MULTINATIONAL DESIGN EVALUATION PROGRAMME

2010 ANNUAL REPORT

June 2011

NUCLEAR ENERGY AGENCY

Table of contents

Appendices

FOREWORD FROM THE POLICY GROUP CHAIRMAN

Paris, 10 May 2011

I wrote this foreword in a very particular context: our Japanese counterparts were facing a dramatic situation, a toll of death and destruction. Furthermore, this powerful natural disaster has a severe impact on the Japanese nuclear power plants (NPPs), in particular on Fukushima Daiichi and Daini sites.

These tragic accidents that occurred in Japan raised many questions and issues concerning both operating and new NPPs and these issues need to be addressed both nationally and internationally. And more than ever, Safety Authorities tasked with regulating operating and new NPPs have to coordinate their efforts and to exchange information on their methodologies and findings.

The MDEP remains a unique 10-nation initiative being undertaken by regulators from Canada, China, Finland, France, Japan, Republic of Korea, the Russian Federation, South Africa, the United Kingdom and the United States with the purposes of cooperating on new reactor safety reviews and of harmonizing regulatory practices and requirements.

Events such as floods, earthquakes, loss of electrical supply and ultimate heat sink have been considered in the on-going new reactor design reviews and have already been partially discussed within some MDEP working groups. In the light of recent developments, efforts will be made in the short and medium terms by MDEP in order to continue the coordination of our national efforts with a specific focus to be considered on lessons learnt from the Japanese accidents.

In 2010, MDEP commenced the formalization of its outcomes, a direct consequence of the pertinent guidance given by the MDEP Steering Technical Committee (STC) to the MDEP Working Groups to carry out their activities according to their Programme Plans, already mentioned in the last MDEP annual report.

One major type of product finalized in early 2011 and released on the MDEP public website (www.oecd-nea.org/mdep) is generic and design-specific Common Positions. According to the methodology defined by the STC, the MDEP Digital Instrumentation and Controls Working Group (DICWG) worked on three draft Generic Common Positions, the EPRWG worked on a Specific Common Position (DSCP) on Digital I&C issues and the AP1000WG worked on a DSCP specifying technical guidance for squib valves.

By sharing such documents according to the conclusions of the 2009 MDEP conference, MDEP improved communications to its stakeholders.

MDEP also increased its interactions with nuclear industry at different levels. MDEP working groups directly interacted with vendors and/or Standard Development Organizations (SDOs). The MDEP Policy Group also met with the Cooperation in Reactor Design Evaluation and Licensing working group (CORDEL) of the WNA in order to discuss the Industry initiatives aiming at harmonization, in particular in the area of Codes and Standards.

In 2010, MDEP also worked on the enhancement of MDEP membership, this decision being also a direct consequence of the 2009 MDEP conference. Based on the MDEP Terms of Reference (ToR), the new criteria for membership make a clear distinction between MDEP members and associate members, and adds a new concept of MDEP candidates, to take into account the interest of experienced regulators not yet having closed their plans for new reactors, but who could benefit from specific MDEP activities. In order to fully implement these enlargement criteria, MDEP also revised its ToR for consistency.

In 2011, MDEP will strive to maintain its high-level expertise exchange forum in a context creating two major challenges: additional national and international efforts expected with regards to the Japanese on-going situation and the MDEP membership enlargement. Both challenges will be addressed at the next Policy Group meeting scheduled in June 2011.

MDEP will organize a second Conference on New Reactor Design Activities on 15-16 September 2011 in Paris. As with the first such event, the main objectives of this conference will be to share and discuss MDEP results and outcomes with our stakeholders and of course, to improve our work by including in our Programme of work the main findings of this conference.

André-Claude LACOSTE
MDEP Policy Group Chairman

March 2010 – MDEP Policy Group meeting

EXECUTIVE SUMMARY

The Multinational Design Evaluation Programme (MDEP) is a multinational initiative to develop innovative approaches to leverage the resources and knowledge of national regulatory authorities who are, or will shortly be, undertaking the review of new reactor power plant designs. Current MDEP members are: Canada, China, Finland, France, Japan, Korea, Russian Federation, South Africa, the United Kingdom and the United States. In addition the IAEA takes part in the work of MDEP. The OECD Nuclear Energy Agency (NEA) performs the Technical Secretariat function in support of MDEP. In January 2011, new levels of membership, as well as specific membership criteria, were established for MDEP. The new membership levels include associate membership for design specific activities only, and candidate, for countries with mid-to-long term plans to pursue new reactor licensing. MDEP incorporates a broad range of activities including enhancing multilateral cooperation within existing regulatory frameworks, and increasing multinational convergence of codes, standards, guides, and safety goals. A key concept throughout the work of MDEP is that national regulators retain sovereign authority for all licensing and regulatory decisions.

The programme of work consists of activities which were chosen because they could be accomplished in the near term, and would result in significant benefits while requiring minimum resources. Working groups are implementing the activities in accordance with programme plans with specific activities and goals, and have established the necessary interfaces both within and outside of the MDEP members. This report provides a status of the programme after its third year of implementation.

Significant progress is being made on the overall MDEP goals of increased cooperation and enhanced convergence of requirements and practices. Particularly noteworthy accomplishments include: completion of 9 vendor inspections with multinational cooperation, development of common positions in the area of digital instrumentation and controls, comparison of the quality assurance requirements used in the oversight of vendors, and issuance of a position paper on safety goals.

MDEP has developed a process for identifying common positions on specific issues among the member countries which may be based on existing codes, standards, national regulatory guidance, best practices, and group inputs. These common positions are endorsed by the MDEP members and are good practices, recommended by MDEP. The issued common positions are included in the Appendices A and B to this report.

MDEP has increased its outreach to external organizations by working with standards development organizations in pursuing harmonization of codes and standards, obtaining information from industry on how regulatory cooperation and convergence impacts them, and communicating MDEP activities and outputs to the public and international organization. The MDEP website (http://www.oecd-nea.org/mdep/) contains information on the program, terms of reference, draft and final Common Positions, and publicly available reports.

Two design specific working groups are facilitating the MDEP programme goal of enhanced cooperation. The EPR working group consists of the regulatory authorities of France, Finland, U.S., UK, China, and Canada. The EPR Working Group has been successful in sharing information and experience on the safety design reviews of the EPR with the purposes of enhancing the safety of the design and enabling regulators to make timely licensing decisions, and to promote safety and standardisation of designs through MDEP cooperation. Four expert subgroups are currently interacting on specific technical issues and additional topics have been proposed. The four subgroups address the areas of digital instrumentation and controls, severe accidents, accidents and transients, and

probabilistic safety assessments. The AP1000 design specific working group consists of the regulatory authorities of Canada, China, United Kingdom, and the United States. Three expert subgroups have been formed in the areas of control rod drive mechanisms, civil engineering, and squib valves.

The Vendor Inspection Cooperation Working Group is well established and succeeding at enhancing vendor inspection activities. The group cooperated on eight witnessed vendor inspections in 2010. In each case one regulator performed an inspection to its criteria while being observed or witnessed by representatives of other MDEP countries. The lead country has the benefit of discussion, insights, and suggestions from the observing countries. The benefits to the observing countries include additional information and added confidence in the inspection results as well as the opportunity to compare inspection practices. The working group coordinated one joint inspection, in which one regulator conducts an inspection according to its own regulatory framework with the active participation of one or more other regulators. Additional joint inspections are planned for 2011. The working group completed a comparison of the quality assurance requirements used in the oversight of vendors to identify those areas where the various regulators have common regulatory frameworks. The long term goal of the working group is to harmonize a significant portion of the quality assurance inspection procedures so that the results of a vendor inspection conducted by one member could be used by the other members as they determine appropriate.

The Digital Instrumentation and Controls Working Group developed common positions on specific issues which are based on the existing standards, national regulatory guidance, best practices, and group inputs using an agreed upon process and framework. To date, the working group has issued three common positions (Appendix A), and has drafted 6 additional positions. The working group continued to achieve the objective of efficient and structured information exchange by generating and processing inquiries from member countries. The working group engaged the International Electrotechnical Commission (IEC) and Institute of Electrical and Electronics Engineers (IEEE), as well as IAEA, regarding their increased coordination.

The Codes and Standards Working Group has completed an evaluation of the code comparison of Class 1 vessels, piping, pumps and valves performed by the standards development organizations (SDOs). The SDOs, with the encouragement and support of the working group, compared the Class 1 pressure vessel codes and developed a database that identified the similarities and differences between the Korean, Japanese, and French codes, and the American Society of Mechanical Engineers (ASME) code. This represents the first step of many to achieve harmonization of pressure-boundary codes. Using the comparison results of Class 1 pressure vessels, the working group has begun to identify the sections of the codes that are equivalent or identical, and the sections that are not equivalent, and to examine potential paths for reconciliation of the differences including identifying those that should be pursued for potential convergence. As an interim measure, the CSWG working group has obtained a commitment in principle from the SDOs to work together to minimize further divergence of code requirements.

Accomplishments to date provide confidence that the MDEP structure and process is an effective method of accomplishing increased cooperation in regulatory design reviews. The interim results for 2010 include:

- Issuing a common position on the digital I&C system for the EPR (Appendix B)
- Establishing a preliminary set of technical considerations to be used for novel civil engineering construction (such as modular steel composite structures) and technical guidelines for the design, qualification, and in-service inspection/testing of explosive-actuated valves
- Publishing an MDEP Vendor Inspection Protocol document (Appendix C) with

guidelines for witnessed and joint inspections to facilitate inspections that are observed and attended by multiple regulators.

- Cooperating on eight witnessed vendor inspections and one joint inspection, with the involvement of eight regulatory bodies.
- Drafting a procedure for sharing vendor inspection results, and improving the MDEP library to include an inspection results data base.
- Completing an evaluation of the quality assurance requirements used in the oversight of vendors including those areas where the various regulators have common regulatory frameworks.
- Completing a comparison table of the ASME (American Society of Mechanical Engineers) Boiler and Pressure Vessel Code, AFCEN's (French Society for Design and Construction and In-Service Inspection Rules for Nuclear Islands) RCCM Code, JSME's (Japan Society of Mechanical Engineering) S NC1, and KEPIC's (Korea Electric Power Industry Code) code for Class 1 pressure vessels, piping, pumps, and valves, and developing a plan to address differences in the codes in coordination with the standards development organizations.
- Issuing three common positions in the area of digital instrumentation and controls, specifically (Appendix A) on simplicity in design, software tools and communication independence. Six additional common positions have been drafted and are under review.
- Issuing an MDEP Position Paper on Safety Goals (Appendix C).

MULTINATIONAL DESIGN EVALUATION PROGRAMME

1. INTRODUCTION

The Multinational Design Evaluation Programme (MDEP) is a multinational initiative to develop innovative approaches to leverage the resources and knowledge of national regulatory authorities who are, or will shortly be, undertaking the review of new reactor power plant designs. MDEP has evolved from primarily a design evaluation program to a multinational cooperation program that includes inspection activities and generic issues. MDEP incorporates a broad range of activities including:

- Enhancing multilateral cooperation within existing regulatory frameworks.
- Increasing multinational convergence of codes, standards, and safety goals.
- Implementing MDEP products and regulatory practices to facilitate licensing reviews of new reactors, including those being developed by the Generation IV International Forum.

A key concept throughout the programme is that MDEP will better inform the decisions of regulatory authorities through multinational cooperation, while retaining the sovereign authority of each regulator to make licensing and regulatory decisions.

The idea for the programme was initiated in 2005, and a planning meeting of the original 10 participating countries and IAEA was held in June 2006. Initial efforts consisted of multilateral cooperation on the European Pressurized Water Reactor (EPR) design reviews, and a pilot project to assess the feasibility of enhancing multinational cooperation and convergence of codes, standards, and safety goals within existing regulatory frameworks. The multilateral cooperation on the EPR expanded on bilateral interactions that had already been established between France and Finland. A structure for the programme was developed consisting of a Policy Group to oversee the programme, and a Steering Technical Committee with Working Groups to implement the programme with the Nuclear Energy Agency (NEA) serving as the Technical Secretariat. In addition the IAEA takes part in the work of MDEP.

The programme of work consists of activities which were chosen because they could be accomplished in the near term, and would result in significant benefits while requiring minimum resources. Working groups are implementing the activities in accordance with programme plans with specific activities and goals, and have established the necessary interfaces both within and outside of the MDEP members. Significant progress has been made over the past year on the overall MDEP goals of increased cooperation and enhanced convergence of requirements and practices. Accomplishments to date provide confidence that the MDEP structure and process is an effective method of accomplishing increased cooperation in regulatory design reviews. The progress that has already been achieved demonstrates that a broader level of cooperation and convergence is both possible and desirable.

This report provides a status of the programme after its third year of implementation (March 2010 – March 2011).

2. PROGRAMME GOALS AND OUTCOMES

The main objectives of the MDEP effort are to enable increased cooperation and establish mutually agreed upon practices to enhance the safety of new reactor designs. The enhanced cooperation among regulators will improve the effectiveness and efficiency of the regulatory design reviews, which are part of each country's licensing process. The programme focuses on cooperation and convergence of regulatory practices that will lead to convergence of regulatory requirements. Cooperation will allow a better understanding of each other's processes to encourage and facilitate eventual convergence. The goal of MDEP is not to independently develop new regulatory standards, but to build upon the similarities already existing, and existing harmonization in the form of IAEA and other safety standards. In addition, the common positions developed in MDEP will be shared with

IAEA for consideration in the IAEA standards development programme.

MDEP continues to meet its goal of enabling increased cooperation through the activities of the working groups. MDEP has been very successful in providing a forum for regulatory bodies to cooperate on design evaluations and inspections. In addition to organizing working groups, MDEP has provided each regulator with peer contacts who share information, discuss issues informally, and disseminate information rapidly. For example, the design specific working group members have benefitted significantly from the sharing of questions among the regulators, resulting in more informed, and harmonised, regulatory decisions. MDEP members have also been highly successful in coordinating vendor inspections in which the regulators share observations and insights. MDEP has made improvements in communicating information regarding the members' regulatory practices through development of an MDEP library which serves as a central repository for all documents associated with the programme.

MDEP is meeting its goal of convergence of regulatory practices by establishing common positions in both the issue specific and design specific working groups. The working groups are making comparisons of the regulatory practices in the member countries, identifying differences, and developing common positions. The working groups are also working with codes and standards organizations to identify differences and propose areas of convergence.

Progress towards harmonised regulatory practices and requirements for Generation IV reactor designs will be a natural outgrowth of this programme, as the participating regulatory authorities find that multinational cooperation and convergence of regulatory practices become routine elements of their planning and execution of new design evaluations. It is noteworthy that 9 of the 10 MDEP member countries are also members of the Generation IV International Forum (GIF).

MDEP has been successful in meeting the expected outcomes as defined in the MDEP Terms of Reference by: increasing knowledge transfer, identifying similarities and differences in the regulatory practices; increasing stakeholders' understanding of regulatory practices; and enhancing the ability of regulatory bodies to cooperate in reactor design evaluations, vendor inspections, and construction oversight, leading to more efficient and more safety-focused regulatory decisions.

3. PROGRAMME IMPLEMENTATION

3.1 Membership

Participation in the Policy Group and Steering Technical Committee is intended for mature, experienced national safety authorities of interested countries that already have commitments for new build or firm plans to have commitments in the near future for new reactor designs. Current MDEP members are: Canada, China, Finland, France, Japan, Korea, Russian Federation, South Africa, the United Kingdom and the United States. In addition the IAEA takes part in the work of MDEP.

In January 2011, the MDEP Policy Group approved additional levels of MDEP membership. The MDEP associate member will be a national regulatory authority without previous licensing experience that has been invited by the MDEP Policy Group to participate in selected MDEP design-specific activities based on evidence that the organization is actively involved in new reactor design review activities relevant to MDEP. Such a regulatory authority would be from a country that has taken a firm commitment in the near term to proceed with safety design review activities, has proprietary agreements with the vendor, and is willing and ready to contribute to specific MDEP activities. It is expected that the associate member would be in a position to exchange information with MDEP members to enhance information sharing and experience in relevant design safety reviews.

The MDEP Policy Group also recognizes that there are other national regulatory authorities that may also benefit from close interaction with MDEP. For example there are several countries that have an experienced nuclear regulatory organization, who are already regulating nuclear power plants and also have mid- to long-term plans to pursue new reactor licensing and construction. Such regulators could clearly benefit from interacting now with MDEP and, in the near future, could be clear candidates to become MDEP members or associate members. It is therefore the intent to invite some experienced

regulators to become MDEP candidates with the purpose of these organizations benefiting from the issue-specific and generic aspects of MDEP.

3.2 Organisational Structure

The programme is governed by a Policy Group (PG), made up of the heads of the participating organizations, and implemented by a Steering Technical Committee (STC) and its working groups. The STC consists of senior staff representatives from each of the participating national safety authorities, plus a representative from the International Atomic Energy Agency (IAEA).

The Policy Group provides guidance to the STC on the overall approach; monitors the progress of the programme; and determines participation in the programme.

The Steering Technical Committee manages and approves the detailed programme of work including: defining topics and working methods, establishing technical working groups, and nomination of experts; approving procedures and technical papers developed by the working groups; establishing interfaces with other international efforts to benefit from available work and avoid duplication; developing procedures for the handling of information to be shared in the project; reporting to the Policy Group; identifying new topics for the programme to address; and establishing subcommittees of the STC to study specific topics.

The OECD Nuclear Energy Agency (NEA) performs the Technical Secretariat function in support of MDEP.

Two lines of activities have been established to carry out the work.

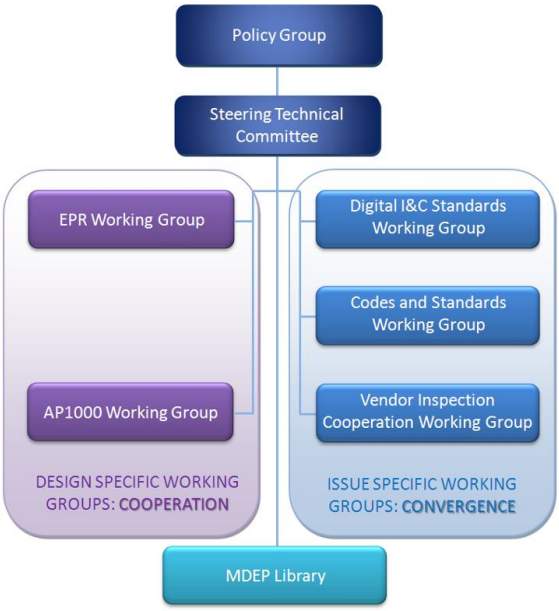
Design-specific activities

Working groups for each new reactor design share information on a timely basis and cooperate on specific reactor design evaluations and construction oversight. Participants in these working groups are the regulatory authorities that are actively reviewing, preparing to review, or constructing the specific reactor design. A design specific working group is formed when three or more MDEP member countries express interest in working together. An “Observer” level of engagement is available for MDEP regulatory bodies engaged in regulatory action based on interest expressed by governmental authority and/or by a utility for exploring the potential for licensing new nuclear power plants of certain designs. Observers can participate in the meetings as long as appropriate controls regarding the use and discussion of proprietary information are established. This status is temporary with expectations that circumstances and the necessary agreements that will allow full participation will develop in a short time period. Under the design specific working groups, expert subgroups have been formed to address specific technical issues.

Issue-specific activities

Working groups are organized for the technical and regulatory process areas within the programme of work. These currently include, but are not limited to, vendor inspections, pressure boundary component codes and standards, and digital instrumentation and control standards. Membership in issue specific working groups is open to all MDEP participating countries and the IAEA representatives.

The following chart illustrates how the programme is organised



3.3 MDEP Library

MDEP information is communicated among the members through the MDEP library which serves as a central repository for all documents associated with the programme. NEA provides the technical support for development and maintenance of the MDEP library on a website. The website includes a folder structure and provides for 2 levels of access which are password protected: (1) MDEP member countries, and (2) member countries participating in design specific working groups. Access to the library is based on requests of the STC member for each participating country and generally consists of the STC members and members of the working groups. Publicly available documents related to MDEP are available on the MDEP page of the NEA website. The STC, through the secretariat, will continue to add documents and make enhancements to improve the effectiveness of the library.

In order for MDEP to be successful at fulfilling its goal of leveraging the work of peer regulators in the licensing of new nuclear power plant designs, a framework was developed to facilitate the sharing of technical information among MDEP participants which at times may include the sharing of proprietary and other types of sensitive information. As a general rule, the information exchanged as part of the MDEP in meetings and the MDEP library is for the use only by the participating national regulators. The members of the design specific working groups also have a communication protocol to share MDEP positions on topics with other members in advance of release of this information into the public domain. A large portion of the information shared may not be proprietary or sensitive; however, all participating members must protect and properly handle the information that an originator claims to be proprietary or sensitive.

3.4 Common Positions

MDEP has developed a process for identifying and documenting common positions on specific issues among the member countries which may be based on existing standards, national regulatory guidance, best practices, and group member inputs. Design Specific Common Positions document common conclusions that each of the working group members have reached during design reviews. Discussions among the members and sharing of information in these areas help to strengthen the individual conclusions reached. Because of the need to issue these statements more quickly, and because responsibility for these decisions rests with the regulators who are performing the design reviews, Design Specific Common Positions require only agreement by the working group members.

Generic Common Positions apply generically rather than only to one design. Generic Common Positions document practices and positions that each of the working group members find acceptable. The common positions are intended to provide guidance to the regulators in reviewing new or unique areas, and will be shared with IAEA, and other standards organizations, for consideration in standards development programmes. Proposed Generic Common Positions will be made available to external stakeholders on the NEA website during the approval process. After a Generic Common Position is agreed to by a working group, it is presented to the STC for endorsement. Upon endorsement by the STC, the proposed Generic Common Positions are made publicly available on the NEA MDEP website for external stakeholder information and comment. Those Common Positions will become best practices, recommended by the MDEP. There is no obligation on the part of any regulatory body to follow them. If a regulatory body chooses to adopt a Generic Common Position, it would be through that country's normal processes.

4. INTERACTIONS WITH OTHER ORGANISATIONS

MDEP recognizes that other organizations are implementing programmes to facilitate international cooperation on new reactors. Because of MDEP's limited membership, these other avenues should be available to countries who are interested in new build, but do not meet the criteria for entrance to MDEP. MDEP strives to maintain an awareness of, and interact with, these other groups to ensure that it does not duplicate efforts, to benefit from the results of these activities, and to communicate MDEP activities and results to other organizations. To ensure that efforts are not duplicated between the groups, MDEP scope is focused on short-term activities related to specific design reviews being conducted by the member countries, and

efforts to harmonize specific regulatory practices and standards.

Brief descriptions of these other programmes and their interfaces with MDEP are below.

4.1 NEA Committee on Nuclear Regulatory Activities (CNRA)

The CNRA Working Group on the Regulation of New Reactors (WGRNR) examines the regulatory issues of siting and licensing processes, and regulatory oversight of Generation III+ and Generation IV nuclear reactors. The current focus areas of the WGRNR are construction experience and siting issues. The WGRNR co-ordinates its work with the work performed by MDEP such that it utilises its outputs and does not duplicate its efforts, and extends the results of MDEP to other CNRA members. MDEP interacts with the CNRA WGRNR and Working Group on Inspection Practices through the NEA staff who also serves as the Technical Secretariat for the CNRA. In addition, the chairs of CNRA WGRNR and MDEP STC meet frequently to discuss on-going activities and plans. WGRNR is the focal point of interactions between MDEP and the CNRA and its working groups, and will assist in coordinating communications and requests between the two activities.

4.2 International Atomic Energy Agency (IAEA)

IAEA participates in the work of MDEP through participation in the Policy Group and STC meetings, and issue specific working groups. In addition, the Generic Common Positions developed in MDEP will be shared with IAEA for consideration in the IAEA standards development programme.

4.3 Western European Nuclear Regulators Association (WENRA)

WENRA is a non-governmental organisation comprised of the Heads and senior staff members of nuclear regulatory authorities of European countries with nuclear power plants. The main objectives of WENRA are to develop a common approach to nuclear safety, to provide an independent capability to examine nuclear safety in applicant countries, and to be a network of chief nuclear safety regulators in Europe exchanging experience and discussing significant safety issues. The WENRA Reactor Harmonisation Working Group (RHWG) issues common reference levels with the objective of attaining a common approach to nuclear safety within Europe. Reference Levels for Existing Reactors have been issued and are in the process of being implemented in WENRA countries. In November 2010, the RHWG issued Objectives for new reactors. Three members of the MDEP Policy Group are also members of WENRA. The MDEP STC has had the benefit of presentations on WENRA activities at meetings. In addition, WENRA documents are recognized as a valuable source of information and insights and can assist the MDEP STC in selecting future topics. In the area of safety goals, MDEP recognizes the work already underway by the WENRA RHWG in this area.

.

4.4 Generation IV International Forum (GIF) Risk And Safety Working Group (RSWG)

MDEP interacts with GIF through the NEA staff who also serve as the Technical Secretariat for GIF, as well as through the U.K. representative to the MDEP STC who is an observer at all RSWG meeting. The MDEP Safety Goals Subcommittee has held discussions with the RSWG. In addition, the chairman of the STC met with chairman of the GIF RSWG, and the GIF Policy Group, to discuss activities of mutual interest.

4.5 Industry Groups

The MDEP working groups are very interested in understanding the perspectives of the design vendors, codes and standards organizations, and component manufacturers in the MDEP activities, and the challenges they face in dealing with numerous regulators and regulatory systems. The MDEP working groups interact with, and invite industry groups to participate in, selective portions of meetings and other activities. For example:

- The Codes and Standards Working Group is interacting with a committee of standards

development organisations (SDOs) (ASME, JSME, KEPIC, AFCEN, NIKIET and CSA) in a code comparison project. The STC issued letters to the SDOs encouraging them to work together to prevent further divergence of the codes and received a verbal commitment from the SDOs.

- The Vendor Inspection Cooperation Working Group heard presentations by EDF, South Texas Nuclear Operating Company, Westinghouse, AREVA, Kansai Electric Power Company and Mitsubishi Heavy Industries of the vendors' perspectives of the regulatory requirements regarding pressure containing components at the working group meetings.

- The Digital Instrumentation and Controls Working Group issued letters to IEC and IEEE encouraging their continued cooperation on MDEP initiatives. IEEE and IEC representatives attended meetings of the working group. The Chair of the Working Group met with the Chair of the IEEE Nuclear Power Engineering Committee (NPEC) and participated in a meeting of the Committee.

- World Nuclear Association's Working Group on Cooperation in Reactor Design Evaluation and Licensing (WNA/CORDEL), an organisation representing many international nuclear industry vendors and operators, met with members of the MDEP Policy Group and with the CSWG. Both MDEP and WNA/CORDEL see some benefits in collaborating in the areas of codes and standards harmonization and safety classification.

5. CURRENT ACTIVITIES

The current activities of MDEP were initiated as a result of the MDEP pilot project, and are being implemented through design specific working groups, issue-specific working groups, and subcommittees of the STC. The members of the design specific working groups share information and co-operate on specific reactor design evaluations and construction oversight. Issue-specific working groups are organised for the technical and regulatory process areas within the programme of work. Each working group has a lead and co-lead country designated, and has developed a programme plan which identifies specific activities, schedules and contacts.

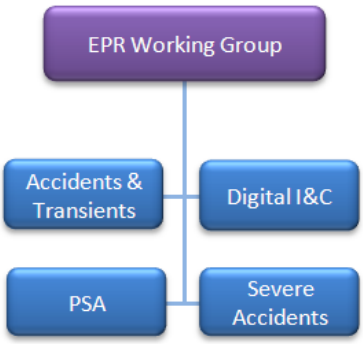
5.1 EPR Design-Specific Working Group

Highlights

The MDEP EPRWG national regulators continued to cooperate on the safety reviews that are being undertaken in Canada, China, Finland, France, the United Kingdom, and the United States.

Most notably the group exchanged information and co-operated on the reviews of the Digital Instrumentation and Controls safety systems, Accidents and Transient and Severe Accidents analyses and evaluations, and Probabilistic Safety Assessments. These efforts have enabled the national regulators to become stronger in their individual safety evaluations and to make timely and effective licensing decisions in each country.

The EPRWG conducted its first meeting in China in November 2010 at which all six EPRWG countries were represented – a notable first for the EPRWG. Coupled with a visit to the Taishan site where the world's third and fourth EPRs are under construction, this EPRWG meeting highlighted the importance of multinational cooperation in design-specific working groups.



The EPR working group currently consists of the regulatory authorities of France, Finland, U.S., U.K., China and Canada. This working group was established in January 2006 as multilateral cooperation between France, Finland and the US. Numerous meetings and technical exchanges have taken place to exchange information on the reviews being conducted in each country: Olkiluoto 3 (OL3) which is under construction in Finland; Flamanville 3 which is under construction in France; and the US version of the EPR which is under review for design certification in the United States and is referenced by 4 combined license applications currently under review. In November 2008, China and the UK were added as members. China -NNSA issued construction permits for two EPRs at the Taishan site in 2009, and construction is underway. UK/NII is performing a Generic Design Assessment of the UK- EPR at the joint request of EDF and Areva. Canada- the review of the EPR design is currently on hold but is still being considered by an applicant for a possible construction licence in Canada.

The EPR DSWG chair is Finland, which is in the process of constructing an EPR; and France, as the country of the design originator, is the co-chair. The goals of the WG are to leverage MDEP regulatory resources by sharing information and experience on the regulatory safety design reviews of the EPR with the purposes of enhancing the safety of the design and enabling regulators to make timely licensing decisions to ensure safe designs, and to promote safety and standardisation of designs through MDEP cooperation.

EPRWG site visit in Taishan (EPR under construction)

The working group currently includes four subgroups that are addressing: Accidents and Transients, Digital Instrumentation and controls, Probabilistic Safety Assessment, and Severe Accidents. The subgroups meet regularly to exchange information on relevant aspects of the design review status, share relevant evaluations when they become available, produce technical reports to identify and document similarities and differences among designs, regulatory safety review approaches and resulting evaluations. In addition to the expert subgroups, the EPR WG addressed important ad hoc issues to support design safety review decision making, such as fire protection, radiation protection, human factors engineering, internal hazards, and grouted tendons in civil structures. The WG provides recommendations, when appropriate, to issue-specific working groups or the STC for considering possible items as a topic to address generically (for example, common positions on digital instrumentation and controls separation of safety and non-safety communications, and issues related to the different safety classification schemes employed by the various MDEP regulators)

Accomplishments

The EPR WG has documented common MDEP positions on aspects of the review to enhance safety and standardization of designs, coordinated communications on MDEP views and common positions to vendor and operators regarding the basis of safety evaluations and standardization; drafted technical reports to identify and document similarities and differences among designs, regulatory safety review approaches and resulting evaluations, and Documented lessons learned from design reviews and design issues faced during construction. The WG developed a plan of coordination of sharing of evaluations and a communications plan that covers publishing significant documents.

EPR Probabilistic Safety Assessment Subgroup

The Probablistic Safety Assessment subgroup is identifying the design differences and modifications affecting risk and the main differences in PSAs. The issues being addressed by the subgroup include: potential loss of two safety divisions, fire risks, I&C, level 2 PSA and severe accidents, and use of a simplified PSA model. The subgroup is drafting a technical report documenting the differences among the designs being reviewed in each country that affect risk assessment, and the main differences in the PSA results and risk profiles. A preliminary comparison will be completed by the end of 2011

Flamanville 3 – Construction site -© EDF

EPR Accidents and Transients subgroup

The Accidents and Transients subgroup is identifying differences in regulatory criteria and approaches among the member countries. The topics being addressed by the subgroup include: evaluation methodologies for accident and transient analysis, containment response evaluation, mass and energy release in containment, containment sump design issue, criticality issues during fuel loading, fuel performance, and boron dilution events. The subgroup is working on a potential common position regarding the evaluation of EPR containment mixing and mass and energy release in co-operation with Severe Accidents subgroup.

EPR Digital Instrumentation and Controls subgroup

The Digital Instrumentation and Controls subgroup focused on the following five core areas of the EPR I&C design: I&C System Independence (particularly for data communications); Information Security; Level of Detailed Design Specifications; Level of Defense and Diversity; and Verification and Validation of Software. Progress is being made by all countries on the EPR digital I&C review, particularly for major technical challenges associated with independence and qualification. The WG issued a common position (Appendix B) documenting aspects of the EPR design where the countries had common agreement. To address the EPR I&C independence issues, AREVA and its customers have implemented design changes. Every EPR now has a backup system for the purpose of either addressing common-cause failure of the primary safety systems or to address the inadequate demonstration of qualification for some primary safety systems.

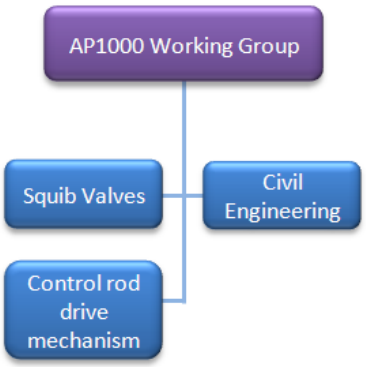
Some members of the subgroup participated in a design-related quality assurance inspection of the I&C design process lead by STUK on an OL3 digital I&C vendor. The observation was open to all members and provided the opportunity to exchange information, particularly on the most advanced EPR in construction.

5.2 AP1000 Design-Specific Working Group

Highlights

The AP1000WG continues to share insights and evaluations of safety reviews and evaluations of the AP1000 designs that are being considered in Canada, China, the United Kingdom, and the United States. Significant progress is being made in the safety reviews in these countries and being shared through the MDEP AP1000WG.

MDEP cooperation in the AP1000WG is significantly enhancing already established bilateral exchanges on the issues of civil engineering (shield building design), squib valve design, and control rod drive mechanisms. Cooperation also extends to providing issue-specific common positions on design characteristics of the AP1000 squib valves.



The AP1000 design specific working group was established in November 2008 with initial participation by China (NNSA), U.K. (NII), and U.S (NRC). Canada (CNSC) was added as a member in March 2009. A total of 4 AP1000 units are under construction in China at the Sanmen and Haiyang sites. The NRC completed its technical review of the AP1000 design and is reviewing combined license applications for 12 AP1000 units. The Vogtle plant, for which NRC has issued an early site permit and Limited Work Authorization, is expected to be the first AP1000 to go into construction in the US. NII has completed Step 3 of the 4-step generic design assessment process of the AP1000 design. CNSC completed phase 1 of its pre-project design review on the potential choices for new reactor construction, including the AP1000. The AP1000 DSWG chair is the US, the country of the design originator; and China, as the first country to begin the construction of an AP1000, is the vice-chair

A status of the expert subgroups follows.

Civil Engineering Subgroup

The civil engineering subgroup was formed primarily to address the unique design of the shield building, and outstanding questions regarding the modular construction techniques to be used. The subgroup members compared results of their separate reviews of the shield building design and came to similar conclusions regarding fundamental concerns. The discussions were helpful in confirming conclusions already identified by the regulators. In the absence of applicable design standards for concrete composite structures, the expert subgroup developed a preliminary set of technical considerations to be used for novel civil engineering construction (such as modular steel composite structures). These considerations may be used to provide input to the standards organizations in developing a code case for modular construction.

Squib Valve Subgroup

The squib valve subgroup was formed to address the unique design of the in-containment refueling water storage tank injection valves (squib valves). The squib valves to be used on the AP1000 are much larger than those used in existing nuclear applications. The members agreed that the lack of experience with large squib valves required particular care in the design, qualification, and in-service inspection/testing of these valves. The Squib Valve subgroup issued a common position (Appendix B) on technical guidelines for the design, qualification, and in-service inspection/testing of explosive-actuated valves. The guidelines are intended to be helpful to regulators and the nuclear industry in understanding the technical issues associated with large explosive-actuated valves used in AP1000 reactors and other reactor designs.

Control Rod Drive System Subgroup

The Control Rod Drive System Subgroup was formed to address the safety classification, particularly the classification of the latch mechanisms and the adequacy of any associated testing or analysis to show that the latch mechanisms can perform their intended safety function. The subgroup members compared information on the design and the reasons for their conclusions on safety classification.

Potential new activity

Another area of interest that was discussed by the WG members is digital I&C. The WG members held discussions on the issues and in July 2010, NII and NRC representatives visited the vendor to discuss the subject issues and develop resolutions.

AP1000 under construction, Sanmen, China; © SNMPC 2010.

5.3 Vendor Inspection Co-operation Issue-specific Working Group

Highlights

The goal of the VICWG is to leverage each MDEP country's expertise and experience in conducting vendor inspections to support more efficient use of resources and identifying and resolving emergent issues. In 2010 the VICWG coordinated 8 witnessed inspections to further this goal.

Members of the MDEP VICWG and EPRWG also conducted the first joint inspections to support resolution of issues involved in manufacturing of important structures, systems, and components of new reactors.

The VICWG shared its Inspection Protocol document with vendors that are subject to VICWG inspections in an effort to better communicate the role of various organizations involved in witnessed and joint inspections. This Inspection Protocol document was also used by other design-specific working groups to support inspections of digital I&C vendors.

Background

The Vendor Inspection Cooperation Working Group (VICWG) was formed because component manufacturing is currently subject to multiple inspections and audits similar in scope and in safety objectives, but conducted by different regulators to different criteria. The primary goal of the VICWG is to maximize the use of the results obtained from other regulator's efforts in inspecting vendors.

The VICWG enhances the understanding of each regulator's inspection procedures and practices by coordinating witnessed inspections of safety related mechanical pressure retaining components (Class 1) such as pressure vessels, steam generators, piping, valves, pumps, etc., and quality assurance (QA) inspections. In addition, they share various vendor inspection results with each other in the MDEP library which is set up to contain the regulators inspection reports. In the longer term, a process will be developed to adapt the scope of an inspection according to the need of other regulators.

Accomplishments

In 2010, the VICWG coordinated eight witnessed inspections and one joint inspection, with the involvement of eight regulatory bodies. Witnessed inspections consist of one regulator performing an inspection to its criteria, observed or witnessed by representatives of other MDEP countries. The benefits to the observing countries include additional information and added confidence in the inspection results. MDEP regulators are using the experience gained during conduct of the VICWG witnessed inspections in their inspection planning and execution. Joint inspections consist of one regulator conducting an inspection according to its own regulatory framework with the active participation of one or more other regulators. This would allow the participating members to use the results of the inspection that are applicable to their regulations. The VICWG maintains a Vendor Inspection Planning Table with a list of scheduled vendor inspections to assist the member regulators in identifying opportunities to observe an inspection, or obtain the results of an inspection carried out by another member.

The VICWG developed an MDEP Vendor Inspection Protocol document (Appendix C) with guidelines for witnessed and joint inspections. This document facilitates inspections that are observed and attended by multiple regulators.

In order to improve the process for sharing inspection results, the VICWG agreed on a procedure to share inspection results, and improved the MDEP library to include an inspection results data base. This data base will include not only the reports of witnessed and joint inspections, but all inspections that may be of interest to the MDEP members.

The VICWG conducted a survey on QA requirements used in the oversight of vendors to identify those areas where the various regulators have common regulatory frameworks. A comparison table was finalized and analyzed.

Future Actions

The participating regulators have gained much experience in each other's inspection processes through the MDEP witnessed

inspections conducted since 2008. Therefore, the VICWG will continue to coordinate witnessed inspections and will increase its focus on joint inspections in 2011. Two joint inspections are currently planned for 2011. This will continue to enhance the exchange of information between the regulators and provide better understanding of the inspection scopes and safety findings and how these findings may be utilized.

The VICWG will explore expanding their activities beyond pressure boundary components into areas such as electrical and mechanical components, concrete, and examine modular construction as areas where vendor inspections can be useful to MDEP members.

The VICWG plans to identify common quality assurance requirements that could be acceptable to MDEP regulators. The VICWG plans to supplement the table of QA requirement comparisons by comparing with ISO 9001+ and GSR 3. The long term goal of the VICWG is to harmonize a significant portion of the quality assurance inspection procedures so that the results of an inspection conducted by one member could be used by the other members, requiring that other member countries only inspect that portion of their requirements not covered by the common inspection procedure.

In the longer term, the VICWG is considering developing a common MDEP vendor inspection procedure that could be used for multinational vendor inspections.

OL3 Steam generator installation; © TVO 2010.

5.4 Codes and Standards Working Group

Highlights

The goals of the MDEP CSWG include promoting harmonisation of mechanical Codes and Standards, where possible, as well as exploring how to potentially utilize another country's Codes and Standards in national regulatory processes. The CSWG continued to work closely with the various Standards Development Organisations (SDOs) from France, Korea, Japan, Canada, Russia, and the United States to fully comprehend the nature of the differences among these various mechanical Codes and Standards for Class 1 pressure vessels, piping, pumps, and valves.

The CSWG achieved agreement in principle with the SDOs to pursue options to preclude further divergence among the various Codes and Standards.The CSWG also interacted with industry representatives from the World Nuclear Association to encourage identifying resources to promote potential Code harmonisation.

The CSWG is exploring regulatory options to be able to evaluate a structure, system, or component that was produced and manufacturing to a foreign Codes.

Background

The primary goal of the Codes and Standards Working Group (CSWG) is to achieve harmonization of codes and standards for components important to safety. Harmonization is defined as establishing a framework for code convergence and for reconciliation of differences with Code requirements. The key to achieving harmonization is to understand the source of and reasons for differences of Code requirements in order to assess their significance from a safety and risk perspective. A major initial step towards this goal is establishing a retrievable data base of the similarities and differences among the codes and standards used in the design of pressure boundary components. The working group's goal is to perform an assessment of the similarities and differences for the codes and standards, and identify the most beneficial areas for convergence. Changes in codes and standards can only be made by the standards development organizations (SDOs) themselves and therefore, the role of the working group is to assist the SDOs in identifying and resolving important differences. The goal of both the SDOs and the CSWG is to achieve global harmonization of pressure-boundary design codes for nuclear power plants. The Code-comparison project performed by the standards development organizations (SDOs) from Japan, France, Korea, Canada, the Russian Federation and the United States represents the first major step towards this goal. The results of the Code comparisons provided the necessary information for the MDEP/CSWG to develop its next steps towards achieving its long-term goal of harmonization of Code and standards.

Accomplishments

The CSWG interacted with SDOs which formed a steering committee composed of the representatives of ASME, JSME, KEPIC, AFCEN, CSA, vendors, and utilities. The CSWG is represented on the steering committee by the representative from the US NRC. The SDOs performed a Code-comparison project in conjunction with the working group's efforts. More specifically, the SDOs compared requirements of their pressure-boundary codes and standards including JSME's S-NC1 Code (Japan), AFCEN's RCC-M Code (France), KEA's KEPIC Code (Korea), CSA's N285.0 standard (Canada) and NIKIET's PNAE G-7 Code (Russia) against the requirements of Section III of the ASME Boiler and Pressure Vessel Code (United States) for Class 1 vessels, piping, pumps and valves. The results provided a significant amount of information about the comprehensiveness and technical adequacy of each country's pressure-boundary codes and standards and produced a wealth of useful information about the technical and programmatic similarities and differences between each country's codes including the reasons for these differences. Consequently, the results will enable regulators as well as other users of the Code-comparison report to determine the impact of those differences and their safety significance as well as provide insights into the level of effort needed to reconcile those differences.

Finally, the results of the Code-comparison project enabled the CSWG to understand from a global perspective how each country's pressure-boundary code or standard evolved into its current form and content. This allowed the

CSWG to recognize the important fact that each country's pressure-boundary code or standard is a comprehensive, living document that is continually being improved to reflect the changing technology and common industry practices unique to each country.

The code comparison results identified the major categories of differences between each code (i.e., technical, administrative, and requirements addressed in only one code), and identified the extent of similarities and differences between each countries code to the ASME code. This represents the first step of many to achieve harmonization of pressure-boundary codes. Using the comparison results of Class 1 pressure vessels, the working group has begun discussions to identify the sections of the codes that are equivalent or identical, and the sections that are not equivalent, and to examine potential paths for reconciliation of the differences in the codes including identifying those that should be pursued for potential convergence. Convergence will be limited to technical differences because convergence of administrative differences have cultural, historical, industrial, and legal backgrounds that are difficult to change.

As an interim measure, the working group has obtained a commitment in principle from the SDOs to work together to minimize further divergence of code requirements.

The WG is developing several work products separate from the SDO code comparison activity. A Fundamental Attributes of Mechanical Codes document was drafted that establishes high-level requirements or fundamental concepts for codes and standards. The WG also established mid-level guidance to identify the common code aspects based on the evaluation and analysis of code similarities and differences. This guidance is planned to be documented by the CSWG on the issues of fundamental attributes of Mechanical Codes, essential safety references of Mechanical Codes, means to converge Code differences, reconciliation of Code differences, and how to preclude further diverge among the Codes.

Next Steps

The WG has identified a step-wise approach to progress towards convergence on specific parts of the codes. The WG would first help the SDOs identify a few code requirements where differences have the most impact and convergence could be achieved without significant effort. The SDOs would be solicited to take a further step in converging these differences, and then encouraged to incorporate the converged portion into their own codes. If successful, additional areas would be pursued for convergence. The WNA/CORDEL Group is supportive of MDEP's code comparison effort and has proposed to coordinate and fund a pilot project for selected code convergence. CORDEL has met with the CSWG to discuss its plan to work with the SDOs and independent experts to identify parts of the codes where convergence is most beneficial, and propose a harmonized version of the selected part or demonstrate equivalence.

The WG is also pursuing the development of a process to assist regulatory bodies in the review of designs that are based on foreign codes and standards. This should involve regulatory practices for reconciliation of differences among the various codes. Once an understanding is gained of the differences between the codes, each MDEP participant could initiate their national process to endorse, in whole or in part, the pressure boundary codes and standards of other countries.

Plans to further expand the scope of work to include Class 2 and 3 vessels, piping, pumps and valves will depend on the success of the project for Class 1 components.

.

5.5 Digital Instrumentation & Controls Working Group

Highlights

A key goal of the DICWG is to encourage harmonisation of national and international Codes and Standards affecting the digital instrumentation and controls for nuclear power plant safety systems. This organization worked closely with representatives from IEC and IEEE to find harmonisation opportunities and to provide key regulatory input on important safety issues.

The DICWG developed common positions on specific issues among the member countries. Common Positions on important topics were issued in the areas of software tools, communication independence, and simplicity in DI&C design.

The DICWG remains closely engaged with key organizations to ensure that digital instrumentation and control design aspects are addressed.

Background

The objective of the digital instrument and controls working group (DICWG) is to identify opportunities for convergence of applicable standards. The working group's activities include: identifying and prioritizing the member countries' challenges, practices, and needs regarding standards and regulatory guidance regarding digital instrumentation and controls; identifying areas of importance and needs for convergence of existing standards and guidance or development of new standards; sharing of information; and developing the common positions among the member countries for areas of particular importance and need.

The DICWG is enhancing its cooperation with the standards organizations, IEEE and International Electrotechnical Commission (IEC). Both organizations expressed a significant interest in DICWG and expressed their commitment to cooperate with the working group. Representatives from IEEE, IEC, and IAEA participate in most of the working group meetings, and both IEC and IEEE allowed a number of their standards relevant to digital I&C to be made available in the MDEP library for use by the working group members. The IEC formalized an agreement with the OECD to facilitate co-operation between the two organizations

Accomplishments

The working group identified the member countries' most significant technical issues regarding standards and regulatory guidance related to digital instrumentation and controls and prioritized the differences that should be addressed for increased convergence work. In all of the priority areas, the working group identified that there were significant similarities and overlaps in the regulatory approaches.

The working group compared the list of IEC standards and IEEE standards relevant to digital instrumentation and controls. A detailed comparison table has been developed and reviewed by the working group. This comparison resulted in significant findings regarding the standards in terms of the development status, scope and details as well as the differences and similarities at a high level. The working group engaged IEC and IEEE, as well as IAEA, regarding their participation in a comparison exercise of the standards and increased coordination related to digital instrumentation and controls. Based on the results of the comparison exercise, the working group issued letters to IEC and IEEE recommending that the standards organizations consider the MDEP common positions when revising their standards and increase their cooperation to achieve enhanced harmonization of relevant standards.

The DICWG developed common positions on the members' most significant technical issues. Additionally, the working group has identified numerous other areas for potential convergence and has been developing common positions to address those issues. The three common positions already completed (Appendix A) address the areas of simplicity in design, software tools and communication independence. There are, at this time six additional common positions under development in the areas of: Software common cause failures, independent verification and validation, complex electronics, adequate diversity, qualification of industrial digital devices of limited functionality for

use in safety applications, and security. It is anticipated that additional topics will be identified as the working group continues to develop and completes these common positions. The completed common positions are included as an appendix to this report.

The working group continued to achieve the objective of sharing of valuable information. The working group developed a formal "Quick Inquiry" process to generate and process inquiries from member countries to promote an efficient and structured information exchange and provide for storing this information in a retrievable database. The working group also continued to exchange information regarding the status of and issues associated with licensing of new reactor digital instrumentation and control. The DICWG maintains frequent communication with the design-specific working groups, mainly with the EPR digital instrumentation and controls subgroup.

Next steps

The working group will continue to develop additional Generic Common Positions as technical issues are identified and addressed.

The working group will communicate specific suggestions to the standards organizations and IAEA for consideration of harmonization in a timely manner when they are identified during its activities.

The working group will continue to exchange information among members to contribute to efficiency and effectiveness of the licensing of new reactor digital instrumentation and controls.

The working group will continue to engage digital instrumentation and controls vendors and utilities to share experience and insights toward developing common positions that are based on a broad spectrum of inputs.

DICWG members – 8th meeting in October 2010

5.6 Safety Goals

Highlights

A subcommittee of the STC developed a framework paper, based on the Defence-in-Depth concept and probabilistic considerations that can be useful for development of safety goals and support of safety decisions by safety authorities and the designers.

Background:

One of the original ten recommendations of the MDEP pilot project was to compare how top level safety goals are derived, expressed, and achievement is judged among the participating countries, and to determine the extent to which they can be considered equivalent. MDEP recognised that the route to harmonisation of safety goals must start with high level, mainly qualitative goals, which are not dependent on the reactor technology considered. This understanding is expected to enhance cooperation in using other regulators' assessments and the understanding of how decisions have been reached.

This issue was addressed through a subcommittee consisting of STC members or their representatives with technical expertise in the safety goals arena. The objectives of the subcommittee were to 1) start with the high level safety goals; 2) determine a structure for safety goals that can be used for all types of technology; and 3) develop a method to derive lower tier safety goals so they are consistent for different technologies and clearly related to the higher tier goals. The subcommittees work did not include the development of detailed safety goals. The subcommittee initiated discussions with other groups including CSNI/WGRisk, WENRA RHWG, Gen IV Risk and Safety Working Group, and IAEA's International Safety Group (INSAG), with the goal of using MDEP to complement their work.

Accomplishments

The subcommittee identified work being accomplished by other groups, surveyed committee members approaches determined commonalities, and developed a procedure for developing lower tier safety goals in a consistent way.

From the survey results and other considerations, the subcommittee developed a set of possible safety goals and proposed a hierarchical structure in which to develop them which extends the defense in depth approach to integrate the elements of safety during normal operation and accident conditions for the whole plant lifecycle. The outcome of the group's efforts was a report on the Structure and Application of High Level Safety Goals, and a position paper detailing the MDEP position on safety goals (Appendix C).

Next Steps

The MDEP recommendations related to high level safety goals will form the basis for MDEP contributions to the work being performed in this area by WENRA, NEA/CNRA, and IAEA.

.

6. INTERIM RESULTS

In March 2009, the MDEP Policy Group agreed that the programme must continue beyond the original two year mandate to fully achieve the established goals. Therefore, MDEP is considered a long term programme with interim results. Interim results are those products that document agreement by the MDEP member countries and are necessary steps in working towards increased cooperation and convergence. The interim results for 2010 include:

- Issuing technical expert subgroup technical reports that identify and document similarities and differences among designs, regulatory safety review approaches and resulting evaluations.
- Issuing guidance to all working groups regarding the process to develop and approve common positions
- Issuing a common position on the digital I&C system for the EPR.
- Establishing a preliminary set of technical considerations to be used for novel civil engineering construction (such as modular steel composite structures) and technical guidelines for the design, qualification, and in-service inspection/testing of explosive-actuated valves
- Publishing an MDEP Vendor Inspection Protocol document with guidelines for witnessed and joint inspections to facilitate inspections that are observed and attended by multiple regulators.
- Cooperating on eight witnessed vendor inspections and one joint inspection, with the involvement of eight regulatory bodies.
- Drafting a procedure for sharing vendor inspection results, and improving the MDEP library to include an inspection results data base.
- Completing an evaluation of the quality assurance requirements used in the oversight of vendors including those areas where the various regulators have common regulatory frameworks.
- Comparing the ASME Boiler and Pressure Vessel Code, AFCEN's RCCM Code, JSME S NC1, and KEPIC code for Class 1 pressure vessels, piping, pumps, and valves, and developing a plan to address differences in the codes in coordination with the standards development organizations.
- Issuing three common positions in the area of digital instrumentation and controls, specifically on simplicity in design, software tools and communication independence. Six additional common positions have been drafted and are under review.
- Issuing an MDEP Position Paper on Safety Goals.

7. NEXT STEPS – FUTURE OF THE PROGRAMME

MDEP has begun to consider the addition of new topics and how they could be addressed by the program. The criteria that will be used in evaluating whether an activity should be undertaken as part of MDEP include

- the activity is of generic interest and of safety significance to the licensing of new reactors in MDEP member countries
- the approach followed by the MDEP regulators is not completely similar
- successful completion of the activity would likely result in increased harmonization/ convergence in regulatory practices or increased cooperation within a reasonable timeframe and resource expenditures
- any new MDEP activity should not duplicate similar efforts that are already ongoing or are planned to be undertaken by other more –appropriate organizations such as the CNRA/WGRNR (or other NEA WGs), IAEA, GIF, WENRA, etc. except where MDEP could contribute to the ongoing work of these groups
- each new activity should have a lead country willing to take an active leadership role, and should have a defined product

In addition, a number of topics have been identified in which MDEP can play a significant, positive role by cooperating with current efforts in other organizations such as safety goals as discussed earlier.

Another topic under discussion by MDEP is safety classification. Several of the MDEP working groups raised concerns regarding challenges encountered by the use of different safety classification schemes by the members. A subcommittee of the STC was formed to explore the issues association with safety classification, perhaps in coordination with industry groups. MDEP will focus its efforts on providing input to a draft IAEA standard DS367, "Safety Classification of Structures, Systems and Components in Nuclear Power Plants".

The MDEP STC will continue to search out areas where it can act as a catalyst for enhanced regulatory cooperation and convergence in other forums. MDEP is in a unique position to effect positive change because it includes the regulatory authorities of over three quarters of the reactors world-wide and represents those agencies at the highest levels. MDEP is using its influence to initiate change and will contribute to the success of other initiatives including those of IAEA, NEA, and WENRA.

APPENDIX A

GENERIC COMMON POSITIONS

DICWG-06: COMMON POSITIONS ON PRINCIPLE ON SIMPLICITY IN DESIGN

DICWG-02: COMMON POSITION ON SOFTWARE TOOLS FOR THE DEVELOPMENT OF SOFTWARE FOR SAFETY SYSTEMS

DICWG-04: COMMON POSITIONS ON PRINCIPLE ON DATA COMMUNICATION INDEPENDENCE

Date: 8 February 2011
Validity: **until next update or archiving**
Version 1

MDEP Generic Common Position No DICWG-06

Related to : Digital Instrumentation and Controls Working Group activities

COMMON POSITIONS ON PRINCIPLE ON SIMPLICITY IN DESIGN

Multinational Design Evaluation Programme
Generic Common Position
DICWG No6 – PUBLIC USE

Date: 8 February 2011
Validity: until next update or archiving
Version 1

Multi-National Design Evaluation Programme

Digital Instrumentation and Controls Working Group

GENERIC COMMON POSITION DICWG NO6: PRINCIPLE ON SIMPLICITY IN DESIGN

Summary:

The Digital Instrumentation and Controls Working Group (DICWG) has agreed that a common position on this topic is warranted given its growing applications to the new reactors, its safety implications, and the need to develop a common understanding from the perspectives of regulatory authorities. This action follows the DICWG examination of the regulatory requirements of the participating members and of relevant industry standards and IAEA documents. The DICWG proposes a common position based on its recent experience with the new reactor application reviews and operating plant issues.

Context:

The use of digital technology typically allows the achievement of more complex functionality. This increase in functionality can accommodate both essential and non-essential functions associated with safety. Although the increased functionality can result in benefits, the increased complexity can also have negative effects. Requirements that are unnecessary or that specify unnecessarily stringent performance criteria cause extra work and add complexity. Complexity can generate additional faults in design, difficulty in detecting and correcting faults, introduction of failure modes and effects that are not present in simpler design, and challenge in demonstrating conformance to safety system design criteria such as independence, testability and reliability. It can also increase licensing uncertainty during the review by the regulatory authorities. The actual licensing experience by some of the regulatory authorities has shown that simplicity provides greater licensing certainty. This common position provides the agreed-upon principle of the MDEP DICWG member states on simplicity for the design of the digital systems of the highest classification. Other design principles (e.g., independence and redundancy) for essential safety functions should continue to be met as this common position is applied.

Generic Common Position for Treatment of Simplicity in Design:

1) Design of digital systems for the highest classification should be as simple as practical.

2) All unnecessary complexity should be avoided both in the functionality of the system and in its implementation.

3) All features should be demonstrated to be beneficial to safety in consideration of the impact of their added complexity to the design. This complexity cannot lead to violation of other design principles (for example, independence, redundancy, diversity).

Definitions:

Complexity is defined in IEEE Std 7-4.3.2 and IEEE Std 610 as the following:

1. *The degree to which a system or system component has a design or implementation that is difficult to understand and verify*

2. *Pertaining to any set of structure-based metrics that measure the attribute in definition 1.*

Complexity is defined in IEC 61513 as the following:

3. *The degree to which a system or system component has a design or implementation that is difficult to understand and verify [IEEE Std 610 modified]*

Simplicity is defined in IEEE Std 610 as the following:

The degree to which a system or component has a design or implementation that is straightforward and easy to understand. Contrast with complexity.

References

NS-G-1.1, "Software for Computer Based Systems Important to Safety in Nuclear Power Plants," 2000

NS-G-1.3, "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants," 2002

IEEE 610.12 "IEEE Standard Glossary of Software Engineering Terminology" 1990

IEEE 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of

Nuclear Power Generating Stations," 2003

IEC 61513, "Nuclear power plants - Instrument and control for systems important to safety - General requirements for systems"

IEC 60880, "Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions"

Four Party Report, "Four Party Regulatory Consensus Report on the Safety Case for Computer-Based Systems in Nuclear Power Plants"

Seven Party Report, "Licensing of safety critical software for nuclear reactors. Common position of seven European nuclear regulators and authorised technical support organizations"

Simplicity in design (IEC 60880)

Considering SW tools, specifically related to translators/compilers. The size and complexity of many compilers can make it extremely difficult to demonstrate that a compiler works correctly. However, extensive experience of use can increase confidence that the compiler works correctly (extracted from 880)

The disadvantages introduced by diversity may include a greater overall complexity (extracted from 880)

Simplicity in design (IEC 61513)

The choice of system architecture may be restricted in order to limit the complexity to facilitate implementation of functions of high safety category (extracted from IEC 61513)

Simplicity in design (NS-G-1.1)

3.2. It should be demonstrated that all unnecessary complexity has been avoided both in the functionality of the system and in its implementation. This demonstration is important to safety and is not straightforward, as the use of digital programmable technology permits the achievement of more complex functionality. Evidence of obedience to a structured design, to a programming discipline and to coding rules should be part of this demonstration.

3.3. For safety systems, the functional requirements that are to be fulfilled by a computer system should all be essential to the achievement of safety functions; functions not essential to safety should be separated from and shown not to impact the safety functions.

3.4. For computer based system applications, top-down decomposition, levels of abstraction and modular structure are important concepts for coping with the problems of unavoidable complexity. They not only allow the system developer to tackle several smaller, more manageable problems, but also allow a more effective review by the verifier. The logic behind the system modularization and the definition of interfaces should be made as simple as possible (for example by applying 'information hiding' (see Section 3.3.4 of Ref. [4])).

3.5. In the design of system modules, simpler algorithms should be chosen over complex ones. Simplicity should not be sacrificed to achieve performance that is not required. The computer hardware used in safety systems should be specified with sufficient capacity and performance to prevent software from becoming too complex.

Simplicity in design (7 party report)

2.12.3.6 The systems and software architecture design shall have the minimum complexity commensurate with the design requirements.

2.2.3.8 It shall be ensured that the use of these fault tolerant, exception handling and hazard mitigating mechanisms is appropriate and that they do not introduce unnecessary complexity.

2.3.2.4 Despite all best endeavours to produce fault free software through good design practices and thorough testing, there is always the potential for unforeseen error conditions to arise. Therefore the technique of incorporating error checking (which may be based on formal assertions) into software is regarded as a sound policy. This technique is known as defensive programming. It should cover both internally and externally arising exceptions, without adding unnecessary complexity to the software.

Simplicity in design (4 party report)

5.1.3 Minimising faults in the design

(a) complexity avoidance;

5.2.4 System design principles

(b) avoidance of complexity, so far as is practicable, should be the guiding aim;

Date: 8 February 2011
Validity: until next update or archiving
Version 1

MDEP Generic Common Position No DICWG-02

Related to: Digital Instrumentation and Controls Working Group activities

COMMON POSITION ON SOFTWARE TOOLS FOR THE DEVELOPMENT OF SOFTWARE FOR SAFETY SYSTEMS

Multinational Design Evaluation Programme

Digital I&C Working Group

PROPOSED GENERIC COMMON POSITION DICWG NO2: MDEP COMMON POSITION ON SOFTWARE TOOLS FOR THE DEVELOPMENT OF SOFTWARE FOR SAFETY SYSTEMS

Summary:

The Digital Instrumentation and Controls Working Group (DICWG) has agreed to this generic common position on the selection, qualification, and use of software tools used for the development of safety system software in nuclear power plants. This action follows the DICWG examination of the regulatory requirements of the participating members. This generic common position is based on the software tools guidance of IEC 60880, "Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions."

Context

The use of appropriate software tools can increase the integrity of the I&C development process, and hence product reliability, by reducing the risk of introducing faults during the process. The use of tools can also have economic benefits as they can reduce the time and human effort required to produce systems, components, and software. Tools can be used to automatically check for adherence to rules of construction and standards, to generate proper records and consistent documentation in standard formats, and to support change control. Tools can also reduce the effort required for testing and to maintain automated logs. In some cases tools are necessary because a specific development methodology requires their use.

Tools are most powerful when they are defined to work co-operatively with each other.

Scope and Definition

This common position applies to software tools used in the development of software for safety systems and software tools are defined to:

- support the capture of requirements,
- support the transformation of requirements into the final system code and data (there may be many intermediate steps),
- directly support the performance of verification, validation and testing,
- prepare and control application data, and

- manage and control of the processes and products involved in the software development.

In this document *safety system* means a Class 1 system as defined in IEC 61226. The term safety system as used in this document is equivalent to the term *safety system* as defined in IEEE 603 which is incorporated into 10 CFR 50.55a (h) and the term *safety related system* as defined in 10 CFR 50.2.

This common position does not apply to:

- tool support for complex programmable logic devices such as FPGAs,
- off-line tools, used to calculate important variables used during the design and analysis of safety systems, or
- office administration tools used to support tasks not directly concerned with software development (e.g., word processors and project management tools).

Generic Common Position for Software Tools:

1. Tools should be used to support all aspects of the I&C life cycle where benefits result through their use and where tools are available.

A key element of integrated project support environments is to ensure proper control and consistency. If tools are not available, the development of new tools may need to be considered.

2. The benefits and risk of using a tool should be balanced against the benefits and risk of not using a tool.

The important principle is to choose tools that limit the opportunity for making errors and introducing faults, but maximise the opportunity for detecting faults.

System development may be adversely affected by the use of tools in several ways. For example, design tools may introduce *faults* by producing corrupted outputs; and *verification* tools may fail to reveal certain *faults* or types of *faults*.

3. The functionality and limits of applicability of all tools should be identified and documented.

4. The tools and their output should not be used outside their declared functionality or limits of application without prior justification.

For example, tools cannot replace humans when judgement is involved. In some cases, tool support is more appropriate than complete automation of the process

5. Tools should be verified and assessed consistent with the tool reliability requirements, the type of tool, and the potential of the tool to introduce faults.

For example:

- Verification is not necessary for tools that cannot introduce or fail to detect faults.
- Less rigor in tool verification may be accepted if there is mitigation of any potential tool faults (e.g. by process diversity or system design,),
- Verification is not necessary for the tool outputs that are always systematically verified.

6. The qualification process should take into account experience from prior use.

7. All tools should be under appropriate configuration management.

8. Tool parameters used during the development, verification, or validation of baseline equipment or software should be recorded in the development records.

This is useful not only for the final software consistency; it also helps in assessing the origin of a fault, which may lie in the source code, in the tool, or in the tool parameters. It may also be necessary in the assessment of the potential for common cause failures due to software tools.

9. Section 14 of IEC standard 60880 provides acceptable guidance for the selection, qualification, and use of software tools for the development of software for safety systems.

References

Four Party Regulatory Consensus Report On The Safety Case For Computer-Based Systems In Nuclear Power Plants, November 1997

IAEA NS-G-1.1, "Software for Computer Based Systems Important to Safety in Nuclear Power Plants"

IEC 60880, "Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions"

IEC 61226 Ed. 3, "Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions," International Electrotechnical Commission, Geneva, Switzerland, 2009.

IEEE 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"

Licensing of safety critical software for nuclear reactors. Common position of seven European nuclear regulators and authorised technical support organisations, 2007.

Date: 2 March 2011
Validity: until next update or archiving
Version 1

MDEP Generic Common Position No DICWG-04

Related to: Digital Instrumentation and Controls Working Group activities

COMMON POSITIONS ON PRINCIPLE ON DATA COMMUNICATION INDEPENDENCE

Multi-National Design Evaluation Programme

Digital Instrumentation and Controls Working Group

GENERIC COMMON POSITION DI&C-04: PRINCIPLE ON DATA COMMUNICATION INDEPENDENCE

Summary:

The Digital Instrumentation and Controls Working Group (DICWG) has agreed that a common position on this topic is warranted given its growing applications to the new reactors, its safety implications, and the need to develop a common understanding from the perspectives of regulatory authorities. This action follows the DICWG examination of the regulatory requirements of the participating members and of relevant industry standards and IAEA documents. DICWG proposes a common position based on its recent experience with the new reactor application reviews and operating plant issues. The DICWG proposes a common position based on its recent experience with the new reactor application reviews and operating plant issues.

Context:

I&C architectures in new plants will make extensive use of digital communications, both between safety systems and between systems of different safety classes. One of the more significant regulatory implications is maintaining not only physical and electrical independence but also data communication independence between different safety systems, thereby guaranteeing that errors in one channel or division or lower class systems will not cause the failure of another channel or division or higher class systems. This common position provides the agreed-upon principle of the MDEP DICWG member states on data communication independence for the design of the digital systems.

Generic Common Positions for Treatment of Data Communication Independence:

1. Communication between safety divisions

Communications between computers in different safety divisions should have no detrimental effect on the safety division in question due to any failure or error in communications either from or to another division.

Broadcast communication is an acceptable approach for the communication independence between computers in different safety divisions. “Broadcast” means that transmitter put data into the designated space for the buffering function, and then receivers just read the data from the buffering space without handshaking.

Architectures utilizing a central hub or router where communications from multiple safety division are transmitted across a single channel should be prohibited.

2. Communication between systems of different safety classes

Communication computers performing functions of a higher safety category should be adequately isolated from communication computers performing functions of a lower safety category

(including non classified functions). When the communication between systems of different safety classes is required, then the plant data flow should be from the higher safety classified systems to the lower safety class systems. For data flows from lower to higher classified safety systems, there should be a demonstrable safety benefit and a demonstration that safety functions of the higher category cannot be adversely affected by such a connection. Data flows from lower to higher classified safety systems that are not necessary for safety, even if they enhance reliability, should be prevented.

3. Priority function

A priority function should be a safety function. Devices that perform safety functions may be actuated by both safety systems and systems of a lower safety class provided that the completion of safety actions cannot be interrupted by commands, conditions, or failures outside the function's own safety division. This is commonly accomplished by use of a priority function.

4. Communication interfaces and buffering function

Devices (e.g., processors) that perform safety functions should perform no communications handshaking or interrupts that could disrupt deterministic safety function processing. Buffering should be provided between communications links and devices performing safety functions. The buffers should ensure that faults and failures on communications originating outside of a safety division do not propagate to the devices performing the safety function within the division.

References

IEEE Std. 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations", 2010

IEC 61500, "Instrumentation and Control Important to Safety – Data Communication in Systems Performing Category A Functions", 2009

DI&C-ISG-04, "Highly-Integrated Control Rooms – Communications Issues (HICRc)", Rev.1 2009

IEC 60709, "Instrumentation and Control Systems Important to Safety – Separation", Ed2, 2004

IEC 61513, "Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems", Ed1, 2001

APPENDIX B

DESIGN SPECIFIC COMMON POSITIONS

AP1000-01: THE DESIGN AND USE OF EXPLOSIVE - ACTUATED (SQUIB) VALVES IN NUCLEAR POWER PLANTS

EPR-01: COMMON POSITIONS ON THE EPR INSTRUMENTATION AND CONTROLS DESIGN

Date: 3 December 2010
Validity: until next update or archiving
Version 1

MDEP Common Position No AP1000-01

Related to : AP1000 Working Group activities

THE DESIGN AND USE OF EXPLOSIVE - ACTUATED (SQUIB) VALVES IN NUCLEAR POWER PLANTS

Multinational Design Evaluation Program

AP1000 Design Specific Working Group

Squib Valve Subgroup

COMMON POSITION ON THE DESIGN AND USE OF EXPLOSIVE - ACTUATED (SQUIB) VALVES IN NUCLEAR POWER PLANTS

Purpose

To communicate a common position among regulators reviewing squib valve designs in order to:

- Promote and understand each country's regulatory decision and its basis.
- Aid in the assessment of explosive-actuated valves (squib) valves that are used to perform a safety function within a nuclear power plant.

Background

The nuclear industry has a limited amount of experience with the use of squib valves. The available operating experience is typically from small squib valves in the standby liquid control system at boiling water reactor (BWR) nuclear power plants. The design, qualification, procurement, and in-service testing and inspection activities for squib valves to be used in new reactors represent a significant engineering challenge because of their risk and safety importance, large size range, and new design aspects.

A squib valve ensures zero leakage during normal operations by its sealed closure. Actuation occurs by a pyrotechnic process that is triggered by an electric control signal. Actuation of the squib valve results in the shearing of a pipe cap to allow fluid to flow through the valve. Squib valves can be used to depressurize plant systems, or to provide for coolant to flow to the reactor core or containment building. Actuation of a squib valve is a once-only sequence that requires refurbishment to return the valve to service.

Discussion

In the absence of regulatory experience with valves of this type, the regulators participating in the MDEP AP1000 working group (US NRC, UK NII, Canada CNSC, and China NNSA) developed design principles that they believe are required to be considered in the design, qualification, procurement and life management (examination, inspection, testing and maintenance) of a squib valve.

The principles consider: the design process; reliability; margins; integrity; redundancy; diversity; common cause failure; defence in depth; fault tolerance; aging; degradation; obsolescence; and the examination, maintenance, inspection and testing (EMIT) requirements.

The aim of issuing high-level technical guidance on novel aspects that are being introduced to new nuclear power plants, where there is likely to be limited regulatory experience, is to:

- promote a common approach to regulatory assessment and the harmonisation of regulatory standards;
- develop new power plants with the highest level of safety; and
- inform power plant design organisations of the regulators' expectations.

Position

Listed below are the principles that are expected to be considered in the design, qualification, procurement and in-service activities (such as examination, inspection, testing and maintenance) of a squib valve.

1. Evaluate the basis for use of squib valves versus alternative valve types.
2. Identify safety functions.
3. Categorise and classify safety functions.
4. Determine environmental parameters.
5. Specify codes and standards to be satisfied.
6. Evaluate design to perform the safety functions through techniques such as a Failure Modes and Effects Analysis (FMEA).
7. Establish qualification process to support the required reliability for the safety functions.
8. Establish qualified life (operating hours, actuations, shelf life, and any post-accident life).
9. Determine the examination/maintenance/inspection/testing requirements.

Below is a table of examples of information required to support the safety justification for the performance of squib valves to be used in nuclear power plants. The table also identifies, where applicable, design principles, aging/degradation, and EMIT activities relating to the design, qualification, and in-service surveillance, inspection/testing information items.

The table is not intended to provide a complete or exhaustive list of requirements as these can only be determined by the design authority

	Examples of Squib Valve Design, Qualification, and In-Service Inspection/Testing Information	Design Principles							
		Design process	Reliability	Margins	Integrity	Redundancy/ Diversity	Defence in Depth	Aging/ Degradation	EMIT
1	Design process satisfies applicable regulatory requirements	x							
2	Design achieves appropriate seismic categorisation and classification	x	x		x		x		
3	Design achieves appropriate I & C categorisation and classification	x	x		x		x		
4	Design achieves appropriate mechanical and integrity categorisation and classification, taking into account the harsh operating environment and the design life (60 years)	x	x	x	x		x	x	x
5	Safety functions have been identified (including number of explosive firings for which squib valve assembly will be qualified)	x							
6	Valve availability is consistent with its safety function throughout operational life for normal and accident conditions	x	x		x				
7	Valve leakage criteria is within safety limit and consequences adequately considered	x	x	x	x			x	x
8	Actuation logic satisfies safety analysis (including any need for direct actuation from control room)	x	x		x	x	x		
9	Positional indication (remote and local) achieves safety functional requirements, including consideration of position and integrity of internal parts (such as tension bolt and piston)	x	x		x				
10	Design ensures 72 hour post accident life	x	x		x				

No.	Examples of Squib Valve Design, Qualification, and In-Service Inspection/Testing Information	Design Principles							
		Design process	Reliability	Margins	Integrity	Redundancy / Diversity	Defence in Depth	Aging/ Degradati	EMIT
11	Valve opens on demand with single actuation reliability and remains full open without interference	x	x						
12	Spurious opening probability is sufficiently low to satisfy the safety criteria	x	x		x				
13	Pressure retaining parts satisfy recognised nuclear design codes and standards such as ASME Code Section III	x			x				
14	Design considers output from FMEA, other analysis, and relevant experience with independent analysis review	x							
15	Design provides adequate level of diversity and redundancy during the actuation process	x	x			x	x		
16	Comprehensive understanding of the energy distribution during the actuation process and the transfer of energy through the different components or bypassed through the valve	x		x					
17	Comprehensive assessment of the assembled valve components, including tolerances, clearances and fits for the harsh operating environment	x	x	x	x			x	x
18	Comprehensive assessment of the process flow performance and characteristics (including potential water hammer effects), such that the valve adequately opens to achieve the required flow rate	x	x	x				x	x

No.	Examples of Squib Valve Design, Qualification, and In-Service Inspection/Testing Information	Design Principles							
		Design process	**Reliability**	**Margins**	**Integrity**	**Redundancy/ Diversity**	**Defence in Depth**	**Aging/ Degradation**	**EMIT**
19	The actuation loads (forces and moments) that are transferred to the attached piping system (including piping and component supports) are specified to the piping designer to allow consideration of those loads in piping analyses and support design to maintain system, valve, and pipe support integrity following valve actuation	x			x				
20	The as-qualified valve support structure and its anchorages are adequately reflected in the as-installed design	x			x				
21	The maximum loads (forces and moments) from the interfacing piping system onto the squib valve are specified to ensure that the valve's operability is not adversely impacted	x			x				
22	Material selection achieves design and safety intent, including consideration of potential temperature differential expansion e.g. tension bolt shears within a known range, and potential degradation due to boron crystals	x	x	x	x			x	x
23	Design avoids water and debris interfering with the actuation process	x	x						
24	Design allows removal of explosive charge for periodic inspection and replacement	x	x					x	x
25	Design evaluates effects of propellant blow-by into reactor coolant	x							

No.	Examples of Squib Valve Design, Qualification, and In-Service Inspection/Testing Information	Design Principles							
		Design process	Reliability	Margins	Integrity	Redundancy/Diversity	Defence in Depth	Aging/ Degradation	EMIT
26	Establishment of a robust test-based equipment qualification process such as ASME QME-1-2007 and IEEE 323, 344, and 382 as addressed by NRC regulatory guides (that includes consideration of valve orientation and submergence, and performance of sensitivity analyses and testing to address uncertainties in valve design, manufacture, installation, actuator explosive charge, and in-service activities)	x	x	x	x	x	x	x	x
27	Demonstration of material capability: for example, tension bolts that break at necessary load (not prematurely or too high of a load)	x	x	x	x			x	x
28	Design includes adequate provision for installation of squib valve and its supports considering orientation, tolerances and periodic examination, maintenance, inspection and testing activities	x							x
29	Establishment of a robust quality assurance program (such as 10 CFR Part 50, Appendix B) for design, qualification, and in-service testing/inspection activities	x	x						x

No.	Examples of Squib Valve Design, Qualification, and In-Service Inspection/Testing Information	Design Principles							
		Design process	**Reliability**	**Margins**	**Integrity**	**Redundancy/ Diversity**	**Defence in Depth**	**Aging/ Degradation**	**EMIT**
30	Development of a robust surveillance and Examination, Maintenance, Inspection and Testing (EMIT) program that considers ASME Code and other applicable codes as well as lessons learned from design, qualification, and operating experience; and takes into consideration new valve design to obtain sufficient initial performance data to support in-service inspection/testing and periodic in-service maintenance intervals (e.g., EMIT activities should consider periodic visual examination for presence of boron crystals and non-destructive examination for shear cap thinning)	x	x						x
31	Adequate consideration of the effects of aging (e.g. stress corrosive cracking of the shear cap, propellant, seals, valve body, etc) with establishment of applicable replacement intervals	x			x			x	x
32	Design process ensures proper component and parts control and valve replacement activities to prevent incorrect components and parts being installed in similar squib valves	x			x				x
33	Documentation is generated and maintained in an auditable manner describing the design, design development and qualification process, including the analyses and test results, issues identified during the design and qualification process, and corrective action taken to resolve those issues	x			x				

MDEP Common Position No EPR-01

Related to : EPR Working Group activities

COMMON POSITIONS ON THE EPR INSTRUMENTATION AND CONTROLS DESIGN

Multinational Design Evaluation Program

EPR Working Group

EPR Instrumentation and Controls Technical Expert Subgroup

COMMON POSITIONS ON THE EPR INSTRUMENTATION AND CONTROLS DESIGN

Purpose

To identify common positions among the regulators reviewing the EPR Instrumentation and Controls (I&C) Systems in order to:

1. Promote understanding of each country's regulatory decisions and basis for the decisions,
2. Enhance communication among the members and with external stakeholders,
3. Identify areas where harmonization and convergence of regulations, standards, and guidance can be achieved or improved, and
4. Supports standardization of new reactor designs.

Discussion

Since January 2008, the EPR I&C Technical Expert Subgroup (TESG) members met five times to exchange information regarding their country's review of the EPR I&C design. The EPR I&C TESG consists of regulators from China, Canada, Finland, France, the United Kingdom, and the United States. The information exchange includes presentation of each country's review status and technical issues, sharing of guidance documents, and sharing of regulatory decision documents. The TESG focused on the following four core areas of the EPR I&C design:

1. I&C System Independence (particularly for data communications)
2. Level of Defense and Diversity (back-up systems)
3. Qualification/quality of digital platforms
4. Categorization/classification of systems and functions

As meetings were conducted, some areas were emphasized more depending on the significance of the issues for each country. During the TESG interactions, it became apparent that there were aspects of the EPR design where the countries had common agreement. On November 2, 2009, three of the subgroup countries, France, Finland and the United Kingdom, issued a joint regulatory position on the EPR I&C design as result of the Groupe Permanent meeting in France. This statement of common positions expands upon that joint regulatory position.

Positions

1. **The regulators identified differences between the EPR I&C design presented to each country. To the extent possible, regulators will communicate and coordinate regulatory decisions to support standardization of the EPR I&C design.**

At the beginning of each country's review, there was an impression of a standard EPR design. However, as the countries discussed their reviews, it became apparent that there were different EPR I&C designs for Finland, France, the U.K., China, and the U.S. The differences were primarily in the areas of diverse back-up systems, prioritization of commands (priority modules), safety classifications, and the perceived ability of digital platforms to support safety functions. The differences in design are driven by meeting regulatory requirements, customer preferences, and the overall I&C designer's choice.

2. **Design simplicity is a fundamental principle for developing safety systems with high reliability. The regulators recommend that guidance for simplicity be addressed generically through MDEP.**

Design simplicity is a fundamental principle for development of safety/high-reliability systems. However, the regulators have found the EPR I&C architecture and systems to exhibit a high degree of complexity. Much of the complexity arises from the high level of interconnectivity between I&C systems of different divisions and safety classes. It appears there are little to no regulations, standards, or guidance to address the aspect of simplicity because there is no objective definition of simplicity/complexity. Regulators are addressing the specific effects of simplicity/complexity such as testability or proof-of-determinism. The subgroup recommends that the MDEP Digital I&C Issue Working Group consider complexity of digital I&C architecture and systems as a topic to address generically, as the issue will appear in other new reactor reviews.

3. **Independence between systems and divisions is essential to the safety of I&C design, but portions of the original EPR design did not demonstrate adequate independence in data communications. Regulators are addressing data communications independence by requiring safe data communication design practices and thoroughly reviewing the EPR data communication architecture, processes, logic, and information exchange.**

Independence between redundant safety divisions and between I&C system of different safety classes is necessary to ensure a failure in one portion of the I&C system will not prevent the safety function from being accomplished. The EPR I&C design is highly interconnected through data communication links. To ensure adequate independence with data communications, the overall I&C designer (which is not AREVA NP in all cases) must demonstrate electrical and functional isolation, such that either hardware failures or subtle data transmission or timing errors over communication links will not affect one or more safety functions. Portions of the original EPR I&C design did not adequately address these criteria or aspects of the design were found to be non-compliant with the independence principle. The independence issue is a high priority technical issue for each country, and the regulators continue to engage the overall I&C designer to address the issue.

4. **To date, the regulators' assessment of the TELEPERM XS digital platform has not identified any significant design issues. The platform is being used in the highest I&C safety classes.**

The member countries have reviewed the TELEPERM XS platform to various levels of detail. To date, no country has identified any significant issues from their assessments of the platform.

5. **To date, the regulators have not identified significant issues regarding the assessment of the application software used to run on the TELEPERM XS platform; however the assessments are ongoing for all countries.**

The member countries have reviewed the application software used to run on the TELEPERM XS platform to various levels of detail. To date, no country has identified any significant issues from their assessment of the application software they have reviewed.

6. **The design, quality, and qualification of digital devices will influence the safety of plant systems in which they are embedded. The regulators recommend that acceptance criteria for digital devices be addressed generically through MDEP.**

As digital technology gains expanded use in nuclear power reactors, digital devices will appear in plant systems where they have not previously been used. For example, embedded digital devices will be utilized in EPR plant systems such as circuit breakers, diesel generators, and cooling systems. In discussions with the overall I&C designer, each member country acknowledges the use of these embedded digital devices and is engaging the overall I&C designer regarding their design, quality, and qualification. It appears there are little to no regulations, and limited information in standards, or guidance to address the aspect of embedded digital devices. The subgroup recommends that the MDEP Digital I&C Issue Working Group consider embedded digital devices as a topic to address generically as it will appear in other new reactor reviews.

7. **The regulators find back-up systems as an effective means to enhance defense-in-depth of the EPR I&C design.**

The regulators find that each EPR uses some type of back-up system. If the backup systems are sufficiently qualified for the functions they perform and meet applicable regulatory criteria, then they can be effectively used to support defense-in-depth of I&C safety functions.

APPENDIX C

OTHER MDEP PRODUCTS

VICWG-01: MDEP PROTOCOL: WITNESSED AND JOINT VENDOR INSPECTION PROTOCOL

PP-STC-01: MDEP STEERING TECHNICAL COMMITTEE POSITION PAPER ON SAFETY GOALS

MDEP Protocol VICWG-01

Related to: Vendor Inspection Cooperation Working Group activities

MDEP Protocol: Witnessed and Joint Vendor Inspection Protocol

Multi-National Design Evaluation Programme

Vendor Inspection Cooperation Working Group

MDEP PROTOCOL: WITNESSED AND JOINT VENDOR INSPECTION PROTOCOL

1) Background

The MDEP is a unique 10-nation initiative being undertaken by regulators from Canada, China, Finland, France, Japan, Republic of Korea, the Russian Federation, South Africa, the United Kingdom, and the United States with the purposes of cooperating on safety design reviews of new reactors and indentifying opportunities to harmonize and converge on safety licensing review practices and requirements.

The Vendor Inspection Cooperation Working Group (VICWG) is one of the issue-specific working groups that the MDEP members are undertaking with one long term goal of the VICWG being to maximize the use of the results obtained from other regulator's efforts in inspecting vendors. To accomplish this goal, it is vital that the regulators learn about each other's procedures, processes, and regulations. To facilitate the learning process the VICWG is coordinating vendor inspections among the involved regulatory authorities with the purpose of enhancing the understanding of each other's vendor inspection procedures. This programme is administered by the NEA. Involvement in specific inspections provides a number of opportunities for member state regulators to witness other regulators' inspection methods, gain useful information on the quality systems and manufacturing arrangements of specific vendors and where appropriate, actively participate in the inspection.

Throughout this document, for brevity, member states' national nuclear safety regulators are referred to as regulators.

2) Purpose and Scope

The purpose of this protocol is to provide guidance to regulators that wish to carry out vendor inspections or participate in or witness other regulators' vendor inspections. It also provides guidance for the sponsoring regulator with regard to its interactions with inspecting, witnessing or participating regulators.

3) Policy

These arrangements provide regulators with guidance on how to witness or participate in vendor inspections that have been arranged by the sponsoring regulator.

4) Definitions

The following definitions apply to these arrangements and are intended to provide clarity of understanding.

4.1 Host regulator- the regulatory body located in the country in which the inspection is taking place regardless of whether or not it is actually conducting the inspection.

4.2 Joint inspection – an activity in which one regulator conducts an inspection according to its own regulatory framework with the participation of one or more other regulators' inspectors.

4.3 Parallel Inspections – inspections that are carried out at the same time on the same vendor by two or more regulators in accordance with their own inspection framework and procedures.

4.4 Participate – to act as an inspection team member in line with the inspection procedures, or agreed alternatives, of the sponsoring nuclear regulator.

4.5 Sponsoring regulator – the regulatory body that recognises the need for the inspection and formalises this as part of its inspection programme.

4.6 Training – the aspect of familiarisation with and understanding of the specific aspects of the sponsoring regulators' standards, requirements and systems of working to enable effective witnessing or joint participation in the inspection.

4.7 Witness – to observe how the inspection is conducted, to take notes, to attend opening, interim and closing meetings but not to take part in, or directly influence the outcome of the inspection.

4.8 Witnessed inspection – an activity in which a regulator conducts an inspection according to its own regulatory framework and one or more regulators witnesses it.

5) Procedure

5.1 The sponsoring regulator will ascertain from the VICWG integrated inspection schedule the level of interest in witnessing or participating in a specific planned inspection. If there is significant interest the sponsoring regulator will decide, based on need, who will attend and, where necessary, in what capacity. The effectiveness of the inspection should not be compromised by the desire or attempt to involve all the regulatory organisations that have registered an interest.

5.2 Organisations invited to witness should be guided by paragraphs 5.8 to 5.12 of this procedure, whilst those participating in joint inspections should be guided by paragraphs 5.13 to 5.20. The sponsoring regulator should inform those selected to witness or participate of the confirmed dates, location and schedule of the inspection together with the name and contact details of the inspection team leader. Due to the timescales of arranging travel and accommodation (especially international) the sponsoring regulator should inform the interested parties as early as possible of their involvement so that arrangements can be made. Unless otherwise agreed with the sponsoring regulator, interested parties should make their own travel and accommodation arrangements.

5.3 All due consideration should be given to the need of informing the host regulator (even if a non-MDEP regulator) of the planned inspection, consistent with the sponsoring regulator's established framework. There may be instances in which it may not be possible to inform the host regulatory body in a timely manner but the sponsoring regulator should keep in mind that informing the host regulatory body may facilitate conduct of the inspection.

5.4 Prior to any firm arrangements being made the sponsoring regulator will inform the vendor of the proposed involvement of the interested parties and, where necessary obtain permission for their presence. Where agreement is not given the sponsoring regulator will inform the interested party(ies) and, where provided by the vendor, will explain the reason for the decision.

5.5 The sponsoring regulator will determine in its normal consultations with the vendor the language in which the inspection will be conducted. In general it is expected that the language will be either the language spoken by the sponsoring regulator and/or the language spoken by the vendor being inspected. In any case, the sponsoring regulator, in accordance with its normal procedures, will determine the translation resources that it needs to conduct its inspection. The sponsoring regulator will inform other invited regulatory bodies of the arrangements that it has made with regard to the language of the inspection and any translation services. Any other regulatory bodies that need additional translation sources should discuss this with the sponsoring regulator and should NOT pose any unnecessary burden on the vendor.

5.6 Care should be taken not to release any sensitive or proprietary information.

5.7 The participating countries may use the information gained during the inspection to increase their knowledge of the vendor to inform future inspection activities.

Witnessed Inspections

5.8 For those witnessing the inspection, they should take their own notes and, as appropriate, attend opening, interim and closing meetings and, receive a copy of the final report. They, however, should not take part in, or directly influence the outcome of the inspection. The control, storage and disposal of notes should be as specified by the sponsoring regulator.

5.9 Witnessing inspectors, using discretion, may ask questions of the vendor to aid their understanding and can discuss issues with the inspection team at planned meetings. Additional involvement by witnessing inspectors can be agreed at the time of the inspection with the agreement of all parties.

5.10 In addition to gaining information about the vendor's organisation and procedures the witnessing inspector should also take note of the sponsoring regulator's inspection processes, with the intention of comparing/sharing inspection practices.

5.11 Following the inspection, witnessing inspectors should prepare a record of their involvement (one per regulatory body) and send copies to the sponsoring regulator and the NEA MDEP library. Information relating to inspection processes is of particular interest. Care must be taken not to include in the report information that may be commercially sensitive with respect to the vendor's organisation.

5.12 An acknowledgement of the presence of the witnessing inspectors will be made in the sponsoring regulator's inspection report.

Joint Inspections

5.13 The sponsoring regulator will inform the vendor of the participation of other regulators and explain to the vendor the latter's role, inspection scope and the benefits of participation. Should the vendor object to the involvement of a particular regulator(s) the sponsoring regulator will inform the interested party(ies) accordingly.

5.14 Regulators participating in inspections should follow the sponsoring regulator's inspection methodology. These arrangements will necessitate prior discussions and planning sessions between the sponsoring regulator and the other participating regulators. The sponsoring regulator will supply the other participating regulators with its inspection arrangements appropriate to the nature and scope of the inspection in sufficient time to allow those involved to study the arrangements.

5.15 The inspection programme, duration and scope will be developed by the sponsoring regulator and shared with the other participants accordingly. The sponsoring regulator will indicate the control, storage and disposal requirements for these documents.

5.16 Unless otherwise agreed the sponsoring regulator's inspection team leader will manage the team and act as spokesperson for the team.

5.17 The participating regulators will carry out their inspection duties in a manner consistent with that of the personnel of the sponsoring regulator. All findings identified by the participating regulator will be agreed by the sponsoring regulator's team leader.

5.18 Participating regulators will prepare a record of their involvement in the inspection and forward contributions for the inspection report to the sponsoring regulator's team leader. Participating regulators may be asked to comment on the draft report and will receive a copy of the final inspection report.

5.19 The responsibility for subsequent monitoring of the closeout of corrective actions placed on the vendor will rest with the sponsoring regulator. The sponsoring regulator may inform the participating regulators periodically of its monitoring of the vendor's progress to close out the corrective actions.

5.20 Participating inspectors should comply with the policies and guidelines of the sponsoring regulatory authority with respect to interactions with the inspected vendor.

5.21 Joint inspections may be witnessed by other MDEP VICWG regulators as this would be a very good opportunity for some of the regulators to observe the conduct of a joint inspection.

Training

5.22 The extent of required training, or familiarisation of persons witnessing or participating in joint inspections, should be considered on a case by case basis following appropriate discussions between the sponsoring regulator and the persons witnessing or participating jointly. In all cases, the sponsoring regulator shall make the final decision on the level of training required.

5.23 The specific requirements of this protocol and any information confidentiality requirements should be included as part of the training given.

6) Records

The sponsoring regulator will ensure that the formal records of the inspection are retained in accordance with the sponsoring regulator's requirements. It is encouraged that the sponsoring regulator provides the inspection report to the MDEP technical secretariat staff for inclusion in the MDEP library. Those regulators observing or participating will retain whatever records they require as part of their arrangements. It is anticipated that the following will be included in the inspection record of the sponsoring regulator;

1) Inspection scope and programme.

2) Final inspection report.

3) Corrective Actions (proposals, correspondance etc.) in the case of joint inspections. (NOTE : Vendor's responses to the sponsoring regulator regarding corrective actions may be considered for inclusion in the NEA MDEP library but, based on the potentially sensitive nature of the documents,

may not be appropriate for inclusion in the library. The sponsoring regulator will decide which documents should be placed in the NEA MDEP library.)

Regarding input and feedback from witnessing regulators, it is recommended that witnessing regulators document their observations of the witnessed inspection as a short report, and provide this for inclusion in the MDEP library. This report should have particular emphasis on the process of inspection as compared to that of the witnessing inspector's own organisation. This will assist in the identification of any significant differences in process and approach of the different regulators.

MDEP Position Paper PP-STC-01

Related to: STC's subcommittee on Safety Goals activities

MDEP Steering Technical Committee Position Paper on Safety Goals

Multi-National Design Evaluation Programme

Steering Technical Committee

1. **MDEP expects that higher levels of safety will be achieved in the design and operation of new reactors.**
2. **MDEP strongly supports the structure of safety goals and targets, as set out in this paper, for consideration of its members and IAEA and other organisations, in moving towards international harmonisation of regulatory requirements;**
3. **MDEP strongly supports the use of integrated decision-making for design evaluation and operational safety**
4. **MDEP recognises the need to develop the process, through continued interactions with other international organisations, to further harmonise regulatory requirements**.

1) Background

In considering the acceptability of a nuclear facility in relation to safety, Governments and regulatory bodies define a range of legal, mandatory requirements which are supplemented by regulatory requirements and expectations which may not have a mandatory nature. The term "safety goals" is used to cover all health and safety requirements and expectations which must be met: these may be deterministic rules and/or probabilistic targets. They should cover the safety of workers, public and the environment in line with the IAEA's Basic Safety Objective[1] encompassing safety in normal operation through to severe plant states.

Although all regulators have safety goals, these are expressed in many different ways and exercises in comparing them frequently are done at a very low level e.g. specific temperature limits in the reactor core. The differences in the requirements from different regulators are difficult to resolve as the goals are derived using different principles and assumptions and are usually for a specific technology. Therefore MDEP set up a sub-committee to investigate a different approach. This approach was to start with the high level safety goals and try to derive a structure and means of deriving lower level safety goals that can be seen to be clearly related to the higher level ones. The work will greatly assist in the process of harmonisation of regulatory requirements and enhance coherence and consistency between goals for different technologies.

2) Fundamental Requirement

It is recognized that the fundamental basis for protecting the health and safety of the workers and the public as well as protection of the environment, requires that normal exposures and discharges are controlled, accidents are prevented and should they occur, mitigation measures are provided to protect people and the environment by limiting any radiological releases.

[1] IAEA Fundamental Safety Principles, SF-1, 2006

Many countries considered in this position paper subscribe to the view that operation of NPP should only add insignificantly to the risks to which the population is exposed and in many cases this is based on 1% or 0.1% of risks of death of individuals or cancer. The safety goals and targets developed to meet these requirements usually cover normal operational exposures of workers, radioactive emissions and discharges to the environment as well as accidents. Although many safety goals and targets are based on the effects on individuals, all countries recognise that the consequences of a nuclear accident can affect wider societal aspects such as effects on use of land or food production.

In the following sections a structure for developing safety goals and targets, which can be applied to different technologies in a consistent and coherent manner, is proposed.

3) Defence-in-Depth

All countries utilize a Defence-In-Depth (DID) concept, which has proved to be a useful concept for considering deterministic safety requirements and the reliability of safety systems. However, some explicit and implicit probabilistic risk considerations were used. These included: dividing the design basis faults into groups according to frequency with different acceptable consequences and the use of engineering safety margins, which had been determined heuristically. Different approaches were used in different countries, with some making greater use of formal risk analyses than others, but in all cases, a DID philosophy, centred on several levels of protection including successive barriers and conservative considerations to prevent the release of radioactive material to the environment, was, and still, is employed. Increasingly, the techniques of Probabilistic Safety Assessment (PSA) [sometimes referred to as Probabilistic Risk Assessment (PRA)], which explicitly consider the possible faults, accident sequences and their likelihoods and consequences, are used to develop risk metrics and insights.

4) Hierarchy of Safety Goals: Extended DID Approach

To achieve a balanced view on applying the full suite of safety goals and targets they should be considered within a structure that encompasses the basic DID approach. It is proposed here that the established form of DID structure should be extended to include a wider range of elements, including both deterministic and probabilistic safety goals and targets. The figure sets out an Hierarchical Structure for Safety Goals, with a top level safety goal and a set of high level safety goals, that can be used to integrate the elements of safety desired to protect health and safety during normal operation and accident conditions for the whole plant lifecycle. The high level safety goals need to be developed, in a coherent and consistent manner, into lower level safety goals and targets that can be applied within the design and operation of reactors, with a clear connection between the different levels. This structured approach is technology-neutral and is sufficiently flexible that it can be used for developing and applying safety targets to water-cooled and non-water cooled reactor designs.

Both qualitative and quantitative safety goals and targets are necessary in developing a technology-neutral approach and the difference between safety goals and targets, as used in this paper, should be understood. Goals are generally qualitative, or define upper limits, and set out what has to be achieved. Targets, which are usually quantitative and developed from the goals, set out the measure of achievement. Safety cases should address the way the goals have been achieved: failure to address all of the goals could result in regulatory enforcement. Failure to meet a target must be justified and may result in regulatory enforcement; failure to do better than a target must be explained.

It is a generally agreed aim that there should be a continual aim of improving safety, building on the current high levels. The following goals have been developed to ensure that higher levels of safety will be achieved in the design and operation of new and future reactors:

4.1) *Top-level Safety Goal*

Provide a level of safety such that the risks to people and environment from the whole lifecycle of a nuclear power plant is only a small fraction of the risks from other hazards to which these are otherwise subjected.

Figure: Hierarchical Structure of Safety Goals and Targets

4.2) High level DID goals

1. Occupational and public dose during normal operation, should be as low as reasonably achievable (ALARA[2]) and below regulatory limits, consistent with the IAEA Basic Safety Standard, which is derived largely from the ICRP recommendations.

2. Prevention should be the focus by designing for fault tolerance through application of good engineering principles.

3. For all accident sequences taken into account in the design basis, there should be no offsite effects and no significant onsite doses for workers, as far as reasonably practicable3.

4. The frequency of large offsite releases due to accidents should be as low as reasonably practicable.

5. Any offsite releases that could occur should only require limited offsite emergency response.

[2] In applying the ALARA concept, social and economic factors should be taken into account.

[3] "reasonable practicability" requires a comparison of the sacrifice (time, trouble and money) in implementing a safety measure with the risk averted by its implementation.

4.3) Extended DID high level goals

I. Integration of safety and security measures should ensure that neither compromises the other.

II. Siting factors, in addition to being considered within the design should also be taken into account in considering emergency arrangements.

III. Where improving safety is, or over the lifetime of the plant becomes reasonably practicable, then this improvement should be implemented.

IV. Where an exposure occurs, the likelihood should decrease as the potential magnitude increases.

V. Independence of the barriers and systems that form the protection at the different DID levels is a fundamental aspect of the safety concept, which should be ensured and enhanced in new and future reactors, as far as practicable.

VI. Consideration of the management of radioactive waste during the design and operation and decommissioning phases of the reactor lifetime should be such that the generation of waste is minimized.

VII. Arrangements to ensure effective management of safety should be made at all lifecycle phases of a reactor.

VIII. Arrangements to make future decommissioning easier should be considered at all stages of the reactor lifecycle including the design stage.

5) Developing Lower Level Safety Goals and Targets

Some examples of how the framework can be developed to the lower level safety goals and targets, both qualitative and quantitative, are given in the following paragraphs. Lower level goals and targets for existing technology have been developed for many years and can be seen to fit into the extended DID framework. It is recommended that this approach is extended to new reactors and other technologies. Further work, building on experience from the existing technologies to develop more detailed lower level goals and targets that can be considered within the MDEP group, would be valuable before involvement with the IAEA Safety Standard development.

5.1) Defence-in-Depth

The implementation of DID is centred on the use of several barriers (usually physical) to prevent the release of radioactive material or radiation shine. It is fundamental to the DID approach that the level of independence between the barriers should be as high as possible; therefore the deterministic engineering and safety concepts of redundancy, diversity, separation and segregation must be applied during development of the design. These should ensure, as far as possible, that failure or damage to one barrier should not result in failure or damage to another. Should a barrier fail or be damaged it is essential that this is revealed to the operators. By carrying out a design basis and severe plant state analysis, the ability of the design to meet the requirements of DID should be demonstrated.

5.2) Normal Operation

Safety in normal operation due to worker (or other persons on site) exposure or discharges to the public is usually expressed as a dose limit with the requirement to further reduce them using ALARA principle. This approach is based on the IAEA's Basic Safety Standard (op cit) which is itself based on the recommendations of the ICRP

5.3) Accident Prevention

There is broad international consensus that prevention of accidents is the first means of protection. The following have been considered in relation to new water-cooled reactor designs safety targets for accidents (assuming a single reactor on a site):

- WENRA propose that the potential for escalation to accident situations for new NPP should be reduced by enhancing the capability to control abnormal events
- An NEA survey (WGRisk Task (2006)-2 - Probabilistic Risk Criteria) showed, in general, a core damage frequency target of 1 E-5 per reactor year is being applied for new reactors, by most countries which use this metric (cf 1 E-4 per reactor year for most current applications).
- The same NEA survey showed that large offsite releases should be either "practically eliminated" or must be of a very low frequency, typically figures of 1 E-6 to 1 E-7 per reactor year are used for this metric.

5.4) Accident mitigation

Albeit that the first means of protection is prevention, it is not possible to ensure the elimination of accidents completely, hence, designers should also include features to minimise the potential for large releases. The following have been considered in relation to new water-cooled reactor designs safety targets for accidents (assuming a single reactor on site):

- All countries propose that, for new reactors, offsite radioactive releases should be reduced to a low level (i.e. the ALARA concept).
- WENRA have suggested that limited off site emergency response could be defined "no permanent relocation, no need for emergency evacuation outside immediate vicinity of the plant, limited sheltering, no long term restrictions in food consumption".
- Ensuring containment integrity for the more likely accident scenarios will provide protection from accidents that could lead to early containment failure and sufficient time to plan and implement any additional accident management measures.

5.5) Continual Improvement

As noted, it is generally agreed that there should be continual effort to make reasonably practical safety improvements, building on the current high levels. On the basis of extensive Level 3 PSA studies, it is apparent that adoption of the proposed goals and targets for limiting radioactive releases and core damage likelihood will, respectively, promote reducing risks to public health and safety to a very small fraction of other risks and a high focus on preventing accidents. However, improvement should not be limited to the initial design considerations. Where improving safety beyond the goals is, or over the lifetime of the plant becomes, feasible at reasonable cost, this improvement should be implemented.

5.6) Frequency-Consequence Curves

Considerable effort is underway, as part of Gen-IV and other initiatives, to develop significantly different NPP designs than the current water reactor designs. It is important to develop safety goals to allow full up front consideration of the above safety objectives in these developing designs. A frequency-consequence (F-C) curve specifies low doses for high frequency events with larger allowable doses for lower frequency events. Doses should be consistent with international standards and calculated so as to correspond to the maximum dose any member of the public could receive from an individual event. The curve should ensure that various elements of the proposed probabilistic goals will remain internally consistent. This concept is independent of any specific nuclear power plant design technology. This curve can also support the siting and emergency planning policy decisions. This F-C concept can also be applied to establish the level of safety for water cooled designs but there is limited experience with such an application.

5.7) Technology Specific Safety Goals and Targets

The development and application of technology specific safety goals and targets are the responsibility of the designers/operators of the plant and this is not the subject of this paper. However, any proposed goals and targets adopted in the design process should be clearly derived from higher levels in the hierarchy. The design approach should include a demonstration that it is capable of meeting and complying with all the safety goals and targets in the hierarchy.

6) Integrated Decision-making

All countries have established occupational and public dose limits during normal operation, and these generally conform to the IAEA Basic Safety Standard[4], which is derived largely from the ICRP recommendations. In addition, all countries have developed deterministic goals in relation to accidents and many have also developed probabilistic targets (in the form of risk metrics which are expressed as frequencies of fatalities, doses, and core damage or release quantities). In the past, combining these into a single decision-making process has typically not been carried out in a formal, systematic manner.

The more recent development of integrated risk-informed decision making provides a systematic process taking into account all major considerations affecting safety, to achieve a balanced safety decision. In this context, risk should be considered to cover the whole range of safety concerns from normal operational exposure through to severe accidents. A recent report by INSAG on integrated risk-informed decision-making is summarised in the annex.

[4] IAEA Safety Series 115 (In revision as DS 379)

Annex

INSAG-25, "A Framework for Integrated Risk-Informed Decision-Making Process" (about to be published)

The report states in its preamble:

"There is general international agreement, as reflected in various IAEA Safety Standards for nuclear reactor design and operation, that both deterministic and probabilistic analyses provide insights, perspective, comprehension, and balance to reactor safety. Accordingly, the spectrum of applications for integration of these approaches continues to increase. Such applications support design, construction, safety assessment, licensing, operation, and regulatory oversight. Additionally, applications related to physical security are now being considered by member states.

Increasingly there is interest in using a structured framework for optimal decisions, which is based on taking account of deterministic and probabilistic techniques and findings. It is timely, therefore, to establish international good practice on the balance between deterministic approach, Probabilistic Risk Analysis (PRA), and other factors, in an integrated decision making process for ensuring nuclear safety…"

INSAG 25 states that risk-informed decision-making applications must satisfy the following objectives:

- Relevant regulations are met;
- Defence-in-depth is maintained;
- Safety margins are maintained;
- Engineering and organizational good practices are taken into account;
- Insights from relevant operating experience, research and advances in methodologies are taken into account;
- An adequate integration of safety and security is established.

The INSAG report considers a wide range of deterministic and probabilistic elements that should be included in an integrated risk-informed decision-making process. It sets out a methodology for integrating these elements to ensure a balanced, high level of safety is achieved. The integration of the elements is part of an iterative process, which can result in the identification of new design/licensing basis events and criteria for deterministic safety classification of structures, systems, and components as a result of risk insights.

The key elements are considered under the following headings:

- Standards and Good Practice
- Deterministic Considerations: Safety Criteria, Defence-in-Depth, Safety Margins
- Probabilistic Considerations: Probabilistic targets; PSA Quality and Scope
- Organisational Considerations: Management Systems, Operational Experience, Training and Procedures
- Other Considerations: Radiation Doses, Economic Factors, Research Factors
- Security Considerations

The integrated decision making process is based on understanding the strengths and limitations of probabilistic and deterministic analyses. The results of applying these methods of analysis can be compared with quantitative safety goals, but it is recognized that security threats, organizational factors and areas such as software reliability are difficult to quantify and therefore the decisions cannot solely be based on quantitative estimates. To utilise the integrated process, it is necessary to determine a suitable set of safety goals and targets of the sort proposed in the main text.

Table of acronyms

AP1000 WG	*Advanced Pressurised Reactor Working Group (MDEP)*
AFCEN	*French Society for Design and Construction and in-Service Inspection Rules / Association Française pour les règles de Conception, de construction et de surveillance en exploitation des matériels des Chaudières Electro Nucléaires*
ASME	*American Society of Mechanical Engineers*
CNRA	*Committee on Nuclear Regulation (NEA)*
CNSC	*Canadian Nuclear Safety Commission*
CORDEL	*Co-operation in Reactor Design Evlatuion and Licensing*
CSA	*Canadian Standards Association*
CSWG	*Codes and Standards Working Group (MDEP)*
DI&C	*Digital Instrumentation and Control*
DICWG	*Digital Instrumentation and Control Working Group (MDEP)*
EDF	*Electricity of France/Electricité de France*
EPR	*Evolutionary Pressurised Reactor*
EPRWG	*Evolutionary Pressurised Reactor Working Group (MDEP)*
GIF	*Generation IV international Forum*
GSR-3	*IAEA Safety Standards/the Management System for Facilities and Activities/Safety Requirements*
IAEA	*International Atomic Energy Agency*
I&C	*Instrumentation and Controls*
IEC	*International Electro-technical Commisstion*
IEEE	*Institute of Electrical and Electronics Engineers*
INSAG	*International Nuclear Safety Group*
ISO	*International Standards Organisation*
JSME	*Japan society of Mechanical Engineering*
KEA	*Korean Electronic Association*
KEPIC	*Korea Electric Power Industry*
MDEP	*Multinational Design Evaluation Programme*
MHI	*Mitsubishi Heavy Industries*
NEA	*Nuclear Energy Agency*
NII	*Nuclear Installations Inspectorate (United Kingdom)*

NIKIET	*Russian Research and Development Institute of Power Engineering*
NNSA	*National Nuclear Safety Agency (China)*
NPEC	*Nulcear Power Engineering Committee*
NRC	*Nuclear Regulatory Commission (United States)*
OECD	*Organisation for Economic Co-operation and Development*
OL3	*Olkiluoto-3*
PNAE G-7	*Russian Rules for Deisgn and Safety Operation of Equipment and Piping of Nuclear Installations*
PG	*Policy Group (MDEP)*
PSA	*Probabilistic Safety Assessment*
QA	*Quality Assurance*
RCC-M	*Design and Construction Rules for Mechanical Components of PWR Nuclear de Conception et de Construction des Matériels mécaniques des îlots nucléaires des REP*
RHWG	*Reactor Harmonisation Working Group*
RSWG	*Risk Safety WorkingGroup*
SDO	*Standards Development Organisations*
S-NCI	*Japanese Standards for Nuclear Power Generation Equipment: Design and Construction Standards*
STC	*Steering Technical Committee (MDEP)*
STUK	*Finnish Nuclear Regulatory Authority*
TOR	*Terms of Reference*
VICWG	*Vendor Inspection Co-operation Working Group*
WENRA	*Western European Nuclear Regulators Association*
WNA	*World Nuclear Association*
WGRNR	*Working Group on the Regulation of New Reactors (NEA)*

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 34 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1 February 1958. Current NEA membership consists of 29 OECD member countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, the Republic of Korea, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission 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 the 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.

Corrigenda to OECD publications may be found online at: *www.oecd.org/publishing/corrigenda*.

Photo credits for cover: OL3, Finland (TVO) Flamanville-3, France (EDF). AP1000 Sanmen, China (SNMPC 2010). Page 6: Policy Group meeting, Nuclear Regulatory Commission, United States (NRC). Page 9: MDEP Steering Technical Committee. Page 17: Taishan EPR under construction (EPRWG). Page 18: Flamanville-3, France (EDF). Page 21: AP1000 Sanmen, China (SNMPC 2010). Page 23: OL3, Finland (TVO) Page 27: MDEP Digital I & C Working Group. Back Cover: AP1000 Sanmen, China (SNMPC 2010), OL3, Finland (TVO), Flamanville-3, France (EDF)

OECD Nuclear Energy Agency
Le Seine Saint-Germain – 12 Boulevard des Iles
F-92130 Issy-les-Moulneaux, France
www.oecd-nea.org/mdep