



SURVIVABILITY & SAFETY ENGINEERING

SUMMARY

This paper describes key issues regarding systems survivability and safety engineering; specifically, systems survivability and safety:

- Requires Rigorous Engineering
- Requires Human Systems Integration
- Requires an Understanding of Hazards
- Includes Recoverability
- Can be Improved by Applying Lessons Learned Across Industries

The paper summarizes key engineering features which address those system survivability/safety issues, basic systems survivability/safety principles, and the benefits derived from performing good survivability/safety engineering.

The paper concludes with a summary of selected MPR experience related to systems survivability and safety engineering.

SURVIVABILITY AND SAFETY

Survivability and safety are closely related, and in many cases are the same. Engineering for both has similar issues and features. If there are differences, it would be in the hazards considered; survivability might consider more hazards from outside the system (such as a terrorist attack) while safety might consider hazards more inherent in the system (such as the failure of a critical piece of equipment). The topics in this paper apply to both system survivability and system safety.

ENGINEERING FOR SYSTEM SURVIVABILITY/SAFETY - KEY ISSUES

Systems Survivability/Safety Requires Rigorous Engineering. Hazards can stress systems to the limits of their capabilities. Engineering systems for survivability requires exceptional rigor to ensure that every part of critical systems will function to their maximum potential given the effects of the hazard. This is particularly important since it may not be feasible to operate or test systems under the conditions that would exist when survivability capabilities are needed, and one cannot predict, or test, with certainty the future hazards to which a system will be subjected during its operational life. For example, a new ship is not subjected to weapon hits to validate survivability performance. Or, in an operating nuclear plant, it is not practical to test emergency heat exchangers at the large flows and high temperatures that would occur in some design basis accident scenarios. The survivability performance of such systems cannot be validated by testing; it is completely dependent on the engineering of the systems.

Survivability/Safety Requires Human Systems Integration. Systems survivability usually involves the integrated functioning of multiple systems (such as a mission critical system supported by electrical, ventilation, cooling and digital control systems), and operator interaction with those systems. Operator interaction becomes particularly important when a hazard occurs. An integrated, multi-disciplined, “human centered” approach to engineering is essential to achieving survivability and safety.

Systems Survivability/Safety Requires an Understanding of Hazards. One must understand how hazard events can affect operators and integrated systems to design safe, survivable systems. Hazards can affect systems in many ways, for example: loss of power, loss of other support services such as cooling, physical damage to equipment from events such as explosive blast, being struck by objects, seismic accelerations, and degrading or incapacitating environments such as fire. Software malfunctions, either from errors in the code or from malicious intrusions, also need to be considered. Operators can be physically incapacitated by a hazard, and crisis situations can affect an operator’s cognitive abilities to understand the situation (“situation awareness”) and make decisions.

Systems Survivability/Safety Includes Recoverability. Systems survivability includes not only designing systems to minimize the immediate effects of a hazard on critical functions (called “vulnerability”), it also includes “recoverability”, quickly restoring functions to intact portions of systems to restore critical functions and prevent the degradation of critical functions with time. Designing systems for recoverability requires an understanding of the dynamic behavior of hazard events (such as fire spread) and the dynamic interdependencies of critical systems (such as the shutdown of electronics equipment after cooling is lost), integrated to understand how to minimize the primary, or immediate, damage from a hazard, how to prevent cascading secondary damage and how to recover functions of surviving portions of systems.

Systems Survivability/Safety Can be Improved by Applying Lessons Learned Across Industries. Severe hazard events are not common. Consequently, in any specific industry, typically there is not a large body of experience with how operators and systems respond to severe hazard events. Applying lessons learned from other industries, therefore, can lead to design improvements in system safety and survivability.

ENGINEERING FEATURES TO ADDRESS SYSTEM SURVIVABILITY ISSUES

Systems Survivability/Safety Requires Rigorous Engineering. Rigorous engineering for survivability requires a culture of quality, engineering based on first principles, and quality procedures. Achieving consistent quality requires both adherence to well defined processes and a culture of ensuring that the “answer is right.” Adherence to processes alone will not produce quality work; nor can quality be “reviewed” into a product or design. The engineer performing the work must understand first principles and have a questioning attitude to ensure it is done right. The organization must have a culture that supports and nurtures this attitude. All of these features are needed to consistently produce rigorous engineering.

Since engineering new systems often involves first-of-a-kind engineering, and designing for safety and survivability often involves system performance beyond what is practical to validate with testing, simply following past practice and code requirements usually is not sufficient to produce an effective design. Engineering must be based on first principles, building on past practice and code requirements, to ensure an effective design. Finally, experience with first-of-a-kind engineering helps produce cost-effective survivability engineering. This entails engineering processes that recognize and mitigate risks. Using established tools, such as “technology readiness levels” and project planning to allow for risk mitigation also are key to successful first-of-a-kind engineering.

Survivability/Safety Requires Human Systems Integration. Critical, high-level systems typically depend on support systems, and those support systems may depend on other support systems. For example, critical equipment usually requires electrical power. Emergency generators may be provided as backup to power from the grid. The emergency generators probably are dependent upon fuel and cooling systems. For example, a casualty that disables the electric power from the grid and the cooling for the emergency generators would result in loss of critical system functions. The complete train of integrated systems necessary for the critical systems to function must be considered in the survivability design.

Typically, operators interact with the system. When a hazard occurs, operator actions usually become critical. Essential to timely, effective operator action is operator “situation awareness;” understanding enough about the situation to make an adequate decision. For example, a primary contributor to the severity of the Three Mile Island nuclear plant incident in 1979 was the inability of the plant operators to understand the plant status due to numerous, simultaneous, confusing alarms.

The degree to which systems design is an integrated process, including human tasks in the design process, affects safety and survivability. Systems designed from the concept stage to explicitly consider operator tasks and to be integrated will perform better and be more cost-effective than systems that are “integrated” after the sub-systems are designed. For example, facilities often are designed as individual subsystems designed more or less independently of one another and then “integrated.” The fluid systems would be designed by the fluid systems engineers, and the design then turned over to the control systems designers to add on the controls. The fluid systems design and the control system design then are passed to human factors engineers to “add on” the human factors features. With such an approach, the fluid systems and the control systems each have their own set of hazards and vulnerabilities which add up to increased hazards and vulnerabilities for the overall system. (Of course, human performance will be sub-optimal with this approach as well.)

A design that addresses systems and human systems integration rigorously from the beginning will result in systems with improved performance. Functional analysis is a method for integrated design that can be applied at the earliest stages of system design and carried through to any level of detail desired. Tightly integrating the designs of the fluid and control systems, with a “human centered” design process, from the concept design stage, on the other hand, results in reduced hazards, improved survivability, and improved operator performance. With such tight

integration, the control system is designed based on an in-depth knowledge of the behavior of the fluid system and the fluid system is designed to take maximum advantage of the control functions. In all cases, system functions and operator tasks are designed so that the actions of systems and operator actions complement one another for maximum performance, particularly during a casualty. This approach produces a more robust, safe, survivable design, often with little or no increase in cost in the system acquisition, and likely life-cycle cost savings. Successfully achieving such “tight integration” requires engineers working on the design with multi-disciplinary experience who understand the engineering principles involved.

Systems Survivability/Safety Requires an Understanding of Hazards. The engineer must understand how hazards cause systems to fail to design safe, survivable systems. For example, when exposed to heat from fire, fiber optic cable fails by losing strength and stretching until it breaks. The survivability can be improved by supporting the cable, perhaps in metal conduit, so that it is restrained from stretching until it breaks. Understanding how seismic accelerations cause equipment, or supporting foundations, to fail enables the engineer to design or modify equipment to prevent such failures. This process starts with a definition of the kinds of hazards, threats, casualties, etc. that are the basis for the safety and survivability design. Hazards and threats can include, for example: weapon or bomb detonation, tornadoes or other severe weather events, earthquakes, loss of normal electric power, terrorist attacks, accidents such as aircraft or land vehicle impacts, cyber attacks, and simple failure of critical equipment. The magnitude of the event needs to be defined as well. For example, one might design to survive a detonation equivalent to 500 lbs of TNT, but not for a near-direct hit from a nuclear weapon.

For nuclear power plants, the design basis events are well established in regulations. For warship designs, threat analyses are used to define the types and sizes of weapons that a ship will be designed to survive. Criteria for surviving hazards such as severe weather and collisions also are well established. In both industries, criteria such as surviving a hazard event with the unrelated failure of a single piece of critical, active equipment also are well established. Past experience with hazard events also provide useful information about the kinds of hazards a system might experience in the future.

Potential software failures need to be considered in digital control systems. Unlike hardware, which usually has well established failure rates for different types of hardware in different types of service, there are not well established standards for software failures. Factors such as the software architecture and basic control logic to avoid software common mode failures in redundant systems, and the software development process need to be considered to ensure safe, survivable operation.

Operator errors need to be considered in systems safety and survivability. Operator errors typically are considered as human mistakes. Intentional sabotage by an operator also has been considered in more recent infrastructure system designs.

Finally, it is important to understand how to apply hazard mechanisms in the design process. Specific hazard scenarios are useful for helping to understand the range, or envelope, of hazard mechanisms to use as the basis for design, and specific hazard scenarios are very useful for validating the survivability performance for design. There are so many variables that affect

severe hazard scenarios that it is highly unlikely that any actual hazard event that occurs in the future would follow exactly a scenario used in the design. (The one constant in actual severe events is that unexpected things happen.) Using a single hazard scenario, or a small set of scenarios, as the basis for design, generally would be misleading. Rather, a generic set of hazard mechanisms and magnitudes should be used as the basis for design. For example, rather than defining the volume damaged by blast from a specific detonation, a design should be based on a generic blast volume; the system would survive any smaller blast, regardless of the specific warhead or bomb. Scenarios with specific types and locations of bombs then can be used to validate (by analysis) that the design performs as intended.

Systems Survivability/Safety Includes Recoverability. Damage in complex, integrated systems typically is a dynamic event. For example, if power is lost to a cooling system, the damage does not stop there. With loss of cooling, a vital piece of electronics equipment may overheat and shutdown. In liquid cooled equipment, shutdown may occur within a matter of seconds to a few minutes. In air cooled equipment, shutdown may occur within a half hour to an hour (depending on equipment load and ambient conditions). When the critical electronics equipment shuts down, the associated mission system fails. This dynamic, cascading damage often has been considered as an inevitable consequence in past designs. Considering recoverability, however, can improve the survivability performance of the system. In the foregoing example, if cooling can be restored before the electronics equipment shuts down, then there would be no interruption of mission function. Depending on the timeframes involved, recoverability actions may need to be automatic (when the response must occur in seconds), or they could be manual (when response in a half hour or more is adequate); a manual response requires good information systems to enable effective operator situation awareness.

Systems Survivability/Safety Can be Improved by Applying Lessons Learned Across Industries. Fortunately, severe hazard events that stress systems to their limits are not common. As a result, in any particular industry, there is not a wealth of lessons from past experience to draw on for survivability design. Codes, standards, and well established design practices tend to be industry specific, so, engineering based only on the application of existing codes, standards and design practices limits the design to what is learned from experience in that industry. Engineering first principles, on the other hand, are universal; all systems must adhere to those first principles, even though we may not explicitly apply those first principles in designing the systems. Understanding systems safety and survivability based on first principles enables lessons learned and practices from one industry (such as the military or nuclear power industries) to be applied to another industry (such as transportation). In addition, new approaches and capabilities developed in one industry can be applied to improve survivability in other industries.

Basic Survivability/Safety Design Principles

Survivability and safety, although closely related, usually are approached differently in a design. Survivability can be divided into three functional areas: susceptibility, vulnerability, and recoverability. “Susceptibility” is preventing the system from being exposed to the hazard. In the military, this means, among other things, detecting and disabling a threat before it hits. For infrastructure systems, this means, among other things, intelligence, law enforcement, and security force actions to deter or prevent terrorists, or others, from conducting an attack that can impact mission systems.

“Vulnerability” is the immediate affect of a hazard. This happens so quickly (such as the immediate effects of a bomb detonation), or involves events that cannot be controlled (such as severe weather or loss of power from the grid) that operator or automated system actions can do nothing to prevent the effects (or “primary damage”) from happening.

“Recoverability” is the actions taken (automatically by systems or by operators) after damage to prevent the spread of damage and to prevent the loss of mission systems that were not immediately impacted by the hazard.

Safety design, on the other hand, generally is approached by understanding potential hazards, the consequences of the hazards, and the probability that the hazard might occur. “Risk” is the combination of severity of a hazard and the probability that it will occur. For example, catastrophic events that are “probable” (say 5% chance of occurring during the life of the system) might be considered “high” risk. A probable event with negligible consequences, on the other hand might be considered “low” risk. Typically, actions should be taken to mitigate or eliminate “high” risks and, perhaps, “medium” risks. “Low” risks might be accepted. The design approaches to mitigate or eliminate unacceptable hazards could include (but not be limited to) the approaches to improve survivability discussed below.

Susceptibility generally involves functions other than the mission systems that are being protected. Mission system design, nevertheless, should consider susceptibility and may include features to minimize susceptibility. For example, a digital control system can reduce susceptibility to cyber attacks from outside the system by eliminating any means of communication outside the system itself.

Minimizing vulnerability is accomplished by:

- Designing equipment to withstand design basis hazard mechanisms, such as seismic accelerations. This applies to hazard mechanisms that involve the entire facility, such as seismic accelerations and shock from weapon detonations.
- Providing redundancy and separation. To be effective, the redundancy and separation must consider all of the integrated supporting systems as well as the primary mission systems. Redundancy often is provided to ensure adequate reliability for normal operations, so achieving survivability through redundancy and separation may not entail substantial cost increases. Physical separation decreases the probability that both redundant systems or system components will be damaged by a localized hazard event such as a fire. Providing

adequate physical separation throughout the entire train of mission and support systems often is a design challenge that requires a highly integrated and analysis intensive design effort.

- Providing protection or armoring. In some cases it is not practical or affordable to provide adequate redundancy and physical separation. In such cases, the non-redundant mission systems and their associated dependencies should be located in a small, contiguous volume to minimize the target size, and that area should be protected to the extent practical and affordable. Protection could involve features such as armor, shock mounting or heightened security.

Maximizing recoverability is accomplished by:

- Where feasible, designing components to “ride through” interruptions in support systems. For example, sometimes electronics components can be designed to continue to function at an acceptable level with a temporary loss of cooling. This can be coordinated with the recoverability design of the cooling system so that the electronics component can function for the time it takes to restore the cooling system. Conversely, the ride through capability of the electronics components defines recovery requirements for the cooling system.
- Designing mission and support systems to isolate damage and restore function to surviving portions of the systems. This requires that mission systems and their corresponding support systems be designed with an architecture that enables isolation and restoration in a manner that results in operation and support of the surviving portions of the mission systems. This requires close integration of the design of all of the vital systems and intensive analysis of the post-damage recoverability performance of the integrated design.
- Providing robust, survivable automation where rapid response is required. This likely requires a tight integration of the systems designs with the controls designs as well as novel approaches to controls. “Device level control” has proven to be highly survivable and robust where it can be implemented. Device level control is an architecture where the device being controlled does not require data or commands from any other part of the system to automatically make an informed control decision and affect that control decision. A simple circuit breaker is an example of device level control. A “smart valve” that includes the onboard sensors, processor, control logic, and actuator to determine if there is a rupture downstream and close to isolate the rupture, without communicating with any other device, is another example of device level control.
- Providing information systems designed for operator decision making in crisis situations. This involves an understanding of the actions an operator can take (or direct), the optimum information needed by the operator to make a decision about those actions, and the human factors involved in making the display of that information intuitive to the operator (not necessarily the same as a display that intuitive to the designer).

System design also can be improved to address risks identified by the safety analysis. Typically, safety design improvements involve one or more of the following:

- Eliminate the hazard,
- Mitigate the hazard with passive design features, and/or
- Mitigate the hazard with active design features.

For example, if fire started by a piece of equipment is the hazard of concern, the hazard might be eliminated by selecting a different piece of equipment. For a fire to ignite, a fuel source and an

ignition source have to come together in the presence of air (or oxygen). It might be feasible to eliminate either the fuel source or the ignition source in the system design; or to separate them such that they could not come together to ignite a fire. Insulating a hot surface could be a passive design feature to prevent fire. Adding a fire detection and suppression system could be an active design feature to protect from fire. In practically every case, passive design features, if feasible, more reliably mitigate risk than active design features.

Additional system maintenance directed at safety or survivability features may be required to provide sufficient confidence in the safety and survivability performance of the system throughout its life. Most systems for normal operation are monitored during operation and impending or actual failures are detected and corrected without severe consequences. Survivability features, on the other hand, often are not exercised during normal operation. As a result, a survivability feature may fail without detection and, when needed, not function. This dilemma is resolved by “surveillance testing,” a term used in the commercial nuclear power industry. This is testing conducted during the normal operation of the system, or during planned maintenance activities, to test the survivability features of the system. For example, periodically starting and loading emergency generators. The system should be designed to accommodate surveillance testing, when needed.

BENEFITS FROM GOOD SAFETY AND SURVIVABILITY ENGINEERING

Too often when a severe hazard event occurs, critical systems fail to function as expected and dire consequences result. As noted above, it often is not feasible to test systems under such extreme conditions, so, their safety and survivability performance is completely dependent on the quality of the engineering in designing those systems. Modern mission systems typically depend upon the integrated functioning of several support systems and interacting mission systems. Successful integration of such complex systems requires a multi-disciplinary approach to design that often is attempted as an “add on” to the end of a design rather than a fundamental approach to the design from the beginning. This is another reason for systems not achieving their required potential performance when a severe event occurs. Good survivability engineering overcomes these problems and produces systems that perform with confidence at their full, required potential under severe and unpredictable hazard conditions. This avoids the damage, loss of expensive equipment and facilities, and loss of life that often occurs when critical systems fail to function as needed.

When a severe hazard event does occur and critical systems are damaged and fail, systems designed for good survivability can be restored with less cost and time. This means less down time before a system is restored to operation.

Good safety and survivability engineering often improves the survivability/safety performance of systems with little or no added cost of the systems. This is because improving safety and survivability often involves locating equipment, provided already for other reasons, somewhere that enhances survivability and connecting components in a manner that considers integrated survivability performance (for example, determining which power panels to connect to which critical components).



Applying lessons learned, approaches and innovations from other industries can improve survivability and safety while also reducing system cost. Other industries may have developed more efficient or effective design tools, integrated system approaches, or novel capabilities that could lead to performance improvements and reduced costs when applied to new industries. This transfer of knowledge enables improvements without having to bear the cost and time for developing those capabilities.

MPR SURVIVABILITY & SAFETY ENGINEERING CAPABILITIES AND EXPERIENCE

Systems Survivability/Safety Requires Rigorous Engineering. MPR was founded 45 years ago by three of the senior leaders who developed nuclear power for submarines. That development of nuclear power was first-of-a-kind engineering, developing and implementing components and systems that did not exist before, that was done with a level of engineering rigor and quality that was new to much of industry. This rigorous approach to engineering and culture of quality is the foundation of MPR. While maintaining this foundation in our culture to this day, 45 years of experience has refined our approach to first-of-a-kind projects and expanded our culture of quality engineering to work in several diverse industries.

Our rigorous approach to first-of-a-kind projects and effective management of risks has made MPR a leader in the development of medical products and pharmaceutical processes. We typically get products from concept to market in substantially less time than others, our systems readily pass regulatory tests and inspections, and our products meet our clients' expectations without rework.

MPR is known throughout the commercial nuclear power industry, with regulators as well as plant owners and operators, for consistent quality and for getting to the root cause of problems and finding practical solutions to those problems. A fundamental objective in nuclear power engineering is preventing the release of radiation to the environment in the event of severe casualties and hazards. Much of MPR's work in the industry is related to safety and survivability – maintaining critical safety functions in the event of equipment failures, loss of power, and other casualty events. We have successfully applied capabilities developed by the nuclear power industry, such as tools for probabilistic risk assessments, to survivability engineering in other industries, such as fire protection in Navy ships.

MPR has performed critical engineering for the Navy for decades. We helped the Navy develop and implement the SubSafe program to ensure the reliable performance of systems and equipment vital to the safety of the submarine. The Navy comes to MPR to make improvements in critical systems, for example, we currently are developing a comprehensive standard for ship fire protection as a follow up to a recent severe fire aboard an aircraft carrier. MPR determined the root cause of the production of hydrogen sulfide in Aqueous Film Forming Foam (AFFF) fire suppression systems and developed the system and design criteria to mitigate the hydrogen sulfide production and prevent the personnel casualties that occurred in the past. We also



defined the architecture and supported the design of an innovative fire protection system to automatically suppress fire after a weapon hit for the Navy's advanced new destroyer design.

MPR's decades of work on critical systems across several industries has built a strong culture of exceptional engineering rigor that provides a solid foundation for our work in systems safety and survivability.

Survivability/Safety Requires Human Systems Integration. Since we develop our engineers with real-world experience in multiple disciplines, we inherently take a multi-discipline approach to our engineering. The analysis tools we've developed and use for survivable systems design integrates systems from both geometrical and functional perspectives, both of which are needed to understand how integrated systems respond to hazard events.

MPR applied a human systems integration approach to our successful design and development of a supervisory control system for the Navy's Damage Control Automation for Reduced Manning Program. As a result of completing the functional analysis in the initial phase of the design, the software development was completed ahead of schedule and the system met requirements with only minor debugging.

MPR performed a leading role in the integrated survivable systems design for the Navy's new, advanced destroyer. This included a key role in human systems integration for survivability, damage control and related control and automation systems. Multi-discipline teams performed in-depth functional analyses using rigorous systems integration to accomplish human systems integration and define the requirements for the subsequent design of individual systems and complementary operator functions. This ship design incorporates advanced, automated systems survivability well beyond any previous Navy ship design to survive and recover from damage with minimum manning. MPR defined the architecture of the innovative fire suppression system that automatically recovers from weapon damage to suppress post-hit fire. This system was successfully demonstrated with a full-scale, at sea, weapon effects test. MPR led the Navy's Recoverability Working Group in defining the process for rigorously assessing the integrated survivability performance of vital data networks, mission systems, cooling water systems, fire suppression systems, electrical distribution systems, and ship control systems. This analysis provided derived survivability requirements to individual system designers to achieve survivability performance objectives. One of the challenges in this project, which MPR led the way in solving, was conducting the survivability analyses within the time required to implement identified design improvements before the design was complete. MPR also had a key role in defining the functions and manpower for the damage control teams that would complement and backup the new, automated systems.

MPR developed the technology for fluid systems to automatically recover from damage in a highly survivable manner with a robust design that inherently adapts to multiple unpredictable component failures. We currently are providing the "smart valves" and electronics equipment for this system for new DDG 51 class destroyers. As part of the design of this system we developed a computer based simulator that includes the ship compartmentation, chilled water system, supporting data networks, and supporting electrical distribution system as part of the analysis. The simulator includes high fidelity geometric models of the ship compartmentation



and systems, an integrated functional model of the systems, and a weapon damage model. The simulator includes a user friendly graphic interface that enables the rapid definition of damage scenarios and assessment of survivability performance that provides the designer with insights into how to modify the systems architecture, if necessary, to correct survivability deficiencies.

Systems Survivability/Safety Requires an Understanding of Hazards. MPR has analyzed hundreds of hazard events to identify lessons learned to improve systems safety and survivability with respect to related doctrine as well as system design. We have conducted or participated in many full-scale damage tests (fire tests, weapon effects tests, shock tests, manned live-fire tests). This experience provides us with a realistic, first-hand understanding of how hazard events affect integrated systems. We have developed damage models (including the effects of fire, blast and fragments on systems) for use in systems design analyses, and we often work closely with experts in areas such as fire, blast, fragmentation, and seismic engineering to refine our design models and to bridge across these specialty areas and engineering for systems safety and survivability.

MPR evaluated Navy test results and industry standards to create a post-weapon hit fire scenario for fire and developed the “Operational Objectives for Firefighting” which is the basis for survivable fire protection systems design for Navy ships today.

One of the fundamental issues with post-weapon hit fire protection is a lack of understanding of the configuration of combustible materials after a weapon hit. Scattered, splintered materials will burn differently than intact components (for example, toothpicks will ignite easier and burn faster than a solid piece of wood with the same mass). MPR was the principle investigator for a major, full-scale, live-fire weapon effects test with aircraft aboard a decommissioned aircraft carrier. We developed the rationale for the conduct of the test, defined the test objectives, prepared the test plan, managed the preparation of the test articles (including the ship and the aircraft), and set up the test instrumentation. (We did not get test results because the ship was sunk unintentionally during a prior weapon effects test conducted by another organization.)

MPR analyzed Navy experience with warhead detonations aboard ships and developed realistic, generic weapon damage models for use in design analyses. Based on this experience, we included realistic damage and fire spread models in the supervisory control system we developed for the Navy’s Damage Control Automation for Reduced Manning Program. We defined the approach to damage modeling that enabled the effective analyses of systems survivability to support the recent design of the new DDG 1000 advanced destroyer. And, we developed the Damage Modeler software program to provide understanding of damage events for shipboard training.

MPR is a recognized leader world-wide for the qualification of digital control equipment for nuclear power plants. This qualification work requires an in-depth understanding of how hazards can affect the equipment hardware and software and how to conduct qualification testing to ensure that defined hazards will not affect the safe operation of the equipment.

Human error is an important factor in assessing the reliable performance of systems that require human decisions and actions. There is substantial data on human error performance from



nuclear industry data. MPR has drawn on that nuclear industry data and adapted it to a variety of analyses. This includes factors to adjust human error probabilities to account for training, stress, and display quality. We've enhanced our understanding of human capabilities in stressful situations with participation in over a decade of full-scale, manned firefighting tests conducted by the Navy.

Systems Survivability/Safety Includes Recoverability. MPR leads the Navy in recoverability design of complex, mission critical systems in advanced surface combatant ships, advancing the state-of-the-art over the last decade.

In the mid-1990's MPR performed the Navy's first analysis of damage control performance to define quantitative performance benchmarks for shipboard damage control. Based on this and other experience with systems safety and survivability, in 1997 we defined the concept of systems "recoverability" as part of survivability design and recommended to the Navy that systems recoverability be addressed with rational analysis as part of ship design (before then, design for recoverability meant merely evolving legacy designs based on lessons learned from incidents).

As a follow up to the USS COLE terrorist attack incident, MPR developed a "Recoverability Design Guide" for the Navy to provide guidance for designing systems for recoverability.

Applying the foregoing MPR work, the Navy (with MPR in a lead role) applied rigorous analysis to the recoverability design of vital mission support systems for the advanced DDG 1000 design. This work was key to advancing the state-of-the-art for automated systems recovery from damage, enabling a substantial reduction in the size of the ship's crew. The successful performance of some of the key, high risk, systems designs was demonstrated with full-scale, at-sea weapon effects tests.

Systems Survivability/Safety Can be Improved by Applying Lessons Learned Across Industries. MPR's culture of approaching challenges from first principles enables us to easily translate lessons learned and concepts from one industry to solve problems in other industries, and it enables us to advance the state-of-the-art in challenging areas such as systems safety and survivability. Our "organization without boundaries" in which each engineer typically works in all of the industries we support (commercial nuclear, energy, DoD, DoE, USDA, medical products and pharmaceutical processes) also facilitates transferring knowledge and lessons learned across industries.

For the Navy's Damage Control Automation for Reduced Manning Program, MPR developed a supervisory control system for systems survivability and damage control. As part of the program we invented device level control logic for "smart valves" to provide robust, highly survivable, automatic isolation of ruptures in fluid systems. For integrating the supervisory control system and the smart valve device level controls, we applied lessons learned *from the aviation industry* and used fundamentally different logic for the supervisory and device level controls to avoid common mode failures in the control logic. The MPR system performed successfully over several years with dozens of tests with actual system damage.



One of MPR's engineers led the Hull, Mechanical, and Electrical (HM&E) portions of the Navy's first Survivability Review Group in the mid-1980's that investigated ship systems survivability in depth and developed the Navy requirements and methods for the survivable design of ship systems. This effort analyzed damage events and lessons learned from British ships damaged during the Falklands War. Building on a methodology from the aviation industry, the engineer developed the "damage tolerance / deactivation diagram" method for assessing integrated systems survivability. This method became a Navy standard for ship designs that was applied first to the very successful DDG 51 class destroyer design, and most recently by MPR to the advanced DDG 1000 destroyer design now starting construction.

MPR is a recognized leader in digital control systems for the commercial nuclear power industry. The reliable functioning of critical controls during severe casualties is a primary concern for nuclear plant control systems. MPR developed the control system requirements for the Advanced Light Water Reactor design developed by the commercial power industry. MPR had a leading role in representing the plant owners and the regulatory agency in ensuring adequate design and implementation of the state-of-the-art digital instrumentation and controls in a new nuclear power plant in Taiwan. Working for the Electric Power Research Institute (EPRI), MPR developed the industry standards for qualification of digital control hardware and software for nuclear plant safety related service. MPR is the recognized leader for the qualification of digital control equipment for nuclear plant safety related service. The Nuclear Regulatory Commission recommends MPR to vendors who want to get their equipment qualified. MPR conducts qualification programs for vendors in the US and around the world. MPR also supports plant owners in the upgrade of their control systems from legacy analog controls to modern digital controls. We have applied lessons learned from our nuclear industry experience to the design, development and qualification of digital controls for the Navy and for medical products, as well as to "owner's engineer" oversight of safety related digital controls for the design and construction of new DoE nuclear processing facilities. MPR can readily transfer these capabilities and lessons to other industries, such as air traffic control.

MPR developed a transient analysis model of a nuclear plant emergency power distribution system using the Electrical Transient Analysis Program (ETAP) commercial software package. We used the model to investigate the voltage and frequency response of an emergency diesel generator with the proposed digital governor upgrade during loss of coolant and other accident scenarios. With the increasing electric loads aboard new Navy ships, the Navy is moving from the traditional 440 VAC distribution systems to higher voltages, and they are concerned about the survivability and safety implications of these higher voltages. Building on our nuclear plant experience, MPR used the ETAP software to evaluate the hazards from faults in the 4.6KV and 13.8KV electrical distribution systems in a new ship design. We characterized the safety hazards associated with specific equipment (the distance within which equipment could be damaged and personnel injured in the event of an electrical fault), and we identified the need to provide arc fault detection and isolation for certain pieces of equipment.

MPR developed and is providing automated digital controls for damage recovery in the chilled water systems of new Navy destroyers. In addition to developing the software in accordance with IEEE 12207, we applied lessons learned and quality assurance procedures from our commercial nuclear power work in designing and developing reliable software. Our system has



successfully performed during dozens of land based tests over several years and recently passed the first shipboard test aboard a new ship.

Survivability/Safety Design Principles.

MPR developed the Navy's standards and design methods for the integrated design of vital ship systems to minimize their vulnerability.

MPR performed the Navy's first analysis of damage control performance to define quantitative performance benchmarks for shipboard damage control. Having such quantitative performance benchmarks is the first step in enabling a rational design process to achieve an optimal design. MPR's work on the Navy's Damage Control Architecture Program in the early 1990's showed the need for improved survivability (particularly recoverability) for fluid systems such as the firemain and chilled water systems, and led to R&D programs to dramatically improve the survivability performance of these systems.

MPR developed the Navy's formal fire risk assessment methodology, adapting the requirements of MIL-STD 882, System Safety Program Requirements, and adapting a risk assessment methodology from the petrochemical industry. MPR applied this risk assessment methodology (which is very similar to the Integrated System Hazard Analysis in the "FAA System Safety Handbook") to many fire hazards and several ship designs over the last 15 years. The Navy has adapted the MPR fire risk assessment methodology in a formal design data sheet.

MPR also developed a probabilistic risk assessment model for fire protection. The model includes the behavior of fire hazards, fire protection equipment and systems reliabilities, and human error probabilities. The model approach is built on the nuclear industry probabilistic risk assessment methodology (we use nuclear industry software for the model). MPR has applied this probabilistic model, which provides in-depth understanding of system safety, to selected critical hazards aboard Navy ships.

MPR did the early engineering to define the basic approach and component performance requirements for the automated firemain recovery system that was developed by the Naval Surface Warfare Center – Carderock Detachment (NSWC-CD) formally the Naval Ship Systems Engineering Station, Philadelphia (NAVSSSES-Philadelphia). MPR also supported the warhead live-fire testing of this system conducted by NAVSSSES in the mid-1990's at the Aberdeen Proving Ground. This was the first development and test of the programmable automated valve technology that now is providing to the Navy for new DDG 51 class destroyers.

MPR conducted all of the development, engineering, and installation of the fluid systems automated recoverability for the Navy's Damage Control Automation for Reduced Manning (DC-ARM) program. A key challenge of the DC-ARM program was the development of the technology for the highly survivable isolation of ruptures in fluid systems, particularly the firemain. MPR developed, and patented, the "hydraulic resistance" logic that enabled the DC-ARM "smart valve" (the same programmable automated valve technology that is the basis for the CWAS Upgrade) to utilize true device level control for the survivable isolation of firemain ruptures.



As part of the DC-ARM program work, MPR clarified the concept of device level control for survivability and applied an effective approach to the design of hierarchical control systems that starts with an understanding of the control logic architecture of the system. This provides the basis for the rational design of complex control systems that are highly survivable and practical to develop and maintain.

MPR developed a “Smart Valve Design Guide” for use by shipyard designers. This includes basic information on systems survivability design to provide the foundation for designing fluid systems using MPR’s smart valve technology.