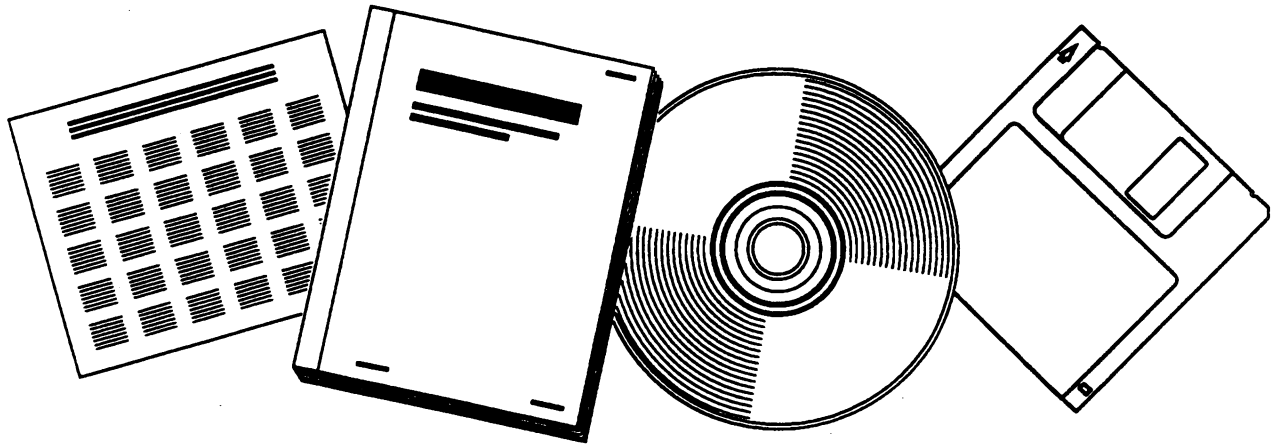

U.S. DEPARTMENT OF COMMERCE
National Technical Information Service

CONF-970625--4 -- INEL/CON-97-00419

Integrated Design Environment for Human Performance and Human Reliability Analysis

William R. Nelson
Lockheed Martin Idaho Technologies Company
Idaho National Engineering and Environmental Laboratory
P.O Box 1625
Idaho Falls, Idaho 83415-3855
wnr@inel.gov

Abstract: Work over the last few years at the Idaho National Engineering and Environmental Laboratory (INEEL) has included a major focus on applying human performance and human reliability knowledge and methods as an integral element of system design and development. This work has been pursued in programs in a wide variety of technical domains, beginning with nuclear power plant operations. Since the mid-1980's we have transferred the methods and tools developed in the nuclear domain to military weapons systems and aircraft, offshore oil and shipping operations, and commercial aviation operations and aircraft design. Through these diverse applications we have developed an integrated approach and framework for application of human performance analysis, human reliability analysis (HRA), operational data analysis, and simulation studies of human performance to the design and development of complex systems. This approach was recently tested in the NASA Advanced Concepts Program "Structured Human Error Analysis for Aircraft Design." This program resulted in the prototype software tool THEA (Tool for Human Error Analysis) for incorporating human error analysis in the design of commercial aircraft, focusing on airplane maintenance tasks. We are currently working to apply our framework to the development of advanced Air Traffic Management (ATM) systems as part of NASA's Advanced Air Transportation Technologies (AATT) program. This paper summarizes our approach, describes recent and current applications in commercial aviation, and provides perspectives on how the approach could be utilized in the nuclear power industry.

Keywords: Human factors, human error, human reliability analysis, human performance, system design, nuclear power, aviation.

I. INTRODUCTION

Many methods of assessing human performance have been developed over the years to better understand human roles in complex systems, particularly focusing on system operation. These methods have been successfully applied to a large number of diverse domains, including military weapons and aircraft, nuclear power plants, offshore oil processes, space operations, and commercial aviation. Also, in certain domains (especially nuclear power), methods of human reliability analysis (HRA) have been developed to better understand and quantify the human role in system reliability for the purpose of Probabilistic Risk Assessment (PRA). The result of these activities is that powerful analytic, simulation, and predictive methods are available to describe how humans contribute to overall system performance. However, in many applications, efforts to date have focused on only certain human roles in complex systems, especially operations and, to a lesser degree, maintenance. Relatively little attention has been given to the human role in other phases of system development, such as design, construction, programming, assembly, and testing. Also, in most cases, methods of human performance and human reliability analysis have been applied to assess systems after they have been placed in operation rather than during design.

Human performance assessment methods have also been developed for analysis of operational data, to understand the human role in the initiation, development, and mitigation of accidents and incidents. These assessments, in many cases, have focused on identifying the causes and contributing factors that lead to accidents and incidents, and sometimes to assess broader trends that can only be detected when a large number of events have been reviewed. However, for the most part, the lessons learned from operational experience have not been effectively utilized to modify existing designs or to guide the design of new systems to prevent operational problems that have been detected in past operations.

Human factors research at the Idaho National Engineering and Environmental Laboratory over the last few years has focused on the development of an effective framework to apply human performance and human reliability methods

DISCLAIMER

to the full system development cycle, so that the full effectiveness of the methods to enhance design quality and system performance can be realized. We believe that the maximum leverage of human factors methods is obtained when applied as early as possible in system development, for example during the identification of requirements and during the process of system design. Also, we believe that human performance and human reliability methods can be applied to engineering processes as well as to the operation and maintenance of the resulting system. For example, system design is a human activity just as much as is operation, so human performance and reliability in performing design tasks can be evaluated using the same methods. We also believe that system design should rely to the greatest degree possible on the lessons learned from operational experience, so that design mistakes of the past are not repeated. Finally, we believe that human performance and human reliability methods should be directly integrated with the engineering processes and program management activities involved in system development, rather than functioning as an add-on to the system development process. The methods and framework developed can serve as a common language for communication among engineers, designers, human factors personnel, risk management experts, and program management.

II. APPROACH

Fig. 1 illustrates the main features of the integrated design environment for human performance and human reliability analysis that is under development at INEEL. The framework is comprised of five major elements:

- Lessons learned
- Functional analysis
- Simulation
- Human performance and human error analysis
- Design engineering tools

Each of these elements is described in greater detail in the following sections.

A. Lessons Learned

The effective extraction of lessons learned from operational experience is a key factor in the development of quality designs for complex systems. Much operational data analysis focuses on statistical analysis of key parameters associated with a class of accidents and incidents. However, it is difficult to extract usable design guidance from such quantitative analyses. Rather, we believe that it is important to extract qualitative, contextual information from operational experience so that lessons can be learned about the influences that lead to human error and to guide designs to eliminate to the degree possible those error inducing situations. To this end, we have developed and applied analytic methods that can be used to interpret operational data to extract qualitative lessons learned across a range of events. We have applied these methods to the evaluation of incidents in nuclear power plants, offshore oil operations, nuclear medicine, marine casualties, and commercial aviation.

B. Functional Analysis

An important foundation of system development is functional analysis. Functional analysis is used to identify those critical functions related to safety, production, economics, etc. that must be optimized during design and maintained during operation to ensure that system objectives are achieved. The functional analysis approach that we have developed at INEEL is based on the systematic identification of critical functions, the tasks (human, hardware, and software) that are performed to maintain them, the resources that can be utilized to maintain the functions, and the support systems that are required for the operation of the resources. Once a functional model is developed, it can be used to identify system vulnerabilities to single or combined component and human failures, explore the performance of the system in response to any number of operational scenarios, explore various design alternatives from a functional perspective, or assess human performance in simulation or operational tests. In addition, a functional model can serve as the basis for procedures or computerized operator support systems, particularly to guide critical function maintenance during off-normal conditions.

At INEEL we have developed and applied functional analysis methods in a number of domains. Our first application was to the development of procedures and computerized operator support for an INEEL test reactor [1]. More recently, we have used functional models to identify information requirements for severe accident management in commercial nuclear power plants [2], assess the problem solving performance of fighter pilots in simulated air combat [3], and evaluate human errors in altitude deviations in commercial glass cockpit aircraft [4].

C. Simulation

Simulation of course can play an important role in helping incorporate human performance and human reliability knowledge into system design. Various design

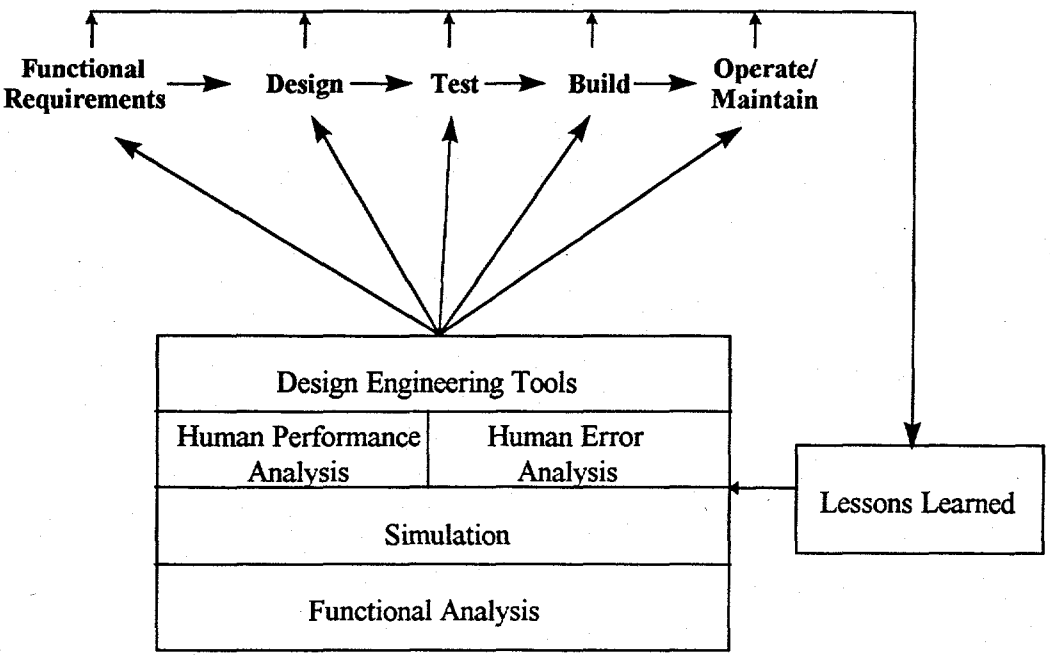

Fig. 1. Integrated Design Environment for Human Performance and Human Reliability Analysis

alternatives can be tested in the simulation laboratory to investigate the advantages and disadvantages of various design features relative to human performance and reliability. Simulation is particularly effective when it is integrated into the total design environment, so that the insights gained from operational data analysis and human reliability evaluations can be used to identify what information is required from a simulation study and to assist the experimental design. Simulation is used most effectively when it is an integral part of the design-test-modify process rather than simply a "laboratory" for major experiments where "statistically significant differences" are sought to support a theoretical hypothesis regarding human behavior. Rather, simulation should be viewed as a powerful tool with which to try out various design alternatives in a tightly-coupled feedback loop to investigate design options.

INEEL experience in utilizing simulation to support system development includes a major series of studies in the early 1980's to test and evaluate display concepts and decision support systems for nuclear reactor operators [5]. A major feature of this program was a close coupling to the experimental program in the Loss of Fluid Test (LOFT) facility, so that results gained from simulation study could be compared with experience in an operating test reactor where system and crew performance could be examined under actual accident situations.

D. Human Performance and Human Error Analysis

Other key components of the INEEL integrated design environment include structured methods for human performance analysis and human error analysis. These are largely based on task modeling methods, performance shaping factors, and logic structures developed for human reliability analysis. We have expanded them and adapted them for use in system development. For the purposes of this paper, HEA is the systematic identification and modeling of potential human errors in the design, construction, operation, or maintenance of a technical system. As a means of comparison, HRA is specifically aimed at the development of quantitative estimates to support PRA, and thus is a specific type of HEA application.

Structured methods of human performance and human error analysis can be used to systematically evaluate system design features and assess their suitability when compared with functional or reliability objectives for overall system performance. In particular, human error analysis can be used to help identify potential human errors, how they interact with other errors and component failures to lead to serious consequences, and potential strategies to prevent or mitigate the consequences of specific errors.

INEEL has developed and applied numerous HRA techniques in performing PRAs and other analyses for the Nuclear Regulatory Commission. Since 1994 we have led a partnership comprised of INEEL, NASA Ames

Research Center, and Boeing Commercial Airplane Group to develop HEA methods suitable for use in the design of commercial aircraft in a program called "Structured Human Error Analysis for Aircraft Design". This effort, sponsored by the NASA Advanced Concepts Program, has focused on identifying errors that could occur in airplane maintenance, and strategies for design or procedure modifications that could minimize the likelihood or consequences of such errors. Trial applications of the methods to airplane engine maintenance tasks confirmed the applicability of the selected HEA methods in the aviation environment.

E. Design Engineering Tools

The final element of the INEEL integrated design environment for human performance and human reliability analysis is a set of design engineering tools. These tools, currently under development, allow the systematic application of the other elements of the design environment in the system development process. As illustrated in Fig. 1, these tools will allow the results of analyses to be applied at all phases of the system development process. Different tools will be appropriate for different stages in the process. For example, functional analysis tools can be used very early in the development process, before any design details are available. Even at this stage, systematic identification and evaluation of the critical functions and possible task structures will allow a systematic assessment of system vulnerabilities to functional failures, and to support the development of design requirements that will optimize system design from the functional perspective. Later in the process when design details become available, human reliability analysis and human error analysis can be called upon to perform detailed assessments of different design options.

The first major design engineering tool developed at INEEL is the Tool for Human Error Analysis (THEA), developed as a major product for the NASA "Structured Human Error Analysis for Aircraft Design" program. THEA builds upon a methodology called FRANCIE (Framework Assessing Notorious Contributing Influences for Error) to model human tasks for airplane maintenance, identify potential performance shaping factors that contribute to error, and to estimate the likelihood of error combinations to lead to serious consequences. In addition, THEA facilitates the evaluation of different design options to determine those that will be most effective in reducing the likelihood and consequences of maintenance errors. THEA is designed to be used by airplane designers and procedure writers, to make available the expertise of human reliability experts for their design or procedure development tasks.

III. PLANNED APPLICATIONS OF THE INTEGRATED DESIGN ENVIRONMENT

We have developed our approach for an integrated design environment through the conduct of a large number of design and analysis programs at the INEEL over the last twenty years. Now that we have developed a framework to integrate the methods and tools that have been developed, we are seeking applications that will allow us to test and further develop the framework in the full scope system development process. Our first major application of this nature will be the NASA Advanced Air Transportation Technologies program. This program will develop and test the technologies and systems required to implement next-generation air traffic management systems. Our role will be to incorporate human reliability considerations in the system development, testing, and evaluation processes for AATT. This represents an excellent opportunity to perform an extensive test of our design environment, and to identify and implement additional methods and tools that are needed to fully realize the benefits of an integrated design environment for human performance and human reliability analysis.

IV. APPLICATION TO NUCLEAR POWER DESIGN AND OPERATION

Many of the methods and tools that we have utilized in developing our design environment were originally developed and tested in the nuclear power domain in studies for the Nuclear Regulatory Commission and the Department of Energy. Thus we are certain that the basic methods can be readily applied to the design and operation of nuclear power plants. However, the bulk of the studies we performed in the nuclear industry were focused on the assessment of existing systems rather than during design, and most focused on plant operations rather than maintenance or other tasks that are part of system development. However, our experience in applying the methods to design tasks for commercial aviation gives us confidence that similar applications would be possible in the nuclear power industry. In particular, we believe that such an integrated design environment would be particularly beneficial for the development of control strategies and operator support systems for advanced reactor designs.

V. CONCLUSIONS

An integrated design environment for human performance and human reliability analysis is under development at the Idaho National Engineering and Environmental Laboratory. Various elements of this environment have been developed and tested in numerous applications in a wide variety of domains. We are currently beginning a large scale application and test of the design environment

for the development and evaluation of advanced air traffic management systems. Such an integrated design environment, if applied during the development of nuclear power plant systems, could help ensure that knowledge of human performance and reliability is effectively utilized, and potential human errors have been identified and systematically controlled.

VI. ACKNOWLEDGMENTS

Work supported by the National Aeronautics and Space Administration, under DOE Idaho Operations Office Contract DE-AC07-94ID13223.

VII. REFERENCES

[1] Nelson, W.R. (1980). "Response Trees for Emergency Operator Action at the LOFT Facility," ANS/ENS Topical Meeting on Thermal Reactor Safety, Knoxville, TN, April 7-11, 1980.

[2] Hanson, D.J., L.W. Ward, W.R. Nelson, and O.R. Meyer (1990). "Accident Management Information Needs," U.S. Nuclear Regulatory Commission, NUREG/CR-4966, October 1990.

[3] Blackman, H.S., H.A. Hahn, and W.R. Nelson (1992). "Complex Human Performance Measurement in an Aviation Environment," Human Performance, Vol. 5, No. 4, 1992.

[4] Nelson, W.R., J.C. Byers, L.N. Haney, L.T. Ostrom, and W.J. Reece, 1993. "Lessons Learned from Pilot Errors Using Automated Systems in Advanced Technology Aircraft," ANS Topical Meeting on Nuclear Plant Instrumentation, Control, and Man-Machine Interface Technologies, Oak Ridge, TN, April 18-21, 1993.

[5] W.E. Gilmore, D.I. Gertman, and H.S. Blackman, *User Computer Interfaces in Process Control: Essential Human Engineering Guidelines*, Cambridge: Academic Press, 1989.

VIII. BIOGRAPHY

William R. Nelson is the Group Leader for Human Factors for Lockheed Martin Idaho Technologies Company at the Idaho National Engineering and Environmental Laboratory. He has been at INEEL since 1976 except for the period 1988-91, when he served as the Section Leader for Man-Machine Interaction Research at the OECD Halden Reactor Project in Norway. His research interests focus on the development of methods to incorporate human performance and human reliability methods in the system development process. He holds a B.S. Degree in Physics from Seattle Pacific College and an M.S. Degree in Nuclear Engineering from the University of Washington.

This report was printed specifically for your order from nearly 3 million titles available in our collection.

For economy and efficiency, NTIS does not maintain stock of its vast collection of technical reports. Rather, most documents are printed for each order. Documents that are not in electronic format are reproduced from master archival copies and are the best possible reproductions available. If you have any questions concerning this document or any order you have placed with NTIS, please call our Customer Service Department at (703) 487-4660.

About NTIS

NTIS collects scientific, technical, engineering, and business related information — then organizes, maintains, and disseminates that information in a variety of formats — from microfiche to online services. The NTIS collection of nearly 3 million titles includes reports describing research conducted or sponsored by federal agencies and their contractors; statistical and business information; U.S. military publications; audiovisual products; computer software and electronic databases developed by federal agencies; training tools; and technical reports prepared by research organizations worldwide. Approximately 100,000 *new* titles are added and indexed into the NTIS collection annually.

For more information about NTIS products and services, call NTIS at (703) 487-4650 and request the free *NTIS Catalog of Products and Services*, PR-827LPG, or visit the NTIS Web site **http://www.ntis.gov**.

NTIS
Your indispensable resource for government-sponsored information—U.S. and worldwide

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Technical Information Service
Springfield, VA 22161 (703) 487-4650