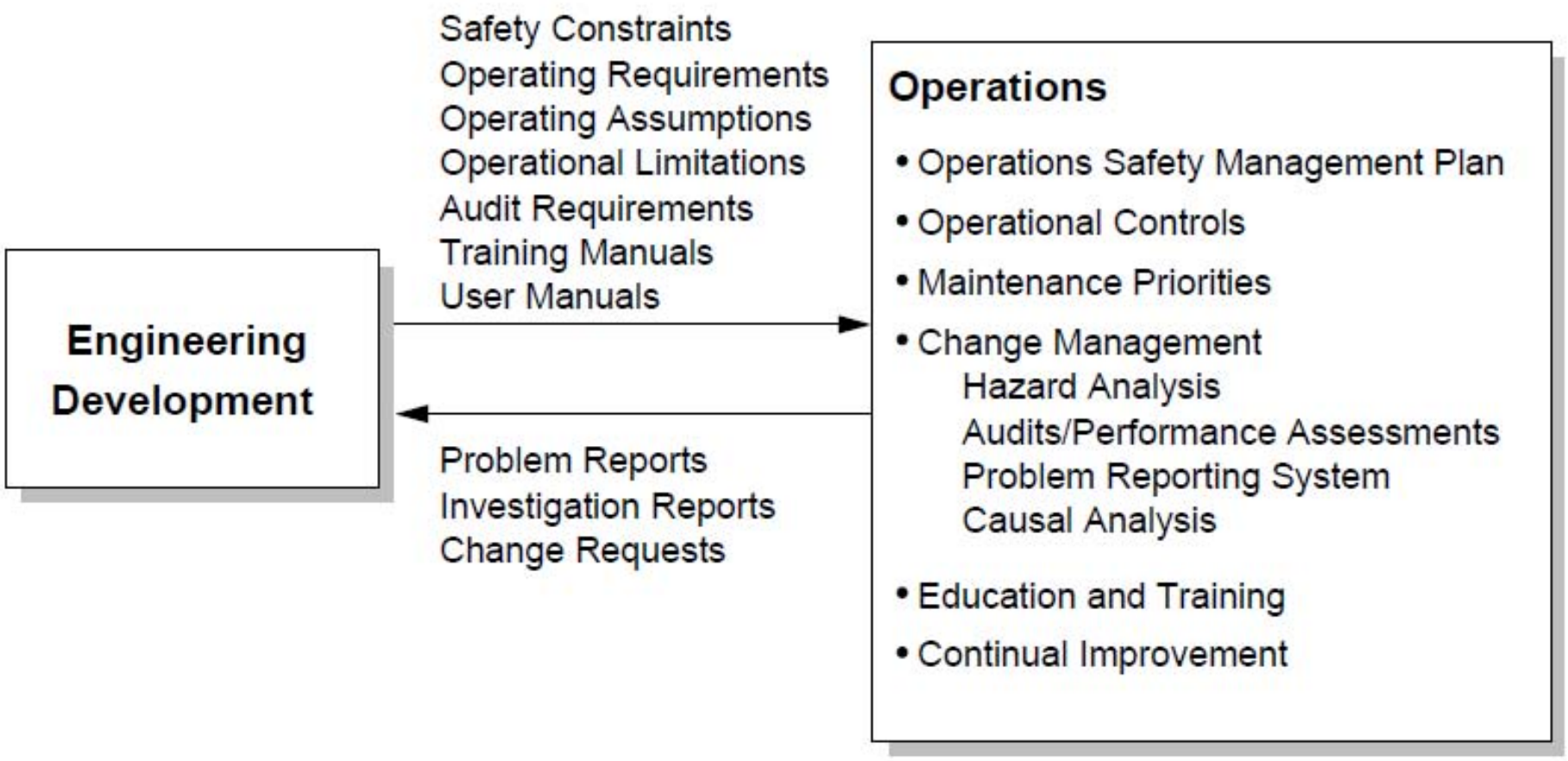
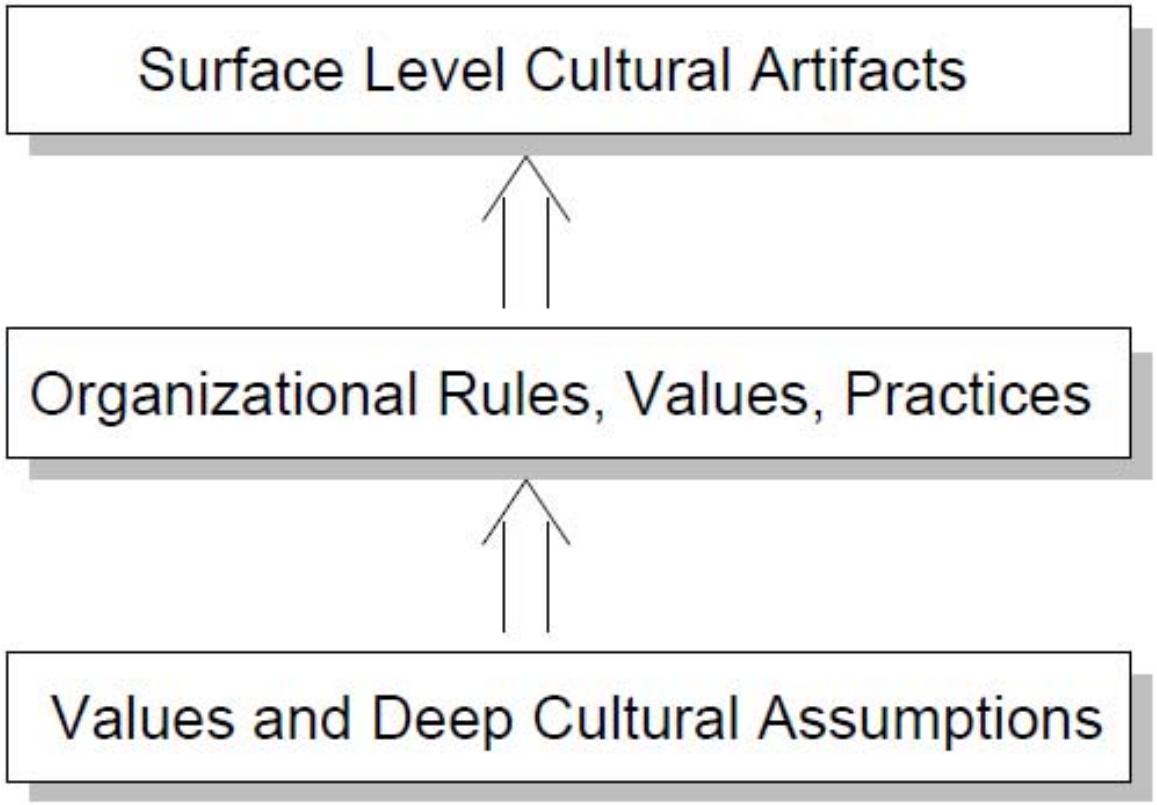
Social Systems and Operations

STPA on Social Systems

- NASA Shuttle management structure
- Effect of policy changes following the Vioxx events
- Accident analysis and system redesign (PCA)


Safety Constraints
Operating Requirements
Operating Assumptions
Operational Limitations
Audit Requirements
Training Manuals
User Manuals
Engineering Development
Problem Reports
Investigation Reports
Change Requests
Operations
• Operations Safety Management Plan
• Operational Controls
• Maintenance Priorities
• Change Management
Hazard Analysis
Audits/Performance Assessments
Problem Reporting System
Causal Analysis
• Education and Training
• Continual Improvement

Three Levels of Organizational Culture: Edgar Shein



(Organizational values underlying decision making)

Examples of Positive Cultural Values and Assumptions

- Incidents and accidents are valued as an important window into systems that are not functioning as they should – triggering causal analysis and improvement actions.
  - Safety information is surfaced without fear
  - Safety analysis is conducted without blame
- Safety commitment is valued

Example Cultural Values and Assumptions (2)

- There is a feeling of openness and honesty, where everyone's voice is valued. Employees feel managers are listening.
  - Trust among all parties (hard to establish, easy to break).
  - Employees feel psychologically safe about reporting concerns
  - Employees believe that managers can be trusted to hear their concerns and will take appropriate action
  - Managers believe employees are worth listening to and are worthy of respect.

Safety Culture

- Safety culture is a subset of culture that reflects general attitude and approaches to safety and risk management
- Trying to change culture without changing environment in which it is embedded is doomed to failure
- Simply changing organizational structures may lower risk over short term, but superficial fixes that do not address the set of shared values and social norms are likely to be undone over time.
- “Culture of denial”
  - Risk assessment unrealistic and credible risks and warnings are dismissed without appropriate investigation

Culture of Denial Examples

- “Our accident rates are going down”
  - Look at worker injury rates: personal or occupational safety vs. system or process safety
  - Choose statistics that give best result
- “Accidents are the price of productivity. A dangerous domain” (explosives)
- “Mines: Everyone has lots of safety violations”

Leadership is Key to Changing Culture

- Safety requires passionate and effective leadership
- Tone is set at the top of the organization
- Not just sloganeering but real commitment
- Setting priorities
  - Adequate resources assigned
  - A designated, high-ranking leader
- Safety and productivity are not conflicting if take a long-term view

Just Culture

Basic Principle: An organization can benefit more by learning from mistakes than by punishing people who make them.

- Reporting errors and suggesting improvements is normal, expected, and without jeopardy.
- Mistake or incident seen not as a failure but a chance to learn
- People are participants in change and improvement
- Information provided in good faith not used against people who report it.

Example Operational Safety Philosophy (1) (Colonial Pipeline)

- All injuries and accidents are preventable.
- We will not compromise safety to achieve any business objective.
- Leaders are accountable for the safety of all employees, contractors, and the public.
- Each employee has primary responsibility for his/her safety and the safety of others.
- Effective communication and the sharing of information is essential to achieving an accident-free workplace.
- Employees and contractor personnel will be properly trained to perform their work safely.

Example Operational Safety Philosophy (2) (Colonial Pipeline)

- Exposure to workplace hazards shall be minimized and/or safeguarded.
- We will empower and encourage all employees and contractors to stop, correct and report any unsafe condition.
- Each employee will be evaluated on his/her performance and contribution to our safety efforts.
- We will design, construct, operate and maintain facilities and pipelines with safety in mind.
- We believe preventing accidents is good business.

Safety Regulation Approaches

- Prescriptive
  - Product
    - Specific design features (e.g., electrical codes)
    - General design features (e.g., fail-safe, protection system)
  - Process: process to be followed in
    - Designing and implementing the system
    - Assuring safety
- Goal or Performance-Based

MIL-STD-882

- First version in 1969: has gone through various incarnations
- Includes both technical and management aspects

System safety covers the entire spectrum of risk management. It goes beyond the hardware and associated procedures of system safety engineering. It involves: attitudes and motivation of designers and production people, employee/management rapport, the relation of industrial associations among themselves and with government, human factors in supervision and quality control, documentation on the interfaces of industrial and public safety with design and operations, the interest and attitudes of top management, the effects of the legal system on accident investigations and exchange of information, the certification of critical workers, political considerations, resources, public sentiment and many other non-technical but vital influences on the attainment of an acceptable level of risk control. These non-technical aspects of system safety cannot be ignored.

Jerome Lederer, 1968

Mil-STD-882 (2)

- Purpose:

  "Provide uniform requirements for developing and implementing a system safety program of sufficient comprehensiveness to identify the hazards of a system and to impose design requirements and management controls to prevent mishaps."

- Applies to entire lifecycle
- Specifies *what* but not *how*
- Tailorable: written as a set of tasks

Safety Program Objectives

The safety program shall specify a systematic approach to make sure that:

- Safety, consistent with mission requirements, is designed into the system in a timely, cost-effective manner.
- Hazards associated with each system are identified, tracked, evaluated, and eliminated, or the associated risk reduced to a level acceptable to the MA [managing authority] throughout the entire life-cycle of a system. Risk shall be described in risk assessment terms [the risk matrix]
- Historical safety data, including lessons learned from other systems, are considered and used.
- Minimum risk is sought in accepting and using new technology, materials, and designs; and new production, test, and operational techniques.

Safety Program Objectives (2)

- Actions taken to eliminate hazards or reduce level acceptable to the MA are documented
- Retrofit actions required to improve safety are minimized through the timely inclusion of safety features during research, technology development for, and acquisition of a system.
- Changes in design, configuration, or mission requirements are accomplished in a manner that maintains a risk level acceptable to the MA.
- Consideration is given early in the life cycle to safety and ease of disposal (including ordnance disposal) and demilitarization of any hazardous materials associated with the system. Actions should be taken to minimize the use of hazardous materials and, therefore, minimize the risks and life-cycle costs associated with their use.
- Significant safety data are documented as “lessons learned” and are submitted to data banks or as proposed changes to applicable design handbooks and specifications.

Task 100: Program Management and Control

101: System Safety Program

102: System Safety Program Plan (components of the plan)

103: Integration/Management of Associate Contractors, Subcontractors, and Architect and Engineering Firms

104: System Safety Program Reviews and Audits

105: System Safety Working Group Support

106: Hazard Tracking and Risk Resolution

107: System Safety Progress Summary

System Safety Program Plan (102)

- Program scope and objectives
- System safety organization
- System safety program milestones
- General system safety requirements and criteria
- Hazard analysis
- System safety data
- Safety verification
- Audit program
- Training
- Incident reporting
- System safety interfaces (with other parts of the program)

Task 200: Design and Integration

201: Preliminary Hazard List

202: Preliminary Hazard Analysis

203: Safety Requirements/Criteria Analysis

204: Subsystem Hazard Analysis

205: System Hazard Analysis

206: Operating and Support Hazard Analysis

Task 300: Design Evaluation

301: Safety Assessment

302: Test and Evaluation Safety

303: Safety Evaluation of Engineering Change Proposals, Specification Change Notices, Software Problem Reports, and Requests for Deviation/Waiver

Task 301: Safety Assessment

Purpose: To perform and document a comprehensive evaluation of the mishap risk being assumed prior to test or operation of a system.

Contents:

- The safety criteria and methodology used to classify and rank hazards, plus any assumptions on which the criteria or methodologies were based or derived including the definition of acceptable risk as specified by the MA
- The results of analyses and tests performed to identify hazards inherent in the system, including
  - Those hazards that still have a residual risk, and the actions that have been taken to reduce the risk to a level contractually specified as acceptable.
  - Results of tests conducted to validate safety criteria, requirements, and analyses

Task 301: Safety Assessment (2)

- The results of the safety program efforts. Include a list of all significant hazards along with specific safety recommendations or precautions required to ensure safety of personnel, property, or the environment.
- Any hazardous material generated by or used in the system, including
  - Identification of material type, quantity, and potential hazards
  - Safety precautions and procedures necessary during use, packaging, handling, storage, transportation, and disposal.
  - … (some detailed requirements for space vehicles, like orbital debris)

- Concludes with a signed statement that all identified hazards have been eliminated, or their associated risks controlled to levels contractually specified as acceptable, and that the system is ready to test or operate or proceed to next acquisition phase.
  - Includes recommendations applicable to hazards at interface of his system to other systems.

Task 400: Compliance and Verification

- Safety Verification
- Safety Compliance Assessment
- Explosive Hazard Classification and Characteristics Data
- Explosive Ordnance Disposal Data

Homework Questions

- Does system-level analysis "excuse" the operator's actions? Does the just culture movement promote irresponsible behavior?
- Discuss the roles of quantitative vs. qualitative information in engineering.
- What type of regulation exists in your industry? Is it effective? If there is none, should there be?

Effective Safety Management Systems

- Process safety is integrated into the dominant culture, not a separate sub-culture
- Safety is integrated into line operations: a mixture of top-down re-engineering and bottom-up process improvement
- Individuals have required knowledge, skills, and ability
- Organization has clearly articulated safety vision, values and procedures, shared among stakeholders
- Tensions between safety priorities and other system priorities are addressed through a constructive, negotiated process.
- Key stakeholders (e.g., unions) have full partnership roles and responsibilities regarding system safety
- Passionate, effective leadership at all levels committed to safety as a high priority for the organization

Safety Management System (2)

- Early warning systems for migration toward states of high risk are established and effective
- Effective communication channels exist for disseminating safety information
- Visibility of state of safety at all levels through appropriate feedback
- Results of operating experience, process hazard analyses, audits, near misses, or accident investigations are used to improve process operations and process safety management system.
- Deficiencies found during assessments, audits, inspections and incident investigation are addressed promptly and tracked to completion

Are Accidents Inevitable?

SUBSAFE (An Example Process Safety Program and Culture)

On April 10, 1963, while engaged in a deep test dive, approximately 200 miles off the northeastern coast of the United States, the *U.S.S. Thresher,* (SSN-593), was lost at sea with all persons aboard - 112 naval personnel and 17 civilians.

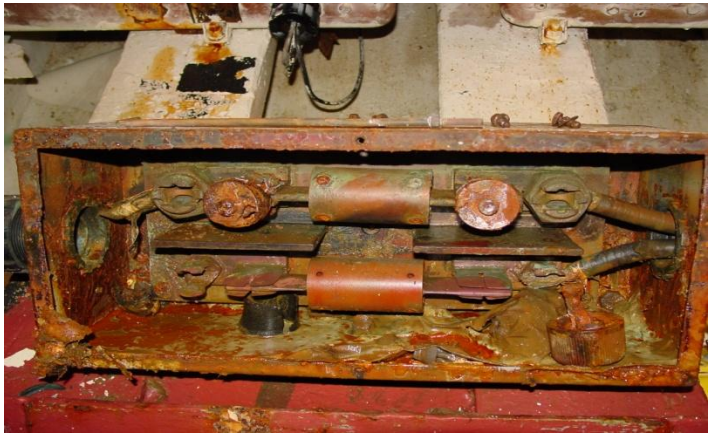
Image courtesy of US Naval History and Heritage Command.

Loss Events

Flooding in the engine room

Unable to secure from flooding

Spray on electrical switchboards



Loss of propulsion power

Unable to blow ballast tanks

Our investigations concluded:

- Failure of a deficient silver-braze joint led to flooding in the engine room
- The crew was unable to access vital equipment to stop the flooding
- Saltwater spray on electrical components caused short circuits, reactor shutdown, and loss of propulsion
- When the crew attempted to blow Main Ballast Tanks, excessive moisture in the air system froze, causing a loss of air flow

Of note:

- THRESHER had about 3000 silver-brazed pipe joints exposed to full submergence pressure
- During her last shipyard maintenance period, 145 of these joints were inspected on a not-to-delay vessel basis using a then new technique call Ultrasonic testing
- 14% of the 145 joints showed sub-standard joint integrity
- Extrapolating these test results to the entire population of 3000 silver-brazed joints indicates that possibly more than 400 joints on THRESHER could have been sub-standard.

Did we determine the full scope of the problem? What rationale did we use to talk ourselves into letting the ship go to sea in this condition?

Technical Deficiencies

- Deballasting System
- Access to Vital Equipment
- Piping Joints
- Piping Flexible Connections
- Aluminum Bronze
- Fasteners
- Diving Plane Reliability

Needed Design Improvements

- Trim & Drain System
  - Minimize exposure to submergence pressure
- Freshwater Cooling System
  - Utilize freshwater cooling systems instead of seawater where possible
- Protection for Electrical Switchboards
  - Modify enclosures to prevent seawater spray from entering
- Remote Flood Closure System
  - Quickly close critical sea valves
- Emergency Main Ballast Tank (EMBT) Blow System
  - Quickly achieve positive buoyancy

Systemic Factors

- Deficient **Specifications**
- Deficient **Shipbuilding and Maintenance Practices**
- Incomplete or Non-Existent **Records**
  - Work Accomplished
  - Critical Materials
  - Critical Processes
- Deficient **Operational Procedures**

SUBSAFE Program Success

1915 – 1963 16 submarines lost to non-combat causes

1915: USS F-4 (SS-23)
1917: USS F-4 (SS-20)
1920: USS H-1 (SS-28)
USS S-5 (SS-110)
1923: USS O-5 (SS-66)
1926: USS S-51 (SS-162)
1927: USS S-4 (SS-109)
1939: USS SQUALUS (SS-192)
1941: USS O-9 (SS-70)
1942: USS S-26 (SS-131)
USS R-19 (SS-96)
1943: USS R-12 (SS-89)
1944: USS S-28 (SS-133)
1949: USS COCHINO (SS-345)
1958: USS STICKLEBACK (SS-415)
1963: **USS THRESHER (SSN-593)**

Average of 1 loss every three years (473 lives lost)

SUBSAFE Program inception after THRESHER was lost

1963 - Present

1 submarine lost to non-combat causes

1968: USS SCORPION

– SCORPION was **not** SUBSAFE certified

NO SUBSAFE-CERTIFIED SUBMARINE HAS EVER BEEN LOST

SUBSAFE Goals

- Hull integrity to preclude flooding
- Operability and integrity of critical systems to control and recover from a flooding casualty

Other aspects of process safety and safety engineering

- Mission assurance
- Fire safety
- Weapons safety
- Occupation health and safety
- Nuclear reactor systems safety

are handled separately

SUBSAFE Requirements

- Administrative
- Organizational
- Technical
- Unique Design
- Material Control
- Fabrication
- Testing
- Work Control
- Audits
- Certification

⇨ SUBSAFE requirements permeate the entire submarine community.

⇨ Invoked in Design, Construction, Operations and Maintenance

⇨ Renewed every 10 years

Risk Management Fundamentals

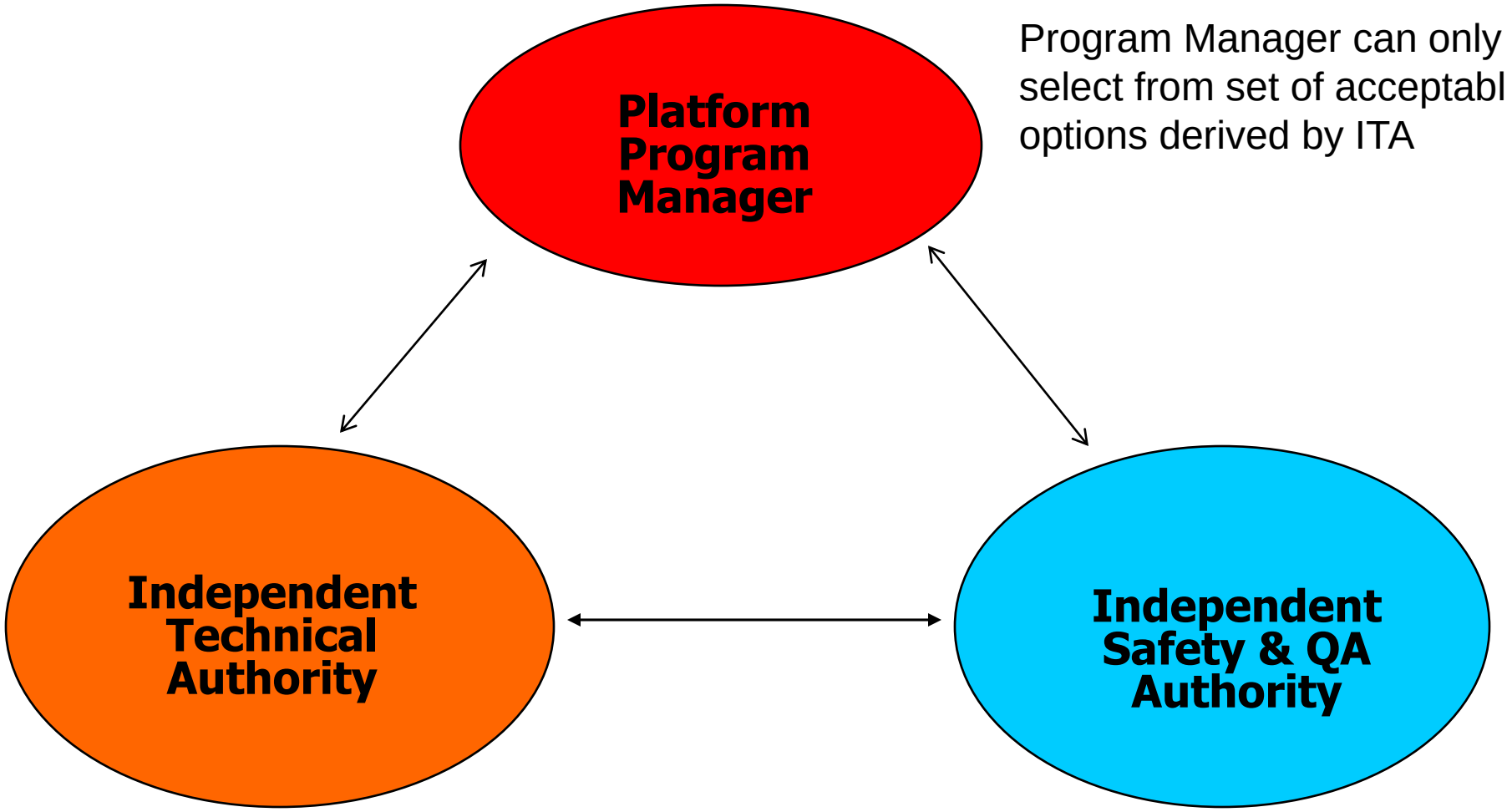
- Work Discipline
  - Knowledge of and Compliance With Requirements
- Material Control
  - Correct Material Installed and Installed Correctly
- Documentation
  - Design Products (Specs, Drawings, Maintenance Standards, System Diagrams, etc.)
  - Objective Quality Evidence (OQE)
- Compliance Verification
  - Inspections, Surveillance, Technical Reviews, Audits

    “Trust everybody but check up”
- Learning from inspections, audits, non-conformances

Cultural Risk Management Approach

- Questioning Attitude
- Critical Self Evaluation
- Lessons learned and continuous improvement
- Continuous Training
- Separation of Powers

SUBSAFE Separation of Powers



Program Manager can only select from set of acceptable options derived by ITA

Technical Authority

- What is Technical Authority?
  - "The exercise of Technical Authority is a process that establishes and assures adherence to technical standards and policy…a range of technically acceptable alternatives with risk and value assessments…."
- Responsibilities of Technical Authority
  - Setting and enforcing technical standards
  - Maintaining subject matter expertise
  - Assuring safe and reliable operations
  - Ensuring effective and efficient systems engineering
  - Making unbiased independent technical decisions
  - Providing stewardship of technical and engineering capabilities
  - Being held accountable

Certification

- Focuses on critical structures, systems, components
- Strictly based on OQE
- Goal: Provide maximum reasonable assurance through
  - Initial SUBSAFE certification
  - Maintaining certification throughout sub's life
- Types
  - Design certification
  - Material certification
  - Fabrication certification
  - Testing certification

Objective Quality Evidence (OQE)

- Certification is strictly based on OQE.
  - OQE: Any *statement of fact*, either quantitative or qualitative, pertaining to the quality of a product or service based on observations, measurements, or tests *that can be verified*.
  - OQE provides *evidence* that *deliberate steps were taken* to comply with requirements.
  - Founded on the **integrity** and **responsibility** of individuals.

SUBSAFE Audits

- Multi-layered approach
  - Contractor/Shipyard responsibilities
    - Inspections, Surveillances, Document Reviews, Audits
  - Local government oversight authority responsibilities
    - Inspections, Surveillances, Document Reviews, Audits
  - Headquarters responsibilities
    - Document Reviews, Audits
- Multi-faceted approach
  - Ship Specific Audits
  - Facility Functional Audits
    - Activity (e.g., shipyard) specific review (policies, procedures, practices)
    - Verify organizational compliance with SUBSAFE program requirements

Audit Philosophy

- Focus on audits as a constructive, learning experience
- Objective is to make our subs safer
- A team effort
  - Audit team plus facility personnel
  - Continuous communication
  - Full understanding of identified problems
- Audit is a peer review: 80% from other SUBSAFE facilities
- Assume policies, procedures, and practices are in compliance (audit confirms compliance)

Lessons Learned

- Clear ground rules for audits must be established, communicated, and adhered to
- The best audit teams are made up of personnel who have a “day job” working in the business.
- The compliance verification organization must be an equal with the program managers and the technical authority
- Headquarters must be willing to accept and resolve audit findings just like any other member of the community
- You cannot ‟audit in″ requirements

Trouble Reports/Critiques

- Trouble reports/critiques are used to report significant problems to NAVSEA.
- Lessons learned are integral to submarine safety.
- Distributed to all SUBSAFE responsible activities.

Challenges

- Ignorance

  (do not know)

- Arrogance

  (pride, self-importance, conceit, or assumption of intellectual superiority and presumption of knowledge that is not supported by fact)

- Complacency

  (satisfaction with one's accomplishments accompanied by a lack of awareness of actual dangers or deficiencies)

"A constant struggle every day"

"Safety requires passionate and effective leadership"

Continuous Training

- Annual training for everyone
- Yearly Headquarters meeting on Thresher anniversary
- Annual refresher at all contractors
- Content
  - Thresher video (reminder of Thresher loss)
  - Overview of the SUBSAFE program (their responsibilities)
  - Recent lessons learned and deficiency trends encountered throughout the previous years

Continuous Training

- Goals
  - Serve as a reminder of the consequences of complacency in one's job.
  - Emphasize the need to proactively correct and prevent problems.
  - Stress the need to adhere to the program fundamentals
  - Convey management support for program
- Level of knowledge assessments are performed during audits of organizations that perform SUBSAFE work (continuous improvement of and feedback to training program)

SSN 711 – A Success Story

- On 8 January 2005 at 1142 Guam time, the USS SAN FRANCISCO (SSN 711) crashed head-on into an underwater sea mountain.
- Major damage occurred to the front of the ship.
- Many crew members injured. One died.
- The damaged ship was able to emergency blow to the surface and make it to Guam under its own power.


Image courtesy of the US Naval History and Heritage Command.

SSN 711 Functioned as Designed

- No Breach of the Pressure Hull
- Nuclear Reactor Remained On Line
- Emergency Main Ballast Tank Blow System Functioned as Intended
- Control Surfaces Functioned Properly
- The damaged ship was able to surface and make it to Guam under its own power

Some Reasons for SUBSAFE Success

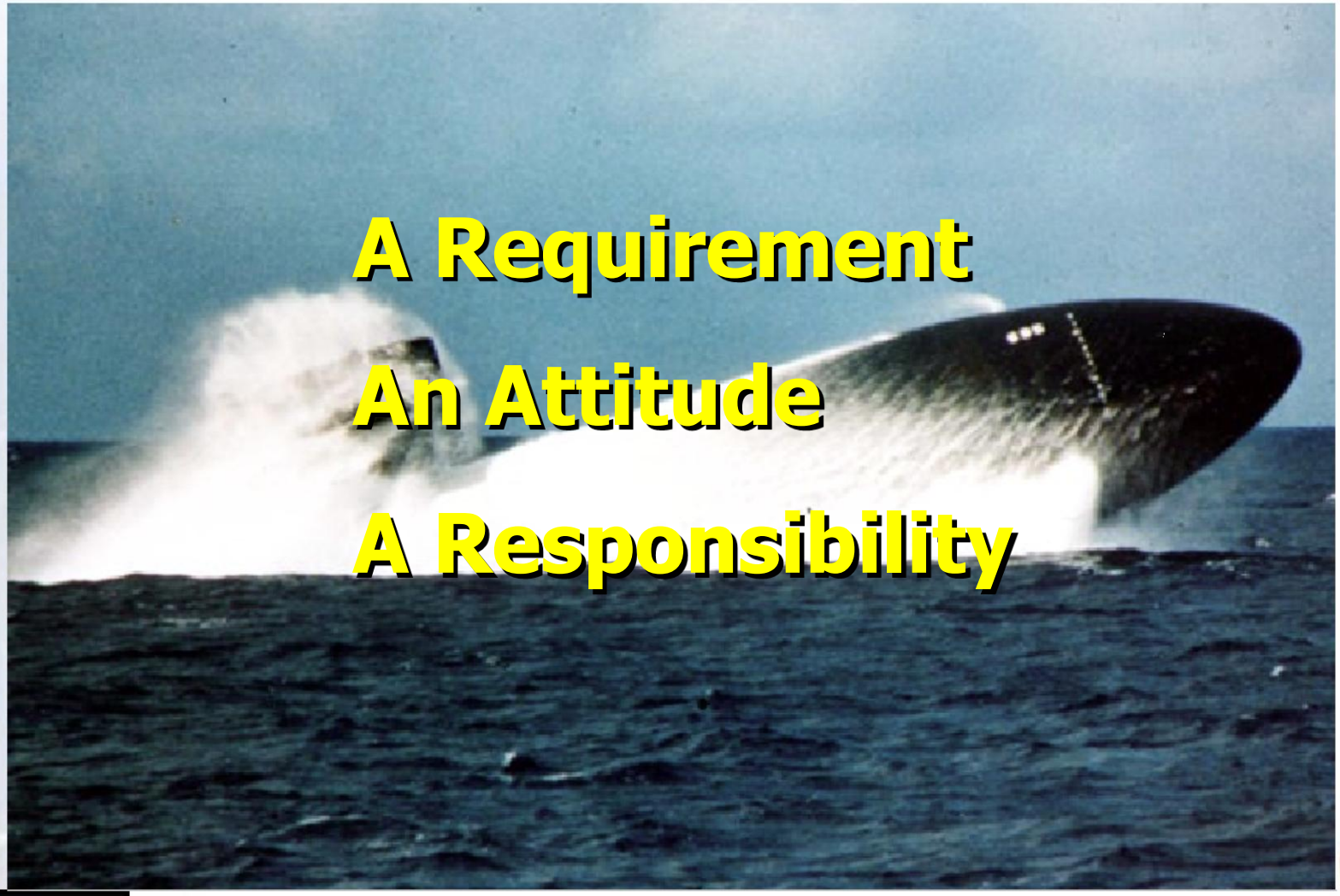
- Education (not just training), yearly reminders of past, continuous improvement and input
- Redo requirements every 10 years

  Renew program and commitment
- Separation of power (PM only chooses from acceptable solutions)
- Rigor and technical compliance
- Capture what do and why do it
- Audit philosophy and Objective Quality Evidence

Some Reasons for Success (2)

- Written procedures; not personality driven
- Not afraid to say “no”
- Anytime something does not conform with specification, have 24 hours to find root cause and report to head of fleet (Admiral)
- Accountability accompanies responsibility
  - Stress personal integrity and personal responsibility
- Shared responsibility
- Vigilance – fight complacency

SUBSAFE!



Discussion

Why do you think SUBSAFE has been so successful?

Could such a program be practical in a profit-making, competitive industry?

"Final Exam" question: Have you changed your opinions about safety engineering in this class? Confirmed the old ones? What do you think is the most important “learning” that you are coming away from the class with?

16.863J / ESD.863J System Safety

Spring 2011