INEL--95/00174
CONF--9506175--5

LESSONS LEARNED FROM THE INTRODUCTION OF COCKPIT AUTOMATION IN ADVANCED TECHNOLOGY AIRCRAFT

William R. Nelson, James C. Byers, Lon N. Haney, Lee T. Ostrom, and Wendy J. Reece
Idaho National Engineering Laboratory
Lockheed Idaho Technologies Co.
P.O. Box 1625
Idaho Falls, ID 83415-3855
(208) 526-0575

ABSTRACT

The commercial aviation industry has many years of experience in the application of computer based human support systems, for example the flight management systems installed in today's advanced technology ("glass cockpit") aircraft. This experience can be very helpful in the design and implementation of similar systems for nuclear power plants. The National Aeronautics and Space Administration (NASA) sponsored a study at the Idaho National Engineering Laboratory (INEL) to investigate pilot errors that occur during interaction with automated systems in advanced technology aircraft. In particular, we investigated the causes and potential corrective measures for pilot errors that resulted in altitude deviation incidents (i.e. failure to capture or maintain the altitude assigned by air traffic control). To do this, we analyzed altitude deviation events that have been reported in the Aviation Safety Reporting System (ASRS), NASA's data base of incidents self-reported by pilots and air traffic controllers. We developed models of the pilot tasks that are performed to capture and maintain altitude. Incidents from the ASRS data base were mapped onto the models, to highlight and categorize the potential causes of the errors. This paper reviews some of the problems that have resulted from the introduction of glass cockpit aircraft, the methodology used to analyze pilot errors, the lessons learned from the study of altitude deviation events, and the application of the results to the introduction of computer-based human support systems in nuclear power plants. In addition, a framework for using reliability engineering tools to incorporate lessons learned from operational experience into the design, construction, and operation of complex systems is briefly described.

I. BACKGROUND

A significant effort is underway to introduce advanced technology into the control rooms of nuclear power plants. Outdated analog control systems are being replaced by digital systems. In some cases the system functionality remains the same, but in other cases the digital technology is utilized to change system operation and thus the role of the operating crew. Also, evolutionary and advanced "passive" reactor designs will make fundamental changes in the control systems and the roles of the operating crew. In general, there will be a greater tendency to automate certain subsystem functions to optimize plant operation and transient response. These changes are revealing human factors issues associated with the introduction of advanced technology and the resulting effects on crew performance.

The introduction of advanced technology into power plant control rooms is often done with a technology-driven motivation. That is, advanced digital systems have the capability to monitor more parameters, perform more analyses, display more data, and automate more functions than ever before. Plant designers are selecting such technologies with a view toward reducing operating costs and improving plant availability and efficiency. However, to achieve such goals requires the effective integration of the new technology with the humans that operate the plant.

Other industries have longer experience with the introduction of advanced technology into the operating environment, and the resulting influences on human performance. In many cases the results have not been entirely positive. The introduction of automation can reduce operator workload and error for many tasks, but entirely new interactions and error modes can be inadvertently introduced. The nuclear industry would do well to learn from the positive and negative experiences of other industries before making irrevocable choices regarding the functionality of advanced control systems.

One industry with substantial experience in the use of advanced technology and automated systems is commercial aviation. From the introduction of autopilots in the 1930's to today's CRT- and flat panel-based "glass cockpit" aircraft with Flight Management Systems (FMSs) that can automate essentially all phases of flight, the aviation industry has a large experience base that the nuclear industry can benefit from. Advanced technology in the cockpit has, for the most part, increased pilot efficiency and reduced workload. However, some unexpected results have been observed. It has been found

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

that the primary reduction in workload occurs during periods when workload is already low (e.g., during long periods of cruise), but that workload can actually increase during busy times (e.g., when the landing clearance is changed during descent into a busy terminal control area). In addition, entirely new types of error have been introduced.

The introduction of sophisticated autopilot, flight control, and flight management systems on modern aircraft such as the Airbus A310, A320, A330, and A340 series, the Boeing 747-400, 757, 767 and 777, and the McDonnell Douglas MD-80/90 and MD-11 has resulted in significant changes in the operation of these aircraft. The flight crews have shifted to more of a system manager role rather than that of in-the-loop pilots. The advanced technology has reduced workload so that crews have been reduced from three to two, with the role of the flight engineer taken over by the computerized flight management system. Workload has been reduced for many inflight tasks, but increased for others, for example reprogramming the FMS to implement flight plan modifications specified by air traffic control.

There is a growing awareness in the aviation industry that the introduction of advanced technology into the cockpit has not been without drawbacks. A number of accidents and incidents involving glass cockpit aircraft have revealed significant issues regarding the design of the flight management systems and their user interfaces. For instance, advanced cockpit technology may have played a role in crashes involving three Airbus A320 aircraft, at Habsheim in 1988, Bangalore (1990), and Strasbourg (1992), and an Airbus A300-600 at Nagoya in 1994.[1] Also, an Airbus A330 crashed at Toulouse on June 30, 1994 while undergoing flight tests with the Airbus chief test pilot in the captain's seat.[2] In addition, a study of Aviation Safety Reporting System incident reports has revealed at least 184 mode awareness incidents (in which confusion about flight management system status leads to a reportable incident) during a four year period.[3] Sufficient concern has been raised in the aviation industry that the National Transportation Safety Board (NTSB) has recommended that the Federal Aviation Administration (FAA) require additional training on autopilot operation and changes to certain autopilot functions.[4] Finally, the FAA itself has commissioned an in-depth study to help determine how problems in interaction between the flight crew and automated systems may influence flight safety.[5]

A number of research programs have been conducted to help identify the factors that may lead to errors in advanced technology aircraft. For example, Sarter and Woods performed a study of pilot experiences and opinions regarding the advanced systems available in the cockpit.[6] They found that many pilots do not understand the logic and algorithms that underlie the automation, and hence cannot always anticipate what the automation will do, and are sometimes surprised by mode transitions they do not expect. Pilots have also expressed the concern that they may not adequately understand the effects of a partial failure of the flight management system.

This study and others have identified certain factors that may lead to flight crew errors in glass cockpit aircraft:

- Too much complexity has been built into flight management systems, so that pilots cannot understand all the possible modes of operation nor their interactions with flight controls.

- The user interfaces sometimes provide inadequate feedback about what the automated systems are doing.

- Pilots aren't always aware when the flight management system changes from one mode to another, and don't understand why the airplane is responding the way it does.

- In some airplanes the automated systems can actually "fight against" the pilot's control actions. This is particularly true on Airbus airplanes, which have "hard automation" envelope protection that puts limits on the control actions the pilot can take. Boeing and McDonnell Douglas airplanes allow the pilot to overcome the automated actions by applying more force to the control column.

- Some airlines have modified their training programs so that managing the automated systems is given more attention than in-depth understanding of system functions.

In order to gain increased understanding of flight crew interactions with automated systems, NASA commissioned a study at the Idaho National Engineering Laboratory to investigate the applicability of methods of human error analysis and human reliability analysis, as used in the nuclear power industry, to the study of altitude deviation errors that occur in "glass cockpit" aircraft. The following sections describe how these methods were used to analyze pilot errors, the results of the analysis, and potential applications of the lessons learned to the nuclear industry.

II. METHOD

A. Development of Task Models.

Models of the tasks that are performed to capture and maintain altitude in "glass cockpit" aircraft were developed. In order to provide a more complete picture of altitude deviation errors, two complementary perspectives were used, based on different approaches to the modeling of human error. The first, called the sequential model, was designed to show the prescribed sequence of actions involved in altitude maintenance, and the points at which errors can occur. Human reliability analysis (HRA) event trees[7] were used to develop the sequential models. Functional models provided a complementary perspective. The functional model is a hierarchical structure that starts at the top with an overall objective, the critical functions that must be performed to reach the objective, the tasks and subtasks that contribute to the performance of the critical functions, and the resource options (e.g. hardware systems) that are available to the crew for performing the tasks. Modern transport aircraft are designed so that there is more than one way to perform many of the critical functions, so that safety can be maintained even if certain component failures occur. The different methods for maintaining each critical function are referred to as success paths.

The top level functional model that was developed for this project includes six functions: Takeoff, Flight Control, Monitor Flight Conditions, Navigation Planning, Monitor Navigation Process, and Landing. These were broken down into tasks, and the tasks were further broken down into subtasks and the resources needed to perform each of the tasks and/or subtasks.

B. Analysis of Data.

The primary source of data used for this study of altitude deviation events was the Aviation Safety Reporting System (ASRS), NASA's third-party reporting system for incidents that occur in flight. The most common type of incident that is reported to the ASRS is altitude deviations, so the ASRS is a rich source of data regarding actual events. Two hundred ASRS reports were reviewed. These reports were generated by a search of the database for reports that referenced altitude deviations in advanced glass cockpit aircraft. The reports were drawn from full-form records and describe altitude deviations that occurred between April 1991 and January 1992. These ASRS reports were subjected to an initial screening to identify those where the advanced technology (e.g. autopilot, flight management system, etc.) actually played a role in the incident. Then, the remaining reports were "mapped onto" the sequential and functional models to allow consistent interpretation. Mapping of the ASRS report onto the sequential model highlighted the location in the sequence of actions where the error occurred, whether available recovery paths were used, and what interventions could have been used to prevent such errors. Mapping of the ASRS reports onto the functional model highlighted the context in which the error occurred, and whether inappropriate attention to other critical functions contributed to the occurrence of the error.

III. RESULTS

A. Altitude Deviation Errors in Advanced Technology Aircraft.

The application of model-based human error analysis has revealed many things regarding the characteristics of altitude deviation events in advanced technology aircraft. The mapping of ASRS reports of altitude deviations has provided a systematic method for classifying the errors that occur. These classifications can then be used to suggest remedies for preventing the errors or mitigating their consequences.

Within the grouping of errors, we observed that three specific types of errors were predominant.

- Errors that occurred because the flight crew did not understand the details of FMS functions. These types of errors could possibly be prevented by improved training regarding FMS functions, or the redesign of the systems so that the representation of status is more apparent to the crew.

- Errors that resulted from incorrect manipulation or monitoring of automated systems. This type of error could potentially be prevented by redesign of the displays and controls to provide better feedback to the flight crew.

- Errors that occur when the pilot understands the function of the autoflight systems, but errors have been introduced from an external source such as maintenance or design errors. These errors could potentially be prevented by a redesign of automated systems taking into account the pilots' expectations of the system.

Our study of altitude deviation errors has led us to a number of general observations about the factors that lead to these incidents. It appears that pilots have learned to rely on their automated systems, and have delegated control of not only flight functions, but also monitoring functions, to the automation. Thus, they are not watching for deviations to occur, but tend to assume that the autoflight systems will take care of altitude capture and maintenance. Some pilots seem to be predisposed to assume that the automated systems will do what they (the pilots) expect them to do, when in some circumstances the automation "wants" to do something else. These factors imply that the role of the pilot has in some circumstances changed so that they are flying the flight management system rather than the aircraft itself. The final result is the relaxation of the pilot's instinct to "stay ahead" of the airplane and decreased vigilance regarding the maintenance of critical flight functions.

B. Application of Results to the Nuclear Industry.

The lessons learned from this study of pilot errors in advanced technology aircraft can be applied in the nuclear industry on a number of levels. On a high level, the general results obtained from this study can be used to sharpen our expectations of what we will observe when advanced technologies are introduced into the control rooms of nuclear power plants. We should not assume that the introduction of advanced technology will be an unmixed blessing, resulting only in reduced operator error and workload. Rather, we should probably expect that, similar to the flight environment, control room workload may decrease during periods of low activity, but that workload may actually increase during busy times such as mode changes or disturbances.

On a more detailed level, we may expect that some of the specific results obtained from the study of pilot errors may also carry over into the nuclear application. For example, it is quite possible that we may observe errors that result when reactor operators do not understand the details of the functioning of their advanced automated systems, or errors that occur when automated systems are activated or manipulated incorrectly. Because these errors still persist in aircraft after many years of experience, it would be beneficial for the nuclear industry to attempt to explicitly eliminate or compensate for these types of errors in the design of advanced systems.

C. Design for Safety Framework

At the Idaho National Engineering Laboratory we are building upon the above methods to develop a framework for designing complex systems and structures to ensure that the maximum level of safety and reliability is achieved. This framework is designed to provide a systematic way to apply lessons learned from operational experience to the design of new systems. The approach is based on the following major elements:

- A systems engineering perspective is used to ensure that safety is designed into the system from the beginning and maintained throughout the system lifecycle.

- Reliability engineering tools are utilized to ensure that potential hazards are identified early in the design process and are eliminated by system design or reduced to a level such that remaining risks are known and acceptable.

- Operational data analysis is used to ensure that maximum information is gained from system testing and operation, and that effective lessons learned are identified and fed back into system design and operating procedures.

These three elements are combined and integrated into the system development cycle as shown in Figure 1. This framework is being applied to a joint INEL/NASA/Boeing/America West Airlines program for incorporating human error analysis into the design of commercial airplanes. The focus to date has been on the identification and resolution of potential human errors in system design, although the framework and methods are equally applicable to hardware design and system integration. We believe that such an approach could also be used to incorporate advanced technology into the design of new nuclear power plant control rooms.

As illustrated in the figure, six separate levels of safety assurance are integrated to create maximum confidence that all significant safety and reliability issues are systematically identified and resolved as early as possible during system design, construction, and testing. The cornerstone of the INEL approach is the application of reliability engineering methods for the systematic assessment of system reliability and potential failure modes. These methods have been adapted from the fields of Probabilistic Risk Assessment (PRA) and functional analysis and tailored for application to system design. The reliability engineering methods are applied in two ways. First, system reliability models are developed and exercised to identify potential functional vulnerabilities and system failure modes that could cause system shutdown, damage to system components, or injury to system users or the public. These specific vulnerabilities can then be eliminated or accommodated through modification to system design or operating procedures. Secondly, the system reliability models are used to interpret the significance of operational experience (including data from system test and evaluation) so that the incidents of degraded operation and system failure can be evaluated and eliminated prior to full system implementation.

As shown in the figure, the reliability engineering tools are used throughout the system development cycle to assess the reliability of the system design and to evaluate potential design changes for their effects on system reliability. In this manner, the design can be incrementally refined and improved throughout the process, and proposed changes can be quickly evaluated to ensure that safety is not compromised.

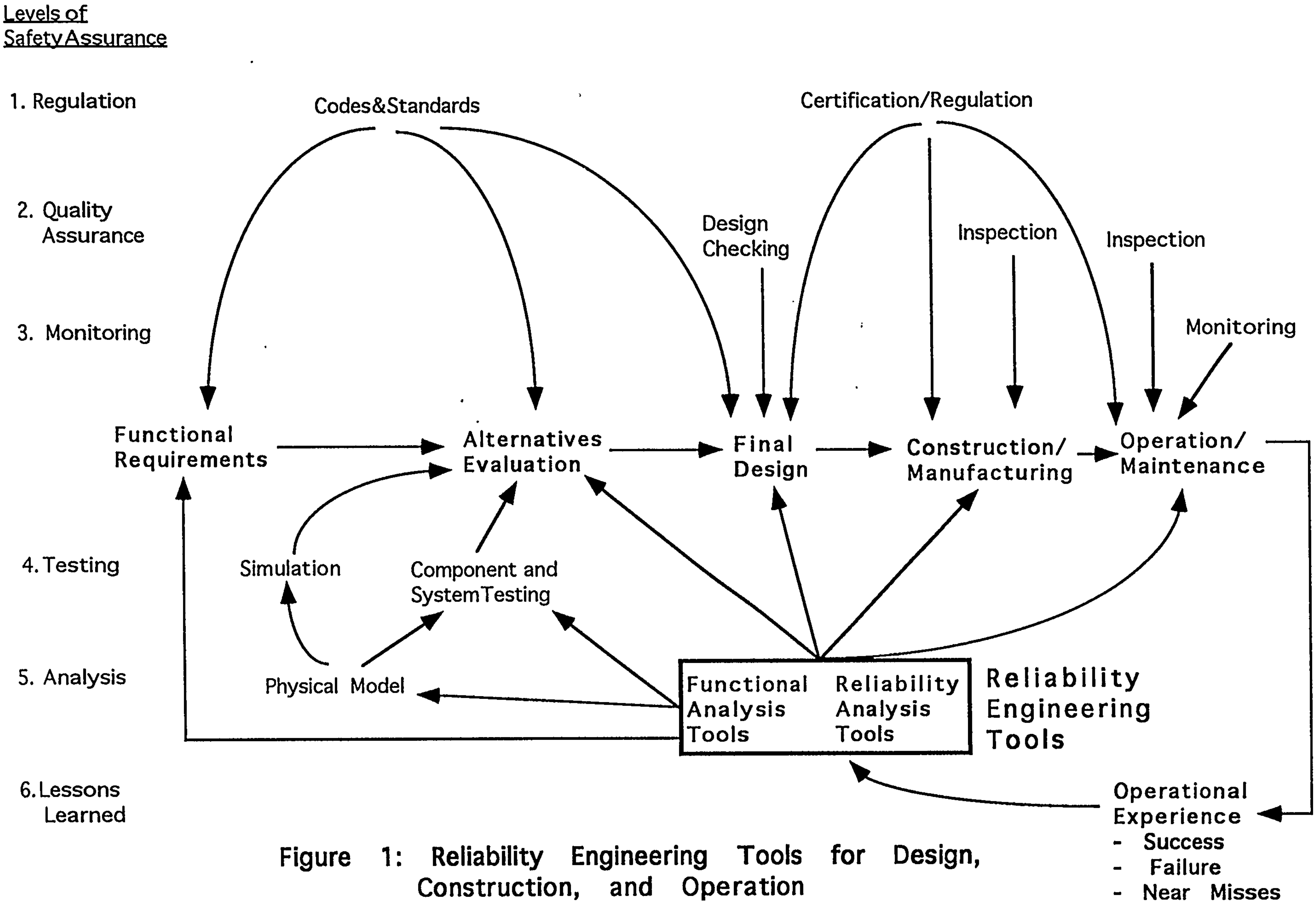

Figure 1: Reliability Engineering Tools for Design, Construction, and Operation

IV. CONCLUSIONS

The introduction of advanced technology and automation into the control room of nuclear power plants must be accomplished with great care. Experience from commercial aviation has shown that a technology-driven approach to system design can introduce unexpected sources of human error. It is necessary to design new control rooms with explicit consideration of the interactions between the operating crew and the advanced control systems, so that technology will serve and assist the human operators in the safe and efficient operation of the facility. Analytic tools such as HRA event trees and functional models can be used to interpret operating experience and analyze operator tasks to help identify potential human errors. Then it will be possible to explicitly account for potential errors in system design, so that the likelihood of system failures due to human error can be decreased.

ACKNOWLEDGMENTS

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

REFERENCES

1. D. Hughes and M.A. Dornheim, "Accidents Direct Focus on Cockpit Automation," *Aviation Week and Space Technology,* January 30, 1995.

2. M.A. Dornheim, "Dramatic Incidents Highlight Mode Problems in Cockpits," *Aviation Week and Space Technology,* January 30, 1995.

3. D. Hughes, "Incidents Reveal Mode Confusion," *Aviation Week and Space Technology,* January 30, 1995.

4. M.A. Dornheim, "Modern Cockpit Complexity Challenges Pilot Interfaces," *Aviation Week and Space Technology,* January 30, 1995.

5. E.H. Phillips, "FAA To Study Human Factors," *Aviation Week and Space Technology,* October 24, 1994.

6. N. B. SARTER and D. D. WOODS, "Pilot Interaction with Cockpit Automation I: Operational Experiences with the Flight Management System (FMS)," Draft, The Ohio State University, Cognitive Systems Engineering Laboratory (1991).

7. A. D. SWAIN and H. E. GUTTMAN, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, U.S. Nuclear Regulatory Commission (1983).

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.