2011 Naval Submarine League Symposium
Admiral Kirkland H. Donald, U.S. Navy
Director, Naval Reactors
19 October 2011

ADM Mies, thank you for the warm introduction. Fellow Flag Officers, distinguished guests, Submarine Force, and Naval Submarine League members: it is a privilege to be here again this year to discuss the future of our community. Thank you to the Naval Submarine League for hosting this symposium and to all the individuals that helped to put this event together.

The Submarine Force operates in complex, high consequence environments where vigilance is always required. In times like these – with the design of a new submarine class in progress, continued operations with an aging Fleet, and exceptionally high public sensitivity for technology gone awry – any sort of news worthy failures will certainly undermine the public's limited trust in our abilities and significantly increase the difficulty of our work. Therefore, it is imperative that the Submarine Force continuously embody the fundamentals that have made us so successful.

The Naval Nuclear Propulsion Program's history of success is sustained by a strong culture of careful and conservative engineering. We honestly assess what is unknown, pre-engineer tests/limits/margins as appropriate, take cautious approaches to change, and formally include diverse and dissenting opinions in decision making. These fundamentals keep the Program technically grounded when facing challenges under external and economic pressures.

As with any intelligent organization, our Program not only fosters a culture that analyzes its mistakes and then shares the lessons learned with others to promote improvement throughout the enterprise, we also examine the mistakes of other organizations involved with high consequence technology in order to apply their lessons learned to our organization.

For my part today, I will discuss some of the lessons from three unique and tragic events in order to remind all of us how our Program's fundamental principles keep us successful. I will also point out that as a community, we are not immune to catastrophic failures. But before I begin, a brief synopsis of those three events:

- First, the nuclear disaster at the Fukushima Dai-ichi Nuclear Power Plant was caused by two "beyond design basis" natural events that resulted in over 25,000 dead or missing, tens of thousands displaced, and infrastructure and industry severely impacted. As a result of the earthquake and tsunami, all facility and offsite electrical power was lost to reactor Units 1-5, causing a condition known as station blackout. Ultimately, the Tokyo Electric Power Company (TEPCO) and plant operators were unprepared to deal with the long term station blackout which resulted in core meltdowns and the release of fission products to the environment.
- Second, the catastrophe that sank the Deepwater Horizon drilling rig resulted in the death of 11 men, spilled over 4 million barrels of crude oil into the Gulf of Mexico and disrupted an entire region's economy while damaging fisheries and critical habitats. The leak was caused by the failure of a cement barrier in the ocean floor used to isolate the well. This failure was caused by the combination of using an insufficient volume of cement in the barrier which was also poorly mixed, as well as an application

procedure which required a certain degree of “finesse” from the operators to ensure success. Additionally, late changes to the temporary abandonment procedure resulted in the placement of an inadequate secondary barrier. And finally, the blowout preventer – a failsafe valve on the ocean floor that is used to seal the well – experienced mechanical binding and could not stop the flow of oil into the Gulf of Mexico.

- Third, the loss of the USS Thresher which resulted in the death of 129 officers, crew members and civilian technicians. The most likely cause of the accident was the failure of a silver-brazed joint in seawater piping while operating at or near test depth which allowed high pressure seawater spray to short out electrical equipment and led to a reactor scram. At this point in Program history, a scram would have prevented the quick restoration of propulsion and when combined with a failed blow system, the crippled submarine could not make it back to the surface.

Now that I provided some background on the three events, I would like to highlight six fundamental principles that help all of us safeguard our technology from catastrophic events:

1. Robust safety and hazard analysis
2. Careful assessment and management of the risk versus reward associated with new technologies
3. Strong technical competency to ensure effective regulatory oversight
4. Strict management of emergent change
5. Accessible policy documentation to enable continuity, formality, and consistency in work execution and emergency response

6. Active sharing of lessons learned and documenting them for future reference

The first principle is the importance of safety and hazard analysis. As a Program, we must guard against the “compliance equals safety” mindset by fully evaluating all of the potential hazards associated with our work – including hazards not addressed by existing requirements – and ensure that systems and processes critical to safety are identified and prioritized.

As seen with the Deepwater Horizon accident, British Petroleum and the Mineral Management Service – the industry’s oversight entity – focused on reducing the rate of reportable personnel injuries but ignored the potential for catastrophic events such as explosions and well blowouts. They falsely believed that their operations were safe based on personnel injury rate statistics and compliance with prescriptive, but inadequate, requirements.

In the case of the Thresher accident, safety and hazard analysis was not sufficiently evaluated for the abilities of nuclear powered submarines to combat all casualties. Specifically, a court of inquiry found that the blow system was not adequately designed given the higher performance of nuclear powered submarines. World War II boats could only submerge to about 400 feet, while the newer, heavier boats were going significantly deeper and for longer periods of time, but no additional blow capacity had been built in or more stringent Quality Assurance applied. To counteract this oversight, submariners changed the way they did business to include design, material control, work control practices, and quality

assurance. Born from this was the Submarine Safe Program, also known as SUBSAFE, to provide the maximum reasonable assurance of watertight integrity and recovery capability. Objective Quality Evidence became a way of life and we created an auditable trail to verify work was authorized, the materials were correct, the worker doing the work was qualified, the work was performed correctly, and the system was tested satisfactory.

The Fukushima reactor accidents were the result of what is known as “beyond design basis” conditions caused by natural phenomena. While seismic and tsunami conditions were addressed in plant safety analysis and design, nothing assumed the magnitude experienced on that day. Knowing it is impossible to drive risk to zero, a careful and skeptical review of our assumptions and evaluation of our technologies’ response to “beyond design basis” conditions, be they externally or internally initiated, is prudent given the high consequence of failure. Once the expected response is evaluated, consideration must be given to an organization’s ability to mitigate negative consequences. Furthermore, Fukushima highlights the need for a realistic approach when evaluating the abilities of operators to work in the expected environment of a casualty.

The second principle is the importance of carefully assessing and managing the risk versus reward associated with new technologies. The implementation of novel methods in design work and new technology bring inherent risks with their benefits. The basis for deviating from proven technology solutions must always be justified, intended benefits should honestly be weighed against intrinsic risks, and accumulated risk – particularly associated with hazards not covered by existing requirements – should be monitored. For new technologies with long

development cycles, engineers must be willing to periodically evaluate the basis for implementing new technology to determine whether it still makes sense.

With Deepwater Horizon, government policy and regulation drove the oil industry to pursue rich oil reserves in deeper water which pushed the limits of what available technology allowed. To sustain this, technological innovation largely focused on enabling exploration and drilling while advances in understanding the new environments and preparing for or safeguarding against new or evolving “pinnacle events” lagged.

The importance of managing new technologies is not just limited to internal developments. New external technologies may provide the ability to revalidate or update internal design bases. For instance, significant advancements in the physical understanding of seismic and flooding hazards may aid in protecting other facilities from the events experienced at Fukushima. Similarly, a more stringent evaluation of the numerous failures found while using the newly developed ultrasonic testing on Thresher’s silver-brazed joints may have prevented the tragedy.

The third principle affirms that strong technical competency is essential for effective regulatory oversight. For the Naval Nuclear Propulsion Program, Naval Reactors is solely responsible for oversight of the development, safe operation, and eventual dismantling of all of the Navy’s nuclear assets. To do this, we employ the nation’s top engineers and scientists as well as the Fleet’s proven officers and enlisted sailors.

Conversely, the regulatory oversight of the offshore drilling industry became ineffective because the engineering capabilities at Mineral Management Service did not keep pace with that in the oil industry as they rapidly expanded into deepwater drilling. This lack of knowledge at the Mineral Management Service led to an overreliance on the oil industry for technical assessments and perfunctory reviews and approvals.

While the technical competency of Japan's nuclear oversight division – the Nuclear and Industrial Safety Agency – is not in question, an organization's oversight ability is significantly impacted by its ability to collect and analyze data. During the Fukushima accident, the NISA's offsite center – a 15 minute drive from Fukushima – had no power or land/cell/satellite phone lines and the backup generator was not working. This left government officials dependent on TEPCO headquarters for information which caused crossed signals at times and blurred the lines of command and control, hampering critical oversight.

The fourth principle stresses the need for us to manage emergent change. We must continue to reinforce formal concurrence and technical approval processes and not allow cost and schedule pressures to dictate the consideration of technical compromises and other mitigation actions in order to meet or recover schedules.

History shows that the Program was not always as good as we could have been on this principle. While not ideally designed by today's standards, Thresher's blow system was most likely crippled by strainers the shipyard had installed – on its own – to prevent foreign material from damaging system valves. These strainers facilitated the growth of ice plugs in

the air lines during an emergency blow that prevented air from entering the ballast tanks. Even though today this informal system modification seems inconceivable, at the time shipyards were allowed to make deviations to drawings without any oversight, which clearly undermined the ability of technical authorities to ensure the safety of alterations.

Similarly, British Petroleum and the Mineral Management Service did not formally manage changes to the Macondo well design and temporarily abandonment procedures, making significant last minute changes with informal agreements via email. The lack of formal change management led to inadequate technical review of planned well conditions which were attributed to the blowout.

The fifth principle is that accessible policy documentation enables continuity, formality, and consistency in work execution and emergency response. At the Macondo well, there was a lack of consistent and standardized procedures for critical operations such as the temporary abandonment of the well and the pressure test used to verify the well was not leaking. While British Petroleum procedures stated the number of required barriers when isolating a well, the specifics of how to conduct this isolation were left up to Macondo engineers on an ad hoc basis. Since there was no written procedure for the pressure test used to verify the well was isolated, common practice allowed experienced operators on scene to analyze the test results and certify the well as sealed. However, at Macondo a lack of experienced personnel led to the misinterpretation of test data and with no formal procedure or technical guidance on station to state expected results, rig leadership did not request an offsite technical review of the data.

Accidents at Fukushima highlight the importance of having plant operators who are well prepared and well supported by technically sound and practical procedures, guidelines, and strategies. During emergencies, a clear and preplanned command and control system that supports streamlined decision making must be at the ready. Heated discussions between TEPCO and Japanese government officials concerned about the international perception of venting the reactors wasted significant amounts of time. Additionally, protocols prevented the plant manager from taking casualty actions for the high pressure conditions until permission was received from top officials at TEPCO and in the government of Japan.

As I stated earlier, intelligent organizations learn from their own mistakes as well as the mistakes of others. As operators and maintainers of high consequence technology, we must be ever vigilant in our search for learning opportunities. This leads into my final principle that actively sharing lessons learned and documenting them for future references is a cornerstone of our success.

If you look at the early history of submarines, between 1915 and 1963 the Navy had 17 non-combat losses of submarines – an average of 1 every 3 years for a total of 473 submariners killed. With this statistic in mind and after reviewing the piping system failures of some other early nuclear submarines, it seems that a tragedy like Thresher was almost inevitable because the Submarine Force was not learning from its mistakes.

- USS SKATE had two silver-brazed joint failures, one during each shot of shock testing.

- USS ETHAN ALLEN had a threaded plug blow out of a strainer in the trim system, there were minor fires and a reactor scram.
- USS SNOOK found a five inch silver-brazed seawater line leaking.
- USS Thresher had two failures during builder's trials – the first was a seawater vent line that was made of steel instead on monel pipe and then a 1-inch joint in the trim system that lacked a silver-braze insert ring.

Likewise, a failure to actively share lessons learned in drilling led directly to the loss of well control and blowout at Macondo. The National Commission concluded that if the crew on Deepwater Horizon had known and trained on a very similar incident – a near-miss that occurred in the North Sea a few months earlier – their accident and subsequent oil spill would likely have been averted.

The organizations involved in all of the previously mentioned accidents did not intentionally walk towards disaster. Keep in mind all the organizations involved in these tragedies had engineers and operators working with highly complex systems operating in difficult and challenging environments. Additionally, they were routinely faced with decision points that required engineers and managers to make judgments impacting the balance between acceptable risk, continuous cost and schedule pressure. In all cases, the impact of failure had significant consequences for both personnel and the environment.

Every day nuclear powered submarines and aircraft carriers "have the watch" throughout the world. Our shipyards safely and effectively build our newest vessels while overhauling and

refueling our current workhorses. And a pinnacle milestone for our Program will occur next month as USS ENTERPRISE celebrates her 50th birthday after having safely steamed over 2 million miles and completed 20 full deployments.

As the Naval Nuclear Propulsion Program undergoes a broad and significant demographics shift, and without recent marquee failures or Cold War challenges to reinforce our principles and focus our efforts, the lessons presented by these three incidents could also be seen as timely warnings to stave off our own organizational arrogance and success-driven numbness to the serious risks involved in our daily work.

Thanks again to the Naval Submarine League and to all of you for participating in this symposium. I am looking forward to the remaining presentations and I would be happy to take some questions.