SURVICE ENGINEERING COMPANY

System Safety in Systems Engineering Process

SURVICE Engineering Company
4695 Millennium Drive
Belcamp, MD 21017

Ray C. Terry, Ph.D.
ray.terry@survice.com

NDIA 8th Annual Systems Engineering Conference

SURVICE ENGINEERING COMPANY

Overview

- The Big Question
  - System Safety
  - Systems Engineering
- Classic System Safety Model
- OSD(AT&L) Life Cycle Management Framework
- Systems Engineering V-model
- "Integrated" System Safety Model
- Summary

SURVICE ENGINEERING COMPANY

The Big Question

- **Have you ever wondered:**
  - **Why is it that it's *Systems* Engineering,**
  - **But it's *System* Safety?**
  - **What happened to the "s"?**
  - **Have you asked yourself this same question?**
  - **And, it's been used inconsistently at this conference!!**
- **Let's explore this for a few minutes**

SURVICE ENGINEERING COMPANY

What is System Safety?

- **Engineering of Safe Systems or Safety of Systems**
- **Systems Safety – the discipline**
- **System Safety – the application of the discipline of systems safety to a specific system or a system of systems**
- **and…**

SURVICE ENGINEERING COMPANY

What is Systems Engineering?

- Engineering of Systems
- Systems Engineering – the discipline
- System Engineering – the application of the discipline of systems engineering to a specific system or a system of systems
- One Air Force Program Office used the terminology Director of "System Engineering" because according to the Director, they were working on only one system (contextually-based)
- But what it points to…

SURVICE ENGINEERING COMPANY

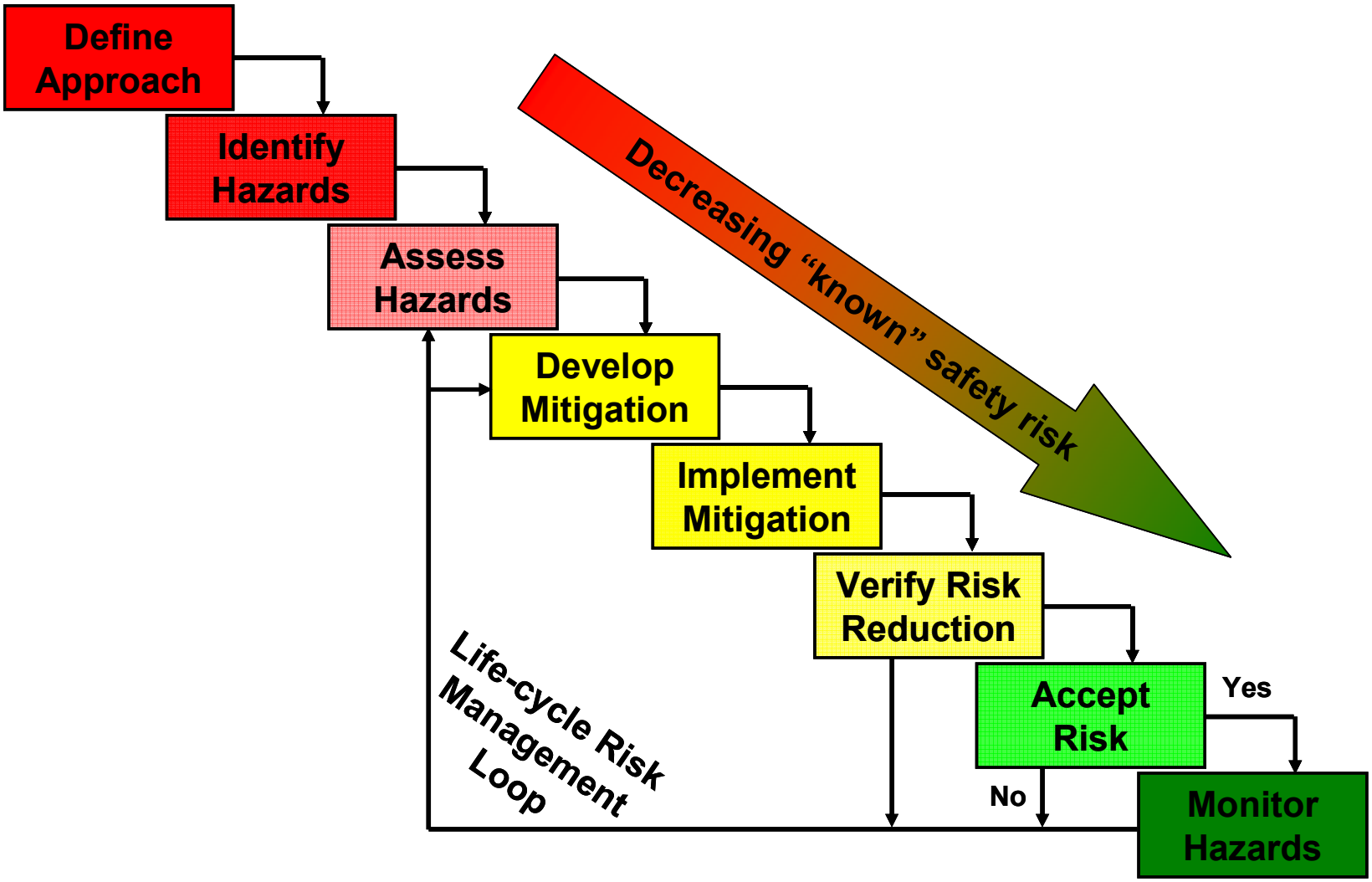
System Safety versus Systems Engineering

- Lack of effective integration of Systems Safety within Systems Engineering (or System Safety within System Engineering at the project level)
- Real issue is System Safety Requirements and ensuring System Safety is effectively integrated into product realization
- So…what do we do?
- First, we might use a standard definition of system
- But keep that question in mind while we discuss some other ideas

SURVICE ENGINEERING COMPANY

Classic System Safety Model

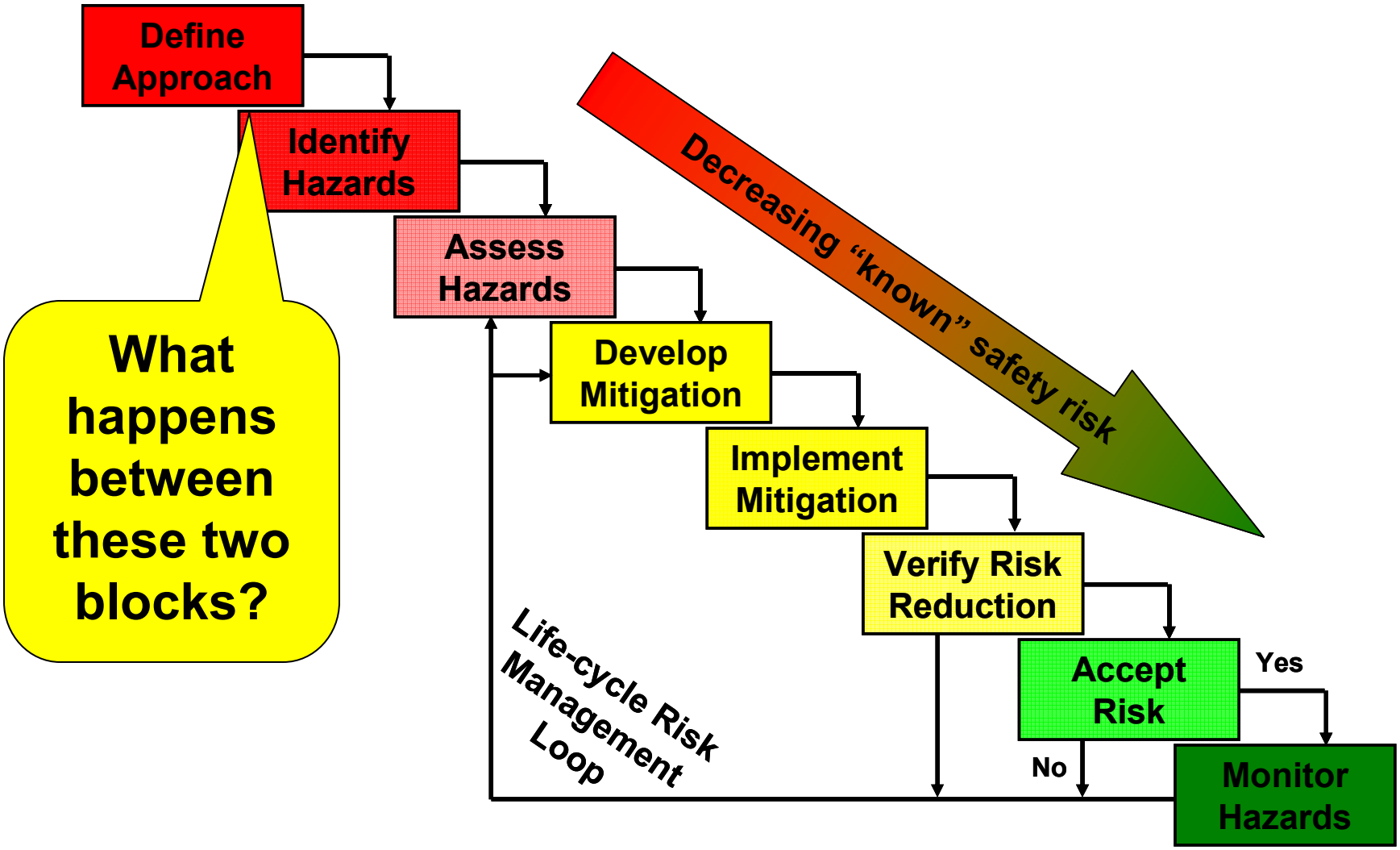
(MIL-STD-882D)



SURVICE ENGINEERING COMPANY

Classic System Safety Model

(MIL-STD-882D)



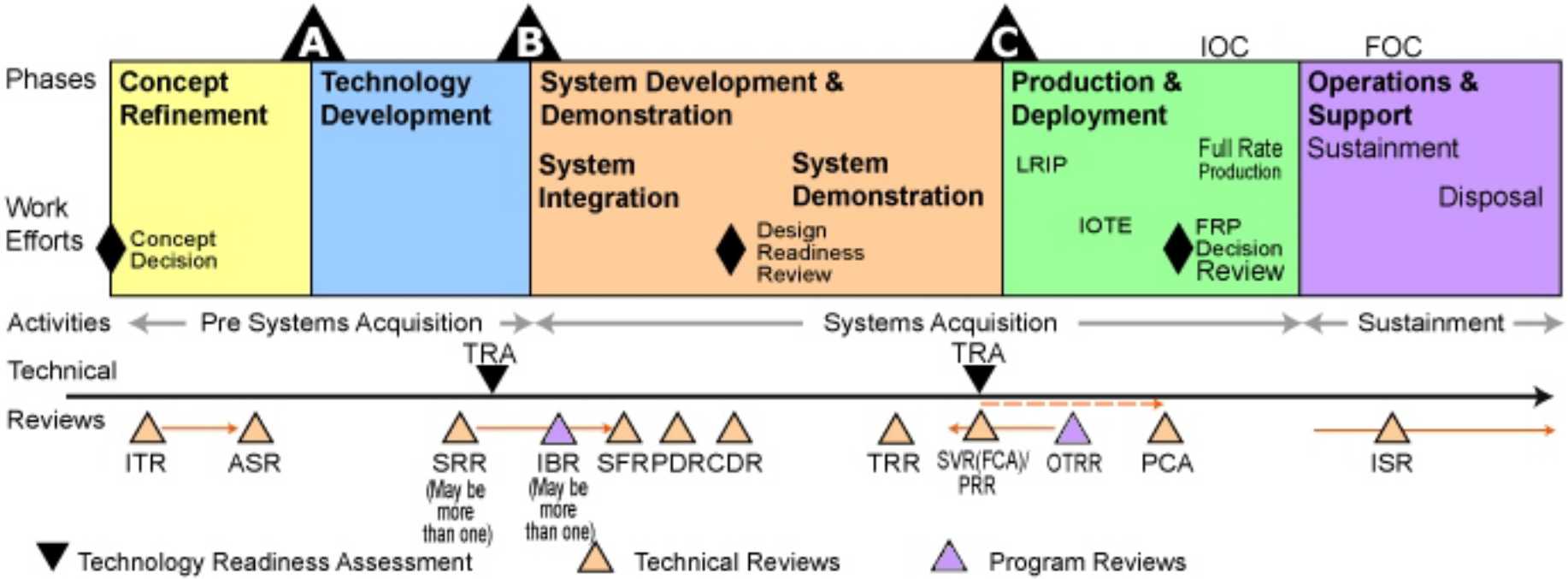
SURVICE ENGINEERING COMPANY

DoD 5000.1 Acquisition Phases

- **Major System Acquisition Phases**
  - **Concept Refinement**
  - **Technology Development**
  - **System Development & Demonstration**
    - **System Integration**
    - **System Demonstration**
  - **Production & Deployment**
    - **Low-rate Initial Production**
  - **Operations & Support**
    - **Full-Rate Production and Deployment**
    - **Sustainment**
    - **Disposal (Recycle/Reuse, Reprocessing or Disposal)**

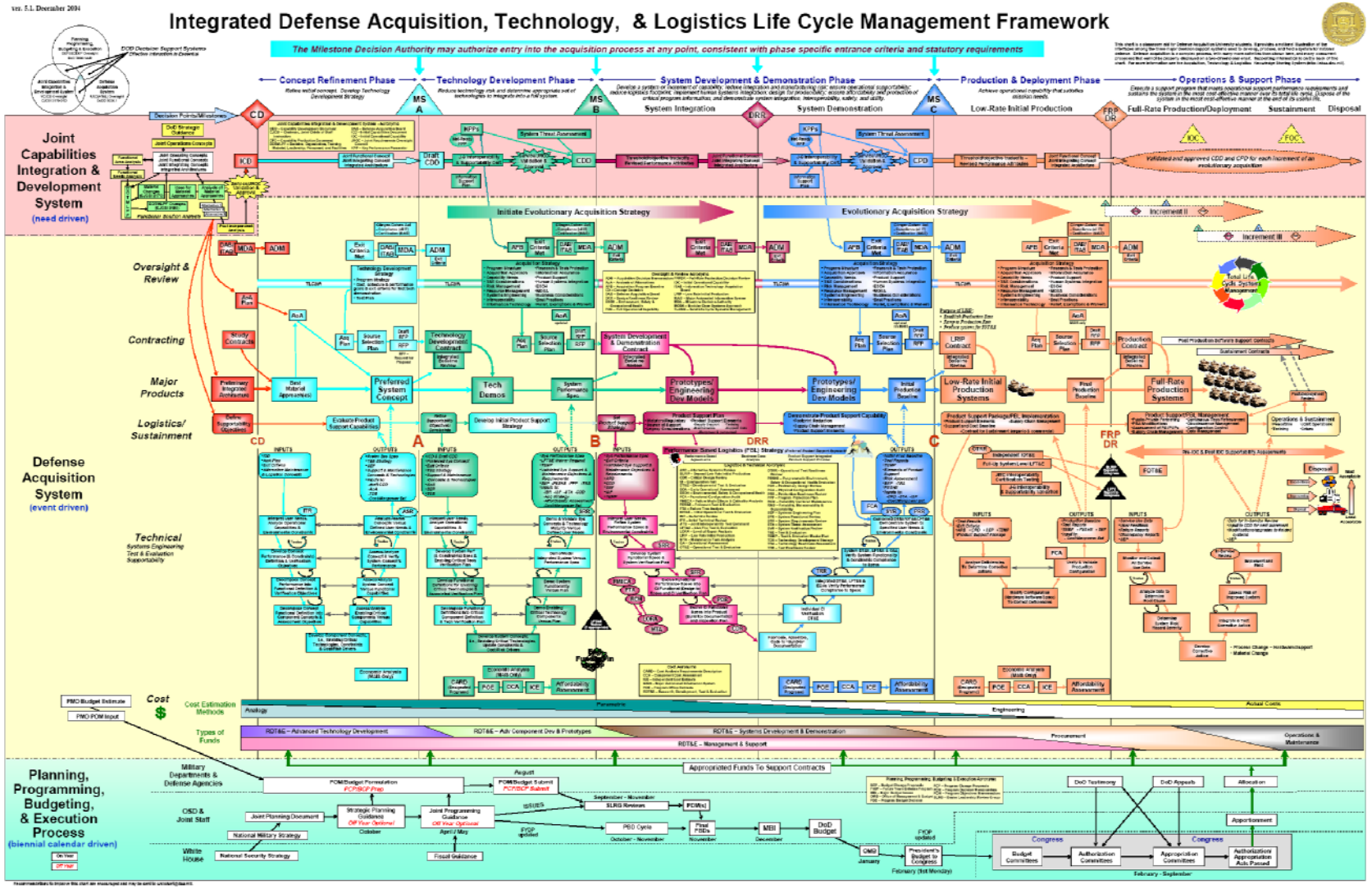
SURVICE ENGINEERING COMPANY

DoD 5000.1 Acquisition Phases



SURVICE ENGINEERING COMPANY

Integrated Systems Engineering "The Wall Chart"



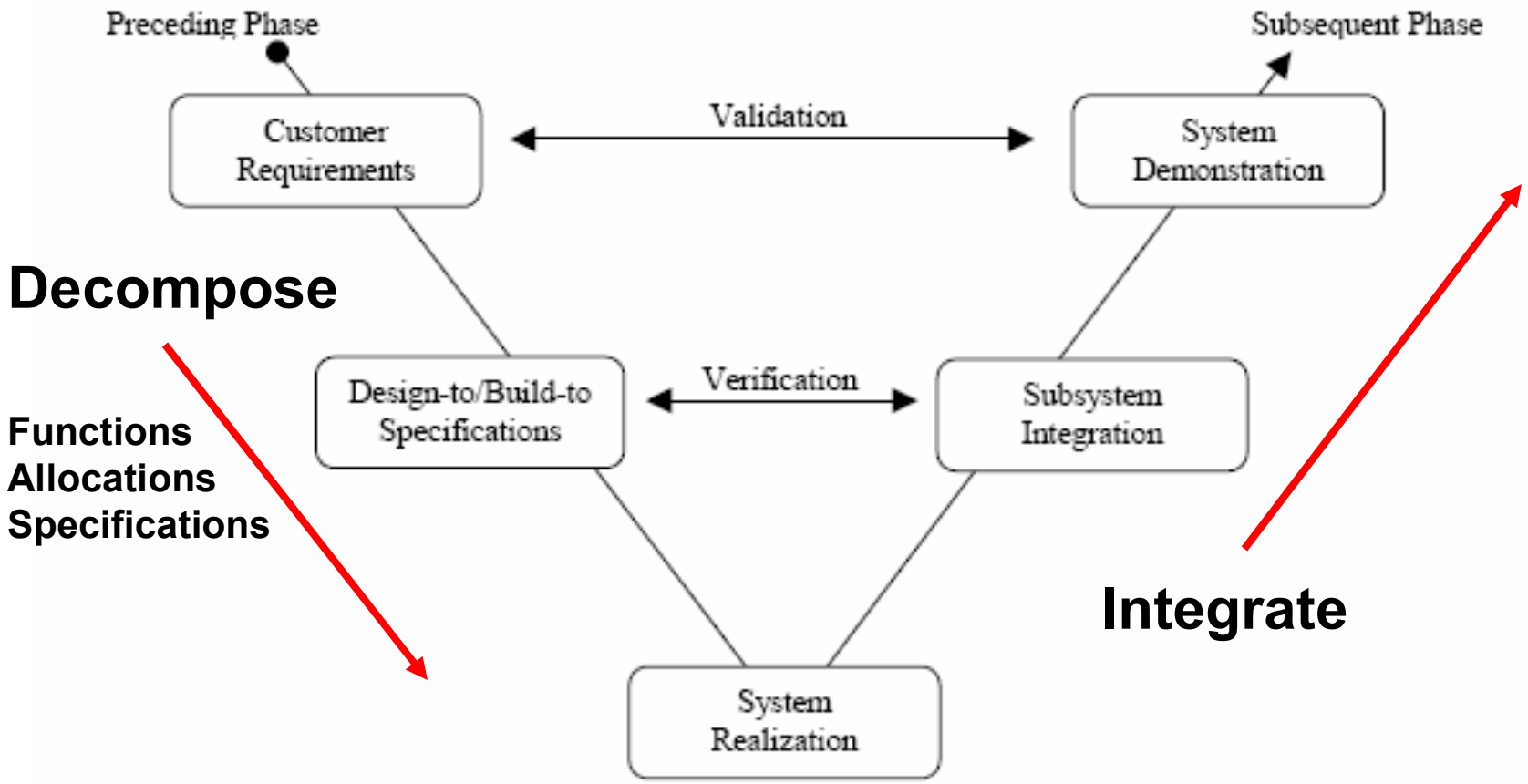
SURVICE ENGINEERING COMPANY

Phase Characteristics

- Phase-specific Technical Baseline
- Phase-specific “Requirements” Review including “Derived” Requirements
- Requirements Analysis
- Functional Decomposition
- Functional and Physical Allocations
- Subsystem and Component Specifications
- Component, Subsystem & System Integration
- Verification and Validation Activities

SURVICE ENGINEERING COMPANY

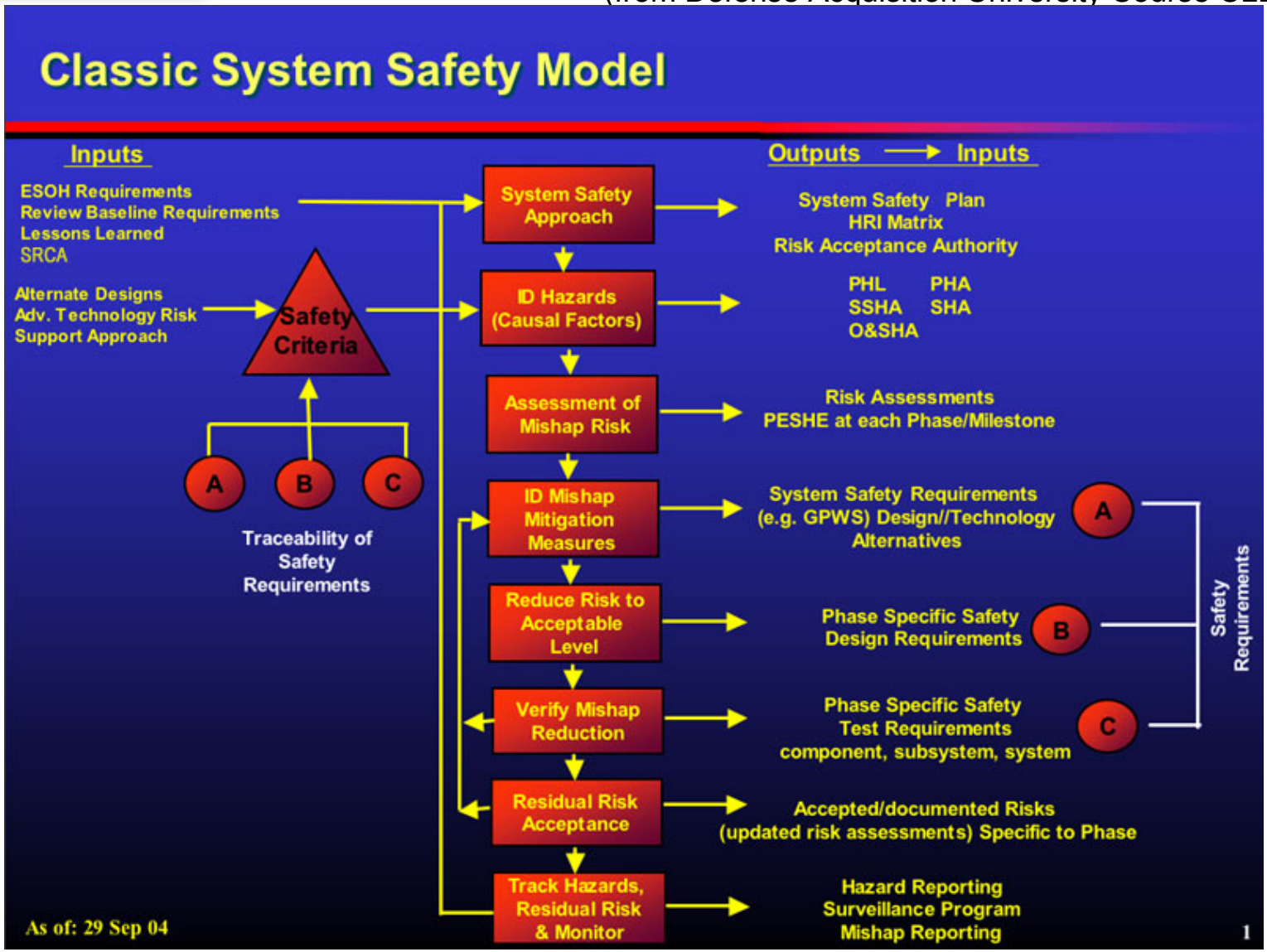
Systems Engineering V-model
(generalized)



SURVICE ENGINEERING COMPANY

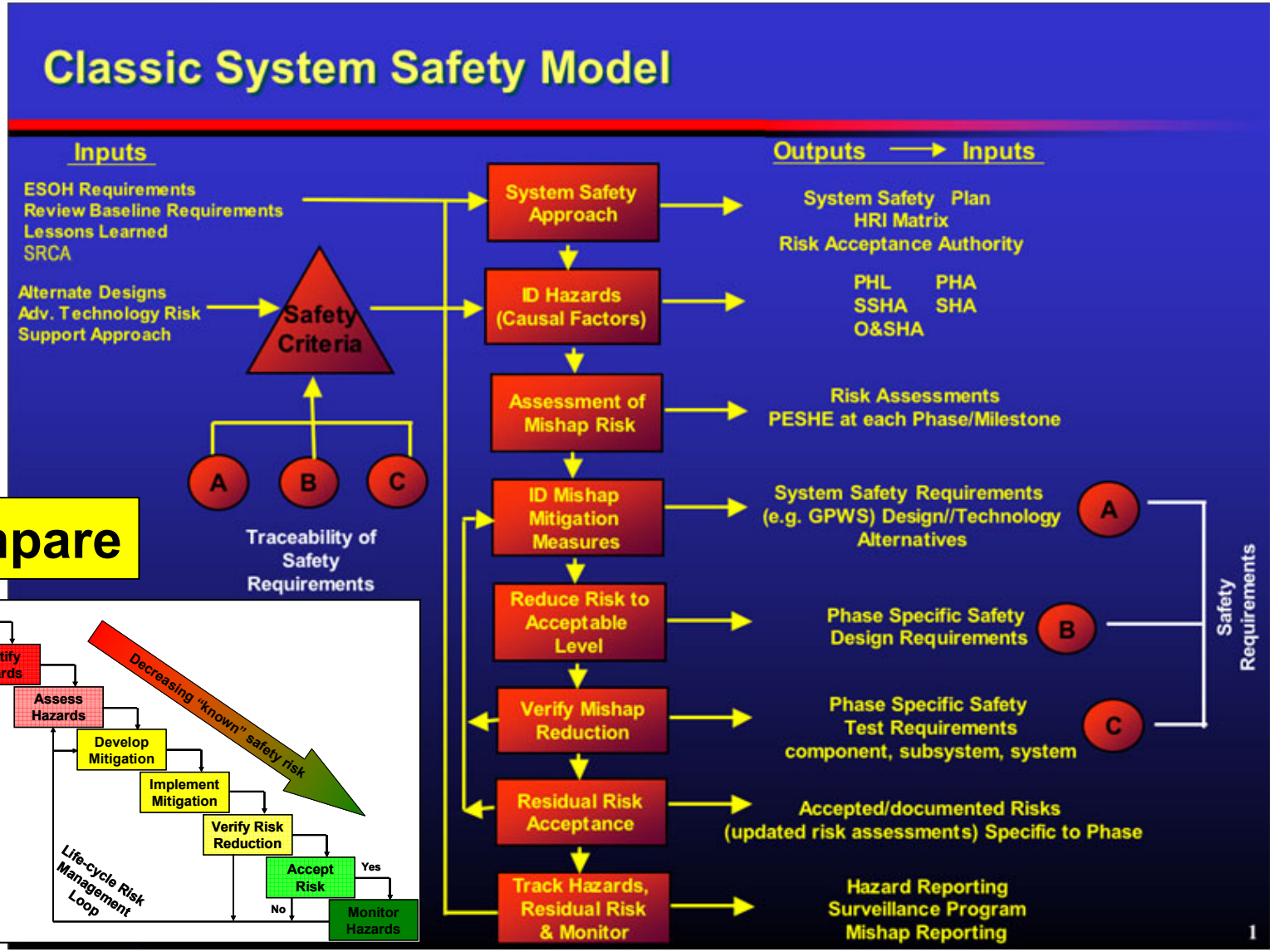
"Integrated" System Safety Model

(from Defense Acquisition University Course CLE009)



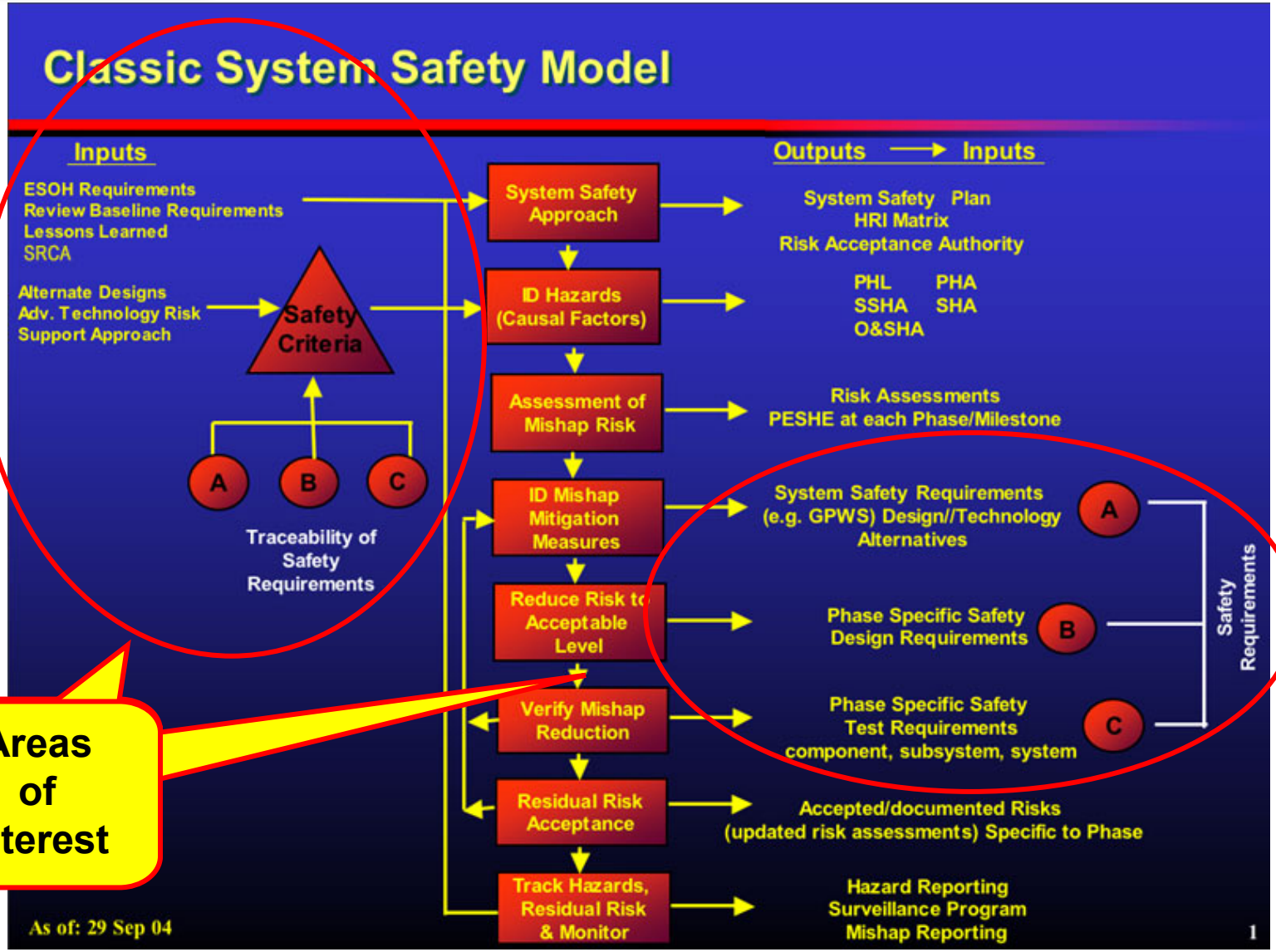
SURVICE ENGINEERING COMPANY

"Integrated" System Safety Model



SURVICE ENGINEERING COMPANY

"Integrated" System Safety Model



Areas of Interest

SURVICE ENGINEERING COMPANY

System Safety Requirements

- **Phase Specific**
- **Managed with Other System Engineering Artifacts**
  - **Requirements Traceability (requirements tool)**
  - **CONOPS, Conceptual Design & System Architecture**
  - **Verification and Validation Tests (e.g., TEMP)**
- **Part of Technical Baseline for Each Phase**
  - **Alternative System Review**
  - **System Functional Review**
  - **System Requirements Review**
  - **Preliminary Design Review**
  - **Critical Design Review**
  - **Test Readiness Review**

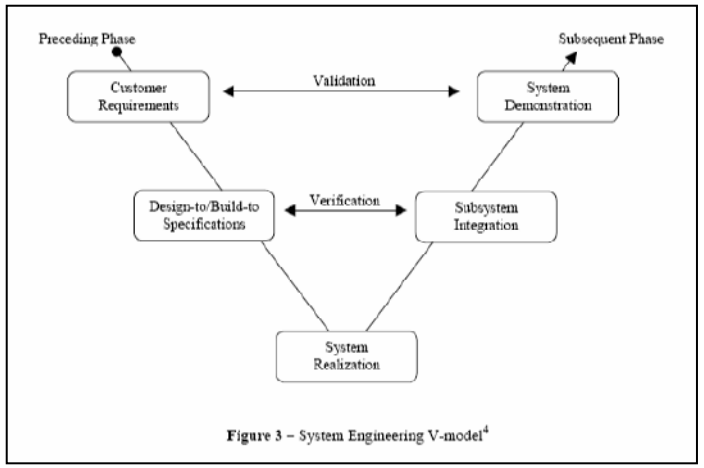


Figure 3 – System Engineering V-model[4]

SURVICE ENGINEERING COMPANY

System Safety Requirements

- **Phase Specific**
- **Managed with Other System Engineering Artifacts**
  - **Requirements Traceability Matrix**
  - **CONOPS, Conceptual Design & System Architecture**
  - **Verification and Validation Tests (e.g., TEMP)**
- **Part of Technical Baseline for Each Phase**
  - **Alternative System Review**
  - **System Functional Review**
  - **System Requirements Review**
  - **Preliminary Design Review**
  - **Critical Des n Review**
  - **Test Read Review**

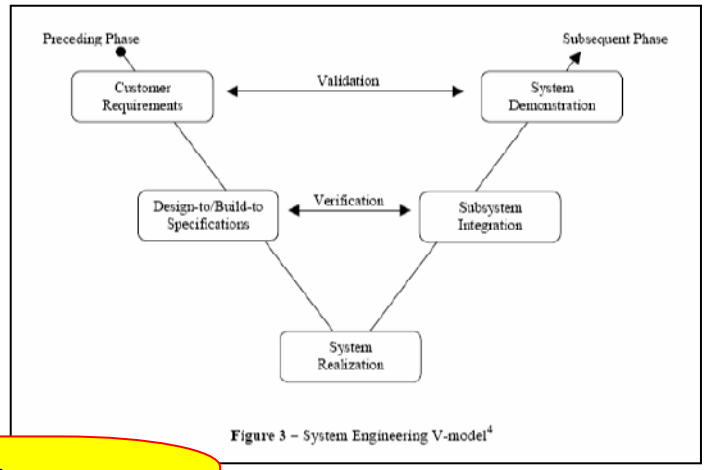
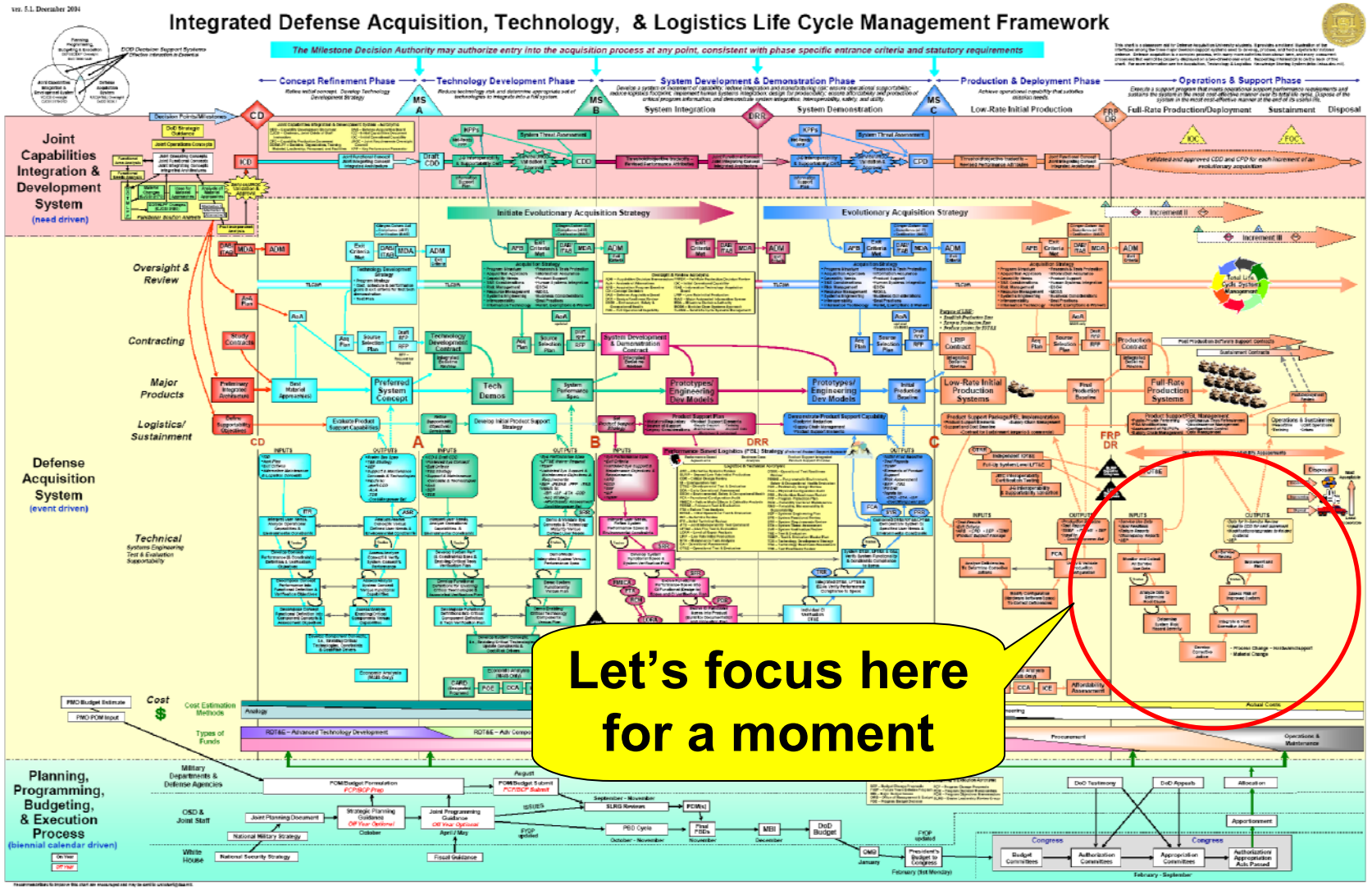


Figure 3 – System Engineering V-model[4]

Somewhere just before here is typical entry point!!

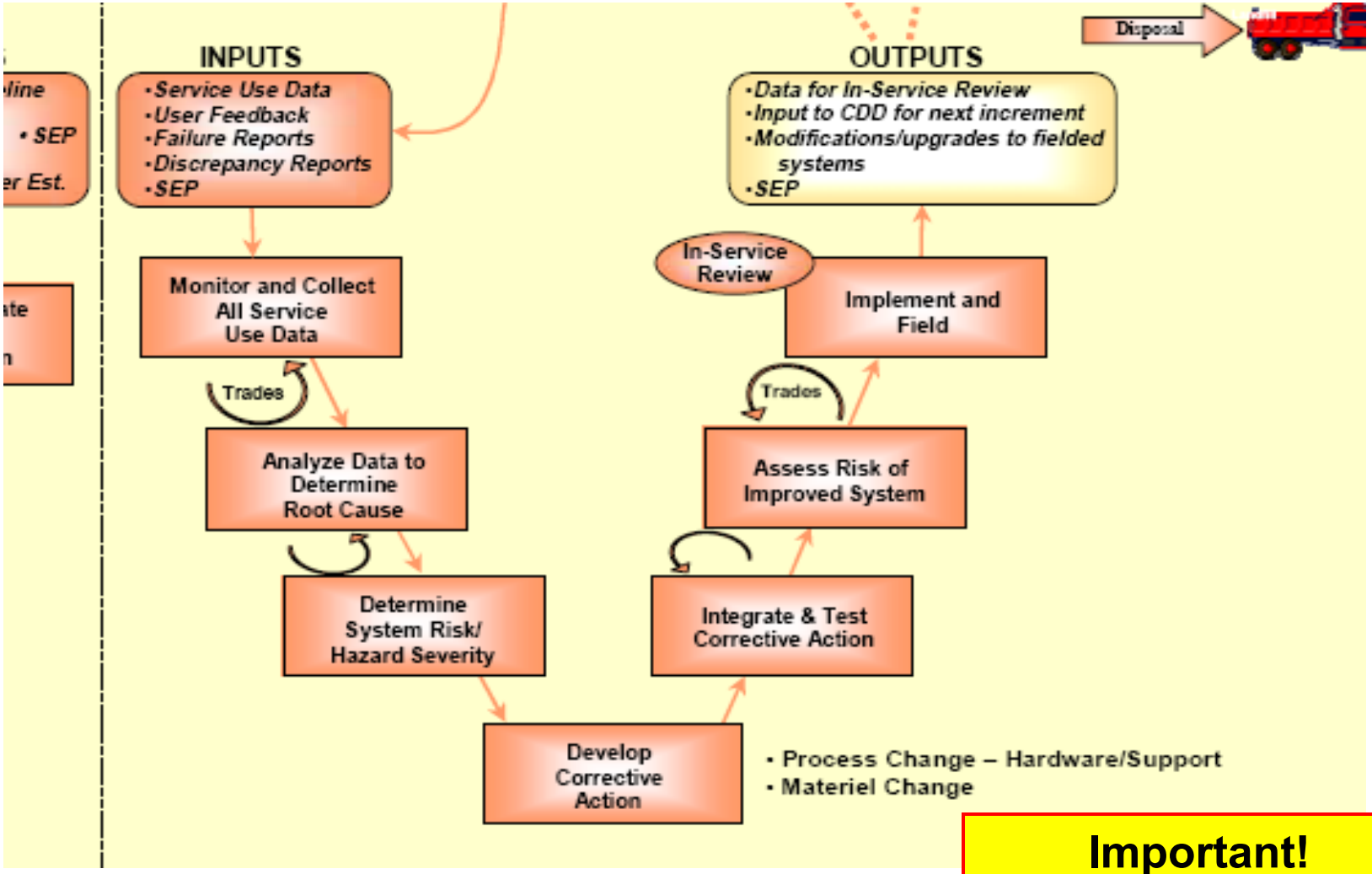
SURVICE ENGINEERING COMPANY

Integrated Systems Engineering "The Wall Chart"



SURVICE ENGINEERING COMPANY

Life Cycle Framework In-service System Safety Requirements

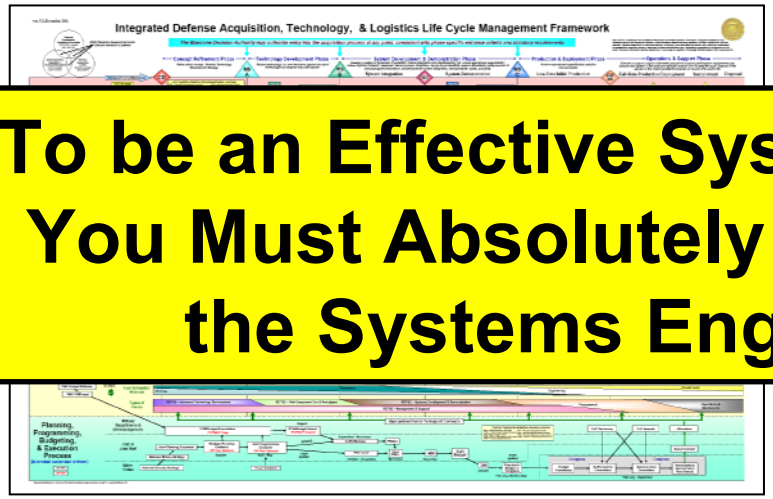


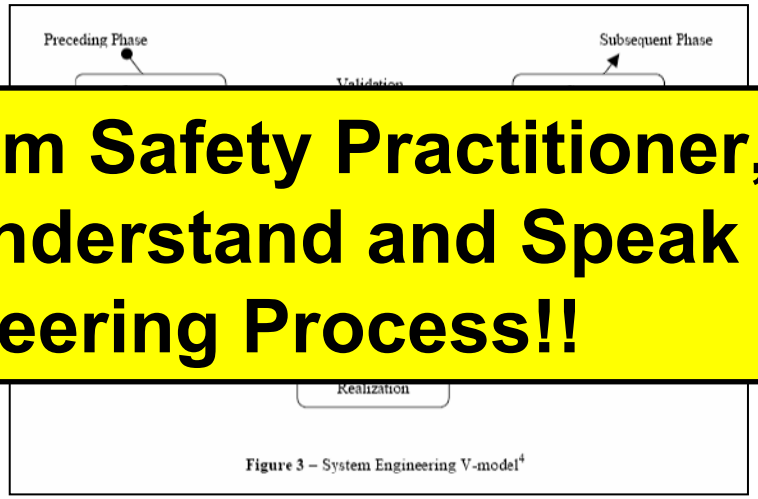
Important!

SURVICE ENGINEERING COMPANY

Conclusions

- **Requirements, Requirements, Requirements**
  - **The language of the systems & design engineers**
- **Integration of System Safety into System Engineering Framework is Critical**
- **Framework is the Key**
- **Conditions are Right (OSD is an Advocate)**
- **Must Understand and Spread the Word**





To be an Effective System Safety Practitioner, You Must Absolutely Understand and Speak the Systems Engineering Process!!