BAE SYSTEMS

Industry Perspectives and Identified Barriers to the Use of MIL-STD-882D for integrating ESOH Considerations into Systems

Jon Derickson, PE, CSP
Manager, FCS Environmental, Safety and Health
Ground Systems Division
BAE Systems, Land & Armaments

Outline

BAE SYSTEMS

- Systems and Safety Engineering
- MIL-STD-882D
- Potential Barriers for Integrating Safety into Systems Engineering

Systems and Safety Engineering

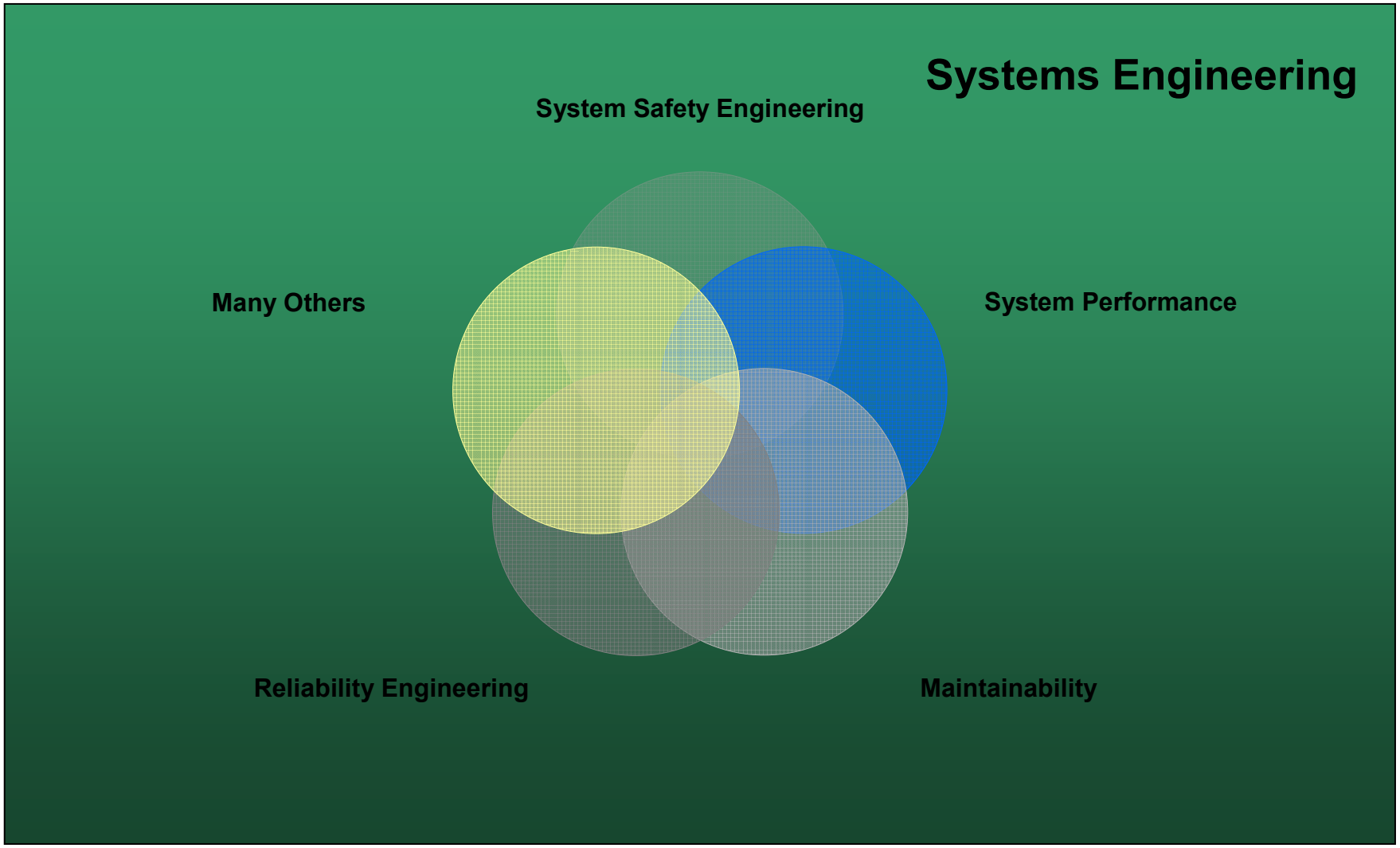
BAE SYSTEMS

- **Systems Engineering – The design of a complex interrelation of many elements (a system) to maximize an agreed upon measure of system performance, taking into consideration all of the elements related in any way to the system, including utilization of worker power as well as the characteristics of each of the system's components**
- **System Safety – The optimum degree of safety within the constraints of operational effectiveness, time and cost, attained through specific application of system safety engineering throughout all phases of a system**
- **System Safety Engineering – An element of systems management involving the application of scientific and engineering principles for the timely identification of hazards and initiation of those actions necessary to prevent or control hazards within the system**

Reference: McGraw-Hill Dictionary of Scientific and Technical Terms

One Aspect of Systems Engineering

BAE SYSTEMS



MIL-STD-882D Objectives

BAE SYSTEMS

- The DoD is committed to protecting:
  - private and public personnel from accidental death, injury, or occupational illness
  - weapon systems, equipment, material, and facilities from accidental destruction or damage
  - public property while executing its mission of national defense.
- Within mission requirements, the DoD will ensure that the quality of the environment is protected to the maximum extent practical.
- The DoD has implemented environmental, safety, and health efforts to meet these objectives. Integral to these efforts is the use of a system safety approach to manage the risk of mishaps associated with DoD operations.
- A key objective of the DoD system safety approach is to include mishap risk management consistent with mission requirements, in technology development by design for DoD systems, subsystems, equipment, facilities, and their interfaces and operation.
- The DoD goal is zero mishaps.

Major Elements of MIL-STD-882D

BAE SYSTEMS

- Document your approach
- Identify Hazards
- Assess Risk
- Identify hazard risk mitigations (requirements)
- Reduce the risks to acceptable levels
- Verify risk reduction
- Formally obtain approval of residual risk
- Conduct hazard tracking of hazards and risk

System Safety Objectives

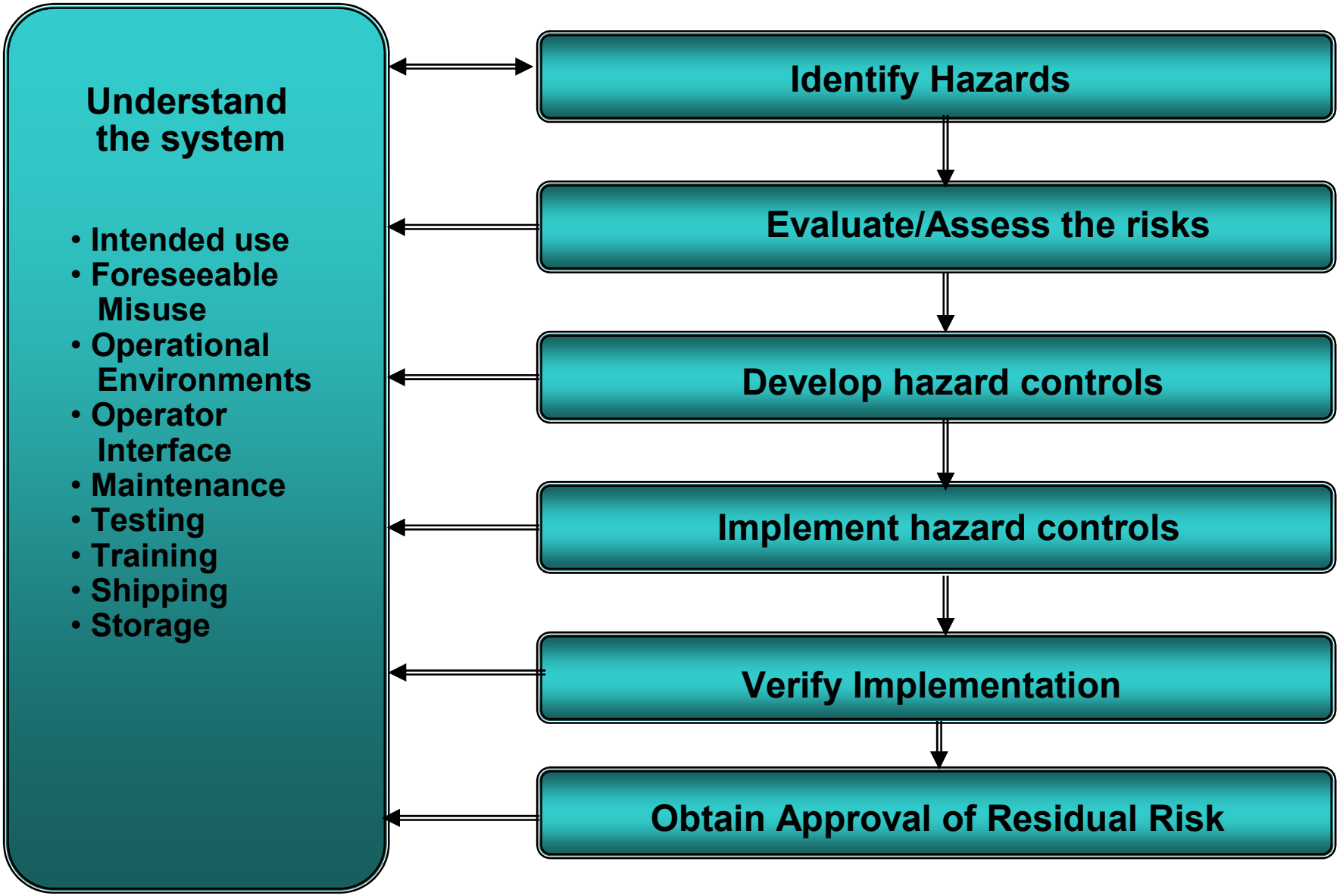
BAE SYSTEMS

"The principle objective of a system safety program within the DoD is to make sure safety, consistent with mission requirements, is included in technology development and designed into systems" (Ref MIL-STD-882C)

- **Safety, consistent with mission requirements is designed into the system**
- **Hazards are identified, tracked, evaluated, and eliminated or the risk is reduced to acceptable levels**
- **Historical safety data is considered and used in new designs**
- **Changes in design or mission requirements maintain an acceptable level of risk**
- **Significant safety data is documented as "lessons learned" for future development**

Overall System Safety Process

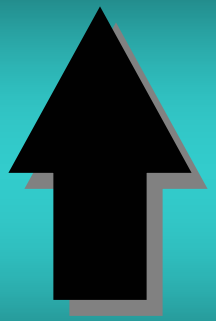
BAE SYSTEMS



Precedence for Hazard Mitigations

BAE SYSTEMS

Always do #1 first



1) Design to Eliminate Hazards
2) Incorporate Safety Devices
3) Provide Warning Indicators
4) Develop Procedures, Warnings, and Training

Work down the list only after previous items have proven not effective

Combinations of these controls are used to develop "System" of hazard controls

Potential Barriers – Speed Bumps

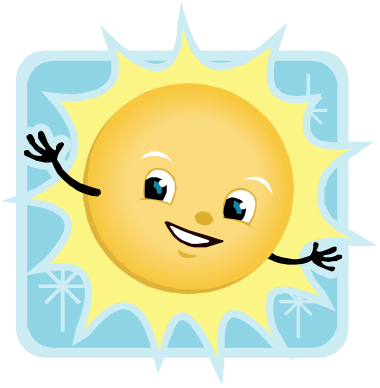
BAE SYSTEMS

- Systems engineers are not always familiar with System Safety approaches, terms and processes
- System safety engineers are not always familiar with systems engineering approaches, terms and processes
- Timing
  - Safety often gets involved too late in the process
  - They don't always know about key systems deadlines
  - They often are asked for inputs at the end – during document release process

Potential Barriers – Jersey Barriers

BAE SYSTEMS

- Process Barriers
- Tools Barriers
- Rainy Days and Sunny Days



Process Barriers

BAE SYSTEMS

- Systems engineering processes change significantly from program to program
  - Safety engineering needs to be involved in the definition of processes in addition to definition of safety requirements and constraints
- Bait and switch
  - Everyone agrees on one process and then the process is over-taken by program schedules and other events
- Hazard discovery often continues through system development so key requirements sometimes come late
- System safety is not a Key Process area for CMMI so it often gets left out of systems engineering processes

Tools Barriers

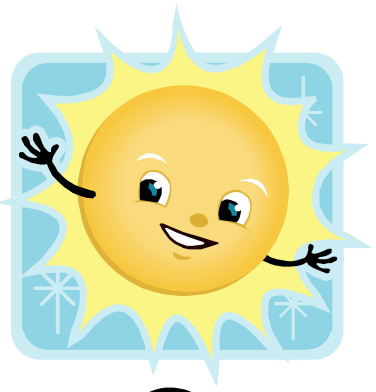
BAE SYSTEMS

- How to integrate hazard tracking into systems tools (UML, RTM, DOORS, etc)
  - Not always effective to implement tracking in the systems tool
  - This needs to be thought through early in a program to ensure effective implementation and to avoid false starts
- Different disciplines of systems engineering use different tools and/or different documents for different parts of a system
  - This often makes it difficult to fully specify hazard controls that thread through an entire system
  - We end up developing a safety view of mitigation approaches that captures hardware, software, and functional aspects of the system

Rainy Days and Sunny Days

BAE SYSTEMS

- Systems engineers are often concerned with what we WANT the system to do (Sunny Day Scenario's)
  - They strive for clear concise requirements that are verifiable



- Safety engineers are often concerned with what we DON'T want the system to do (Rainy Day Scenario's)
  - Accidents are often caused by a string of unlikely events
  - The combinations and permutations of possibilities become very complicated and is very difficult to clearly specify in neat little requirements at the beginning of a program

- Need to find Effective ways to capture what we <u>Don't Want</u> in a way that can be verified and validated

Summary

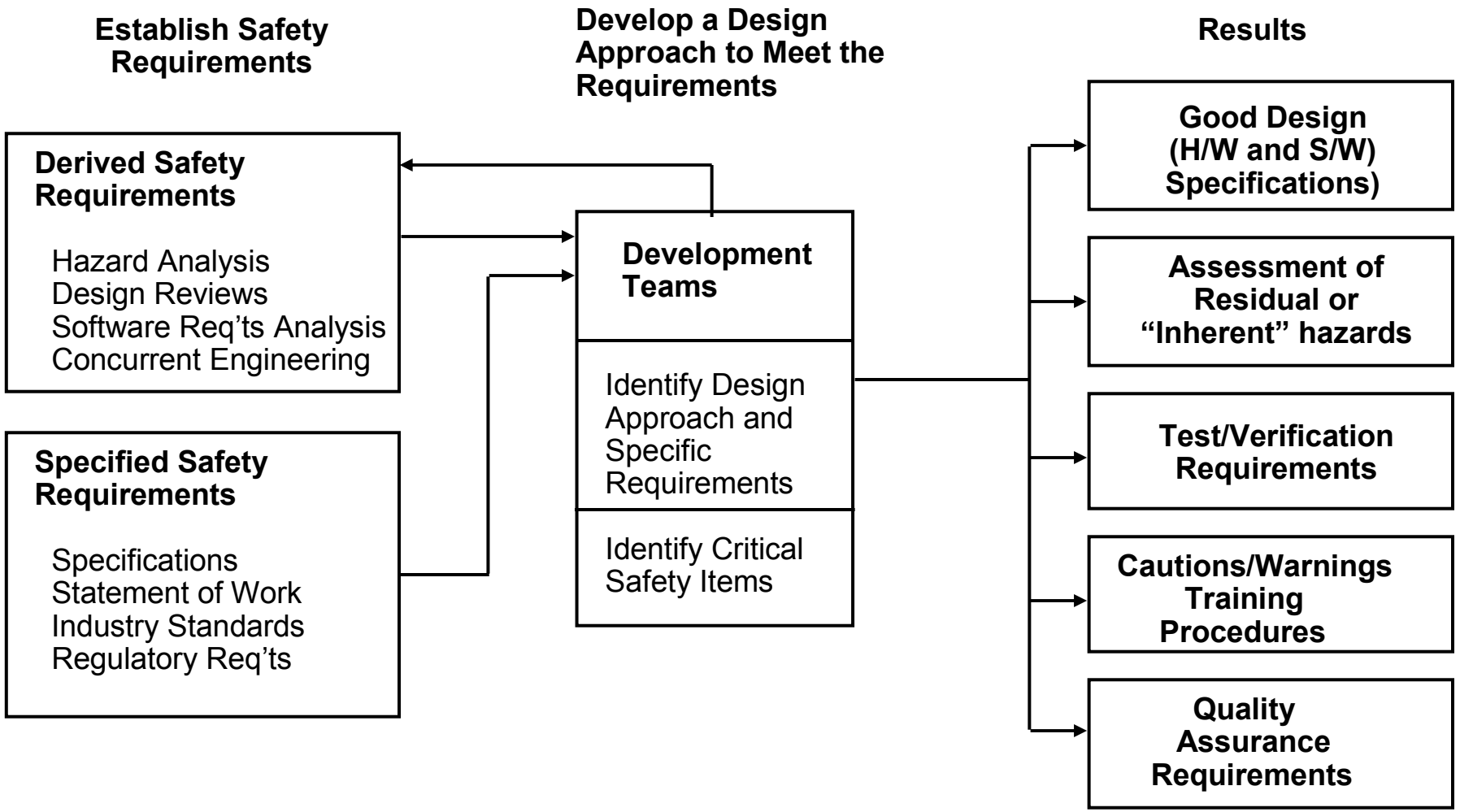
BAE SYSTEMS

- Recognize that system safety is part of systems engineering and sometimes plays a key role
  - Cultivate and nurture a cooperative environment between system safety and systems engineering
  - Make sure that system safety is integrated in the systems processes
  - Know when you need to get safety involved
- Make sure system safety is involved early in both requirements development and process development
  - Make sure they are aware of your processes and key deadlines
- Look for the win-win opportunities

BACKUP SLIDES

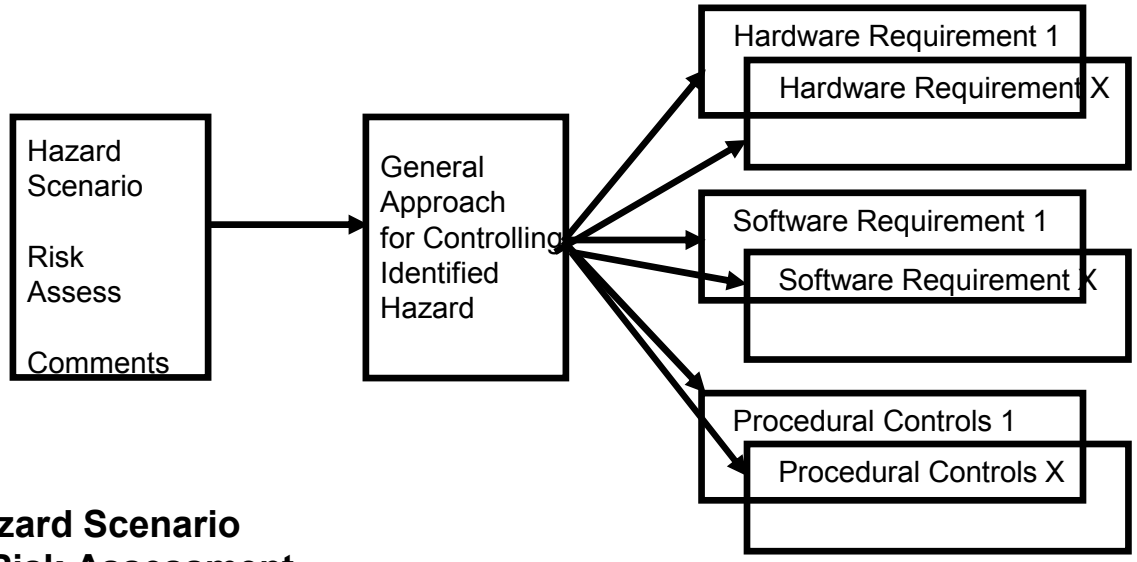
System Safety Approach

BAE SYSTEMS



Hazard Control Development

BAE SYSTEMS



Hazard Scenario & Risk Assessment

- Description of Concern
- Effects on People & Equipment
- Risk Assessment
  - Probability
  - Severity
  - Risk Assessment Code
- Background Information

Documented in Hazard Tracking System

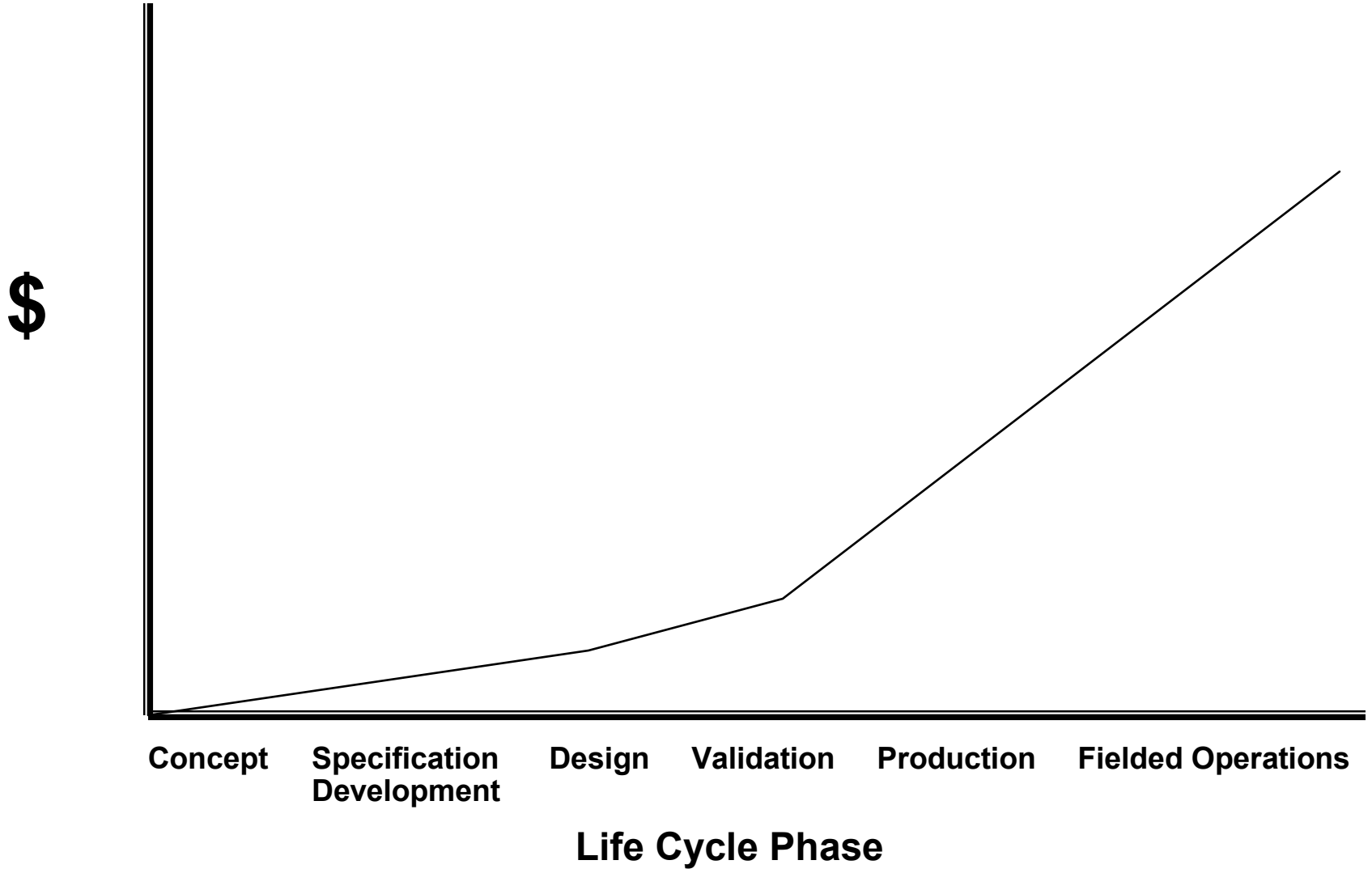
Hazard Controls

- Design Approach
- Software Requirements
- Hardware Requirements
- Interface Requirements
- Warnings and Cautions
- Procedures

Documented in Hazard Tracking System and Software Safety Tracking System

Cost of Safety Changes

BAE SYSTEMS



Risk Assessment Criteria

BAE SYSTEMS

SEVERITY

Category	Level	Description
Catastrophic	I	Event results in death, permanent total disability, loss of FCS assets exceeding $1M, or irreversible severe environment damage that violates law or regulation and/or FCS Program stoppage.
Critical	II	Event results in permanent partial disability, injuries or occupational illness that may result in hospitalization of > 5 days, loss of FCS assets exceeding $200K but less than $1M, or a reversible environment damage causing a violation of law/regulation, or a FCS Program delay.
Marginal	III	Event results in injury or occupational illness resulting in hospitalization of < 5 days, loss exceeding $40K but less than $200K, or mitigatible environment damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Event results in injury or illness not resulting in hospitalization of < 1 day, loss exceeding $2K but less than $40K, or minimal environment damage not violating law or regulation.

PROBABILITY

Qualitative Description			
Level	**Likelihood**	**Individual Item**	**Fleet or Inventory**
A	Frequent	Likely to occur often in the life of an item, with a probability of occurrence greater than 1×10^{-1} in that life.	Continuously experienced.
B	Probable	Will occur several times in the life of an item, with a probability of occurrence less than 1×10^{-1} but greater than 1×10^{-2} in that life.	Will occur frequently.
C	Occasional	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 1×10^{-3} in that life.	Will occur several times.
D	Remote	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 1×10^{-6} in that life.	Unlikely, but can reasonably be expected to occur.
E	Improbable	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 1×10^{-6} in that life.	Unlikely to occur, but possible.
F	Extremely Improbable	So improbable, it can be assumed occurrence is impossible probability of occurrence less than 1×10^{-7} in item life.	Extremely unlikely to occur, but not impossible.

FCS Hazard Risk Management Matrix

BAE SYSTEMS

Hazard Severity	Probability of Occurrence					
	Frequent (A)	Probable (B)	Occasional (C)	Remote (D)	Improbable (E)	Extremely Improbable (F)
Catastrophic (I)	High	High	High	Medium	Medium	Low
Critical (II)	High	High	Medium	Medium	Low	Low
Marginal (III)	Medium	Medium	Medium	Low	Low	Low
Negligible (IV)	Low	Low	Low	Low	Low	Low

Hazard Decision Authority Matrix

Residual Risk	Integrating Contractor Risk Acceptance	Government Risk Acceptance
HIGH	Program Director/Senior Leadership	Army Acquisition Executive (AAE)
MEDIUM	Program Manager and Technical Director	Program Executive Officer (PEO)
LOW	Technical Director	MGV Program Manager (MGV-PM)

Bio for Jon Derickson

BAE SYSTEMS

Jon S. Derickson, PE, CSP, Manager FCS ESOH, BAE Systems, PO Box 58123, MD C16, Santa Clara, CA 95052 USA, telephone - (408) 289-4797, e-mail – jon.derickson@baesystems.com.

Mr. Derickson is currently the Manager for Environment, Safety and Occupational Health for the Future Combat System (FCS) Programs at BAE Systems - Ground Systems Division in Santa Clara, CA. He was previously the System Safety Group Lead for Bradley Fighting Vehicle Systems.

He has a Bachelor of Science in Agricultural Engineering from California Polytechnic State University in San Luis Obispo, CA and a Masters in Computer Engineering from San Jose State University. He is a Registered Professional Safety Engineer and a Certified Safety Professional in system safety. He has over 20 years experience in system safety that includes commercial products, military combat vehicles, explosive devices, large rocket motor manufacturing, and autonomous ground vehicles.