INEEL/CON-99-00295

SESSION: C1
Paper No.: 3

Human-System Safety Methods for Development of Advanced Air Traffic Management Systems

William R. Nelson
Idaho National Engineering and Environmental Laboratory
P.O. Box 1625
Idaho Falls, ID 83415-3855 USA
Wnr@inel.gov

Abstract

The Idaho National Engineering and Environmental Laboratory (INEEL) is supporting the National Aeronautics and Space Administration in the development of advanced air traffic management (ATM) systems as part of the Advanced Air Transportation Technologies program. As part of this program INEEL conducted a survey of human-system safety methods that have been applied to complex technical systems, to identify lessons learned from these applications and provide recommendations for the development of advanced ATM systems. The domains that were surveyed included offshore oil and gas, commercial nuclear power, commercial aviation, and military. The survey showed that widely different approaches are used in these industries, and that the methods used range from very high-level, qualitative approaches to very detailed quantitative methods such as human reliability analysis (HRA) and probabilistic safety assessment (PSA). In addition, the industries varied widely in how effectively they incorporate human-system safety assessment in the design, development, and testing of complex technical systems. In spite of the lack of uniformity in the approaches and methods used, it was found that methods are available that can be combined and adapted to support the development of advanced air traffic management systems.

BACKGROUND

New concepts for air traffic management are under development that will significantly change the way the U.S. National Airspace System (NAS) is operated. The Federal Aviation Administration (FAA) and the National Aeronautics and Space Administration (NASA) are working together to develop and test new technologies for air traffic management that will ultimately replace current air traffic control systems. NASA's efforts are organized under the Advanced Air Transportation Technologies (AATT) program.

The new ATM technologies being developed are intended to support a new NAS operational concept known as free flight. Free flight calls for increased flexibility in the selection of routes for individual aircraft, with substantial support by on-board and ground-based decision support tools (DSTs) to assist the flight crew in maintaining separation from other aircraft and resolving potential conflicts. Ground based controllers will under normal circumstances monitor traffic flow and separation, but will be expected to step in to prescribe corrective actions if separation minimums are expected to be violated.

DISCLAIMER

Implementation of such a free flight concept will fundamentally alter the roles and responsibilities of flight crews and ground controllers. Additionally, new computer-based decision support tools will assume certain responsibilities. The division of responsibility among flight crews, ground controllers, and computerized aids will be dynamic, varying with operating conditions. Flight crews will assume new tasks compared to current operational practices, such as monitoring traffic information, monitoring and interacting with the DSTs, and communicating with other flight crews to resolve potential airspace conflicts. Ground controllers will assume a largely supervisory role, monitoring the "health" of the airspace, looking for potential conflicts that may require active intervention, and developing corrective actions (supported by the DSTs) when such actions are warranted.

The dilemma of this approach is that the above factors could add increased complexity to the operation of the NAS, even while they contribute to the goals of increasing NAS capacity and efficiency while decreasing operational costs. One of the most important components of system safety for ATM systems is the human contribution. All of the computer-based DSTs and other systems are intended to support the ultimately human responsibility to maintain adequate aircraft separation. Experience has shown that the introduction of computer-based systems to support human tasks can have unanticipated effects on human performance, including the possible introduction of new types of human error.

HUMAN-SYSTEM SAFETY APPROACHES IN OTHER INDUSTRIES

Offshore Oil and Gas

The approach to human-system safety used in the offshore oil and gas industry has been greatly influenced by the fire and explosion that occurred on the Piper Alpha platform in the North Sea on July 6, 1988. In part because the platform was laid out so that the living quarters were inaccessible to rescuers, 167 lives were lost. The resulting investigation and recommendations had a great influence on the safety evaluation and regulation of offshore facilities, particular in the U.K. and the North Sea[1].

The public inquiry concluded that the fire and subsequent explosion occurred because workers were unaware that certain piping had been removed for maintenance, leading to the release of volatile condensate. The inquiry also concluded that this situation was the result of inadequate management systems for controlling the work, and that safety systems were inadequately designed for the scenario that was experienced. This accident occurred in spite of the fact that the platform had recently been inspected by the regulatory authorities, and had been found in compliance with all existing regulations.

The Piper Alpha accident was a watershed incident for the offshore oil and gas industry in the same fashion that Three Mile Island led to fundamental changes for the worldwide nuclear industry. Piper Alpha brought home the lesson that compliance with static safety regulations is not always adequate, but rather that regulators, designers, and operators of high risk facilities need to pay attention to the processes by which systems are designed and work is planned and carried out. Piper Alpha had different effects on industry practices in the U.K. and U.S., in part due to the different proximity to the event and degree of public awareness in the two countries.

UK Safety Case Regulations

In the aftermath of the Piper Alpha accident all regulation of U.K. offshore activities was transferred to the Health and Safety Executive[2]. HSE established regulations regarding the

development and evaluation of the Safety Case for each offshore facility. The Offshore Safety Division of HSE is charged to ensure that risks to people from work activities in the "upstream" petroleum and diving industries are properly controlled.

Each safety case must include a full determination of:

- Significant hazards present on the installation
- Risks of their occurrence
- Options for treating unacceptable risks
- Proper systems for emergency evacuation, escape, and rescue.

All possible accidents must be considered including fires and explosions, structural damage, loss of stability, and helicopter and diving accidents. The safety case should describe the approach to preventing accidents, mitigating the effects of any which occur, and providing for emergency response, evacuation and rescue.

In addition, rather than establishing a specific safety goal for all installations, the requirement is that all facilities will seek to drive risk to the level described as "as low as reasonably practicable" (ALARP). This implies that organizations should not be satisfied by achieving a certain prescribed level of safety, but should continuously work to identify, reduce, and manage hazards and the associated risks. Methods of Quantitative Risk Assessment (QRA) are used to model and quantify the risks and to evaluate possible methods for reducing risks.

Safety and Environmental Programs in the U.S.

In contrast to the U.K. Safety Case approach, the U.S. offshore oil and gas industry is currently testing the suitability of voluntary practices for controlling the safety of offshore installations. The U.S. Minerals Management Service (MMS), the government agency responsible for regulation of offshore facilities, recommended in 1991 that all facilities should develop a Safety and Environmental Management Program (SEMP) (Reference 2). In 1994 MMS endorsed the American Petroleum Institute Recommended Practice API RP 75 "Recommended Practices for Development of a Safety and Environmental Management Program for OCS (Outer Continental Shelf) Operations and Activities.[3]" The philosophy of API RP 75 is that management of hazards should be an integral part of the design, construction, maintenance, and operation of offshore facilities. Another API Recommended Practice, API RP 14J, "Recommended Practice for Design and Hazards Analysis of Offshore Production Facilities" presents design principles for mitigating hazards and possible methods for performing hazards analysis.

In lieu of mandatory government regulations, MMS is currently monitoring the progress of the U.S. offshore industry toward voluntary compliance with the provisions of API RP 75. By 1997 93% of operators on the Outer Continental Shelf had implemented some form of SEMP, representing 99.2% of the total production capacity on the OCS. If MMS deems that voluntary compliance with the goals of SEMP is adequate to control the hazards of offshore operations, government regulation of SEMP will not be instituted.

Military

The program names are different, but the total system integration approach is utilized throughout the American armed forces. Theses military programs integrate management, human factors engineering, manpower, personnel, training and health hazard assessment throughout the systems design, operational and decommissioning life cycle. These programs emphasis front end

planning (including user consideration) with a strong emphasis on the controlling management structure. These total system programs stress systems integration as the key element to proper system design. The program used by the U.S. Army is called MANPRINT[4].

MANPRINT

MANPRINT is a comprehensive philosophy for material acquisition and system integration. Its primary focus is to enhance overall system quality in order to maximize benefits and reduce waste and harm. MANPRINT represents an attempt to shift from an "equipment oriented culture" to a "people oriented culture" within the military. A primary hallmark of MANPRINT is that it considers soldier performance and equipment reliability together in a "total system" view.

Within the Army, the MANPRINT Program evolved from concerns about the lack of adequate consideration to human factors, manpower, personnel, and training (HMPT) issues in the weapon system acquisition process. The Army Research Institute's Reverse Engineering Program, initiated in 1982, documented shortfalls in system design and performance resulting from inadequate attention to HMPT issues. MANPRINT was designed as the human systems integration process to ensure that the human is fully and continuously considered as a part of the total system in the development and/or acquisition of all systems. Additionally, MANPRINT ensures that human performance is always considered as part of "total system performance."

MANPRINT is an umbrella concept encompassing human factors, engineering, manpower, personnel, training, health hazards assessment, and system safety. The focus of MANPRINT is on total system planning. MANPRINT examines management's influence on system design and associated support requirements to ensure that military systems can be operated and maintained in the most cost effective and safest manner. An essential point of the methodology is that it emphasizes front-end planning. As currently used by the Department of Defense, MANPRINT integrates system training and material development with personnel resources, capabilities, and constraints during all phases of the life cycle of material systems.

Aviation

Flight Deck Design

One of the first aviation fields to benefit from explicit treatment of human factors was flight deck design. In the early years of airplane design it became apparent that "flyability" of the airplane was a significant design issue. Experienced pilots were enlisted to fly (and perhaps crash) new designs and to provide feedback on "flying qualities" to the design team. Rapid advances in airplane responsiveness and controllability were made possible by this approach. To this day the test pilot is a valued member of the airplane design team, and his (and more recently her) recommendations are always an important factor in flight deck design.

As human factors techniques and guidelines were developed in the years following World War II, military and later commercial airplane designers were some of the first groups to apply them as an integral portion of flight deck design. In recent years, emphasis has been given increasingly by airplane manufacturers to the integration of human factors engineers as integral members of the airplane design team.

Boeing's philosophy for an effective aircraft system is the requirement to incorporate human factors input throughout the design life cycle, from concept formulation, through detailed design,

to fabrication and operation. Boeing utilizes an integrated product team approach. The team consists of human factors engineers (both physical and cognitive), operational experts (former or current test pilots) and design engineers. The design process for a new or improved aircraft usually spans three to four years. Human factors support continues through the entire life cycle.

Cockpit Automation

In recent years the transition from analog displays and manual control to digital displays and automated systems has presented many significant human-system safety issues, especially related to cockpit automation. While automated flight management systems are intended to reduce flight crew workload and (at least indirectly) opportunities for human error, many unexpected issues have arisen, including the introduction of entirely new opportunities for human error. As the role of the flight crew has shifted from manual control to supervisory control of automated systems, increased attention has been given to the cognitive and communication activities of flight crews, including situation awareness, crew resource management, and information presentation and integration. This trend will only be accelerated as free flight technologies are introduced, and as new cognitive tasks and dynamic responsibility shifts will be added to pilot and controller job descriptions. Much research in commercial aviation has been devoted to the issues of cockpit automation, including a NASA study conducted by INEEL to discover how the use of automated cockpit systems contributed to human errors leading to altitude deviations.[5]

The China Airlines Nagoya accident highlighted the potential hazards that can be introduced through the introduction of cockpit automation. In the aftermath of this accident (perhaps another "watershed" event) the FAA chartered a human factors team to identify human factors issues associated with cockpit automation, and to provide recommendations for how these issues might be resolved. Following a comprehensive review of the experience involving modern flight deck systems, the human factors team identified the following broad categories of issues[6]:

- Measurement of and incentives for safety
- Management of automation
- Flightcrew situation awareness
- Communication and coordination
- Processes for design, regulatory, and training activities
- Criteria, regulatory standards, methods and tools for design and certification
- Knowledge and skills of designers, pilots, operators, regulators, and researchers
- Cultural and language differences.

Comprehensive recommendations were made to address each of these categories of issues. While these recommendations focused primarily on current automation such as flight management systems, the findings, recommendations, and resulting actions should be taken into account for the development and implementation of advanced ATM systems as well.

Airplane Maintenance

In spite of all the attention given to human factors issues and human-system safety in flight deck design, relatively little attention has been paid until recently to the issues of human-system safety for airplane maintenance. In recent years, however, the FAA has conducted a program to address human factors issues for airplane maintenance. In addition, beginning in 1994, NASA Ames sponsored a program explicitly aimed at the development of methods and tools to evaluate human-system safety in airplane design. The particular emphasis of the program was the

identification and reduction of human errors associated with airplane maintenance tasks. This project[7] was conducted by a partnership of INEEL, NASA Ames, Boeing Commercial Airplane Group, and America West Airlines. A major theme for the program was to adapt human reliability methods developed in the nuclear industry for risk assessment purposes so that they could be applied to support airplane design.

Two products were developed as the result of this project: a framework for human error analysis called FRANCIE (FRamework Assessing Notorious Contributing Influences for Error) and a software tool to support human error analysis called THEA (Tool for Human Error Analysis). These tools are currently undergoing testing by U.S. airlines, NASA aeronautics and space programs, and (in the case of FRANCIE) for the certification of instrument landing systems.

Assessment of Operational Experience

Another major activity focused on human-system safety for commercial aviation is the continuous assessment of operational experience to identify human-system safety issues. The NASA Aviation Safety Reporting System (ASRS) collects self-reported incident data from commercial (and to a lesser degree military) flight operations. The data collected in these reports can be used to explore human-system safety issues that have led to incidents or near misses. NASA regularly sponsors issues-oriented research to explore specific issues, such as an INEEL study of human error associated with the use of automated flight management systems[8]. The National Transportation Safety Board (NTSB) includes treatment of human factors and human error when it conducts investigations of aircraft accidents. The NTSB recommendations to FAA sometimes include suggestions for regulatory, design, or procedural changes that could reduce the occurrence of human-related causal factors for airplane accidents.

Nuclear Power

Three Mile Island and Its Aftermath

The Three Mile Island accident resulted in fundamental changes in the worldwide nuclear industry. Most importantly was the recognition of the extremely critical role played by the operating crew in overall reactor system safety. Also, the philosophy of reactor operations for emergency response was dramatically altered. Instead of procedures organized around individual events ("event oriented procedures"), explicit guidance was added to help operators diagnose events based on combinations of symptoms ("symptom oriented procedures"). An even more fundamental change was the recognition that the more fundamental requirement for emergency response was to maintain certain "critical safety functions" (CSFs) such as core cooling, reactor containment, etc. for situations where the diagnosis of a specific event is not possible. This led some plants to develop "function-oriented procedures" that provided guidance for the assessment of the status of the critical safety functions and actions to restore any CSFs that were challenged by the accident.

Another major development in the wake of TMI was substantial efforts by the nuclear community to develop computerized operator support systems to support diagnosis and treatment of nuclear reactor accidents. In spite of significant early optimism regarding the potential of such systems to address fundamental issues of emergency response, difficulties in demonstrating the value of such systems, concerns about software reliability, and the conservative nature of the NRC's regulatory processes has limited the application of such systems in the U.S. By contrast, such computerized operator support systems have been implemented more widely outside the U.S., especially in

France and Japan. In the U.S., the application of digital technology has primarily been limited to functional replacements of outdated analog systems. In many cases the regulatory certification of such systems has been streamlined by the deliberate limitation of system functions to those of the analog system being replaced. However, even in such cases knotty issues of software reliability have arisen, issues that have yet to be fully resolved. The Nuclear Regulatory Commission has expended large research investments to address issues regarding the risk impacts of the introduction of digital technology in commercial nuclear power plants.

Regulatory Approaches to System Safety

The overall current NRC approach to system safety is based on the use of probabilistic risk assessment to support risk-informed regulatory processes. This emphasis has created a strong drive to quantify risk assessment analyses for nearly the past twenty years. Even after all this effort, there is still a tremendous shortage of raw data to support quantitative risk assessment in the nuclear industry. Because of the basically adversarial relationship between regulator and licensees, it is nearly impossible to obtain good quantitative failure probabilities to support PRA. This is especially true when performing human reliability analysis. As a result, much of the quantification depends on methods for estimating the base human error rates. Unfortunately, the estimation methods have been subject to very little formal validation, so the quantitative human reliability analyses are most valuable for sensitivity studies and for comparison between different risk estimates. A more subtle side effect of this emphasis on quantification that relatively fewer resources have been devoted to the development of qualitative safety insights from the logic modeling structures that are developed for human reliability analysis.

The NRC also conducts large programs for these the analysis of operational data to identify influences and trends that contribute to reactor accidents. These analyses include the identification of human performance factors that contribute to incidents. The NRC also conducts in-depth investigations of various categories of events and near misses that occur at NPPs. Human factors specialists are included on the teams that investigate these events. Various methods and tools have been developed to assist the identification of human-related causes and contributing factors that contribute to operating events.

Summary of Lessons Learned from Other Industry Approaches to Human-System Safety

In the industries reviewed, there are many qualitative and quantitative methods to model human contributions to system safety. These methods range from very simple checklists for identifying hazards to very complex modeling structures to assess and measure the human contribution to overall system safety. Many of the most powerful methods have not been specifically developed for treating human-system safety during design, but for "after the fact" assessment of human reliability for risk assessment or "post-mortem" incident investigations. However, most if not all of the modeling approaches developed for assessment purposes can be adapted for use during system development.

A common problem in the assessment of human system safety is the shortage of data to support quantitative determination of human reliability. The estimation methods that have been proposed to substitute for actual data have not been adequately validated to provide confidence in their application to calculate point estimates of human error probabilities. These factors have limited the value of human reliability quantification, except possibly for comparison purposes and sensitivity analyses. Qualitative logic models of human system interactions can be used to gain insights that can guide design, but additional development is required to gain maximum benefit

from their application to system development. Operational evaluations through simulation or field testing are necessary to ensure that design decisions aimed at enhancing human-system safety have achieved their intended benefits.

Assessment of human-system safety has not achieved the same degree of maturity when compared to the methods for assessing the safety of hardware systems. However, research and applications of human-system safety methods over the past twenty years have resulted in a number of approaches that can be effectively applied to the development of advanced air traffic management systems.

ACKNOWLEDGMENTS

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

REFERENCES

1. W. Cullen, *The Public Inquiry into the Piper Alpha Disaster,* London: HMSO, November 1990.

2. TAF Powell, "US Voluntary SEMP Initiative: Holy Grail or Poisoned Chalice," *Offshore Technology Conference, Houston TX, 6-9 May 1996,* OTC 8111.

3. P.K. Velez, "An Overview of API RP 75 and RP 14J," *Offshore Technology Conference, Houston TX, 1-4 May 1995,* OTC 7732.

4. H.R. Booher, *MANPRINT,* New York: Van Nostrand Reinhold, 1990.

5. W.R. Nelson, J.C. Byers, L.N. Haney, L.T. Ostrom, and W.J. Reece, "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.*

6. Federal Aviation Administration, *The Interfaces Between Flightcrews and Modern Flight Deck Systems,* June 18, 1996.

7. L. Ostrom, W. Nelson, L. Haney, R. Richards, C. Wilhelmsen, and R. Owen, *Structured Human Error Analysis for Airplane Maintenance and Design,* INEEL/EXT-97-01093, October 1997.

8. W.R. Nelson, J.C. Byers, L.N. Haney, L.T. Ostrom, and W.J. Reece, "Lessons Learned from the Introduction of Cockpit Automation in Advanced Technology Aircraft," *ANS Topical Meeting on Computer-Based Human Support Systems: Technology, Methods, and Future, Philadelphia, PA, June 25-29, 1995.*