Enabling System Safety Through Technical Excellence

8th NDIA SE Conference
October 25, 2005

Warren M. Anderson, Colonel, USAF
Deputy for Systems Engineering Plans and Policy
Office of the Under Secretary of Defense (AT&L), Defense Systems, Systems Engineering, Enterprise Development

Top Five Systems Engineering Issues

- Lack of awareness of the importance, value, timing, accountability, and organizational structure of SE on programs
- Adequate, qualified resources are generally not available within government and industry for allocation on major programs
- Insufficient SE tools and environments to effectively execute SE on programs
- Poor initial program formulation
- Requirements definition, development, and management is not applied consistently and effectively

NDIA Study in January 2003

DoD Systems Engineering Shortfalls*

- Root cause of failures on acquisition programs include:
  - Inadequate understanding of requirements
  - Lack of systems engineering discipline, authority, and resources
  - Lack of technical planning and oversight
  - Stovepipe developments with late integration
  - Lack of subject matter expertise at the integration level
  - Availability of systems integration facilities
  - Incomplete, obsolete, or inflexible architectures
  - Low visibility of software risk
  - Technology maturity overestimated

Major contributors to poor program performance

* DoD-directed Studies/Reviews

USD(ATL) Imperatives

- “Provide a context within which I can make decisions about individual programs.”
- “Achieve credibility and effectiveness in the acquisition and logistics support processes.”
- “Help drive good systems engineering practices back into the way we do business.”

No Course Change from Mr. Krieg—Press On

What We Have Done To Revitalize Systems Engineering

- Issued Department-wide systems engineering (SE) policy
- Issued guidance on SE and test and evaluation (T&E)
- Established SE Forum—senior-level focus within DoD
- Instituted system-level assessments in support of OSD major acquisition program oversight role
- Working with Defense Acquisition University to revise SE, T&E, and enabling career fields curricula (Acq, PM, CM, FM)
- Integrating Developmental T&E with SE policy and assessment functions—focused on effective, early engagement of both
- Instituting a renewed emphasis on modeling and simulation
- Leveraging close working relationships with industry and academia

Necessary but not sufficient!

Striving for Technical Excellence

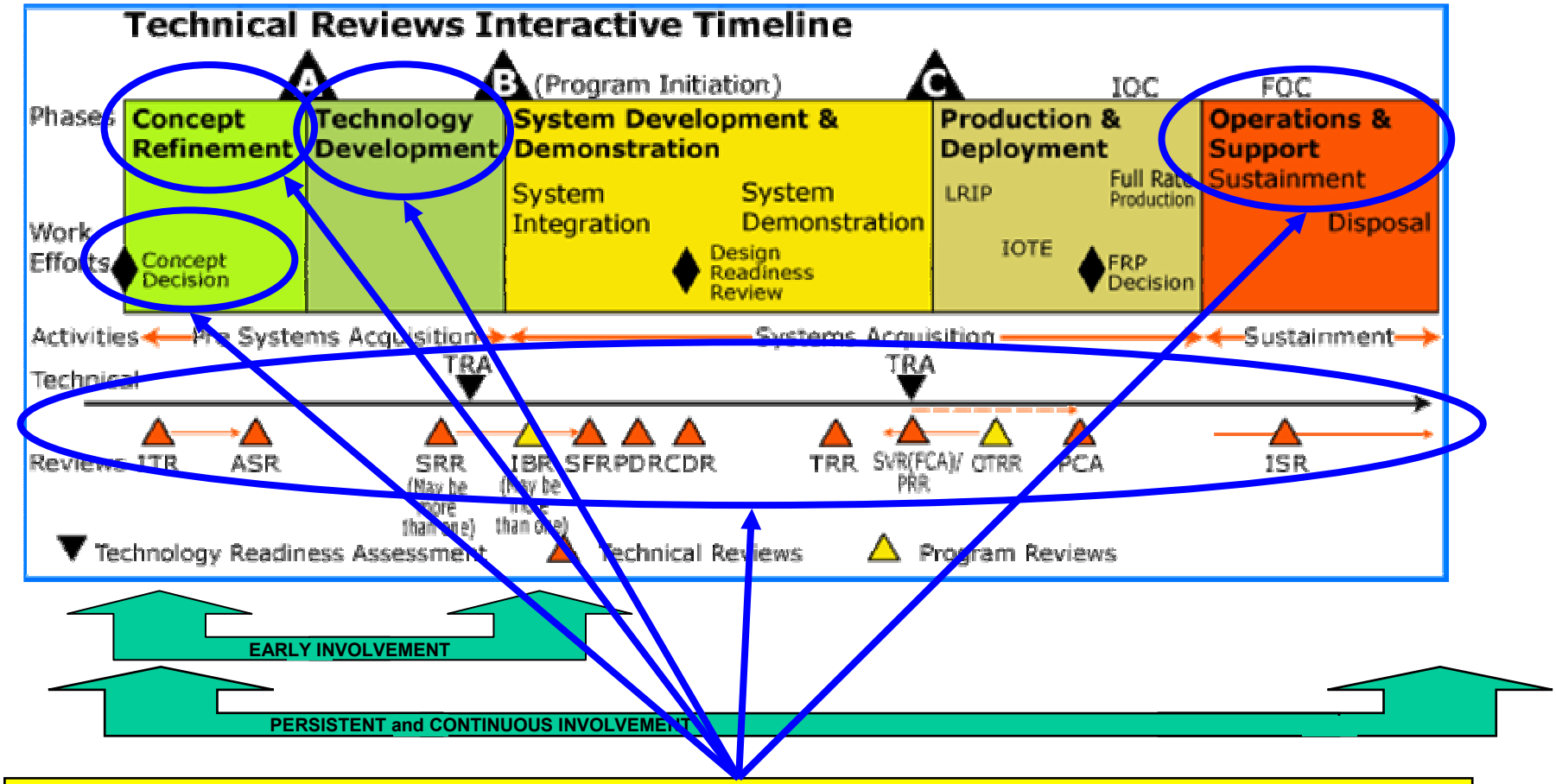
- All programs shall develop a SE Plan (SEP)
- Each PEO shall have a lead or chief systems engineer who monitors SE implementation within program portfolio
- Event-driven technical reviews with entry criteria and independent subject matter expert participation
- OSD shall review program's SEP for major acquisition programs (ACAT ID and IAM)

- Technical planning
- Technical leadership
- Technical execution

Technical excellence

Strong technical foundation is the value of SE to the program manager

SE Role in Acquisition



Increased use of disciplined Systems Engineering, including formal technical reviews, to effectively address technical issues

Reducing Preventable Accidents

- In FY 2002 DoD mishaps resulted in:
  - 550+ active duty fatalities
    - 308 were POV accidents
    - 67 were aviation-related deaths

1 military death every 16 hours

  - Over 1,474,000 military injury cases
    - 348,683 cases with duty limitations
    - 31,631 cases with hospitalization or quarters
    - 91,448 days lost

168 active duty injuries every hour

  - 2.0 Class A Aviation accident rate
    - Losses valued at $1.8 billion

1 aircraft destroyed every 5.2 days

"We need to turn this situation around."
SECDEF Memo, May 19, 2003

Defense Safety Oversight Council Governance Role

- Ensure personal involvement of senior leadership
- Promote the 50% accident reduction effort to all levels of military and civilian leadership
- Execute the specific initiatives to reduce accidents and time lost due to injuries
- Garner the resources to support the initiatives
- Manage progress toward goal
- Provide periodic updates to the Secretary

DSOC Membership

- **Principal Members**
  - Under Secretary of Defense for Personnel and Readiness (as Chair)
  - Under Secretary of Defense for Acquisition, Technology, and Logistics
  - Under Secretary of Defense (Comptroller)/Chief Financial Officer
  - Vice Chairman of the Joint Chiefs of Staff
  - Assistant Secretary of Defense for Health Affairs
  - Under Secretary of the Army
  - Under Secretary of the Navy
  - Under Secretary of the Air Force
- **Associate members**
  - Deputy Under Secretary of Defense (Installations and Environment)
  - Deputy Under Secretary of Defense (Readiness)
  - Deputy Under Secretary (Civilian Personnel Policy)
  - Deputy Inspector General of the Department of Defense
  - Deputy Assistant Secretary of Defense (Clinical and Program Policy)
  - Deputy Director (Administration & Management), OSD
- **Executive Secretary**
  - Joseph J. Angello, Jr., Director, Readiness Programming & Assessment

7

Improving Safety Performance

- Eight DSOC Task Forces
  - Deployment and Operations
  - Aviation Safety Improvements
  - Military Training
  - Personal Motor Vehicle Accident Reduction
  - Installation and Industrial Operations
  - Worker's Compensation
  - Enterprise Information and Data
  - Acquisition and Technology Programs (ATP)

Acquisition and Technology Programs (ATP) Task Force

- Purpose
  - Recommend or implement changes to policies, procedures, initiatives, education and training, and investments to ensure programs address safety throughout the life cycle
- Goals
  - Ensure acquisition policies and procedures for all systems address safety requirements
  - Review and modify, as necessary, relevant DoD standards with respect to safety
  - Recommend ways to ensure acquisition program office decisions consider system hazards
  - Recommend ways to ensure milestone decision reviews and interim progress reviews address safety

Establish dialogue between System Safety and Systems Engineering communities

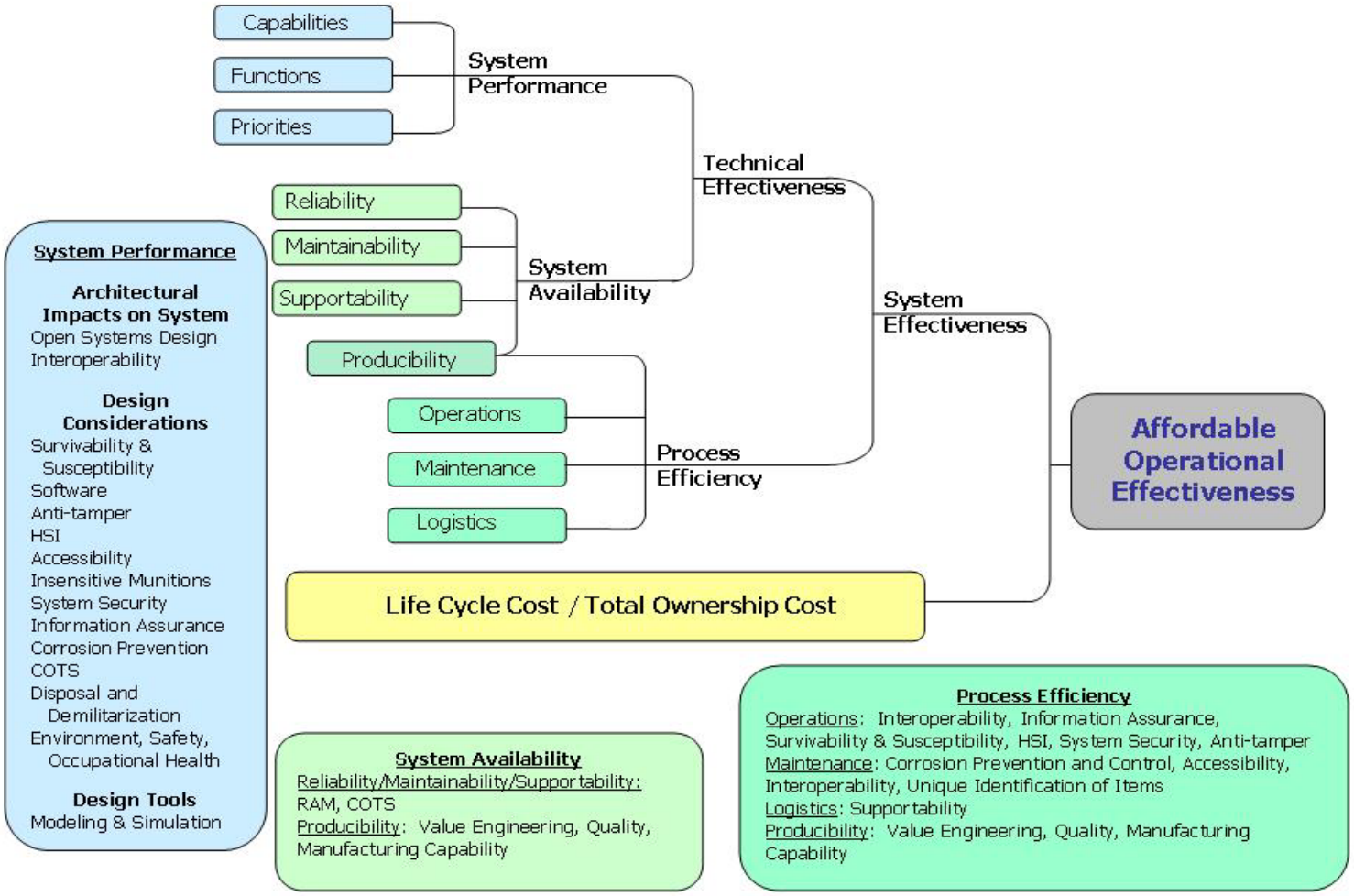
How the ATP Task Force Has Responded

- Issued DoD-wide policy on "Defense Acquisition System Safety" (USD(AT&L) Memo, Sep 23, 2004)—Program Managers shall:
  - Integrate system safety risk management into their overall systems engineering and risk management processes
  - Use Standard Practice for System Safety, MIL-STD-882D, in all developmental and sustaining engineering activities
  - Ensure the Environment, Safety, and Occupational Health (ESOH) risk management strategy is integrated into the SE process and incorporated in the Systems Engineering Plan
  - Identify ESOH hazards, assess the risks, mitigate the risks to acceptable levels, and report status of residual risk decisions at appropriate program reviews per MIL-STD-882D

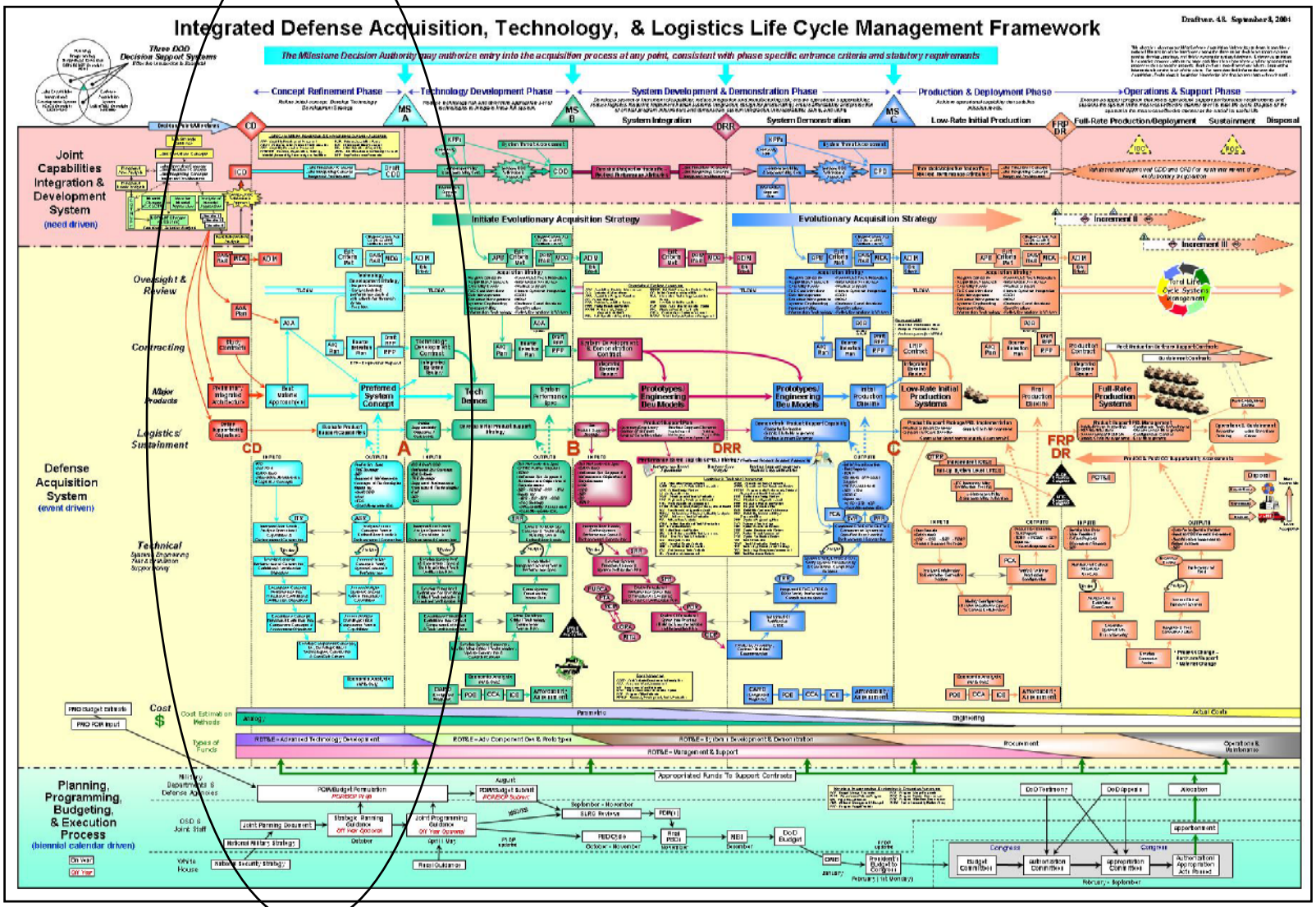
How the ATP Task Force Has Responded (con't)

- Incorporated ESOH into *Defense Acquisition Guidebook*
  - Programmatic ESOH evaluation (PESHE)
  - ESOH risk management process
- Developed Defense Acquisition University continuous learning course, "System Safety in Systems Engineering" (CLE009)
  - Based on use of MIL-STD-882D
  - Provides roadmap for linking System Safety into SE process
  - Maps System Safety tasks into SE process for each phase

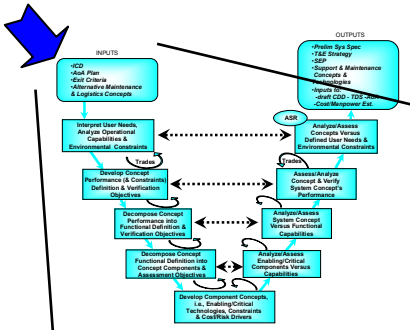
Important Design Considerations
"The Fishbone"



SE in the System Life Cycle
"The Wall Chart"

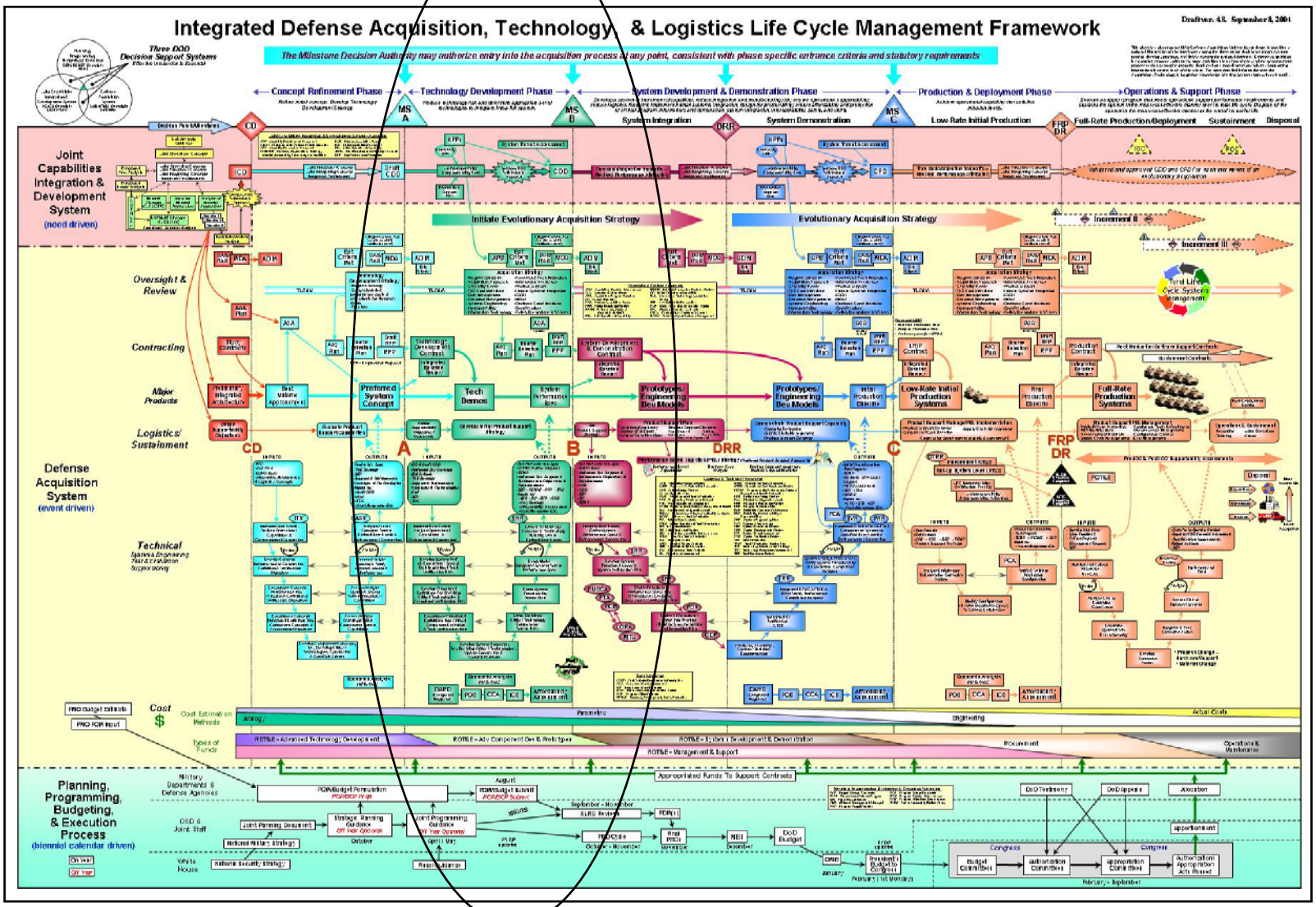


System Safety in SE Process
Concept Refinement Phase

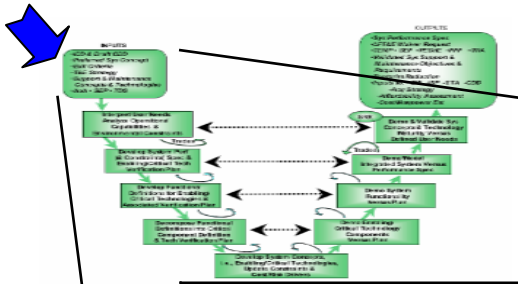


Inputs	System Safety Should:
Initial Capabilities Document (ICD)	Provide inputs as requested
Analysis of Alternatives (AoA) Plan	Participate in AoA development
Exit Criteria	Provide the following exit criteria: 1. Preliminary Hazard List (PHL) 2. Strategy for integrating Environment, Safety, and Occupational Health (ESOH) risk management into systems engineering (SE)
Alternative Maintenance and Logistics Concepts	Provide inputs as requested

SE in the System Life Cycle
"The Wall Chart"

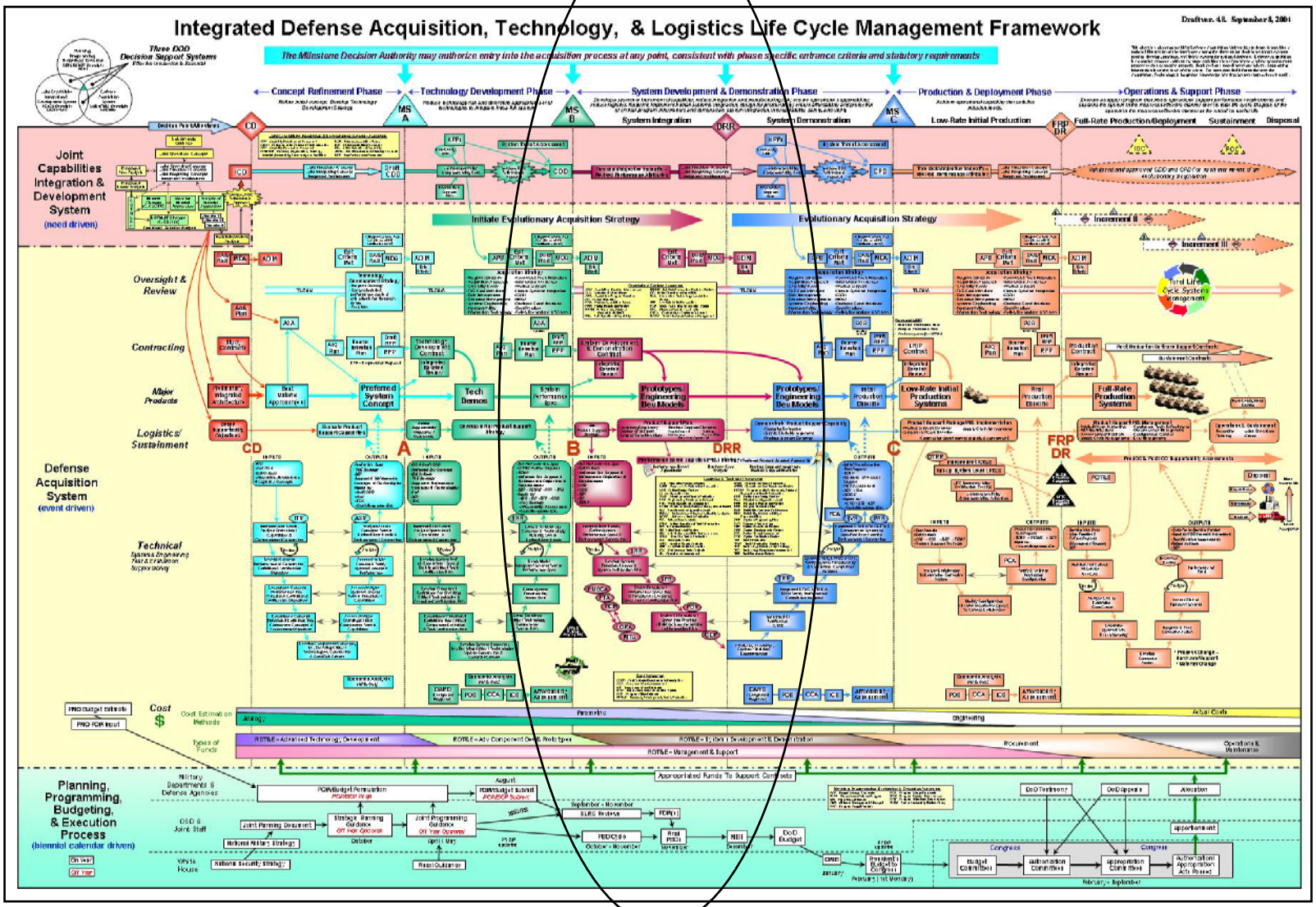


System Safety in SE Process
Technology Development Phase

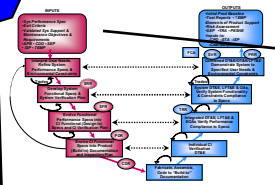


Inputs	System Safety Should:
Initial Capabilities Document (ICD) and Draft Capability Development Document (CDD)	Develop system safety criteria and requirements
Preferred System Concept	Evaluate system concept against identified system safety criteria
Exit Criteria	Provide the following exit criteria: 1. Update Preliminary Hazard List (PHL) 2. Update strategy for integrating Environment, Safety, and Occupational Health (ESOH) risk management into systems engineering (SE)
Test and Evaluation (T&E) Strategy	1. Incorporate hazard risk mitigation test and verification methodologies 2. Provide approach toward obtaining safety release(s)
Support and Maintenance Concepts and Technologies	Provide inputs as requested
Analysis of Alternatives (AoA)	Characterize ESOH footprints or risks for AoA development
Systems Engineering Plan (SEP)	Update strategy for integrating ESOH risk management into SE
Technology Development Strategy (TDS)	1. Include strategy to identify hazards 2. Identify needed ESOH technology development

SE in the System Life Cycle
"The Wall Chart"

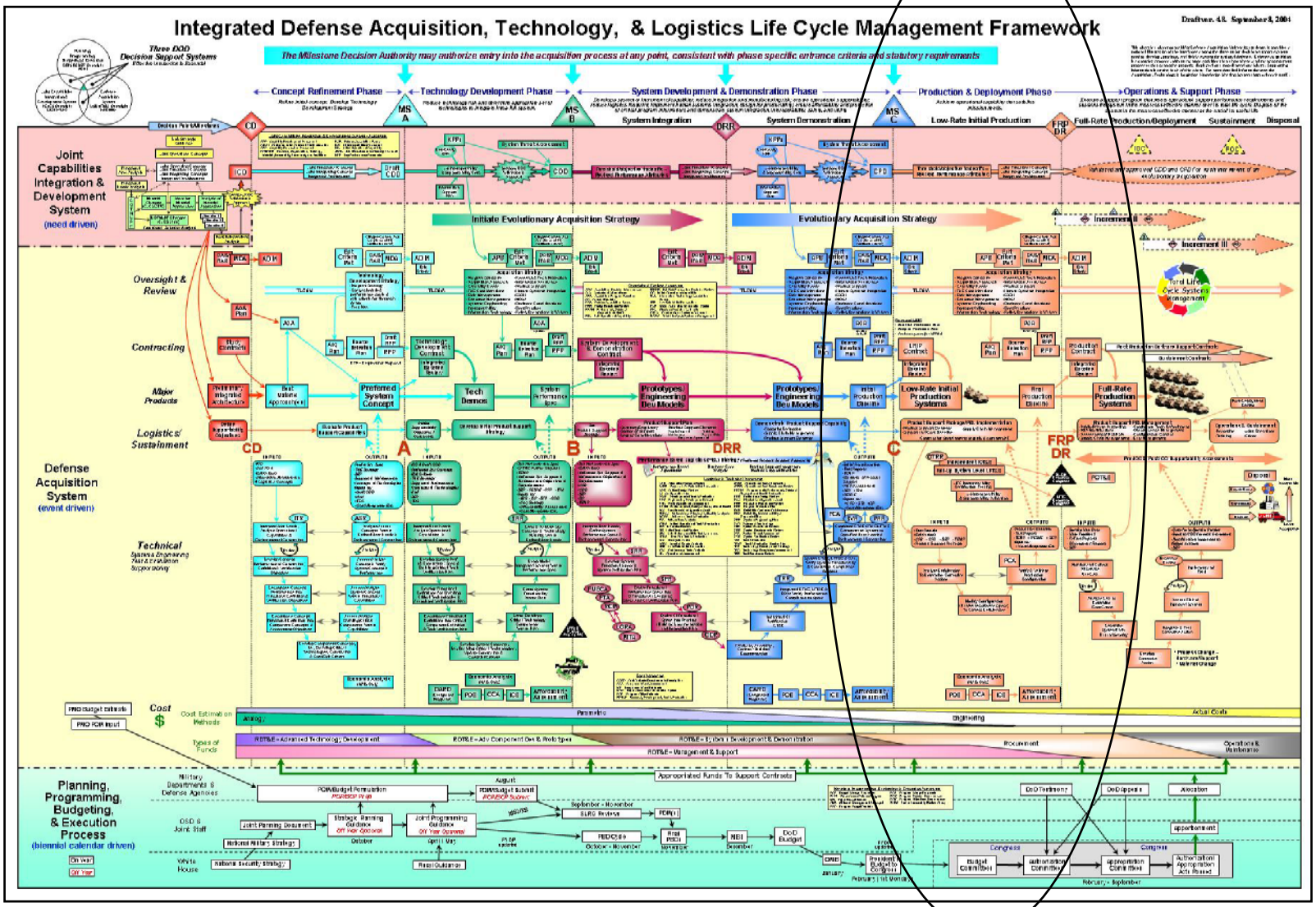


System Safety in SE Process System Development and Demonstration Phase

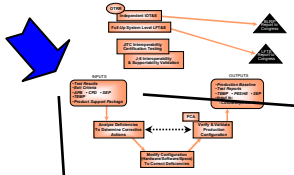


Inputs	System Safety Should:
System Performance Specification	1. Include the Safety Requirements/Criteria Requirements Analysis (SRCA) data 2. Include applicable specifications (e.g., MIL-STD-2105C, MIL-STD-1316, MIL-STD-331, MIL-STD-1901, MIL-STD-464, IEEE/EIA 12207, HAZMAT list to avoid, 29CFR1910)
Exit Criteria	1. Document risk disposition of identified hazards, e.g., Safety Assessment Report (SAR) 2. Obtain concurrence/approval of appropriate safety boards 3. Update Programmatic Environment, Safety, and Occupational Health Evaluation
Validated System Support and Maintenance Objectives & Req.	Identify operating, maintenance, and support hazards
Acquisition Program Baseline	Provide inputs as requested
Capability Development Document (CDD)	1. Identify hazard mitigation requirements 2. Identify insensitive munitions requirements 3. Identify mishap reduction requirements
Systems Engineering Plan (SEP)	1. Update strategy for integrating ESOH risk management into SE (e.g., Integrated Product Team (IPT) Process, technical reviews, etc.) 2. Identify applicable safety boards and process for concurrence/approval
Integrated Support Plan (ISP)	Provide guidance on performance feedback and hazard communication
Test and Evaluation Master Plan (TEMP)	1. Identify specific test requirements (e.g., MIL-STD-2105C, MIL-STD-1316, MIL-STD-331, MIL-STD-1901, IEEE/EIA 12207, 29CFR1910) 2. Identify requirements for verification of risk mitigation controls (based upon system safety analyses) 3. Identify safety release requirements, e.g., SAR

SE in the System Life Cycle
"The Wall Chart"

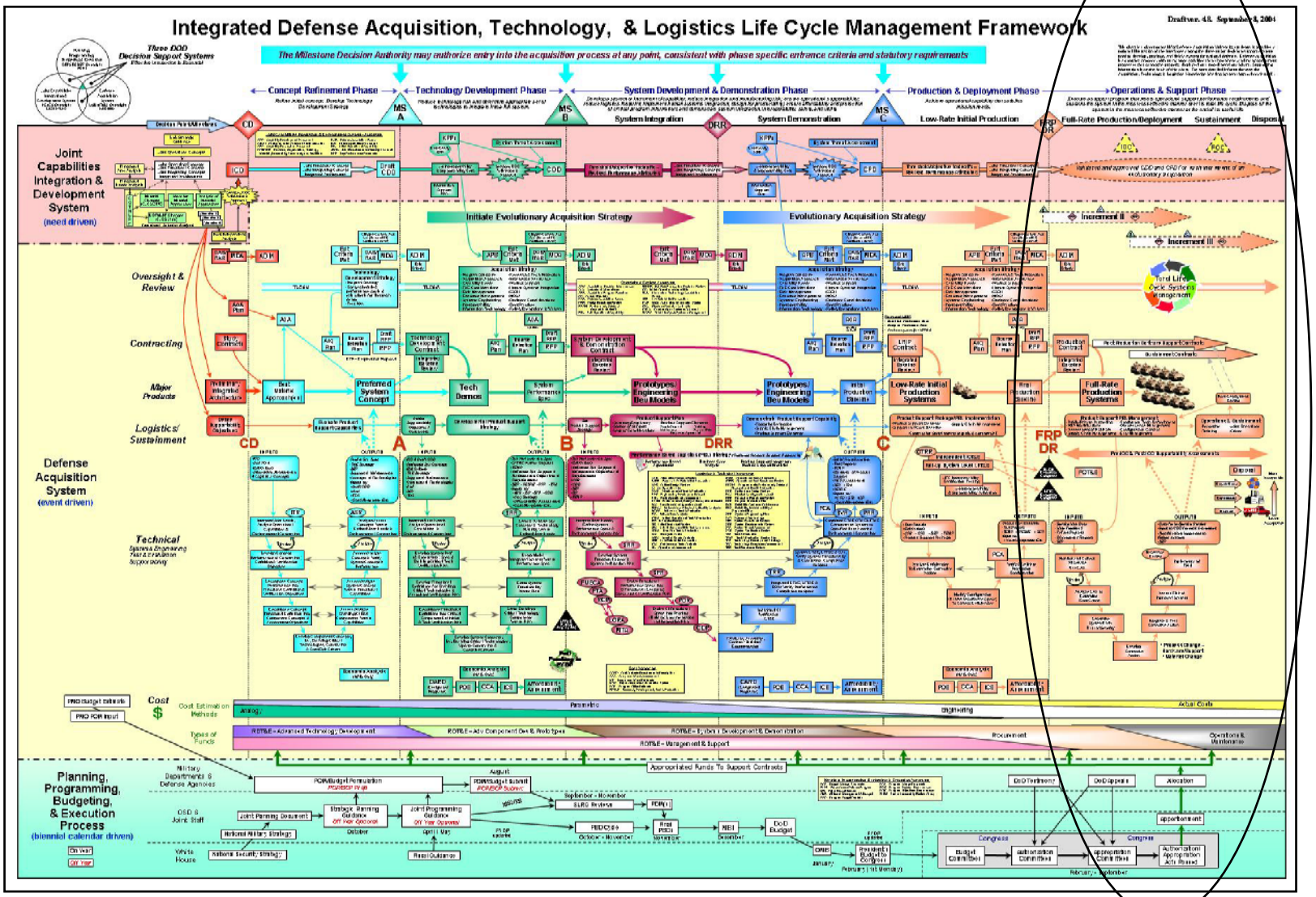


System Safety in SE Process Production and Deployment Phase

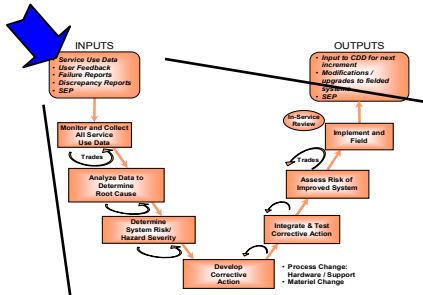


Inputs	System Safety Should:
Test Results	1. Review Initial Operational Test & Evaluation (IOT&E) results for the effectiveness of risk mitigation controls 2. Analyze anomalies, incidents, and mishaps
Exit Criteria	1. Document formal risk disposition of identified hazards, e.g., Safety Assessment Report 2. Obtain concurrence/approval of appropriate safety boards 3. Update Programmatic Environment, Safety, and Occupational Health Evaluation 4. Provide updated inputs for demilitarization/disposal plan
Acquisition Program Baseline	Provide inputs as requested
Capability Production Document (CPD)	1. Update hazard mitigation requirements as necessary 2. Update insensitive munitions requirements as necessary 3. Identify mishap reduction requirements as necessary
Systems Engineering Plan (SEP)	1. Update strategy for integrating ESOH risk management into SE 2. Identify applicable safety boards and process for concurrence/approval
Test and Evaluation Master Plan (TEMP)	1. Update specific test requirements (e.g., MIL-STD-2105C, MIL-STD-1316, MIL-STD-331, MIL-STD-1901, IEEE/EIA 12207, 29CFR1910.95) 2. Update requirements for verification of risk mitigation controls (based upon system safety analyses) 3. Update safety release requirements, e.g., SAR
Product Support Package	Include O&SHA results

SE in the System Life Cycle
"The Wall Chart"



System Safety in SE Process Operations and Sustainment Phase



Inputs	System Safety Should:
Service Use Data	Review for system safety implications
User Feedback	Review for system safety implications
Failure Reports	1. Review Follow-On Operational Test & Evaluation (FOT&E) results for system safety implications 2. Review failure/mishap reports for causal factors or mitigation failures and recommend alternative mitigation measures 3. Assist in mishap investigations as requested
Discrepancy Reports	Review discrepancy reports for system safety implications
Systems Engineering Plan (SEP)	1. Update strategy for integrating ESOH risk management into SE 2. Identify applicable safety boards and process for concurrence/approval

Program Support Reviews System Safety Metrics

- Developing evaluation criteria for System Safety
  - Emphasizing effective integration into Systems Engineering
  - Focused on assessing performance of System Safety
    - Identifying environment, safety, and occupational health hazards
    - Influencing design development to eliminate or mitigate hazards
- Integrating System Safety into Defense Acquisition Executive Summary (DAES) quarterly reporting
  - Piloting with DAES-Sustainment
  - Four System Safety Metrics for Sustainment phase
    - Hazard with highest risk category
    - Class A, B, and C mishap rate trends
    - Open Safety or Hazardous Material technical data change requests
    - System Safety level-of-effort

Summary

- OSD's fundamental role is to set policy, provide relevant and effective education and training, and foster communication throughout the community
- OSD cannot do everything…NOR should we
- Challenges Remain
  - Refocusing Acquirer and Supplier on technical management of programs throughout the life cycle
  - Getting System Safety fully and effectively integrated into the Systems Engineering process to reduce Environment, Safety, and Occupational Health risks & costs