nks

Nordisk kernesikkerhedsforskning
Norrænar kjarnöryggisrannsóknir
Pohjoismainen ydinturvallisuustutkimus
Nordisk kjernesikkerhetsforskning
Nordisk kärnsäkerhetsforskning
Nordic nuclear safety research

NKS-228
ISBN 978-87-7893-299-0

Human Reliability Guidance – How to Increase the Synergies between Human Reliability, Human Factors, and System Design & Engineering.

Phase 1: The Nordic Point of View – A User Needs Analysis

Johanna Oxstrand 1 and Ronald Laurids Boring 2

1 Vattenfall Ringhals AB
2 Sandia National Laboratories

December 2010

Abstract

The main goal of this Nordic Nuclear Safety Research (NKS) council project is to produce guidance for how to use human reliability analysis (HRA) to strengthen overall safety. This project is intended to work across (and hopefully diminish) the borders that exist between human reliability analysis (HRA) and human-system interaction, human performance, human factors, and probabilistic risk assessment at Nordic nuclear power plants. This project consists of two major phases, where the initial phase (phase 1) is a study of current practices in the Nordic region, which is presented in this report. Even though the project covers the synergies between HRA and all other relevant fields, the main focus for the phase is to bridge HRA and design. Interviews with 26 Swedish and Finnish plant experts are summarized the present report, and 10 principles to improve the utilization of HRA at plants are presented. A second study, which is not documented in this preliminary report, will chronicle insights into how the US nuclear industry works with HRA. To gain this knowledge the author will conduct interviews with the US regulator, research laboratories, and utilities.

Key words

human reliability analysis; design; nuclear power plant; Nordic

NKS-228
ISBN 978-87-7893-299-0

Electronic report, December 2010

NKS Secretariat
NKS-776
P.O. Box 49
DK - 4000 Roskilde, Denmark

Phone +45 4677 4045
Fax +45 4677 4046
www.nks.org
e-mail nks@nks.org

NKS_R-2009_77 Interim Report

Human Reliability Guidance – How to Increase the Synergies between Human Reliability, Human Factors, and System Design & Engineering

Phase 1: The Nordic Point of View – A User Needs Analysis

Johanna Oxstrand & Ronald Laurids Boring
September 2009

This page blank

Human Reliability Guidance – How to Increase the Synergies between Human Reliability, Human Factors, and System Design & Engineering

Phase 1: The Nordic Point of View – A User Needs Analysis[1]

Johanna Oxstrand
Human Performance Department (RQH)
Vattenfall Ringhals AB
Väröbacka, Sweden
johanna.oxstrand@vattenfall.com

Ronald Laurids Boring[2]
Risk and Reliability Analysis Department
Sandia National Laboratories
Albuquerque, New Mexico, USA
rlborin@sandia.gov

[1] Earlier versions of this report first appeared in Oxstrand and Boring [1] and in Boring, Oxstrand, and Hildebrandt [2].

[2] The second author participated in this research as an employee of Sandia National Laboratories. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

This page blank

ABSTRACT

The main goal of this Nordic Nuclear Safety Research (NKS) council project is to produce guidance for how to use human reliability analysis (HRA) to strengthen overall safety. This project is intended to work across (and hopefully diminish) the borders that exist between human reliability analysis (HRA) and human-system interaction, human performance, human factors, and probabilistic risk assessment at Nordic nuclear power plants. This project consists of two major phases, where the initial phase (phase 1) is a study of current practices in the Nordic region, which is presented in this report. Even though the project covers the synergies between HRA and all other relevant fields, the main focus for the phase is to bridge HRA and design. Interviews with 26 Swedish and Finnish plant experts are summarized the present report, and 10 principles to improve the utilization of HRA at plants are presented. A second study, which is not documented in this preliminary report, will chronicle insights into how the US nuclear industry works with HRA. To gain this knowledge the author will conduct interviews with the US regulator, research laboratories, and utilities.

Keywords—*human reliability analysis; design; nuclear power plant; Nordic*

This page blank

Table of Contents

This page blank

Human Reliability Guidance – How to Increase the Synergies between Human Reliability, Human Factors, and System Design & Engineering

Phase 1: The Nordic Point of View – A User Needs Analysis

Johanna Oxstrand and Ronald Laurids Boring

I. INTRODUCTION TO HUMAN RELIABILITY ANALYSIS AND HUMAN FACTORS

Human reliability analysis (HRA) originated as a subfield of human factors. The earliest approaches to HRA attempted to predict human performance probabilistically [3]. This approach was backed by early efforts to catalog human errors from military and other applications for the purpose of quantitative prediction [4]. Meister [5] has suggested that HRA filled an important void in the early science of human factors. Whereas much of human factors was *diagnostic*—designed to identify shortcomings in designed systems and ultimately to make design recommendations—HRA remained *predictive*, attempting to anticipate how already built systems might degrade human performance.

This early distinction between human factors as a diagnostic science and HRA as a prescriptive science was cemented by the engineering disciplines to which human factors and HRA aligned themselves. Human factors initially provided design guidance for military applications but gradually became involved in industry applications and ultimately consumer products—mirroring the transfer of technology in the second half of the twentieth century. In fact, as a testament to the growing influence of human factors, by the 1980s, consumer product design regularly featured usability engineering, user-centered design, and human-computer interaction elements.

In contrast, HRA started and remained closely aligned with safety-critical applications for which human error had the potential to have high consequences. Like human factors, HRA was initially closely aligned to military applications, namely nuclear weapons manufacturing and handling safety in the US. However, by the early 1980s [6], HRA was closely associated with the nuclear power industry, an association maintained internationally to this day. HRA emerged parallel with the development of probabilistic risk assessment (PRA) [7] for hardware systems in the safety certification primarily of as-built plant designs.

More recently, coinciding with the modernization of existing nuclear power plants—especially control rooms—and the construction of new plants, there has been a strong movement to reconsider the use of HRA solely in a verification role for as-built systems. New guidance has been proposed within the nuclear industry [6], suggesting a tighter integration of HRA with human factors design activities. Additional research [9-11] has clarified the opportunities to utilize HRA to inform design and realign itself with core human factors work. In practice, however, the application of HRA for design, both inside and outside the nuclear industry, remains a largely untested principle. Some notable

exceptions can be found in [12-14], but the reach of such an approach could be much expanded. This study attempts further to bridge HRA with risk and human factors fields (with the interaction between HRA and design as the main focus) by surveying cognizant Nordic power plant personnel and support staff about opportunities they envision for utilizing HRA for design.

II. THE NORDIC NUCLEAR SAFETY RESEARCH PROJECT – HRA GUIDANCE

A. Background

The Nordic Nuclear Safety Research (NKS) council is sponsoring the current project, *Human Reliability Guidance – How to Increase the Synergies between Human Reliability, Human Factors, and System Design & Engineering* (NKS Project Code: NKS_R_2009_77). This project is intended to work across (and hopefully diminish) the borders of human-system interaction (HSI) and human reliability analysis (HRA) that we experience and that exist today. Each discipline does great work individually, but without the full collaborative picture they cannot determine the most suitable solution to reduce the overall risk at nuclear power plants. One of the reasons for the problem is the fact that different methods have been developed to fit different regulatory needs and therefore have created their own languages that are not adapted to communication across disciplinary borders. It is important to create synergies between the different approaches to increase the level of safety in the nuclear industry.

The project idea was born while the authors worked with the International HRA Empirical Study [15]. That study is a unique collaborative effort in that it brings together 13 international teams representing 11 different human reliability methods. During work with the International HRA Empirical Study, the question arose about how the results of the HRA are communicated back to the organizations and how they utilize it. This inspired the authors to investigate how the organizations use the results from risk and human factors analyses that they themselves conduct.

The main goal of the *Human Reliability Guidance* project is to produce guidance for how to use HRA to strengthen overall safety. This guidance should cover how to establish communication between HRA work and other disciplines such as human factors and system design and engineering. This guidance should especially aim to reconcile disparities between disciplines. As a long-term goal, the work should result in a positive change in the way human factors and HRA are thought of and worked with in the Nordic nuclear industry.

The project consists of two major phases, where the initial phase (phase 1) is a study of current practices in the Nordic region, which is presented in this report. Even though the project covers the synergies between HRA and all other relevant fields, the main focus for the study is to bridge HRA and design. This study was partly conducted as a user needs analysis of the Swedish nuclear industry in collaboration with Dr Ronald L. Boring of Sandia National Laboratories in the USA. The results of that user needs analysis were presented at ISRCS 2009, the 2nd International Symposium on Resilient Control Systems, in Idaho Falls, USA [1]. This report, *Phase 1: The Nordic Point of View – a User Needs Analysis*, is an expansion of the Oxstrand & Boring's user needs analysis. Additional data from the Finnish nuclear industry have been incorporated into the user needs analysis.

The second phase will be a study conducted in the USA in collaboration with Sandia National Laboratories (SNL). SNL's primary role in the context of human reliability is to serve as a research arm of the US Nuclear Regulatory Commission (US NRC). When so

tasked, it serves as a research conduit between the US NRC and industry. This second study will chronicle insights into how the US nuclear industry works with HRA. To gain this knowledge the author will conduct interviews with the US NRC, research laboratories, and utilities. The experience the US nuclear industry has concerning human factors and HRA will be useful and necessary when the final version of the *Human Reliability Guidance* for the Nordic region is composed. This final guidance document will summarize the findings from both phases, and will be completed during the spring of 2010.

III. CURRENT RESEARCH PROJECT: THE NORDIC POINT OF VIEW – A USER NEEDS ANALYSIS

A. Purpose of Survey

The aim of the survey is to understand how HRA is used today in the Nordic nuclear industry and how its use could be improved to achieve synergies with other disciplines. The Nordic nuclear industry implies the nuclear industry in Sweden and Finland, where operating commercial nuclear power plants are found.

This study takes previous explorations of HRA for design one step further by conducting a user needs analysis on opportunities for using HRA in control room modernizations. There is a greater focus on human factors in the nuclear industry than ever before. The Swedish nuclear industry and the Swedish Nuclear Radiation Safety Authority (SSM), for example, want to gain more knowledge about how to, in a suitable and effective way, address the issue of human factors in control room modernizations and upgrades. This was the main driving factor for the Oxstrand and Boring user needs analysis [1]. Oxstrand and Boring argue that HRA is an important tool when dealing with human factors in control room design or modernizations.

The end product of the user needs analysis of the Nordic nuclear industry is a concrete set of HRA design principles derived from comments and recommendations made by the interviewees. A high-level summary of the interviews precedes the principles below. While this report stops short of providing a proof-of-concept example for HRA in the design process in the nuclear industry, the principles nonetheless provide concrete requirements and a blueprint for HRA as a design tool integrated with human factors, system design, and HSI functions at the plants.

B. Method and Participants

In the Oxstrand and Boring study [1], 23 Swedish nuclear power plant specialists, with research, practitioner, and regulatory expertise in HRA, PRA, HSI, and human performance (HuP) were interviewed. At the time of this report, additional data from three Finnish nuclear power plant specialists have been incorporated into this report. Due to time constraints for the present report, the amount of data from the Finnish nuclear industry is unfortunately low. More interviews with the Finnish industry will be conducted during the second phase of the project.

The distribution of specialists and their type of employment are shown in Table 1. Because some interviewees represented multiple areas of expertise, they are counted more than once in the table. The most common combinations of specializations were PRA + HRA and HSI + HuP. To ensure the anonymity of the interviewees, the level of background detail provided here regarding the individuals is purposefully kept low.

TABLE I. NUMBER OF INTERVIEWEES AND THEIR TYPE OF EMPLOYMENT – CONTRACTOR (C), PLANT (P), RESEARCHER (R), AND REGULATOR (REG).

	HRA	PRA	HSI	HuP
Number of interviewees	8	13	8	8
Type of employment	C, P, and R	C,P, R, and Reg	C and P	C, P, R, and Reg

The interviews centered on a variety of possible applications for HRA, with an emphasis on identifying needs and gaps toward a more complete utilization of HRA expertise and methods at the home plant. We used semi structured interviews with a protocol of high-level questions. The following questions are the most important ones, in the sense of being good sources of data for informing the interaction of HRA and design at power plants:

- What are the barriers to HRA being used more?
- What is the main strength of HRA in your view?
- What is the main weakness of HRA in your view?
- How could HRA support your job?
- How could you support HRA in your job function?

Additional questions centered on providing background on the job functions and responsibilities of each specialist. The results summarized in this report represent mainly the relevant findings pertaining to how HRA might be used in system design, specifically control room upgrades that are part of the plant modernization plans. This report also briefly discusses the overall interaction between HRA and the other fields.

As a starting point for the study, the authors took a closer look at Vattenfall Ringhals AB with the sole purpose to gain a better understanding of the interactions between human factors and risk groups at a Nordic nuclear power plant. The results of this step serve as a base for the rest of the study. The findings from this Ringhals-specific pre-study are generalizable and useful to the entire Nordic nuclear industry.

IV. HUMAN RELIABILITY AND DESIGN FUNCTIONS AT THE RINGHALS NUCLEAR POWER PLANT

A. Vattenfall Ringhals AB

Vattenfall AB is Europe's fifth largest generator of electricity and the largest generator of heat. Vattenfall AB has operations in Sweden, Finland, Denmark, Germany and Poland,

and the company is wholly owned by the Swedish state. Ringhals Nuclear Power Station (Ringhals) is the largest nuclear power plant in Sweden, of which Vattenfall AB owns 70.4%. Ringhals has four reactors (one boiling water reactor and three pressurized water reactors), and a product capacity of approximately 28 TW/h/year, which covers about 20% of the total demand of electricity in Sweden. Ringhals has about 1,500 employees, with an additional 500 contractors on site each year.

As part of a general reorganization at Ringhals in 2008, the technical competence in HRA was transferred from the Ringhals Safety Analysis (RTAS) department to the Ringhals Human Performance (RQH) department. This transfer brought with it two significant changes:

- the departmental decoupling of HRA from PRA
- the merger of the HRA technical competence with human performance activities in RQH

These changes brought both challenges and opportunities. A survey was commissioned by Ringhals to evaluate those challenges and provide concise guidance on how to maximize the collaboration between human performance—including human-system interface design functions—and HRA capabilities at the plant.

The interaction between different human factors and risk groups is depicted in Fig. 1. Prior to the reorganization (depicted by the solid lines in Fig. 1), the design capability at Ringhals was based in the Human-System Interaction (HSI) group, with inputs from the Probabilistic Risk Assessment (PRA) group. HRA supported PRA on these tasks. There was no direct interaction between HSI and HRA, nor was there a clear tie-in to the role of the Human Performance (HuP) group in the organization, which traditionally was involved in the human factors part of incident investigations. The reorganization introduced the possibility of stronger interaction with the human factors roles, including direct interactions between HSI, HuP, and HRA. These interactions are depicted as dashed lines in Fig. 1. The actual mechanism or method for these interactions has not yet been formalized. As such, there is currently an emphasis to articulate explicit interactions between these groups.

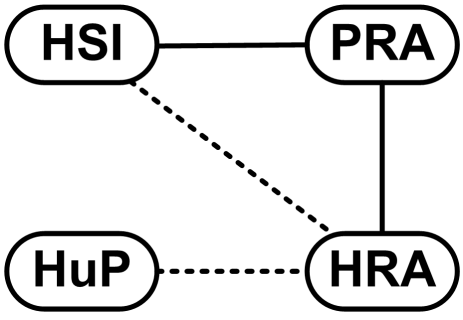

Figure 1. Interaction between human factors and risk groups at Ringhals.

B. Current Design Process

In the design of new systems or upgrades of older systems, HRA has mainly been used as a validation tool. In this capacity, HRA ensures that reactor safety is not compromised by the new design or the upgrade. In order to pass the validation, the level of reactor safety has to be demonstrably at least as good as it was before the change. At this stage, if any performance issues were detected, these would be hard to rectify. Many of the

human factors and HRA experts are brought in as contractors late in the project, i.e. in the verification phase. As such, these experts do not have any opportunity to influence the design. If the HRA had been used earlier in the process, as NUREG-0711 [8] suggests, negative design impacts on operator performance could be detected at a stage where there still is time to make changes. The design process in all major upgrade and modernization projects at Ringhals is based on NUREG-0711, but all projects have modified the process to fit their own work process. In practice, these modifications have relegated HRA to a tail-end activity. The reorganization of groups at Ringhals affords the opportunity to have HRA involved earlier in the design process by interacting directly with the HSI group.

V. FINDINGS

A. Data Analysis Overview

The data collected during the interviews were analyzed and summarized with the objective to catalog the findings according to common themes. The catalog of interview data was built by categorizing the data by the different fields of interest, i.e., PRA, HSI, and HuP. The live interviews were recorded, and two separate analysts reviewed these recordings and notes to capture insights. These findings from the individual analysts were aggregated into a single set of mutually agreed findings. High-level summaries of comments are provided in sections below.

A few caveats are necessary to understand the findings captured from the interviews.

- All but one of the HRA specialists have multiple areas of expertise. Therefore, the data collected from these specialists were incorporated into other categories in the analysis, resulting in the removal of the standalone HRA category.
- In most cases, the findings represent remarks made by more than a single interviewee. However, relevant comments made by a single interviewee are also presented below for the sake of capturing a wide range of ideas on the use of HRA in design.
- In order to preserve the anonymity of the interviewees, the findings below are not attributed to specific people.

B. Probablistic Risk Assessment (PRA)

Even though PRA and HRA could be helpful to modernization projects earlier in the design process, they are almost exclusively used as a validation tool to ensure reactor safety is not compromised by the new design or the upgrade.

HRA is an integral part of PRA and PRA applications and is a necessity for making PRA complete, satisfactory, and realistic. HRA invokes new questions and provides new inspiration in the context of PRA, and therefore awakens new areas for PRA. Hence, HRA needs to keep a strong connection to PRA even though it might be used for other applications as well.

New applications for PRA, such as fire actions and low power/shutdown, involve human performance. Due to ongoing developments in the PRA field, HRA must mirror these developments in order to be applicable to PRA. When developing HRA, there should also be a greater emphasis on maintenance and organizational issues, areas that are currently underestimated in the HRA work. There is no need to use a “one size fits all” approach in HRA, but there should not be too many different methods to choose from either. Since there is no universally accepted method, some guidance of which method to use for certain applications is needed. Newer HRA methods tend to have a greater cognitive and HSI focus than their predecessors. There is still no evidence that

these methods actually provide more accurate results than the older methods. The newer methods, however, rely for the most part on the same data as the older methods, i.e., the human error probabilities in THERP [6]. There is no evidence that this dataset is valid for digital instrumentation and control systems and advanced displays.

To validate both old and new methods, more relevant data need to be collected. There is some resistance to collect data within the PRA community that are based on the assumption that the data in THERP [6] are internally consistent. There is no guarantee that new data would point to something different. However, new data could suggest that most of the existing analyses have been made on faulty assessments.

There is disagreement on the value of the qualitative information provided by the HRA. Some more seasoned PRA analysts tended to view the main value in HRA coming from the quantitative values. Younger analysts tend also to see value in qualitative insights for the PRA, but also outside the PRA where the insights can increase the plant's safety by improving practices, procedures, and training. The younger analysts' view concurs with that of the Swedish regulator. The regulator views qualitative insights as important for tracing the root cause in retrospective analyses. This qualitative result also needs to be thoroughly documented to make the HRA traceable and usable by reviewers or other safety personnel.

There is an issue of communication between HRA and the other fields, but also within the HRA community. When conducting an HRA, experts from different fields take part. These experts might have different backgrounds, agendas, and terminology, which could lead to culture clashes and misunderstandings. The difference in terminology is also believed to be the reason for the poor communication between HRA and the other fields. The communication between the HRA and the technical parts of the organization also needs to be improved.

In the PRA community, there is a notion of HRA being too soft, i.e., the receiver of the analysis does not know how to deal with the findings, because some findings may be qualitative and not expressed in terms of familiar risk metrics. Dealing with human behavior introduces assumptions and subjectivity. There is also a concern that the scope of the HRA is too limited. Most HRAs do not cover outages or severe accidents, which could result in issues with validity.

C. Human-System Interaction (HSI)

It is important to determine common goals for HRA and HSI, since they both are conducted within the design process for modernization and upgrades, and have potential to benefit from each other. HRA also needs to be implemented earlier in the design phase. Currently it is used in validation, at which point any performance issues detected are hard to rectify. HRA could help identify errors early in the design of the human-system interaction, and help to correct those. Many of the HSI and HRA subject matter experts are brought in as contractors in the verification phase, and therefore have no opportunity to influence the design.

Even though HRA should be implemented earlier in the design phase, HRA could help set acceptance criteria and determine potential testing scenarios for validation. Such acceptance criteria are used as part of verification and validation of new systems to ensure the systems are compliant with reliability and safety requirements of the plants. Modeling performance deficits and knowing the effects on system safety may serve as a better basis than "arbitrary" regulatory safety thresholds. It is difficult to perform a thorough HRA for something as complex as control room operations. There needs to be a way to scale HRA appropriately for the level of effort required.

Some control room systems have automated second-checking and correction. Whenever an operator makes an error, the system will catch it and correct it. The drawback is that the operator is not learning from his or her mistakes, and might repeat the error without knowing it. Such auto correction may ultimately serve to decrease situational awareness and increase the likelihood of human performance issues in future system interactions.

D. Human Performance (HuP)

At the Nordic nuclear power plants, retrospective human factors investigations are conducted regularly. These investigations are sometimes viewed as being too qualitative. The receiver of the investigation is mainly someone within a technical/engineering department. Employees in these technical departments do not generally work with qualitative measures and can therefore have a hard time relating to the results of the investigations. There is a perception of psychology and/or human factors as being a soft science that does not help plant safety or operations. The ability of HRA to translate qualitative insights into quantitative terms is seen as a positive example for HuP. Since HRA is related to both the technical side but also to the human factors field, it could serve as a bridge between the psychological and technical work at the plant. Having quantitative results for a human performance analysis could be helpful in the communication of the results and recommendations. In order to successfully communicate the importance of human factors and HRA, the organization is dependent on champions or strong networks of HRA proponents.

VI. PRINCIPLES FOR HRA USE IN DESIGN

In order to gain synergies and to improve the contributions of both human factors and HRA in upgrade and modernization projects at the plant, common goals must be identified. These goals must give guidance to which information both fields could provide to each other to make the final design safer and more reliable. The following guidelines are derived from an expert assessment conducted by a plant expert, human factors expert, and HRA expert. The findings on HRA and design from the interviews were reviewed, and a set of guidelines for facilitating this interaction was posited. These guidelines are preliminary and may be subject to refinement as additional analyses are conducted on the interview data. Nonetheless, we believe the guidelines provide a strong starting point and framework for how HRA can actively contribute to design projects. They also serve as a mechanism for integrating the human factors and HRA work at a nuclear power plant.

The principles are supported by statements made by various interviewees in this study. While we endorse the principles outlined here, it must be noted that the views represented are those of individuals and may not represent the views of the authors of this report.

A. Principle 1—Early Implementation Rather than Late Verification

HRA needs to be implemented earlier in the design phase instead of at the system verification phase. In this way, it may influence the system design rather than serve simply as a tool to verify the quality of a design. In a worst case scenario, post-design verification may only serve to nullify a design that has been in development for years and cannot practically be altered. A better approach, therefore, is to develop qualitative insights from HRA in the form of identifying system designs and configurations that would decrease the likelihood of operator errors. Recent research [12] has suggested that when used early in the process, HRA can identify a large number of changes in

proposed designs and operations that need to be made in order to prevent errors later on. This has potential to save the organization a lot of money. Further, quantitative estimates may determine the likelihood and consequence of particular operator errors, thereby allowing a ranking of competing design concepts linked to particular classes of errors. In this way, HRA could help to prioritize the safest among competing design alternatives.

The information gained early in the design phase by the HRA can be used to improve other areas. As well At Loviisa nuclear power plant in Finland, for example, HRA findings have been used to improve practices, procedures, and training. These are areas that all need to be considered early in the design project in order to have all required documentation ready in time. Hench, HRA will have a positive effect on work in these areas as well.

Even though we argue that HRA should be implemented earlier in the design process, HRA should, of course, continue to be used in the verification phase. HRA can determine different testing scenarios, which can be used for validation of the system or design. The same scenarios are also used in the baseline analysis, which is one of the first human factors activities in a project. The baseline analysis documents operator performance in using the current design. These results are later compared with the analysis results in the verification phase in order to conclude that reactor safety has not been compromised. Therefore, the scenarios have to be the same in both the baseline and the validation analyses. To determine the scenarios before the baseline analysis is conducted, HRA should be incorporated very early in the design process. In the case of significant modernizations such as a complete control room upgrade, it is insufficient to rely on operator action tables provide by the PRA or by the vendors. These operator action tables are often legacy documents based on operating experience. They may not, however, fully anticipate operator actions or inactions in the face of new human-machine interface technology.

B. Principle 2—Tailored HRA Methods for Design

Currently, there is a strong emphasis on a one-size-fits-all approach to HRA. The HRAs conducted in the Nordic nuclear industry are mainly based on the THERP method [6]. The main reason behind this is the ease of utilizing the human error probability tables provided in the THERP documentation. Another, almost as important reason is the fact that the regulatory body has historically accepted THERP as the HRA methodology used in practice at the plants. Neither the utilities nor the vendors would like to invest in an HRA if they are unsure that the regulatory body would approve the method's findings. While THERP is a suitable and comprehensive HRA method for contemporary applications, its suitability for modern human-machine interfaces has not been established. Barring a significant update to bring THERP in alignment with new technologies, it is necessary to consider newer HRA methods.

Despite these uncertainties over the suitability of the dominant HRA method, there is a more fundamental issue at hand: it should not be necessary to use the same method for all analyses conducted at the plant. Instead, the plant should use methods and analyses that are tailored for specific applications. Not all applications have the need to be analyzed by a complex and resource consuming method. The analyst should choose a method, or type of analysis, that suits the purpose of the application. This statement does not mean that all available HRA methods should be used. There are too many methods available to make that feasible. Instead, a consolidation or harmonizing of methods needs to be conducted to ensure consistent results.

HRA work in the Nordic nuclear industry is moving toward more prospective (or proactive) analyses, and a few prospective HRAs have been conducted so far to anticipate and prevent sources of human error. The prospective approach for gleaning error insights is much the same as used for the retrospective (or reactive) HRA investigations of plant events, i.e., interviews and expert judgment. The prospective HRA approach can easily be adapted to design applications—the predictive nature of HRA lends itself well to making recommendations about safe courses of activity and to prioritizing those recommendations when considering design alternatives. Nonetheless, such a framework of using HRA prospectively should not be linked to any specific method. Instead, like the *PRA Standard* [16] or the *Good Practices for HRA* [17], the optimal process of using prospective HRA for design should be method independent.

C. Principle 3—Scalable HRA

Closely related to the previous principle, it is important that HRA be scalable to fit the application at hand. For example, a complete, detailed task analysis for purposes of an HRA may not be practicable at the early design phase of a modernization project. There may be knowledge limitations on operator tasking prior to completion of the design specification, which may compound with time and budget constraints. A simplified task analysis may therefore be necessary to identify only the most critical operator actions for purposes of evaluation. HRA commonly offers screening and detailed analysis approaches. The need for different levels of analysis is not diminished when considering operator performance on newly designed systems, and HRA for design should scale to the level of analysis required.

In order to successfully scale-up an HRA, it is important that the scope match the scale and purpose of the analysis. It might not be relevant for an analysis of a small set of actions to consider outages or severe accidents. In an analysis of a new control room, however, such actions would be most relevant to analyze.

D. Principle 4—Better Use of Qualitative HRA

As stated in the summary of findings, there is a disagreement on the value of the qualitative information provided by the HRA. The Swedish regulator views qualitative insights as important for tracing the root cause in retrospective analyses. The qualitative information also needs to be thoroughly documented to make the HRA traceable and usable by reviewers or other safety personnel.

HRA is closely related to PRA but has human factors roots. Therefore HRA could serve as a bridge between the psychological and engineering work at the plant. Having quantitative results, as a part of the retrospective investigation, could be helpful in the communication of the results and recommendations. Retrospective investigations often have multiple recommendations for which the receiver should take responsibility. Having multiple recommendations could make it difficult to know where to start and to understand which recommendations are the most important ones. HRA could ease this selection process by providing qualitative or quantitative results suitable for ranking or prioritization of the recommendations.

The importance of qualitative information becomes even more evident in the prospective analyses required for design. Quantitative HRA measures may, technically speaking, be adequate to populate the PRA model. However, for design work, the true value comes from HRA's determination of possible contributors to degraded operator performance, not from the ability of HRA to generate human error probabilities. HRA affords the ability to determine root causes of many possible operator errors, thereby allowing system designers to determine ways to prevent those errors. A tertiary approach may be taken to address those errors—procedures may be written or clarified,

specialized operator training may be offered, or the system may be redesigned to prevent the error. Understanding the causes of the possible operator error is key to developing the best of these strategies to minimize the error occurrence.

E. Principle 5—HRA Design Acceptance Criteria

Contemporary HRA includes a significant quantitative element that is used in risk-informed decision making. This framework can and should be extended to establish operator performance thresholds for novel control room designs. The goal thereby is to model performance deficits and know their effects a priori on system safety. Such safety limits are already understood from the verification and validation phase of system design, but they must be adapted for use early in the system design. HRA verification criteria may consider overall performance as a product of hardware and human actions. As noted in the data analysis summary, there is the danger that the system may have automated second-checking and correction such that operators may not ever become fully aware of errors they have committed. Such a system precludes the opportunity for the operators to learn from their errors, resulting in the potential for the operators to commit the error repeatedly. While in the advanced system, this error may have negligible consequences in a particular context, the situational awareness of the operators is nevertheless compromised such that the missed error may resurface in another context that actually has direct consequences on the safety of the plant. For design applications, it is therefore crucial that HRA help identify the potential for both low and high consequence errors in operator errors. In cases where high consequence errors are identified, HRA should provide design guidance to minimize their occurrence in addition to standard design practice to mitigate the effects of those errors through hardware and software systems.

F. Principle 6—HRA Sensitivity to Human-Machine Interface Issues

Legacy HRA methods may not provide a nuanced account of the issues affecting operators in modern interfaces. Even many newer HRA methods are loosely based on older methods and may not have expanded the fundamental performance shaping factors or generic error types that are the basis for the qualitative and quantitative analyses. In the realm of HRA for design, however, it is crucial that the methods adequately address digital instrumentation and control, advanced displays, and increased opportunity for automation so that they can help the analyst to predict where related deficits might occur. It may be necessary to develop new HRA methods or tools that are attuned to advanced technologies, e.g., to marry HRA methods with advanced usability checklists [18]. Such an HRA approach must help anticipate sources of operator error endemic to advanced technologies and be sensitive to design factors such as the usability of interface technologies or the consistency of interface elements provided by different vendors.

G. Principle 7 – Better Integration of HRA with PRA

It is important to keep a strong connection between HRA and PRA, even when we present new applications for HRA outside PRA. HRA should not be detached from the PRA, because HRA forms an essential part in the search for the most realistic core damage frequency. HRA also provides categories of human errors, influencing factors, and quantitative human error probabilities to the PRA group. HRA also serves as a link between the technical areas and the human factors and human performance areas to make sure the human aspects are not forgotten in the risk assessment. The different perspectives in HRA compared to PRA also invokes questions that could lead to new and relevant areas for the PRA to explore.

H. Principle 8 – Need for Data to Support HRA

While HRA has evolved considerably since the early advent of THERP [6], newer HRA methods have not demonstrated a clear data pedigree. Newer HRA methods, sometimes referred to as second-generation methods, have brought new approaches for looking particularly at the cognitive aspects underlying human error. However, these newer methods have been slow to produce good evidence to support the quantification of cognitive errors. HRAs should focus on areas where data can be collected and verified. The cognitive aspect is still too unexplored and will therefore add too much subjectivity to the result.

The newer methods have not been verified enough. Do we know that they are as good as, or better than the old ones? Since the newer methods, for the most part, rely on old data, is there no evidence that they will assess actions in advanced control rooms in a more accurate manner? Some of the newer HRA methods utilize expert judgment for quantification. It was felt by several interviewees that these methods should use data instead of experts making assumptions. Improvements of these newer methods (or even refinements of older methods) are made possible with more data. These data may be collected in simulators.

One HRA expert noted that analysts keep using THERP data instead of collecting new data. What would happen if we started to collect data today and found out that the data in THERP are wrong for contemporary applications? This could be the "cracked pillar on which the house stands," i.e., the house could crumble. We have used THERP for so long, and it seems to work fine. Why should we put in resources to get new data? We want proof that something better exists before we put any effort into it. It is a vicious cycle that may have stunted the emergence of better HRA methods.

I. Principle 9 – HRA Method Development

New areas of HRA require method development, both in the context of PRA and without. As mentioned in *Principle 6 – HRA Sensitivity to Human-Machine Interface Issues*, HRA methods need to be able to assess correctly all the challenges that come with advanced control rooms. To successfully bridge between the technical risk perspective and the human factors groups, HRA also needs to incorporate safety culture and organizational issues, at least in the qualitative part of the HRA. Before these issues could be quantitatively assessed properly, more data on the matter must be collected. In addition, many areas of interest to plants as PRAs are refined—areas such as low power, shutdown, fire, or severe accidents—need to be supported by HRA with accompanying method development efforts. Currently, HRA method development has lagged the emergence of these areas in PRA. As noted in the previous section, where applicable, HRA method refinement and development needs to be carefully data based.

J. Principle 10 – Communication

Communication is a broad principle that spreads over multiple fields. It concerns the exchange of information between risk and human factors groups, but also the mission to inform the organization of the importance of risk and human factors work. HRA could be immensely improved by gaining information from the other human factors fields regarding human failure events that have occurred, findings from retrospective or prospective human factors analyses, and positive improvements that have been reinforced in the organization. Such information would help the HRA group to conduct more accurate assessments. It would also give them valuable knowledge regarding actions to include in an upcoming analysis.

Prospective human factors analyses and retrospective investigations are often viewed as being too qualitative. The receiver of the analysis is usually a manager at a technical

department, who might be a novice to qualitative data. It is important to communicate findings and recommendations in a manner that the receiver can relate to. HRA could therefore help translate the qualitative findings into a more quantitative summary and thereby ease the communication of the findings from the human factors analyses or investigations.

Both human reliability and human factors are psychological undertakings in an engineering based organization. Psychological concepts are not always understood or appreciated, and there exists a perception in some minds that this is a soft science that cannot help to improve plant safety or operations. It has to be a joint mission between the risk and human factors champions to inform the organization of the benefits of working with these issues. Human reliability and human factors need to have been reconciled before this successfully can be carried out.

VII. DISCUSSION

Clearly, the foregoing discussion is not an exhaustive list of principles to guide the transition of HRA to support plant upgrades and design projects at nuclear power plants. This list does, however, represent ten concrete changes that must be adopted in order for HRA to make a more complete contribution to the design process. Such a contribution is highly desirable, as evidenced across the spectrum of interviews, because HRA is seen as a potentially useful tool to predict design issues that might negatively affect operator performance and decrease plant safety. Incorporating HRA as another tool in the design process ultimately provides the opportunity to design a system that is more robust or resilient to operator error.

An important byproduct of implementing HRA in the design process is the potential to reduce costly redesigns that are necessitated by findings during the verification phase. HRA, along with human factors, must in the future anticipate many problems before they are implemented into the system design. As mentioned, HRA may prioritize the safest among competing design alternatives. Prioritization may serve another end: where limited resources are available for verification during the design phase, HRA may pinpoint the most important areas for using costly humans-in-the-loop validation testing. Testing may be focused in those areas where safety or operator reliability may in any way come into question.

It next falls upon Ringhals and other Nordic nuclear power plants to implement these ten principles and to validate the assumptions presented in this report. Work is currently underway to adapt HRA to meet these requirements at Ringhals. More importantly, we plan to introduce HRA as part of a forthcoming upgrade effort at Ringhals. This example in practice will serve as the litmus test for the approach and will be presented in future papers. Of particular interest is the extent to which HRA adds value to the design process. Additionally, it will be interesting to note if HRA's contribution to design will reconcile it with the aims of its sibling field, human factors.

ACKNOWLEDGMENTS

This work was supported by a grant from the Nordic Nuclear Safety Research (NKS) council, with matching funds provided by Vattenfall Ringhals AB. The authors wish to thank Michael Hildebrandt, OECD Halden Reactor Project, Norway, for his invaluable assistance in coordinating this research. The authors also gratefully acknowledge the many people in the Nordic nuclear industry who agreed to be interviewed as part of this research project. The ultimate success of this project should be credited to their desire

to improve safety and design practices. Any omissions, errors, or shortcomings are the sole fault of the authors.

REFERENCES

[1] J. Oxstrand and R.L. Boring, "Human reliability for design applications at a Swedish nuclear power plant: Preliminary findings and principles from a user-needs analysis," 2nd International Symposium on Resilient Control Systems, New York: Institute of Electrical and Electronics Engineers, 2009, pp. 5-10.

[2] R.L. Boring, J. Oxstrand, and M. Hildebrandt, "Human reliability analysis for control room upgrades," Proceeedings of the 53rd Annual Meeting of the Human Factors and Ergonomics Society, 2009, in press.

[3] A.D. Swain, J.W. Altman, and L.W. Rook Jr., Human Error Quantification, A Symposium, SCR-610, Albuquerque: Sandia Corporation, 1963.

[4] L. Rigby, "The Sandia human error rate bank (SHERB)," Man-Machine Effectiveness Analysis, Los Angeles: Human Factors Society, 1967, pp. 5.1-5.13.

[5] D. Meister, Conceptual Foundations of Human Factors Measurement. Mahwah, NJ: Lawrence Erlbaum Associates, 2004.

[6] A.D. Swain and H.E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report, NUREG/CR-1278, Washington, DC: US Nuclear Regulatory Commission, 1983.

[7] U.S. Nuclear Regulatory Commission, Reactor Safety Study, An Assessment of Accidental Risks in U.S. Commercial Nuclear Power Plants, WASH-1400, Washington, DC: U.S. Nuclear Regulatory Commission, 1975.

[8] J.M. O'Hara, J.C. Higgins, J.J. Persensky, P.M. Lewis, and J.P. Bongarra, Human Factors Engineering Program Review Model, NUREG-0711, Rev. 2, Washington, DC: U.S. Nucler Regulatory Commission, 2004.

[9] R.L. Boring, "Meeting human reliability requirement through human factors design, testing, and modeling," Proceedings of the European Safety and Reliability Conference (ESREL 2007), London: Taylor & Francis, 2007, pp. 3-8.

[10] R.L. Boring and A. Bye, "Bridging human factors and human reliability analysis," Proceedings of the 52nd Annual Meeting of the Human Factors and Ergonomics Society, 2008, pp. 733-737.

[11] R.L. Boring, E. Roth, O. Straeter, K. Laumann, H.S. Blackman, J. Oxstrand, and J.J. Persensky, "Is human reliability relevant to human factors?" 53rd Annual Meeting of the Human Factors and Ergonomics Society, in press.

[12] B. Kriwan, "An overview of a nuclear reprocessiong plant Human Factors programme", in Applied Ergonomics, vol. 34, pp. 441-452, 2003.

[13] J. Dul and W.P. Neumann,"Ergonomics contributions to company strategies", in Applied Ergonomics, vol. 40, pp. 745-752, 2009.

[14] R.L. Boring, "Meeting human reliability requirements through human factors design, testing, and modeling" in Risk, Reliability and Societal Safety, Volume 1: Specialisation Topics. Proceedings of the European Safety and Reliability Conference (ESREL 2007), T. Aven and J.E. Vinnem, Eds. London: Taylor & Francis, 2007, pp. 3-8.

[15] E. Lois, V.N. Dang, J. Forester, H. Broberg, S. Massaiu, M. Hildebrandt, P.Ø. Braarud, G. Parry, J. Julius, R. Boring, I. Männistö, and A. Bye, International HRA Empirical Study—Pilot Phase Report: Description of Overall Approach and First Pilot Results from Comparing HRA Methods to Simulator Data, HWR-844, Halden: OECD Halden Reactor Project.

[16] American Society of Mechanical Engineers, Addenda to ASME/ANS RA-S-2008, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-Sa-2009, New York: American Society of Mechanical Engineers, 2009.

[17] A. Kolaczkowski, J. Forester, E. Lois, and S. Cooper, Good Practices for Implementing Human Reliability Analysis (HRA), NUREG-1792, Washington, DC: U.S. Nuclear Regulatory Commission, 2005.

[18] R.L. Boring, T.Q. Tran, D.I. Gertman, and A.S. Ragsdale, "A human reliability based usability evaluation method for safety-critical software," Fifth International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology, 2006, pp. 1275-1279.

Bibliographic Data Sheet **NKS-228**

Title	Human Reliability Guidance – How to Increase the Synergies between Human Reliability, Human Factors, and System Design & Engineering. Phase 1: The Nordic Point of View – A User Needs Analysis
Author(s)	Johanna Oxstrand 1 & Ronald Laurids Boring 2
Affiliation(s)	1 Vattenfall Ringhals AB & 2 Sandia National Laboratories
ISBN	978-87-7893-299-0
Date	December 2010
Project	NKS-R / HRA GUIDANCE
No. of pages	23
No. of tables	1
No. of illustrations	1
No. of references	18

Abstract

The main goal of this Nordic Nuclear Safety Research (NKS) council project is to produce guidance for how to use human reliability analysis (HRA) to strengthen overall safety. This project is intended to work across (and hopefully diminish) the borders that exist between human reliability analysis (HRA) and human-system interaction, human performance, human factors, and probabilistic risk assessment at Nordic nuclear power plants. This project consists of two major phases, where the initial phase (phase 1) is a study of current practices in the Nordic region, which is presented in this report. Even though the project covers the synergies between HRA and all other relevant fields, the main focus for the phase is to bridge HRA and design. Interviews with 26 Swedish and Finnish plant experts are summarized the present report, and 10 principles to improve the utilization of HRA at plants are presented. A second study, which is not documented in this preliminary report, will chronicle insights into how the US nuclear industry works with HRA. To gain this knowledge the author will conduct interviews with the US regulator, research laboratories, and utilities.

Key words human reliability analysis; design; nuclear power plant; Nordic

Available on request from the NKS Secretariat, P.O.Box 49, DK-4000 Roskilde, Denmark.
Phone (+45) 4677 4045, fax (+45) 4677 4046, e-mail nks@nks.org, www.nks.org