

2.8 The Need to Improve/Increase the Application of System Safety Engineering and Safety Management Earlier in the Acquisition Process

Acquisition of any complex military hardware is risky and failure to properly consider safety early in the process can be measured in terms of cost, performance and schedule impacts. Unsafe performance in developmental and operational tests, and latent (hidden) safety problems that emerge late in development or after deployment, and even accidents that destroy hardware and injure or kill sailors can adversely affect program schedules and prevent program success. Integrating safety assessment and risk management processes into the early stages of the acquisition life cycle would save costs and preserve schedule. Integrating a process for robust safety evaluation and safety risk mitigation into the acquisition process would provide potentially significant cost savings to program life-cycle costs, and reveal opportunities to eliminate hazards through appropriate engineering means. To integrate safety, we must foster and promote the development of a professional safety element of the acquisition workforce that would staff an effective safety risk management program incorporating system safety, including flight, weapons and ground safety for each Acquisition Program conducted by the Navy. Creating such an integrated approach to safety risk management, one that assists in also providing an effective feedback/hazard tracking system, based on mishap reports, tests, and other periodical reports, could increase the level of safety in new acquisition programs and system modifications. Additionally, analysis and identification for hazards and the systematic and concerted effort to eliminate or reduce those hazards using the hazard mitigation precedence of Mil Std 882 is paramount to production of a safe system.

2.8.1 DISCUSSION

Acquisition reform leaders have proposed further revamping the current DoD acquisition program and policy guidelines by an additional streamlining and simplifying of the present DoD 5000.1 instruction and making the DoD 5000.2R series advisory instead of mandatory. The shift in management philosophy, relying on performance-based criteria and standards, and transferring the primary responsibility for safety awareness and system safety review to the contractor has created significant concerns. Both government and industry representatives have expressed concern that limited resources for oversight and lack of integration of safety into the design process will increase risks, affect performance and ultimately raise liabilities for both government and contractors. In the performance based culture that we are in we need to be “smart buyers” by understanding the of analysis done by the prime contractor and remaining closely coupled with the development process, helping the government understand the risks and properly accept or mitigate those risks at the appropriate time (sooner is better than later). The contractor should be held accountable for assessing and identifying the hazards. As stewards for the taxpayer the government needs to know that the proper effort is being implemented, that it is providing results and that these results are being used for appropriate risk mitigation. The government needs to be involved in this process but the contractor has to own the responsibility for proper and safe design (unless, of course, they are producing to government spec!)

If the limited references to safety and safety review requirements in the present DoD 5000.2R series are further weakened or eliminated, insertion of design safety measures may be reduced. The safety community believes this should greatly concern senior management Navy-wide.

Unfortunately, most failures in safety engineering do not generally manifest themselves as glaring and obvious design defects. There can be major design failures, but most such extremely serious and/or potentially show-stopping errors are usually uncovered by the design review process itself, or become intuitively obvious during attempts to validate the design criteria. Instead, the overriding cause of a system failure results most likely from the interaction of a number of seemingly insignificant design errors. If one were to evaluate the impact of the least favorable potential interaction of each of these separate and seemingly non-consequential safety concerns, a model of the critical path of their interactions might yield evidence of the possibility for a serious or even catastrophic failure that is not readily recognized by simply dealing with each minor safety concern evaluated separately and individually. The system safety process was developed initially in the aerospace industry to address this type of risk factor that allowed the failure of rocket launches and other complex high-risk systems. The system safety engineering and management processes have been used successfully by other industries increasingly over the last 40 years to accomplish these same objectives.

The top managers of the Defense Acquisition process seem to be pushing for greater reliance on contractor performance in an effort to capitalize on economies of scale. However, this change in philosophy is proceeding without budgeting for necessary safety review oversight. In this environment, we are increasingly dependent on the good intentions of the systems builder, while incentivizing the contractor to reduce costs, and by so doing, foster an open invitation to cut corners with regard to a sound safety engineering discipline either by design or benign neglect.

Without a thorough understanding of the ramifications of migrating from a highly disciplined MIL-STD environment to the more flexible performance-based standard, safety reliability and safety confidence levels may be compromised. Incorporating safety and health considerations early in the acquisition process creates an excellent opportunity to protect the Navy's human and economic resources while supporting mission and protecting our people. All acquisition should incorporate current technology to mitigate the hazard to operators, maintainers, and systems in the most cost effective way.

The Weapons Safety Explosive Safety Review Board (WSESRB) becomes fully involved with weapons and explosive safety concerns in the acquisition process beginning with the earliest stages of concept and design and follows the progress in weapon system and/or equipment development through full-scale production and deployment. In contrast, the Environmental Safety and Occupational Health (ESOH) review teams generally do not pursue the safety concerns to the same degree of rigor as the WSESRB and may not remain in existence through the full-scale production and deployment phases. Much like the WSESRB Board, a safety model team could be

initiated by designating and assigning acquisition safety program management responsibilities to a safety organization that is independent from the specific facility (user) management. Responsibility for design and risk acceptance needs to stay with the Acquisition manager and their line organization. The ESOH needs to have independent oversight to assure the proper acquisition safety processes are built in and are functioning properly. There needs to be a proper balance between insight and oversight in this process.

2.8.2 FINDINGS

Several variables continued to rise to the top of the working groups discussions on increasing and enhancing safety in acquisition.

- (a) Various safety disciplines, across the Navy, (e.g., OSH, System, Aviation) are not well integrated as applied to programs and projects. Largely driven by disparate funding sources, (OM&N, NWCF, RDT&E), they are managed as separate entities. There is no standard set of safety guidelines set for Operational requirements documents (ORDs) or Mission Needs Statements MNSs.
- (b) The entry of most safety disciplines into the acquisition process is too late in the life cycle to make a difference. Safety requirements and processes need to be mandated and applied early in concept exploration and used as selection criteria. Guidance in this area is limited and needs to be updated.
- (c) Safety requirements must be incorporated and verified at the System Requirements Review as well as in all subsequent design reviews as the Design matures (e.g., ORD, PDR, CDR, etc).
- (d) True life cycle costs, (including disability payments, court ordered awards, engineering change proposals, etc.) are not effectively calculated and factored into risk trades.
- (e) Operational Risk Management, although being utilized, is not fully implemented Navy-wide. Safety waivers are granted at too low a level and there is no mechanism to ensure technical safety support for decision makers. This is particularly true in the shipbuilding industry.
- (f) Current safety metrics do not provide data to properly justify safety actions. There are no leading proactive metrics.
- (g) Not all current and proposed safety data repository systems include identification for design related accident causes. The safety centers of expertise are not collecting or reporting data in a way that will provide effective input into acquisition risk determination. This is particularly true of the Naval Safety Center which does not plan to incorporate indicators

of system-related accident causes into its planned data base upgrade. Chemical safety and noise data managed by Naval Environmental Health Center is somewhat better linked to processes, but long-term health effects remain difficult to link to a particular weapons system.

- (h) The acquisition process is cost driven and safety of personnel is mistakenly regarded as overhead, or more Base Operating Support in nature, vice mission related.. The acquisition process concentrates reduction in direct cost to fleet introduction vice adequately evaluating Life-Cycle-costs
- (i) Accident reporting requirements investigation training are inconsistent and thus result in information an ineffective analysis of underlying accident causes. In turn, root causes remain undetected and are not, therefore used to effectively influence design. This is particularly true of class C and D events.
- (j) Methods for risk management of chemical hazards in acquisition are inconsistent and are typically focused upon environmental regulators while minimizing safety and health considerations. The DoD mandated management approach of National Aerospace Standard NAS 411 is not even widely known to acquisition managers.
- (k) Industry is consistently concerned about the diminution of the importance of safety in the acquisition of weapons systems by the DoD, a trend that they feel de-emphasized the safety of design and operations. Concerns expressed by the Government industry electronics industry G-48 consortium and at the System Safety Conference included degradation of design safety; potential for adverse media attention associated with failures and cost overruns; and erosion of the government contractor defense with resultant increases in liability and costs.
- (l) Defense Acquisition University provides only minimal ESOH training to Program Managers and other members of the acquisition community.
- (m) There is no acquisition career field for ESOH professionals with the exception of system safety engineers who traditionally focus on systems failures rather than control of occupational safety and health risks.
- (n) There continues to be a huge disparity between environmental a safety resourcing. Additionally confusion regarding the difference between the two disciplines to the point where many non-safety personnel regard the meeting of environmental regulatory criteria as sufficient without addressing physical safety issues or even the impact of environmental controls on the safety of operators. CNO N45, currently responsible for both disciplines, has gone so far as to change its title and focus from

Environmental, Safety and Occupational Health Division to the Environmental Readiness Division.

- (o) Despite SECNAV level support for safety in operations, there appears to be little comparable high-level commitment to incorporation of safety into the design process.
- (p) There is inconsistent, or total absence, of Government test and evaluation on weapons support equipment.

2.8.3. RECOMMENDATIONS

1. Challenge the DoD and SECNAV (under RD&A), to mandate external safety review throughout all acquisition processes, including RDT&E. Mandate, also, that all Program Executive Offices and principal Program Managers designate a Principal for Safety for all ACAT I and II acquisition programs.
2. Develop an accountability mechanism, or reporting process, with input from ASN I&E, N7 and N8 considering Total Ownership Cost (spell out). Consider the development of and support for a program standard that addresses future costs as a penalty tax against future liabilities that could be used to defray costs of effort devoted to system safety pursuits . Make it a requirement and let those that cannot meet it petition for relief by providing the justification.
(Note: This addresses the issue of modifying Congressional allocations by including future liability costs as an incremental aspect of program costs similar to other fixed costs. These may be waived only if the program demonstrates control over these future expenses. Similar “user fees” are routinely applied to utilities, administrative support and other necessary central management functions that may be waived or reduced under specified conditions).
2. Establish , in the acquisition life cycle model multiple review and decision points and expert safety managers for integrating safety requirements at those points.
3. Develop an acquisition review board that participates and contributes at all levels of the acquisition process.
5. Monitor implementation of required NAS Standard 411 for systematic management of hazardous material selection criteria.
6. Update the DFAR on materials use restrictions for such materials as, asbestos, mercury and PCB’s to be used in any Navy acquisition.
7. Develop an audit protocol for the Navy’s new, ongoing, or proposed, acquisition programs to help identify which acquisitions are not being addressed from an SOH considerations standpoint.
8. Continue implementing the ASN direction to integrate all safety disciplines, and Safety Centers of Expertise (SAFCEN, NEHC, etc) and provide strong guidance,

- policy, and support. Increase the participation and focus the needed and related resources of NEHC and the Safety Center on the acquisition process with particular emphasis on input for system safety analysis, weapons system development, chemical risk management and physical agent hazards.
9. Request the SECNAV/ASN RDA issue a policy statement for stressing the importance of safety to acquisition risk management, personnel safety, future readiness and cost containment. (A proposed draft is provided).
 10. Document and track true life-cycle-safety costs. Ensure that the Metrics working group incorporates total systems Life-cycle-cost in their charter.
 11. Improve acquisition guidance to the Occupational Safety and Health and Industrial Hygiene Communities through improved training and instructions. Update of the System Safety Instruction (OPNAVINST 5100.24A dated 1984) is urgently needed.
 12. Improve guidance for ORDs and MNSs by updating N45/ ASN RDA 1999 guidance on pollution prevention and logistically relevant environmental, safety and health requirements. (A draft has been developed for review).
 13. Develop and provide education and training for the DoN/USMC acquisition work force to address ESOH requirements throughout the weapon system's life cycle.
 - Develop/update ESOH lesson learned knowledge center for reference/guidance. (Similar to Army's System Safety Lesson Learned Handbook)
 - Maintain the library of ESOH related references.
 14. Develop an acquisition ESOH career field.

2.8.4 BEST PRACTICES

Best Practice efforts were reviewed for NASA, Space and Warfare, British Safety, Electric Boat, Raytheon, FAA, DOT, DOE, Lockheed and Boeing, Army and Air Force. These reviews were accomplished by Internet query due to time constraints. While our findings noted that industry provides many useful tools to improve government processes, it is recognized that industry is ultimately driven by one thing, the bottom line. Government agencies including the military, while driven to fiscal responsibility and taxpayer accountability, must uphold a higher standard. In addition, acquisition policies designed to improve industry performance are not readily shared outside the company. In the examination of best practices, other government agencies and sister-services provided the best examples of useful practices that can serve the Navy's safety program. The Army, Air Force, FAA and NASA all provide good tools and program requirements and practices that can assist the Navy in improving its overall safety programs.

