developed software is used (unused code),
- unintended resident functions (functions not documented).

A benefit of pre-developed software may be a wide and/or frequent use with positive results, i.e. a long operating time free of failure, or with acceptable few failures. Advantage can only be taken from positive operating experience, if

- enough data are collected,
- the data collection is assessed to be dependable, and
- the evaluation of data is statistically valid.

Besides the compensation for missing knowledge on the product and for its production process by the evaluation of operating experience, there is also the possibility to develop retrospectively by re-engineering techniques missing documentation on product features and levels of product development.

Testing of the pre-developed software has of course to be performed for all safety categories. Even for non-classified software NC, tests will be necessary, as this is the state of practice to demonstrate that the software is suited for its purpose (as required by IEC 60880).

Qualification criteria independent of safety categories

The first step in the acceptance process is the identification of the environment within which the pre-developed software will have to work. This environment is determined by the system-level safety function as described in the system requirements specification. Also the interface and performance requirements, as well as the safety category should be contained in the system requirements specification. This means, that during the establishment of the plant safety design base a risk and hazards analysis has been performed which rendered the categories of safety functions to be implemented by pre-developed software. This risk and hazard analysis – in spite of being out of the scope of I&C engineering – has been taken as the first of four acceptance criteria that should be applied to pre-developed software independently of its safety category.

Besides the requirements which are coming from the system-level safety function, there are also category-independent requirements for the (sub-)function where the function implemented by pre-developed software fills in. There are, the clear identification of the (sub-)function to be fulfilled by the pre-developed software and of the means (software tools) for its production, taking into account their usage category, determination of their safety category, and the configuration management and change control necessary for the pre-developed software. Table 2 summarizes these qualification criteria.

Table 2: Qualification Criteria Independent of Safety Categories

Criterion	Description	Document
I 1	The system-level safety function shall be clearly identified.	IEC 60880-2 [1], 4.3.3.1.1.1; IEC 61513 [6], 6.1.1, 6.1.2
I 2	Risk and hazard analysis shall have been performed to determine the safety category of the system-level safety function.	LLNL [7], Table 4; EUR 19265 [3], 1.1.3.1
I 3	The safety (sub-)function to be implemented with pre-developed software shall be clearly identified.	IEC 60880-2, 4.3.3.1.1.1; IEC 61513, 6.1.1.1.1; LLNL, Table 4; EUR 19265, 1.3.3.1
I 4	The safety category of the pre-developed software shall be determined. GOTO A, B, C.	IEC 61513, 6.1.1.1.1; LLNL, Table 4
I 5	The pre-developed software shall be under configuration and change control	IEC 60880-2, 4.3.3.1.1.2, 4.3.4.3; LLNL, Table 4; EUR 19265, 1.3.3.2

Qualification criterion I 5 is necessary because the whole qualification process cannot be applied to a piece of software which is permanently changing.

Criterion I 4 delivers the output of this preliminary qualification, i.e. the category A or B or C of the pre-developed software under consideration.

First Level Qualification criteria for category A

Pre-developed software for category A functions has to fulfil almost all the stringent requirements that are applied to newly developed software for this category. Therefore, the application of pre-developed software in category A presumes that only small parts of the life cycle documentation are missing, and can be compensated by the evaluation of operating experience and/or additional testing.

Table 3 shows the category A first level qualification criteria. First level in this context means, that these are principal criteria, which must be detailed in subsequent levels.

As an example for a subsequent level, the second level qualification criteria for criterion A 1 (suitability assurance) are given in table S1 . Table S 2 gives the second level criteria of a part (namely the quality assurance part) of first level criterion A 2 (product assurance). The second part would be a table for V&V, which has not been included, as only the principle of the qualification process is shown in this paper. For the same reason, also the further details of the first level criteria documentation, product safety, system safety, interface, compensation by operating experience, error reporting, and modification are not elaborated. Thus the "GOTO ..." and other references in the description part of the tables, which are the pointers to the more detailed criteria are in most cases empty.

Table 3: Category A, first level qualification criteria

Criterion No.	Description	Document
A 1 Suitability Assurance	An evaluation of suitability of the pre-developed software shall be performed, to confirm that the functional, performance and architectural specifications of the pre-developed software comply with the requirements of the system specification. GOTO S 1, No. 1-7	IEC 60880-2, 4.3.3.1
A 2 Product Assurance	A quality evaluation of the pre-developed software shall be performed, to provide evidence that the feature of its design are appropriate to implement a category A function, and that appropriate V&V and quality assurance has been exercised through the life cycle. This evaluation shall be performed against the requirements of IEC 60880. GOTO ...	IEC 60880-2, 4.3.3.2; LLNL, Table 5; EUR 19265, 1.3.3.4, 1.3.3.5
A 3 Docu-mentation	Documentation shall be available for review to demonstrate that criterion A 2 has been met during development of the pre-developed software. GOTO ...	IEC 60880-2, 4.3.3.2; LLNL, Table 5, A6; EUR 19265, 1.3.3.7
A 4 Product Safety	It shall be demonstrated that criterion I 3 is met by the pre-developed software. GOTO ...	IEC 60880-2, 4.3.3.4.2; LLNL, Table 5, A7

Criterion No.	Description	Document
A 5 System Safety	It shall be demonstrated that no features of the pre-developed software violate safety requirements or constraints on the system level. GOTO ...	IEC 60880-2, 4.3.3.1.2.4; LLNL, Table 5, A8; EUR 19265, 1.3.3.8
A 6 Interface	The interfaces through which the pre-developed software is involved shall be identified, clearly defined, thoroughly validated, and under configuration management. GOTO ...	LLNL, Table 5, A9; EUR 19265, 1.3.3.3
A 7 Compen-sation, Operating Exper-ience	If the application of criterion A 2 reveals minor deficiencies, then the evaluating of operating experience may be used for compensation. GOTO ...	IEC 60880-2, 4.3.3; LLNL, Table 5, A10; EUR 19265, 1.3.3.9
A 8 Error Reporting	All errors shall be reported, analyzed and classified according to their severity. Their impact on the function to be fulfilled by the pre-developed software shall be evaluated. GOTO ...	IEC 60880-2, 4.3.3.3.1.6; LLNL, Table 5, A11; EUR 19265, 1.3.3.11
A 9 Modifi-cation	Modification of a piece of pre-developed software shall be performed compliant with IEC 60880. The implementation of the modified component shall be handled in the frame of the system life cycle as in IEC 61513. GOTO ...	IEC 60880-2, 4.3.3.1.2.2; IEC 61513, 6; EUR 19265, 2.7.3.1, 2.7.3.2

First level qualification criteria for category B

Whereas pre-developed software will be exceptional in category A, because of the stringent requirements on product, process and their documentation, this type of software will be found more frequently in category B and C. The proposed relaxations of qualification criteria in category B against category A are mainly the reduced amount of documentation required and a weaker process of product assurance. Table 4 shows the first level qualification criteria for category B.

Table 4: Category B, first level qualification criteria

Criterion No.	Description	Document
B 1 Suitability Assurance	An evaluation of suitability of the pre-developed software shall be performed, to confirm that the functional, performance and architectural specifications of the pre-developed software comply with the requirements of the system specification. GOTO S 1, No. 8-9	IEC 62138, 5.4, 6.2.3

Criterion No.	Description	Document
B 2 Product Assurance	A quality evaluation of the pre-developed software shall be performed, to provide evidence that the features of its design are appropriate to implement a category B function, and that appropriate V&V and quality assurance has been exercised through the life cycle. GOTO ...	LLNL, Table 6, B 5
B 3 Docu-mentation	Documentation shall be available for review to demonstrate that criterion B 2 has been met during development of the pre-developed software. GOTO ...	IEC 62138, 6.2.1; LLNL, Table 6, B 6
B 4 Product Safety	It shall be demonstrated that the pre-developed software can implement its safety function as identified in criterion I 3. GOTO ...	LLNL, Table 6, B 7
B 5 System Safety	It shall be demonstrated that the pre-developed software does not violate safety requirements and/or constraints on the system level. GOTO ...	LLNL, Table 6, B 8
B 6 Interface	The interfaces through which the pre-developed software is communicating shall be identified, validated and under configuration management. GOTO ...	IEC 62138, 6.2.1, 3
B 7 Compen-sation, Operating Expe-rience	If the application of criterion A 2 reveals deficiencies, then the evaluation of operating experience may be used for compensation. GOTO ...	IEC 62138, 6.2.2.2; LLNL, Table 6, B 9
B 8 Error Reporting	All errors shall be repeated and analyzed. Their impact on the system-level function shall be evaluated. GOTO ...	LLNL, Table 6, B 10
B 9 Modifi-cation	Modifications of a piece of pre-developed software shall be performed compliant with the requirements of IEC 62138 (clause 6.9). GOTO ...	IEC 62138, 6.9

First level qualification criteria for category C

The suitability analysis for category C pre-developed software follows no specific requirement; it is just a fit-for-purpose analysis.

The product assurance activities aim to assess whether appropriate standards have been systematically applied during software development, that configuration management is effectively employed, as well as a minimum of V&V activities.

Table 5: Category C, first level qualification criteria

Criterion No.	Description	Document
C 1 Suitability Analysis	The suitability analysis is reduced to a simple fit-for-purpose analysis. GOTO S 1, No. 10	IEC 62138, 7.2.3
C 2 Product Assurance	A quality evaluation of the pre-developed software shall be performed, to provide evidence that the features of its design are appropriate to implement a category C function. Minimum V&V shall have been performed. GOTO ...	LLNL, Table 7, C 1
C 3 Docu-mentation	Minimum documentation as described in table S .., including documentation of V&V required in C 2 and detailed in S .. shall be available for inspection. GOTO ...	IEC 62138, 7.2.1; LLNL, Table 7, C 6
C 4 Product Safety	It shall be demonstrated that the pre-developed software can implement its safety function as identified in criterion I 3. GOTO ...	IEC 62138, 7.2.1, 3
C 5 System Safety	It shall be demonstrated that the pre-developed software does not violate safety requirements and/or constraints on the system level, and those of A and B systems. GOTO ...	LLNL, Table 7, C 8
C 6 Interfaces	The interfaces through which the pre-developed software is communicating shall be identified and under configuration management. GOTO ...	IEC 62138, 7.2.1, 3
C 7 Compen-sation Operating Expe-rience	The pre-developed software shall be shown to have an operating past without serious malfunctions. GOTO ...	IEC 62138, 7.1.5, 4; LLNL, Table 7, C 9
C 8 Error Reporting	An error reporting history to demonstrate fulfillment of criterion C 7 should be available. Within the actual application, there should be an error reporting schema, too. GOTO ...	LLNL, Table 7, C 9
C 9 Modifi-cation	Modifications shall be performed compliant with a reduced set of requirements of IEC 62138. GOTO ...	IEC 62138, 6.9

From the first level qualification criteria “pointers” (GOTO) are leading to a set of second level qualification criteria, which are more detailed requirements than the first level ones.

Second level qualification criteria

The second level qualification criteria are not grouped according to safety categories; they should be regarded as a pool of requirements which are accessed from the first level. In many cases first level C criteria point to a smaller set of second level criteria than first level B criteria, and the same holds for the relationship between B and A first level criteria.

The following tables with second level qualification criteria are not meant to be exhaustive; criteria with this grade of detail may in many cases be project specific.

The tables with second level qualification criteria are denoted with "S". Table S 1 contains criteria for a suitability analysis.

Table S 1: Criteria for suitability assurance

Criterion No.	Description	Document
1	System specification documentation shall be available, containing functional, performance, and interface requirements to be fulfilled by the pre-developed software (PDS).	IEC 60880-2 (Cat. A)
2	Specification and user documentation of the pre-developed software shall be available, defining explicitly all characteristics that are relevant in fulfilling the systems functional and performance specifications.	IEC 60880-2 (Cat. A)
3	The specifications of the PDS shall be evaluated with respect to the system requirements specification. If discrepancies exist, the PDS shall either be rejected or modified or the requirement specifications shall be adapted to resolve them, provided that the overall safety function is preserved.	IEC 60880-2 (Cat. A)
4	If it is necessary to modify the PDS an evaluation shall be completed, based on the PDS design documentation, to determine if the change can be performed in a manner compliant with IEC 60880. If the change cannot be performed in a compliant manner, the use of the PDS shall be rejected.	IEC 60880-2 (Cat. A)
5	For a PDS that is contained in a library except when the whole library has to be assessed, it should be possible to tailor the library to build a restricted library meeting the software needs and to link the program with this restricted library which shall be composed of assessed components.	IEC 60880-2 (Cat. A)

Criterion No.	Description	Document
6	The suitability evaluation shall identify the functions that are included in the PDS which are unintended an unneeded by the system and also the measures to ensure that these functions do not interfere with safety functions.	IEC 60880-2 (Cat. A)
7	When the evaluation is concluded, a document shall be produced to record whether the functional and performance specifications of the PDS comply with the software requirement specifications of the system; and where the PDS is not adequate, the reasons for rejection.	IEC 60880-2 (Cat. A)
8	The safety documentation (for description see IEC 62138, 6.2.1) of operational PDS shall be evaluated against system specification (and system design). Inconsistencies shall be resolved.	IEC 62138, 6.2.3 (Cat. B)
9	The functions of operational PDS which are not required to support the system requirements specifications should be identified. Evidence of harmlessness should be given. For application functions of PDS, see Crit. No. 3 of this table.	IEC 62138, 6.2.3 (Cat. B)
10	No specific requirements are given for a suitability analysis for operational PDS of Class 3. It should be shown to be fit for purpose on the basis of its user documentation.	IEC 62138, 7.2.3 (Cat. C)

This table is an example for more detailed second level criteria to support first level criterion on suitability assurance. Criteria 1 to 7 in table S 1 are supporting criteria A 1, 8 and 9 are supporting B 1, and C 1 is supported by criterion 10.

Table S 2: Product assurance, criteria for software quality assurance

Criterion No.	Description	Document
1	The requirements of the PDS software quality plan and the corresponding verification and documentation shall be evaluated for conformance with the requirements of IEC 60880.	IEC 60880-2, 4.3.3.2.2 (Cat. A)
2	The PDS design shall be consistent with the constraints on the architecture and deterministic internal behavior of the system.	IEC 60880-2, 4.3.3.2.2 (Cat. A

Criterion No.	Description	Document
3	If practices differing from those of appendices A to F of IEC 60880 have been used for the development of the PDS, their adequacy shall be analyzed and justified according to clause 1 of IEC 60880. Their importance in the assurance of the software quality characteristics shall be evaluated in conjunction with the system requirements. The results of the evaluation and analysis shall be recorded for independent review.	IEC 60880-2, 4.3.3.2.2 (Cat. A
4	Non-conformities to IEC 60880 requirements, properties that cannot be verified, weakness or missing steps in the verification or documentation process shall be identified. Each shall be ranked according to its importance in the assurance of the software quality characteristics, and the importance to safety of the functions implemented in the system..	IEC 60880-2, 4.3.3.2.2 (Cat. A
5	The qualification documentation shall provide evidence that PDS integrated in hardware components, has been validated to demonstrate that it meets its functional and performance specifications.	IEC 60880-2, 4.3.3.2.2 (Cat. A
6	Where PDS components contain features that cannot be validated other than in the final system configuration, then validation of these features shall be performed in the final system configuration.	IEC 60880-2, 4.3.3.2.2 (Cat. A
7	The quality and degree of coverage of the validation tests performed on the PDS shall be evaluated with reference to the requirements of clauses 7 and 8 of IEC 60880 and additional validation tests performed if necessary.	IEC 60880-2, 4.3.3.2.2 (Cat. A

Criterion No.	Description	Document
8	When the evaluation of the design and of the life cycle is concluded, a document shall be produced to record that a) the PDS quality has been proved and no additional test or analysis of operating experience is required; b) complementary qualification shall be performed when the system configuration is available; c) lack of information has been detected during the evaluation, but this can be compensated by the completion of additional verification and validation, testing or code analysis and documentation; d) lack of information has been detected during the evaluation, which can be compensated for by use of operating experience; e) the PDS (or part of the PDS) requires modification for the intended use in the system and that it has the appropriate level of quality so the modifications may be performed in accordance with IEC 60880; f) significant problems can be expected because of the transfer of the PDS to new hardware; g) the PDS quality is not adequate and the PDS shall be rejected on grounds that the weakness are to great or the information inadequate for effective compensation; and h) the independence of the qualified functions/properties of the PDS from those not qualified has/has not been established.	IEC 60880-2, 4.3.3.2.2 (Cat. A
9	The criteria 1 to 8 may be reduced, especially those requiring full application of IEC 60880. Quality assurance shall divide the development and the modification phases of the software safety life cycle into specified activities. These activities shall include all what is necessary to achieve the required software quality, to verify that this quality is achieved, and to provide objective evidence to that effect.	IEC 62128, 6.1, 7.1 (Cat. B) and (Cat. C)

Also in this example for second level criteria supporting the first level criterion on product assurance, there is a staggered stringency; criteria 1 to 9 support the first level criterion A 2, criterion 10 support B 2 and C 2.

The missing difference in criterion 10 must be put in further details concerning “activities necessary to achieve the required software quality”, i.e. in “third level” criteria.

The tables S 1 and S 2 in this example are dealing only with the first level criterion “suitability assurance” and one part of the aspects of the first level criterion “product assurance”, i.e. with software quality assurance. The other part of the criterion “product assurance” is verification and validation, V&V, which also has to be broken down in more detailed criteria. Also the other first level criteria of tables 3, 4 and 5, i.e. documentation, product safety, system safety, interface, compensation by operating experience, error reporting, and modification should be detailed into appropriate levels of refinement. Examples for this process can be found in [7].

Conclusion

Extensive research work has been performed, mainly in the last ten years, to tackle the problem of qualifying pre-developed software for inclusion into systems important to safety. This research work did not render a unique solution how to do this, because of the great variety of applications, the differences in the usage of the software (application software, system software, tools, ...), and the safety relevance.

The results of this work, however, influenced some practical approaches, which tried to analyze systematically the issues involved, and to provide recommendations for the use of pre-developed software.

Also standardization groups in the nuclear field issued or are about to issue requirements for the application of pre-developed software.

In this paper an attempt is made to demonstrate exemplary a procedure how the different approaches can be brought together, to form a usable set of staggered criteria for the acceptance of pre-developed software.

This first examples show, that there will be no principal difficulty for a unified approach, because there are no major contradictions in the requirements / recommendations of the analyzed documents. The acceptance of such a unified procedure, however, needs the involvement of a broad international group of experts.

Literature

[1] IEC 60880-2: Software for computers important to safety for nuclear power plants – Part 2: Software aspects of defense against common cause failures, use of software tools and of pre-developed software, Dec. 2000

[2] IEC 61226: Nuclear power plants – Instrumentation and control systems important for safety – Classification, May 1993

[3] EUR 19265 EN: Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors, May 2000

[4] RSK-Leitlinien für Druckwasserreaktoren, Fassung 11.96, Kapitel 7: Elektrische Einrichtungen des Sicherheitssystems und der anderen Systeme mit sicherheitstechnischer Bedeutung, Nov. 1996

[5] IEC 62138 Draft: Software for I&C systems of safety class 2 & 3, March 2001

[6] IEC 61513: Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems, March 2001

[7] Preckshot, G.G., Scott, J.A:
A proposed acceptance process for commercial-off-the-shelf (COTS) software in reactor applications, Lawrence Livermore National Laboratory, UCRL-ID-122526, 1995

[8] Scott, J.A:, Preckshot, G.G., Gallagher, J.M.
Using commercial-off-the shelf (COTS) software in high-consequence safety systems, Lawrence Livermore National Laboratory, UCRL-JG-122246, 1995

[9] IEC 60880: Software for computers in the safety systems of nuclear power stations, 1986

[10] IEC TR 61838: Nuclear power plants – Instrumentation and control functions important for safety – Use of probabilistic safety assessment for the classification, Feb. 2001

[11] IAEA Technical Reports Series No. 384: Verification and validation of software related to nuclear power plant instrumentation and control, May 1999

[12] IAEA Safety Guide No. NS-G-1.1: Software for computer based systems important to safety in nuclear power plants, Sept. 2000

A Bayesian Approach to Risk Informed Performance Based Regulation for Digital I&C QA Programs

Swu Yih[1] Chin-Feng Fan[2] Sun-Li Chyou[1] Li-Sing Wang[1]

[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

Summary

The purpose of applying Risk Informed Performance Based Regulation (RIPBR) is to reduce unnecessary conservatism existed in current regulations. This paper proposes a systematic way to find such unnecessary conservatism based on Bayesian Belief Network (BBN) modeling technique. First, a Bayesian based QA process model is developed, and the correspondent event tree based on the BBN is then derived. Risk insight into different QA activities can thus be investigated by comparing their contribution to final quality to determine their necessity. Independent V&V, prescribed by RG 1.168, is selected as a case study to demonstrate the effectiveness of this approach. The proposed Bayesian approach appears to be very promising in supporting the RIPBR practice for digital I&C QA programs. Related issues and future work are also discussed.

Introduction.

In last few years NRC has announced its PRA Policy Statement (NRC, 1995) and a series of Regulatory Guides (RG1.174~RG1.178) to promote the application of Risk Informed Performance Based Regulation (RIPBR) in all its regulatory activities. The purpose of RIPBR is to reduce *unnecessary conservatism* existed in current regulations, and thus reduce unnecessary burden to both licensees and regulators. This policy has created much incentive to nuclear industry to actively look for potential areas for cost saving. This paper introduces one of such potential areas and explains how to prepare evidence to justify it is unnecessary.

Based on a reported study (Waite, 2000) and our licensing review experience (Yih, 1999), we consider the current regulatory requirements for QA programs of digital I&C systems to be a proper candidate for applying RIPBR. On one hand, the current digital I&C QA program regulations probably are the most complicated in terms of the number of documents involved (Waite, 2000). On the other hand, digital I&C system development, especially in software quality assurance aspect, always involves certain degree of uncertainty and unpredictability (Padberg, 1999). Moreover, industry experience clearly shows that various nuclear digital I&C projects exhibited a large fluctuation in resource utilization efficiency. For example, Sizewell B (Marshall, 1994) and Chooz B (MacLachlan, 1994) spent significant resources on their QA program, while they still suffered from critics and doubts about their safety quality. On the contrary, K6/K7 digital I&C project (Fukumoto,1998) consumed relatively less resource on its QA program, but still achieved satisfactory safety performance. Obviously, these realistic cases reveal that the current regulations of digital I&C system QA programs indeed do have ample space for resource efficiency improvement. Meanwhile, our on-going Lungmen Project is gradually showing difficulty in fully complying with the current digital I&C regulations (Yih, 1999). All these cases justify the need for application of risk-informed approach to digital I&C systesms. The problem is how to meet relevant RIPB regulatory requirements. This problem can be divided into two questions. The first one is whether RIPBR

is applicable to digital I&C systems? If the answer is *yes*, then the second question will be how to prepare needed information to meet regulatory requirements. Our previous paper (Yih, 2000) has investigated the applicability of RIPB and the answer is positive. The purpose of this paper is to further develop a practical approach to implementing the concept.

In the following, we will first describe the related regulatory issues. Then, we will present the basic approach to performing qualitative risk analysis based on Bayesian Belief Network (BBN) to identify unnecessary conservatism. A case study dealing with the issue of independent verification and validation (IV&V) will then be discussed, followed by a conclusion.

Regulatory issues for applying RIPBR to QA programs of digital I&C systems.

We will give an overview of the current digital I&C QA requirements to show their complexity and overwhelming document size. Then we will explain relevant regulatory requirements needed when applying RIPBR to digital I&C QA programs.

Current licensing requirements for digital I&C QA programs.

The major regulatory requirements for digital I&C QA programs are described in Chapter 7 of Standard Review Plan and associated references. There are more than 30 documents related to QA program requirements. The general structure of these documents can be presented in a hierarchical format as shown in Fig. 1.

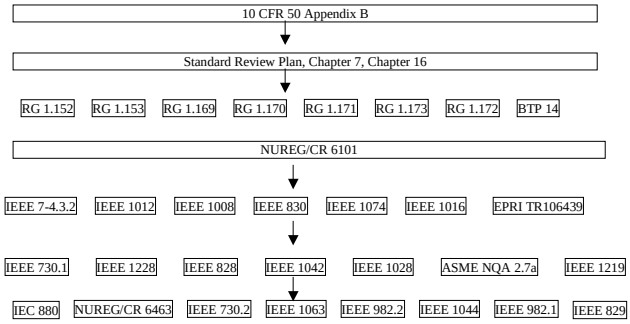


Fig. 1. Document structure of regulation and guides for digital I&C QA programs

The kernel part of these documents consists of IEEE Software Engineering Standards. IEEE standards are written for general application purpose; therefore, they tend to be very comprehensive and generic. The total number of pages of QA related standards exceeds 2,000. One can easily imagine what a huge load it will be on those people who have to prepare documents and those who have to review the documents. On the other hand, it should not be too difficult to find unnecessary conservatism for a specific case from these general-purpose documents.

Applicable regulatory guides for applying RIPBR to digital I&C QA program.

First we will review the RIPBR in general, then we will discuss Regulatory Guide 1.176 in more details because it is the most relevant guidance to digital I&C QA activities.

On August 16, 1995, NRC announced its Policy Statement (USNRC, 1995) of applying PRA techniques to "*all regulatory activities*" to the extent supported by the state-of-art methods of PRA. The phrase "*all regulatory activities"* naturally encompasses digital I&C QA programs but under the pre-

condition that the *state-of-art* PRA techniques can support the corresponding risk-informed decision-making process. The purpose of this policy statement is to improve the regulatory process by promoting "*more efficient use of agency resources*," and "*reduction in unnecessary burden to licensees."* Several Regulatory Guides have also been issued to help the industry to implement this policy. The most important guide is RG1.174: "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis." (USNRC, 1998a) This guide sets up the basic principles and procedure of using PRA insights to modify existing licensing basis so as to reduce burden to public utility. The application of RIPBR has been expanded to several areas, and the results are promising. For example, South Texas Nuclear Power Plant has applied RIPBR to component classification. The number of safety components is significantly reduced; it is estimated that two million dollars can be saved due to this re-classification (Apostalakis, 2000). This also reduces the workload of regulators because fewer components need to be inspected.

RG 1.176: "Approaches for Applying RIPB to Graded QA Programs" (NRC, 1998b) is the most suitable guide for the digital I&C QA programs. RG 1.176 prescribes basic concept and necessary steps when evaluating a graded QA program application. Fig. 2 shows five principles to be considered during evaluation process. Our preliminary evaluation concludes that digital I&C RIPBR can meet four of the five principles quite straightforwardly. Only the fifth principle needs to be elaborated in more details. In the next section, we will present a technique for assessing risk impact due to a QA program change.

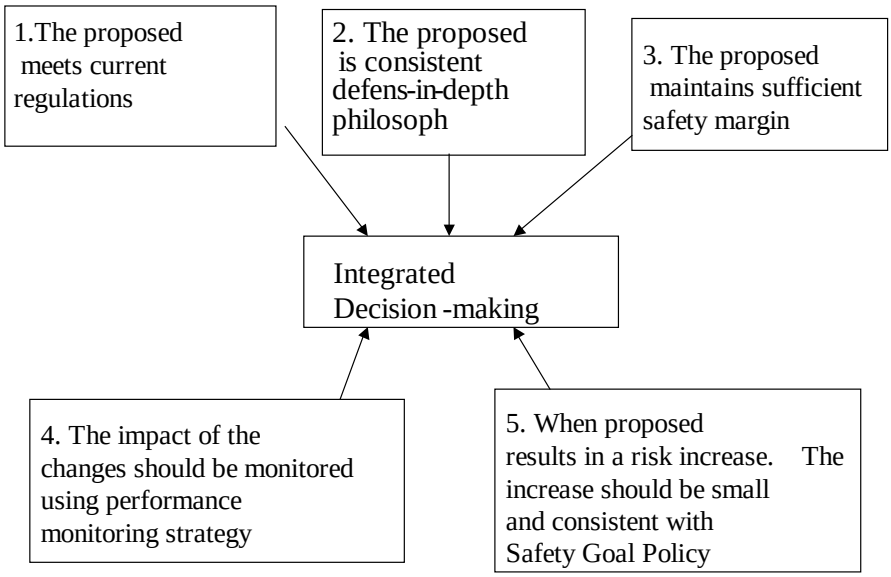


Fig. 2. Principles of RIPBR Decision-Making Process

Development of a risk analysis technique for digital I&C QA programs.

Our intention of applying RIPBR to digital I&C system is to reduce unnecessary conservatism existed in QA requirements. To justify such reduction, RG 1.174 requires an assessment of risk impact due to the proposed reduction. However, current state-of-art PRA techniques do not support an acceptable quantitative risk assessment for a typical QA program. Fortunately, RG 1.176 accepts a *qualitative* risk assessment for the graded QA activities that do not have quantitative PRA data. In this section, we will present our proposed approach to such assessment.

Basic concept of risk analysis for QA programs.

The purpose of QA program risk analysis is to explore the detailed information of undesired events associated with the QA program. Its task is to analyze potential scenarios and their occurring probabilities of a poor quality product produced under this QA program. Once such information is available, we can compare and rank the importance of relevant QA activities, and thus, identify the location of the vulnerable weak points. Our approach to obtain such scenario information is to develop a QA process model to generate QA failure scenarios.

A QA process model consists of elements representing software development staffs, software QA staffs, development activities, QA activities and documents generated. Our major concern, quality, is represented as defects density. Each element is represented as a node and is connected based on its casual relation with other elements. Each node is further designated with 2~5 states representing its status, for example, the undesired event is represented as defect density at *high* status. In reality, the relation between QA process elements is not static and fixed, i.e., the influence of one node on the other node often exhibits probabilistic and interactive behavior. In order to represent the probabilistic behavior of QA process, we apply Bayesian Belief Network (BBN)(Jensen, 1996) technique. A typical QA process represented in BBN is shown in Fig 3.

Concept of Bayesian Belief Network (BBN).

Bayesian Belief Network is a system modeling technique for representing systems that exhibit probabilistic behavior. A BBN consists of groups of connected nodes; it is basically a directed acyclic graph representing the causal influence between nodes. Each node represents a random variable with discrete values, and edges represent cause-effect relationship between nodes. The influence relations between nodes are described by Conditional Probability Tables (CPT). The value represents the degree of strength of the casual relation between two linked nodes. BBN provides formula to update CPT values once an entry of CPT changes. The initial values of CPT can be determined by experts; the table indicates that the node is in a specific state given the state

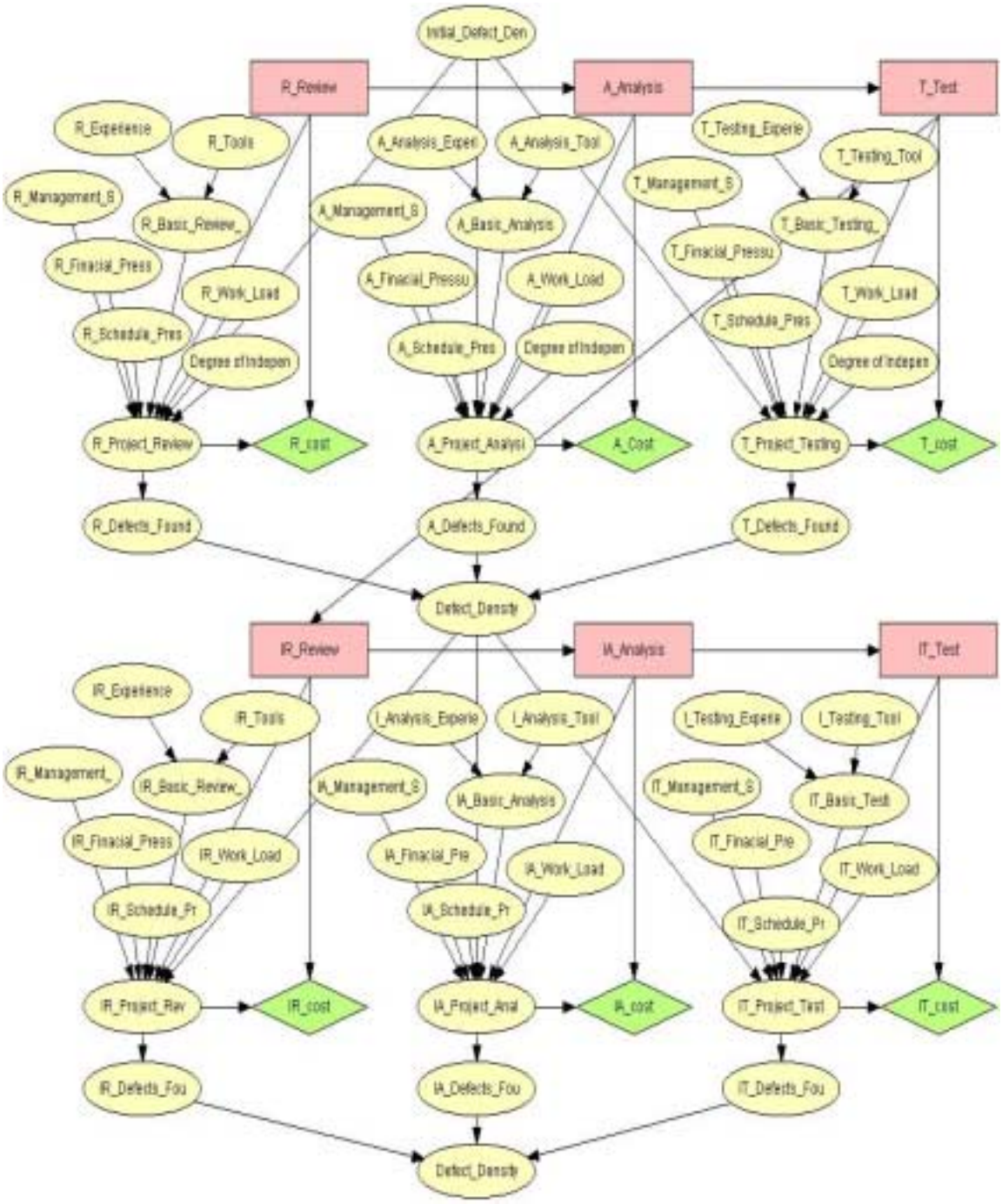


Fig. 3.
BBN Model of Software QA Process

of the influence nodes (parent nodes). Once there is a new evidence, the values of nodes can be recalculated either from parent nodes to child nodes or vice versa. Thus the dynamic behavior of modeled system is determined by CPT values. A BBN based QA process model is shown in Fig. 3.

Derivation of QA program failure scenarios.

The QA process model then is used to generate complete QA process scenarios. The process of failure scenario generation is shown in Fig. 4 and also explained as follows:

Step 1: From the BBN, get the next node, which either has no parents or whose parents have been all processed.
Step 2: add the node to the event tree and calculate its path probability
Step 3: examine whether truncation or stopping rules are met
Step 4: if yes go to Step 7
Step 5: mark this node as processed
Step 6: Increase the event sequence number by 1 and go to step 1
Step 7: Is there undeveloped node, if yes go to Step 1
Step 8: stop

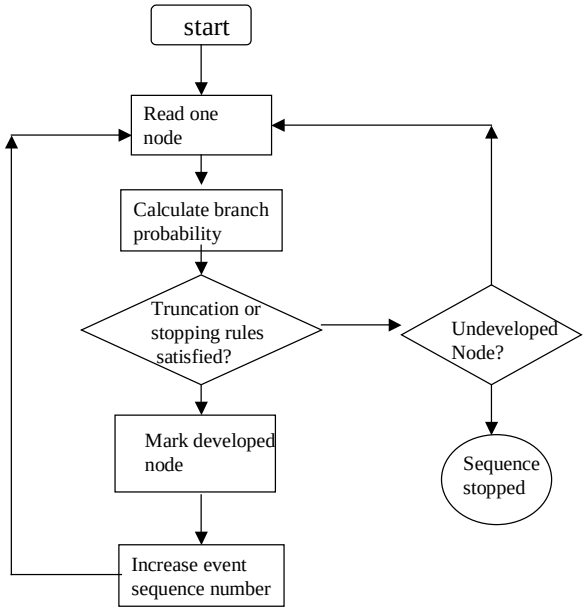


Fig. 4. Event Tree Derivation Process

Our proposed method first enumerates major influence factors, and constructs the BBN for system risk; an event tree based on same influence factors is then generated using the above procedure. Tree trimming will be 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 will then be counted to draw the *risk profile* graph. The graph can help identifying potential areas of unnecessary conservatism. It can also help determining whether the resulting outcomes of proposed QA program change are acceptable or not.

Case Study: Is IV&V requirement prescribed by RG 1.168 an unnecessary conservatism?

In this section we apply the proposed technique for finding a potential unnecessary conservatism existed in current digital I&C QA requirements.

Background and motivation.

Software *verification* and *validation* (V&V) is a critical task of digital I&C QA programs. Verification determines whether the output of a given development phase satisfies the requirements of a previous phase and validation determines whether the final product satisfies intended use and user needs. Independent Verification and Validation (IV&V) is the V&V performed by independent group other than the development team. The V&V can be done internally or externally (i.e., IV&V). Obviously the cost of later (IV&V) will be significantly larger than the former (V&). Thus, the issue of IV&V naturally becomes a critical concern for every stakeholder involved in digital I&C projects. The issue whether to use IV&V or not has drawn lots of questions and hot debate. In the following, we will briefly describe IV&V related experience and reports that can demonstrate its importance and controversy.

Nuclear Industry

- Sizewell B ((Marshall, 1994) invested a great amount of resource in conducting an independent verification and validation task. This IV&V added 60% extra cost to the overall expense without finding any important defects. This is the most famous case of an over-killed digital I&C IV&V project in nuclear industry.
- Because RG 1.168 explicitly requires that V&V has to be done *independently*, Lungmen I&C project therefore still needs to hire another consultant company to perform IV&V in order to comply with this requirement.

Aviation / Space Industry

- After spending 3.2 millions per year on IV&V activities (Gruman, 1992) without significant defect finding, NASA space shuttle software QA program considered IV&V was not worthwhile and decided to stop its IV&V contract with Intermetrics. But US Congress stepped in, and NASA decided to resume its IV&V project due to Congress' intervention.
- The Airworthiness regulation mandatory requires some software QA activities be performed "with independence" (RTCA, 1992). In a large scope industry survey (Hayhurst, 1999), digital avionics manufactures considered *independence* as a questionable requirement and asked Federal Aviation Agency to re-consider its value.

Academic /Research

- A research was conducted by J.D. Arthur (Arthur, 1999) to evaluate the effectiveness of IV&V. It found that IV&V is more effective in requirement and design phrase.
- A project sponsored by NASA evaluates the financial effectiveness of IV&V (Raffo, 2001). Its purpose is to convince stakeholders that IV&V is important and worthwhile.

These reports and experiences clearly demonstrate the controversial nature of IV&V within a QA program. Thus it is worthwhile to conduct risk analysis of IV&V to explore more detailed information of its cost-effectiveness.

Assess risk impact of IV&V for a digital I&C QA program.

In the following, we will use IV&V as a case study to demonstrate the usage and effectiveness of the proposed approach. We proceeded the case study as follows:

Steps 1: Collect influence factors of QA program and IV&V.

In general, IV&V may be performed through review, testing, and analysis. The technique differences mainly lie in that analysis needs mathematical skill and maturity, review depends on experience, while

testing requires comprehensive test cases and tools. As to the differences of IV&V and V&V, we focus on the schedule and financial pressure of the internal V&V, while the IV&V can be free from it. Thus, the influence factors for verification and validation are listed in Fig. 3. These factors can be categorized into four groups:

(1) General factors
(2) Technique-related factors
(3) Activity-related factors
(4) Performance shaping factors

General factors deals with schedule/financial pressure and degree of independence. Technique-related factors consist of review experience, analysis capability, as well as testing and analysis tools. Activity-related factors may have review depth and scope, testing coverage, as well as analysis rigorousness. Performance shaping factors consist of documentation quality, software initial defects, workload, and management support.

Step 2: Bayesian-based QA causal influence model

We then construct the corresponding BBN, shown in Fig.3. Note that in the network, technique-related factors influence verifiers' potential; while verifiers' potential, and the rest types of factors influence V&V effectiveness. The rectangles in Fig. 3 are decision nodes; the diamond nodes represent costs of different activities.

Steps 3 : Event Tree and failure scenarios derivation

We now can construct the event tree with the same influence factors using the procedure described in Fig. 4. However, the original BBN is somewhat complicated for our explanation. Instead of considering analysis, review, and testing, we simplified the network to include general internal V&V and IV&V parts. We also further simplify the factors by starting with V&V potential, and by considering only the initial defects and time pressure. Fig. 5 is a portion of the generated event tree.

Step 4: Create Risk Profile

In the event tree, results both from V&V and IV&V will be categorized into five levels (very high, high, medium, low, and very low). There exist many unlikely branches, which can be trimmed. For example, when the initial defect density is low, the resulting V&V defect density cannot be *very high* or *high.* For the remaining branches, since there is no evidence of their occurring frequencies, we may assume evenly distributed probabilities among them. We calculated the numbers of occurrences in each level of the product's final defect density for the cases with IV&V and that without IV&V. Resulting figures are shown in Table 1. After getting the occurrence counts, we can draw the risk profile graph as shown in Fig. 6, where the region under the dashed line represents acceptable risk.

Step 5: Performance Monitoring (Update BBN based on performance data)

If IV&V requirements is relaxed then a performance monitoring scheme is needed. Once the project starts, more information can be gathered. The BBN built in Step 2 can then be used to assess the potential risk of the project. BBN can be employed to constantly monitor and assess the potential project risk using the evidence (data) observed during the progress of the project. Predictions can be made to answer the what-if questions; thus, appropriate process and resource adjustment can be made based on BBN assessment.

Two extreme cases were examined to judge the effectiveness of IV&V. Case 1 deals with a good quality product with capable internal V&V team. Case 2 considers a poor quality product with low capability internal verifiers. In the former, the costly IV&V is not justified; while in the

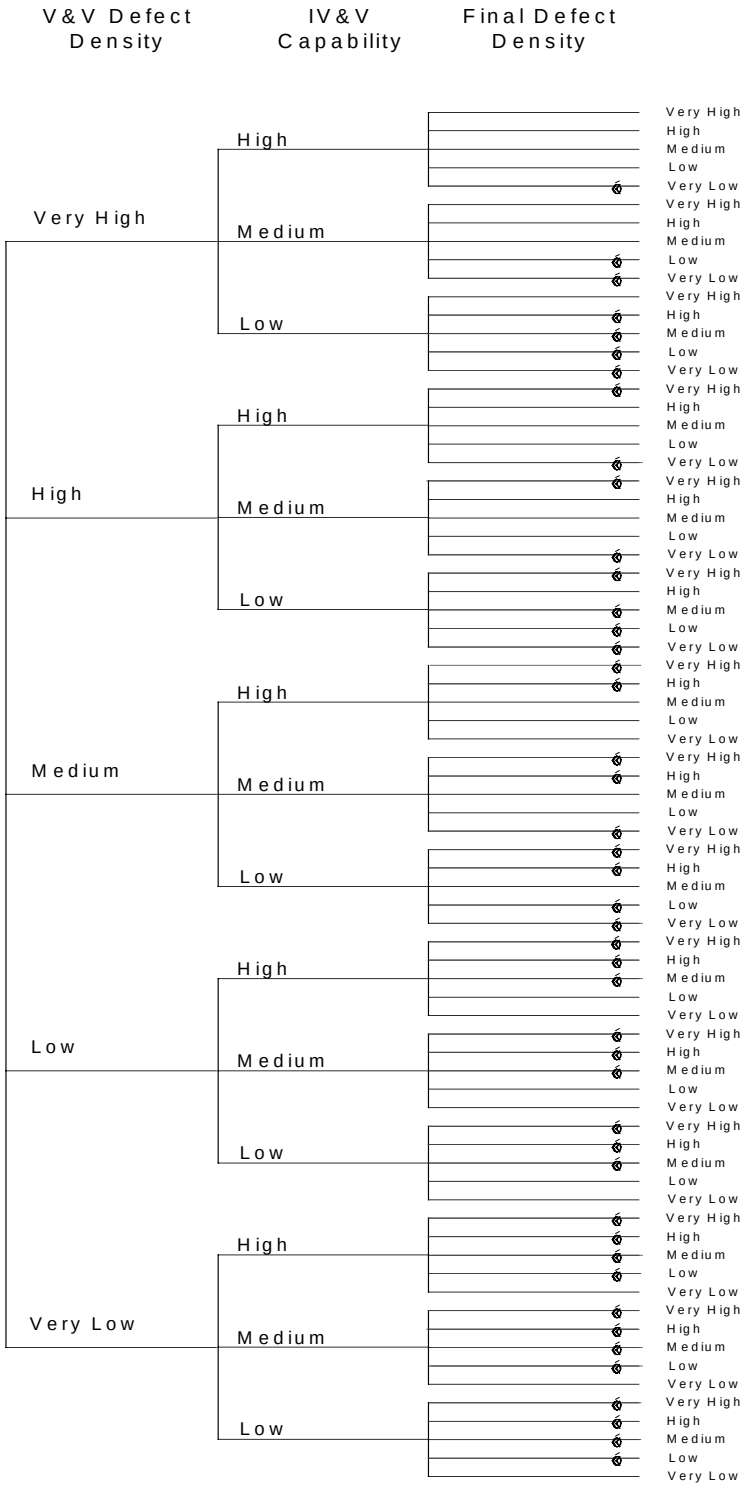


Fig. 5. Partial event tree for simplified IV&V

Table 1. Counts of resulting branches in the event tree

Item counts	With internal V&V & IV&V	Without IV&V
Total branches	1350	90
trimmed	1058	42
Valid	292	48
Final defect density(=*very high*)	12/292=0.041	4/48=0.083
high	41/292=0.140	11/48=0.229
medium	78/292=0.267	16/48=0.333
low	94/292=0.322	12/48=0.250
Very low	67/292=0.229	5/48=0.104

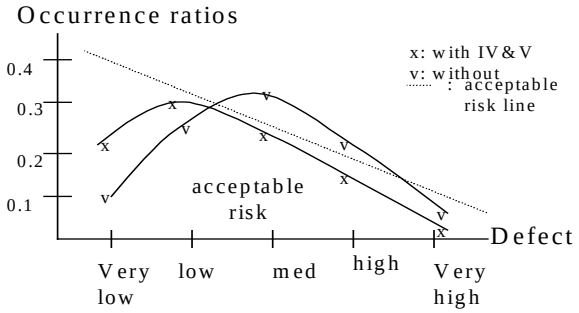


Fig. 6. Risk Profile generated by factors with equal probabilities

latter, IV&V does greatly improve the product quality. It can be seen from this risk profile that whether IV&V is conservatism really depends on various initial conditions. That is, the conservatism can be determined only after these initial conditions are identified. This figure can also be used to explain why Sizewell B was an over-killed case and K6/K7 was successful.

Conclusion

It is a consensus view between licensees and regulators that there may exists unnecessary conservatism in current digital I&C QA regulatory requirements. If such conservatism can be identified and reduced then the limited resources of both licensees and regulators can be utilized more effectively. The goal of RIPBR promoted by USNRC is to provide a generic regulatory framework to eliminate such conservatism in all NRC's regulatory activities (NRC, 1995). However, in order to take the advantage of RIPBR, one needs to develop techniques to *identify* unnecessary conservatism, and such techniques have not been fully established for digital I&C systems yet. This paper proposed a Bayesian-based approach to identifying unnecessary conservatism in current digital I&C QA program requirements. A QA program causal influence model is developed first, and then a correspondent event tree enumerating potential scenarios is derived based on this model. Thus risk insight into different QA activities can be investigated by comparing their contribution to scenario results. The QA activities that do not have significant impact on results apparently can be classified as unnecessary conservatism. *Independent V&V*, prescribed by RG 1.168, is selected as a case study using the proposed technique to assess its necessity.

In summary, the proposed Bayesian approach appears very promising in supporting the RIPBR practice for digital I&C QA programs. However, there is still more work yet to be done before this technique can be fully utilized; for example, issues of uncertainty, sensitivity and importance, criticality measures, etc.; all are necessary information items to be submitted in a formal RIPB application. In the future, we will conduct a more comprehensive investigation to consider more QA related factors and to develop methods to address the sensitivity and uncertainty issues.

References

(Apastolakis, 2000) Apastolakis, G, Speech presented at Atomic Energy Council, Taipei, Taiwan, July 17,2000.

(Arthur, 1999) Arthur, J.D., et al., Evaluating the Effectiveness of Independent Verification and Validation, *IEEE Computer* 32(10): 79-83.,1999.

(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.

(Gruman, 1992) Gruman, G., Under Pressure, NASA Renews IV&V Contract, IEEE Computer, p.106, November, 1992.

(Hayhurst, 1999) Hayhurst, K. et al., Streamlining Software Aspects of Certification: Report on the SSAC Survey, NASA/TM-1999-209519, August 1999.

(Jensen, 1996) Jensen, F. V., *An Introduction to Bayesian Networks*, UCL press, 1996.

(NRC, 1995) NRC, Use of Probabilistic Assessment Methods in Nuclear Activities, Final Policy Statement, Federal Register, V60P42622, August, 1995.

(NRC, 1998a) NRC, RG 1.174: An Approach for using Probabilistic Risk Assessment in Risk-Informed Decisions On Plant-Specific Changes to the Licensing Basis ,

(NRC, 1998b) NRC,RG 1.176 An Approach for Plant-Specific, Risk-Informed Decision-making: Graded Quality Assurance

(MacLachlan, 1994) MacLachlan, A, French Regulators 'lost hope' of Proving Chooz-B Digital I&C System., *Inside NRC*, 30 May, p6-7, 1994.

(Marshall, 1994) Marshall, P and Silver, R. Sizewell B Computer Controversy Looms Over Fuel Load Schedule, *Nucleonics Week*, 34, p1. 1994

(Padberg, 1999) Padberg, F., A Probabilistic Model for Software Projects, ESEC/FSE'99, LNCS 1687, pp.109-126, Springer-Verlag, 1999.

(Raffo, 2001)NASA, Financial Measures for Evaluating Software IV&V Activities, www.sba.pdx.edu/faculty/davidr/draccess/web/reasearch

(RTCA, 1992) RTCA/DO 178B, Software Considerations in Airborne Systems and Equipment Certification, Dec. 1992. (Waite, 2000)

Waite, C., Digital System Assessment: Great in Practice, But It Will Never Work in Practice, NPIC&HMIT 2000, Washington DC, Nov. 2000.

(Yih,1999) Yih, S, Chan-Fu Chung, 1997~1999 Lungmen I&C Licensing Progress Report, AEC Internal Report, Oct.,1999.

(Yih, 2000) Yih, S, et. al., The Applicability of Applying Risk Informed Performance Based Approach to Digital I&C Regulation, NPIC&HMIT 2000, Washington DC, Nov. 2000.

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

Implementation of Software Independent Verification and Validation for Lungmen Distributed Control and Information Systems

Jiin-Ming Lin[1] - Jeen-Yee Lee[2]

[1]*20F, 242, Roosevelt Road, Sec. 3. Taipei, Taiwan Power Company, Taiwan, ROC*
Tel.: +886 2 23667165, Fax: +886 2 23671675, U827725@taipower.com.tw

[2]*20F, 242, Roosevelt Road, Sec. 3. Taipei, Taiwan Power Company, Taiwan, ROC*
Tel.: +886 2 23667156, Fax: +886 2 23671675, D02705@taipower.com.tw

Summary

This report presents the implementation of the software independent verification and validation (IV&V) for the Distributed Control & Information Systems (DCIS) of the Lungmen Project. It covers the codes and standards as applicable, the scope of the software IV&V and the documents reviewed, the organizational structure and activities for performing the IV&V work. Furthermore, the problems which were encountered during the implementation are discussed, along with solutions for them.

1. Introduction

Digital instrumentation and control systems share data transmissions, functions, databases, and process equipment to a much greater degree than analog systems. While this sharing forms the bases for many of advantages of digital systems, it also raises concerns with respect to its vulnerability to a different type of failure. A concern is that using shared databases and process equipment has a potential for common cause failure in redundant equipment. Another concern is that the software, if not properly designed, may have errors which may defeat the redundancy achieved by the hardware architectural structure. Because of these concerns, the software of digital I&C systems must be verified and validated by a rigorous certification process to ensure with high confidence that the requirements of the software were met. This is particularly important for applications in nuclear power plants.

Based on the country of origin concept, in performing the software V&V for the Lungmen project, the USNRC Standard Review Plan (SRP) Chapter 7, BTP-14 and USNRC Regulatory Guide 1.168 are followed. Two teams-the GE independent verification and validation team (GE IVVT) and the owner (the TPC) IVVT (OIVVT), are organized by GE and TPC respectively to carry out the IV&V tasks.

In this paper, Section 2 first presents the codes and standards as applicable. In Section 3 we describe the scope of the software IV&V and documents reviewed. In Section 4 we describe the organizational structure and the IV&V activities performed at different levels of the organizations. In Section 5 we discuss the problems encountered during the implementation process, along with solutions for them. Finally, conclusions and recommendations are given.

2. Applicable Codes and Standards

Codes and Standards that are applicable for the software development and IV&V in the DCIS for Lungmen Project are primarily those of the country of origin, i.e., the United States of American. The major Codes and Standards are as follows:

- 10 CFR 50, Appendix B
- Regulatory Guide 1.168, Verification, Validation and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Sept. 1997
- NUREG/CR-6101, Software Reliability and Safety in Nuclear Reactor Protection Systems, Nov. 1993
- Lungmen Standard Review Plan (SRP), Chapter 7, Branch Technical Position (BTP)HICB-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation & Control Systems.
- IEEE 1012-1986, Standard for Verification and Validation Plans
- IEEE 1028-1994 Standard for Software Reviews and Audits
- IEEE 7-4.3.2 1993, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.
- EPRI TR-106439, Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment in Nuclear Safety Applications.

3. IV&V Work Scope and Documents Reviewed

All safety systems of the Lungmen plant are covered in the software IV&V work. In addition, five (5) R (reliable)- class systems are selected and included. The work scope is described in this section. Design documents related to all of these systems are reviewed by the OIVVT, the GE IVVT reviewed only design documents related to safety systems.

3.1 Safety Systems

There are five safety systems in Lungmen DCIS. They are Reactor Protection System (RPS), Neutron Monitor System (NMS), Process Radiation Monitoring System (PRMS), Containment Monitoring System (CMS), and Engineered Safety Features (ESF). The software development for all these safety systems follows the BTP-14 requirements. Along with the development, the IV&V activities are performed. Of the safety systems, RPS, NMS, PRMS and CMS are designed by GE NUMAC, and ESF is sub-contracted by GE to Eaton Corporation.

3.2 Control Systems (Class R system)

According to the USNRC SRP Section 7.7 requirements, control systems having a significant impact on plant safety, should be a focal point of regulatory review. Considering this five class R control systems, which are Feedwater Control System (FWCS), Recirculation Flow Control System (RFCS), Automatic Pressure Regulator (APR), Steam Bypass and Pressure Control System (SBPC), and Rod Control Information System (RCIS) are selected and included in the software OIV&V scope. For these five systems, GE sub-contracts to Foxboro with FWCS, RFCS, and APR, and Foxboro uses Intelligent Automation (I/A) Platform to perform the software development. Also, GE sub-contracts SBPC to GEIS

(GE Industrial Systems) and GEIS uses GEIS MARK VI SPEEDTRONIC turbine control system to implement software for SBPC. Still another sub-contractor from GE for the RCIS, Hitachi base on K7 experience to manufacture the I&C of Lungmen RCIS. In the development process, GE provides a system design description (SDD), hardware/software specification (HSS), hard/software I/O, and logic diagrams (LD) to sub-vendors for all functions of the above five systems. Then, the sub-vendors follow GE's requirements to develop hardware and software design.

3.3 Documents to be Reviewed

As part of the IV&V activities, the documents that are to be reviewed for Lungmen project are as follows:

3.3.1 Design Documents

For each phase, design documents of safety systems, based on SRP BTP-14, of the software development life cycle, include software plans, software requirement specification, software design output, source code listing, and test reports. These documents are subject to the IV&V review.

3.3.2 Software Safety Analysis Reports

Software safety analysis reports are prepared by the software safety engineers of software design team based on IEEE 1228-1994 standard requirements in each software development phase. These reports are reviewed by the IV&V teams.

3.3.3 Internal V&V Reports from Vendor

As a general engineering practice, most companies have design reviews or verification by peers or qualified engineers other than the engineers responsible for the work. The reports from this effort are called internal V&V reports in the Lungmen project.

- **GE NUMAC**

The internal V&V reports will be prepared by software design organization in accordance with EOP 42-6.00 (Independent Design Verification) and EOP 40-7.00 (Design Reviews) of GE engineering operation procedure (EOP) or equivalent to ensure the quality of the design process and the associated documents produced.

- **Eaton**

The internal V&V reports of Eaton will be prepared by Eaton nuclear quality assurance team based on Eaton's software V&V plan to perform the internal V&V activities. These reports and abnormal condition event reports will be summarized to V&V summary reports and delivered to GE IVVT for review.

3.3.4 The Evaluation Report for Acquired Software

Acquired software refers to:

1. Support software: such as commercially available software and development tools (i.e., compilers and databases).
2. Third party software: software produced from outside sources and incorporated into the final software-based product.
3. Previous developed software

All acquired software should be evaluated, reviewed, or tested by GE responsible engineers in design team based on relevant code or standard prior to use. Also, these evaluation reports will be submitted to GE IVVT for review.

4. Organizational Structure and Activities for Software IV&V

Software IV&V tasks of Lungmen project are performed by GE IVVT and the OIVVT. Furthermore, the regulatory authority, the ROCAEC will perform the audits, on as-needed basis, to TPC and vendor site during the software development. The organizational structure basically corresponds to the licensing frame as shown in Figure 1. Also, the software V&V activities performed at different organizational levels are briefly described as follows:

4.1 GE IVVT

4.1.1 Members

The GE IVVT members include: individuals transferred from the GENE service department that do not participate in the Lungmen design activities; qualified third-party organizations for specific independent V&V tasks; TPC engineers; experts from Institute of Nuclear Energy Research (INER).

4.1.2 Activities

The GE IVVT is responsible for

- Preparation of the software IV&V plan, according to the applicable Code and Standard in Section 2.
- Reviewing internal V&V reports, acquired software evaluation reports, software safety analysis reports, and Eaton's V&V summary reports.
- Review of all software development plans and software requirement specification based on NUREG/CR-6101 checklist for safety systems developed by GE NUMAC and Eaton.
- Preparing the sampling criteria to perform the independent review of the software design output during detail design, coding, and testing phase.
- Establishing the GE IVVT Tracking System. The GE IVVT Tracking System is for record tracking for evaluation records, meeting minutes, anomaly items, open items, and review status. This system allows GE IVVT and TPC to track the anomaly and open items.

In addition, as the consultant to the GE IVVT, Computer Dependability Associates (CDA), provides advice on GE IVVT strategy, IV&V plan and other software development Plans. Also, they evaluate the performance of GE IVVT in each software phase, and provide support in interpretation of the Codes and Standards as necessary.

4.2 OIVVT

4.2.1 Members

The OIVVT consists of members from MPR Corporation, TPC, INER, and Stone & Webster (S&W). MPR is responsible for conducting and coordinating all OIV&V activities.

4.2.2 Activities

The OIVVT performs the following activities to assist TPC in fulfilling the role of self-regulation, as expected by the regulatory authority.

- Document Reviews

Based on Section B.4 on Review Procedure, BTP-14 of SRP Chapter 7, document reviews are required to ensure that the software of GE and his sub-contractors meets the acceptance criteria as defined in Section B.3 Acceptance Criteria, BTP-14 of SRP Chapter 7.

- Site Visits:

Site visits are conducted during each phase. A minimum of 30 site visits is planned to GE and his sub-contractors. The objective of the site visit is to observe and obtain objective evidence that programs, policies, and procedures are being appropriately applied.

- Thread Audits:

Thread audits are conducted during each phase. The OIVV team will "pull" a minimum of 50 threads for audit. The objective of the thread audit is to evaluate the consistency in translation from requirements to designs through review of documents and procedures.

- Phase Reports

The OIVV team prepares phase reports and submits to regulatory authority for reference after accomplishing each phase. The report covers document review reports, site visit reports, thread audit reports, and anomaly reports completed by OIVV team during each phase. Also, all anomaly items are

delivered to GE and his sub-vendors for process, and tracked by the tracking system provided by MPR until accepted by the OIVVT

4.3 Republic of China Atomic Energy Council (ROCAEC)

As Lungmen project is the first application of software in protection, control, of a nuclear plant in Taiwan, ROCAEC has high concerns about the software development and V&V activities of Lungmen DCIS. For these activities, ROCAEC required that TPC periodically report to ROCAEC on the status of these activities. In addition, ROCAEC performed audits on TPC's management of Lungmen DCIS at TPC headquarters in April, 2000, and in June 2000, participated in an OIV&V site visit to GE, Eaton, and Foxboro to evaluate compliance by the vendor to the regulatory requirements in the software development. From these audits, ROCAEC issued audit reports requesting improvements by TPC. ROCAEC will keep performing such audits to TPC, GE, and sub-vendors to ensure the quality of Lungmen DCIS software meets regulatory requirements. .

5. Problems & Solutions

Problems that are encountered during the implementation are originated primarily from the first implementation of the related codes and standards, and include independence of the organizations performing IV&V and potential over-oversight of the software development.

5.1 Interpretation of R.G. 1.168 for Requirements on Independence

GE IVVT is organized under GE Nuclear Engineering (GENE) and is independent of the design team for the Lungmen project. However, measured from a restrictive perspective the independence of the GE IVVT is questioned, and an issue as to the interpretation of the real regulatory requirement came up. In addition, there seems to exist an inconsistency among 10CFR 50 App. B, BTP-14, and R.G. 1.168 requirements, in regards the V&V independence requirements[1]. For resolution of this issue, TPC, MPR, GE IVVT, and CDA held a meeting in San Jose in July, 1999. From this meeting, a resolution was reached based on CDA's proposed interpretation for the independence of R.G. 1.168 that "*The person accountable for V&V must also be independent of the person accountable for the design*." And that "*This independence must be sufficient to ensure that the V&V process is not compromised by schedule and resource demands placed on the design process.*" A key word here is "accountable," and it means exactly what it says. No more and no less. In GE's context, the IVVT Chairperson is accountable for the software V&V and he has sufficient independence from the designers. On this subject of independence, there is a good discussion in the 1998 edition of IEEE 1012, Annex C, which can be used for background reading and clarification.

During planning stage for the Lungmen project, TPC had surveyed the implementation of software IV&V activities in Chooz B of France and Sizewell B of U.K. Recognizing the importance of software V&V, TPC allocated a special budget for an OIV&V to enhance independence of the V&V.

In addition, due to the large amount of documentation produced during software development cycle, TPC also allocated another budget to contract with INER for reviewing all software design outputs. This also somewhat enhanced independence of the software IV&V.

5.2 Potential Work Duplicate between the OIVVT and GE IVVT

In order to augment the independence of software V&V, TPC organized the OIVVT to perform the V&V activities. This resulted in the OIVVT having scope of work which has some potential duplicate with the GE IVVT, and the software design team of GE having to make more efforts in addressing duplicated comments from GE IVVT and OIVVT, and schedule became a concern. Finally, through coordination, an agreement was reached that GE IVVT summarized the OIVVT and GE IVVT comments before delivering to GE design team for resolution. All open items were followed up through the GE IVVT tracking system. Of course, OIVVT used its own tracking system to follow up items of anomaly in design reviews, site visits, and thread audits from OIVVT activities.

When the OIVVT activities were planned to be included into the Lungmen project, GE had objection because they believed that OIVVT activities, such as site visit, would affect the design schedule. TPC clarified that the OIVVT activities would serve the function as self-regulation so as to facilitate licensing, and in the long run, would be beneficial to schedule control. This view point was finally accepted by GE and the work proceeded smoothly.

6. Conclusions

Since the establishment of the IV&V teams (the GE IVVT and the OIVVT) in 1999, the IV&V activities have been progressed smoothly. Two problems have been encountered though, but resolved. Also, from this implementation, a couple of recommendations for performing future software IV&V activities can be made. 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.

7. Reference

1. Swu Yih, et al, ":Preliminary Evaluation of NRC Digital & Regulations based on Lungmen Licensing Experiences". In NPIC&HMIT 2000, Nov. 2000.

* Note•OIVVT(Owner Independent Verification & Validation Team)
ROCAEC(Republic of China Atomic Energy Council)

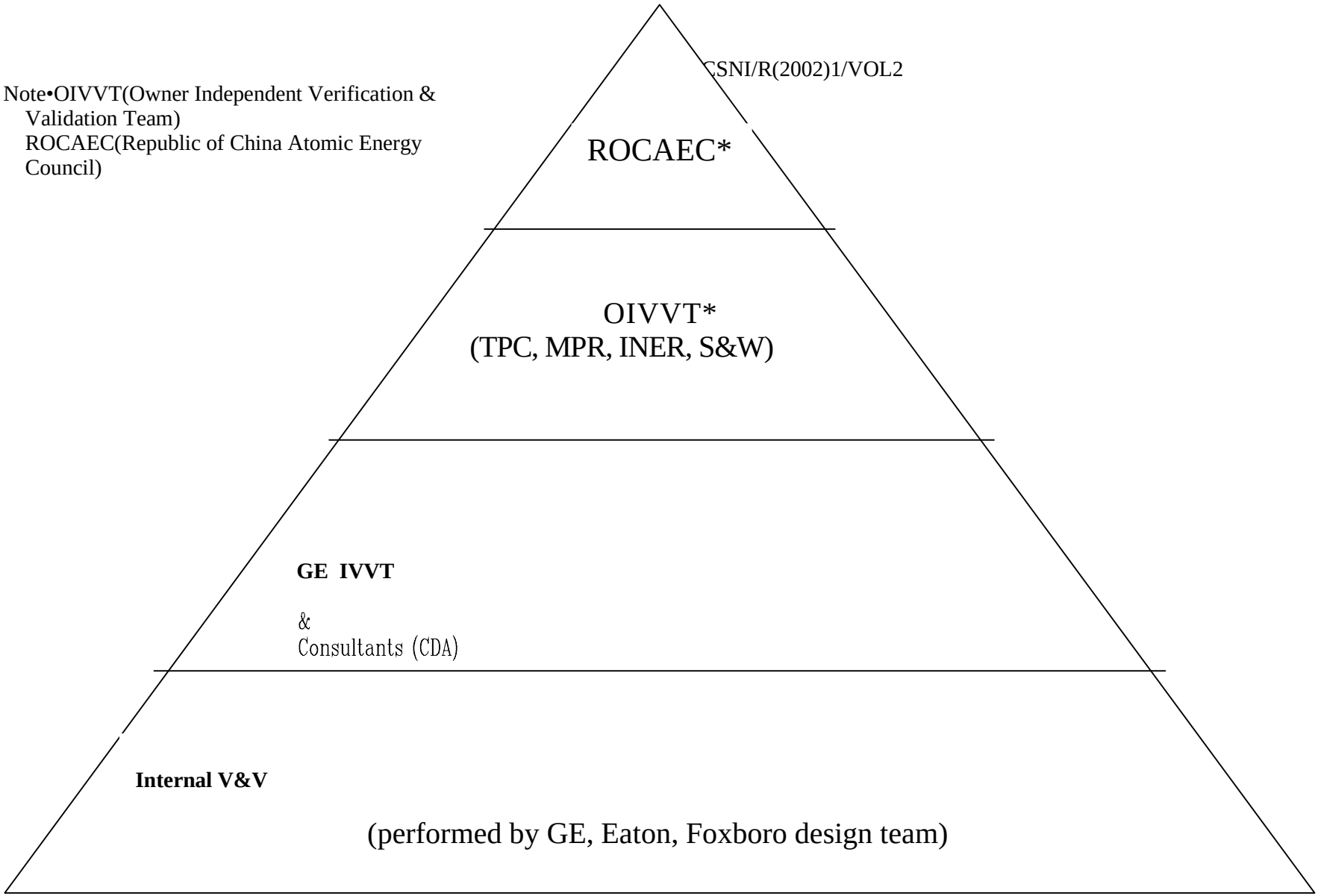


Fig. 1•Licensing frame of software IV&V on Lungmen Project

Static Analysis of the Software used in Safety Critical System of the NPP Temelin

Z. Piroutek, S. Roubal, J. Rubek

I & C Energo s.r.o., 190 11 Praha 9 – Bechovice, Czech republic
Tel.: +420 2 67062182, Fax: +420 2 67062182, e-mail: zpiroutek@ic-energo.cz, sroubal@ic-energo.cz, jrubek@ic-energo.cz

Summary

The presentation describes the Static Analysis used in project the Independent Assessment of the Temelin Safety System Software. There is described used methods, tools and process of performing of activities which were performed in collaboration of I&C Energo company with TA Group.

Introduction

The Independent Assessment of the Temelin Safety System Software was required by the Czech State Office for Nuclear Safety as a part of licensing process. The Independent Assessment was performed by the consortium under leading of American company SAIC (Science Applications Internal Corporation - founded in 1969) in 1999 - 2000. The other members of the consortium were TAG (TA Consultancy Service Ltd.), RRA (Rolls Royce and Associates Ltd.). As subcontractors were British Nuclear Electric and Czech company I&C Energo.

Independent Assessment was required on the four safety systems: Primary Protection System (PRPS), Diverse Protection System (DPS), Post Accident Monitoring System (PAMS), Diverse Monitoring System (DMS).

The assessment activities were performed on system documentation and source code included the following:

- assessment of adequacy of system software,
- verification of system requirements,
- verification of software requirements against system requirements,
- verification of source code against software requirements by using static analysis,
- dynamics testing of one PRPS division,
- verification of configuration and calibration data,
- safety case preparation.

General Description of NPP Temelin Primary Reactor Protection System (PRPS)

The PRPS is divided into three redundant reactor trip and ESF actuation safety Divisions (Divisions I, II and III). All reactor trip and ESF actuation Divisions are physically and electrically separated from each other. Each of the three redundant safety Divisions is composed of safety grade field sensors, Nuclear Instrumentation System (NIS) excore flux monitoring detectors and equipment, the Integrated Protection Cabinet (IPC) and associated Reactor Trip Switchgear (not supplied by I&C vendor). Each of the three redundant ESF actuation Divisions consist of the Engineered Safety Features Actuation Cabinet (ESFAC), the Integrated Logic Cabinets (ILCs) with associated Non-Programmable Logic Cabinets (NPL), the Main Control Board and Emergency Control Board Multiplexers (MMC) and the Data Highway Gateway cabinets (DHG). The Main Control Board and the Emergency Control Board manual system level signals interface directly to the IPCs and the ESFACs via hardwired I/0 lines. Manual control of each of the ESF components in each Division is provided through the Control Board Multiplexer cabinets to the Integrated Logic Cabinets over the optical Logic Bus data highways.

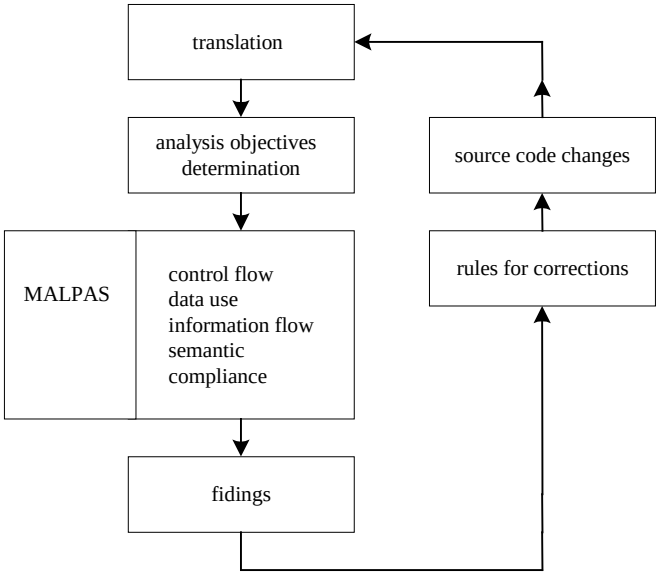
Static Analysis

The standard way of the SW testing is to use the dynamic testing method when the testing data are entered to the code input and the calculation is performed consequently. The results of this calculation are then compared with expected values and evaluated. However, this method is based on testing on the target hardware, but for large distributed system like protection system the problem of generating test data which exercises every path through the software adequately, in insoluble. Static analysis, which used mathematical techniques, is capable of achieving full path coverage. Using such technique it is therefore possible to demonstrate to high degree of confidence the absence of errors.

For complete static analysis the support tools are necessary. Such a tool can be the MALPAS code of English company TAG, which has been originally developed for military purposes and modified for civil purposes consequently. MALPAS uses directed graphs and regular algebra to represent the program under analysis. This tool was successfully used for independent testing of the protection system of the Sizewell B NPP in the UK. Because the similar protection system is used also in case of the Czech NPP Temelin, this tool was used for testing of the reactor protection system (PRPS and DPS). Our company I&C Energo participated under this project. of Independent Assessment of the Temelin Safety System Software.

Scope of Static Analysis

The static analysis process can be drawn in the following figure:



Documentation
Requirements are normally specified in the following documents:
Composite Block Diagrams
Software Design Description
Software Requirements Specification
Software Design Specification
Application Data Sheet

The main stages in the analysis process can be divided in the following:
- Translation + Review
- Goal Setting
- Syntax Analysis
- Semantic Analysis
- Optional Review
- Compliance Analysis
- Creation of PROCSPECS
- Review
- Finding + Sentencing

Translation

The first stage in the analysis process is to perform translation of the source code into MALPAS Intermediate Language (IL) program.
The translation process adopted for each of the safety critical modules consists of the following stages:
- Perform the actual translation. This may involve some degree of modification to the source code (pre-translation edits). Translation of a module is normally possible when PROCSPECs of the procedures are available.
- Perform any necessary post-translation edits.
- Run the IL Reader to identify all remaining IL errors.

The translation report shall be written including the resolution of errors and warning messages, any pre or post translation edits that were made.

Goal Setting

The goal setting is the process by which correctness properties are identified and the corresponding analysis objectives are captured. It is necessary to perform a subsystem - wide review of the software to identity correctness properties and corresponding analysis objectives prior to the start of the analysis proper.

These fall into two categories:
- Ensure integrity of language use (goal setting identify functional integrity properties, non-functional properties are checked by the other MALPAS analysers).
- Identify hidden assumptions.

The Goal Setting report should identify the analysis objectives for each procedure in the module or subsystem. The report should also include an overview of the module or subsystem's functionality.

Syntax Analysis

Syntax analysis is a collective term used to encompass Path Assessor, Control Flow, Data Use and Information Flow analysis, and it is used for the initial investigation of the software under analysis.
Control Flow analyser examines the structure of a procedure to identify all entry and exit points. It also identifies all loops with their entry and exit points. Control flow analysis also reveals more serious errors within the source code such as unreachable code and dynamic halts.
Data Use analyser checks how data (variables and formal parameters) is used within the procedure and from this one can check (for example that all outputs are written on each path through the procedure).
Information Flow analyser identifies all information upon which each output depends and provide an initial check that the procedure outputs are depend upon the correct inputs. If the dependencies are specified in a

DERIVES list than the analyser compares these against the calculated dependencies. DERIVES list reflects the intended or specified information flow properties. The aim of Data Use and Information Flow analysis is to choose access modes that reflect the true data use properties; not to get empty error sets.

When completing the Syntax Analysis report care must be taken that all the sections of the report are completed correctly. The Syntax Analysis report should provide a complete description of the Syntax Analysis activity in terms of changes made to the IL model, the classification of parameters given access mode and any anomalies discovered.

Semantic Analysis

The principal aim is to show conformance of the source code to its design documentation. The analysis identifies each path through the procedure by a condition on the input value. For each path, the analyst reveals the actions taken when the path condition is met. The analyst should then compare this against the design documentation to decide if the procedure will behave correctly.

The analysis has the following objectives:

- checking that each source module implements its module design specification,
- correctness of real arithmetic will be informally considered,
- consider the possibility of overflow during expression evaluation without making implementation dependent assumptions about order of evaluation,
- possible ambiguities are flagged and explained,
- only legitimate values are written to variables,
- confirm that base pointers are correctly set for all accesses to based variables,
- aliasing of parameters does not occur,
- addressability of objects is investigated where necessary,
- all preconditions for changed to the IL model should be formalised in IL wherever possible,
- demonstration that return values for typed procedures are well-defined for all inputs.

At completing the Semantic Analysis report care must be taken that all the sections of the report are complex correctly.

PROCSPEC

PROCSPEC is an IL representation of the interface and behaviour of an analysed procedure, and is used in the Malpas analysis of higher-level procedures. When an analysis subtask is completed, it is subjected to review. Once the analysis is judged satisfactory and approved, any PROCSPECs are released for use in subsequent analyses.

The PROCSPEC file is produced for each procedure and the analyst should test it.

Peer Reviewing

All the analysis work shall be reviewed to ensure that it meets the required standards. The aim of reviewing is as follows:

- to ensure that specified quality standard was met,
- to ensure that all found anomalies were adequately reported,
- to assist in achieving consistency of analysis among the assessment team,
- to identity inconsistencies in the specifications and coding of different parts of the SW,
- to agree a satisfactory interface description of each procedure.

The Review Comments form is used to record all deficiencies found in an analysis during the course of a review. All work performed to correct deficiencies identified during a review shall be documented to the same standard as required for the original work by updating the analysis report as necessary. If the rework requires any of the MALPAS analysers to be re-run, the analysis record should be updated to record the new files created. However, the previously reviewed files should still be recorded on the analysis record.

Finding

As the analysis proceeds, anomalies are found in the software or its documentation, and are documented in the various analysis reports. Anomalies shall be reported as findings.

The following activities are:

- Anomaly categorisation
- Finding reporting
- Finding sentencing

Process Activities to Quality Assurance

Training

In order I&C Energo to undertake work on the static analysis it was necessary for them to resource up team of software engineers who could be trained and work in English and be capable of undertaking the technical analysis to the required standard. In order to facilitate this initial training course in the UK for several I&C Energo engineers was organised. After this course these engineers led the I&C Energo analysis work in Czech Republic and provided the necessary technical interaction with TAG. Also, they held technical training courses for the other I&C Energo engineers.

Engineer Selection and Qualification Acceptance

I&C Energo engineers were selected by I&C Energo management based on their technical experience and training plus feed back from the team leaders on particular skills considered to be important. During the first month of the Czech training course TAG was provided with feedback from I&C Energo on the progress of each engineer. When I&C Energo team leaders had been satisfied that an engineer can perform the analysis to an acceptable standard one of the last analysis undertaken was provided to TAG for review. TAG examined the technical accuracy of the work to confirm that it is technically correct and contains the correct information. Based on this review this engineer became a full team member.

I&C Energo's Review of Completed work

As part of the analysis process it was required that all analyses were peer reviewed and then updated to take account of the comments raised in the review. The Czech team leaders undertook an additional review of each analysis and the analysis report in particular to confirm that it met the required technical standard. All work was countersigned to indicate that such a review has taken place and found to be acceptable.

TAG Review and Acceptance of Completed Analyses

A technical review of all work delivered to TAG by I&C Energo was undertaken. This review has ensured that all outputs were complete and that build standard references were correct. The review also confirmed that the anomaly report was supported by the analysis. The annotations were also examined to confirm that they were sensible and appropriate. If the raised problems could not be satisfactorily resolved by email/fax then the rework was required and a new delivery of outputs and results prepared by I&C Energo and subsequently delivered to TAG for acceptance.

TAG Sample Audits

The acceptance process outlined above has ensured that the work delivered by I&C Energo is consistent, complete and from a brief review is technically acceptable. The acceptance process did not provide a full and detailed confirmation of the correctness of the work as this would require much of the analysis to be repeated by a TAG engineer. However, to provide added assurance that I&C Energo are providing work at the required standard a sample audit was undertaken of delivered analyses.

The audits were be organised so that all engineers on the team were examined at least once during the period of the I&C Energo work programme.

Resource Planning

The need to plan the way, in which the work was performed, was under continuous management attention in order to prevent non-productive effect. To minimise non-productive effort the decomposition procedures were examined by TAG and I&C Energo and detailed plans were prepared for each software module and progress monitored during analysis.

Progress Reporting

After the end of each accounting month Progress report was prepared and sent to TAG providing a monthly overview of work performed on the static analysis an the time sheets of each engineer. The progress metrics developed by TAG was applied on the analysis activities assured overview of the development status of each analysed module.

Risk Management

The potential risk for the project was evaluated at the first phase of the project (during the training of two I&C Energo training in the UK). The minimisation of the risk was solved by the introduction of the Czech language for the work, by strict selection of the candidates for the work and by good preparation of the training process and organisation of the real analysis. At the current time it is considered that this solution has been effective.

Quality Control

I&C Energo‘s Quality Control was defined in the I&C Energo document „Quality Assurance Programme“ prepared as part of the subcontract work. This programme deals with the whole process from the general company quality system, subcontract review to quality assurance and control during the project realisation.

The scope of the main quality objectives was the following:

- to meet TAG technical and quality requirements of the contract specification,
- to assure that quality, audits, reviews and inspections will be performed according to the Quality Assurance Programme and procedures and applicable codes or standards,
- to achieve professional level comparable with TAG,
- to assure that all significant deviations from specification, procedures, etc., will be submitted to TAG for review before applying,
- to ensure that the Quality Assurance Programme will be correctly applied.

Configuration Control

Configuration management process was defined in the I&C Energo document „Configuration management for Static Analysis”. This document ensured that all elaborated input/output software files had been correctly and consistently configured on VAX computer and all elaborated report on PC so that TAG could provide an identical file structure for VAX computer or PC and the contrary I&C Energo to TAG.

Conclusion

The used approach for the Static Analysis of software used for the Independent Assessment of the Temelin Safety System Software was cost consuming. However it makes possible to discover software anomalies which could be not found in manual check. It results from experience, that this way of assessment software is suitable not only for safety control system analysis in nuclear power systems but for transport and aviation as well.

Assessment Methodology of the Temelín NPP Control System Performance and Quality

I. Petružela [1], K. Bednařík [2], J. Rubek [3]

[1] *I&C Energo, Areál VÚ, 190 16 Praha 9 - Běchovice, Czech Republic*
Phone: +420 2 6706 2181, Fax: +420 2 6706 2182, e-mail: ipetruzela@ic-energo.cz

[2] *I&C Energo, Areál VÚ, 190 16 Praha 9 - Běchovice, Czech Republic*
Phone.: +420 2 6706 2185, Fax: +420 2 6706 2182, e-mail: kbednarik@ic-energo.cz

[3] *I&C Energo, Areál VÚ, 190 16 Praha 9 - Běchovice, Czech Republic*
Phone: +420 2 6706 2183, Fax: +420 2 6706 2182, e-mail: jrubek@ic-energo.cz

Summary

The performance and quality of the NPP Temelín control system is demonstrated by means of tests during the power ascension testing stage. A methodology has been developed in I&C Energo for the test assessment in which there are defined criteria determining the grade of meeting the design requirements. The assessment of the control process quality is based on the evaluation of the behaviour of the main controlled quantities in the course of transients of the test.
The design responses of the transient processes have been acquired by means of the unit model DYTE. Eight criterial conditions are assessed which are posed on the controlled quantities. It is by meeting these criteria that it can be demonstrated that control system quality corresponds to the requirements defined in the design specifications. The criteria structure makes possible an automated processing of the measured data.

1. The Method Of The Control System Quality Assessment

A control system makes it possible to purposeful act on the controlled object so that the required conditions of the process system are always reached in compliance with the design, at meeting technical standards and regulations. The supplier of the control system is obliged to demonstrate to the customer both performance and quality of the provided work.

The control quality parameters are always defined by the customer and they become then an integral part of the design. Already in the course of the control system development, definitions of the control system quality features are mutually agreed upon, including the methods and conditions under which the required quality is to be achieved.

For complex process facilities, the criteria for the control system determination would not be unambiguously established. In practice, the assessment of the controlled technology process at dynamic events is used for the evaluation of the control system quality. The control quality is then assessed by means of the response patterns to a unit impulse or to a unit jump or by means of integral criteria.

At the Temelín NPP, the I&C supplier is not the supplier of the technology in the same time. That called for the need of an exact formulation of the control system quality criteria. The criteria serve for the check whether the unit control system (major unit controllers, logical control, limitation system) perform in compliance with the design requirements.

1.1. Mathematical Formulation of the Control Quality in Complex Processes

The NPP process system can be subdivided into the controlled object and to the control system. The controlled object are the process systems that are usually mutually interconnected, complex non-linear systems. From the mathematics point of view

- it is composed from finite number of elements each of which is unambiguously described by a finite number of measurable quantities
- it has mutual links among the elements unambiguously formulated

Therefore, we can describe the dynamic features of the controlled object by means of differential equations the solution of which is a status vector. The status vector enables us to determine the system conditions at any time by means of a minimum number of quantities.

The control system must maintain certain physical quantities at predefined values. During the dynamic processes the control system modifies the process system conditions through action quantities so that design conditions are to be achieved. The mathematical notation of it is the following equations system

$$\dot{\vec{x}}(t) = \vec{f}[\vec{x}(t), \vec{v}(t), t] + G[\vec{x}(t), \vec{v}(t), t]\vec{u}(t) \qquad (1)$$

where there is

$\dot{\vec{x}}(t)$ the derivation of the status quantities vector (change of the TP status)

$\vec{x}(t)$ the status quantities vector (TP status)

$\vec{f}[\vec{x}(t), \vec{v}(t), t]$ the vector function (TP description)

$\vec{v}(t)$ the perturbation variables vector (TP perturbations)

$G[\vec{x}(t), \vec{v}(t), t]$ the functional matrix (describing the control system

$\vec{u}(t)$ the control variables vector (status of the control system)

If the control system meets all requirements defined in the design specifications, the time courses of the status variables vector $\vec{x}(t)$ achieved at the power ascension testing must be equal to those acquired in analyses provided by the manufacturer. A deficiency of this procedure is the fact that the above shown formalized notation is impossible with complex process systems and that not all status variables are measurable.

Therefore, the control quantities vector $\vec{r}(t)$ is used instead of the status quantities. In the course of the control process, the real values of the controlled quantities are measured and compared with the required values $\vec{z}(t)$. In accordance with the found deviations, individual controllers intervene into the process in compliance with the design requirements. The control deviations vector is marked $\vec{e}(t)$. The shown equation system (1) is reformed to:

$$\vec{r}(t) = \vec{f}\left[G\left(\vec{z}(t) - \vec{r}(t)\right), \vec{v}(t)\right] \qquad (2)$$

The diagram on the Fig. 1 corresponds to this simplified equation

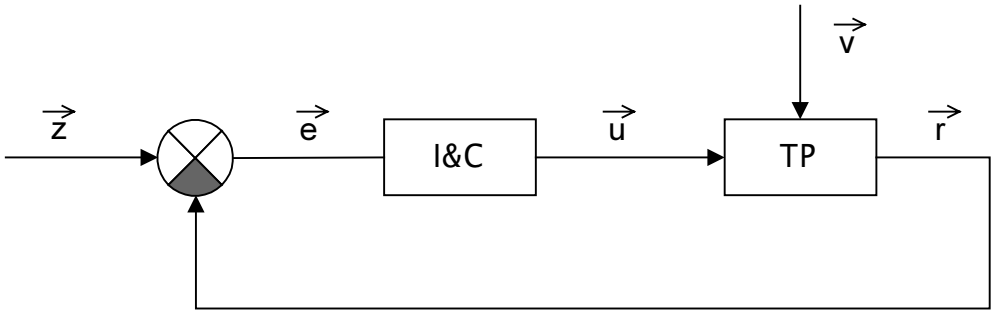


Figure 1: Principle diagram of the process control

1.2. Requirements Posed by the CSN on the Process Control Systems and on the Methods of Their Assessment

Generally, we can perform assessment of the control features of the control systems in the following states of the process system

1. steady state operation
2. transients (changes of the controlled quantities from the time $t=t_o$ into the state in time $t=\infty$)
3. long-term operation (stability of the results of the repeating control processes)

The behaviour of the shown states is not exactly defined in the standards and there is a requirement that the corresponding indicators must be a part of the supply of the manufacturer.

The first two states relate to the assessment of the dynamic features of the system at control as the result of the change of the process state (e.g. power change, failures of the equipment functions or due to fluctuations of the measured values. The third is used for the judgement of the fact whether the achieved quality has a long-term character. The basis is the comparison of the repeated processes. During the Temelín NPP commissioning, it would mean an exact circumscription of the controlled processes that will be more times repeated during the commissioning period under the same or similar conditions. Therefore, the indicators of this did not become a part of the control system quality assessment even if the I&C system supplier gives the necessary data in the documentation.

The methods of the assessment of the process control systems in accordance with ÈSN 180005 are based on the determination of the characteristics of the required functions accuracy meeting. Those functions are subdivided into

- static transfer function
- dynamic characteristics

1.3. Description of the Accuracy Characteristics of the Required Functions Performance

Static transfer function. It is the dependence of the output signal values on the values of the input signal or of the measured quantity or on the physical quantities coming to the input in the steady state.

Generally, it is determined as the line fitted to average values of the monitoring results in the measurement points. The evaluated transfer function, characteristics or quantity are marked with the fact that the influence of random failures has been removed. However, they include systematic errors due to the product features.

Dynamic characteristics. It is the dependence of the information parameter of the output signal on the prescribed time change of the information parameter of the input signal. It could be expressed by

- Transfer function
- Transient characteristics
- Impulse characteristics
- Frequency characteristics

The complete dynamic characteristics is a graphical transformation of the dynamic behaviour of the product at prescribed time changes of the input signal. There are given the following partial dynamic characteristics.

- Amplitude-frequency characteristics
- Phase frequency characteristics.
- Stabilization time
- Time of transportation delay
- Time constant
- Time of overshoot
- Value of maximum overshoot
- Time of the query

1.4. Assessment of the Control System Quality

The basic condition of the correct performance of the controlled process is its stability. The system is in an equilibrium state if the controlled quantity does not change with the time. The control is stable when the system returns into the original equilibrium state within a period after the system's deviation from the steady state and removal of the reason of the perturbation (that caused the deviation).

Simplified, we can say that after the transient event decay the controlled quantities stabilize within the band defined by the design and the control vector is no more changed. The band is called the control accuracy.

The stability condition is a necessary, however, not a sufficient condition of correct performance of the regulated systems. The behaviour of the systems is essential during the transient that could have various patterns. The system is controlled foremost for failure responses of the unit jump pattern since this is one of most adverse events that could be mastered by the control.

The most accurate picture of the system behaviour can be acquired by the explicit solution of the differential equations system. Due to the difficulty of an accurate formalization of all terms of the equations is the quality of the control process mostly defined as selected parameters of the dynamic characteristics. The deciding aspect is the way and velocity of the new required system state achieving.

The system assessment lies in the check of

- rated static transfer functions
- rated complete dynamic characteristics

The requirement of all Czech standards is that the system dynamic features must be described by the manufacturer and the description must be part of the delivery.

2. Draft Of Criteria For The Assessment Of The Temelín Npp Unit Major Controllers

2.1. Indicators Assessing the Process Control Quality at the Temelín NPP

In the preceding chapter, optional approaches have been presented to the assessment of the control systems quality. Not all of them are applicable for the NPP Temelín control system assessment. We have selected several basic indicators from the standards by which we will characterize the control process quality at the Temelín NPP. Those are:

1. the control accuracy- gives limits in which the control circuit keeps the controlled quantity
2. the control time (response time) - is the time period that lapses from the start of the perturbation till the moment when the controlled quantities of the process achieve the required values with the given accuracy
3. the maximum deviation of the controlled quantity (maximum overshoot) - it is the greatest value of overshoot in the response of the closed control circuit to a jump change of the specified quantity
4. the number of overshoots during the control process – it is equal to the number of extremes (maxima, minima) during the control process the value of which lies off the control accuracy band
5. the quadratic control area – the calculation of the quadratic control area is finished when the controlled quantity is kept in the limits or the operator intervenes into the process

In the same time, we have to supplement the above shown parameters by parameters that characterize safety. The system must not cause by its action any possible dangerous conditions in its surroundings. The safety properties of the instrumentation and control system of industry processes (mechanical, electrical, etc.) depend on its own (intrinsic) system safety and on external (extrinsic) aspects on the protection included into the system.

2.2. Design, Power Ascension Tests

We have to make the above shown concrete at the generation of criteria in accordance with the design documentation (diagrams of the control circuits, setup of the control circuits constants, accuracy of the control circuits). This is based on data given in the following documentation:

- The requirements on the unit control system in the scope of reactor protection, limitation systems and unit control, A1-3.2, EGP Praha, December 1993
- Reactor Control and Limitation System dPS-202A, Functional Design Report, TEM-I&C-RCLS-014, Revision 5, January 2000
- PCS Control Builder, TEM-I&C-PCS-2161, Revision 3, May 2000
- Nuclear Unit Operation Modes - 1st stage, dÚP (Supplement of the Input Design) No.463, EGP Praha, March 1998

The check of the design is performed during the power ascension stage of the commissioning by means of special tests a part of which will be evaluated from the point of view of the major control circuits quality.

We can acquire the necessary examples of the transient characteristics by means of a model that describes the simulated object in terms of mathematical equations. The equations are currently available and create a basis of the DYTE simulation code. The code makes it possible to acquire the missing transient characteristics of the non-linear systems of the Temelín NPP units. (As is shown on figure 2.)

The assessment of the Temelín NPP units major controllers performance can be then based on the evaluation of the control process quality of selected tests and their comparison with the design

specifications. The success of the tests, i.e. statement „complied - not complied„ corresponds to the degree of meting the criteria that characterize the control process quality.

After the test completion, following questions are assessed from the point of view of major control circuits quality:

1. Steady system state
   - stability of the steady state
   - variation band in the steady state (control accuracy)
2. Transient process of the controlled quantity
   - the time of achieving the target steady state (control time)
   - the maximum overshoot
   - the number of overshoots during the control time
   - the way of achieving the steady state (quadratic control area)
3. Functions of the logic circuits
   - the performance of the logic circuits of the major controllers including the Control Coordinator (CC) in the transient process
   - the following of the desired value in the controllers that are not in action
4. CC, Limitation System (LS) and local protections performance
   - in case of LS actuation (in accordance with the design) time and reason of the LS actuation are evaluated
   - the actuation of local protections during the transient process
   - the margin to CC, LS or local protections actuation due to other reasons

2.3. Major Control Circuits and Controlled Quantities

The Temelín NPP unit control system is a sophisticated complex of mutually interconnected controllers, limitation system and protections. Individual control circuits have different effect on the way of achieving the desired state. From this aspect, we can select the so-called major control circuits that are part of the unit power control. In the CC documentation there is given the control accuracy that is in sense of the first chapter one of the most important parameters of the static characteristics. U the reactor controller has as well given insensitivity, i.e. magnitude of the deviation within which the controller does not respond. The parameters are shown in the following overview table:

Control circuit	Controlled quantity	Accuracy	Insensitivity	Units
Reactor controller	Reactor power	±3	±2	%
	Steam pressure	±0.2	±0.13	MPa
	Average temperature	±1.5	±1	°C
Turbine controller	Turbine power	±10		MW
	Steam pressure	±0.07		MPa
Controller of the steam dump to condenser	Steam pressure	±0.1		MPa
PZR pressure controller	PZR pressure	-0.12		MPa
	PZR pressure	+0.2		MPa
PZR level controller	PZR level	±15		cm
SG feeding controller	SG level	±1 to 3		cm
Deaerator level controller	Deaerator level	±2.5		cm
Deaerator pressure controller	Deaerator pressure	±0.05		MPa

The quantities on which the controllers act are the main controlled quantities. They represent the basic part of the state vector. Therefore, we can assess the Temelín NPP control system quality based on their evaluation.

2.4. Indicators and Criteria Definitions for the Assessment of the Performance of the Temelín NPP Unit Major Controllers

Based on the preceding analysis, we can assess the control system quality by eight indicators of dynamic characteristics of the main controlled quantities. Those are

K1 Control quantity variation band width after the transient decay

K2 Control time, i.e. the time necessary to bring the controlled quantity into the K1 band from the start of the actuation event

K3 Magnitude of the quantity maximum overshoot during the transient

K4 Number of the quantity overshoots during the transient off the K1 band

K5 Magnitude of the quadratic control area of the controlled quantity

K6 Performance of major controllers logic circuits including the CC during the transient

K7 The method of following of individual setting devices of the CC and of the major unit controllers

K8 The magnitude of margin to LS, protection system and local protections actuation

These indicators are required in the form of numeric values for analogue quantities (K1 through K5 and K8), for the logic circuits in their state (K6 and K7).

A criterial conditions corresponds to each indicator that determines the boundary between “satisfied-not satisfied” at the control system assessment. The criteria 1 through 5 relate to main controlled quantities, the criteria 6 and 7 to the activity of major unit controllers including the CC and LS, the criterion 8 relates to LS, protection system and to local protections.

Criterion 1 – the achieving of the system target state the variation of which in less than the control accuracy defined by the design is considered satisfying

Criterion 2 – the achieving of the control time that does not exceed the control time defined by the design (or in accordance with the design conditions determined by the DYTE model) is considered satisfying

Criterion 3 – not exceeding of the overshoot magnitude that is defined by the design (or in accordance with the design conditions determined by the DYTE model) is considered satisfying

Criterion 4 - not exceeding of the overshoots number that is given by the design (or in accordance with the design conditions determined by the DYTE model) is considered satisfying

Criterion 5 – achieving of the quadratic control area that is less than the quadratic control area defined by the design (or in accordance with the design conditions determined by the DYTE model) is considered satisfying

Criterion 6 – it is considered satisfying if the sequence of the activities of the logic circuits of the major controllers including the CC corresponds to the sequence required by the design (or in accordance with the sequence determined by the DYTE model)

Criterion 7 – it is considered satisfying if the following of the individual setting devices of the CC and of the major unit controllers corresponds to the design

Criterion 8 - it is considered satisfying if the minimum margin will be greater than a value agreed upon by experts

If, howbeit, a single condition is not met from the above shown, the performance of the control circuit cannot be considered a quality one.

3. Conclusion

The criteria serve to the check of the performance of the Temelín NPP unit control system (major unit controllers, logical control, limitation system) 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 criterial values make it possible to determine the achieved quality of the NPP Temelín unit major controllers after the completed test.

The construction of the criteria makes use of the automated measured data processing and makes it possible to formulate the assessment result in the form – "met, not met". Additional outputs are the determination of :

a) the magnitude (range) of the non-compliance of the real unit behaviour against the requirements of the design (or against the specifications requirements for the control system supplier)

b) the reasons of non-compliance found at testing in the frame of the power ascension stage of the commissioning

c) the impact of the found non-compliance on the further continuation of the power ascension stage of the commissioning, i.e. providing data for the Commissioning Control Group decision making, whether it is necessary to remove the reasons of the non-compliance

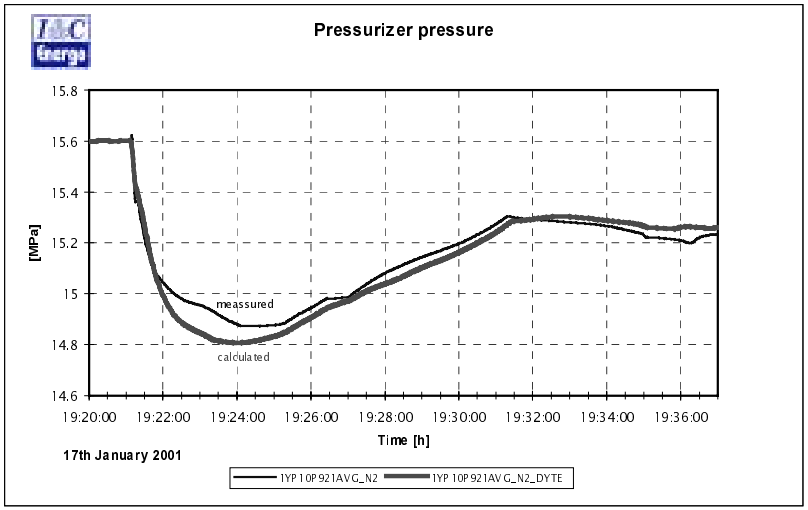
   – before any continuation of the power ascension testing

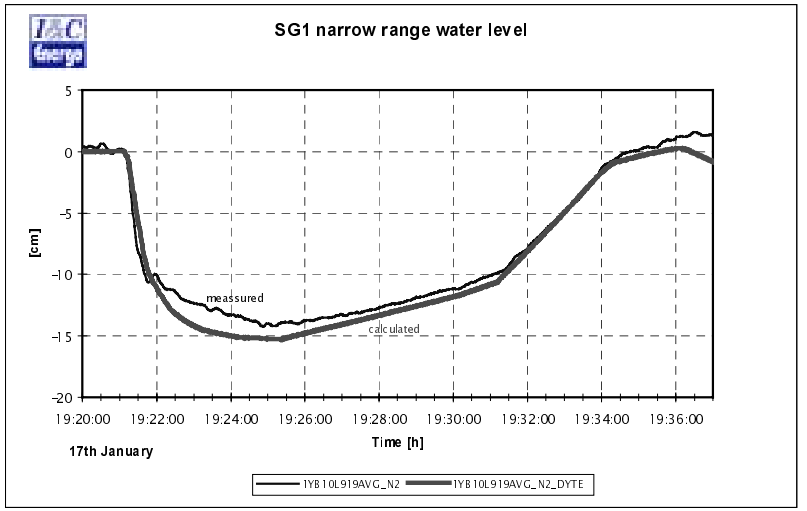
   – after the power ascension testing, in the frame of the tuning of the complete control system based on the commissioning results

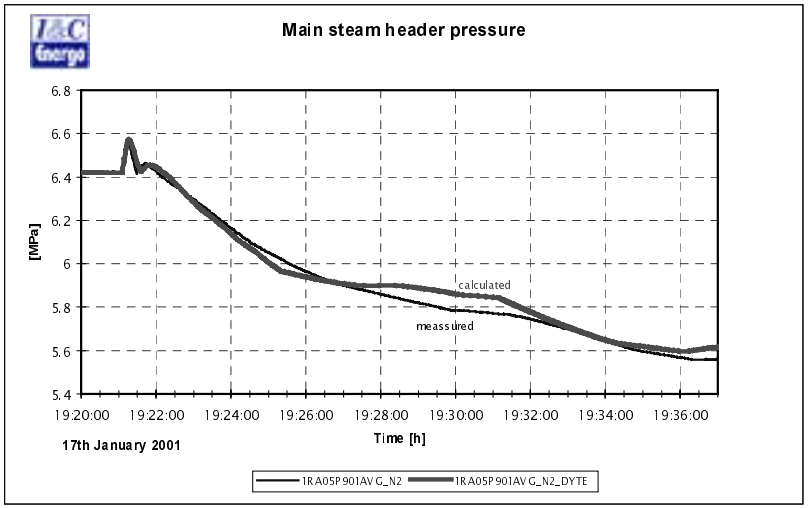
List of Abbreviations

PZR Pressurizer

LS	Limitation System
CC	Control Coordinator
SG	Steam Generator
NPP	Nuclear Power Plant
TP	Technology Process


Pressurizer pressure
[MPa]
Time [h]
meassured
calculated
17th January 2001
1YP10P921AVG_N2
1YP10P921AVG_N2_DYTE


SG1 narrow range water level
[cm]
Time [h]
meassured
calculated
17th January
1YB10L919AVG_N2
1YB10L919AVG_N2_DYTE


Main steam header pressure
[MPa]
Time [h]
calculated
meassured
17th January 2001
1RA05P901AVG_N2
1RA05P901AVG_N2_DYTE

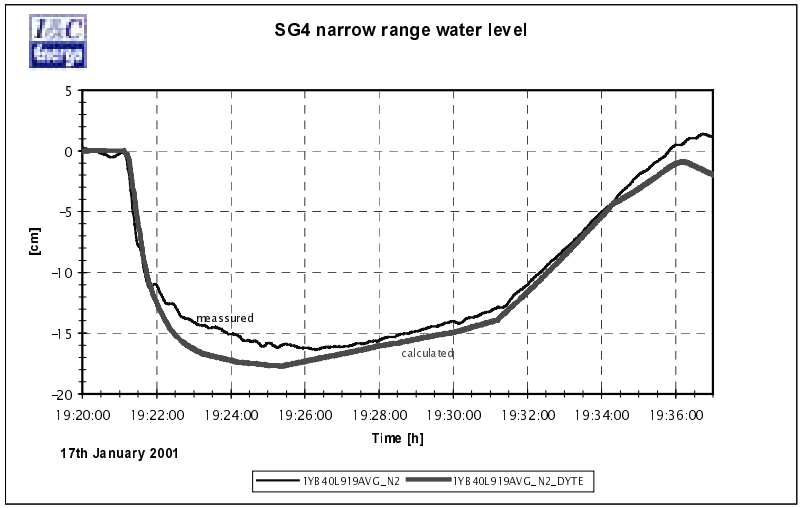

SG4 narrow range water level
[cm]
Time [h]
meassured
calculated
17th January 2001
1YB40L919AVG_N2
1YB40L919AVG_N2_DYTE

Figure 2

Methodology of NPP I&C System Algorithms and Software Verification Expert Analysis

V. Kharchenko, L. Lyubchik, M. Yastrebenetsky

State Scientific and 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: rel@online.kharkiv.com

Summary

The process of NPP I&C systems verification and validation (V&V) and expert analysis of V&V includes the stages of V&V and expert analysis of V&V both algorithms and software (A&SW). This paper is devoted to the elements of methodology development for complex expert analysis of NPP I&C systems A&SW verification and verification. One of the most important phases of A&SW verification and verification assessment is the stability analysis of digital closed-loop control circuits. The paper represents the technique of the main features of V&V and V&V expert analysis of technological controlled plants mathematical models, digital control algorithms, methods and software for stability analysis. The proposed methodology of A&SW verification and validation assessment was approbated during the expertise of a number state-of-the-art Ukrainian NPP I&C systems, particularly during the expertise of computer-based control system ASUT-1000M for Zaporozhey NPP.

Introduction

The process of NPP I&C systems V&V and expert analysis of V&V includes the stages of verification and validation and expert analysis of V&V both algorithms and software (A&SW). The quality of A&SW V&V execution is very important for the computer-based critical I&C systems reliability and safety ensuring. The requirements for verification have actually become more strict and methodology of V&V is the subject of regulatory bodies assessment. The problems of regulation of V&V are inseparable components of both national and international standards in critical engineering [1-3].

The process of A&SW verification and validation assessment is one of the essential parts of NPP I&C expert analysis and licensing. For the broad number of systems, particularly computer-based control systems, the problems of A&SW verification and validation assessment is desirable to consider simultaneously. This is a reason for theoretical and technological basis improvement for developing and realization of A&SW verification and validation assessment process.

The main problems of A&SW of NPP I&C verification and validation assessment are:

- analysis of requirements for control algorithms and software starting from the general requirements determined by the standard documents;
- checking of control algorithms developing and software design tasks statement conformity to the requirements mentioned above;
- review the quality of and V&V plans, testing methodology and completeness in accordance with the A&SW tasks;
- review the quality of and V&V reports and their conformity to the plans and methods of verification and validation.

It is necessary to underline that such problems are difficultly formalizing from the safety requirements ensuring point of view. In general case the assessment of V&V is performed by the traditional methods of inspection and analysis of documentation [4-6], and the single results may be performed using the specially design tools [7,8]. At the same time taking into account the great liability and importance of objectivity and completeness of A&SW verification and validation assessment, it necessary to develop its complex methodology.

This paper is devoted to the consideration and development of methodology elements for complex expert analysis of NPP I&C systems A&SW verification and validation. The proposed expert analysis methodology includes:

- strategy of complex A&SW expert analysis;
- system of A&SW verification and validation assessment criteria;
- requirements detailing the features of A&SW verification and validation assessment;
- methods of A&SW verification and validation assessment;
- elements and phases of A&SW verification and validation assessment technology.

The proposed methodology also covers the developing of conceptual scheme, criterions, requirements and elements of A&SW verification and validation assessment process technology for safety-related systems, as well as recommendations for its utilizations in practical applications. The presented results are obtained during the generalization of practical experience of expert analyzing of real NPP I&C A&SW, in particular ASUT-1000M system for Zaporozhey NPP.

1. Complex approach to A&SW verification and validation assessment

Proposed complex approach to A&SW verification and validation assessment is based on the next principles:

- algorithms and software verification and validation assessment of computer-based automatic control and regulation systems must execute simultaneously;
- main requirements and accepted criteria of algorithms and software assessment may be uniform;
- assessment of stability or robustness NPP safety related control systems must consist of plant modeling and simulation A&SW verification and validation assessment and closed- loop control system A&SW verification and validation assessment.

2. General scheme of A&SW verification and validation assessment

General scheme of the process of A&SW verification and validation assessment for safety-related I&S systems is based on the following principles:

- forming and structuring of the set of requirements for A&SW, which must be reviewed under the V&V process in the different steps of life cycle;
- development of the system of A&SW verification and validation assessment criteria;
- comparison of A&SW verification and validation assessment criteria system against set of requirement for the A&SW;
- formalization of the V&V process and assessment expert analysis using the basic criteria;
- development and utilizing of the utilities for automated safety analysis support under V&V, licensing and expertise.

Fig.1 illustrates the proposed general scheme of A&SW verification and validation assessment. The scheme includes three main stratums - A&SW requirements, verification and validation assessment requirements and assessment criteria.

2.1. Stratum of A&SW requirements, reviewed under verification

This group of requirements divides into the *A&SW characteristics requirements* and *A&SW development requirements*. In turn the characteristics requirements divides into *A&SW functional requirements* determined by the system specification in accordance with its assignment standards in the field of computer systems important for NPP safety [1,6,9,10] (Fig. 1).

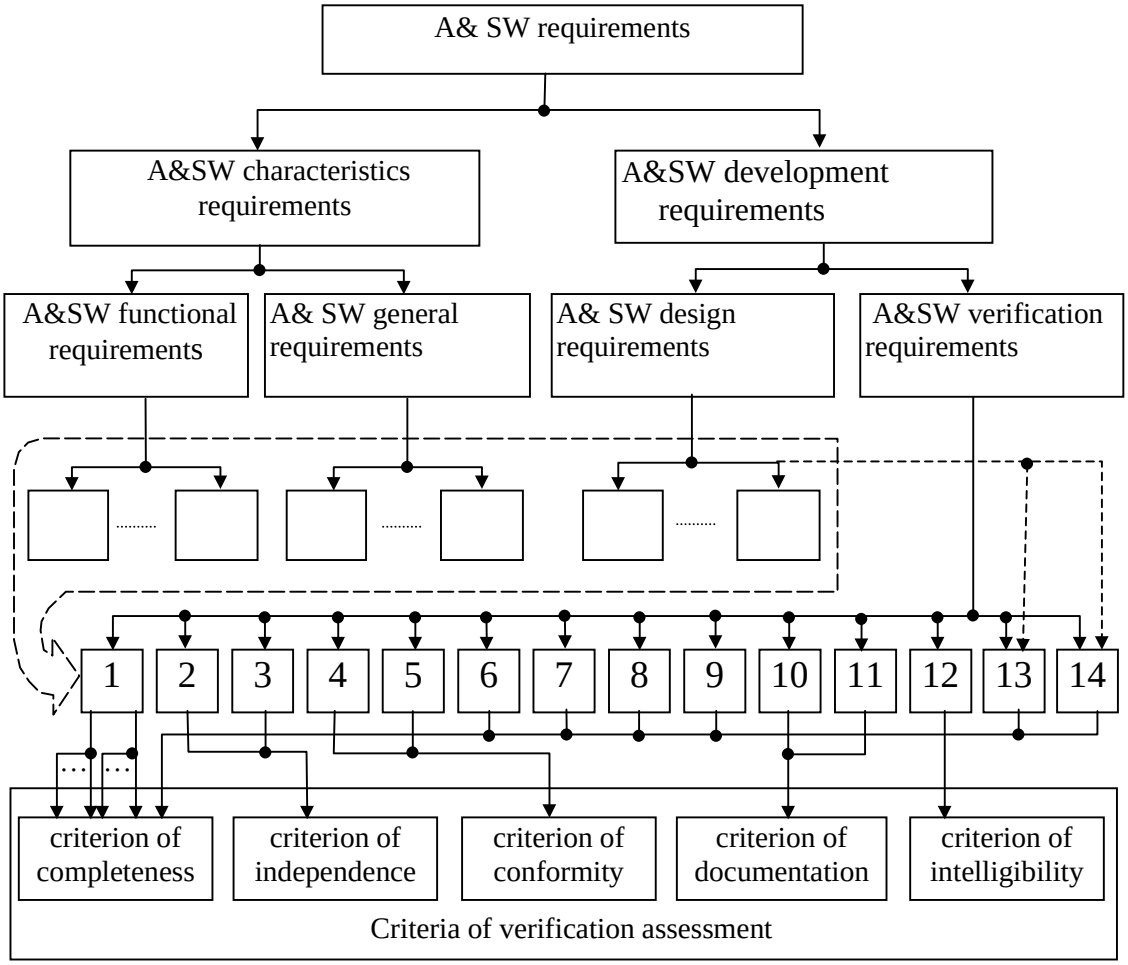


Fig.1. General scheme of A&SW verification and validation assessment

The *A&SW general requirements* include the groups of requirements to:

- A&SW structure and elements;
- diagnostics and self-testing;
- protection against failures because A&SW and human errors.

The *A&SW development requirements* including A&SW design and V&V requirements divide into the groups of requirement to:

- ensuring under development the A&SW accordance to the stated criteria of quality (reliability, correctness, modifiability etc.);

- utilization of the automated instrumental facilities (tools) for A&SW development and V&V;
- programming methods and techniques.

2.2. Stratum of A&SW verification requirements

On the assumption of expert analysis experience and normative documents, which are in service in Ukraine [10], it is possible to separate out the requirements into:

- execution of verification upon the stages of life cycle (requirement 1);
- independence of specialists caring out the verification process for the systems of different classes of safety (requirements 2,3);
- completeness of verification and discovered current shortcomings elimination (requirements 4,5);
- review of protection of general purpose failures (requirement 6);
- verification of previously developed A&SW (requirements 7-9);
- A&SW verification plans and reports (requirements 10,11);
- form of verification materials statement (requirement 12);
- instrument facilities (tools) utilizing under A&SW verification (requirement 13);
- formal methods utilizing under A&SW verification (requirement 14).

The detailed statement of the requirements to the SW V&V is described in [5,6,9,10]. The requirements to the control algorithms verification and validation have many particularities and specific features and will be considered below.

2.3. Stratum of A&SW verification assessment criteria

By analogy with expert analysis methodology for digital safety-related control systems SW verification [5,6], a number of criteria are used under A&SW verification assessment. They correspond the systematized set of showings and rules in accordance with that the assessment is carried out and final conclusion concern A&SW conformity to the presented safety requirements are come about. The proposed criteria system for A&SW verification includes the criteria of completeness, independence, conformity, documentation and intelligibility.

A&SW verification corresponds to *completeness criterion* if under verification the A&SW correspondence to all requirements of specifications, standards and over normative documents was reviewed.

A&SW verification corresponds to *independence criterion* if testing was carried out by group of specialists (organization) which is administrative and/or financially independent fro the specialists (organization) which has developed A&SW.

A&SW verification corresponds to *conformity criterion* if verification was completely finished before the system was put into operation, i.e. all detected failures was analyzed and eliminated by that time.

A&SW verification corresponds to *documentation criterion* if all plans and reports reflected verification process and results in details was issued.

A&SW verification corresponds to intelligibility criterion if all documentation of A&SW verification was stated in the form, which is clear to the specialists, doesn't involve in the developing and verification process.

Fig.2 illustrates correspondence between the requirements and verification assessment criteria. As a result under A&SW verification assessment the fulfillment of all requirements mentioned above must be checked. The model base for the verification assessment process formalization is [9]:

- model of A&SW functional requirements fulfillment review;
- model of A&SW and developing process general requirements fulfillment review;
- model of verification correspondence to assessment criteria review.

3. Technological control algorithms verification assessment features

The assessment features for verification of technological control algorithms (TCA) are closely connected with the character of TCA verification process and methodology [12]. The main tasks, which must be solved during TCA verification, may be divided in two groups:

- logical part of control algorithms verification;
- closed-loop systems stability analysis.

Verification of the logical part of TCA is connected with accuracy testing of technological blocking and protection operation, controller's mode changing, fulfilling of switch over condition from manual to automatic mode of operation. The review of operation requirements correspondence and accuracy carries out by TCA testing by means of special sets of input signals generation and output signals recording with sequential analysis of the testing results. In such a case the testing may be carried out with the help of control system program model as well as special testing hardware.

3.1. Logical part of TCA verification assessment

The assessment of logical part of TCA must include:

- test set completeness analysis, which must cover all typical situations both in normal operations and possible accidents;
- validity analysis concern conclusions about testing conformity and successfulness;
- detected failures and undertaken actions concern their elimination presence analysis.

One of the very important part of such a task is the verification assessment of special and instrumental SW used under the CA logical part verification, which must be performed using the criteria and requirements similar to the SW NPP I&C ones.

3.2. Expert analysis of stability of closed-loop control systems verification

One of the most important phases of A&SW verification and verification assessment is the stability analysis (SA) assessment of digital closed-loop control systems. The requirements of control systems stability is one of the most critical for the NPP safety and must be performed carefully elaborated. Under the SA many important features should be taken into account, particularly input and internal disturbances influence, technological plants nonlinearities and parameters variations, local control systems interconnections, measurement signals corruptions by random noise and so on.

The most widely distributed methodology of complex control systems SA is based on computer modeling and simulation (M&S) using special methods and software for stability analysis. The typical phases of closed-loop control systems SA by means of M&S are the following:

- technological controlled plants mathematical models design and evaluation;
- simulation SW design and verification;
- technological controlled plants mathematical models verification via the comparison of the simulation results and real transient characteristics obtained during the industrial experiments;
- pick of digital controllers algorithms tuning parameters;
- computer simulation of transient process in typical closed-loop control systems (TCLCS) in representative technological regimes;
- 'controllers part' of TCA evaluation upon the result of transient process simulation.

Under the assessment of closed-loop stability analysis results the following typical review steps must be fulfilled:

- technological controlled plants mathematical models verification assessment via the inspection of simulation and experiment results;
- completeness of simulated technological regimes, possible accidents and accountable disturbance factors evaluating;

- stability assurance testing for all typical regimes of NPP operation;
- digital TCA evaluation and controllers tuning parameters picking expediency assessment.

The SA report must be examined using the assessment criteria, which are similar to the criteria used for I&C SW verification assessment, which was described in section 1. A great attention should also be devoted to the verification assessment of special and instrumental SW, designed and used for the simulation purposes.

4. Experience of methodology of complex A&SW verification and validation assessment

4.1. Stages of A&SW verification and validation assessment

The proposed methodology of complex A&SW verification assessment was approbated during the expertise of a number state-of-the-art Ukrainian NPP I&C systems. Particularly the proposed methodology was used during the expertise of computer-based control system ASUT-1000M for Zaporozhey NPP. It is system for automatic control of turbine. The developed approach ensures the possibility of unification and standardization of A&SW assessment verification process. ASUT-1000M A&SW verification and validation expert analysis consists of three stages.

At the *first stage* preliminary analysis (inspection) of documentation (system and A&SW specification, algorithms and software verification and validation plans and reports, etc.) was carried out.

At the *second stage* V&V expert analysis working group performed assessment of A&SW verification and validation technology and V&V results on the manufacturing firms (LvivORGRESS and Kharkiv Plant named after Shevchenko) where system ASUT-1000M was developed. The selected testing of most important A&SW functions was carried out.

At the *third stage* summary assessment of A&SW verification and validation was formulated.

4.2. The general scheme and elements of A&SW verification and validation assessment

Taking into account features of ASUT-1000M A&SW verification and validation expert analysis performed in two "sections": "horizontal" section and "vertical" section. The general scheme of A&SW verification and validation assessment shown in the Fig.2.

In the "horizontal" section the next elements was analyzed:

- typical A&SW consisting of unified algorithm and program modules set. The technology control algorithms (TCA) and functional software developed by the use of these typical modules (TM);
- system A&SW. Expert analysis of this element introduced assessment of TCA, functional software and stability analysis (SA) of typical closed-loop (TCL) control systems (CS) and SA of multivariable (MV) CS;
- A&SW design and V&V tools. The base tools used for A&SW V&V was:
  - A&SW design tools (DT);
  - TCL control systems modeling and simulation (M&S) tools;
  - plant M&S (PM&S) tools;
- A&SW V&V carried out by developers.

In the "horizontal" section expert analysis performed on stages of system and A&SW development starting from EA of system and A&SW specification to functional software V&V on the computer-based control systems of ASUT-1000M. In this section V&V assessment carried out by use of:

- documentation (A&SW V&V plans and reports);
- results of A&SW testing by V&V working group.

Expert analysis of A&SW V&V (technology and process, plans and reports) performed taking into account the requirements and criteria described in the part 2. The most difficult stage of expert

analysis was assessments of stability analysis of TCLCS and MVCS. These assessments carried out on real plant models.

Conclusion

Expert analysis of NPP safety related computer-based automatic control systems algorithms and software expediently to perform simultaneously. Besides, tasks of V&V assessment are need to divide on the:

- tasks of V&V assessment of typical algorithm and software modules;
- tasks of V&V assessment of technology control algorithms;
- tasks of stability analysis taking into account results of plant models verification..

The requirements and criteria of algorithm and software verification may be uniform. For assessment algorithm V&V the some requirements and criteria must be modified.

The proposed methodology is base for development some techniques and tools for expert analysis processes decomposition, planning, management and A&SW assessment by use of formalized models [9].

References

1. IEC - 880, Software for Computers in the Safety Systems of Nuclear Power Stations, Geneva, 1986.

2. ECSS - E - 40A, Software Engineering for Space Systems, Paris, 1998.

3. IAEA Technical Reports, Series 384. Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control. International Atomic Energy Agency, Vienna, 1999.

4. Leveson N. Safeware: System Safety and Computers, New-York: Addison-Wesley, 1995.

5. Vilkomir S.A., Kharchenko V.S. Methodology of the Review of Software for Safety Important Systems// Safety and Reliability. Proceedings of ESREL'99 - The Tenth European Conference on Safety and Reliability, Munich-Garching, Germany, 13-17 September, 1999, vol. 1, pp. 593-596.

6. Vilkomir S.A., Kharchenko V.S. An "Asymmetric" Approach to the Assessment of Safety - Critical Software During Sertification and Licensing// Proceeding of the ESCOM - SCOPE 2000 Conference "PROJECT CONTROL: THE HUMAN FACTOR", Munich, Germany, 18 - 20 April, 2000, pp. 467 - 475.

7. TACS/1019/N7. User Guide for MALPAS Release 6.0// TA Consultancy Services Limited, The Barbican, East Street, Farnham, Surrey GU9 7TB, December, 1992.

8. Vilkomir S.A., Kharchenko V.S., Ponomarev A.S., Gorda A.L. The System Safety Assessment by the Use of Programming Tool During the Licensing Process// Proceeding of the 17th International System Safety Conference, Orlando, FL, August 16-21, 1999, pp. 222 - 227.

9. Kharchenko V.S. Vilkomir S.A. The Formalized Models of an Evaluation of a Verification Process of Critical Digital Systems Software// Proceedings of PSAM 5, International Conference on

Probabilistic Safety Assessment and Management, vol. 4, November 27 - December 1, 2000, Osaka, Japan, pp. 2383-2388.

10. NP 306.5.02/3.035-2000. Requirements of Nuclear and Radiation Safety to NPP I&C Systems Important to Safety/ M.A.Yastrebenetsky (ed.), Yu.V. Rozen, V.S.Kharchenko et al., Nuclear Regulatory Administration of Ukraine, Kiev, 2000.

11. NP 306.7.02/2.041-2000. Technique of Nuclear and Radiation Safety to NPP I&C Systems Important to Safety Expert Analysis/ M.A.Yastrebenetsky (ed.), S.V. Vinogradskaya, V.S.Kharchenko et al., Nuclear Regulatory Administration of Ukraine, Kiev, 2000.

12. Lyubchik L.M. Engineering Aspects of Advanced Model-based Control Techniques for Industrial Applications// Proceeding of the 2-nd AMETMAS Workshop "Advanced Control Concepts for Manufacturing Systems", St. Petersburg, Russia, 2000.

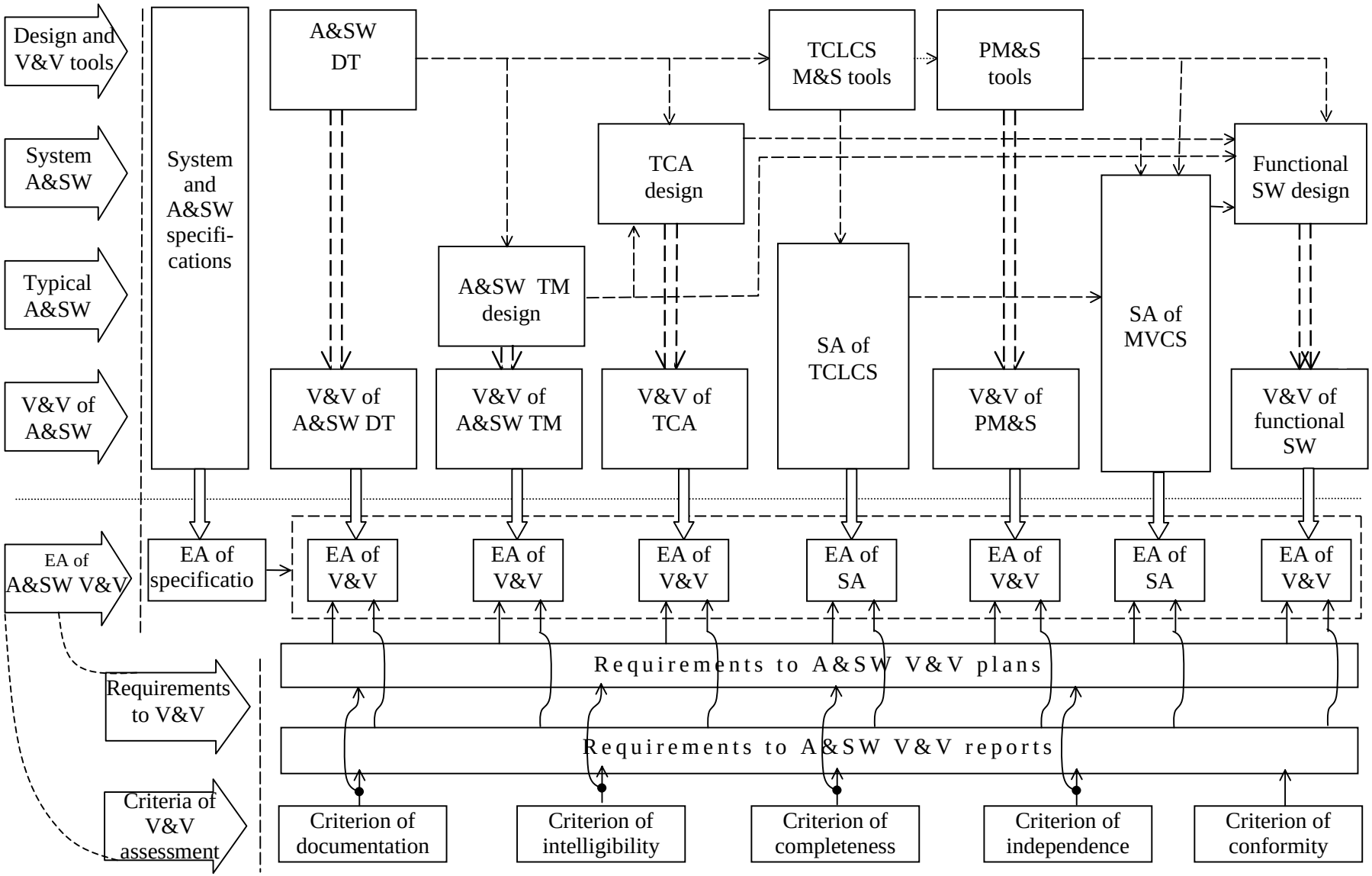


Fig. 2. Correspondence between the stages of A&SW development and V&V expert analysis

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

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

Shigenori Makino[1]

[1]*Tokyo Electric Power Company, 1-3 Uchisaiwai-cho 1-chome Chiyoda-ku Tokyo 100-0011 Japan*
Tel.: +81 3 3501 8111, Fax: +81 3 3596 8562, e-mail: Makino.S@tepco.co.jp

Summary

The digital safety systems were developed and installed to Kashiwazaki-Kariwa Unit 6 and 7 for the first time in Japan, based on these over 10 years experience of digitization of I&C systems. In the development and application process of the digital safety systems, the methodology to prove its reliability were discussed such as QA/QC including V&V procedures, the hazard analysis described in this paper etc.. The hazard analysis was performed in order to fully re-evaluate reliability of the digital safety systems. The results of the hazard analysis by FTA shows that the hazards latent in the software lifecycle, were extracted and verified completely. In this paper, the policies for application of the digital safety system are described to enhance its reliability.

Introduction

The digital control and network systems have been applied to the I&C systems in BWRs in Japan since 1980s. During the course of the application, careful stepwise introduction of digital controllers has been employed, so the scope of the application has been also widened gradually. The highly reliable redundant main controllers were first installed in 1980s, followed by the digital controllers and the network system for the radwaste plants, the non-safety systems introduced to Kashiwazaki-Kariwa Units 3 and 4 (K-3/4). Based on the results and experience gained through the stepwise introduction, almost whole I&C systems including the safety-related systems were finally digitized in Kashiwazaki-Kariwa units 6 and 7 (K-6/7) which first adopted the safety grade digital systems in Japan.

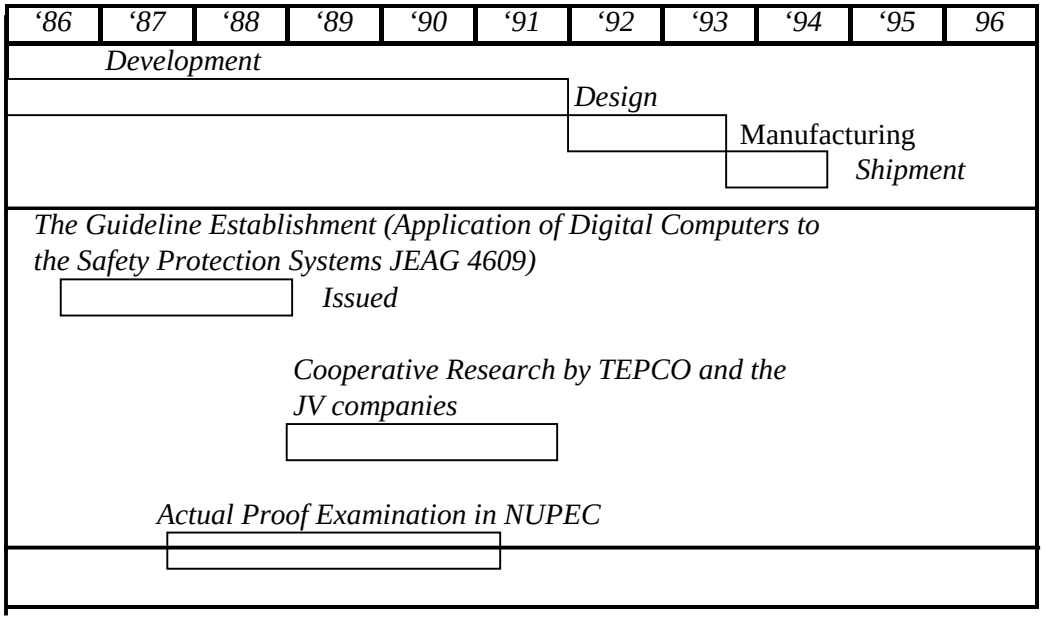
Experience on Digital Safety Protection System in K-6/7

Development Process

The introduction of the digital reactor protection system (RPS) was begun with the intensive study of the related guidelines and/or standards. Based on ANSI/IEEE Std.7-4.3.2 published in 1982, the development of Japanese domestic guidelines for the digital safety system of the nuclear power plants, was started in 1986. The development process had been continued for three years, which led to the publication of JEAG 4609:"Guidelines for Application of Digital Computers to Safety Protection Systems".

After the publication of JEAG 4609, the reliability analysis of the digital control systems were performed, in parallel with the verification test of digital control systems, which was performed by NUPEC (Nuclear Power Engineering Corporation) since 1989. The design of digital safety system for K-6/7 was started in 1991. Figure-1 shows the development process.

Figure 1: The development process of safety digital systems for K-6/7



Quality Assurance and Design

Quality Assurance

ANSI/IEEE Std. 7-4.3.2 requests to maintain the reliability of the software applied to safety system and to carry out V&V (Verification and Validation) in such a way that the independent personnel or organization can clearly understand.

Based on JEAG 4609 (1989) that also requires V&V, the concrete V&V procedures were discussed and first applied to the digital safety system for K-6/7. In addition, the digital control systems, that had been proved to have high reliability and good performance by their preceding application to non-safety systems in the previous plants, were applied to the safety system.

Design

In order to execute the above QA/QC activities effectively, following design was taken into consideration.

In application of the digital control systems to the safety system, a software language, POL (Problem Oriented Language), was adopted because of its visibility and good operating experiences gained through the application to the existing plants. The algorithm of safety system consists of and/or logic, which is defined by the document called IBD (Interlock Block Diagram). The syntax of POL is very similar to that of IBD, so the utilization of it brought lots of merit in performing V&V.

Regarding the software architecture of the safety system, the following features were introduced in order to make the processing simpler.

- No interruption in external signal processing
- Static memory allocation to avoid complex resource allocation
- Periodic processing

The safety system consists of 4 divisions and the 2 out of 4 logic is employed. As for consideration for common mode failures, some hard-wired back-up countermeasures were installed based on the defense-in-depth concepts. Figure 2 and 3 show the configuration of RPS (Reactor Protection System) and ESF (Engineering Safety Features), respectively.

Test Process

Factory Test

In manufacturers' factory tests, the combination test was performed after the component tests. In the combination test, the whole systems such as control systems in the main control room, local multiplex units, signal transmission networks etc., were connected and fully tested. The tests covered signal connection validity, system logic/interlock and so on. Through the factory tests, more than 2000 test cases were carried out to confirm the integrity for the single failure criterion, including single CPU failure in the redundant systems, single transmission line failure in the redundant network system and loss of power etc.

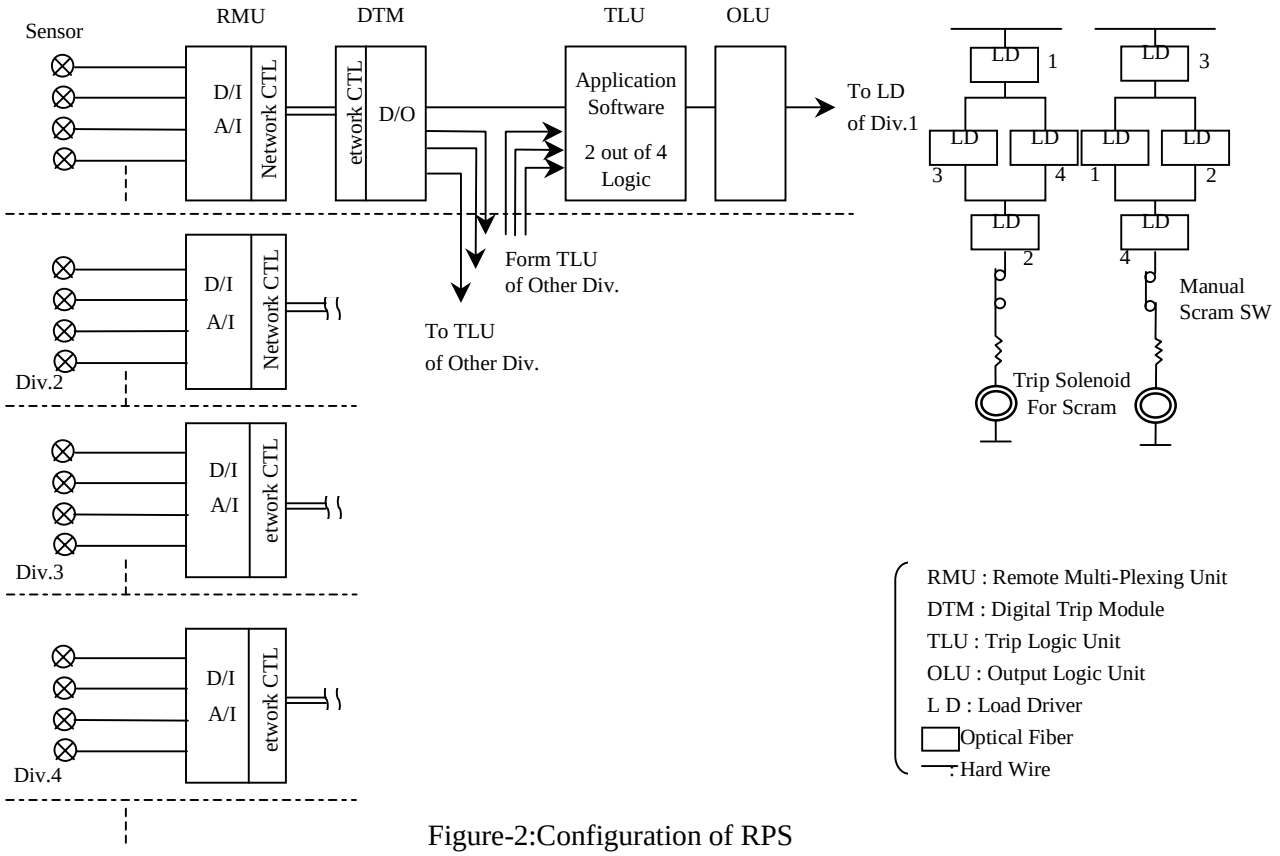


Figure-2:Configuration of RPS

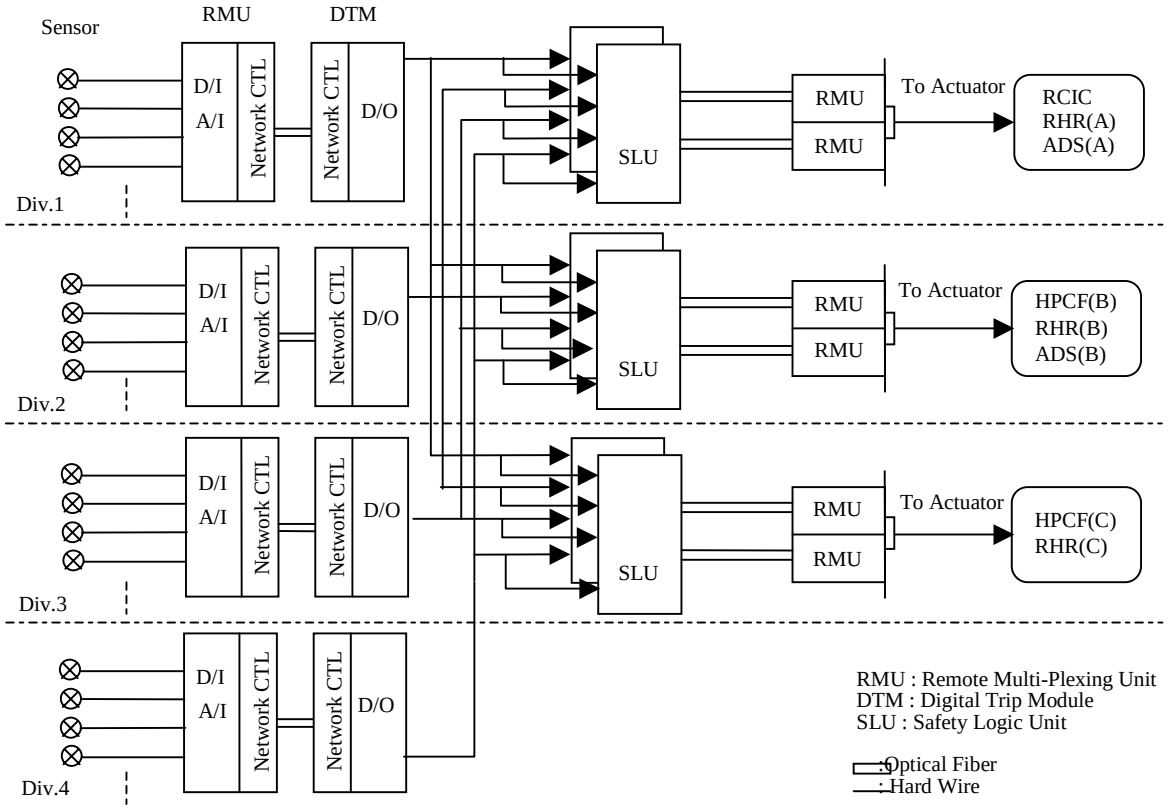


Figure-3:Configuration of ESF

Typical V&V tests were carried out strictly based on the guidelines and standards.

In addition to above, the integrity of POL software installed on the system was carefully checked by the comparison of graphically represented POL software diagram and graphically displayed actual software logic on system maintenance tool to investigate the POL compiler (Reverse Compilation Tests).

In validation process, the semi-dynamic simulation tests were also performed additionally to investigate the integrity for system requirement. By use of the plant simulators, their response to the transients were verified such as LOCA, LOPA, and Main Steam Isolation Valve Closure etc.

Figure 4 shows an example of the semi-dynamic simulation test result simulating a failure of reactor pressure control system.

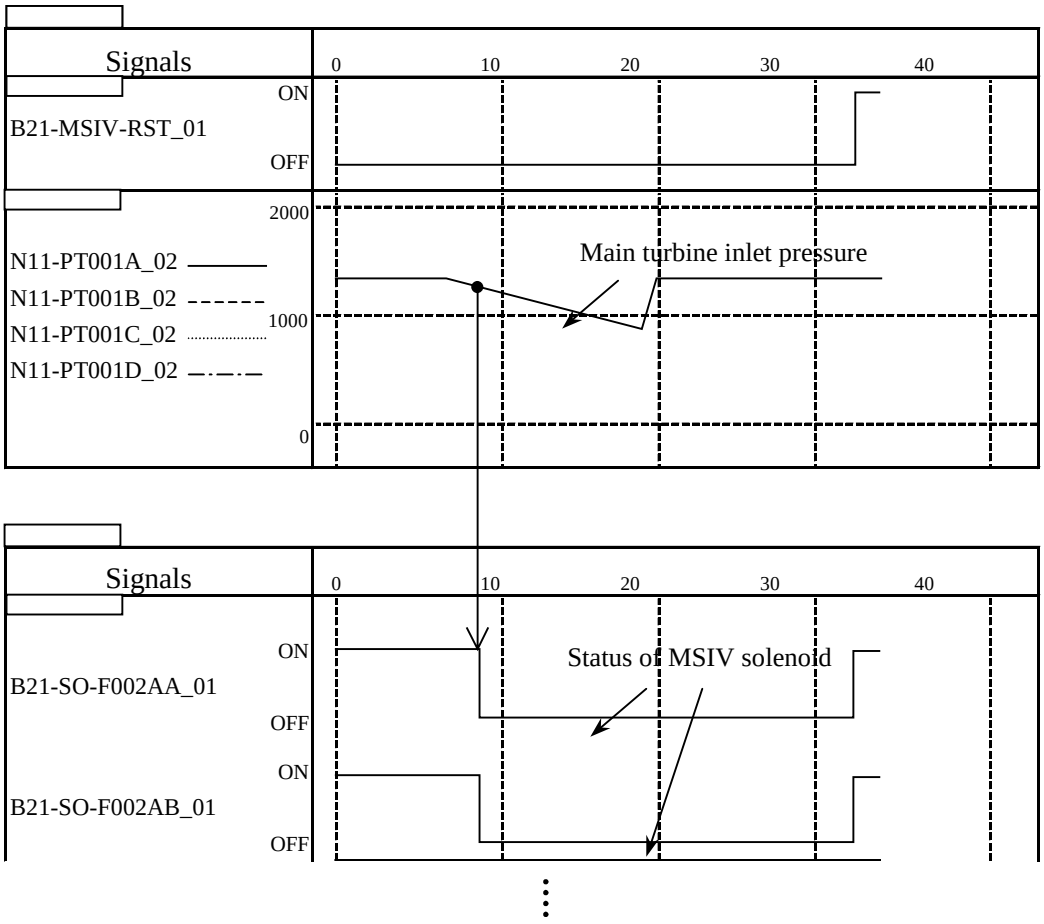


Figure-4: an example of the semi-dynamic simulation test results

Site Test (Pre-operation Test)

After the installation of the system, the whole system was tested to prove the installation integrity. This covered test items as same as the factory tests. In the pre-operation test, the system experienced more than 10 initiation against the transients such as load rejection at 20%, 50%, 75% and 100% power, LOPA at 20% power, plant trip at 50% power and Main Steam Isolation Valve Closure at 100% etc..

Evaluation of V&V activities

To investigate more efficient V&V methods, we evaluated the actual V&V activities of K-6/7 digital safety protection system.

Evaluation Results

Effectiveness of V&V

No major discrepancy was found in the factory and the site test, that demonstrates the effectiveness of V&V test.

Work-force Required

Most of man-hours were consumed for the documentation amounting to several thousand pages. The total man-hours required for them were about a few thousand man-days per plant. This amount of man-hours increased the plant cost.

Consideration on cost-effective V&V Method

In order to reduce the man-hours, the following improvements were discussed.

Software Modularization

The safety logic in BWR is quite simple and the similar software logic is used for initiation of some of ESF. So, by the help of the configuration management method, it is expected that design, manufacture and V&V could be achieved more efficiently. In order to apply the configuration management effectively, the modularization and capsulation of software are very important.

Software Reuse

Once the software is verified and validated through V&V procedures, it may be applicable to other BWR plants without V&V except for verification of the limited software which is unique to the target plant or modified from the baseline, and validation to confirm the system integrity.

Evaluation by means of Hazard Analysis

The hazard analysis is an method to identify the system element, design process, management process which might bring the plant to accidental state (called hazardous state). The hazard analysis aims at reducing the possibility to fall on the hazardous state by performing the intensive evaluation and verification of extracted elements through the hazard analysis. NUREG/CR-6430 introduced several techniques of the hazard analysis. In accordance with the technique, TEPCO performed the hazard analysis utilizing FTA method as follows.

Definition of Top hazard

The safety system initiates the trip function in the case that the values of monitoring parameters increase/decrease compared with their thresholds. Therefore, the system hazard could be actualized as an anomaly of trip initiation signals. So anomalies of the safety system are categorized into the following two cases.

- Failure of initiation against the trip request
- Unnecessary (erroneous) initiation with no trip request

In our analysis, these two are defined as the top hazards.

Development of the Top Hazard

The defined top hazard of the safety system is developed into the hazard of the lower layer step by step. And finally, the bottom hazard elements are extracted and identified in details.

Figure 5 shows an example of the development of the erroneous initiation of SCRAM with no request, that is the top hazard. In this example, the 4 bottom elements are extracted in 3rd or 4th layer, but most of the elements are developed into the still lower layers.

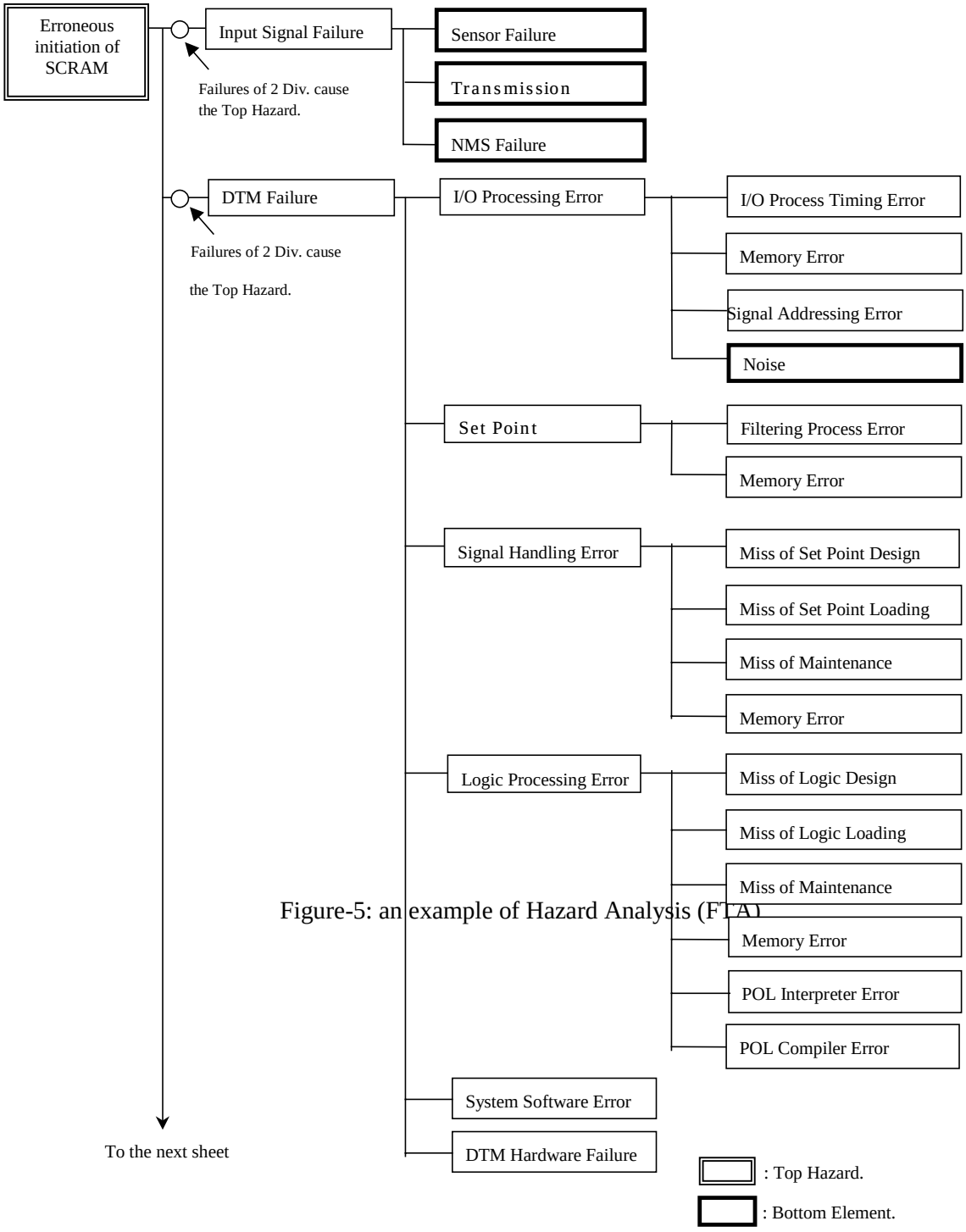


Figure-5: an example of Hazard Analysis (FTA)

Results of Hazard Analysis

FTA extracts a lot of bottom elements that seem to be latent in design process, manufacturing process, management process and so on. We examined every identified bottom elements and their verification process. An example of summary table is shown in Table-1.

It is found that the hazard elements latent in the application software can be found and solved by V&V, while the hazard elements latent in the system software can be solved by the design verification, V&V, the reverse-compilation and the semi-dynamic simulation test.

Table-1: an example of Hazard Analysis results

Category	the Bottom Element	Verification Process
System Software	POL Interpreter Error	- White Box tests and Black Box tests in Developing Phase - Validation - Semi dynamic Simulation tests - SSLC System tests and Startup tests on site
	System Software Designing Error	- Controller qualification Tests - Validation - Semi dynamic Simulation tests - SSLC System tests and Startup tests on site
	Diagnosis Error	- FMEA - Controller qualification Tests - Validation
Compiler	POL Compiler Error	- Controller qualification Tests - Validation Tests - Reverse Compilation between source code and object code
Application Software	I/O Process Timing Designing Error	- Verification (step3/4) - Validation
	Process Timing Designing Error	- Verification (step3/4) - Validation
	Memory Allocation Error	- Verification (step3/4) - Validation
	Filter Designing Error	- Verification (step2/3) - Validation

In specialty, as for the system software, it is very difficult to investigate details of it, because of its complexity. But the most important thing to achieve the high reliability of the safety system is not only to perform various tests in table-1 but also to choose the right software, which has the features as follows;

- Small size,
- Limited function,
- A lot of operation experience.

Conclusion

Policies to be applied to the digital safety systems

The good operating experience of K-6/7 demonstrates its high reliability and performance.

From the viewpoint of the experiences gained through the development, installation and operation of K-6/7, TEPCO believes that the following policies should be universally applied to the digital safety systems.

- Utilization of the digital control systems which have proved the performance and most operating experiences.
- Simple Software Architecture:

Static memory allocation, Avoidance of external interrupts, Periodic processing etc.

- Utilization of the graphical language in order to keep transparency and traceability for independent reviewers
- Execution of V&V
- Modularization of the safety software for its reuse and effective execution of V&V
- Considerations for common mode failures

The suitable backup measures against CMF should be applied.

Future Trends on the application of digital safety systems

In order to reuse the highly reliable software resource of K-6/7 effectively and to make this approach practical, JEAG 4609 (1989) was revised and published as JEAG 4609 (1999).

It covers the new subjects such as:

- Software Revision Control by Configuration Management
- Reuse of Software with Configuration Management
- Suitable Design Considerations for CMF

In Japan, several ABWR plants are under construction now. We believe that the digital safety systems developed and validated in K-6/7 would be basically applied to these plants.

Reference

1. K.Iwaki, "Control Room Design and Automation in Advanced BWR", In proceedings of the 1990 OECD/NEA international symposium, March, 9-13 July, 1990
2. Takao Tochigi, Yusuke Kajikawa, Chikara Takayama, "Development of integrated digital instrumentation and control system", In proceedings of 1992 OECD/NEA international symposium, Tokyo, 18-22 May, 1992
3. Hiromu Kikuchi, "Digital control technologies applied to TEPCO nuclear power plants", In proceedings of the 1995 INE international conference on C&I in nuclear installation, UK, 19-21 April, 1995
4. Takaki Mishima, Tomoaki Shirakawa, "The design requirement and development of software for the digital safety protection system in Kashiwazaki-Kariwa units6 and 7", In proceedings of the 1996 OECD/NEA international workshop on technical support for licensing issues of computer-based systems important for safety, Germany, 5-7 March, 1996

Technical Requirements on Maintenance of Digital I&C Systems Important to Safety

G. Schnürer[1], M. Kersken [2], F. Seidel[3]

[1] Institute for Safety Technology (ISTec), Garching
Tel.: +49 89 32004-523, Fax: +49 89 3200-300, e-mail: sgu@grs.de
[2] Institute for Safety Technology (ISTec), Garching
Tel.: +49 89 32004-546, Fax: +49 89 3200-300, e-mail: ker@grs.de
[3] Federal Office for Radiation Protection (BfS), Salzgitter
Tel.: +49 5341 885-863, Fax: +49 5341 885-865, e-mail: Fseidel@bfs.de

Abstract

The operation of digital safety I&C systems requires the availability of spare parts as well as the so-called configuration management procedures within the framework of maintenance and upgrading strategies. Requirements which are treated and discussed in this paper are (technical) solution oriented versus Guidelines do have an overall (general) character. This 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. Also the adoption of existing rules and guidelines is taken into account for precising these additional requirements for safety relevant I&C. Main goal of this paper is the introduction of possible safety relevant requirements with respect to

- maintenance of digital (hardware and software) safety relevant and safety I&C
- tracing and route cause analysis of incidents, caused by I&C maintenance
- support of the regulatory body as well as technical experts concerning the state of the art.

Introduction

Contrary to the complex of upgrade and refurbishment procedures In this paper the term maintenance is used in the following manner: Maintenance is the combination of all measures which ensure the specified system function. Maintenance procedures should have a small effort and a limited duration. For safety reasons maintenance procedures in NPP can just take place in one redundancy without reducing the availability of parallel systems as well as combined systems (e.g. CPU of software based systems) in an irregularly way. Consequently the update with new or modified SW-versions in this sense is no part of maintenance for safety systems.

With respect to the operational life time of more than 30 years for German NPPs the rapid innovation cycles of new I&C systems and the non availability of spare parts are leading to different maintenance and upgrading strategies for safety I&C systems. Generally, there are 3 different strategies The first one is based on a redesign of operation proved hardwired I&C electronics (sub-assemblies) on basis of compact electronic devices, like I&C circuits for o-ver-voltage protection, etc. Such redesigned sub-assemblies are to be qualified according to the German KTA-standards. the replacement with that redesigned sub-assemblies normally is part of a maintenance process. The second way is based on a redesign of hardwired I&C electronics with ASICs and/or FPGA. These ASICs/FPGA do not have any micro controller by means of they do not need any software support during operation. The advantage is an eased qualification in comparison to a software-based ASIC. The replacement with ASIC (FPGA) based

redesigned sub-assemblies may also be a part of a maintenance process. The third upgrade strategy is the introduction of PLCs by means of software-based I&C systems. This paper deals prior with safety relevant requirements on maintenance and SW-upgrading of digital safety I&C systems.

Whereas maintenance requirements for hardware in Germany are already existing or treated by ”business as usual”, respectively, requirements for software-based systems are only partly treated in the national and international regulations.

Consequently the missing requirements are to define and to elaborate. Requirements for maintenance and upgrading of digital systems should cover the following aspects:

- New designed software for a specific application. Therefore requirements for the specifi-cation (refurbishment procedure, formal methods, traceability and testability) as well as configuration and parameterization (requirements for tool application, software testing) are to fulfill.
- Software of existing systems (COTS) which needs to be adopted (configured) to a special application. Therefore requirements for development documentation, state of software modules as well as testing are to investigate.
- Hardware of the system or component (replacement of components). Requirements for the design tool, specification of the hardware architecture, documentation, testability are needed.
- Requirements for the factory acceptance tests (integration; in the case of maintenance, as far as it is a prerequisite for field testing) and field testing are to specify.
- Requirements for manual testing procedures are to elaborate.

This paper gives a brief overview of already existing requirements and discusses the necessity of additional national and international requirements on maintenance of digital I&C sys-tems important to safety.

State of the art

Software tools which are used for design, construction and implementation planning as well as qualification management do also have to specify the hardware structure and modules according to the computer system. This means, that instead of manual programming of I&C functions the configuration, parameterization and automatic coding of pre-developed soft-ware modules will take place. Such software programs are planned and task specific. Be-sides, tool systems are also managing software modules, which are developed by conventional methods of software engineering. This kind of software could be the operating system, in- and output drivers, communication software, self-testing procedures, diagnostic software as well as software for the treatment of exceptions. Therefore , there are also programs to add, which realize the processing of the automatic generic code, like functional diagrams and functional diagram groups. Such programs realize the runtime environment.

The runtime environment software contains the software which - also named as application software - is performed in the target system of nuclear power plants.

This paper deals with already existing requirements and with the elaboration of new requirements concerning testing and safety assessment of procedures to maintain and upgrade of digital I&C.

International requirements according digital upgrades important to safety during maintenance

Digital upgrades during maintenance for software of the highest category

The international standard IEC 60880 /1/ for software of the highest safety category contains the necessary elements for an acceptable software modification process. This software change process may be necessary during software production, i.e. design, coding, system integration, system validation and commissioning, but also during maintenance (see Fig. 1). The documentation related to the software modification comprises anomaly report, software modification "field document" and software modification field history, where the latter collects the information concerning software changes from the production and maintenance processes.

The necessity for the modification of software may be due to the occurrence of an anomaly, a change of functional requirements after delivery, new technological solutions (upgrading) and a change in operating conditions.

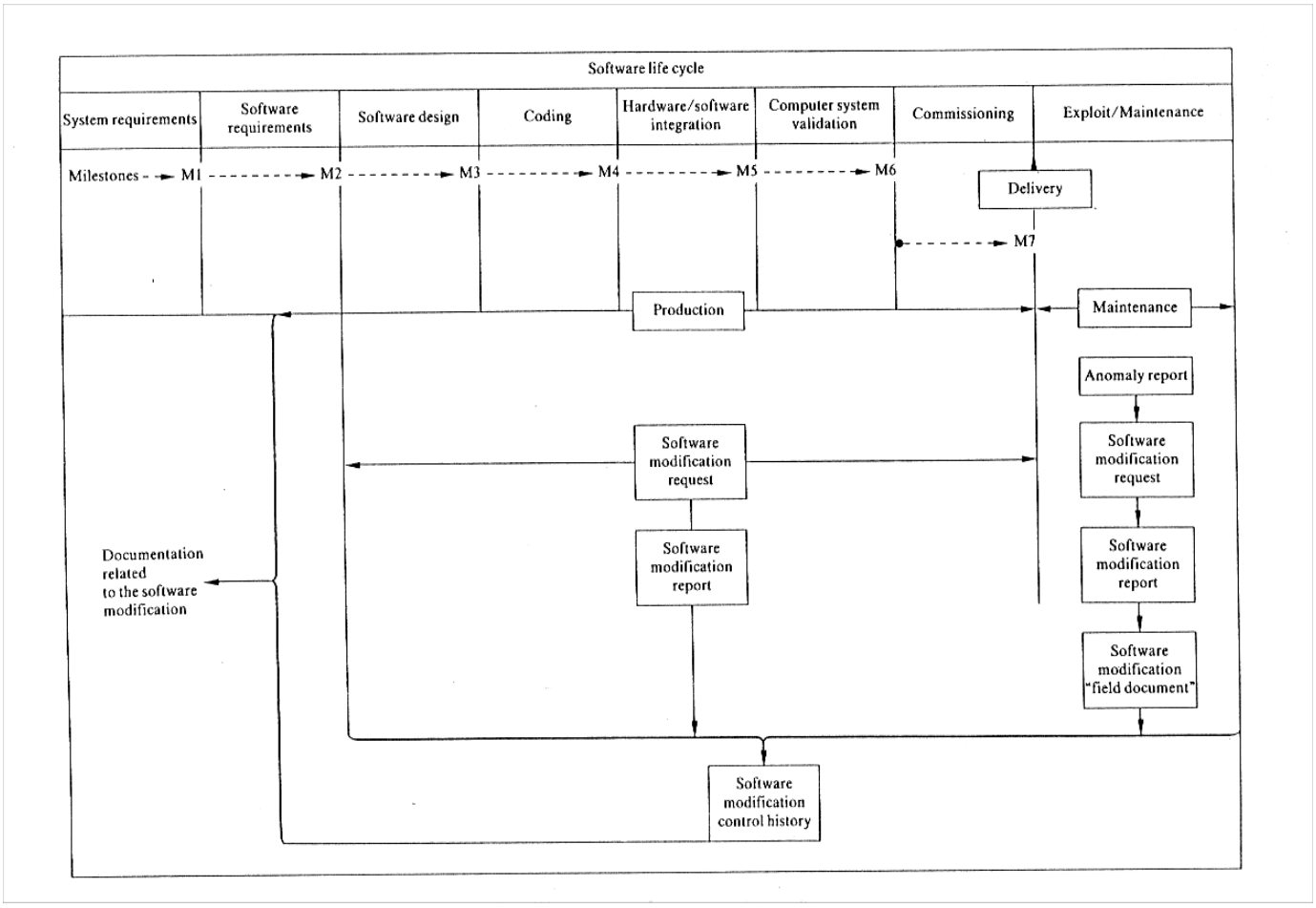


Fig. 1: Software change processes during production and maintenance /1/

In case of an anomaly, an anomaly report is written giving the symptoms, the system environment and system status at the time at which the anomaly was discovered and the suspected causes.

Anomaly correction requires the generation of a software modification request, the execution of which follows the modification request procedure described below.

In case of a change in software functional requirements or in operating conditions, the whole software development process is re-examined for that part of the system impacted by the change.

Any new hardware requirements and capabilities are examined with respect to their potential impact on the software systems. This evaluation should include all hardware considerations reviewed in the original software design. If it can be shown that the new system does not impact the software requirements, a simplified procedure may be used to implement the modification either at the design or coding phase.

In all cases, after implementation of the modification upon the in-the-field equipment, a field documentation is issued which gives the date of the implementation and the result of the specified observations. This document is filed in the software modification control history for the project.

The following aspects of maintenance and modification of software-based systems are covered in [1].

Modification request procedure for software of the highest category

This software modification request should identify its originator, the reason for the request, its aim and the functionality affected by the change.

Persons which are independent from those who issued the modification request should evaluate it, the result being either

- acceptance of the request, or
- rejection with the appropriate reasoning, or
- approve the request of minor importance and impact, or
- requiring a detailed documented analysis, written by software personnel knowledgeable in the system software.

The following items are examined in the evaluation of the modification request with respect to

- technical feasibility,
- impact upon hardware (e.g. memory extension) or upon other equipment (e.g. test sys-tems) in which case the request for modification addressing this impact area must be documented for the equipment,
- impact upon software including a list of affected modules,
- impact upon performance (including speed, accuracy, etc.)
- necessary effort for verification and validation; the analysis of the software reverification needed is documented in an audible form,
- the set of documents to be reviewed.

The software modification request is pending until the decision is made:

- to accept it (immediately, or after examination of the software modification analysis re-port) and to execute it, or
- to reject it and justify the rejection.

Execution of a modification

The procedure for executing a modification follows the development process; i.e. all phases of the software development lifecycle have to be repeated for any part of the system im-pacted by the change. This means that the modification is carried out according to the (many) rules for good (error-poor) development of software (as e.g. laid down in chapter 5 of /1/).

All the documents affected by the modification must be corrected and refer to the identification of the software modification request. a software modification report sums up all the actions made for modification purposes.

All these documents are dated, numbered and filed in the software modification control history for the project, i.e. they are held under configuration control.

A configuration management system provides a means to ensure this.

After implementation of the modification, the whole or part of the verification and validation process must be performed again according to the software modification analysis.

For modifications on site, the software supplier should have access to a test configuration which is identical to the real system in all relevant aspects (including installed machine, translator, testing tools, plant simulator, etc.) to ensure the validity of the modifications.

Licensing issues

The international standard IEC 60880 /1/ contains the necessary elements for an acceptable software change process. However, for regulatory purposes and for safety systems there is a need to add an additional dimension to the change process /2/. This additional dimension results from the need for : (i) an analysis of the effect of the change on safety; (ii) the provision of documentary evidence that the change has been conceived and implemented correctly; and (iii) a process of independent review and approval of the change. The requirements coming from this regulatory view are of course partly overlapping with the requirements imposed to the production (and V&V) process. They are summarized according to /2/ in the following.

General

The software change procedure and documentary process shall be applied to all elements of the software system including its documentation. This procedure shall apply equally to sys-tem functionality enhancements, environmental adaptations (resulting in a modification to the system requirements) and corrections of implementation errors.

An appropriate software architecture and a suitable software configuration management system shall be used during the lifecycle process in order to maintain safety. For safety sys-tems, no distinction shall be drawn between major and minor software changes since a wrongly implemented minor change could challenge safety.

Once a software or documentation item has been approved, i.e. has been placed under con-figuration control (usually following its initial verification and placing in the soft-ware/documentation library for release), any changes to this item shall be controlled by a procedure containing the elements given in the following paragraphs.

The software change procedure and the configuration management system shall include an adequate problem reporting and tracking system.

The software change procedure shall contain the following basic elements.

(i) the identification and documentation of the need for the change;

(ii) the analysis and evaluation of the change request, including: a description of the design solution and its technical feasibility; and its effect on the safety of the plant and on the software itself;

(iii) the impact analysis of each software change: for each software change, the implementers of the change shall produce a software impact analysis containing a short description of the change plus a list of software parts affected by the change plus the effect on non-functional system properties as, e.g. dependability, response time, system accuracy, hardware performance. Objective evidence that the full impact of each software change has been considered by the implementor for each software part affected shall be provided. As a minimum this shall consist of a summary description of the change to be implemented, plus documentary evidence of the effect of the change on other software parts. The software impact analysis shall also list data items (with their locations – scope of the data item) that are affected by the change plus any new items introduced.

(iv) the implementation (consistent with the standards employed in the original production process), verification, validation (as appropriate) and release of the changed software or document item. The V&V phases may make use of the software impact analysis to perform regression testing.

(v) The requirements of IEC 60880 sections 9.1, 9.2 and 9.3 shall apply.

Faults shall be analyzed for cause and lack of earlier detection. Any generic concern shall be rectified and a report produced.

Software Modification

A correction to a wrongly implemented software change, if found at the stage of site testing (i.e. following installation of the software on the plant), shall be processed as though it were a new software change proposal.

The commissioning team shall use the software impact analysis and the factory V&V report to develop their own series of tests in the form of a site commissioning test schedule.

Software Maintenance

All software changes in operation following the completion of commissioning at site (called software maintenance changes in the following), shall be controlled by procedures which meet the requirements of this section on software maintenance.

For safety systems, program and fixed data (including operational data) shall be held in read only memory (ROM) so that they cannot be changed on-line either intentionally or due to a software error.

For safety systems, software maintenance changes shall be tested on the computer system installed at site. Any divergence from this shall be justified in the test documentation.

Software maintenance changes shall be reviewed, from a safety perspective, by suitably qualified and experienced staff – e.g. manufacturers (suppliers), system designers, safety analysts, plant and operational staff – that are independent from those persons proposing, designing and implementing the change. The above review shall consider manufacturers (suppliers) V&V and independent assessment reports, as well as test specifications and test reports, or other such documentation as appropriate to the change being proposed. The results of the review shall be documented and shall include a recommendation for approval, or rejection of the change from the safety perspective.

Only software approved for release shall be installed at site.

Before the start of site testing of any changes to the software of a safety system, the test specifications shall be reviewed by independent reviewers.

Before permitting the operational use of software following a change, an updated and checked version of the system and safety demonstration documentation (including any routine test schedules) shall be available, fully reflecting the changes that have been made. This shall be confirmed by independent review

The independent reviews shall be documented.

Configuration management

All the items of software including documents, data (and its structures) and support software shall be covered by a suitable, readily understood and fully documented configuration management system (CMS) throughout the lifecycle. An item of software or documentation shall not be accessible (to persons other than those responsible for its design and verification) until it is approved and under configuration control.

A formal procedure shall be set up for version control and the issuing of correct versions. Provision shall be made for informing all relevant personnel of pending changes and approved modifications.

All software copies, including any pre-existing software that is being used, shall be clearly and uniquely labeled with at least title, version number and creation or acquisition date. Pro-vision should be made for the inclusion in the source code listing of information on changes made, approval status, and authors, reviewers and approvers names. The identification and version number shall be included in the code so that this can be checked by other software items.

After delivery of the software and its documentation, the same level of configuration management shall be maintained at the site where the delivered software is stored.

A configuration audit shall be performed on the safety system software prior to loading to establish that the correct items and versions have been included in the system. Following system loading, the loaded version shall be verified as being uncorrupted.

Conclusions

As already mentioned, IEC 60880 describes the modification process for software in computer-based systems of the highest safety category. Taking into account, that most of the software-based systems important to safety are also to be installed in lower safety classes, the importance and necessity of

staggered requirements for the lower safety categories is obvious. The German Guidelines of the Reactor Safety Commission contain already staggered requirements to prove the qualification of the software-based systems of lower safety classes in a general way. Furthermore, in Germany we have already requirements for hardware modifications within the lower safety categories. As a general requirement, in Germany the modified system must have at least the same qualification level than the previous system. Furthermore, also after modification the I&C shall not limit the availability of the safety system. For hardware the qualification level can be demonstrated via operational experience or via a type test procedure according to the German KTA rules, or, in case of introduction of new technologies a demonstration according to the state of the art.

For software-based systems important to safety following questions are to be answered:

- What qualification procedure is necessary in the case a hardwired equipment important to safety will be exchanged by a new software-based system? If the origin hardwired equipment is qualified via operational experience how to confirm the same qualification level of the new software based system?
- How to confirm the necessary qualification level considering the lack of operational experience with the new system?

How to consider the sufficient extent and deepness that in general any modification of the application software leads to a new software product? Within the frame of a research project of the German Ministry of Environment, Nature Conservation and Reactor Safety (BMU) ISTec is investigating different options for establishing new qualification and assessment requirements in the case of software modifications during maintenance. First results of that investigation are:

- Any modification within application software results in a new software product. Already existing operational experience of the former software product can hardly be used for qualification issues. Except, the operational experience is based on a unchanged soft-ware routine within the application software (e.g. functional software blocks inclusive in-terface environment).
- For the highest safety category operating experience can not replace a detailed documentation of the software product and its development process. Only missing parts of the necessary set of documentation can be replaced by operating experience.
- The collection of operating experience must also be governed by a whole set of requirements which ensures completeness, correctness and non-ambiguous of the data and their collection process. It should be possible to demonstrate that the data collection is appropriate although from the statistical point of view. Additional information concerning data acquisition are already introduced in an other contribution of this meeting.
- The need of requirements concerning software modifications during maintenance of the lower safety classes is obvious.
- Requirements according to IEC 60880 concerning maintenance and modification of soft-ware do have a general character. They should be specifically applied. Part 2 of IEC 60880 contains more details concerning the application of pre-developed software. But there remains also a certain area of free interpretation. Actual software modification proj-ects will show, whether at least the requirements of IEC 60880, part 2 are sufficient by means of covering all regulatory issues.
- Starting from the requirements of the German RSK-Guidelines or IEC 60880, respec-tively, staggered safety requirements should be elaborated. Possible requirements for the qualification of pre-developed software in staggered categories are introduced in another contribution of ISTec to this meeting.

Information about the project's further progress will follow.

Summary and Outlook

This paper describes the already existing requirements concerning maintenance and upgrading of digital safety systems according to IEC 60880 and the common position of the European nuclear regulators for the licensing of safety critical software for nuclear reactors /2/. Whereas the requirements for hardware upgrades are already covered by the German nuclear standards additional guidelines for software maintenance are under discussion. Following aspects are 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.

Literature

/1/ IEC 60880: Software for computers in the safety system of nuclear power stations, 1986

/2/ EUR 19625 EN: Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors, May 2000

Requirements Management of I & C System Refurbishment of NPP Dukovany

J. Pliska [1], J. Cendelín [2]

[1] *I&C Energo, Prazská 684, 67401 TREBÍC, Czech Republic*
Tel.: + 420 618 893 300, Fax: + 420 618 893 999, e-mail: jpliska@ic-energo.cz
[2] *West Bohemian University in Pilsen, Faculty of Applied Sciences, Department of Cybernetics, Univerzitní 22, 30614 PLZEN, Czech Republic*
Tel.: + 420 19 7491 155, Fax: + 420 19 279 050, e-mail: cendelin@kky.zcu.cz

Summary

The Requirements Management System is a necessary precondition for the organisation, management, coordination, 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 into a hierarchic structure which observes the structure of the application area. Individual requirements are mutually interrelated in various ways. Each requirement is expressed in form of a written description. Some significant features of the requirements are clearly and simply expressed with a set of assigned attributes.

Introduction

Using an example of the Requirements Management System as implemented in the project: I&C System Refurbishment for NPP Dukovany the paper describes capabilities and usefulness of system analysis methods and the corresponding tools – generally designed CASE systems.
The purpose of this paper is to provide a closer look at these system analysis methods and tools. These methods and tools have not been sufficiently widespread in technical practice, although they offer a number of advantages and may significantly influence the resulting quality of the Work.
Frequently, the field of application for these methods and tools is confined to large-scale data processing and software engineering.

Basic Data of the Project: I&C System Refurbishment for NPP Dukovany

The described Requirements Management System has been used in the project of I&C System Refurbishment for NPP Dukovany. The project is very extensive and complicated and from the viewpoint of functions it includes the following I&C systems at NPP Dukovany:

A) Safety systems, participating in the implementation of safety functions:

- Reactor Trip System,
- actuation of technical means for safety assurance,
- gradual actuation of devices supplied from assured power sources,
- Post Accident Monitoring System.

B) Safety related systems, participating in the implementation of safety-related functions:

- supporting actions to actions which assure safety,
- protection of steam generators,
- automatic limitation and reduction of reactor power output,
- regulation of the reactor power output.

C) Not safety systems, participating in the implementation of functions monitoring condition of the unit:

- In-Core Measurements System,
- Computer Information System.

In all cases, with the exception mentioned below, the listed existing systems will be entirely replaced with new ones. The only exception is the Post Accident Monitoring System (PAMS) which is not currently a part of the I&C structure at NPP Dukovany.

Specification and Requirements for the Requirements Management System

The Requirements Management System has been created through a controlled transformation of the Contract and its appendices containing requirements for supplies, works and services into a file of requirements which make up the system.

This transformation into the system has enabled well-organised administration and control of the requirements and has brought a number of other advantages.

Specification of the Requirements Management System.

The process of requirement management ranks among the essential processes in the project initiation and management. Its objective is to provide for the mechanisms to:

- analyse and review the input data, to check that they are formally and factually correct, complete, understandable and unambiguous,
- unambiguously identification and documentation of user requirements,
- identify and describe mutual relations between the requirements,
- change management of the requirements and to analyse impacts of such changes,
- monitoring, evaluation and documentation fulfilment of the user requirements and to implement corrective measures.

The Requirements Management System serves as an input for:

- Basic Design,
- Test Planing and Inspections,
- Detail Design,
- Realisation,
- Supplies and Installation,
- Commissioning.

A quality system of requirement management contributes to the development of effective partnership with the customer.

Characteristic Features of Correctly Defined Requirements.

A correctly defined requirement shall have a number of features. They include, in particular:

- Necessity (basic function)

  The requirement shall define a basic capability, physical characteristic or quality factor. Removal of the requirement without replacement shall result in a failure.

- Briefness

  The requirement description shall contain a single requirement. The requirement shall express WHAT is required but not HOW it should be achieved.

- Feasibility

  The requirement shall be feasible using one or more variants of system designs.

- Completeness

  The requirement shall be complete and shall not require any additional explanations or supplements. Each requirement shall be capable to exist independently of the other requirements.

- Consistency

  No requirement shall contradict to the other requirements.

- Unambiguous Description

  Each requirement shall have only one interpretation.

- Verifiability

  No requirement shall be general. It shall be possible to verify its fulfilment with a test or analysis.

Implementation of the Requirements Management System.

Application of System Methods and Tools.

System analytical methods may be efficiently and successfully used whenever a system is the subject matter – an object made up of mutually interrelated elements. These methods, which have been used and developed in system engineering for half twenty century, are truly universal.

The requirements file is a system made of elements - individual requirements. Each requirement is described with a structured text. Individual requirements are mutually interrelated in various ways. The requirements may be arranged into a hierarchic structure. Some important properties may be expressed in a clear and simple way with the assigned attributes.

Efficient implementation of the system is strongly dependent on the quality of applied supporting tools. The suitable tools for these purposes are generally designed CASE systems. There are not many suitable systems of this type suitable for the purpose because their significant proportion specializes in partial tasks, particularly in data processing and software engineering.

The general tool for system analysis - *case/4/0* , in its current 5.0 version, by microTOOL, Germany, has been used for the Requirement Management System in the project: I&C System Refurbishment for NPP Dukovany.

Description of the Implemented System based on case/4/0.

The Requirements Management System has been implemented using *case/4/0*. The tool contains a complete range of system analytical methods. A prevailing part of these methods is of graphic nature.

The key step for each solution is correct assignment of methods to structural properties of the requirements file.

There is a certain limitation caused by the fact that *case/4/0* has firmly established names of the objects it works with. Therefore the following pairs of terms have been introduced, see Table 1.

Requirement	=	Function
Hierarchic structure of requirements	=	Functional structure
Relations between requirements	=	Information flows between functions
Elements outside the requirements system (other projects)	=	External interface
References to standard and on	=	Data structure
Physically existing component of the requirement's content (text, attribute value)	=	Data element
Summary of information about the requirements and its factual content	=	Module
Structure of the requirement's factual content	=	Type structure (analogy of data structure)

Table 1

Apart from the these, additional terms have been introduced, see Table 2

Internal interface	-	Different graphic displaying of a requirement from the remote area of the requirements system; it is used to express relations between requirements
Memory	-	Summary identification of a data structure; it is used to identify a related documentation unit. e.g. standard, regulation etc.

Table 2

Requirements Hierarchy

Hierarchy of the requirements is displayed in a hierarchic functional diagram (functional structure). The diagram presents decomposition of requirements down to the basic units. The requirements are split into groups containing requirements with similar meaning.

The final product of decomposition is a requirement of reasonable scope, up to one page of text. At this level the text is structured into marked paragraphs.

Relations between:

- elements within one group,
- elements from one group and elements from other groups (internal interface),
- elements from one group and other projects,
- elements from one group and related documents (standards etc.)

are expressed with a information flows diagram. The above-mentioned elements represent junction points of the diagram.

The links between elements in the diagram represent relations between the elements and are identified (described) with terms referring to the data structure. The data structure may then express a simple or fairly complicated structure of the relationship.

Requirements Content and Attributes.

The set of requirements is displayed in a graphic form with a module structure. The requirements are always the so-called "leaf – requirements" from the hierarchic tree of requirements.

Each requirement in a module has an assigned element representing reference to the type structure, expressing the structure of the requirement's textual content (the requirement's content is structured).

The text expressing factual content of the requirement is linked to a data element. The data element may be linked to a leaf element of the data or type structures. One data element may be linked to more leaf elements of the data or type structures. This may be used in a case where the content of different requirements is factually identical.

A data element represents an actually existing data object, in this case a text. An element of the data structure only symbolically represents an information unit as a part of the requirement's text.

Each requirement (function element) may be complemented with attributes.

Change Management

The factual content of a requirement may change in time and the changes need to be recorded in the documentation for the purposes of change management. Therefore texts of the requirements are stored in individual versions of data elements, which may be positively identified with a number of the version and date of origin.

Generally, all elements of all diagram types may be complemented with a text commentary.

Monitoring and Evaluation of Requirements Fulfilment

A dedicated item in the type structure is used to monitor and evaluate the changes, i.e. to find out:

- how the requirements are being or have been fulfilled,
- how the fulfilment is checked,
- results of the checking.

Repository and Evaluation Functions

All data about the requirements system are entered into the CASE system via a database - repository and are available for further use.

The *case/4/0* system is provided with an extensive set of evaluating and generating functions. It is also possible to enter additional evaluation functions into the system. For this purpose a simple programming language of the BASIC type is available, which enables to use all types of information in the repository and generate arbitrary formatted prints using the MS Word processor.

The evaluating functions support creation and utilization of the requirements system by automatically checking it for errors and reporting them. They also provide to the user lists of requirements, sorted out based on entered criteria.
HTML Format.

The newly available HTML format has been used to generate outputs from the Requirements Management System. It enables to generate a document in which the user may easily browse a current version of the requirements file. Also an analogy of fulltext search has been implemented, using special evaluating functions.

Hierarchic Requirements Structure

One of the fundamental procedures in requirements analysis is a design of the n-level hierarchic structure of the requirements.

To design the first two levels the Work has been physically structured into the so-called parts of the Work, see Table 3.

Ident.	**Level 1**	**Ident.**	**Level 2**	**Note**
AXX	Common Part			Basic Design
BXX	Control Points/MMI	B1X	Control Rooms	Main Control Room and Emergency Control Room
		B2X	Control Counters and Panels	
		B3X	Local Switchboards	
		B4X	Controllers	
CXX	Field Instrumentation	C1X	Measuring and Sampling Points	Including Sensors
		C2X	Measuring Circuits	
		C3X	Actuators	
DXX	Cabling	D1X	Penetrations	
		D2X	Cables	
		D3X	Cable Supporting System	
EXX	Power Supply			Level 2 left out
FXX	HVAC			Level 2 left out
GXX	Mechanical Engineering Part			Level 2 left out

HXX	Construction Part			Level 2 left out
RXX	Control Systems	RTS	Reactor Trip System	RTS
		TRIP	TRIP Breakers	RTS
		ESF	Engineered Safety Feature Actuation System	ESFAS
		EXC	Ex-core Neutron Flux Measurement System	EX-CORE
		REKT	Reactivity Meter	EX-CORE
		RLS	Reactor Limitation System	RLS
		RCS	Reactor Control System	RCS
		RRC	Reactor Rod Control System	RRCS
		SGP	Steam Generator Protection System	SGPS
		SAS	Support Actions System	SAS
		ELS	Emergency Load Sequencer	ELS
		PCS	Computer Information System	PCS
		INC	In-core Measurement System	IN-CORE
		PAM	Post Accident Monitoring System	PAMS

Table 3

The functional viewpoint has been adopted to design additional (lower) hierarchic levels. Examples of the hierarchic levels 3 and 4 for control systems are shown in Table 4.

Ident.	**Level 3**	**Ident.**	**Level 4**	**Note**
01	Harmonization Concept			
02	Basic Requirements			
03	Initial Condition			No requirement
04	Operational Requirements			
05	Service Requirements			
06	Performance Requirements	06.0	Basic Requirements	
		06.1	Function	
		06.2	Capacity	
		06.3	Reserves of the Equipment	
		06.4	Availability and Reliability	
07	Architecture Requirements	07.0	Basic Requirements	
		07.1	Integrity	
		07.2	Diversity	
		07.3	Redundancy	
		07.4	Design and Implementation	
		07.5	Links to the Surrounding Environment	

		07.6	Placement in the Layout	
		07.7	Computer Systems	
08	Testing and Maintenance Requirements			
09	Documentation Requirements			
10	Legislation and Standards Requirements			
11	Limitations			
12	Quality Requirements			
13				Not used
14				Not used
15				Not used
16	Implementation Requirements			
17	Requirements for Works			
18	Requirements for Services			
19	User's rights			

Table 4

Requirements Identification.

Unambiguously identification of user requirements is a fundamental for the Requirements Management System. In the example below a structured alphanumeric symbol has been selected:
XXXCC.D.D.D.D

where:

- **XXX** three-letter symbol; see Table 3
- **CC** two decadic digits; see Table 4
- **D** one decadic digit; see Table 4

The selected alphanumeric code is closely related to the requirement's position in the hierarchic structure and enables more organized and easier work with the requirements.

Requirements Attributes and Relations between Requirement

Requirements Attributes are a very powerful tool which enables additional manipulations with the requirements and various analyses in a selected set of requirements to study them from different viewpoints and find new interrelations between them.

In the concerned case the following attributes have been used:

- requirement status,
- traceability,
- affiliation to a particular part of the Work,
- requirement type (e.g. influence on nuclear safety),
- and other attributes added on as-needed basis in the course of individual stages of the Work implementation.

Another significant characteristic of the requirements are their mutual relations. In the concerned case there are two types of relations:

- relation between local requirements – relation between requirements at the same hierarchic level and subordinated to one common requirement at a higher level,
- relation between remote requirements – agreement, connection, parent/child.

Each relation between requirements may be described with an arbitrarily complex data structure.

Other important relations include:

- relation between a designed requirement and a requirement resulting from legislation or standards (one-way dependence),
- relation between a designed requirement and the so-called other project (one-way or two-way dependence).

Each relation may be described with an arbitrarily complex data structure.

Conclusions

The concerned solution represents an example of system approach in the application area outside the so-called data processing or general software development. The solution shown here is an example of its use on a potentially huge market – industrial computer applications.

The practical experience has proved that a good CASE system provides many more options for solutions in Requirements Management Systems than common specialised tools. Moreover, the CASE system may be used in the projects to solve other tasks too.

The use of the CASE system has increased efficiency of the work due to the extensive potential of this system to identify errors.

The basic version of the requirements file is a repository of 50 MB. It takes less than an hour to generate an updated version of the documents on a computer (500MHz, 64MB operating memory). However, partial and the most significant portions of the documents may be generated in a few minutes.

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. In case 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 system refurbishment project

OECD/CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-Based I&C Systems, Hluboká nad Vltavou, 25 – 27 September 2001

Author: Ceslav Karpeta (Scientech, Inc.- organizational component in the Czech Republic)

Co-author: Josef Rosol (CEZ – NPP Dukovany)

Abstract

A brief outline of the NPP Dukovany I&C system refurbishment project is given including a survey of the equipment and services suppliers and the scope of their involvement in the project activities. The adopted licensing process for the overall project is described and the Czech Republic regulatory authority project specific requirements relating to the digital computer-based I&C safety systems are summarized. The methods and ways the plant operator has adopted to ensure meeting some of those requirements are presented.

1. Introduction

The NPP Dukovany operates four units of the VVER-440/213 type. The design of the plant dates back to the 1970-ties. The designer of the Nuclear Steam Supply System (NSSS) was LOTEP Leningrad, the designer of the Balance of Plant (BOP) was Energoprojekt Praha which was bearing also the responsibilities of the so-called general designer and design supervisor during the plant construction. The first unit went operational in 1985. The other three units followed within next two years and the plant reached the rated capacity at the end of the year 1987.

I&C equipment for the NSSS was designed, manufactured and delivered by companies from the former Soviet Union. I&C systems of the BOP were designed, manufactured and installed by companies of the former Czechoslovak Republic.

During the 16 years of operation the NPP Dukovany has been achieving very good performance which provides evidence that it is a safe, efficient and reliable source of electric power.

The results of a number of assessments and audits conducted at the plant by national and international organizations in the 1990-ties indicated that the plant operation could continue till the year 2025, as a minimum. To ensure the achievement of such a goal an extensive and comprehensive program has been launched to support the plant long time competitiveness and public acceptability. This program is also intended, to the extent reasonably achievable, for the plant harmonization with the current safety requirements and practices.

One of the components of this program is the plant I&C system refurbishment. The existing plant I&C was grouped into the following 5 modules which could be refurbished relatively independently one from the other:

- module M1: reactor protection and limitation, engineered safety features actuation, post-accident monitoring, reactor power control
- module M2: unit information system

- module M3: logic/modulating control of the NSSS
- module M4: turbine-generator protection and control
- module M5: logic/modulating control of the BOP.

This paper addresses some licensing aspects of that portion of the refurbishment activities, which cover the modules M1 and M2. They are implemented under a separate project, which is referred to in the sequel as the I&C refurbishment project.

2. Scope of the I&C system refurbishment project and the vendors involved in its implementation

The scope of the module M1 and M2 refurbishment project is as follows:

- Design, manufacture, installation, and documentation of the replacement of the module M1 consisting of:
  - Digital Neutron Instrumentation System (DNIS) which is a replacement of the existing AKNT system
  - Digital Process Parameters Instrumentation System (DTPIS)
  - Digital Reactor Protection System (DRPS) which is a replacement of the existing HO-1 and SOB
  - Diesel Load Sequencer (ELS) which is a replacement of the existing APS system
  - Digital Reactor Limitation System (DRLS) which is a replacement of the existing HO 3, HO 4, and ROM systems
  - Control Rods Control System (RRCS), which is a replacement of the existing PNČI system
  - a replacement of the existing reactor trip breakers
  - Reactor Control System (RCS) which is a replacement of the existing ARM system
  - Support Actions System (SAS) which is a replacement of the existing TOPG system plus the non-trained part of the existing SOB, i.e. SOB-N.
- Design, manufacture, installation, and documentation of the replacement of the module M2 which consists of:
  - Steam Generator Protection System (SGPS) which is a replacement of the existing LOPG system
  - In-core instrumentation system (IN-CORE) which is a replacement of the data acquisition and processing portion of the existing KVRK system
  - Unit computerized information system (PCS) which is a replacement of the existing IVS-URAN system.
- Design, manufacture, installation, and documentation of a Post Accident Monitoring System (PAMS), which is an entirely new system. The scope includes all data acquisition and data processing equipment, any necessary new measurement circuits, and MMI equipment. This system is included in module M1.
- For module M1, replacement of:
  - Sensors associated with the upgraded systems including installation of new cables when required

  - Installation of all the other equipment that is needed for the new systems to function such as transducers, power supplies, etc.

- The module M2 systems will use the existing field instrumentation (measurement circuits).
- Interconnecting of all the new systems, connections to new cabling and to existing plant equipment. This includes temporary connections required because of step-by-step implementation of the Project during three or four refueling outages.
- Construction modifications in the main and emergency control rooms due to removal of the old I&C equipment and installation of new equipment.
- Local construction modifications to accommodate the replacement of old I&C equipment with new equipment and the installation of new cables.
- Modification of the existing full-scope unit simulator so that it reflects the main control room of unit 2 after completion of the I&C refurbishment project for this unit.

A prime contractor and several sub-contractors are involved in the refurbishment project. The prime contractor is ŠKODA JS a.s., located in Plzen, Czech Republic. ŠKODA JS is responsible for overall management of the project and it oversees the activities of the subcontractors.
FRAMATOME and SCHNEIDER have formed a consortium and share the responsibility for various portions of the supply of the module M1 systems.
The various sub-contractors that provide essential services or equipment for the replacement are:

- FRAMATOME ANP, France. FRAMATOME has overall responsibility for all activities needed to implement the module M1 systems including documentation, design, manufacturing, and participation in installation and commissioning, and personnel training.
- SCHNEIDER ELECTRIC, France. SCHNEIDER is responsible for the documentation, design, manufacture, and test of the DRPS, DTPIS, DNIS, DRLS, RCS, SAS, and ELS systems, plus the reactor trip breakers.
- CERME, France. CERME, as a sub-contractor to FRAMATOME, is responsible for the development of the PAMS system software, and for the manufacture and test of the PAMS.
- ŠKODA ENERGO s.r.o., Controls Division, Plzen, Czech Republic. ŠKODA ENERGO is responsible for the design, documentation, manufacturing, and installation of the RRCS system of Module M1.
- ZAT a.s., Příbram, Czech Republic. ZAT is responsible for the design, documentation, manufacturing, and installation of the module M2 systems, which are the IN-CORE, SGPS, and PCS systems. The in-core upgrade is the data processing portion only. The in-core instruments (thermocouples and neutron detectors) will not be replaced.
- IFE Halden, Norway. IFE was a direct contractor to ČEZ for the supply of the core monitoring software (SCORPIO – VVER), which was developed under an OECD sponsored project.
- I&C ENERGO a.s., Třebíč, Czech Republic. I&C ENERGO is responsible for the design, documentation and supply of the field instrumentation of the replacement systems. Regarding the implementation of the core monitoring system SCORPIO I&C was the prime contractor for the design and installation of the interfaces to the existing HINDUKŠ data acquisition subsystem and for the design and installation of the SCORPIO hardware.

- ORGREZ SC a. s., Brno, Czech Republic. ORGREZ, a direct contractor to ČEZ, is responsible for the development and verification of algorithms used in the existing I&C systems and for verifying the algorithms used in the innovative I&C systems.
- MEACONT PRAHA s.r.o., Praha, Czech Republic. MEACONT is a sub-contractor to ŠKODA JS and is responsible for developing and coordinating the basic design documentation for the whole Project. The basic design covers the interfaces and interconnections between the various systems and between the systems and the plant equipment.

All of the suppliers must provide support for training and for commissioning of the equipment they are responsible for.

The relationship between the various contractors and subcontractors is shown in Figure 1. The architecture of the refurbished module M1 systems, based on the use of the SPINLINE 3 platform, as designed during the basic design phase of the project is shown in Figure 2.

3. Licensing process applied to the refurbishment of the NPP Dukovany I&C systems important to safety

As per the provisions of the Atomic Act, reconstruction or implementation of other changes in nuclear facilities that affect nuclear safety, radiation protection, emergency preparedness and security falls into the category of activities for which a permission (license) must be granted by the Czech Republic regulatory authority, i.e., the State Office for Nuclear Safety (SUJB). The Act also outlines the contents of the documentation that must be submitted to the SUJB in support of the application for such a license. The documentation shall include the following information:

- description and justification of the planned reconstruction or other changes
- updating of the documentation that was approved by the regulatory authority during the nuclear facility commissioning and operation
- time schedules for implementation of the planned reconstruction or other changes
- evidence that the reconstruction or other changes will not negatively affect nuclear safety, radiation protection, emergency preparedness and security of the nuclear facility.

Documentation quoted in the second bullet has to be approved by the SUJB. It includes, among others, the limits and conditions of safe operation (plant technical specifications – Tech Specs) and the list of the so-called Selected Equipment as stipulated by the SUJB Regulation No.214/1997 Coll.

The “one-step” licensing process stipulated by the provisions of §9, (1), f) of the Atomic Act and commonly applied to the implementation of smaller scope reconstructions or other changes that affect nuclear safety, radiation protection, emergency preparedness and security of nuclear facilities, was felt to be not quite adequate for the NPP Dukovany large-scope several-stage I&C system refurbishment project. Therefore, a project specific licensing process has been conceived in several rounds of discussions between the plant operator and the regulatory authority. This process is copying to certain extent the licensing process applied to new nuclear power plant projects.

More specifically, the licensing process applied to the refurbishment of the NPP Dukovany I&C systems important to safety is structured to the following stages.

Stage 1

The objective of this stage is to obtain the regulatory authority position on the concept of the refurbishment project based on the evaluation by SUJB of the general technical and implementation aspects of the project. This stage is broken down into two phases:

Phase 1A:
The safety case of this phase is based on the information generated by the conceptual design of the refurbishment. The following topics are addressed in the documentation submitted to SUJB for assessment:

- description and justification of the plant I&C system refurbishment project
- general specification of the plant I&C system after completion of the refurbishment project
- preliminary discussion of the plant Tech Specs changes
- draft attachment to the list of the Selected Equipment
- preliminary time schedules of the refurbishment project implementation
- evidence on meeting the applicable requirements for ensuring nuclear safety at the level of detail corresponding to the outputs from the conceptual design.

Phase 1B:
The safety case of this phase is based on the information generated by the next stage of the conceptual design that is referred to as the preliminary design. The topics addressed in the documentation submitted to SUJB for assessment are the same as those of the phase 1A but the level of detail reflects the evolvement of knowledge resulting from the next stage of the design. Main focus of the phase 1B safety case is on the conservative safety analyses results to support the intended implementation of some new and modified functions of the reactor trip system and the engineered safety features actuation system.

Both the conceptual design and the preliminary design as well as the safety case documentation were worked out by the Czech design company Energoprojekt and reviewed by the project team members and their consultants. Some outputs of these efforts were also used in preparation of the documentation that was passed on to the bidders for the refurbishment project implementation.

Stage 2

The objective of this stage is to obtain, as per the provisions of §9(1)f) of the Atomic Act, the permission (license) to implement the refurbishment of the plant I&C systems important to safety. The safety case of this stage is based on the results of the basic design of the refurbished I&C systems important to safety performed by the supplier contracted for the implementation of the project and by its subcontractors. The documentation submitted to the SUJB for licensing assessment consists of:

- a series of Topical Reports covering the following subject areas:
  - software life cycle planning (software development plan, software quality assurance plan, software verification and validation plan, software configuration management plan, software safety analysis plan)
  - equipment qualification (description of methodologies to be used in the environmental, seismic and electromagnetic compatibility qualification)
  - system reliability (description of methodologies to be used in qualitative and quantitative reliability analysis of the individual I&C systems and, at least, some preliminary results of these analyses)
  - design of the individual I&C systems

- amendment to the existing Final Safety Analysis Report (evidence that the applicable requirements of the design for safety have been met is provided here at the level of knowledge reflecting the results of the basic design to document that the refurbishment will not impair the nuclear safety of the plant)
- draft update of the limits and conditions of the plant safe operation
- draft attachment to the list of the Selected Equipment
- time schedules of the project implementation.

Stage 3

This stage is also broken down into two phases.

Phase 3A:
The objective of this phase is to obtain the regulatory authority position on the implementation aspects of the refurbishment project in each individual unit of the plant. The safety case will be a kind of an update of the stage 2 safety case based on the results of the detail design of the refurbished I&C systems for each unit. It will also include plans for installation, testing, and commissioning of the refurbished I&C systems during individual implementation phases of the project at the subject plant unit. Positive position will provide the plant operator with a sound basis for giving its consent to the commencement of manufacturing of the I&C equipment by the suppliers.

Phase 3B:
This phase is aimed at obtaining the regulatory authority consent to the implementation of a specific part of the refurbishment, which is to be accomplished during a particular planned outage of the subject unit for refueling. Hence, it will be repeated as many times as is the number of outages necessary for the completion of the refurbishment at this unit. The safety case will again be a kind of an update of the previous phase safety case, i.e. either of the 3A phase or 3B phase safety case, and will in addition include:

- description of the initial and final state of the unit I&C system with respect to the actual phase of the refurbishment implementation
- installation, testing and commissioning plans specific to the actual implementation phase
- updates of the Tech Specs and of the list of the Selected Equipment specific to the actual implementation phase
- reports on the results of the equipment qualification and system verification and validation activities performed at the manufacturer on the systems to be implemented during the actual implementation phase
- evaluation of the quality assurance plan fulfillment during manufacturing of the equipment to be implemented during the actual implementation phase.

Stage 4

The objective of this stage is to obtain the SUJB permission for the reactor start-up after refueling as per the provisions of §9(1)e) of the Atomic Act, which at the same time will include the SUJB consent to the operation of the refurbished I&C systems important to safety implemented during the current implementation phase. Hence, this phase will also be repeated as many times as is the number of outages necessary for the completion of the refurbishment at the subject plant unit. The safety case will again be a kind of an update of the preceding phase 3B safety case, and will in addition include:

- description of the actual state of the plant I&C system after completion of the current implementation phase
- evidence of the equipment and personnel readiness for operation (this will include the evaluation of the refurbished I&C system installation and pre-operational tests)

- update of the Tech Specs (if necessary).

After the completion of the last refurbishment implementation phase at a particular unit, the outcome of the stage 4 of the licensing process will be the SUJB permission for permanent operation of the unit refurbished I&C systems important to safety.

The safety case documentation providing evidence that the applicable requirements of the design for safety have been met in the design and implementation of the refurbished I&C systems important to safety will have the format and contents as per the US NRC Regulatory Guide 1.70 and Chapter 7 of the US NRC Standard Review Plan (year 1997 issue).

Present status of the licensing process is as follows: Stage 1A of the I&C system refurbishment project licensing process was completed at the end of 1999. Safety case of the stage 1B was submitted to the SUJB in May 2000. Its assessment has been completed without any significant negative findings. The safety case of the stage 2 of the licensing process was submitted to SUJB in May 2001. Its regulatory evaluation is now nearing completion.

4. Project specific regulatory requirements relating to the digital computer-based I&C safety systems

Czech Republic legislation which governs the safety aspects of siting, design, construction, commissioning, operation and decommissioning of nuclear facilities can be viewed as structured into the following two-level hierarchy:

- the Atomic Act passed by the Parliament (Act No.18/1997 Coll.)
- a series of regulations issued by the State Office for Nuclear Safety (SUJB).

The provisions of the Atomic Act which specifically apply to the implementation of changes affecting nuclear safety, radiation protection, security and emergency preparedness of nuclear facilities, hence also to the refurbishment of the I&C systems important to safety, are those that:

- define the powers and responsibilities of the SUJB
- set forth general and specific conditions for performing activities associated with the uses of nuclear power
- cover handling of radioactive wastes
- define the contents of the documentation that has to be submitted to the SUJB as the documentation accompanying the nuclear facility operator's application for the permission (license) to implement changes affecting nuclear safety.

The lower-level legislation, which is most relevant to the I&C systems of nuclear facilities, is the following group of the SUJB regulations:

- regulation No. 195/1999 Coll. on the requirements for the assurance of nuclear safety, radiation protection and emergency preparedness in nuclear facilities
- regulation No. 214/1997 Coll. on quality assurance in activities relating to the uses of nuclear power and activities having a potential for causing irradiation and on specification of criteria for assignment of the Selected Equipment to safety classes
- regulation No. 106/1998 Coll. on the assurance of nuclear safety and radiation protection in commissioning and operation of nuclear facilities.

Regulation No. 195 sets requirements pertinent to the design of systems important to safety. These requirements are of rather general nature comparable e.g. to the US NRC General Design Criteria. The

provisions of this regulation which address the design for safety of the plant I&C systems provide functional and design requirements covering the following areas:

- defense-in-depth
- quality assurance
- protection against equipment failures
- fire protection
- protection against the effects of natural events
- protection against events caused by human being activities outside the nuclear facility
- plant instrumentation and control systems
- plant protection systems
- relations between the plant protection and instrumentation and control systems
- plant control points
- systems for tripping the reactor
- power supply systems.

Compliance with this regulation was focused upon in establishing the design basis and system requirements both for the innovated plant I&C system as a whole as well as for the I&C portions of the individual plant safety and safety-related systems. Design and implementation of the refurbished I&C systems important to safety will have to meet, in the first place, all the applicable requirements of this regulation.

Regulation No. 214 deals in detail with quality assurance aspects of the activities associated with siting, design, construction, commissioning, operation and decommissioning of nuclear facilities. It covers the following topics:

- implementation of the quality system
- quality system requirements
- requirements for quality assurance of the Selected Equipment as assigned to safety classes
- requirements pertinent to the scope of the quality assurance programs
- criteria for the assignment of the Selected Equipment to safety classes
- the format and contents of the list of the Selected Equipment.

The I&C refurbishment project overall quality assurance program was established in line with the requirements of this regulation pertinent to such entities as processes, activities, products, organizations, personnel, and their combinations. More specifically, the provisions of the article 23 of this regulation which apply to the so-called “special processes”, i.e. processes the results of which cannot be fully verified through checking and testing, have been used as a regulatory basis for setting requirements to be met by the software development process of the safety critical software to be implemented in the refurbished I&C systems built on programmable digital platforms. Quality systems of all the contractors participating in the refurbishment of the I&C systems important to safety will have to be compliant with the applicable provisions of this regulation.

Regulation No. 106 addresses those aspects of safety assurance, which are relevant to the commissioning and operation of nuclear facilities including start-up of nuclear power plants after refueling. It specifies:

- general requirements for the commissioning and operation of nuclear facilities
- technical and organizational conditions of safe commissioning of nuclear facilities which cover, in particular:
  - the specification of the individual phases of the nuclear facility commissioning
  - the specification of documentation to be submitted to the regulatory authority for evaluation in the process of issuing permissions to begin and proceed through the individual phases of the commissioning

- limits and conditions of the nuclear facility safe operation (technical specifications)

♦ technical and organizational conditions of safe operation of nuclear facilities

♦ requirements to be met when reaching reactor criticality after refueling.

Conformance to the applicable provisions of this regulation will be the subject of those I&C refurbishment project activities that relate to updating of the existing plant technical specifications and operational procedures during and after completion of the innovated I&C systems implementation, and to testing of the installed new I&C systems prior to the plant start-up after completion of the individual stages of the I&C system refurbishment.

It is obvious that the design, implementation and operation of the refurbished I&C systems important to safety must meet all the applicable requirements of the above discussed legislation. Being aware of the importance of the licensing process to the success of the project the NPP Dukovany I&C refurbishment project team has been in close touch with the relevant SUJB staff members from the early stages of the project preparation to brief and discuss with them all the applicable safety issues. These efforts resulted in laying down by the regulatory authority, in some areas of concern, project specific requirements with respect to the scope of the refurbishment and the design of the I&C systems important to safety.

A summary of the SUJB project specific requirements is presented in the sequel.

Scope of the refurbishment project

Refurbishment of the following I&C systems shall be implemented:

♦ reactor protection system

♦ engineered safety features actuation system

♦ emergency load sequencer

♦ reactor limitation system.

Common requirements

Common requirements for the reactor protection system, engineered safety features actuation system and emergency load sequencer on one side, and for the reactor limitation system on the other side have been set forth in the following areas:

♦ ensurance of functionality

♦ ensurance of reliability

♦ ensurance of performance

♦ ensurance of equipment qualification

♦ ensurance of quality.

Classification of the I&C systems important to safety

Safety classification of the I&C systems important to safety shall be performed on the basis of deterministic criteria in compliance with the guidance given in the IEC Std. 61226, i.e. assignment of the I&C functions and the associated systems and equipment to the following categories: category A, category B, and category C.

Acceptability of the digital computer-based I&C systems important to safety

Implementation of the refurbished I&C systems important to safety using software-based digital computer technology is acceptable provided that:

- the design, manufacturing, installation, testing, commissioning and operation of those systems will meet all the applicable provisions of the Czech legislation
- those systems will meet all the requirements stated in the SUJB resolution No. 79/1999
- those systems will meet, to the extent reasonably achievable, the requirements and recommendations of the applicable IAEA documents, IEC standards, national industrial standards such as the CSN and IEEE standards, and the US NRC General Design Criteria and Regulatory Guides.

In addition to this, a number of project specific requirements have been set fourth. Those of them, which apply to digital computer-based I&C systems are summarized below.

Software development process for the I&C systems important to safety

Software development process for category A I&C functions shall be a well-structured process consisting of the following activity groups:

- planning activities
- development activities, i.e. requirements activities, design activities, implementation activities, validation activities, and installation activities
- integral activities, i.e. verification activities, configuration management activities, and safety analysis activities.
-

Software development processes for category B I&C functions shall be basically the same as the one for category A functions.

Software development process for category C I&C functions shall be the same as that for high quality industrial I&C applications.

Verification and validation of the software for the I&C safety systems

For the software implementing category A I&C functions the following shall apply:

- V&V activities compliant with the requirements of the IEC Std. 880 and NRC RG 1.152 shall be performed during the software development process as well as during the consecutive life-cycle phases
- no third party independent V&V activities are required provided that the software V&V team at the manufacturer is management and financial independent of the development team
- audits of the software development process shall be performed right from the start-up of this process.

Defense against common cause failures (CCF) in the software of safety systems

With respect to the postulation of CCF the following shall apply:

- CCFs will not need to be postulated in safety system hardware including the sensors
- CCFs will have to be postulated in complex software implementing safety functions
- CCFs will not need to be postulated in simple software modules participating in implementation of safety functions provided that:
  - these software modules can be fully tested, or
  - extensive positive operational experience from previous applications in similar safety applications is available and well documented
- CCFs will not need to be postulated in software modules implementing support functions such as e.g. software for on-line diagnostics provided that it can be proved that errors in this software cannot degrade performance of the safety functions.

Implementation of diverse means of protection against the postulated CCFs:

- is required with respect to the ANSI Condition II and III plant design basis events (postulated initiating events) with the estimated frequency of occurrence greater than 10E-3 per year
- is not required for less frequent plant design basis events, i.e. for some ANSI Condition III events and all ANSI Condition IV events.

The following relaxed acceptance criteria can be applied in the accident analysis of the safety actions initiated by the diverse means of protection:

- maintenance of coolable core geometry
- maintenance of the primary coolant system integrity
- maintenance of the hermetic zone integrity
- availability of sufficient time (not less than 30 minutes) for taking manual safety actions as the diverse means of protection.

The following two approaches in diversity implementation will be viewed as adequate:

- functional diversity implemented in two functionally isolated subsystems of a safety system which process two different groups of input signals, or
- implementation of a separate diverse protection system which features functional isolation of the primary protection system, different hardware and different software.

Adequacy of the diversity implementation shall be supported by analysis.

Communications between subsystems of the digital computer-based I&C safety systems

Requirements set forth on the communications between subsystems of the I&C safety systems are as follows:

- no failure in a subsystem of a safety system division shall affect the performance of safety functions in the redundant divisions of this system
- sharing of data among the redundant divisions of a safety system, including sharing of input signals, shall not degrade the functional isolation of those divisions
- loss of communication between redundant divisions shall not cause interruption of the division activities
- all communication links shall be checked by on-line diagnostics
- the fail-safe design principle shall be applied where practically achievable to provide for pre-defined response of the safety system to the loss or degradation of the communications.

Testability of the digital computer-based I&C safety systems during reactor operation

The SUJB position on testability during operation has been stated as follows:

- the on-line diagnostics shall perform three functions:
  - upon system start-up and re-starts it shall check the status and the correctness of hardware functioning and the configuration of the installed software
  - during system operation it shall check sequentially in each code execution cycle the status and correctness of hardware functioning in such a way that the full-scope checking be completed in about 10 minutes

  - during system operation checking of the communications based on the diagnostic information contained in the messages transmitted over the communication links and supported to the maximum possible extent by implementation of deadman timers which indicate interrupts in the communications
- periodic surveillance testing shall provide for:
  - testing of the hardware of the system equipment involved in information processing portions of the safety functions and in on-line diagnostic functions that is not tested to the full extent by the system on-line diagnostics
  - if there are no hardware components tested completely by the system on-line diagnostics then the periodic surveillance testing need not to be implemented
- the provisions of §18 section (1) of the SUJB regulation No.195/1999 Coll. must be met during system testing, i.e. the single failure criterion and the minimum redundancy requirement.

Compliance to the single failure criterion

The requirement for compliance of the I&C safety systems with the single failure criterion is stated from two perspectives:

- what concerns the type of single failures, the effects of the plant design basis events on the safety systems, and the impacts of a single failure occurrence the provisions of the IEEE Std. 379 are required to be met
- what concerns the impacts of a single failure occurrence the provisions of the §18 section (1b) of the SUJB regulation No. 195/1999 Coll. are also invoked to comply with the minimum redundancy requirement.

Exemptions from the conformance to the single failure criterion under extraordinary situations could be considered by the regulatory authority on a case-by-case basis; this, however, does not apply to regularly occurring situations such as periodic surveillance testing. Separate diverse protection systems if implemented within the I&C system refurbishment project are not required to meet the single failure criterion.

Equipment qualification

The regulatory authority requires that an equipment qualification program be established for the refurbished I&C systems important to safety encompassing the following activities:

- program preparation
- equipment qualification implementation
- maintenance of the equipment qualification.

Program preparation activities should include specification of:

- the equipment to be qualified
- the functions to be performed by this equipment and the time interval during which the functions are required
- the equipment location in the plant
- the environmental and operational conditions of the equipment
- methods and procedures for performing the qualification.

Equipment qualification implementation activities should include one or a combination of the following:

- qualification by type testing as the preferred qualification method
- qualification by analysis
- qualification based on operational experience.

Qualification maintenance activities should include:

- preventive maintenance
- procurement and stock of spares
- monitoring of the environmental and operational conditions
- tracing of failures
- personnel training.

Acceptance of qualification certificates will be governed by the applicable provisions of the Act No.22/1997 Coll.

Reliability

The regulatory authority requires that:

- numerical values of the quantitative reliability indicators be established for the individual I&C systems important to safety
- in setting those values for the safety systems the plant safety goal represented by the calculated core melt frequency of 10E-4/year shall be considered; for the other systems those values should be derived from operational considerations
- as a minimum set of the reliability indicators the instantaneous or average system availability and the frequency of spurious initiations shall be used
- qualitative reliability analyses shall be performed for all safety category A and B I&C systems employing the FMEA methodology or its FBA version for the digital computer-based systems
- quantitative reliability analyses shall be performed for all I&C systems important to safety using the FTA method; in these analyses the potential for CCF and human errors shall be considered, as appropriate.

Documentation

The project specific regulatory requirements include also specification of documentation that is to be submitted for licensing evaluation in addition to the amendment to the existing plant Final Safety Analysis Report, such as a series of Topical Reports addressing specific safety issues.

The above quoted project specific requirements have been derived from the applicable provisions of:

- the Czech Republic legislation
- the IAEA Safety Series documents and Technical Reports
- the IEC standards
- the US NRC Regulatory Guides and NUREGs
- national standards such as IEEE and CSN standards.

The results of the EU project OJC 316 “Licensing-Related Assessment of Digital Computer Based Technology for I&C Important to Safety”, which is aimed at transferring of the licensing methodologies employed in the EU member states to the countries wishing to join the EU, have also been considered in setting those requirements.

5. Planning and conducting audits of the design and manufacturing processes

Many of the to be implemented digital computer-based I&C systems are essential to continued safe operation of the plant, so it is imperative that the suppliers design, manufacture, and install the equipment in conformance to their Quality Assurance (QA) programs, applicable national and international QA requirements, and any additional requirements intended to assure continued safe, efficient, and reliable plant operation.

CEZ intends to perform various audits to assure compliance with the applicable requirements, assure that the installed equipment will operate as intended, and to provide information needed to support the SUJB licensing activities. An Audits Plan has been developed to provide a basis for those activities.

The following were considered in the preparation of this Plan:

- the range and scope of the audits should provide CEZ with objective proof that the supplier processes meet the project quality requirements and SUJB requirements
- the requirements against which compliance is to be verified by the audits should be specified including identification of their sources in the form of references
- the Plan should specify the purpose and timing of the audits.

The objectives of the audits to be conducted during the NPP Dukovany I&C refurbishment project have been defined as follows:

- to support confidence that the hardware and software development processes of the refurbished I&C systems important to safety have been adequately planned for

- to support confidence that the design and manufacturing of the hardware and software of those systems, including the verification and validation activities as well as the configuration management activities, are being performed to the plans.

The following audit types will be conducted to this end:

Audit Type A, Design Requirements.

This audit will be performed only once (prior to the first outage for unit 3) at Framatome/Schneider, SKODA/MEACONT, SKODA ENERGO, and ZAT since they are preparing design requirements.

Audit Type B, Hardware and Software Design.

This audit will be performed prior to each outage for each vendor that is supplying detailed design documentation and equipment for the upcoming outage.

Audit Type C, Manufacturing and Test.

This audit will be performed prior to each outage for each vendor that is supplying equipment for the upcoming outage.

Audit Type B/C, Hardware Design plus Manufacturing and Test.

This audit will be performed at I&C Energo prior to selected outages.

Audit Type D, Algorithm Development.

This audit will be performed only once (prior to the first outage for unit 3) at ORGREZ SC.

The new I&C systems have been assigned classifications in accordance with IEC standard No. 61226. The selection of standards to be used as the basis for the audits follows this classification and addresses all of the important issues at a level of detail that is suitable for conducting the audits and for addressing the applicable SUJB requirements. Hence:

- the software development process for IEC 61226 category A systems (SUJB safety class 2) will be audited for compliance to IEC 60880 and 60880-2; the software development process for IEC 61226 category B and C systems (SUJB safety class 3) will be audited for compliance to ISO 9000-3 and ISO/IEC 12207
- the hardware development process for IEC 61226 category A systems (SUJB safety class 2) will be audited for compliance to IEC 60987. The hardware development process for IEC 61226 category B and C systems (SUJB safety class 3) will be audited for compliance to ISO 9001
- the audits will also address configuration management issues because of the importance of assuring compatibility between the efforts of the several vendors involved in the project. ISO 10007 will be used as the basis for the configuration management auditing.

While performing the audits, US NRC BTP HICB-14 may also be used to provide additional guidance for evaluating the application of the above mentioned IEC standards.

A set of checklists has been has been developed for the following audit groups:

- *Design Requirements Audit.* The standards references in this group include sections that:
  - directly relate to developing the design requirements
  - relate to activities that need to be performed to develop the requirements such as verification, documentation, modifications, etc.
  - relate to items that need to be addressed in the requirements such as CCF, MMI, test requirements, etc.
  - relate to activities that need to be in place prior to start of the hardware and software design such as engineering tools, plans, etc.
- *Hardware/Software Design Audit.* The standards references in this group include sections that:
  - directly relate to performing the design
  - relate to activities that need to be performed to support the design such as verification, documentation, modifications, etc.
  - relate to items that need to be addressed in the design such as integration, validation, operation, etc.
- *Manufacture and Test Audit.* The standards references in this group include sections that:
  - directly relate to performing the manufacturing and factory test
  - relate to activities that need to be performed to support manufacturing and test such as error reporting, control of instruments, documentation, etc.
- *Special Requirements Audit.* The standards references in this group includes sections that:
  - relate to the configuration management issues
  - apply to the preparation and validation of the algorithms for the individual systems.

The Dukovany I&C refurbishment project involves several suppliers with various responsibilities and scopes. Therefore the audits will also consider issues that need to be addressed to ensure adequate co-ordination between the suppliers such as to whether:

- the interfaces between the equipment from the various suppliers are well defined, consistent, and provided to all involved suppliers
- the overall response of the systems adequately consider the cumulative response of equipment from the various suppliers
- the terminology used by the various vendors is consistent and conforms to CEZ's terminology
- installation requirements and restrictions that are placed by equipment supplied by one vendor are defined and provided to other impacted suppliers and to the installer.

6. Conclusions

The first audit in the series of audits to be conducted during the NPP Dukovany I&C module M1 and module M2 systems refurbishment project implementation was performed at Framatome ANP and Schneider Electric companies at the end of June and beginning of July 2001; it took 8 working days. The audit program was to evaluate the preparation of the system requirements, configuration management plans, software requirements and hardware requirements. The audit was performed in accordance with the following three checklists:

- checklist for system requirements preparation per ISO 9000-3 and configuration management per ISO 10007
- checklist for software requirements preparation per IEC 60880 and 60880-2
- checklist for hardware requirements preparation per IEC 60987.

The audit team was composed of four members: two of them, including the audit team leader, were the NPP Dukovany I&C refurbishment project staff members, the other two were I&C consultants of the Scientech, Inc. company. A nuclear safety inspector of the SUJB and two staff members of the prime contractor, i.e. SKODA JS, participated in the audit as observers.

References

1. SUJB position with respect to selected aspects of the NPP Dukovany I&C refurbishment project; Prague, September 2000.

2. Quality assurance program for the I&C refurbishment project; CEZ-NPP Dukovany, October 2000.

3. Safety case of the NPP Dukovany I&C refurbishment project for the stage 2 of the licensing process; CEZ-NPP Dukovany, May 2001.

4. Plan for auditing the design and manufacturing process implemented for the NPP Dukovany I&C Innovation Project; Scientech, Inc.-organizational component in the Czech Republic, June 2001.

5. Implementation of new digital safety systems on NPP Dukovany; WANO-Paris Center workshop on computer based I&C systems: Necessity for continuous improvement; Beznau NPP, Switzerland, August 2001.

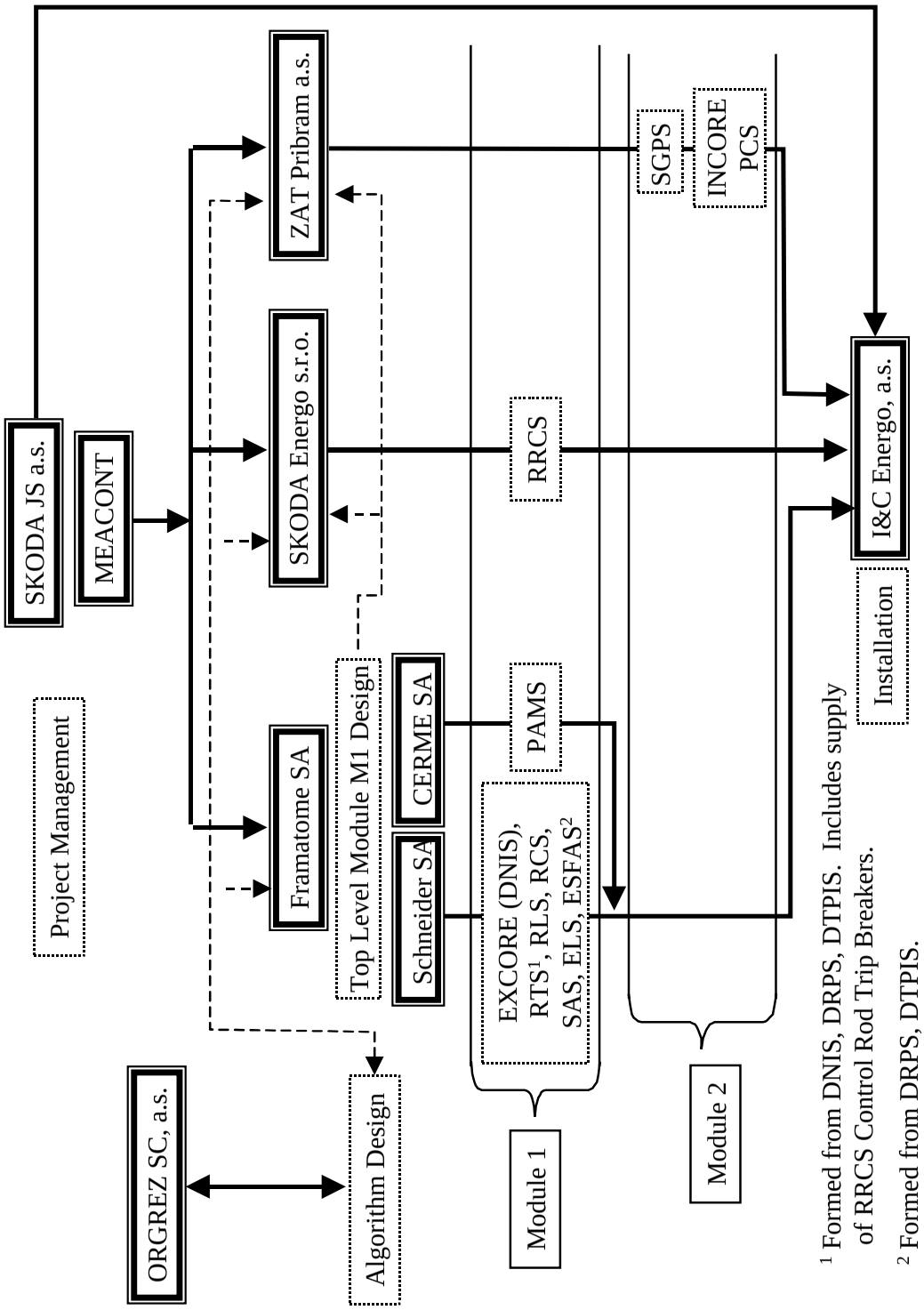


Figure 1. Relationship between suppliers

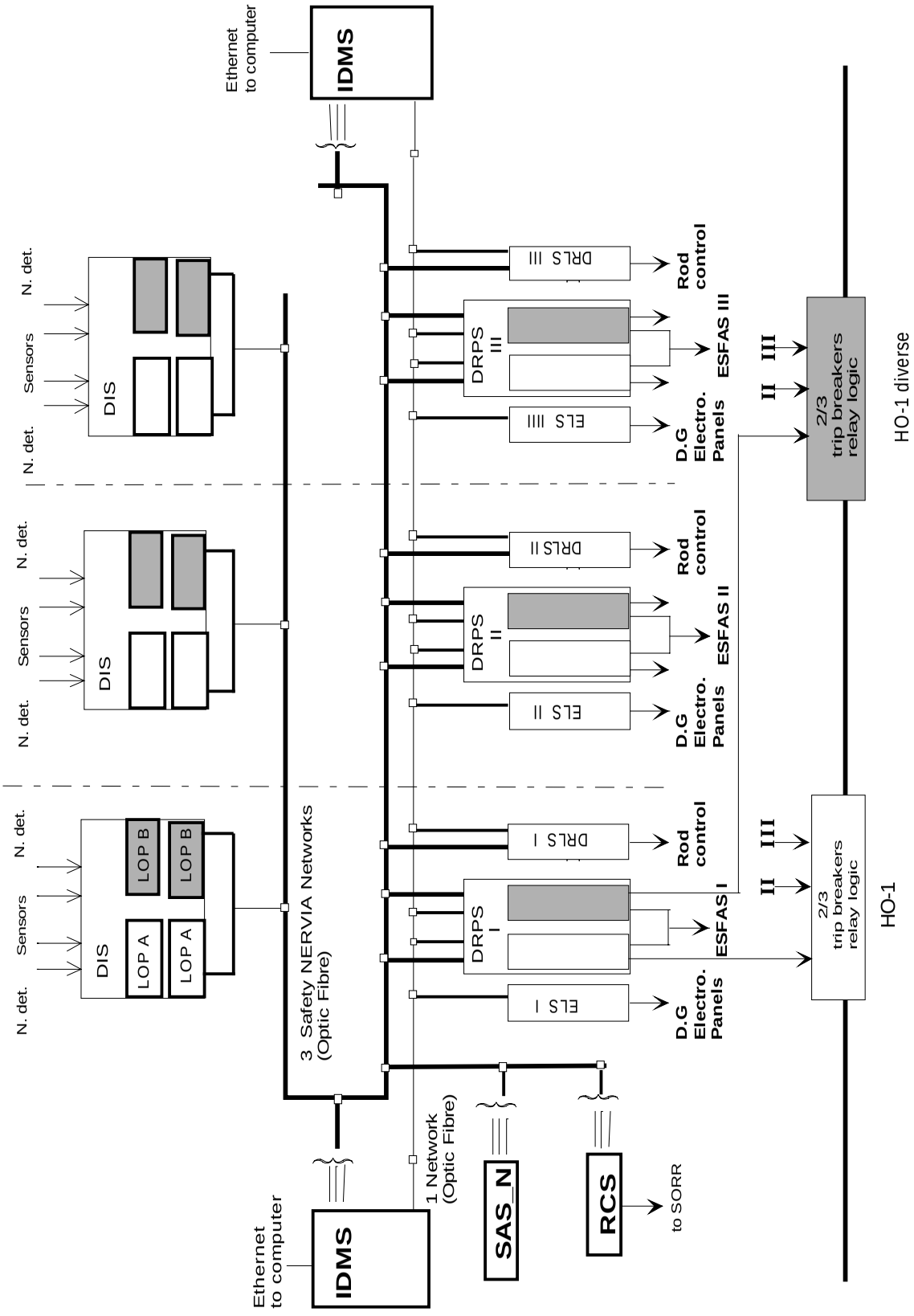


Figure 2. Architecture of the module M1 I&C refurbished systems

E. LIST OF PARTICIPANTS

♠ - visit of NPP Temelin

BELGIUM

COURTOIS, Pierre J.
Advanced Technologies Dept.
AIB-Vinçotte Nucleaire
Avenue du Roi, 157
B-1060 Brussels

Tel: +32 2 536 83 22
Fax: +32 2 536 85 85
Eml: courtois@info.ucl.ac.be

CHINESE TAIPEI

♠JEEN-YEE LEE,
Taiwan Power Company
20F, 242, Roosevelt Road
Sec. 3. Taipei, Taiwan

Tel.: +886 2 23667156
Fax: +886 2 23671675
Eml.: *D02705*@taipower.com.tw

♠SWU YIH,
Institute of Nuclear Energy Research
PO Box 3-11
Lung Tang, Taiwan

Tel: +3-4711400-6335
Fax: +3-4711400-6335
Eml: syih@iner.gov.tw

♠DER-JEH SHIEH
Institute of Nuclear Energy Research
PO Box 3-11
Lung Tang, Taiwan

Tel: 886-3-4711400-6300
Fax: 886-3-4711415
Eml: djshieh@iner.gov.tw

♠CHANG-FU CHUANG
Nuclear Regulation Division
Atomic Energy Council Taiwan
67, Lane 144, Keelung Rd., Sec. 4
Taipei, Taiwan 106

Tel.: +886 2 23634180, ext. 307
Fax.: +886 2 23635377
Eml.: chuang@aec.gov.tw

CZECH REPUBLIC

KRIZEK, Karel
Head of I&C Operation
NPP Temelin
CEZ, A.S.
373 05 Temelin

Tel: +420 334 422 223
Fax: +420 334 422 3815
Eml: Krizek_Karel/4430/ETE/CEZ@.mail.cez.cz

KRS, Petr
State Office for Nuclear Safety
Senovazné Square, 9
110 00 Prague 1
Tel: +420 2 216 24 206
Fax: +420 2 216 24 396
Eml: petr.krs@sujb.cz

PETRUZELA Ivan
I&C Energo s.r.o.
Areál VÚ
190 16 Praha 9 - Bechovice
Tel.: +420 2 6706 2181
Fax: +420 2 6706 2182
Eml.: ipetruzela@ic-energo.cz

BEDNARIK Karel
I&C Energo s.r.o.
Areál VÚ
190 16 Praha 9 - Bechovice
Tel.: +420 2 6706 2185
Fax: +420 2 6706 2182
Eml.: *kbednarik@ic-energo.cz*

PIROUTEK Zdenek
I & C Energo s.r.o.
190 11 Praha 9 – Bechovice
Tel.: +420 2 67062182
Fax: +420 2 67062182
Eml.: zpiroutek@ic-energo.cz

ROUBAL S
I & C Energo s.r.o.
190 11 Praha 9 – Bechovice
Tel.: +420 2 67062182
Fax: +420 2 67062182
Eml.: sroubal@ic-energo.cz

RUBEK J.
I & C Energo s.r.o.
190 11 Praha 9 – Bechovice
Tel.: +420 2 67062183
Fax: +420 2 67062182
Eml.: jrubek@ic-energo.cz

ZAVODSKY Petr
CEZ, a. s.
Division of Construction
NPP Temelín
Tel: +420 334 78 2151
Fax: +420 334 78 3815
Eml: Zavodsky_Petr@mail.cez.cz

PLISKA Petr
I & C Energo s.r.o.
Prazska 684
67401 Trebíc
Tel.: + 420 618 893 300
Fax: + 420 618 893 999
Eml.: jpliska@ic-energo.cz

WAAGE Herbert
CEZ, a. s.
Division of Construction
NPP Temelín
Tel: +420 334 78 3560
Fax: +420 334 78 3815
Eml: waage_herbert@mail.cez.cz

CENDELÍN J.
West Bohemian University in Pilsen
Faculty of Applied Sciences
Department of Cybernetics
Univerzitní 22,
30614 PLZEN
Tel.: + 420 19 7491 155
Fax: + 420 19 279 050
Eml: cendelin@kky.zcu.cz

♠KRYL Petr
Orlík 266
Nuclear Engineering SKODA
316 06 Plzen
Tel.: +420 19 704 2825
Fax: +420 19 75 20 600
Eml.: pkryl@jad.in.skoda.cz

ZATLOUKAL Jan
Nuclear Researh Institute Rez a.s.
250 68 Rez
Tel.: +420 19 7441099
Fax: +420 19 7441097
Eml.: zat@ujv.cz

KRÁKORA Petr
Nuclear Researh Institute Rez a.s.
250 68 Rez
Tel.: +420 19 7441098
Fax: +420 19 7441097
Eml.: krakora@ujv.cz

KUBÍNOVÁ Jana
Schneider Electric CZ, s.r.o.
Thámová 13
186 00 Praha 8
Tel.: +420 2 810 88 634
Fax : +420 2 248 10 849
Eml.: jana_kubinova@cz.schneider- electric.com

♠ KARPETA Ceslav
Scientech, inc. - CR
A. Staška 30
146 00 Praha 4
Tel.: +420 2 22 13 53 38
Fax : +420 2 22 13 53 37
Eml.: scikar@mbox.vol.cz

KUBANOVÁ Iva
I&C Energo a.s.
Husova 17
370 05 Ceské Budejovice
Tel.: +420 38 510 23 11
Fax : +420 38 534 49 17
Eml.: ikubanova@ic-energo.cz

FINLAND

♠REIMAN Lasse
STUK
P.O.Box 14
FIN-00081 Helsinki
Tel.: +358 9 7598 8379
Fax : +358 9 7598 8382
Eml: lasse.reiman@stuk.fi

♠JÄRVINEN, Marja-Leena
Finnish Centre for Radiation
and Nuclear Safety (STUK)
P.O. Box 14
FIN-00881 Helsinki
Tel: +358 (9) 759 88 304
Fax: +358 (9) 759 88 382
Eml: marja-leena.jarvinen@stuk.fi

♠LINDEN Ulf
Fortum power and Heat Oy
Loviisaa Power Plant
P.O. Box 23
07901 Loviisa
Tel.: +358 10 45 53800
Fax:
Eml.:ulf.linden@fortum.com

FRANCE

♠BOUARD, Jean-Paul
Division Contrôle Commande
E.D.F. - SEPTEN
12-14, avenue Dutriévoz
F-69628 Villeurbanne Cedex
Tel: +330472 82 71 66
Fax: +330472 82 77 04
Eml: jean-paul.bouard@edfgdf.fr

SOUBIES, Brigitte
IPSN/DES/SAMS
Centre d'Etudes Nucleaires
60-68 ave General Leclerc
Batiment 08, BP 6
92265 Fontenay-aux-Roses CEDE
Tel: +33 1 46 54 84 06
Fax: +33 1 47 46 10 14
Eml: brigitte.soubies@ipsn.fr

♠POIZAT Francois,
EDF Industry/Basic Design Department,
12-14 avenue Dutrievoz,
69628 Villeurbanne Cedex
Tel.: +33 4 72 827 479
Fax: +33 4 72 82 77 04
Eml.: francois.poizat@edf.fr

♠ESMENJAUD Claude
Schneider Electric Industries M3
38050F Grenoble
schneider.fr
Tel.: +33 476 605 860
Fax: +33 476 606 462
Eml.:claude_esmenjaud@mail.

BUREL Jean-Pierre
Schneider Electric Industries M3
Safety Electronics and Systems, Usine M3
23 Chemin du Vieux Chene
F-38240 Meylan
Tel.: +33 476 606 884
Fax: +33 476 606 992
Eml.:jean-pierre_burel@mail.schneider.fr

MOSIO Bernard
Nuclear International Project Manager
Schneider Electric Industries M3 plant
23 Chemin du Vieux Chene
F-38240 Meylan
F-38050 Grenoble cedex 9
Tel.: +33 476 60 55 90
Fax: +33 476 60 63 52
Eml.:bernard_mosio@mail.schneider.fr

LAPASSAT Anne-Marie
DSIN/SD2
F92266 Fontenay-aux -Roses
Tel.: 33 1 43 19 71 03
Fax : 33 1 43 19 70 66
Eml: anne-marie.lapassat@industrie. gouv.fr

GERMANY

♠LINDNER, Arndt
Institute of Safety Technology (ISTec)
P.O. Box 1213
85 740 Garching
Tel: +49 89 32004 529
Fax: +49 89 32004 300
Eml: lia@grs.de

♠SCHNÜRER Günter
Institute of Safety Technology (ISTec)
P.O. Box 1213
85 740 Garching

Tel.: +49 89 32004 523
Fax: + 49 89 32004 300
Em.: sgu@ grs.de

♠KERSKEN Manfred
Institute of Safety Technology (ISTec)
P.O. Box 1213
85 740 Garching

Tel.: +49 89 32004 546
Fax: + 49 89 32004 300
Eml.: ker@ grs.de

♠SEIDEL Freddy
Federal Office for Radiation Protection (BfS)
P.O. Box 100149
D-38201 Salzgitter

Tel.: +49 5341 885 863
Fax: +49 5341 885 865
Eml.:fseidel@bfs.de

HUNGARY

HAMAR, Karoly
Nuclear Safety Inspectorate, I & C Sec.
Hungarian Atomic Energy Comm.
Nuclear Safety Inspectorate
P.O. Box 676
H-1539 BUDAPEST 114

Tel: +36 1356 5566-2221
Fax: +36 1355 1591
Eml: hamar@haea.gov.h

JAPAN

♠OGISO, Zen-ichi
Manager, Nuclear Power
Engineering Corp. (NUPEC)
Fujitakanko Toranomon Bldg.
17-1, 3-chome, Toranomon
Minato-ku, Tokyo 105

Tel: +81 3 3435 3427
Fax: +81 3 3435 3428
Eml: ogiso@nupec.or.jp

♠MAKINO Shigenori
Tokyo Electric Power Company
1-3 Uchisaiwai-cho
1-chome Chiyoda-ku
Tokyo 100-0011

Tel.: +81 3 3501 8111
Fax: +81 3 3596 8562
Eml.: Makino.S@tepco.co.jp

♠MITO Yoichi
The Kansai Electric Power Co. Inc.
Nuclear Power Division
3-3-22, Nakanoshima Kita-ku
OSAKA 530-8270

Tel.: +81-70-5938-2709
Fax: +81-6-6444-6279
Eml: K576277@kepco.co.jp

♠UTSUMI Utsumi,
Mitsubishi Heavy Industries Ltd
Nuclear Energy Systems Engineering Center
1-1-1, Wadasaki Hyogo-ku
KOBE 652-8585
Tel.: +81-78-672-3305
Fax: +81-78-672-3268
Eml: utsumi@atom.hq.mhi.co.jp

♠MIYAUCHI Katsumi
Design Section Nuclear Power Department
Hokkaido Electric Power Co.,Inc.
Higashi 1-Chome , Ohdori
Chuo-ku , Sapporo , 060-8677
Tel.: 81-11-251-1111
Fax: 81-11-218-5786
Eml: H1998088@epmail.hepco.co.jp

♠YAMAGISHI Hitoshi
Design Section Nuclear Power Department
Hokkaido Electric Power Co.,Inc.
Higashi 1-Chome , Ohdori
Chuo-ku , Sapporo , 060-8677
Tel.: 81-11-251-1111
Fax: 81-11-218-5786
Eml: hitoshi-y@epmail.hepco.co.jp

♠FUJII Sumio
Design Section Nuclear Power Department
Hokkaido Electric Power Co.,Inc.
Higashi 1-Chome , Ohdori
Chuo-ku , Sapporo , 060-8677
Tel.: 81-11-251-1111
Fax: 81-11-218-5786
Eml: s-fujii@epmail.hepco.co.jp

KOREA (REPUBLIC OF)

YUN H. CHUNG
Korea Institute Of Nuclear Safety
19 Guseong-Dong Yusung-Gu
Taejon, 305-338
Tel: +82 42 868 0245
Fax: +82 42 861 9945
Eml.:yhchung@kins.re.kr

D. I. KIM
Korea Institute Of Nuclear Safety
19 Guseong-Dong Yusung-Gu
Taejon, 305-338
Tel: +82 42 868 0246
Fax: +82 42 861 1700
Eml.: dikim@kins.re.kr

♠TAEYONG SUNG
Integrated Safety Assessment Team
Korea Atomic Energy Research Institute
P.O. Box 105 Yusung, Taejon, 305-600
Tel.: 82-42-868-8923
Fax : 82-42-868-8256
Eml.: tysung@kaeri.re.kr

SLOVAK REPUBLIC

♠SÚKENÍK Peter
Nuclear Power Plant Bohunice
919 31 Jaslovské Bohunice
Tel.:+421 33 597 2808
Fax:+421 33 597 4720
Eml.:sukenik_peter@ebo.seas.sk

♠BÁNOVCOVÁ Mária
Nuclear Power Plant Bohunice
919 31 Jaslovské Bohunice
Tel.:+421 33 597 2356
Fax:+421 33 597 4720
Eml.:banovcova_maria@ebo.seas.sk

♠LIBOSVAR Kamil
Nuclear Power Plant Bohunice
919 31 Jaslovské Bohunice
Tel.:+421 33 597 2356
Fax:+421 33 597 4720
Eml.:libosvar_kamil@ebo.seas.sk

♠ARBET Ladislav
Nuclear Power Plant Research Institute
Okru ná 5 Eml.:arbet@vuje.sk
918 46 Trnava
Tel.:+421 33 599 1726
Fax:+421 33 599 1153

♠GESE Augustín
Nuclear Power Plant Research Institute
Okru ná 5
918 46 Trnava
Tel.:+421 33 599 1105
Fax:+421 33 599 1153
Eml.:gese@vuje.sk

SLOVENIA

♠ Pecek Vladimir
Nuclear Regulatory Authority
Vojkova 59
1000 Ljubljana
Tel.: (+386) 1 472 11 42
Fax : (+386) 1 472 11 99
Eml: vladimir.pecek@gov.si

SWEDEN

LIWÅNG, Bo
Deputy Head
Dept. of Plant Safety Assessment
Swedish Nuclear Power Inspectorate
S-106 58 STOCKHOLM
Tel: +46 (0)8 698 84 92
Fax: +46 (0)8 661 90 86
Eml: bo.liwang@ski.se

♠ANDERSSON Jan-Ove
IoC, research and Development
Barsebäack Kraft AB
Box 524
SE-246 25 Löddeköpinge
Tel.: +44 46 72 41 48
Fax: +46 46 72 46 93
Eml.:jan-ove.andersson@ barsebackkraft.se

♠JONSSON Nils
Engineering department
Barsebäack Kraft AB
Box 524
SE-246 25 Löddeköpinge
Tel.: +44 46 72 40 00
Fax: +46 46 77 48 58
Eml.:nils.jonsson@barsebackkraft.se

♠ERIKSSON Karl-Erik
OKG Aktiebolag
Oskarsham NPP
SE-572 83 Oskarsham

Tel.: +46 491 78 76 82
Fax: +46 491 78 68 65
Eml.:karl-erik.eriksson@okg.synkraft.se

SWITZERLAND

REDDERSEN Hans-Georg
Colenco Power Engineering
Mellingerstrasse 207
CH-5405, Baden

Tel.: +41 56 483 1563
Fax: +41 56 493 7356
Eml.:hans-georg.reddersen@colenco.ch

UKRAINE

♠ YASTREBENETSKY Michael
State Scientific and Technical Center
on Nuclear and Radiation Safety
17 Artema str.
Kharkov 6100

Tel.: +38 0572 471 700
Fax: +38 0572 471 700
Eml.: rel@online.kharkiv.com

♠ KHARCHENKO V.
State Scientific and Technical Center
on Nuclear and Radiation Safety
17 Artema str.
Kharkov 6100

Tel.: +38 0572 471 700
Fax: +38 0572 471 700
Eml.: rel@online.kharkiv.com

UNITED STATES OF AMERICA

♠CHIRAMAL, Matthew
Senior Advisor for Digital Technology
Office of Nuclear Reactor Regulation
US Nuclear Regulatory Commission
M.S. 0-11D 19
20555 Washington DC

Tel.: +1 301 415 2845
Fax: +1 301 415 2444
Eml: mxc@nrc.gov

DURYEA John Luis
Westinghouse Electric Co.
Nuclear Automation,
P.O. Box 355, Pittsburg PA 15230

Tel.: +420 334 77 34 46
Fax:+420 334 77 34 49
Eml.: Duryeljl@notes.westinghouse.com

International Organisations

OECD/Halden Reactor Project, Institutt for Energiteknikk, Halden

♠DAHLL Gustav
Institut for Energiteknik
OECD - Halden Reactor Project
Os alle 13, P.O. Box 173
N - 1751 Halden

Tel: +47 69 21 22 00
Fax: +47 69 21 24 40
E-mail: dahll@hrp.no

OECD/Nuclear Energy Agency

♠HREHOR Miroslav
Nuclear Safety Division
12, boulvard des Iles
92 130 Issy-les-Moulineaux
France

Tel: +33 1 45 24 10 58
Fax:+33 1 45 24 11 10
Eml:miroslav.hrehor@oecd.org