

JUNE 11, 1996

FOR: The Commissioners  
 FROM: James M. Taylor /s/  
 Executive Director for Operations  
 SUBJECT: NRC PLANS TO PARTICIPATE IN THE OECD HALDEN REACTOR PROJECT DURING 1997-1999

- PURPOSE:
- SUMMARY:
- BACKGROUND:
- DISCUSSION:
  - Emerging Technology:
  - NAS Issues:
  - Lessons Learned:
  - Fuel Behavior:
  - Materials Performance:
  - Products From Work at HRP During 1994-1996:
  - Plans for Work at HRP during 1997-1999:
  - NRC Participation in 1997-1999 Halden Program:
- CONCLUSIONS:

#### PURPOSE:

To inform the Commission on the results of past participation in the OECD Halden Reactor Project and plans to continue participation during 1997-1999.

#### SUMMARY:

The NRC has participated in the OECD Halden Reactor Project since 1958. During this period, the NRC has received the benefit of numerous research products from this internationally funded cooperative effort. The NRC uses Halden generated products and information and transforms them into analytical tools and regulatory guidance through staff work in response to user needs. The staff plans to continue participation in the 1997-1999 Agreement period because of the benefits received and the leverage of resources by participation with 14 signature and 7 associate members representing 19 countries.

The cost of participation has been about \$800,000 per year during the 1994-1996 agreement period. Based upon renewed interest in the high-burnup fuels program, we anticipate that our yearly fee will increase by about \$400,000 per year. Although the funds are included in the RES budget, this decision may need to be revisited if there are significant budget reductions.

The benefits derived from past and continued participation in the OECD Halden Reactor Project include:

1. Products that form part of the technical bases for the development of new Regulatory Guides on software quality and life cycle, and review guidance such as revisions of the Standard Review Plan (Chapters 7 and 18) in the areas of advanced instrumentation and controls, man-machine interfaces, software quality assurance, and advanced control room design reviews.
2. A facility (Halden Man-Machine Laboratory) and highly qualified staff to conduct human factors research and experiments with computer driven interfaces in direct response to user needs.
3. Test, evaluation, and development information on new and emerging instrumentation and control (I&C) technology.
4. Qualified data on fuel properties changes during service relevant to safety analyses and licensing, especially in the high burn-up range.
5. Access to an irradiation facility suitable for studies on materials degradation.
6. A forum for international cooperation and information exchange.
7. International cooperative funding which provides leverage for NRC research funds.

#### BACKGROUND:

The OECD Halden Reactor Project (HRP) is an internationally funded and staffed nuclear research and development organization located in Halden, Norway. Included in the facilities at the Halden Reactor Project is the Halden Boiling Water Reactor which currently operates at 18 to 20 Megawatts and is contained within a mountain. Norwegian authorities have given clear support to continued long term operation of the reactor. The reactor is fully dedicated to instrumented in-reactor testing of fuel and core materials behavior. It still delivers steam to a nearby paper factory, the purpose for which it was originally built.

The research programs at the Halden Project address: 1) nuclear fuels and materials performance, and 2) man-machine system development and qualification. The programs are structured to respond to the needs of member organizations within the international nuclear community. Since initial startup, the reactor facility has been progressively updated and has now become one of the most versatile test reactors in the world. In the course of this development, over 300 in-reactor experiments have been performed.

The OECD Halden Reactor Project also maintains one of the most comprehensive facilities and research staff in the world for performing experimental research on issues regarding the human-system interfaces for advanced technology in nuclear power plant control rooms. The Halden Man-Machine Laboratory (HAMMLAB) contains a full scope PWR simulator, a modifiable CRT-based operator interface, and an extensive automated system for recording and analyzing experimental data. In addition, Halden has developed, maintains, and continually supplements a set of advanced computerized operator support systems for control rooms. HAMMLAB provides an extensive test bed for performing experimental studies of operator performance using advanced technology. The HAMMLAB includes a prototype advanced control room, the Integrated Surveillance and Control System, which is used as a test bed for exploring human-machine issues regarding the role of the operator and interactions with controls and automation.

The HRP conducts research to assure and enhance the quality of computer-based systems. The research addresses topics covering various types of instrumentation and control systems as well as all the life cycle phases of I&C systems. The development and application of both formal and conventional methods to verify and validate high integrity software are also subjects of research at the Project.

The fuels and materials program at the HRP has become the preeminent program in the world with advanced in-reactor instrumentation and test methods and with an energetic scientific staff.

The international organizations actively participating in the HRP represent a complete cross section of the nuclear industry consisting of licensing and regulatory interests, national research organizations, reactor and fuel vendors, and utilities. [Attachment 1](#) contains a list of the current members of the OECD Halden Reactor Project. [Attachment 1](#) also contains background information on the Steering Bodies for the HRP as well as a discussion of the Project's budget.

The results from the research conducted at Halden are distributed to the signatory members in the form of technical reports. In the man-machine systems research area, Halden publishes on the order of 15-20 reports per year. There are also two workshop meetings per year on specific topics for man-machine systems research. Every 18 months, Halden conducts an Enlarged Halden Program Group Meeting. At these meetings, research results are presented from programs at Halden as well as from member countries. This provides the attendees with a window to international activities on digital instrumentation and control system safety and reliability issues as well as human factors issues associated with computer-driven interfaces.

The HRP's experimental program is conducted in two ways. The first is a jointly agreed upon program of work (by members of the Project) over 3-year periods which is called the Joint Program. All data and information generated from the Joint Program are available to the Halden Project members for their use. These products are obtained with a leverage of NRC research funds since the Joint Program is funded by the members of the Project collectively.

The second way to conduct an experimental program under the provisions of the overall agreement is by bi-lateral contracts with a member organization as a sponsor. These are funded entirely by the sponsor and the data are only disclosed to other Project members at the sponsor's discretion.

The HRP has, through its long operation, proven to be highly versatile and responsive to changes of R&D needs. It is a relatively small and non-bureaucratic operation where recommendations and priorities by members are accommodated in a flexible manner.

## **DISCUSSION:**

### **Emerging Technology:**

Digital instrumentation and control system designs are being proposed for commercial nuclear power plants and for medical treatments that use radioisotopes. Digital systems are being proposed for protection and control systems in all advanced reactor designs. Past experience, standards, and regulatory requirements have been primarily based on analog hard-wired systems. The NRC has programs underway directed at updating the staff's standard review plan for digital technology and reviewing existing standards for endorsement by Regulatory Guides.

Furthermore, digital technology is advancing rapidly, which is compounding the need for new standards, acceptance criteria, and associated technical bases. This new technology brings with it new benefits and the potential for new failure modes. There is a need for continuing research on safety issues related to digital instrumentation and controls as well as a periodic re-assessment of the state-of-the-art. The HRP assists in meeting that need and provides a means to assist in the development of a technical basis for digital instrumentation and control because of its research facilities, programs, and member organizations interested in the development and regulation of the technology.

### **NAS Issues:**

The NRC has contracted with the National Academy of Sciences for a study of the safety and reliability issues for digital instrumentation and control systems in nuclear power plants. This study includes both operating plants and advanced reactor designs during normal, transient, and accident conditions. Although the NRC is primarily interested in issues related to hardware and software, important human-machine interface issues which could affect overall system/plant safety and reliability are also of interest.

A Phase I report titled, "Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues," was published by the National Academy Press in September 1995. The study defined six technical issues: 1) software quality assurance, 2) common-mode software failure potential, 3) system aspects of digital I&C technology, 4) human-factors and human-machine interfaces, 5) safety and reliability assessment methods, and 6) dedication of commercial off-the-shelf hardware and software. Two non-technical issues were also defined dealing with NRC procedures.

In Phase II of the study, these issues will be evaluated in detail and a final report is scheduled for September 1996. We anticipate the final report will contain research recommendations; the HRP is already addressing the six technical issues and is expected to be instrumental in conducting a large portion of the research because of the relevance of the technical issues to the work conducted by Halden.

### **Lessons Learned:**

Halden also provides the NRC with access to design and development information that are otherwise difficult for regulators to obtain. In developing PICASSO, a user interface management system, Halden gained practical experience with a software life cycle in the design, test, and quality assurance of the system. The lessons learned from this and other software programs at Halden have been documented in lessons learned reports and forwarded to the NRC. [Attachment 2](#) contains a summary of the lessons learned reports to date.

### **Fuel Behavior:**

In the early 1980s, the NRC de-emphasized its research and licensing reviews in the area of fuel behavior and did not actively follow the Halden Project's fuels and materials work. Nevertheless, experimental work at Halden continued to explore the regime of higher burnup, and those results were made available to the NRC. With the NRC's recent interest in high-burnup operation, these results are now being used to update NRC's analytical codes (e.g., FRAPCON) and to support licensing reviews for extended burnup. With a continuing interest in high-burnup operation and a modest rebuilding of NRC's capabilities in this area, active participation is anticipated in Halden's fuels and materials program in the 1997-1999 period.

## Materials Performance:

NRC has an extensive research program whose goal is to provide an independent understanding of irradiation assisted stress corrosion cracking (IASCC) of core internals sufficient to permit reliable assessments of licensee submittals concerning such issues as residual life, inspection intervals, and replacement/mitigation strategies. The IASCC research is being performed at Argonne National Laboratory. The Argonne test program relies on Halden to irradiate specimens of known, prespecified chemistry to known, prespecified fluences. The tests done on these specimens provide important input to the Argonne program, and Halden's participation is especially important because it is not possible to obtain the required irradiations at reasonable cost in the U.S. Participation in the Halden Reactor Project has provided resource leverage for research important to licensing. The Halden work on materials performance will be extended in the 1997-1999 period to cover the pressure vessel embrittlement issue.

## Products From Work at HRP During 1994-1996:

SECY-93-203 identified and discussed the four main elements of the 1994-1996 HRP research program. The elements are:

1. Verification and validation of software
2. Man-machine interaction research
3. Surveillance and support systems
4. Advanced control rooms

Two examples of products from this research program and their use at the NRC are presented next. Additional details on research products and the NRC's use of them are presented in [Attachment 3](#).

Data and results from Halden experiments, for example statistical testing, were used as part of the development of NUREG/CR-6293, "Verification and Validation Guidelines for High Integrity Systems, Main Report," which discusses many software issues and provides conclusions and recommendations on each issue. The objective was to develop guidelines to evaluate the adequacy of a validation program. The guidelines address subjects such as: 1) the type and amount of testing necessary, and 2) acceptance criteria for each test method and technique to detect unintended functions. The HRP research results could also be directly applied in the conduct of safety evaluations of software that contains commercial off-the-shelf software where unintended functions may exist.

The HRP has extensive experience in designing and evaluating alarm systems. They have developed technical information from which NRC contractors drew while working on the development of "Human Factors Engineering Guidance for the Review of Advanced Alarm Systems," NUREG/CR-6105. The development of NUREG/CR-6105 also allowed the staff to close-out Generic Issue HF 5.2 on Annunciators. The guidance from NUREG/CR-6105 is used by the staff to review licensee digital upgrades to existing control rooms and for review of advanced reactor control stations.

## Plans for Work at HRP during 1997-1999:

The NRC staff met with members of the HRP staff on October 20, 1995, to begin discussions of the next 3-year program as proposed in the draft report, "Halden Reactor Project Program, Proposal for the 3-Year Period, 1997-1999." This report contains proposals for research and development programs on:

1. Man-machine systems research
2. High burn-up fuel performance, safety and reliability
3. Degradation of in-core materials and water chemistry effects

## NRC Participation in 1997-1999 Halden Program:

The cost of participating in the HRP has been about \$800,000 per year during the 1994-1996 agreement period. This fee was reduced relative to other members of the Halden Project because NRC's primary interest has been with the man-machine research portion of the program, with no formal participation in the fuels program. However, the NRC has renewed its interest in the fuels research at Halden and plans to participate in these activities during the 1997-1999 agreement period. Based on this renewed interest, we anticipate that our yearly membership fee will increase over the current amount by approximately \$400K in FYs 1997-1999 for a total of approximately \$1.2M/yr. Although these additional funds are included in the RES budget, this decision may need to be revisited if these are significant budget reductions. The NRC plans to discuss and negotiate a fee with the Halden Project during calendar year 1996.

The impact of discontinuing membership in the Halden Project would result in many losses, including:

1. Man-machine research results useful as technical basis in the development of guidelines and possibly regulations.
2. State-of-the-art appraisals on software and man-machine interfaces.
3. Use of the Halden Man-Machine Laboratory for experimental studies; an equivalent facility to conduct human factors experiments for nuclear power plant control room interfaces does not exist in the United States.
4. A source of human error data and, potentially, human reliability data.
5. Continued maintenance and upgrades to the PICASSO software through the continued broadening of the Nuclear Engineering Workstation Simulator at the NRC's Technical Training Center (TTC). Without the availability of HRP technical support and software, the implementation of other TTC upgrade projects would be costly and time consuming, and may not be possible at all.
6. A link to international efforts on man-machine systems research, fuels data, and materials data relevant to nuclear power.
7. High burn-up fuels data to upgrade NRC codes.
8. Access to an irradiation facility suitable for studies on materials degradation.

We understand that all other member countries intend to extend their participation in the Halden Reactor Project for the 1997-1999 program period.

Based on past experience, the HRP's technical program has been responsive to issues facing the NRC. Also, the HRP has been flexible in responding to the NRC's request for information, such as their response to provide lessons learned reports ([Attachment 2](#)).

The National Academy of Sciences review of safety and reliability issues associated with the use of digital instrumentation and control systems in nuclear power plants has identified and discussed six technical issues. Because

these are deep rooted issues that have not been easily solved, the NRC anticipates the National Academy of Sciences will make recommendations for additional research on many of these issues. We anticipate the HRP will be flexible enough to address many of these recommendations and to provide research products valuable in the resolution of the issues.

## CONCLUSIONS:

It is in the best interest of nuclear safety within the U.S. for the NRC to participate in the OECD Halden Reactor Project during 1997-1999. We intend to notify the HRP of our continued participation and sign the Agreement on the OECD Halden Reactor Project covering the period 1st January 1997 to 31st December 1999. This action involves no resource adjustments to the NRC 5-Year Plan for fiscal years 1995-1999, November 1994. The Office of General Counsel has no legal objection to this information paper.

James M. Taylor  
Executive Director for Operations

Contact: L. Beltracchi, RES  
415-6558

Attachments: 1. [Background Information](#)  
2. [Lesson Learned Reports](#)  
3. [Description of Specific OECD Halden Reactor Project Activities and Direct Comparison with Items in SECY-93-203](#)

---

ATTACHMENT 1

## BACKGROUND INFORMATION

- [Members of the Halden Reactor Project:](#)
- [Steering Bodies:](#)
- [Halden Project Budget:](#)

### Members of the Halden Reactor Project:

The members of the OECD Halden Reactor Project consist of signatory members and associated party members. Representatives from signatory members of the Halden Reactor Project may vote on issues brought before the Halden Board of Management and the Halden Program Group. Representatives from associated members of the Halden Reactor Project may attend meetings of the Halden Board of Management and the Halden Program Group, but have no vote on issues addressed by these bodies. The signatory members to the current agreement period, 1994-1996 are:

The Norwegian Institutt for Energiteknikk

The Belgium Nuclear Research Center CEN/SCK, acting on behalf of other public or private organizations in Belgium

RISO National Laboratory, Denmark

The Finnish Ministry of Trade and Industry (VTT)

Electricite de France

Gesellschaft fur Reaktorsicherheit, representing a German group of companies working in agreement with the German Federal Ministry for Research and Technology

The Italian Ente per le Nuove Tecnologie, l'Energia e l'Ambiente

The Japan Atomic Energy Institute

Korea Atomic Energy Research Institute

The Spanish Centro de Investigaciones Energeticas, Medioambientales y Tecnologias, representing a group of national and industry organizations in Spain

The Swedish Nuclear Power Inspectorate

The Swiss Federal Nuclear Safety Inspectorate, representing also the Swiss nuclear utilities and the Paul Scherrer Institute

Nuclear Electric plc, representing a group of Nuclear Research and Industry organizations in the United Kingdom

United States Nuclear Regulatory Commission

The associated party members of the Halden Project are:

Nuclear Research Institute, Czech Republic

Atomic Energy Research Institute, Hungary

N.V. Tot Keuring van Elektrotechnische Materialen (KEMA), the Netherlands

Russian National Research Center, Kurchatov Institute

Associated Parties In The USA:

ABB Combustion Engineering N.P.

Electric Power Research Institute (EPRI)

## Steering Bodies:

Under the Halden Agreement, an international committee, known as the Halden Board of Management, reviews and approves the research and experimental program and budgets on a yearly basis. The Halden Board of Management meets twice a year to conduct its business. Each signatory member of the Project has a representative on the Halden Board of Management. The U.S. Nuclear Regulatory Commission's representative to the Halden Board of Management is Mr. M. Wayne Hodges, Director, Division of Systems Technology, Office of Nuclear Regulatory Research.

An international technical group, known as the Halden Program Group, provides input to the research program and reviews and evaluates the products from the research. The Halden Program group meets two to three times a year to conduct its business. Each signatory member and associate member of the Project has a representative on the Halden Program Group. The U.S. Nuclear Regulatory Commission's representative to the Halden Program Group is Mr. Leo Beltracchi, Senior Human Factors Engineer, Controls, Instrumentation, and Human Factors Branch, Division of Systems Technology, Office of Nuclear Regulatory Research.

On a yearly basis, the Halden Project polls the participating members for research needs and solicits comments on its current research programs. The U.S. Nuclear Regulatory Commission responds to the polls through meetings with Halden's staff and through letters and e-mail. The Halden Program Group discusses and resolves comments on the Program Plan in arriving at a final research plan, which is then distributed to all members of the Project. The Project also publishes and distributes an annual technical report that summarizes the accomplishments and research results for the period.

## Halden Project Budget:

The OECD Halden Project Budget is funded by contributions from the signatory members, the associated party members, and from the sale of steam. The Project's budget for 1994 was 14.5 million dollars. The largest fiscal contribution to the Halden Project (35.2 percent) came from Norway. The funding levels for other signatory members are generally proportional to each country's Gross National Product per OECD guidance. The next largest contributor was Japan, with 8.05 percent of the budget. Japan has remained an active participant in both the fuels and the man-machine research activities at Halden. The U.S. Nuclear Regulatory Commission contributed 5.45 percent of the 1994-1996 budget, which reflects a reduced fee based on our participation in the man-machine research activities only.

During the 1994-1996 3-year period, several new members joined the Halden Reactor Project. Nuclear organizations within France and Korea have joined the Project as signatory members. Nuclear organizations within the Slovak Republic, Hungary, and Russia also joined the Project as associated party members. The new organizations contribute funding to the Project as well as research results based on projects within their respective country. The Project's budget for 1996 is approximately 15.9 million dollars. The increased funding for the Project results in greater resources to speed the completion of existing projects and to initiate new projects. Furthermore, at this point, the members of the Halden Project now consist of nearly all the major nuclear powers within the world.

There are four main areas of expenditures in the Halden Budget. The first area is the Man-Machine System research which accounted for about 40 percent of the 1995 budget. These funds provide for the verification and validation activities, man-machine interaction experiments, surveillance and support system development and test control room development and equipment and salaries. The second area is Reactor Operations, which accounted for about 27 percent of the 1995 budget, providing for the operation and maintenance of the plant and experimental facilities, including salaries of the operators. It should be noted that these operators also participate in the Man-Machine Systems research area. The third area of expenditure is the High Burn-Up Fuel Performance research, which accounted for 19 percent of the budget. These funds provide for rig design and fabrication, in-pile testing and experiments, and salaries. The fourth area of expenditure is the In-Core Material and Water Chemistry Effects research, which accounted for 14 percent of the budget. These funds provide for rig design and fabrication, in-pile testing and experiments, and salaries.

ATTACHMENT 2

## LESSON LEARNED REPORTS

- [1. Lessons Learned Report On Testing And Evaluation Methods](#)
- [2. Lessons Learned Report On Design And Evaluation Of Human-Machine Systems](#)
- [3. Lessons Learned Reports On Software Issues](#)
  - ["Project Management:](#)
  - ["Specification:](#)
  - ["Design and Coding:](#)
  - ["Testing:](#)
- [4. Lessons Learned Report On Software Quality Assurance](#)

To enhance the utility of the Halden Reactor Project's research results to the NRC, the NRC asked Halden to prepare a series of lesson learned reports in the areas of software engineering and human factors research from information accrued over the past 10 years or more. The research results contained in these lesson learned reports serve to form part of the technical basis needed to resolve user needs and for the formulation of regulatory guidance. A short summary of the lesson learned reports as of December 1995 follows.

### 1. Lessons Learned Report On Testing And Evaluation Methods

HWR-336, "Lessons Learned On Test And Evaluation Methods From Test And Evaluation Activities Performed At The OECD Halden Reactor Project," September, 1993.

HWR-337, "Source Material For Lessons Learned From Test And Evaluation And Evaluation Activities Performed At The OECD Halden Reactor Project, A Digest Of Studies From 1982 Through 1992," September 1993.

These reports present a summary of experience with different test and evaluation methods used at the Halden Reactor Project. Human-machine interaction studies have been performed at the Halden Man-Machine Laboratory (HAMMLAB) between 1982 and 1992, as well as on site nuclear power plant training simulators among Halden Project member organizations. The studies were conducted to test different aspects related to computerized operator support systems (COSS) for process control.

To provide the results in a relatively consistent format in the report, a classification scheme was developed in order to classify and record all of the test and evaluation activities. The recorded data consists of the characteristics of a study including the quantitative and qualitative findings related to system performance. Moreover, findings on the adequacy of the evaluation methods were also recorded.

These reports identify the types of test and evaluation methods adopted in Halden and discusses experience with the different methods. A brief summary of each individual research study is presented. Results from the research are discussed in terms of the main classes of test and evaluation methods; performance based and non-performance based evaluations. Examples of these methods are described and Halden's experience with them are discussed. Conclusions from this research are organized under a set of headers, reflecting a set of central human-machine evaluation issues that have received considerable attention within the Halden Project.

## **2. Lessons Learned Report On Design And Evaluation Of Human-Machine Systems**

HWR-376, "Summary Of Lessons Learned At The OECD Halden Reactor Project For The Design And Evaluation Of Human-Machine Systems," September 1995.

This report addresses design issues of human-machine systems in process control. The report covers more than ten years of human-machine systems research at the Project, with evaluation studies involving both conventional and advanced technologies for use in nuclear power plant control rooms. The computerized operator support systems tested and evaluated include alarm, diagnostic support computerized procedures, critical function management as well as conventional and advanced information display techniques. In the report, essential technological constituents of modern human-machine systems are outlined and their associated design options, as implemented in the systems tested at Halden, are described. The analysis of system effectiveness, supported by results from Halden evaluation studies, are organized according to the operator tasks supported by the system. The latter are given by a Human Performance Model which decomposes the activities performed by control room operators into a connected sequence of meaningful subtasks. In the conclusion, findings from the analysis of effectiveness are integrated to provide lessons learned on important topics such as automation and integration. The prominent issues are found to be the integration of automation with operator's tasks to support continuity of purpose, and the continuity in task-system integration to allow the smooth transfer between different operator tasks.

## **3. Lessons Learned Reports On Software Issues**

HWR-374, "A Lesson Learned Report On Software Dependability, Part I: Survey & Conclusions & Recommendations," June 1994

HWR-375, "A Lesson Learned Report On Software Dependability, Part II: Technical Basis," June 1994

This report contains a review of all activities OECD Halden Reactor Project has conducted on the field of software reliability and verification and validation since 1977. The report contains descriptions of actual work which has been conducted. The main emphasis is, however, put on the observations and conclusions made from these activities in specific types of organizations, as e.g. licensing authorities to assure adequate integrity of software for safety critical applications safety assessors, power companies, and software developers.

Examples of lessons learned from specific activities consist of:

### **"Project Management:**

Quality Assurance (QA) activities should be precisely defined and made mandatory, and a common level of QA should be enforced on all persons involved in the development. The QA auditor should carry out spot audits to ensure that fault reports and change notes are being applied and maintained correctly."

### **"Specification:**

The specification is the basis for the further development and verification of a software system. Deficiencies in the specification are often a source of faults in the final system. These are also the faults which are most difficult to detect during the verification and validation process."

### **"Design and Coding:**

Design and code inspection are very effective at discovering typical design and coding errors, such as logical errors, counting errors, assembly code errors, and clerical errors."

### **"Testing:**

Back-to-back testing of diverse programs is a very effective method to reveal program faults. All known real and seeded faults were found this way in our experimental investigations."

The above examples of lessons learned are useful to the NRC in the formulation of a technical basis. For example, the NRC is advocating the use of diversity as a means of defense against common mode error. It would then appear that back-to-back testing of diverse safety functions would be a necessary, but not sufficient, means of evaluating the functions and to assess if errors exist in the code.

Part II describes the different projects in more detail. For each project, there is a chapter with sections containing a short description of the project with reference to written material. Emphasis is placed on the observations and conclusions resulting from the project.

## **4. Lessons Learned Report On Software Quality Assurance**

HWR-418, "Lessons Learned From Experience With Development And Quality Assurance Of Software At The Halden Project," August 1995

This report contains the major lessons learned from experience with development and quality assurance of software systems at the OECD Halden Reactor Project since 1985. In the first part of the report, various plant specific software systems are reviewed. A functional description, the development process, and the lessons learned during the development of each specific system are described. The generic software products for user interface

management (PICASSO) and computerized procedures (COPMA) are treated as well. Safety critical software systems have been treated separately in two previous lessons learned reports, HWR-374 and HWR-375. However, the main findings with respect to the QA plan used in the Project On Diverse Software (PODS) and from application of formal methods to computer-based power range monitoring system installed at the Barseback NPP in Sweden are summarized in this report.

As commercial software development tools are gradually becoming available they are utilized in various phases of system development including project management. The tools used at Halden and the advantages and possible problems experienced which such tools are reviewed.

In the last chapter, the lessons learned from Halden's work are organized in accordance with the software life cycle starting with the software planning phase and ending with software operation and maintenance phase. Experience from project management and quality assurance is also summarized. Finally, Halden's viewpoints are given regarding the use of proprietary software and tools in safety related applications.

## DESCRIPTION OF SPECIFIC OECD HALDEN REACTOR PROJECT ACTIVITIES AND DIRECT COMPARISON WITH ITEMS IN SECY-93-203

- **Background:**
- **REVIEW OF THE 1994-1996 HALDEN REACTOR PROJECT RESEARCH RESULTS AND THEIR NRC USEFULNESS**
- **Verification and Validation of Software:**
- **Man-Machine Interaction Research:**
- **Surveillance and Support Systems:**
- **Advanced Control Rooms:**
  - **Staffing Levels for Advanced Reactor Project**

### **Background:**

The Halden Reactor Project is a cooperative agreement among a number of countries belonging to the Organization for Economic Cooperation and Development (OECD). The Project's activities are centered at the Halden heavy-water reactor and its associated man-machine laboratory in Halden, Norway. The programs conducted at Halden consist of studies on software quality assurance, man-machine systems research, high burn-up fuel performance, degradation of in-core materials, and water chemistry effects research.

### **REVIEW OF THE 1994-1996 HALDEN REACTOR PROJECT RESEARCH RESULTS AND THEIR NRC USEFULNESS**

SECY-93-203 identified and discussed the four main elements of the 1994-1996 Halden research program. These elements are:

1. Verification and Validation of Software
2. Man-machine Interaction Research
3. Surveillance and Support Systems
4. Advanced Control Rooms

Each of these elements is now reviewed in the context of the stated goals for the 1994-1996 Halden research program and NRC's research needs, recognizing that the current period is slightly over two-thirds completed.

### **Verification and Validation of Software:**

The Halden Project has conducted several studies on the evaluation of formal methods in the design and development of high integrity software. With the support of the Halden Program Group, the NRC requested that the Halden Project evaluate the use of formal methods in the development of safety critical software systems for nuclear power plants.

The study was performed by selecting an example system based on the following criterion: it should be realistic, preferably a real, safety-critical system related to nuclear power plant operation. After consultation with Sydkraft (Barseback NPP) and ABB Atom in Sweden, it was decided to use the computer-based power range monitoring (PRM) system installed at Barseback NPP as an example system for the project. The project did not address ABB's implementation of the example system, but the development of a similar system using formal methods. The purpose of the PRM system is the monitoring of the average power emission of the core. When high emission occurs, the system must trip the high level alarms.

The results of the study indicated that the practical use of formal methods can be adapted to implementation-oriented requirements to the software or to the implementation language. However, time based requirements were not addressed in this study, and through discussions on these results, we have asked Halden to investigate this problem in the context of additional research on the use of formal methods. Furthermore, the research results to date provide the NRC staff with practical knowledge in the application of formal methods in the software development of a reactor safety system. A description of the study and its results are reported in HWR-397, "Formal Software Development - A Case Study On The Development Of A Reactor Safety System."

HWR-425, "Review of Software Testing And Reliability Assessment Methods (RESTRAM)," September 1995, is a Halden report that reviews the research conducted in the field of software reliability assessment. It also evaluates models and methods concerning software fault tolerance and software testing. In addition to presenting the most commonly used methods/techniques within each field, the report evaluates each method with respect to their advantages and disadvantages. The review and evaluation focus is on the type of data and other information needed for each method, and how available these data are in real applications. The report concludes that software testing should not be restricted to only one method. It also concludes that random testing is the easiest to implement, but requires a large number of tests, which is a disadvantage, especially if outputs have to be checked manually. Other methods, such as structural testing, may require fewer tests to achieve the same confidence in the program's reliability, but will be harder to implement because an analysis of the program's structure is necessary as a basis for formulating test cases. The results presented in this report are useful in the safety evaluation of software in that advantages and disadvantages of various test methods are presented. The work can be used as guidance for a regulator in conducting a safety evaluation of software.

## **Man-Machine Interaction Research:**

In the development of NUREG-0700, Rev. 1, "Human-System Interface Design Review Guidelines," the HRP has been an integral part of the process. The HRP participated in the NRC sponsored peer review workshop on the guidelines. Also, HRP has extensively used the guidelines in the review and update of the Halden Man-Machine Laboratory. The feedback from the HRP on this experience has been substantial and positive, which provided us with further evidence on the use of the guidelines.

The technical basis for the alarm systems section of NUREG-0700 was, in part, derived from the HRP's extensive experience in developing and evaluating alarm systems. NUREG/CR-6105, "Human Factors Engineering Guidance for the review of Advanced Alarm Systems" was also based in part on the research performed at Halden. Further, the staff has selected the HRP because of its HAMMLAB to do additional research on alarm systems to develop a basis for guidance in the areas of display design, prioritization, and reduction. There was no US facility found that has the simulator flexibility available in HAMMLAB.

Another example of how a HRP designed product is used in the NRC research program is presented in NUREG/CR-6398, "Evaluation of the Computerized Procedures Manual II (COPMA II)." The purpose of this study was to evaluate the effects of a computerized procedure system on the performance and mental workload of licensed reactor operators. COPMA II, designed and developed by the HRP, contains features that display system parameters, and provides graphics that allow operators to track their progress through several parallel paths of procedures. COPMA II also provides automatic monitoring and feedback of pre-specified parameters. An experiment was designed and executed wherein licensed operators used COPMA II and the paper procedures in responding to accident scenarios. The most important finding of the study was that operators committed only half as many errors during the accident scenarios with COPMA II as they committed with paper procedures. However, time to initiate a procedure was fastest for paper procedures for accident scenario trials. The NRC benefited in two ways from this study: 1) as a member of Halden, there was no cost in procuring COPMA II for the research and 2) the results from this research will serve as part of the technical basis in the safety evaluation of computer driven operator aids and procedure trackers.

## **Surveillance and Support Systems:**

PICASSO is a user interface management system developed at the HRP and used to generate display formats for computer graphic displays. The PICASSO software developed by the HRP is the foundation of the Nuclear Engineering Workstation Simulator (NEWS) developed by the NRC Technical Training Division (TTD) staff for use at the Technical Training Center (TTC). The NEWS can be connected to the TTC full-scope simulators to display simulator model output that is not readily available on the full-scope simulator benchboards and to show physical phenomena in such a way as to add to the conceptualization of system interactions. The NEWS is also used to independently demonstrate the operation of control systems, component logics, and flow processes -- a full scope simulator does not provide the display data in this mode. All of the data is generated within the graphical interface itself. By using PICASSO to develop it, the NEWS has become an integrated training tool which has been easily incorporated into the TTD training programs. The use of NEWS has added substantially to the efficiency and effectiveness of the NRC Technical Training programs.

PICASSO is also the core of the new Safety Parameter Display System (SPDS), also developed by the NRC TTD staff, which has recently been placed into operation on the BWR/4 Simulator. By using PICASSO as its base, the SPDS development took advantage of work previously done in the development of the NEWS simulator interface software, so minimal new development was required for the interface. The displays are similar to those found on the BWR/6 system, which has greatly shortened the learning curve for use of the system by the instructors. The completed product is a graphical display system which is expected to greatly enhance training conducted on the BWR/4 Simulator.

Without the PICASSO software, the original development of these advanced, computer-based training systems would have required greater monetary and manpower investment. These additional resources were not available and are not expected to become available under the current budget projections. Continued maintenance and upgrades of these systems will not be possible without an on-going relationship with the HRP - improvements to PICASSO are continually being made which increase its performance and versatility. Advances in PICASSO will allow for broadening of the capabilities of the NEWS and SPDS. In addition, the use of PICASSO and other HRP software on other potential simulator upgrade projects is currently being evaluated. Without the availability of HRP technical support and software, the implementation of these upgrade projects would be costly and time-consuming, and may not be possible at all. This could ultimately result in a degradation in the reactor technology training provided to NRC technical personnel.

## **Advanced Control Rooms:**

### **Staffing Levels for Advanced Reactor Project**

This project responds to a high priority Human Factors user need. Vendor submittals for advanced reactors suggest minimum control room staff size; it was anticipated that some vendor applications would challenge the technical basis for using the current regulations on advanced designs. NRR requested "criteria for evaluating the justification for minimum control room crew size that will be supplied by the vendors during the certification stage." In addition, NRR staff need criteria to evaluate function and task analyses performed by these vendors. A statement of work was formulated and a search for a qualified contractor was conducted. The results from this effort concluded that the best facility to carry out such research was the Halden Reactor Project. Using Halden provides the opportunity to use both conventional plant simulator at the Lovissa reactor in Finland and the HAMMLAB simulator at Halden. This approach made it possible to use licensed operators from Lovissa who are also familiar with HAMMLAB.

This project is being conducted as a bilateral contract between the NRC and the Halden Reactor Project. As this work is specific to NRC user need and schedule, it was not incorporated into the Halden Project's general Technical Program. Prior to establishing the bilateral agreement, the staff considered contracting with a national laboratory but none had the necessary access to research simulators or licensed operators. For any of the laboratories to acquire the necessary facilities and staff, the costs would have far exceeded the costs of contracting with Halden.

In the scope of the work, the Halden Reactor Project staff is conducting a study of staffing level requirements focusing on criteria for evaluating minimum control room staff size, functions, and how control room systems for instrumentation and control, together with passive reactor designs may affect required staffing of control room crews. The project has two phases. In the first phase, operator tasks that comprise the basis for vendor assertions of staffing adequacy were identified. These tasks were used to select measures for comparing performance in a conventional nuclear power plant simulator with that in an advanced simulator.

The second phase will produce findings which will be used to evaluate differences in control room crew staffing requirements. Employing realistic control room environments and licensed nuclear power plant operators, an experimental study of operator and crew performance will be conducted. The study will employ highly automated and integrated, as well as conventional control systems to determine how such differences influence operator tasks and performance. The results of this study will be used to identify technical bases for evaluating staffing level adequacy

of advanced control rooms. The work on this research program at the Halden Project began in the fall of 1995 with a duration of 18 months.

Ms. Dolores Morisseau, NRC research staff, is on temporary duty at the Halden Reactor Project as the NRC Program Manager for the staffing study. Ms. Morisseau will also monitor and report on other relevant research programs at the Halden Reactor Project which are of interest to the NRC.