BAE SYSTEMS

Hazard Tracking System
Purpose, Design & Implementation

Jon Derickson, PE, CSP
Manager, Product Safety
US Combat Systems

Jon.Derickson@baesystems.com
(408) 234-4301

Agenda

- Key Concepts
- HTS Purpose and Objectives
- System Safety Approach
- Hazard Analysis Approach
- Hazard Analysis Process
- Risk Assessment
- Hazard Control Development
- Closed Loop Hazard Tracking Process
- Hazard Status
- HTS Data Structure
- Kinds of Reports and Output Data

Key Concepts

- Hazard Analysis vs Hazard Tracking
  - A hazard tracking system is not necessarily a hazard analysis tool
- The Hazard Tracking System is a <u>Tool</u> to facilitate a process
  - Design must support the process
  - The process may have several objectives
  - The design of the tool depends on the needs of the stakeholders who need information to manage the process

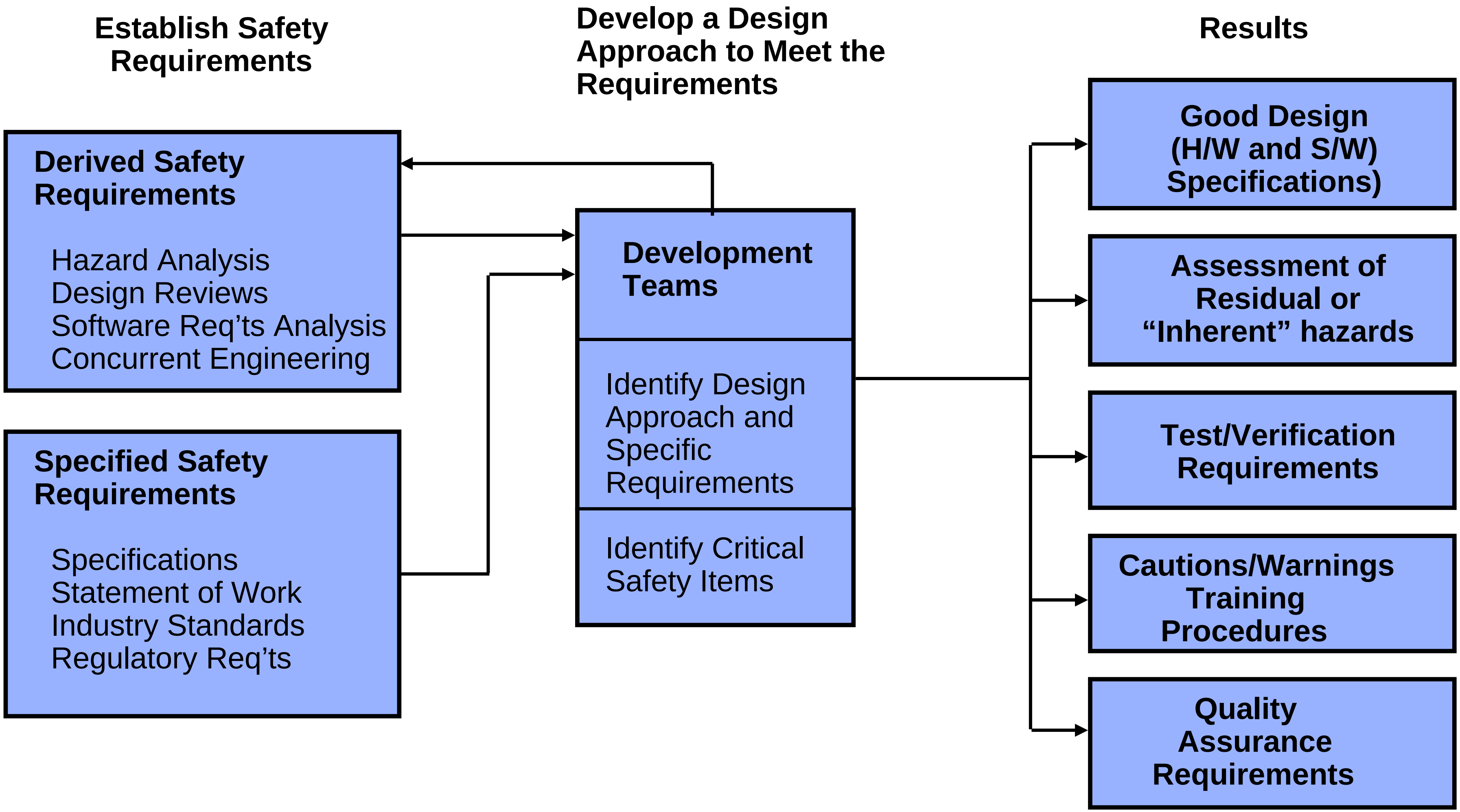
HTS Purpose and Objectives

- Purpose
  - To effectively manage hazard analysis data and facilitate a hazard discovery and hazard risk mitigation process

- Objectives
  - Provide a means to effectively influence design to ensure that safety is optimized in a system
  - Provide data and information necessary to effectively manage risk
  - Document approaches, decisions and actions taken to eliminate or reduce risks of hazards
  - Provide a method for closed loop tracking of actions and/or decisions
  - Provide means for effectively organizing, managing, and updating hazard data

System Safety Approach

BAE SYSTEMS



Establish Safety Requirements

Develop a Design Approach to Meet the Requirements

Results

Derived Safety Requirements

Hazard Analysis
Design Reviews
Software Req'ts Analysis
Concurrent Engineering

Specified Safety Requirements

Specifications
Statement of Work
Industry Standards
Regulatory Req'ts

Development Teams

Identify Design Approach and Specific Requirements

Identify Critical Safety Items

Good Design (H/W and S/W) Specifications)

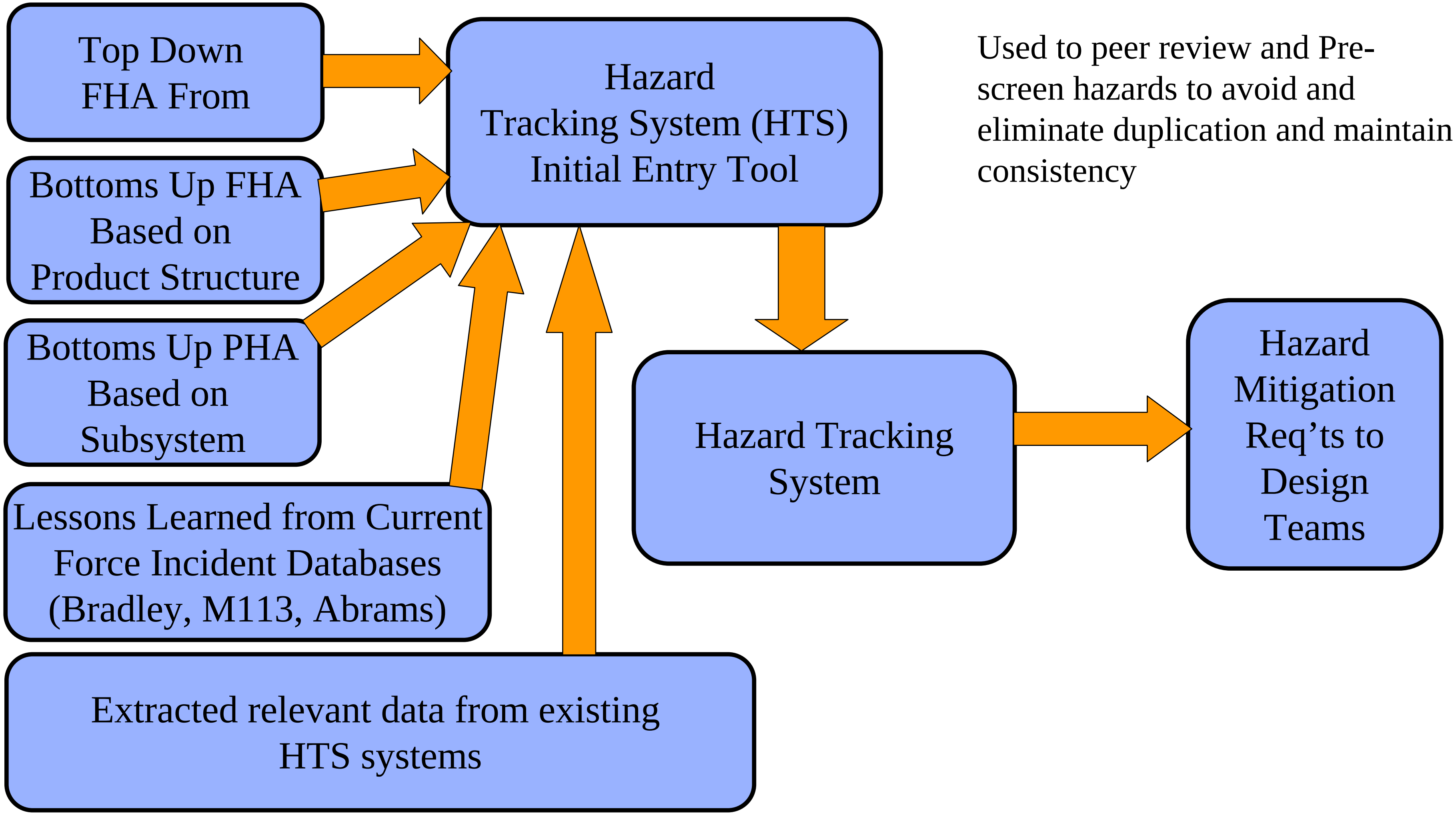
Assessment of Residual or "Inherent" hazards

Test/Verification Requirements

Cautions/Warnings Training Procedures

Quality Assurance Requirements

Hazard Analysis – Approach



Top Down FHA From

Bottoms Up FHA Based on Product Structure

Bottoms Up PHA Based on Subsystem

Lessons Learned from Current Force Incident Databases (Bradley, M113, Abrams)

Extracted relevant data from existing HTS systems

Hazard Tracking System (HTS) Initial Entry Tool

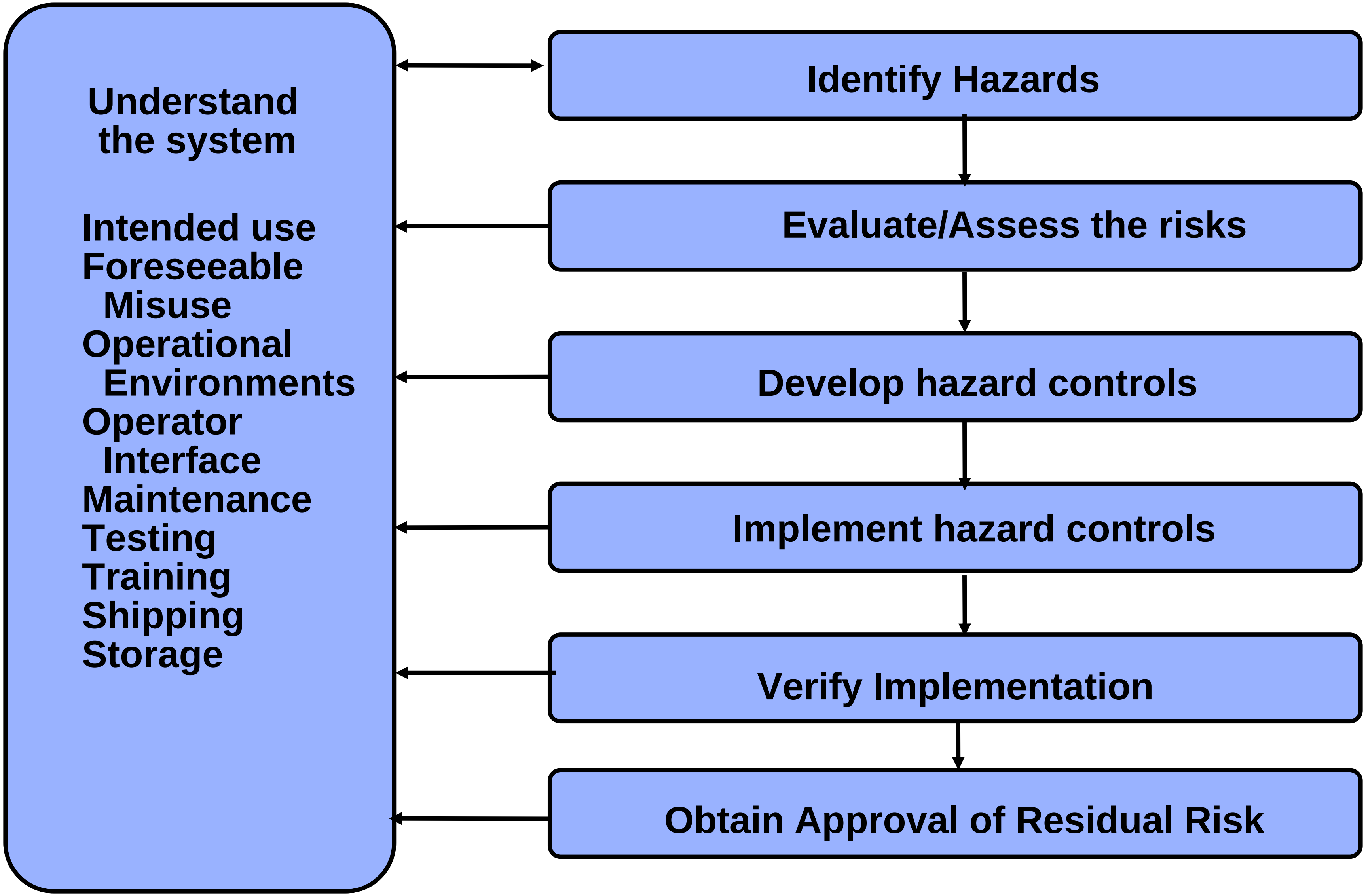
Used to peer review and Pre-screen hazards to avoid and eliminate duplication and maintain consistency

Hazard Tracking System

Hazard Mitigation Req’ts to Design Teams

Hazard Analysis Process

BAE SYSTEMS



Understand the system

Intended use
Foreseeable Misuse
Operational Environments
Operator Interface
Maintenance
Testing
Training
Shipping
Storage

Identify Hazards

Evaluate/Assess the risks

Develop hazard controls

Implement hazard controls

Verify Implementation

Obtain Approval of Residual Risk

Risk Assessment Criteria

SEVERITy

Category	Level	Description
Catastrophic	**I**	**Event results in death, permanent total disability, loss of assets exceeding $1M, or irreversible severe environment damage that violates law or regulation and/or Program stoppage.**
Critical	**II**	**Event results in permanent partial disability, injuries or occupational illness that may result in hospitalization of > 5 days, loss of assets exceeding $200K but less than $1M, or a reversible environment damage causing a violation of law/regulation, or a 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 x 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 x 10^{-1} but greater than 1 x 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 x 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 x 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 x 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 x 10^{-7} in item life.**	**Extremely unlikely to occur, but not impossible.**

Hazard Risk Management Matrix

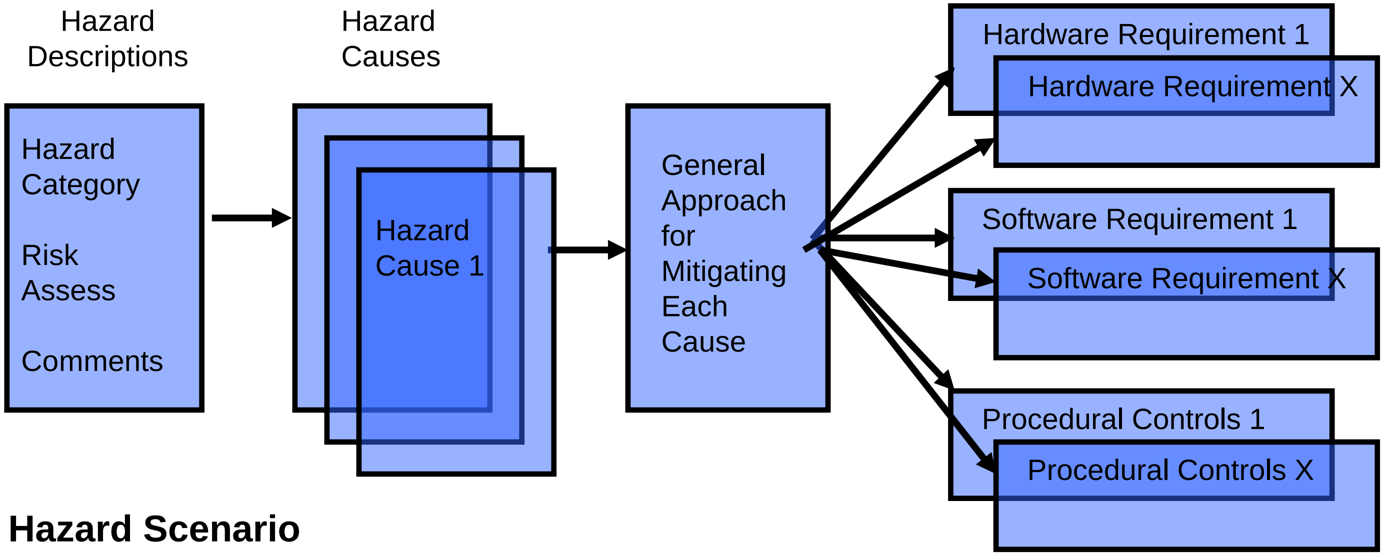
Hazard Severity	Probability of Occurrence					
	Frequent (A)	Probable (B)	Occasional (C)	Remote (D)	Improbable (E)	Extremely Improbable (F)
Catastrophic (I)	**High**	**High**	**High**	**Medium**	**Medium**	**Low**
Critical (II)	**High**	**High**	**Medium**	**Medium**	**Low**	**Low**
Marginal (III)	**Medium**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

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

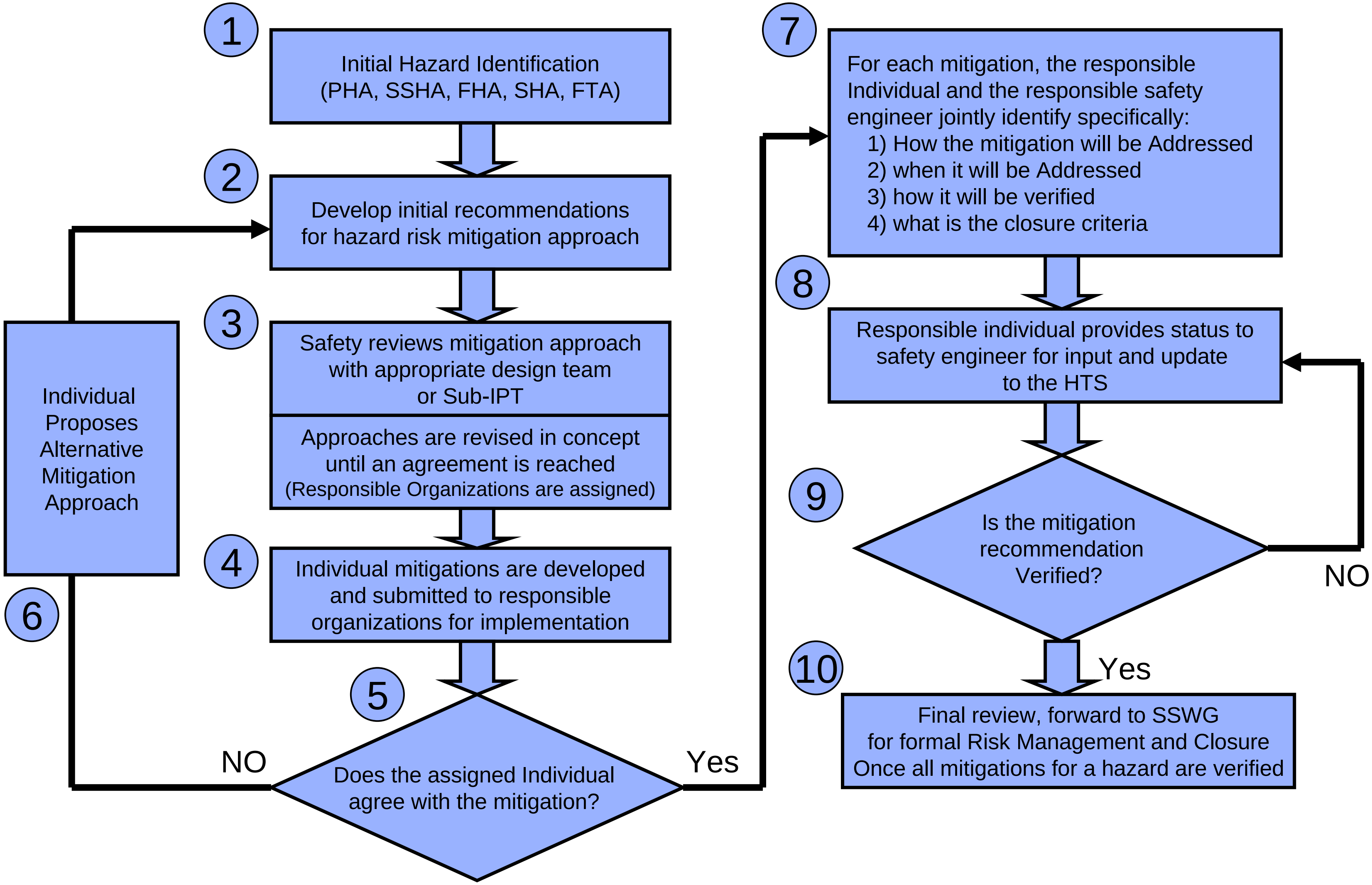
Hazard Controls

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

Documented in Hazard Tracking System

Closed Loop Hazard Tracking Process

BAE SYSTEMS



1
Initial Hazard Identification
(PHA, SSHA, FHA, SHA, FTA)
2
Develop initial recommendations
for hazard risk mitigation approach
3
Safety reviews mitigation approach
with appropriate design team
or Sub-IPT
Approaches are revised in concept
until an agreement is reached
(Responsible Organizations are assigned)
4
Individual mitigations are developed
and submitted to responsible
organizations for implementation
5
Does the assigned Individual
agree with the mitigation?
NO
Yes
6
Individual
Proposes
Alternative
Mitigation
Approach
7
For each mitigation, the responsible
Individual and the responsible safety
engineer jointly identify specifically:
1) How the mitigation will be Addressed
2) when it will be Addressed
3) how it will be verified
4) what is the closure criteria
8
Responsible individual provides status to
safety engineer for input and update
to the HTS
9
Is the mitigation
recommendation
Verified?
NO
Yes
10
Final review, forward to SSWG
for formal Risk Management and Closure
Once all mitigations for a hazard are verified

Hazard Status

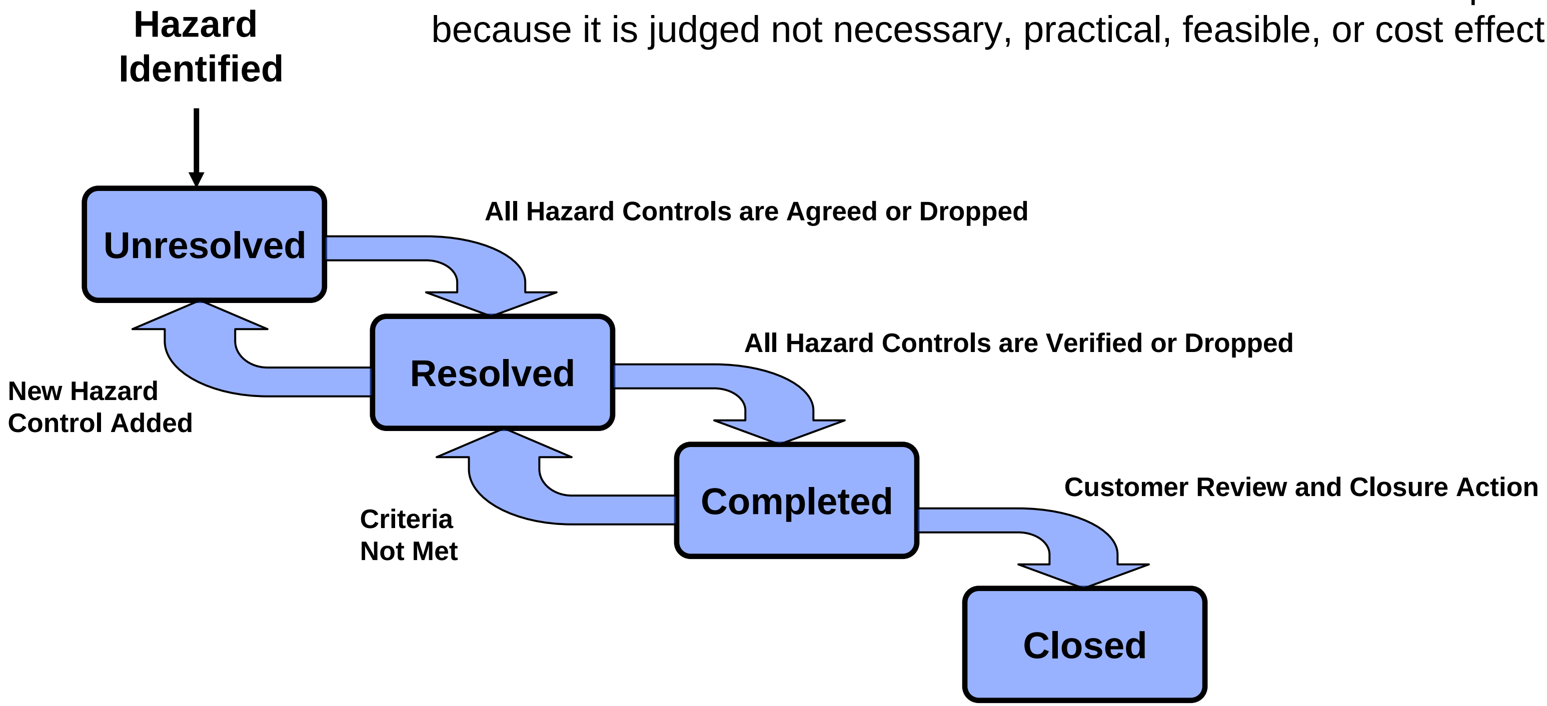
Provide Status of Individual Hazard Controls

OPEN - Indicates that a recommendation has been made to engineering but action to be taken is not established.

AGREED - Indicates that the recommendation has been accepted, and action will be taken. However, implementation is not been verified.

VERIFIED - Indicates that the recommended action has been taken, and implementation is verified.

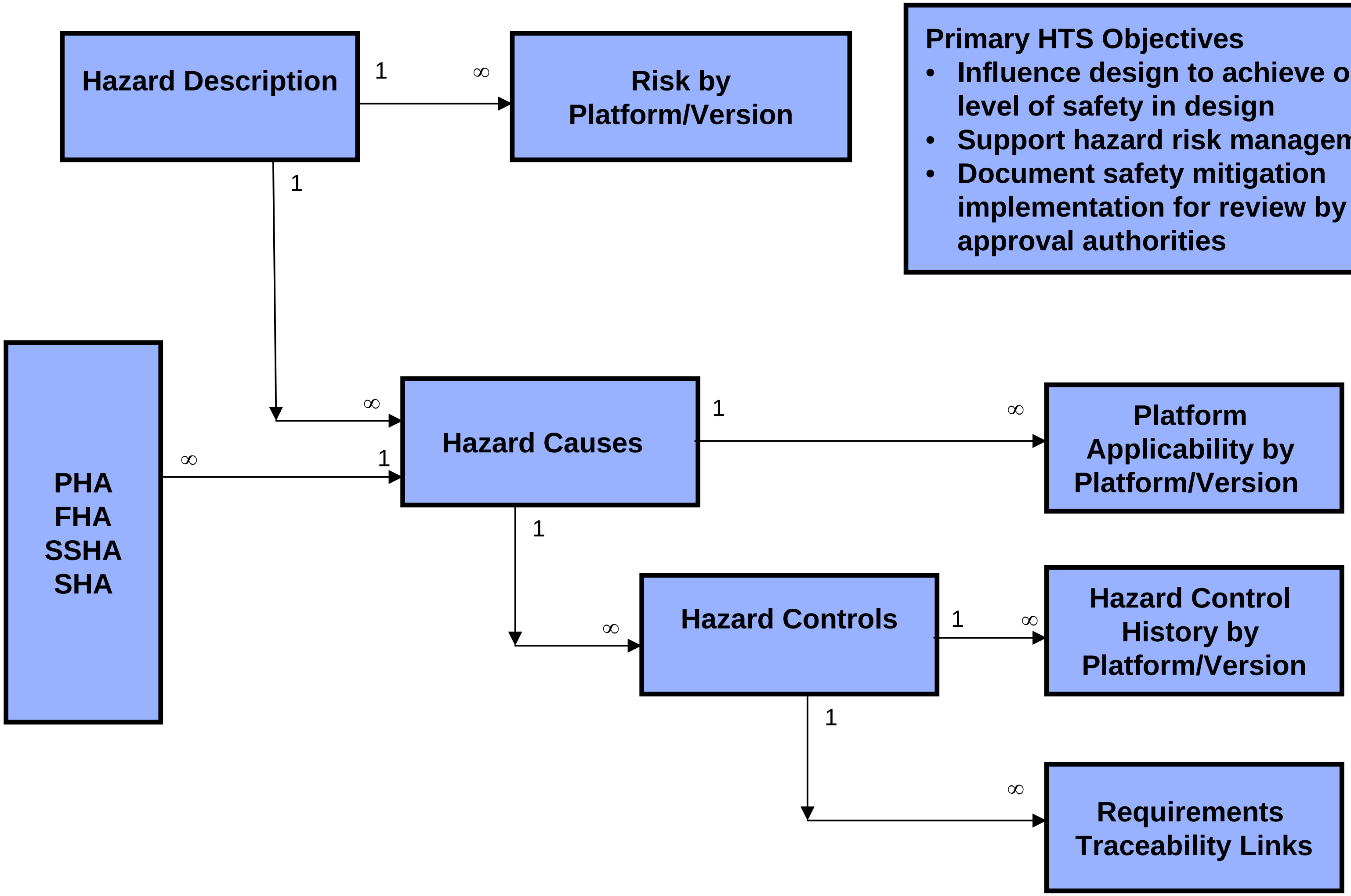
DROPPED - Indicates that the recommended action will not be implemented because it is judged not necessary, practical, feasible, or cost effective.


Hazard Identified
Unresolved
All Hazard Controls are Agreed or Dropped
Resolved
New Hazard Control Added
All Hazard Controls are Verified or Dropped
Completed
Criteria Not Met
Customer Review and Closure Action
Closed

HTS Data Structure

Primary HTS Objectives

- Influence design to achieve optimum level of safety in design
- Support hazard risk management
- Document safety mitigation implementation for review by various approval authorities



Hazard Description

Risk by Platform/Version

PHA
FHA
SSHA
SHA

Hazard Causes

Platform Applicability by Platform/Version

Hazard Controls

Hazard Control History by Platform/Version

Requirements Traceability Links

Reports and Output Data

- Hazard Lists and Hazard Reports
  - by Vehicle
  - by Subsystem
  - by Hazard
- Working Level Reports
- Hazard Metrics
- Risk Metrics
- Various specialized reports

Hazard Tracking System Examples

Questions?

BACKUP SLIDES