Risk Modeling in Distributed, Large-Scale Systems

Martha Grabowski, Jason R. W. Merrick, John R. Harrald, Thomas A. Mazzuchi, and J. René van Dorp

Abstract—**Risk is inherent in distributed, large-scale systems. This paper explores the challenges of risk modeling in such systems, and suggests a risk modeling approach that is responsive to the requirements of complex, distributed, large-scale systems. An example of the use of the approach in the marine transportation system is given. The paper concludes with a discussion of limitations of the approach and of future work.**

I. Introduction

RISK in complex systems can have its roots in a number of factors. One cause may be that activities performed in the system are inherently risky (e.g. mining, surgery, airline transportation); another may be that technology used in the system is inherently risky, or exacerbates risks in the system (e.g. heavy equipment, lasers, and aircraft). Individuals and organizations executing tasks, using technology, or coordinating also cause risk. Organizational structures in a system may also unintentionally encourage risky practices (e.g. the lack of formal safety reporting systems in organizations, or organizational standards that are impossible to meet without some amount of risk taking). Finally, organizational cultures may support risk taking, or fail to sufficiently encourage risk aversion [1]–[9].

Modeling risk in distributed, large-scale systems presents its own challenges. First, because the systems are distributed, risk in the system can *migrate*, making risk identification and mitigation difficult. Risk migrates when the introduction of a risk mitigation measure to address one problem in the system introduces other, unintended consequences in another part of the system. An example of risk migration can be seen when weather-related delays cause aircraft to remain on the ground until the weather clears. During such times, the risk of collision on take-offs and landings decreases, but the risk of ground-based collisions on runways jammed with waiting aircraft increases [10].

Modeling risk in distributed large-scale systems is also difficult because incidents and accidents in the system can have *long incubation periods* due to poor information flow between distributed sub-systems, making risk analysis and identification of leading error chains difficult. When systems have long incubation periods, precipitating factors may lie dormant for long periods of time, until catalyzed by the right combination of triggering events (i.e., a pharmaceutical that provides the right chemical catalyst, interacting personalities that cause dysfunctional organizational and behavioral reactions, or technologies being utilized in pathological ways). Long incubation periods provide particular challenges for risk managers observing short-term changes in a dynamic system [11].

Finally, modeling risk in distributed, large-scale systems is difficult because such systems often have organizational structures with limited physical oversight, which makes the process of identifying and addressing human and organizational error complicated. In a distributed system with limited physical oversight, the normal antidotes to human and organizational error—checks and balances, redundancy, and training—may be defeated by the size and scope of the system, or by subcultures which can develop in the system. In medicine, for instance, the operating room and the intensive care units are “hotbeds” for human error [12]–[14] because of the tempo of operations, volume of information, criticality of decisions and actions, and complexity of interactions. As medicine moves in an increasingly distributed, electronic direction [13], [14], with fewer opportunities for physical oversight, checks and balances, and redundancy, medical systems may have difficulty trying to assess and identify the role of human and organizational error, and its impact on levels of risk in the system [11], [12], [14].

These observations have implications for risk modeling in distributed, large-scale systems. To counter the problem of risk migration, dynamic risk assessment models can be used to capture the dynamics of the complex system, as well as patterns of risk migration. Long incubation periods for pathogens in a system suggest the importance of historical analyses of system performance in order to establish performance benchmarks in the system, and to identify patterns of triggering events, which may require long periods of time to develop and detect. Finally, assessments of the role of human and organizational error, and its impact on levels of risk in the system, are critical in distributed, large-scale systems with limited physical oversight.

To be effective, however, risk modeling requires more than models and analysis. The major element of effective risk modeling in distributed, large-scale systems is a *process* that follows generally accepted guidelines for risk assessment, which can establish credibility for the results of the risk modeling and enhance the success of the modeling effort. Following the approach of Total Risk Management [15], the process should include

- risk indentification;
- risk quantification and measurement;
- risk evaluation;
- risk mitigation.

Manuscript received March 28, 2000; revised August 29, 2000. This paper was recommended by Associate Editor Y. Y. Haimes.

M. Grabowski is with the Business Department, Le Moyne College, Syracuse, NY 13214 USA and the Department of Decision Sciences and Engineering Systems, School of Engineering, Rensselaer Polytechnic Institute Troy, NY USA (e-mail: grabowsk@maple.lemoyne.edu).

J. R. W. Merrick is with the Department of Mathematical Sciences, Virginia Commonwealth University, Richmond, VA 23284 USA.

J. R. Harrald, T. Mazzuchi, and R. Van Dorp are with the Institute for Crisis, Disaster and Risk Management, The George Washington University, Washington, DC 20052 USA.

Publisher Item Identifier S 1083-4427(00)10020-7.

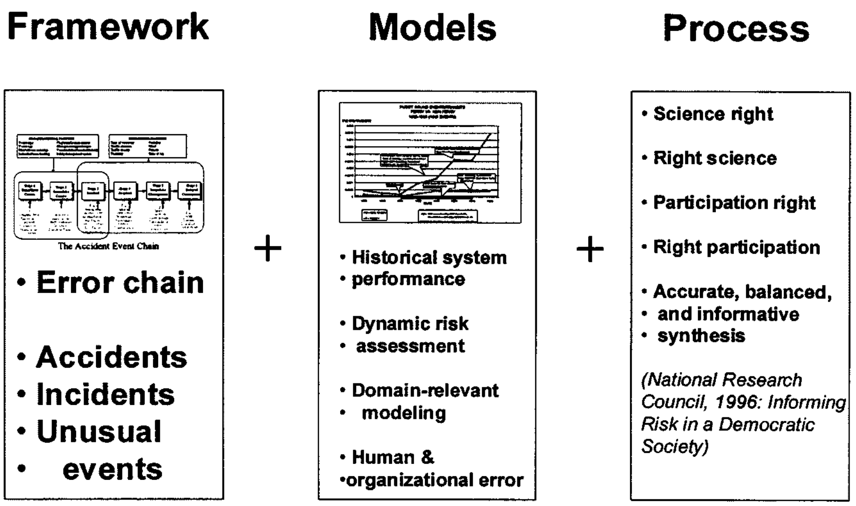

Fig. 1. Risk modeling in distributed, large-scale systems.

Risk identification involves developing a framework for understanding the manner in which accidents, their initiating events and their consequences occur. A *risk framework* [15], [16] can provide a context within which the modeling can take place, and the process used to conduct the modeling and analysis is critical to the effectiveness of the assessment, and the credibility of its recommendations. To measure and evaluate risk, a set of *risk models* is required that capture the historical performance of the system, the dynamic complexity of the system, including risk migration; the role of human and organizational error in the system, and the particular characteristics of the system under study.

It is the process of effective risk modeling in distributed, large-scale systems that we explore in this paper. Fig. 1 illustrates the three elements of effective risk modeling just described: a risk framework, risk models, and a process that adheres to guidelines for effective risk assessment. In the following sections, we describe one risk framework, and the importance of such an orientation tool. We then describe a series of models reflective of the challenges in modeling risk in dynamic systems, followed by a process that subscribes to one set of guidelines for effective risk assessment. The paper concludes with a discussion of the limitations of the suggested approach.

II. Risk Assessment and Management

A. Framework

Risk may be defined as the measure of the probability and severity of an unwanted event. Risk events occur for a variety of reasons, as seen in Fig. 2 [11], [17]. Sometimes risk events are the result of *basic or root causes*, such as inadequate operator knowledge, skills or abilities, or the lack of a safety management system in an organization. Risk events could also result from *immediate causes*, such as a failure to apply basic knowledge, skills, or abilities, or an operator impaired by drugs or alcohol. *Incidents* are unwanted events that may or may not result in accidents; *accidents* are unwanted events that have either *immediate* or *delayed consequences*. Immediate consequences could include injuries, loss of life, property damage, and persons in peril; delayed consequences could include further loss of life, environmental damage, and financial costs.

Fig. 2 depicts the risk event error chain, and illustrates that risk events often occur because the error chain *cascades:* a basic cause can occur *and* an immediate cause *and* an incident will trigger an accident [11]. Absent risk reduction measures to interrupt the error chain, basic causes can cascade into immediate causes, which can cascade into an incident, which can trigger an accident. The key to risk mitigation, therefore, is to introduce risk reduction interventions at appropriate points in the error chain so as to prevent the cascade.

A risk framework such as that provided in Fig. 2 is an important component of risk modeling. It provides organizing and orienting definitions, domain-meaningful context, and a structure around which to organize data gathering and analysis. To provide such a context, therefore, a risk framework should provide:

- a definition of risk in the domain under study;
- definitions and examples for components of the error chain in the domain (e.g., basic/root causes, immediate causes, incidents, accidents, consequences, and delayed consequences);
- descriptions of accidents, incidents, and unusual events in the system; and
- identification of risk mitigation measures in the system, categorized by their impact on the error chain.

B. Models

The second element of effective risk modeling in distributed, large-scale systems is the use of risk models, many of which have been proposed over the past fifty years. The requirements of distributed, large-scale systems, however, suggest the need for specific types of risk models:

- *dynamic risk models* to capture the dynamic nature of risk in complex systems, and to capture risk migration in the system;
- *historical analyses of system performance over appropriately long periods of time* in order to develop benchmarks of system performance;

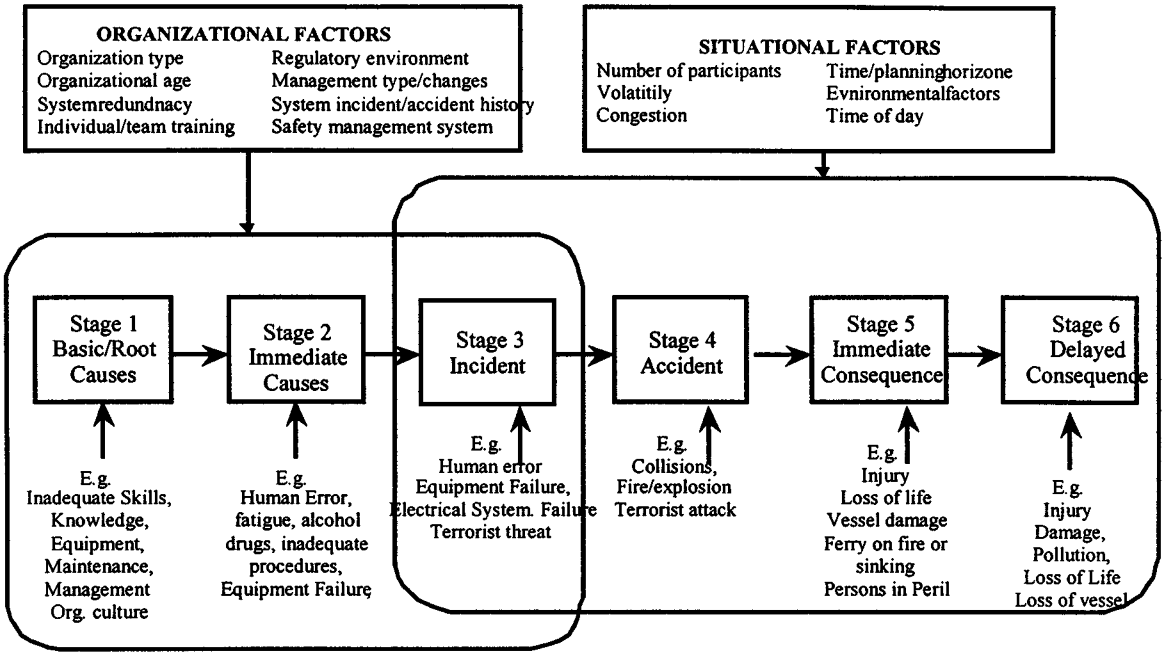
ORGANIZATIONAL FACTORS
Organization type
Organizational age
Systemredundnacy
Individual/team training
Regulatory environment
Management type/changes
System incident/accident history
Safety management system
SITUATIONAL FACTORS
Number of participants
Volatitily
Congestion
Time/planninghorizone
Evnironmentalfactors
Time of day
Stage 1 Basic/Root Causes
Stage 2 Immediate Causes
Stage 3 Incident
Stage 4 Accident
Stage 5 Immediate Consequence
Stage 6 Delayed Consequence
E.g. Inadequate Skills, Knowledge, Equipment, Maintenance, Management Org. culture
E.g. Human Error, fatigue, alcohol drugs, inadequate procedures, Equipment Failure
E.g. Human error Equipment Failure, Electrical System. Failure Terrorist threat
E.g. Collisions, Fire/explosion Terrorist attack
E.g. Injury Loss of life Vessel damage Ferry on fire or sinking Persons in Peril
E.g. Injury Damage, Pollution, Loss of Life Loss of vessel

Fig. 2. Risk event error chain.

- *assessments of the role of human and organizational error*, and its impact on levels of risk in the system; and
- *domain-appropriate models and analyses* to address any special risk requirements in distributed, large-scale systems.

Each of these modeling elements makes an important contribution to risk modeling. Dynamic models can capture fluidity and change in a large-scale system. System performance benchmarks can ensure that risk mitigation measures reflect historical risk patterns in the system, and can ensure that incubation periods and catalysts in the system can be appropriately identified and managed. Formal assessments of human and organizational error can capture important performance parameters and ensure that risk mitigation measures attend to the impact that human and organizational error can have on levels of risk in the system. Finally, domain-appropriate models can focus risk modeling on the salient characteristics of the system under study.

Each of these modeling elements can also inform the other: historical performance assessments can provide critical input to dynamic risk models, and should highlight the role of human and organizational error in the system. Similarly, the need for domain-appropriate models and analyses should be derived from the historical performance assessments, and the results of dynamic risk modeling. Finally, the dynamic risk models, the historical performance analyses, and the human and organizational error assessments should all highlight the needed risk mitigation measures in the system. Following Weick's notion of requisite variety [4], the risk models should be as complex and varied as the system in which they are used.

C. Process

The final component in modeling risk in distributed, large-scale systems is a process that adheres to commonly accepted guidelines for effective risk assessment. One example of such guidelines are those articulated in 1996, by the National Research Council's (NRC's) Committee on Risk Assessment, which identified five general objectives for effective risk assessment:

- get the science right;
- get the right science;
- get the participation right;
- get the right participation; and
- develop an accurate, balanced, and informative synthesis [18].

Getting the science right implies that the risk analysis meets high scientific standards in terms of measurement, analytic methods, data bases used, plausibility of assumptions, and respectfulness of the both the magnitude and character of uncertainty, taking into consideration limitations that may have been placed on the analysis because of the level of effort judged appropriate for informing the decision. In practical terms, this means utilizing a scientifically accepted risk assessment methodology, with careful attention to measurement, analysis, data, assumptions, and the importance of uncertain, incomplete, and unreliable information, and its impact on risk assessment.

Getting the right science means that the risk analysis addresses the significant risk-related concerns of public officials and the spectrum of interested parties and affected parties, such as risks to health, safety, economic well-being, and ecological and social values, with analytic priorities having been set so as to emphasize the issues most relevant to the decision.

Getting the right participation means that the risk analysis has sufficiently broad participation to ensure that important, decision-relevant information enters the process, that all important perspectives are considered, and that legitimate concerns about inclusiveness and openness are met. The NRC Committee specifically recommended using a variety of activities and incorporating broad participation in risk assessment activities, even though it is potentially time-consuming and cumbersome. The NRC Committee advised that it is often wiser to err on the side of too broad rather than too narrow participation in order to ensure the acceptance of the assessment's findings, and to enhance the likelihood of implementation of recommendations.

Getting the participation right means that the risk assessment satisfies the decision makers and interested and affected parties that the risk assessment process is responsive to their needs: that information, view points, and concerns have been adequately represented and taken into account; that all parties have been adequately consulted; and that participation has been able to affect the way risk problems are defined and characterized.

Developing an accurate, balanced, and informative synthesis was the final guideline for effective risk assessment articulated by the NRC. This guideline focuses on risk characterization—presenting the state of knowledge, uncertainty, and disagreement about the risk situation to reflect the range of relevant knowledge and perspectives, and satisfying the parties to a decision that they have been adequately informed within the limits of available knowledge. An accurate and balanced synthesis treats the limits of scientific knowledge (i.e., the various kinds of uncertainty, indeterminacy, and ignorance) with an appropriate mixture of analytic and deliberative techniques.

The five guidelines are related. To be decision-driven, a risk assessment must be accurate, balanced, and informative. This requires getting the science right and getting the right science. Participation helps ask the right questions of the science, checks the plausibility of assumptions, and ensures that any synthesis is both balanced and informative. Thus, each of the steps provides important input to an effective risk assessment.

Each of the components of risk modeling in distributed, large-scale systems thus plays an important role in capturing critical facets of these systems, modeling risk, and suggesting appropriate risk mitigation measures. In the next section, we examine use of this approach in risk modeling for a distributed, large-scale system, the marine transportation system in the U.S.

III. Example: Risk Modeling in Marine Transportation

There is inherent risk in managing the distributed, large-scale system known as marine transportation. Tasks in the system—navigation, vessel loading, propulsion plant engineering, arrivals and departures—are distributed across a large geographical area, are time-critical, and contain elements of embedded risk (e.g., vessel navigation in congested waters, in reduced visibility, carrying passengers on time-critical schedules). The technology used in the system—vessels, equipment, software, control systems, mooring lines, etc.—is also inherently risky. Human and organizational error is present in the system, and organizational structures which result in limited physical oversight and contact make risk mitigation difficult. Finally, as in many large-scale systems, cultures in marine transportation can send confusing or contradictory messages (e.g., safety bulletins that celebrate the number of accident free days while vessel watch schedules, crew rotations, training practices, and work hours raise questions about risk tolerance in the system).

The risk factors introduced in Section II are clearly present in the marine transportation system. Risk in the system can *migrate*, particularly when risk mitigation measures are introduced: one risk problem may be solved with the introduction of a risk mitigation measure (i.e., prohibiting vessel sailings in fog), at the same time that new risk problems can emerge as a result of the introduction of that risk mitigation measure (i.e., traffic congestion problems at terminals clogged with vessels waiting for visibility to lift).

In addition, precipitating factors in the system may also have long incubation periods, and pathological risk factors may lie dormant for long periods of time, until catalyzed by the right combination of triggering events. In the case of the *Exxon Valdez*, those precipitating factors included ice in a channel, a tired crew, a nighttime passage, a captain with impaired decision making abilities, and a host of crew failures, such as mistakes in helm orders, locked-on autopilots, and missed warnings provided by navigational aids.

Marine transportation is, by definition, a distributed system, with limited physical oversight over its members. Traditional antidotes to limited physical oversight—redundancy in the system, training, checks and balances—can be defeated by the size and scope of the system, or by subcultures which develop within it. Thus, identifying and assessing the role of human and organizational error in the system is difficult, although important, as human and organizational error is often quoted as being responsible for more than 80% of accidents in marine transportation [19].

In this section, we describe one use of the Fig. 1 approach, used during a risk assessment for the Washington State Ferries conducted by the authors in 1998–1999. During that study, a framework for risk assessment was used to organize data gathering, analysis and modeling. A variety of models reflecting the needs of the risk assessment and the system under study were used, and the process used to conduct the risk assessment was consistent with the guidelines for effective risk assessment articulated by the National Research Council in 1996. We begin the description of the use of the approach in the following section.

A. Background

The Washington State Ferries is the largest ferry system in the United States, operating 27 vessels, including four passenger only ferries, to 20 terminals on ten routes. In 1998, total ridership for the ferries serving the central Puget Sound region was approximately 26.2 million persons, more passengers than Amtrak handles in a year [20].

In 1998, the Washington State Transportation Commission, at the request of the State Legislature, established an independent Blue Ribbon Panel to assess the adequacy of provisions for passenger and crew safety aboard the Washington State Ferries, following a series of articles in the local newspapers about the adequacy of lifeboats aboard the ferries, following release of the movie *Titanic*. As a result, the Blue Ribbon Panel engaged a consultant team from The George Washington University, Rensse-

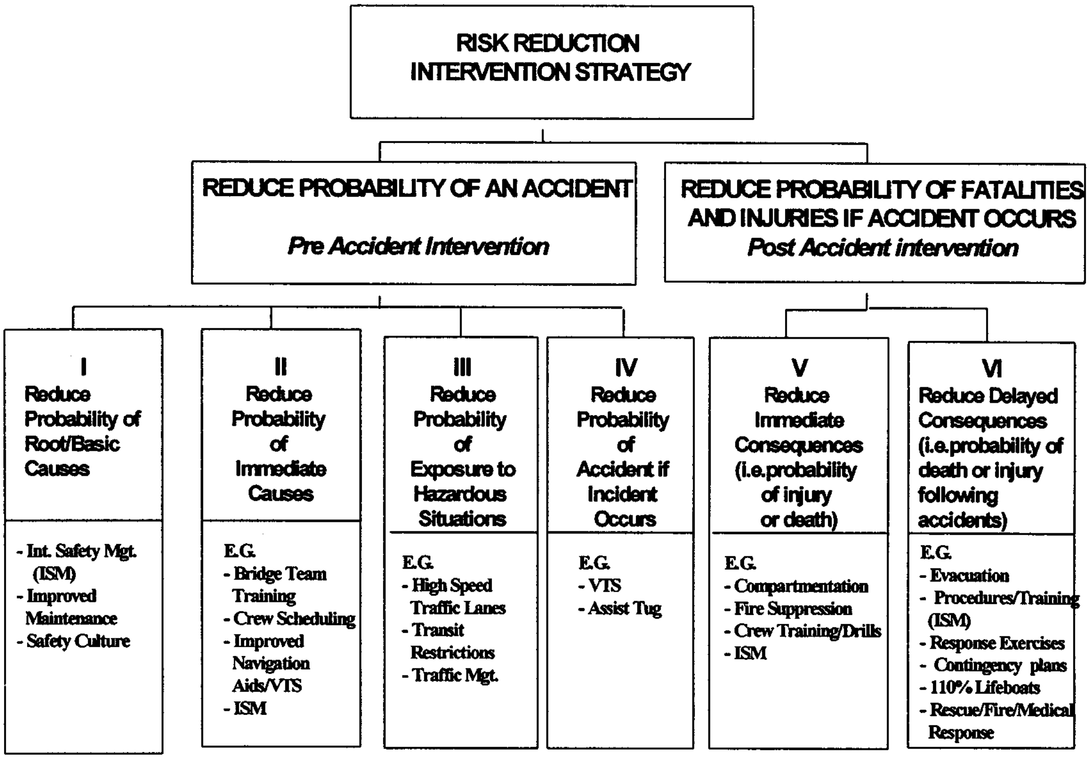
RISK REDUCTION INTERVENTION STRATEGY
REDUCE PROBABILITY OF AN ACCIDENT
Pre Accident Intervention
REDUCE PROBABILITY OF FATALITIES AND INJURIES IF ACCIDENT OCCURS
Post Accident intervention
I Reduce Probability of Root/Basic Causes
- Int. Safety Mgt. (ISM)
- Improved Maintenance
- Safety Culture
II Reduce Probability of Immediate Causes
E.G.
- Bridge Team Training
- Crew Scheduling
- Improved Navigation Aids/VTS
- ISM
III Reduce Probability of Exposure to Hazardous Situations
E.G.
- High Speed Traffic Lanes
- Transit Restrictions
- Traffic Mgt.
IV Reduce Probability of Accident if Incident Occurs
E.G.
- VTS
- Assist Tug
V Reduce Immediate Consequences (i.e.probability of injury or death)
E.G.
- Compartmentation
- Fire Suppression
- Crew Training/Drills
- ISM
VI Reduce Delayed Consequences (i.e.probability of death or injury following accidents)
E.G.
- Evacuation
- Procedures/Training (ISM)
- Response Exercises
- Contingency plans
- 110% Lifeboats
- Rescue/Fire/Medical Response

Fig. 3. Risk reduction intervention principles and strategies.

laer Polytechnic Institute/Le Moyne College, and Virginia Commonwealth University to:

- assess the adequacy of passenger and crew safety in the Washington State Ferry system;
- evaluate the level of risk present in the Washington State Ferry system; and
- develop recommendations for prioritized risk reduction measures which, once implemented, can improve the level of safety in the Washington State Ferry system.

It is this risk assessment that provides the backdrop for illustrating use of the risk modeling approach described in Section II.

B. Framework

In marine transportation, following Fig. 2, risk events can be triggered by *basic or root causes*, and/or *immediate causes*, and may be an *incident* or an *accident*. In the Washington State Ferries Risk Assessment, the unwanted outcome was an accident involving a Washington State ferry. Accidents can have *immediate* or *delayed impacts*.

Consistent with the risk framework adopted during the project, *basic or root causes* in the Washington State Ferries Risk Assessment included lack of operator knowledge, skills and abilities, lack of safety management systems, or inadequate supervisory or management oversight. *Immediate causes* included failures to apply appropriate operator knowledge, skills, and abilities, operator impairment (due to physical, or psychological causes, or substance abuse), and/or human error. *Incidents* were defined as undesirable events related to control or system failures which could be detected or corrected in time to prevent accidents; incidents can also be prevented from developing into accidents by the presence of redundant or back up systems. Examples of incidents include propulsion failures, steering failures, navigational equipment failures, and other equipment failures. *Accidents* were defined as occurrences that cause damage to vessels, facilities, or personnel, such as collisions, allisions, groundings, fires, explosions, or founderings. The potential *impacts* included deaths, injuries, and economic losses that occur as an immediate or delayed consequence of an accident.

In order to reduce risk, we must understand risk events, and the situations that could lead to them, or exacerbate their consequences. The objective of risk management is to take actions and implement policies and procedures that reduce the threat to life, property, and the environment posed by hazards. Fig. 3 shows the taxonomy of risk mitigation used during the Washington State Ferries Risk Assessment. Fig. 3 shows that there are six general opportunities for interrupting this event chain and preventing accidents and/or minimizing their consequences. As shown in Fig. 3, four classes of interventions are intended to reduce the likelihood of occurrence of accidents, and two classes of interventions reduce the consequences of accidents that do occur. The objective of risk management is to choose cost effective risk interventions that impact all areas of the accident event chain.

During the Washington State Ferries Risk Assessment, the framework for risk modeling illustrated in Fig. 2 was adopted in order to provide a common context for analysis and modeling, and a common set of terms and definitions. Definitions and examples for components of the Fig. 2 error chain were identified (i.e., basic or root causes, immediate causes, etc.), and descriptions of incidents and accidents were developed. Finally, risk mitigation measures were identified and categorized by their impact on the error chain, following Fig. 3. Thus, the risk framework definitions, examples, and categorizations provided an important context for risk modeling, as will be seen in the following section.

C. Models

1) Historical System Benchmarks: One of the first tasks during the Washington State Ferries Risk Assessment project was to evaluate baseline levels of risk in the system, and to analyze the Washington State Ferries' historic and present performance. In order to do this, a historical analysis of 1429 incidents, accidents, and unusual events in Puget Sound from 1988 to 1998 was conducted. These historical system benchmarks were important for several reasons. First, they identified patterns of incident and accident occurrence in the system, which was important in identifying effective risk mitigation measures. Moreover, historical analyses covering appropriately long periods of time assisted in identifying latent pathogens, catalysts, and incubation periods in the system.

For instance, despite the fact that Washington State Ferries vessels comprise 75–80% of the traffic on Puget Sound and the San Juan Islands, the Washington State Ferries have been involved in only 43% of the incidents and in 19% of all accidents over the eleven year period. In addition, the historical analysis showed that, of the 46 accidents that occurred to WSF vessels between 1988 and 1998, 26 (or 56.5% of all accidents) were allisions (the striking of a fixed object such as a dock), four (8.7%) were collisions with another vessel, nine (19.6%) were fires and/or explosions, one was a flooding, and six (13%) were groundings. Thus, the greatest number of accidents occurring to WSF vessels over the ten-year period was allisions, followed by fires and explosions, primarily crank case explosions. However, the analysis also shows the difficulty of introducing effective risk mitigation measures when the numbers of reported incidents and accidents is small. Thus, these analyses can provide some measure of historical performance in the system, but caution is advised when the number of reportable incidents and accidents is small.

The historical safety analysis also showed the presence of latent pathogens, with long incubation periods, in the system. The Steel Electric class of Washington State Ferries had installed a particular control system in 1990. At the same time, those vessels experienced significantly higher numbers of propulsion failures. Analysis of the propulsion failure records of different vessels by class, by machinery systems, and appropriate time periods showed this control system to be a contributor to a significant increase in propulsion failures, and the control systems were replaced beginning in 1995. Thus, the historical analysis identified latent pathogens in the system (a problematic control system), with a six-year incubation period, and documented the impact of the introduced risk mitigation measure (replacement of the control system) on levels of risk in the system.

There are a number of implications of the historical safety analysis. Detailed examination of the Washington State Ferries incident records suggested that risk mitigation measures associated with propulsion failures and other equipment failures, rather than those addressing steering failures, would have more utility for the Washington State Ferries. Further, analysis of incident and accident patterns by ferry classes, routes, and machinery systems showed that different risk mitigation measures might have greater utility for different classes of ferries. Thus, performance and trend analysis of machinery, equipment, and personnel were very helpful in assessing the utility of different risk reduction measures.

2) Dynamic Risk Modeling: To ensure that the dynamic nature of risk in the Washington State Ferries was captured, and risk migration assessed, a dynamic simulation tool was used for analysis during the Washington State Ferries Risk Assessment. The basic technique used was Probabilistic Risk Assessment (PRA), extended to address the dynamic nature of a system on risk in the system. The dynamic risk modeling included steps to identify the series of events leading to accidents, estimation of the probabilities of these events, and evaluation of the consequences of different degrees of system failure. These techniques have been successfully used previously in the Prince William Sound Risk Assessment [21].

To do this, a computer system simulation was developed that modeled the operation of the Washington State Ferries, other vessels in the area, and the environmental conditions. The simulation was used to determine exposure to risk of ferries on all routes. Following Fig. 2, exposure to collision risk was based on the number and type of interactions with other vessels; exposure to grounding risk was based on the time actually spent in areas where grounding is possible; allision risk exposure was determined by the number of dockings made, and fire and explosion risk exposure was determined to be a function of the time underway.

Probabilities of occurrences of triggering incidents, and conditional probabilities of an accident given the occurrence of an incident, were based on data where available and expert judgment where data was not suitable. Washington State Ferries relief masters and mates, Puget Sound Pilots, and U.S. Coast Guard Vessel Traffic Service watchstanders formed the pool of experts used as the basis for expert judgment elicitations which provided data where data was not available. The dynamic system simulation was then used to calculate the system risk under four different scenarios—a baseline risk scenario, and three variations on the baseline, which introduced different vessels (i.e., fast ferries), on different routes, under differing environmental conditions.

Potential risk reduction interventions were then collected, classified and grouped, and their impact on events in the causal chain were estimated based on available data, other risk studies, interviews with experts, and the project team's best judgment. Finally, the impacts of risk mitigation measures on levels of risk in the system were estimated by changing parameters or variables in the system simulation. For a more detailed discussion of the modeling process used, see [22].

The dynamic simulation model provided a number of interesting results. First, because dynamics in the system could be modeled, a variety of risk mitigation measures could be tested, and tradeoffs between different measures, or combinations of

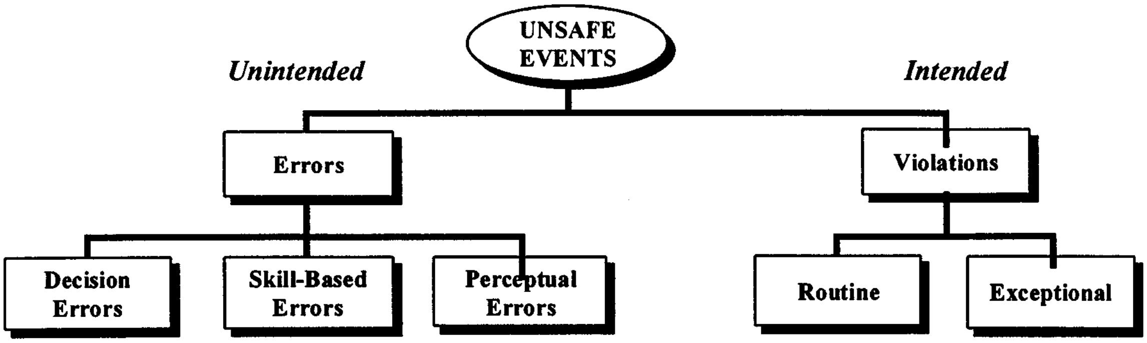

Fig. 4. Human and Organizational Error Taxonomy.

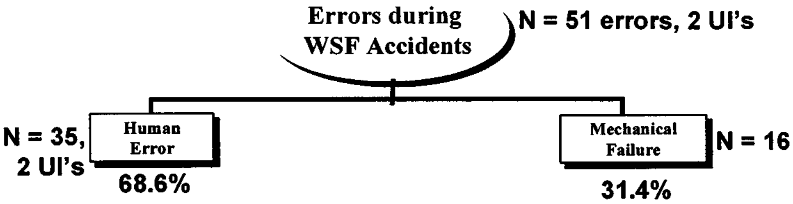

Fig. 5. Human Errors During WSF Accidents, 1988–1998.

measures, could be evaluated. In addition, changes in levels of risk in the system could be assessed under different scenarios, and "what if" analyses incorporating different risk mitigation measures could be conducted. Finally, risk migration in the system could be identified and analyzed, as could be seen in an analysis of the introduction of the high-speed ferries, which were introduced to alleviate system bottlenecks in passenger service in the central part of Puget Sound. The dynamic simulation tool captured, modeled, and analyzed the shift in collision risk from slow speed encounters with large ferries, to high-speed crashes with 46-knot, high-speed ferries. Thus, the dynamic simulation tool provided important assessments of the dynamic nature of risk, and of risk migration, in the Washington State Ferries Risk Assessment.

3) Assessing Human and Organizational Error: In distributed, large-scale systems with limited physical oversight, assessing the impact of human and organizational error on levels of risk in the system is challenging but important, especially as such error is often cited as a primary contributor to accidents. Thus, in order to analyze the role of human and organizational error in the Washington State Ferry accidents, an event analysis of the 46 Washington State Ferries accidents that occurred between 1988 and 1998 was conducted. During this analysis, 51 errors were identified, and then categorized using the human and organizational error taxonomy developed by Reason [11] and illustrated in Fig. 4.

Reason's cognitive framework of human error classifies unsafe acts into two types of activities: *errors*, which are unintended actions; and *violations*, which are intended actions. Errors can be of three types: *decision errors*, encompassing rule-based and knowledge-based errors; *skill-based errors*, and *perceptual errors*. Violations can be either of two types: routine, which are common place abrogations of policies, rules and/or procedures that are condoned by management, or exceptional violations, which are not condoned by management.

The human and organizational error event analysis conducted during the Washington State Ferries Risk Assessment provided some interesting results. As seen in Fig. 5, 68.6% (35 errors) of the errors which occurred during Washington State Ferries' accidents were categorized as human error, and 31.4% (16 errors) of the errors were categorized as mechanical errors. This data provide an interesting contrast to the oft-quoted 80% human error figure used in many maritime studies [19], as in this study, approximately 70% of the errors committed during accidents were related to human and organizational error.

None of the human errors identified during the event analysis were violations: all were unintended errors. However, two unusual incidents represented violations: one routine violation (i.e., a practice condoned by management), and one exceptional violation (not condoned by management).

The human and organizational error analysis thus provided important insight to risk in the Washington State Ferries system. First, human and organizational error was found to be a significant component of accidents that have occurred in the Washington State Ferry system over the past 10 years. Of the errors that have occurred during accidents, almost 70% were human errors, compared to approximately 30% for mechanical errors. However, caution should be exercised with the use of these statistics, as the number of errors and the numbers of accidents is not large over the 10 year period (46 events, 51 errors identified). Despite this caution, however, risk mitigation measures focused on decreasing human and organizational error—training, accountability, checks and balances, safety management systems, certification and re-certification programs—were suggested to have great utility for the Washington State Ferries.

The detailed analysis of the types of human and organizational error also provided interesting insights. The high percentage of human error contribution to accidents in the WSF system suggests that risk mitigation measures focused on addressing basic/root causes, as well as immediate causes, are of significant utility in the WSF system. Similarly, risk mitigation measures focused on personnel selection, training, and system safety issues, rather than on investments in capital equipment, would be of greater utility, based on the historical safety performance analysis. Comparative analyses between aviation human error studies and the WSF data analysis show that the human error contribution to accidents is comparative [23].

4) Domain-Specific Models: To address questions regarding the impact of collisions involving high speed ferries, domain-specific modeling was needed. Thus, collision models involving high speed ferries, traditional ferries, large commercial vessels, and tugs and tows were developed, and the results of the model analyzed. Estimates of the collision damage penetration for selected collision scenarios were made using an engineering model based on the methodology developed by Minorsky [24]. From these damage calculations, estimates of the time available for evacuation of passengers without risk of additional injuries or fatalities were made. The analyses completed with use of the domain-specific models provided the basis for specific recommendations regarding high speed ferry crew selection, certification, training, and re-certification, and permitted analysis of specific, focused questions of interest to policy and decision-makers.

As suggested in Section II, each of the risk models used during the Washington State Ferries Risk Assessment informed the other: the historical system assessments provided critical input to the dynamic risk simulation, specifically in the area of conditional failure probabilities. In addition, the historical system analyses suggested the role of human and organizational error in Washington State Ferries accidents, which was borne out in the human and organizational error analysis. The need for specific high-speed ferry collision analyses was also indicated by the historical system assessments. Finally, the dynamic risk models, the historical system performance assessments, and the human and organizational error analyses all suggested consistent risk mitigation measures: training; safety management systems; and crew certification and re-certification programs were all suggested by the analyses. Most importantly, each of the suggested risk mitigation measures suggested human and organizational performance improvements, rather than capital investments, as the path to mitigating risk in the system. This finding was particularly important in a risk assessment catalyzed by questions regarding capital investment (e.g., should the Washington State Ferries purchase additional lifeboats?).

D. Process

The final element of the risk modeling approach suggested in Section II was a process that adheres to recommended guidelines for effective risk assessment, such as those developed by the National Research Council committee in 1996. In this section, we describe how those guidelines were met during the Washington State Ferries risk assessment.

Getting the science right during the Washington State Ferries Risk Assessment meant utilizing a scientifically accepted risk assessment methodology (probabilistic risk assessment), with careful attention to measurement, analysis, data, assumptions, and the importance of uncertain, incomplete, and unreliable information, and its impact on risk assessment.

Getting the right science meant ensuring that the risk assessment focused on the risk-related concerns of public officials, marine transportation system members, other members of the port and waterway community, regulators, scientists and other specialists, and a variety of interested and affected parties. Those priorities were determined in a variety of ways: by consulting with the applicable Port and Harbor Safety Committees; through analytic deliberation with agency, public, industry, and environmental parties; and through listening sessions, to name a few. Risk priorities were articulated early in the assessment process, and refined as required.

Getting the right participation during the Washington State Ferries Risk Assessment meant ensuring that participation was sought and garnered from a variety of sources: from shipping and towing company employees and operators; from state, federal, and local regulators; from ship's pilot organizations; from ship's agents and representatives; from insurers, brokers and financiers; from maritime interest groups representing all segments and types of waterway users and managers; from the U.S. Navy; from environmental and legal groups and representatives; and from other interested and affected parties.

Getting the participation right meant that vessel masters, mates, engineers and pilots were observed and interviewed aboard vessels, where problems and issues could be demonstrated. This also means that shore-based management, operations, engineering, maintenance, and safety personnel were interviewed in their places of work, and were consulted during the project. This same process was followed with regulators; insurers; agents; brokers, shippers; environmental, legal, and special interest groups, and other interested and affected parties. System stakeholders were identified during the risk assessment, and their participation requested. In each of the interactions with these interested and affected parties, the risk analysts consulted with the parties; sought data and information; strove to understand the viewpoints, concerns, and information provided; and provided feedback as to how the gathered information and viewpoints would be incorporated into the risk assessment. Where appropriate, preliminary data analyses and results were reviewed with interested and affected parties.

Developing an accurate, balanced and informative synthesis during the Washington State Ferries Risk Assessment meant that care was taken in presentations and documentation to illuminate the state of knowledge, uncertainty, and disagreement about the risk situation, so that the relevant knowledge and perspectives about the situation were articulated. Thus, each of the guidelines articulated by the National Research Council in 1996 was adhered to during the Washington State Ferries Risk Assessment.

IV. Limitations

Utilizing the approach to modeling risk in distributed, large-scale systems illustrated in Fig. 1 presents some challenges. First, defining a common risk framework to orient a modeling effort often requires considerable resources and time to produce. This time and resource drain occurs at project inception, often the most challenging time in project management. Moreover, there may be pressures during the risk assessment to produce meaningful results quickly, and thus, pressures to move away from framework, definitional, and context issues.

There are also difficulties associated with the use of the risk models proposed in Fig. 1. First, there are questions associated with the use of dynamic simulation tools as a means to capture dynamic risk in a system [25], particularly questions associated with methods for expert judgment elicitation to augment existing safety databases. Second, there are limits to the use of historical system performance data, particularly when there are small numbers of catastrophic events, as predictors of future system performance [26]. In addition, there are several different issues that continue to plague the analytic use of human and organizational error data: uncertainty in human error probabilities, questions about the transferability of human factors data from different domains, and the compounding influence of environmental factors in accident data [27], [28].

An additional problem is that the data and recommendations contained in the human engineering literature frequently have not been tailored to specific applications. Expert interpretation is often required to determine the applicability (particularly without further validation) of data to a specific research question. Although it is often possible for human factors specialists to extrapolate from the literature to a design application, whenever possible, usability testing (i.e., for user acceptability) should be conducted in a rapid prototyping or other simulation environment [28].

The use of accident data for comparing performance in operational contexts is a problem that plagues many domains. In 1994, the National Transportation Safety Board [21] noted that flight crew performance during accidents is subject to the simultaneous influences of many operational context variables. Because of data limitations—a small number of accidents (due to their rarity), and missing data (due to the nature of the evidence in accident investigations)—the interactions between operational context variables and human performance is difficult to analyze [23, p. 84]. These type of problems also plague marine transportation, and make difficult complete analyses of the impact of human error on safety in large-scale systems.

Thus, use of the approach to risk modeling in distributed, large-scale systems illustrated in Fig. 1 is not without its problems. However, the framework, models, and guidelines provide structure, direction and analytical support that is critical when modeling risk in complex systems. Although the approach has been used successfully in several maritime risk assessments over the past decade, and was peer reviewed by the National Research Council in 1998 as an example of a state of the art risk assessment methodology, further evaluation of the robustness of the approach is warranted before it can be recommended for more widespread adoption [25].

References

[1] C. Perrow, *Normal Accidents: Living with High Risk Technologies*. New York: Basic Books, 1984.

[2] T. R. La Porte and P. Consolini, “Working in theory but not in practice: Theoretical challenges in high reliability organizations,” *J. Public Administration Research and Theory*, vol. 1, pp. 19–47, 1991.

[3] K. H. Roberts, “Some characteristics of high reliability organizations,” *Organization Science*, vol. 1, pp. 160–177, 1990.

[4] K. E. Weick, “The collapse of sense making in organizations: The Mann Gulch disaster,” *Administrative Science Quarterly*, vol. 38, pp. 628–652, 1993.

[5] E. Tenner, *Why Things Bite Back: Technology and the Revenge of Unintended Consequences*. New York: Knopf, 1996.

[6] D. Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. Chicago, IL: Univ. Chicago Press, 1996.

[7] M. Grabowski and K. H. Roberts, “Human and organizational error in large-scale systems,” *IEEE Trans. Syst., Man, Cybern.*, vol. 26, pp. 1–16, Jan. 1–16, 1996.

[8] M. Grabowski and K. H. Roberts, “Risk mitigation in large-scale systems: Lessons learned from high reliability organizations,” *Calif. Manage. Rev.*, vol. 39, no. 4, pp. 152–162, Summer 1997.

[9] M. Grabowski and K. H. Roberts, “Risk mitigation in virtual organizations,” *Organization Science*, Nov./Dec. 1999.

[10] K. E. Weick, “The vulnerable system: An analysis of the Tenerife air disaster,” *J. Manage.*, vol. 16, pp. 571–593, 1990.

[11] J. Reason, *Managing the Human and Organizational Response to Accidents*. Brookfield, VT: Ashgate Publishing, 1997.

[12] M. S. Bogner, Ed., *Human Error in Medicine*. Hillsdale, NJ: Lawrence Erlbaum, 1994.

[13] (1999, June) Physicians On Line (1999). [Online]http://www.physicians-on-line.com

[14] National Academy of Sciences, Institute of Medicine, *To Err is Human: Building a Safer Health System*. Washington, DC: National Academy Press, 1999.

[15] Y. Y. Haimes, “Hierarchical holographic modeling,” *IEEE Trans. Syst., Man, Cybern.*, vol. SMC-11, pp. 606–617, 1981.

[16] D. M. Murphy and M. E. Paté-Cornell, “The SAM framework: A systems analysis approach to modeling the effects of management on human behavior in risk analysis,” *Risk Anal.*, vol. 16, no. 4, pp. 501–515, 1996.

[17] J. R. Harrald, T. A. Mazzuchi, J. Spahn, R. Van Dorp, J. Merrick, S. Shrestha, and M. R. Grabowski, “Using system simulation to model the impact of human error in a maritime system,” *Safety Science*, vol. 30, pp. 235–247, 1998.

[18] National Research Council, *Understanding Risk: Informing Decisions in a Democratic Society*. Washington, DC: National Academy Press, 1996.

[19] National Research Council, *Applying Advanced Information Systems to Ports and Waterways Management*. Washington, DC: National Academy Press, 1999.

[20] (1999, June) Puget Sound Regional Council (1998). [Online]http://www.puget_sound_regional_council.org

[21] J. Merrick, J. R. Van Dorp, J. Harrald, T. Mazzuchi, J. Spahn, and M. Grabowski, “A systems approach to managing oil transportation risk in Prince William Sound,” *Syst. Eng.*, vol. 3, no. 3, pp. 128–142, 2000.

[22] J. R. Van Dorp, J. Merrick, J. Harrald, T. Mazzuchi, and M. Grabowski, “A risk management procedure for the Washington State Ferries,” Risk Anal., 2000, to be published.

[23] National Transportation Safety Board, “Safety study: A review of flightcrew-involved major accidents of U.S. air carriers, 1978–1990,” Dept. Transportation, Washington, DC, NTSB Report no. NTSB/SS-94/01, Jan. 1994.

[24] V. U. Minorsky, “An analysis of ship collisions with reference to the protection of nuclear power plants,” *J. Ship Research*, vol. 3, pp. 1–4, 1959.

[25] National Research Council, *Review of the Prince William Sound Risk Assessment*. Washington, DC: National Academy Press, 1998.

[26] National Research Council, *Minding the Helm: Marine Navigation and Piloting*. Washington, DC: National Academy Press, 1994.

[27] G. Apostolakis, V. M. Bier, and A. Mosleh, “A critique of recent models for human error rate assessment,” *Reliab. Eng. Syst. Saf.*, vol. 22, pp. 201–217, 1988.

[28] National Research Council, *Flight to the Future: Human Factors in Air Traffic Control*. Washington, DC: National Academy Press, 1997.

Martha Grabowski received the B.S. degree from the United States Merchant Marine Academy, Kings Point, NY in 1979 and the M.S., M.B.A., and Ph.D. degrees from Rensselaer Polytechnic Institute, Troy, NY, in 1982, 1983 and 1987, respectively.

She is Professor of Management Information Systems in the Business Department at LeMoyne College in Syracuse, NY, and Research Associate Professor in the Department of Decision Sciences and Engineering Systems at Rensselaer Polytechnic Institute. She served as a Shipboard Merchant Marine Officer, and then spent ten years at General Electric as a Marketing and Advanced Programs Manager. Her research interests include the impact of embedded intelligent real-time systems and networks on systems and humans, human and organizational error in large-scale systems, development and evaluation methods for real-time knowledge-based systems and networks, and methods for mitigating risk in safety-critical large-scale systems.

Dr. Grabowski serves as a Member of the National Research Council's standing Committee on Human Factors and has served in the past as a Member of the National Research Council's Marine Board, and as a Member of the U.S. Coast Guard's Navigation Safety Advisory Council.

Jason R. W. Merrick received the B.A. degree in mathematics and computation from Oxford University, Oxford, U.K. in 1995 and the D.Sc. degree in operations research from the George Washington University, Washington, DC in 1998.

He is currently Assistant Professor of Operations Research and Statistics in the Department of Mathematical Sciences at Virginia Commonwealth University, Richmond, VA. His research interests include probabilistic risk assessment, expert judgment elicitation, system simulation, and Bayesian statistics.

John R. Harrald received the B.S. degree from the U.S. Coast Guard Academy, New London, CT in 1964, the M.S. degree from Massachusetts Institute of Technology, Cambridge, in 1978, and the MBA and Ph.D. degrees from Rensselaer Polytechnic Institute, Troy, NY, in 1973 and 1981, respectively.

He is Professor of Engineering Management in the School of Engineering and Applied Science at The George Washington University, Washington, DC. His research interests include natural disaster vulnerability and mitigation, maritime safety and port risk analysis, response organizations and management systems, organizational learning, and the application of information technology to crisis and disaster management. He is the Director of the Institute of Crisis, Disaster and Risk Management at The George Washington University. He is a Founding Member and Director of The International Emergency Management Society (TIEMS), and a Board Member of the Disaster Recovery Institute.

Thomas A. Mazzuchi received the B.A. degree in mathematics from Gettysburg College, Gettysburg, PA, in 1978, and the M.Sc. and D.Sc. degrees in operations research from The George Washington University, Washington, DC, in 1979 and 1982, respectively.

He is Acting Dean of the School of Engineering and Applied Sciences at The George Washington University and Professor of Engineering Management and Systems Engineering. He served for two and a half years as a Research Mathematician at the International Operations and Process Research Laboratory of the Royal Dutch Shell Company. His research interests are in Bayesian applications in reliability, risk analysis, and quality control problems. Current research interests include reliability growth assessment, software reliability modeling, design and inference in life testing, reliability estimation as a function of operating environment, maintenance inspection policies, and incorporation of expert judgment into reliability and risk analysis.

J. René van Dorp received the D.Sc. degree in operations research from the George Washington University, Washington DC., in January 1998.

He is Assistant Professor in the Engineering Management and Systems Engineering Department at the George Washington University. His current topics of interest are risk management analysis for natural and technological disasters, maritime risk assessment, and project cost risk analysis. His main areas of interest are decision analysis, uncertainty analysis, reliability analysis, and probabilistic risk analysis.