Nuclear Regulation
NEA/CNRA/R(2008)6
July 2008

Inspection of Digital I&C Systems – Methods and Approaches

Proceedings of a CNRA Workshop
Garching, Germany
24-26 September 2007

OECD Nuclear Energy Agency
Le Seine Saint-Germain - 12, boulevard des Îles
F-92130 Issy-les-Moulineaux, France
Tél. +33 (0)1 45 24 82 00 - Fax +33 (0)1 45 24 11 10
Internet: http://www.nea.fr

N U C L E A R • E N E R G Y • A G E N C Y

Unclassified **NEA/CNRA/R(2008)6**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development **01-Aug-2008**

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES

NEA/CNRA/R(2008)6
Unclassified

PROCEEDINGS OF THE CNRA WORKSHOP ON INSPECTION OF DIGITAL I&C SYTEMS - METHODS AND APPROACHES

Garching, Germany, 24-26 September 2007

JT03249400

English text only

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 (14 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 28 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, Slovak Republic, 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 NUCLEAR REGULATORY ACTIVITIES

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

The committee is responsible for the programme of the NEA, concerning the regulation, licensing and inspection of nuclear installations with regard to safety. The committee's purpose is to promote cooperation among member countries to feedback the experience to safety improving measures, enhance efficiency and effectiveness in the regulatory process and to maintain adequate infrastructure and competence in the nuclear safety field. The CNRA's main tasks are to review developments which could affect regulatory requirements with the objective of providing members with an understanding of the motivation for new regulatory requirements under consideration and an opportunity to offer suggestions that might improve them or avoid disparities among member countries. In particular, the committee reviews current management strategies and safety management practices and operating experiences at nuclear facilities with a view to disseminating lessons learned.

The committee focuses primarily on existing power reactors and other nuclear installations; it may also consider the regulatory implications of new designs of power reactors and other types of nuclear installations.

In implementing its programme, the CNRA establishes cooperative mechanisms with the Committee on the Safety of Nuclear Installations (CSNI) responsible for the programme of the Agency concerning the technical aspects of the design, construction and operation of nuclear installations. The committee also co-operates with NEA's Committee on Radiation Protection and Public Health (CRPPH) and NEA's Radioactive Waste Management Committee (RWMC) on matters of common interest.

WORKING GROUP ON INSPECTION PRACTICES

The NEA Committee on Nuclear Regulatory Activities (CNRA) believes that an essential factor in ensuring the safety of nuclear installations is the continuing exchange and analysis of technical information and data. To facilitate this exchange the Committee has established Working Groups and Groups of Experts in specialised topics. The Working Group on Inspection Practices (WGIP) was formed in 1990 with the mandate "... to concentrate on the conduct of inspections and how the effectiveness of inspections could be evaluated...".

FOREWORD

CNRA held several workshops in 1996 and 2001 on the licensing of Digital I&C Systems and a Joint CSNI/CNRA Task Group presented a study on research and regulatory needs in this are in 2006. This workshop is part of the ongoing work in this topic by WGIP relating to inspection practices for digital I&C systems. The objective of the workshop was to bring together I&C experts and regulatory inspectors to:

- Review current regulatory practices and experiences with licensing Digital I&C systems;
- Enhance the dialogue between I&C experts, licensees and regulatory inspectors; and
- Develop commendable practices for inspecting Digital I&C safety systems.

Members of Organising Committee wish to acknowledge the excellent planning and arrangements made by the staff of the hosting organisation Institute of Safety Technology (ISTec), Garching and AREVA NP GmbH, Erlangen. In particular the group wishes to thank Mr. Freddy Seidel, Dr. Hartmut Klonk of BfS and the members of the ISTec Staff who assisted in the arrangements.

Special acknowledgement is given to the WGIP task leader, Mr. Benoit Zerger, ASN, France and the other members of the WGIP Task Group.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Working Group on Inspection Practices (WGIP) organised the workshop which was attended by approximately 50 participants from nuclear regulatory bodies, technical support organizations and licensees in 18 countries plus the NEA. It included both specialists in Digital I&C and generalist inspectors, whose attendance was facilitated by the working group. The workshop comprised structured discussion sessions, in which a set of issues were explored by small discussion groups and then discussed in plenary, complemented by short presentations on national issues.

1. INTRODUCTION

Based on a proposal from the CNRA, WGIP started a task on the inspection of Digital I&C in 2006. The task was set-up to compile information on the development of inspection programmes by the member countries. Based on the results of a survey it was agreed that in order to obtain a better understanding it would be necessary for inspectors and experts to meet and discuss the current state-of-the-art. The workshop and these proceedings were the results of this task group.

2. BACKGROUND

The major issue surrounding the use of Digital I&C in nuclear safety protection systems relates to the introduction of computer software into the process. This includes a range of systems from the introduction of large platform computer systems through microprocessor control systems down to embedded software in primary instrumentation and controllers.

The main concern is that protection systems are required to have high and predictable levels of reliability. Software based systems are prone to be unreliable and our capability to detect this is poor.

With an analogue system, its characteristic is both determinable and reproducible. Once this is determined by test, it will perform in a consistent repeatable way. Periodic checks can be designed which will then allow the periodical calibration of the system. This will ensure that the system will operate within acceptable reliability limits.

Because software systems generate their operating characteristics from a series of discrete logic steps, the situation is far more complex and complicated. Greater number of inputs and algorithm complexity further complicate the situation. Every line of code would have to be tested for every combination of inputs at all conceived rates of change to actually determine the system reliability. It borders on the impossible as the combinations are infinite.

The Digital I&C community therefore adopted an approach based on rules for improved design of software, designed to minimise the consequences of this problem. It should be noted that a number of countries have restricted the use of this equipment to not being used on nuclear safety protection systems.

In more recent times, the use of software in primary instrumentation and controllers is significantly increasing. Here the customer can be left with no knowledge of the complexity of software included. This is an area of increasing challenge.

3. STRUCTURE OF WORKSHOP

The workshop was hosted by the Institute for Safety Technology (ISTec) in Garching, Germany. It comprised two key elements:

- Short presentations on national regulatory positions or technical support organizations works. The individual presentations were the view of the source body and WGIP has neither interfered with these views nor commented on them.
- Structured discussion sessions, in which a set of issues that had been identified by WGIP in an earlier survey were addressed by small discussion groups and then presented and further discussed in plenary.

3.1 Day One

The day started with a plenary paper by Arndt Lindner from ISTec entitled 'Why and how software fails'.

Regulatory position papers were presented by Japan, Germany and Canada, covering the different experience in inspecting the Digital I&C systems.

The remainder of the day was devoted to three working group discussions about the main points of interests which were raised through the survey, e.g.:

- Operating experience involving Digital I&C.
- How to inspect software embedded systems and purpose built designs?
- How to inspect software modifications?

The main points from the discussion were reported back to the main meeting by the working group chairmen. This was followed by a plenary discussion.

3.2 Day Two

The day started with a presentation of Mr. Lindner from ISTec on the NEA Computer Based Systems Important to Safety (COMPSIS) data base. This was followed by regulatory position papers from Czech Republic, Korea and Germany.

The plenary session was followed by another discussion in two sets of two working groups. The first set dealt with the normal operation inspection and the second set with the inspection of software modifications. Each group considered the following points:

- Examples of operating experience involving software;
- What knowledge is needed to inspect Digital I&C?

- What has to be inspected?
- With which tools?
- With what training?

Following the format of day one, the four groups fed back to the main meeting, and there was a plenary discussion.

3.3 Day Three

The third day was dedicated to a technical visit on the AREVA NP GmbH Digital I&C test field. The attendees visited both the TELEPERM XS test field and the Digital I&C forum where the control rod digital pilot was presented.

4. SUMMARY OF DISCUSSIONS

This section provides a summary of the plenary papers and the working group sessions. Additional information, including presentation materials and regulatory position papers is contained in the NEA WGIP Web Site.

4.1 Opening Presentations

The WGIP Chairman, Mr Steve Lewis from NII, UK gave an opening address to set the context for the workshop. The objectives and background to the workshop were explained by the Workshop Chair and NEA.

Mr Benoit Zerger, ASN, France presented a plenary paper on the WGIP Survey results. The paper discussed the main results of the WGIP surveys about Digital I&C. The key points are:

- All countries use Digital I&C in systems important for safety but in various extend (on almost all systems important for safety in some facilities).
- The validation of the reliability of software systems by the regulator is very variable.
- The embedded software equipment is used in all the countries but only a few countries have requirements about it.
- Half of the countries have faced events due to modification of Digital I&C system.

4.2 Plenary Sessions

A summary of the plenary presentations and discussions is provided below.

***Why and How Software Fails**, Arndt Lindner, ISTec Germany*

It's a matter of common knowledge that software often fails randomly - although faults in software are systematic faults. Nevertheless, discussions about common cause failures due to software are an actual issue of digital systems. Conditions and triggers are discussed which result in software failures.

Through examples the presentation shows how software design, qualification and architecture cope with the challenges of digital technology. Due to the application of software based electrical and electronic systems comprehensive measures for self-diagnostics and early failure detection have been integrated in these equipment.

The presentation will explain some of the fundamental characteristics from an analytical point of view.

Consideration of Inspection of Digital Safety Systems in Japan, *Hideo Matsuno, JNES, Japan*

Digital safety systems were applied to several nuclear power plants in Japan, and will be applied to many plants in the near future including replacement of the analogue systems. The digital system has several advantages such as no signal drift in digital parts, software does not degrade, diagnostic capability etc. By the way, periodic test of the digital system in nuclear power plants are performed same as analogue system. Therefore, it is desired to rearrange the contents of periodic test rationally utilizing above advantages of the digital system. I introduce the consideration of the periodic test of the digital safety systems in nuclear power plants. For example, three type of periodic test were performed in nuclear power plant such as surveillance, periodic inspection and periodic test. In the surveillance, confirmation of input output characteristics, set value, connection of wire terminal, and cleaning of cabinet are performed. Furthermore, the software integrity is confirmed by comparing with the master software. In the periodic inspection, confirmation of set value by artificial input signal and conformation of logic function. In the periodic test, the safety components are initiated by manual switch or artificial input signal and confirmed the actions of the component and related equipment. In these tests, accuracy confirmation of instrument loop and confirmation of set value for trip signal actuation function are performed in the surveillance and the periodic inspection respectively. And the software integrity is confirmed in the surveillance, then confirmation of set value and logic function is not necessary in other tests. We have several areas in which the contents of test would be rearranged rationally. The consideration of these tests are performed by JNES which is a technical assistance organization of regulatory body, and the result will be agreed with regulatory body and will be made recommendation that will be described in proper technical standard.

How Digital I&C Systems Change Aspects of Traditional Periodic Technical Inspections at Nuclear Power Plants, *Ferdinand J. Dafelmair, TÜV SÜD Industrie Service GmbH, Germany*

Periodic on-site inspection of I&C systems at nuclear power plants is a task TÜV experts have a long experience with. The basic idea of these inspections is to verify, that the systems in operation are maintained in a good condition. Successful procedures have been developed to accomplish this for classical I&C installations of electrical and electronic systems. For complex Digital I&C systems with microprocessors or highly integrated electronic circuits however, the classical procedures need to be changed to remain effective. Through a couple of practical examples the presentation shows, what challenges the inspectors face at a plant with modern Digital I&C systems in order to gain confidence that the systems are working correctly. Furthermore it shows methodologies suitable to assist the inspectors to identify equipment, its change history and its current functional state such that they can conclude the inspection with the profound statement that everything still is what it has to be.

CNSC's Experience in Reviewing Digital I&C Systems, *Richard Lawson, Athur Faya, CNSC, Canada*

This presentation summarizes CNSC's experience in reviewing Digital I&C systems including lessons learned from a regulatory perspective. As an example we describe our review of Darlington trip computer software re-design which took place in the 1990's. Our regulatory review focuses on four essential elements: software requirements, process and people, systematic inspection and testing. We review the human factors program in detail to ensure that the functional changes to the software adequately supported human performance and hence I&C system overall performance. Inspection techniques should build on the review methodology used during the software development process.

Regulatory activities related to the NPP Temelin Digital I&C System, Zdeněk Tipek, Miroslav Lehmann, SUJB, Czech Republic

Content:

- Short overview of Temelin NPP I&C
- Regulatory approach to licensing and inspections
- Operational experience with digital I&C
- Regulatory approach to Digital I&C design changes

Licensing Experience of the Surveillance Testing of Digital I&C System*, Seonghyon, Ji; Hyun-shin, Park; Dr. Dai. I, Kim; KINS, Korea*

The migration from the analogue systems to the digital systems is significantly increasing in I&C field of Nuclear Power Plants. This trend applies not only to the new plants being constructed but to the operating plants for the upgrades. But since the code and standards for the safety I&C systems have been developed for the analogue systems, they do not completely incorporate the characteristics of digital systems. This paper presents the periodic surveillance testing for the newly installed digital plant protection system at Ulchin 5&6. After the installation and commissioning of the digital plant protection system, the licensee found that the periodic surveillance test for that system took too much time. It means that the time needed for the surveillance test of the digital plant protection system takes about 5 times longer than that of the analogue plant protection system. This is resulted from the direct application of the existing code and standards to the new Digital I&C system that has more complex features than analogue systems. There were a lot of discussions between the regulator and the licensee about the surveillance test during the licensing process. At that time, the decision was made conservatively considering that the digital system was the very first application for the reactor protection system in Korea. In this paper, we will discuss the safety classification of testing equipment that is attached to the digital system and the possibility of utilization of digital system features in the surveillance test. Finally, licensing experience of revising the technical specification regarding the surveillance testing of digital system will be presented.

Progress in the Inspection of Digital Instrumentation and Control Systems Important to Safety*, Günter Glöe, TÜV NORD SEECERT, Germany*

By research and development effort together with the OECD Halden Reactor Project in Norway, Institute for Safety Technology in Germany, Technical University Berlin in Germany and Technical University Munich in Germany progress has been achieved in depth, in efficiency, in reproducibility and with new methods for the Inspection of Digital Instrumentation and Control Systems Important to Safety. Most part of the effort has been funded by the German ministry for economics and work (BMWA) as project 1501282.

Four of the six work packages have been dedicated to the improvement of depth, efficiency and reproducibility of the inspection. The work has been together with OECD Halden Reactor Project as well as Institute for Safety Technology. These packages have been about:

- Capturing the requirements on Digital Instrumentation and Control Systems from standards in such a way that compliance of a system under test with the requirements may be shown in a well documented and such in an auditable way. For this purpose short forms of the requirements may be selected according to the lifecycle phase (e.g. detailed design or coding) or work product (e.g. user's manual) of interest. A link to the original standard clauses is available. The short

forms of the selected requirements may be exported into checklists for use with the developer or the assessor. A tool prototype implementing this approach is available.

- Judging about the compliance of a Control System with a given standard based on test results is a bit arbitrary until now in a lot of cases. Based on earlier projects, an approach (algorithm) has been defined which allows judgement about compliance in a pure automatic manner. The approach has been applied in several real work applications. In all of these cases the automatic judgements conforms to those by senior experts. A tool prototype implementing this approach is available.

- Besides the tools for requirements capturing from standards and those for compliance judgement mentioned above a lot of measurement tools for the verification of Digital Instrumentation and Control Systems Important to Safety are available by the partners as well as commercially. An approach has been developed which starts again from the requirements imposed on Digital Instrumentation and Control Systems e.g. by standards. To a code related subset of these requirements we have assigned those characteristics which would allow deciding about the compliance of a Control System with the requirements. Furthermore we have assigned to each of the characteristics at least one tool capable to measure it. By this we can select now a requirement of our concern and run automatically - that means in a well documented, reproducible and efficient way - the respective measurements as well as the compliance judgement. A tool prototype implementing this approach is available.

- The fourth package is about the possibility to qualify the Software of Digital Instrumentation and Control Systems in spite of missing work products as detailed design or test reports. We try to substitute the missing information by results of static code analysis.

The further two work packages are about new methods for the Inspection of Digital Instrumentation and Control Systems Important to Safety. The work has been together with Technical University Berlin and Technical University Munich. These packages have been about:

- Configuration management;

- Possibilities to create user's manuals consistent with the software Control Systems from Unified Modelling Language (UML) presentations of the software.

Survey of Technical Requirements for Maintenance and Modification of software-based I&C Systems Important to Safety*, F. Seidel, BfS, Germany*

Recently some of the main standards of the International Electrotechnical Commission relevant to software-based I&C systems like IEC 60880, IEC 61513, and IEC 62138 as well as the common positions of the West European Nuclear Regulators Association Task Force on Safety Critical Software (formerly under the umbrella of the European Nuclear Regulators' Working Group) have been established or revised respectively.

These documents have been surveyed particularly taking into account the contained requirements for maintenance and modification of software-based I&C systems during plant operation. Aspects like completeness and applicability of these requirements, as well as maintaining safety properties of the system over the whole life cycle which had been proven during installation and licensing received special attention.

Supplementary requirements are proposed in the national regulatory frame.

Main Risk Contributors of Digitalized Safety-critical Systems from the Viewpoint of PRA, *Hyun Gook Kang, Seung-Cheol Jang, KAERI, Korea*

Safety assessment for digitalized safety-critical systems such as plant protection system and engineered safety feature control system was performed. Fault-tree models were developed to assess the failure probability of a system function which is to generate the automated reactor trip signal and the control signals for complicated accident-mitigation equipment. Since the operator is expected to play actively the role of a backup for these automated system, we also considered the failure of human operators.

The developed fault trees were combined with a plant risk model to evaluate the effect of the digitalized systems' failure on the plant risk. We used Korean Standard Plant (PWR) plant model and newly designed digital safety-critical systems' models. Final integrated model consists of about 2176 basic events and 5464 logical gates.

Based on the cutset analysis result, we found that the digitalized safety-critical I&C system failures contribute about 6% to 10% to the core damage frequency of a nuclear power plant. The quantification results also reveal dominant contributors for system unavailability. We will address the effects of these factors quantitatively and discuss the findings. We will also address effects of some design issues of digital systems such as redundancy of signal paths.

4.3 Working Group Sessions

4.3.1. Operating experience

According to COMPSIS (NEA Data Base Project on Computerised Systems Important to Safety) failures database, 70 % of the failures are from the requirements, 5% from coding and 25% from maintenance and changes.

The working groups gave some operating experience examples:

- Smaller scale components (with embedded software) lead to errors since configuration management is improperly maintained (staff unaware of internal function).

- Graph Platform vs. Application Software: Changes to the platform may create failures due to application out of boundary.

- At Ringhals 2 PWR in Sweden the licensee made an analogue to digital change to equipment used to provide overcurrent protection to many safety related circuit breakers. The design basis of the system was to isolate the safety related equipment at surge currents of 120% of design surge equipment. This was not a safety related change and accordingly was not reviewed by the licensing authority, although they were notified. This modification appears to have been done properly with adequate post modification.

A subsequent "minor change" to the embedded software module was made changing the "sampling frequency." The change was in place for some time until the licensee swapped trains of an operating pump and all the affected breakers tripped. The trip occurred 60-70% of surge current in lieu of the

120% design. Acceptance testing of the "minor change" was performed to ensure that trips occurred at 120%, but there was no testing done to determine what would occur at lower current levels.

- Unqualified Inter-connection of a personal computer used for training purposes on a fuel handling machine. Special data values used for training; left unintentionally after training session completed, and after disconnection of the PC, treated as default values.

- The results of the event assessment were that the modification process was not applied properly when training mode was designed, that the interface was not qualified and that the change of the procedure was managed in an improper way.

- Small LOCA due to refuel machine malfunction after a software modification, due to inadequate V&V.

- Software test of a safety system modification performed concurrently with a related non-safety system test, which resulted in a system interaction that was not identified. This condition would have resulted in a system failure. The main causes were inadequate communications between two test teams.

- Control room display disabled by a software virus induced through the connection of the system to the corporate computer network.

- EMF from a digital camera caused a spurious actuation of a digital fire control system. The pictures were intended for pre work planning.

- Spurious trips of the RPS system due to an original software design issue, which were only apparent at low power operations and due to inadequate V&V.

4.3.2. Use of off-the shelf software?

The attendees deemed that off-the-shelf software mustn't be a black box for safety significant systems or uses. This black box shall be transformed into "grey box" through appropriation of code (e.g. documentation, Quality Assurance) and on a case by case basis.

The off-the-shelf software shall be pre-qualified by the vendor, approved by an independent assessor, through testing to a safety standard.

There was also a discussion about replacement of small analogue pieces of instrumentation by digital ones with respect to:

- Diversity necessity;

- Thorough licensing necessity.

Additional aspects were discussed: When off-the shelf software is modified to fulfil specific requirements, is it still off-the shelf software? Where is the border between configuration and modification?

4.3.3. General considerations about design and upgrading

Some attendees think that the regulators should develop software design requirements that include inspectability and testability of the software. These requirements should also concern documentation and change process.

There were also discussions about the separation of diagnostic and core functions of the software.

Some regulators take into account IEC standards and / or standards from the vendor country (especially for IEEE) but some participants of the working groups feel that national amendments are necessary.

4.3.4. What to inspect?

The main goals of an inspection about Digital I&C could be:

- Identify unauthorized or unintentional modifications (vendors, maintenance personnel, unqualified personnel);
- Identify configuration management issues (inadequate evaluations for modifications...);
- Identify the addition of new programmable digital equipment;
- Identify new security issues (new external connections to site computer systems or system interconnections);
- Identify Test performance non-conformances (verify procedure compliance);
- Identify that test procedures address the current configuration;
- Identify the adequacy of test procedures (specialist Inspector);
- Evaluate corrective actions for test failures;
- Maintain awareness of plant trends;
- Identify system errors through the review of system logs/local indicators;
- Verify equipment environmental conditions remain as designed (temp, humidity, EMF).

To achieve these goals, inspections should be carried out on:

- Procedures maintenance;
- Test results;
- Supplemented documentation;
- Technical specification requirements;
- The utility improvement profile;

- Training of the plant personal;
- Lessons learned from the experience in the plants;
- Maintenance work orders;
- Engineering design change packages;
- Procurement documents/receipt process/component qualification process ;
- Interactions with plant staff (system engineers, operations, maintenance);
- Plant process for general network control (security) and modifications;
- Logs, reports, indicator light status;
- Problem identification reports and corrective actions.

4.3.5. What knowledge?

There was no consensus within the working groups about the knowledge needed to carry out inspections about Digital I&C.

Some people thought inspectors need the same level of knowledge for Digital I&C as for other systems, but others thought that Digital I&C inspection requires more specific knowledge.

Anyway, it was agreed that inspectors need sufficient knowledge to ask intelligent questions, i.e. they must have basic software vocabulary. They also need to know that a change occurred and that this change is a modification, not maintenance.

Some knowledge that non-specialist inspectors could have is about:

- General plant awareness – general walkdowns (identification of new I&C equipment, environmental changes, changes in IT systems…);
- Regulatory body change management process;
- I&C Basics, Workshops; RPS, specific systems, plant and reactor behaviour simulation (special demo; simplified version than reactor operators training;
- Knowledge of software lifecycle;
- Connections to equipment, independence, isolation principles;
- Fundamentals of signal transfer (independence of signals);
- Failure and degradation mechanisms: i.e. electromagnetic interference;
- Main functionality of I&C, but no specific internal functions;
- Awareness of Digital I&C market availability; test equipment;

- Commercial I&C systems;
- Design principles: alternative means to reach safety goal, redundancy, diversity of functions;
- Software V&V principles and practices;
- Strong change management processes in plant;
- QA process for I&C;
- Typical commissioning tests: nature and content;
- Knowledge of I&C related regulations, standards & rules, practices;
- Engineering concepts of safety instrumented system (failure modes) (general, branch independent);
- Knowledge of specialized software tools used by the utility.

4.3.6. What training?

Inspectors should be trained to gain the knowledge that is described above. This training could be done through:

- On-the-job training with specialist inspectors or assessors;
- Self study of documentation, regulatory body and licensees processes;
- Classroom, workshops, simulator based;
- Interview techniques;
- Participation on factory testing;
- Feedback from operators;
- WGIP workshops;
- Operational Experience review;
- Knowledge transfer, part of knowledge management.

4.3.7. Which tools?

The working groups made a list of the tools which could be used to carry out an inspection about Digital I&C:

- Lifecycle management indications;
- Black box on location, connected, identified (tagged), environmentally sound;

- Status in the field of equipment (test mode left on?);
- Licensing assumptions on equipment;
- Interview of licensee system specialist;
- Procedure manual update availability (not content);
- Availability of documentation by vendor (redlined documentation could be useful);
- QA documentation updated (including engineering drawings, flowsheets);
- FSAR main assumptions for specific components as requested by assessor;
- Input-output validation;
- Sampling the testing and maintenance records and results;
- Configuration management application to specific cases;
- Indicators of modifications (Work orders, Security devices, Laptops on the field, Site purchasing process Physical changes in plant;
- Configuration identification document;
- Ability to validate electronic document integrity (digital signatures…);
- Performance indicators (Logs, History reports…);

Several groups agreed that regulators should have inspection guidance developed by specialists.

5. CONCLUSIONS

This section summarises the main conclusions from the workshop and feedback provided by participants about the value and organisation of the workshop.

Generally speaking, this workshop allowed a very fruitful experience exchange between the different countries and mutual discussions between regulators, TSO experts and licensees.

5.1 Key Conclusions

1. A complete change from analogue to Digital I&C will take place in the foreseeable future due to loss of suppliers and knowledge in the field of analogue I&C. Therefore the system of inspections has to be adapted to Digital I&C in a timely manner.

2. Digital I&C does not require a revolution of the system of inspections. Inspections of Digital I&C can be incorporated in the existing national system.

3. Persisting operating experience shows that maintenance of software-based system and software modification have been contributing to operating experience significantly. Therefore inspectors and their technical support organisations should be aware of the specific failure modes of this equipment and consider the various options of the new technology for testing and analysis.

4. Additional training for inspectors is required and should focus on aspects of Digital I&C which are different from analogue I&C. Basic knowledge and knowledge especially required for performing inspections of Digital I&C should be included.

5. Licensees and inspectors should have some knowledge about the way commercial software operates. “Grey box”, no black box.

6. RECOMMENDATIONS

Because of the very innovative nature of the Digital I&C, a follow-up workshop could have a great value and topics to address could be hardware maintenance and software modification.

7. WORKSHOP DOCUMENTS

The workshop documents have been compiled and placed on the NEA Web Site at the following address:

http://www.nea.fr/html/nsd/cnra/wgip.html