8^{th} Annual Systems Engineering Conference

Sponsored by the

National Defense Industrial Association

San Diego CA

October 2005

Integrating MIL-STD-882 System Safety Products Into The Concurrent Engineering Approach To System Design, Build, Test, And Delivery Of Submarine Systems At Electric Boat.

Ricky Milnarik

Introduction

Electric Boat has been building submarines for the U. S. Navy for over 100 years.

In 1900 Electric Boat delivered the U. S. Navy's first submarine, the USS Holland.

Introduction

Subsequent to the USS Holland, Electric Boat has delivered over 270 submarines to the U.S. Navy.

In October 2004 the USS VIRGINIA, the first ship in a new class of fast attack submarines, was delivered the U. S. Navy.

Introduction

The VIRGINIA Class Submarine is the first class of submarine built at Electric Boat that uses the Integrated Product and Process Development (IPPD) process to conduct, manage and status the ship design, ship construction and life cycle support.

The IPPD process is a dynamic concurrent engineering concept that includes integration of system safety engineers into design/ build teams (DBT).

Introduction

Before the IPPD process was implemented a serial approach to submarine design-to-construction was taken.

Upon Navy approval of the drawings a full scale wooden mockup of the lead ship was built and maintained.

The dynamics of the design/build team concept is made possible through the use of the Computer Aided Three-Dimensional Interactive Application (CATIA) software design tool to develop electronic mockups in place of building wooden mockups.

Introduction

The design/build team concept also necessitated tailoring how traditional MIL-STD-882 system safety program products were developed and used to provide a complete evaluation of the system(s) under development.

Integrated Product and Process Development

The basis for IPPD is the design-to-build approach.

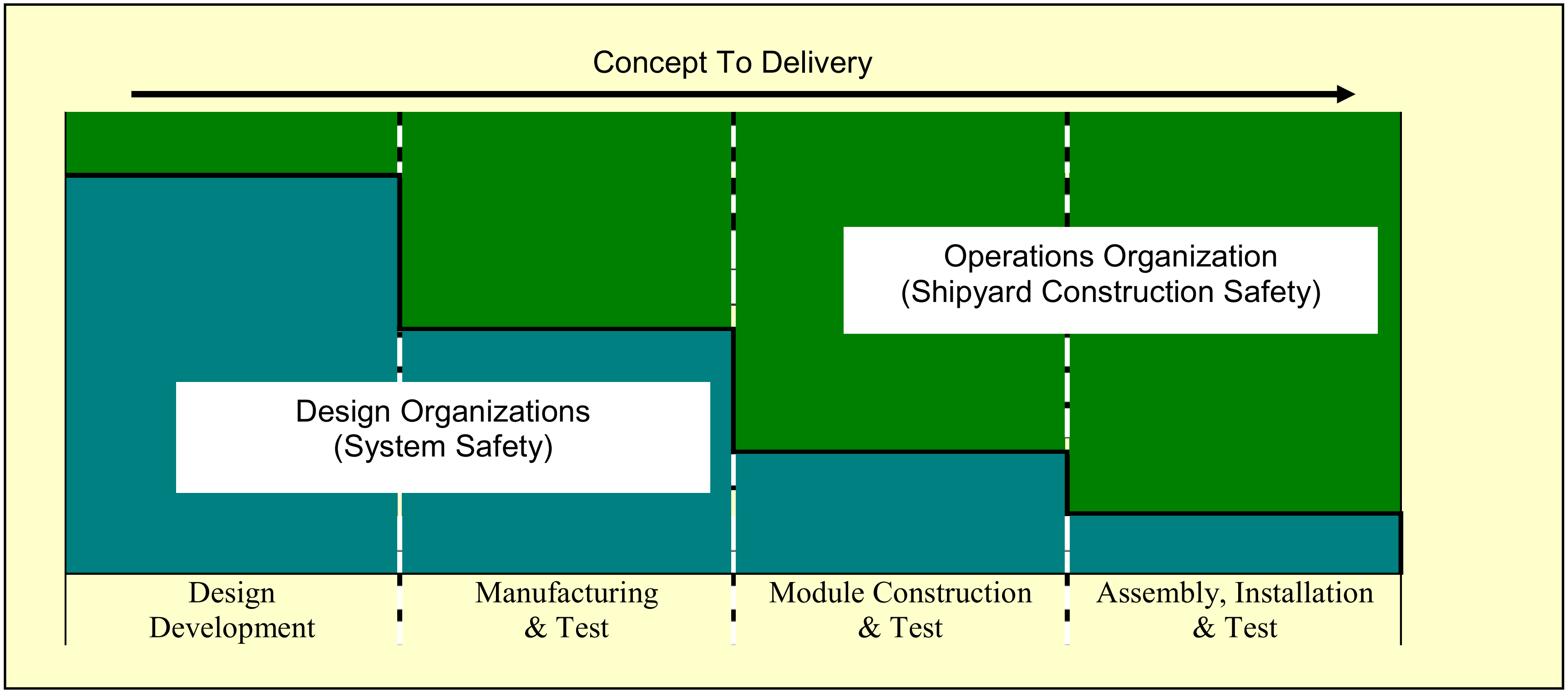
This methodology consists of activity-based product management and concurrent engineering DBTs.

Team assignments are structured in accordance with program development and manufacturing needs.

Integrated Product and Process Development

Ensures that all requirements of conceptual engineering, design, fabrication, assembly, and test, that support system safety are evaluated and analyzed early in the acqusition process.

Integrated Product and Process Development



IPPD Team Staffing

Design / Build Teams

Design Build Teams consist of:

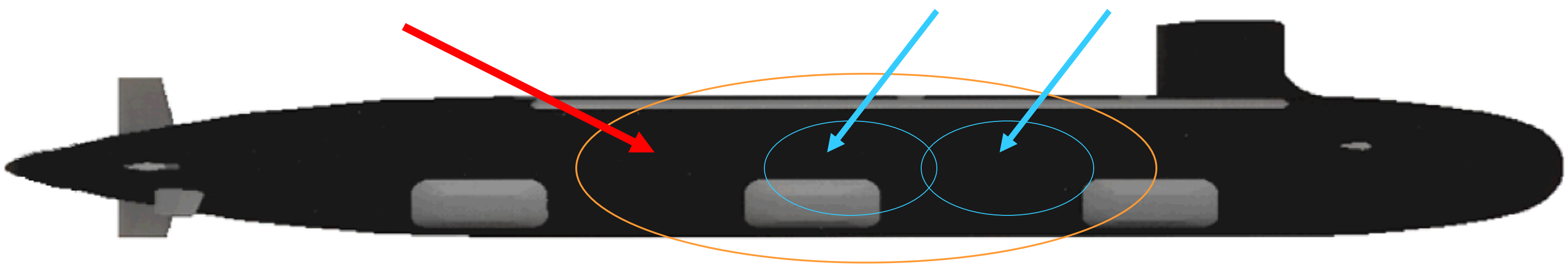
- Program Management Teams
- Functional Area Teams
- System Integration Teams (SIT)

Design / Build Teams

DBT functional managers / technical leaders have direct management and control of their specific functional areas.

FUNCTIONAL AREA TEAM

SYSTEM INTEGRATION TEAMS



Design / Build Teams

DBTs also manage both technology and program development and exercise authority in ensuring component and system integrity via technical design reviews and approval circuits.

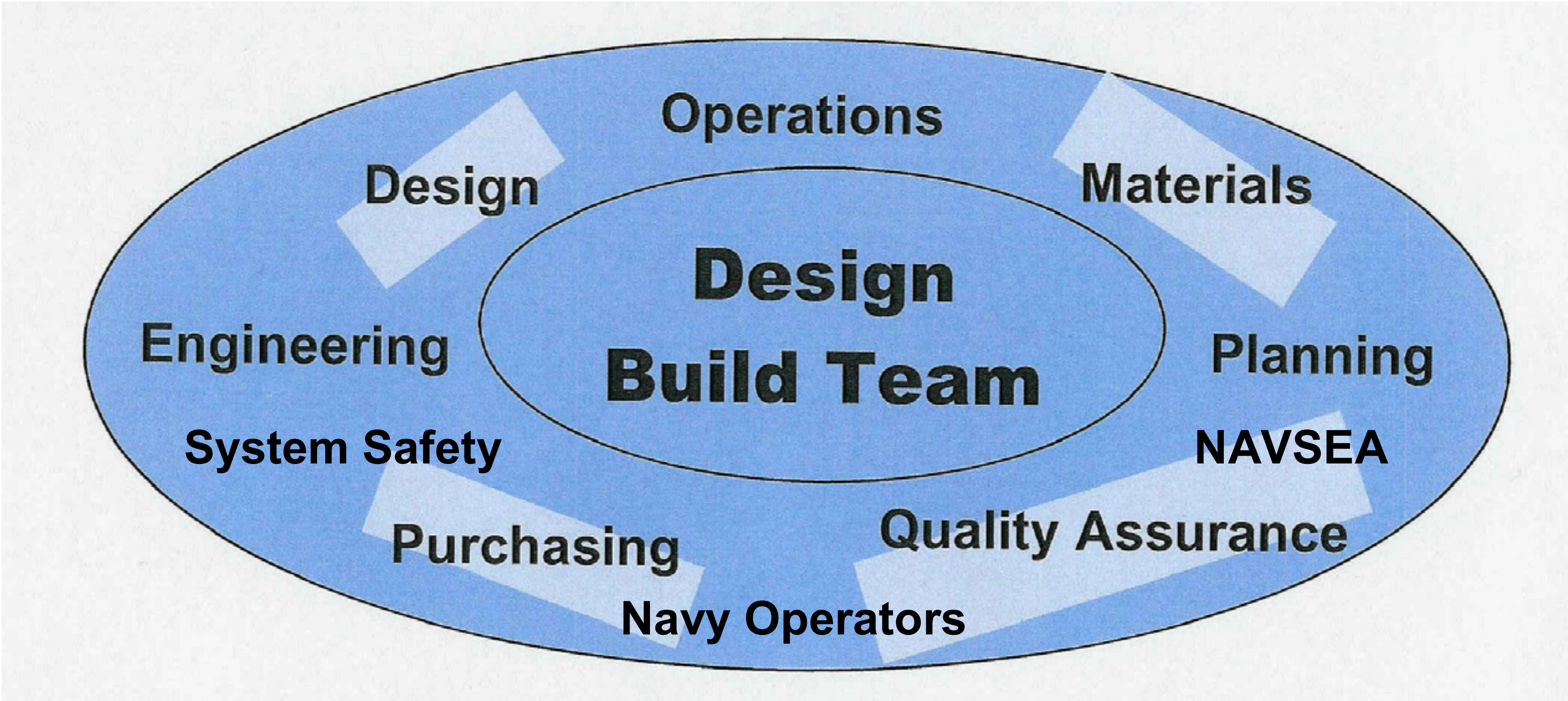
This responsibility broadens the awareness and involvement of team members and creates a sense of ownership of the design efforts and system safety products.

Design / Build Teams

DBTs are made up of representatives from Electric Boat, government suppliers, government laboratory personnel, Navy operators, independent government review/certification board members (e. g. Weapon System Explosives Safety Review Board, SUBSAFE , Deep Submergence System (diver safety) etc.) and teaming shipyards.

Design / Build Teams

A typical DBT makeup is shown below



System Integration Teams

System Integration Teams (SITs) develop, integrate, and optimize systems in the ship and prepare technical deliverables by:

- Developing and evaluating system concepts and new components, conducting trade-off studies, developing system diagrams, class drawings, component specifications etc.
- Performing safety analyses on new and significantly modified legacy ship systems and components in accordance with the System Safety Program Plan.

System Integration Teams

Establishing technical interfaces with government agencies, laboratories, and other contractors.

Integrating discipline-specific individuals and individuals with appropriate specialty expertise (e.g. system safety engineers, production, finance, integrated logistics support environmental compliance etc.).

System Integration Teams

Typical Submarine Systems

Torpedo Ejection	Trim and Drain	Propulsion Plant
Vertical Launch	Low Pressure Air	High Pressure Air
Weapons Handling	Main Hydraulic	Main Seawater
Communications (Radio)	HVAC	Ships Entertainment
Combat Control Subsystem	External Hydraulic	AC Power/Interior
Combat Launch Control	Ship Control	Masts and Antennas
Navigation	Fresh Water	Atmosphere Monitoring
Sonar	AC Electrical Power	Interior Communication
Total Ship Monitoring	DC Electrical Power	Auxiliary Seawater
Non-Tactical Data Processing	Lighting	Main Ballast Tank Low
Escape and Rescue	Fire Fighting	Pressure Blow

System Safety Process

Tailoring of the system safety process centered around:

- Formalized SIT meetings.
- Conduct of safety hazard analyses as a team product.
- Use of CATIA for safety hazard analyses and Human Systems Integration (HSI) into design products.

System Safety Process

SIT Meetings

Since the SITs contain all the key players and decision makers for the system under development. Each SIT meeting:

- doubles as a safety working group meeting
- documents system and safety design decisions
- documents unresolved issues and assigns action items
- is documented on official minutes to ensure continuity

System Safety Process

Safety Hazard Analyses

Traditional MIL-STD-882 system safety tasks were used to identify potential hazards.

- Preliminary Hazard Analyses
- Safety Requirements Analyses
- Software Analyses
- Subsystem Hazard Analyses
- System Hazard Analyses
- Operating and Support Hazard Analyses

System Safety Process

Safety Hazard Analyses (cont'd)

Because of the dynamics of the DBT process it was decided that updating previously completed hazard analyses, when additional information became available, was not feasible.

Instead each completed hazard analysis portrayed a snap shot in time of the system under evaluation.

System Safety Process

Safety Hazard Analyses (cont'd)

Each subsequent hazard analysis built upon the previous analysis conducted.

Significant design changes or identification of new hazards that came up between hazard analyses were documented on an Analysis Completion Summary (ACS) Report for continuity.

System Safety Process

ANALYSIS COMPLETION SUMMARY

System: ______________ Cognizant Engineer: ______________

Date Initiated: __________ Date Completed: ______________

Enclosures:

Analysis Summary:

SAMPLE

SAFETY ANALYSIS WORKSHEETS (attached)

1. ____________________ 2. ____________________

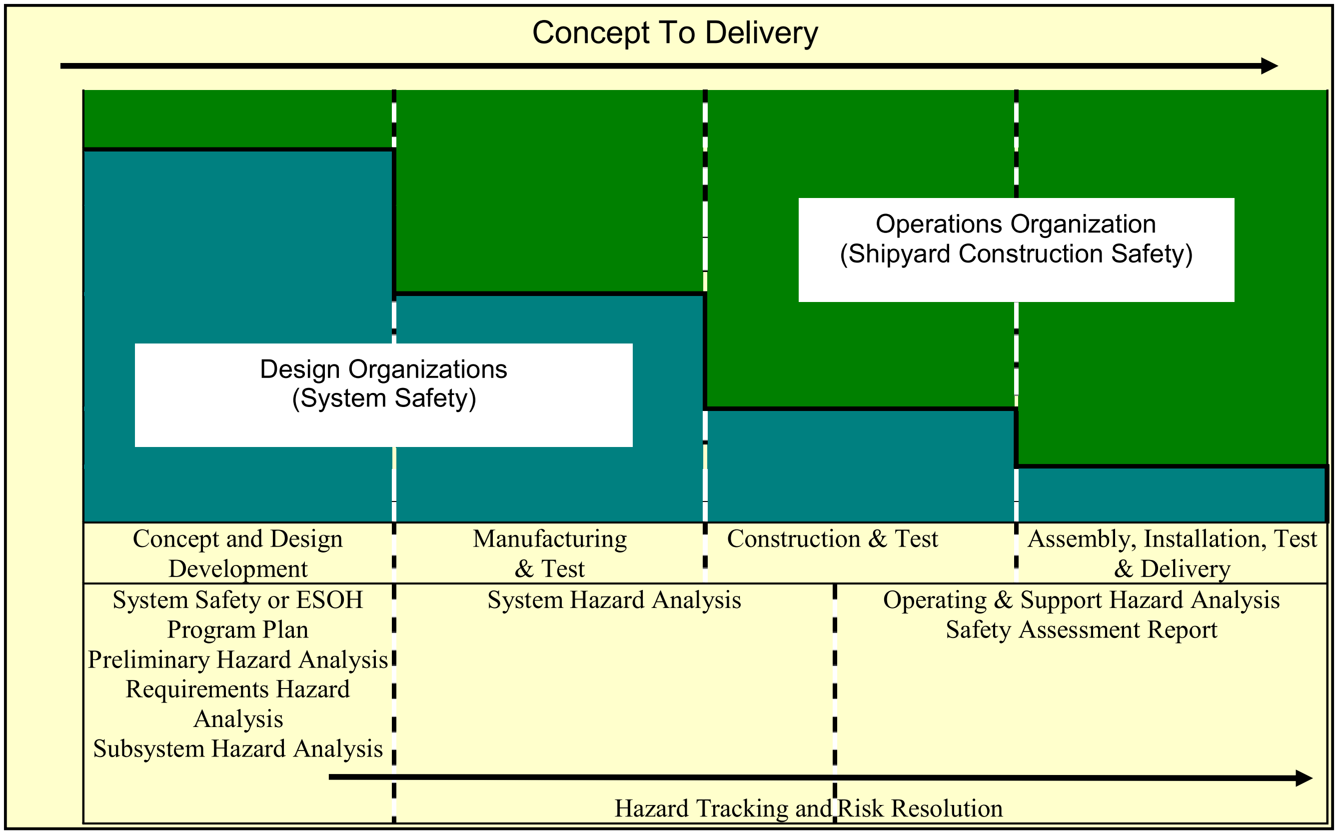
3. ____________________ 4. ____________________

Safety Engineer: ________________________________

Team Leader: ________________________________

System Safety Process

Safety Hazard Analyses (cont'd)



Design Development and System Safety Products

System Safety Process

Safety Hazard Analyses (cont'd)

Provide System Safety Objective Quality Evidence for the systems under development:

- Completed safety hazard analyses
  - Analysis Completion Summary Reports
- SIT meeting minutes
- Program design review findings
- Independent government review board findings
  - Weapon System Explosives Safety Review Board
- Hazard closure forms

System Safety Process

CATIA Program

Electronic design data created in CATIA is controlled and stored in the CATIA Data Manager as the central repository that supports the various elements of the IPPD process.

CATIA displays were projected on screens in Electronic Visualization Simulation (EVS) rooms during SIT meetings allowing SIT members to view the latest system design and arrangements.

System Safety Process

CATIA Program (cont'd)

Examples of HSI efforts through the use of CATIA were:

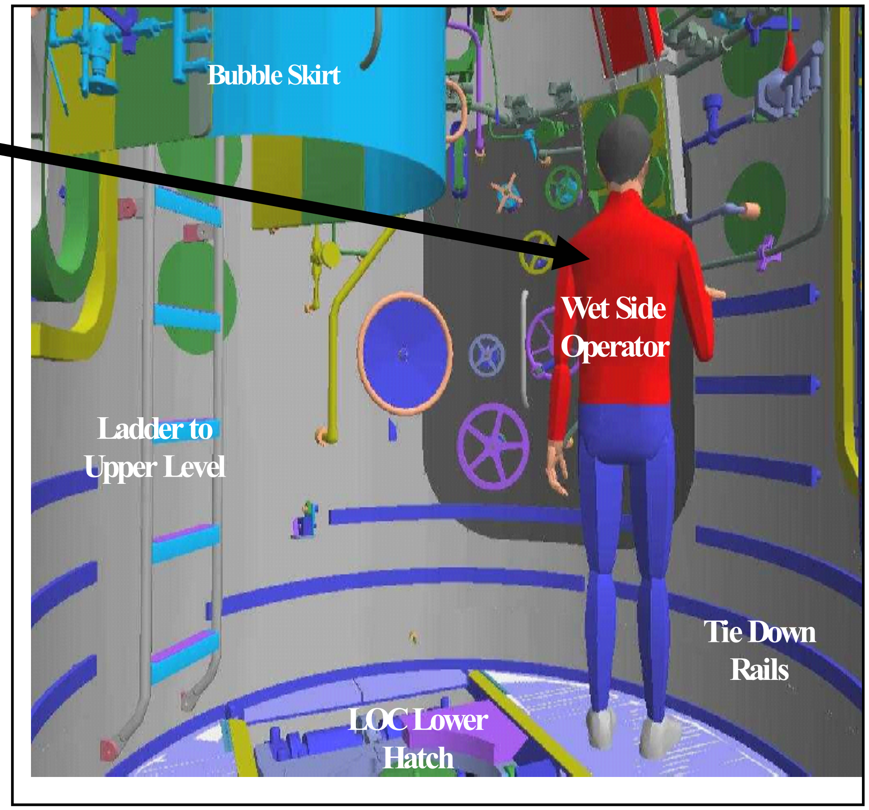
- Reserving pull-spaces on drawings for racking out equipment during maintenance.
- Readily identifying interference with other systems/subsystems/equipment.
- Demonstrating critical equipment removal and replacement flow-paths.
- Reserving spaces on drawings for access to vital equipment (safety of ship).

System Safety Process

CATIA Program (cont'd)

Ergo Man

Representing fifth through ninety-fifth percentile body dimensions) used to evaluate system design in terms of whole-body fit, access/emergency egress, reach and visual field etc.



SSGN Lockout Chamber

System Safety Process

CATIA Program (cont'd)

Through the use of CATIA, system safety engineers identified HSI issues early and throughout the design phase.

- Eliminating the need for separate operator and maintainer human engineering analyses.

Unresolved HSI issues were documented in applicable hazard analyses or analysis completion summary reports.

Lessons Learned

The IPPD process not readily accepted by all DBT members e.g., contractors, subcontractors, government agencies not using or familiar with the design build team process.

The IPPD process only as good as the DBT training provided to team members.

Lessons Learned

The IPPD process resulted in a lower number of documented hazards measured against traditional system safety processes (metrics, added value of a system safety program) because most hazards were designed out during the SIT meetings.

DBT members treated system safety engineers as partners rather than "safety police".