

System Safety 101

Course Improvements Since ISSC 2010

ISSC 2010 Feedback Forms

- Introduction of Attendees
- More, real examples (visual, if possible)
- Remove yellow and light green colors on slides
- More Hardware coverage
- Less Software coverage
- Treatment of uncertainty, how good are the estimates, random variables, modeling/parameter uncertainties

WISE Alignment

System Safety 101

Raytheon Missile Systems

Jean Sauerman

Jean_Sauerman@Raytheon.com

August 2011

Disclaimer:

The following presentation presents the development and implementation of a fictitious US Navy (USN) system safety program from a contractor's perspective. The vast majority of the presentation is also applicable for US Army and US Air Force programs as well. Where differences apply, it will be so stated.

System Safety 101

Purpose:

The following presentation will not make you an expert in System Safety Engineering. Hopefully, it will give a top-level understanding of the main tasks/analyses we perform, an idea of how to perform them and when each of them should be performed. Your co-workers can help provide additional details as required.

There is no need to memorize these slides, just remember you have them as a reference

System Safety 101

Acronyms

AFD – Arm Fire Device
AFSRB – Army Fuze Safety Review Board
APE – Ammunition Peculiar Equipment
APL – Approved Parts List
BI – Bullet Impact
BOE – Basis of Estimate
BPA – Bent Pin Analysis
CCB – Configuration Control Board
CD – Command Destruct
CDR – Critical Design Review
CDRL – Contract Data Requirements List
CI – Configuration Item
CM – Configuration Management
ConOps – Concept of Operations
COTS – Commercial Off The Shelf
CSC – Computer Software Component
CSCI – Computer Software Configuration Item
DFD – Design For Demil
DFE – Design For Environment
DM – Data Management
DM&D – Demil & Disposition
DM&DP – Demil & Disposition Program
DoD – Department of Defense
E³ – Electromagnetic Environmental Effects
ECP – Engineering Change Proposal
EEPROM – Electrically Erasable Programmable Read-Only Memory
EHC – Explosive, Hazardous, Classified
EHS – Environmental, Health and Safety

System Safety 101

Acronyms

EMC – Electromagnetic Compatibility
EMI – Electromagnetic Interference
EOD – Explosive Ordnance Disposal
ESOH – Environmental, Safety, and Occupational Health
ETS – Environmental Trade Study
FCO – Fast Cook Off
FHC – Final Hazard Classification
FI – Fragment Impact
FISTRP – Fuze and Initiation Systems Technical Review Panel
FMEA – Failure Modes Effects Analysis
FMECA – Failure Modes, Effects and Criticality Analysis
FTA – Fault Tree Analysis
FTS – Flight Termination System
FW – Firmware
GFE – Government Furnished Equipment
HAR – Hazard Action Report
HAT – Hazard Assessment Test
HHA – Health Hazard Assessment
HMMP – Hazardous Material Management Plan
HSI – Human/System Interface
HTS – Hazard Tracking System
IHC – Interim Hazard Classification
ILA – Inadvertent Launch Analysis
IM – Insensitive Munitions
IPT – Integrated Product Team
LRIP – Low Rate Initial Production
MA – Managing Activity
MRC – Maintenance Requirement Card
MREB – Munitions Reaction Evaluation Board
MSDS – Material Safety Data Sheet
MTBF – Mean Time Between Failure

System Safety 101

Acronyms

NDI – Non Development Item
NNMSB – Non Nuclear Munition Safety Board
NOSSA – Naval Ordnance Safety and Security Activity
O&SHA – Operating & Support Hazard Analysis
PDA – Preliminary Demil Assessment
PDR – Preliminary Design Review
PESHE – Programmatic Environmental Safety & Health Evaluation
PFS – Principal for Safety
PHA – Preliminary Hazard Analysis
PHL – Preliminary Hazard List
RA – Review Authority
RCM – Requirements Compliance Matrix
RFP – Request For Proposal
RSDP – Range Safety Data Package
SAD – Safe/Arm Device
SAR – Safety Assessment Report
SCB – Slow Cookoff Bomb
SCCB – Software Configuration Control Board
SCCSC – Safety Critical Computer Software Component
SCI – Safety Criticality Index
SCJ – Shaped Charge Jet
SCM – Software Configuration Management
SCO – Slow Cook Off
SCR – Safety Critical Requirement
SD – Self Destruct
SE – Systems Engineer

System Safety 101

Acronyms

SEU – Single Event Upset
SFR – System Functional Review
SHA – System Hazard Analysis
SOO – Statement of Objectives
SOW – Statement of Work
SQE – Software Quality Engineering
SR/CA – Safety Requirements/Criteria Analysis
SRAM – Static Random Access Memory
SRR – System Requirements Review
SRS – Software Requirements Specification
SSCI – Software Safety Criticality Index
SSER – System Safety Engineering Report
SSHA – Subsystem Hazard Analysis
SSPP – System Safety Program Plan
SSSTRP – Software Systems Safety Technical Review Panel
SSWG – System Safety Working Group
STLH – Software Top Level Hazard
SwE – Software Engineer
SwHA – Software Hazard Analysis
SwSPP – Software Safety Program Plan
T&E – Test and Evaluation
TE – Test Equipment
TESTRP – Test Equipment System Technical Review Panel
THA – Threat Hazard Assessment
TIM – Technical Interchange Meeting
TLH – Top Level Hazard
USN – United States Navy
WISE – WSESRB Interactive Safety Environment
WSESRB – Weapon System Explosives Safety Review Board

System Safety 101

AGENDA

- **Before You Start**
- **Pre-Preliminary Design Review**
 - System Safety Program Plan
 - Software Safety Program Plan
 - Preliminary Hazard List/Preliminary Hazard Analysis
 - Threat Hazard Assessment
 - Hazard Assessment Test Plan
 - Safety Requirements/Criteria Analysis
 - Operating & Support Hazard Analysis
 - Health Hazard Assessment
 - Safety Assessment Report
 - Review Authority Evolutions
 - Design For Environment Tasks
 - Environmental Trade Study
 - Hazardous Material Management Program Plan
 - Demilitarization and Disposition Program Plan
 - Preliminary Demil Assessment
 - Design For Environment Analysis
 - Design For Demil Analysis
 - Hazardous Material Management Program Report
- **Pre-Critical Design Review**
 - Subsystem Hazard Analysis
 - System Hazard Analysis
 - System Safety Engineering Report
 - Explosive Ordnance Disposal Data Package
 - Explosive Hazard Classification Data Report
 - Technical Data for Munitions
- **Pre-First Flight Test**
 - Range Safety Data Package
 - DM&DP Plan and Report
- **Other Analyses**
 - Fault Tree Analysis
 - Bent Pin Analysis
 - Inadvertent Launch Analysis
- **Other Topics**
 - Test Set Safety Process
 - Configuration Management
 - Engineering Change Proposals, Deviations, Waivers
 - Hazard Tracking
 - Hazard Action Report

System Safety 101

Before You Start

- Request For Proposal (RFP)
 - Proposal Support
 - Compliance, Compliance, Compliance
- Understanding the Program from the Contractor's Perspective
 - Schedule
 - Deliverables

System Safety 101

Before You Start – RFP – Proposal Support

- A contractor's proposal effort typically has proposal and program managers, Book Bosses, and systems lead
 - System Safety inputs are normally addressed in the Technical Volume/Management Volume or both
- Technical Volume inputs address specific design and test requirements
- Management Volume may require the generation of a System Safety Program Plan (SSPP)
 - What you put in the SSPP is binding, so ensure all tasks identified are adequately funded
 - Make sure all tasks call out in the RFP/Performance Spec/Statement of Work (SOW)/Statement of Objectives (SOO) are addressed in the SSPP
 - Make sure SSPP is compliant with MIL-STD-882 and DI-SAFT-80100
 - Hard to balance between technical SSPP and marketing document

System Safety 101

Before You Start – RFP – Proposal Support

- Page count limitations may be imposed, especially in the Technical Volume
- Must be concise yet consistent with “win themes”
- Don’t regurgitate requirements back
 - Requirement: Hazards identified during testing shall also be assessed and tracked to resolution.
 - Bad - Hazards identified during testing will also be assessed and tracked to resolution.
 - Better - All test anomalies will be reviewed to determine their impact on the safety of the system. Those anomalies that are considered to have a safety impact will have a Hazard Action Report (HAR) generated and tracked as described in paragraph XXX.

System Safety 101

Before You Start – RFP – Proposal Support

- Things to keep in mind
 - Listen to the customer and what they want
 - KISS
 - # Don't overcomplicate when simple will do
 - # Don't give more than what's required if it drives cost, high tech = cost/risk
 - Poor Red/Gold team reviews
 - Difficult to follow write-up, try to respond to requirements in the same order as listed
 - Basis Of Estimates (BOEs) – If proposal/program management decrees a budget cut, modify the SSPP/write up accordingly and identify where non-compliance may be an issue
 - If cuts are too deep, check with legal to ensure Contractor Defense is still valid
 - Product was built pursuant to reasonably precise, government approved specifications
 - Product conformed in all material respects to the approved specification package
 - Contractor warned the government of those hazards related to the product actually known to the contractor but not known to the government
 - **Non-compliant submittal**

System Safety 101

Before You Start – RFP – Proposal Support

- Requirements are found in the Specifications, Standards, & Related Documents; CDRLs; RFP; SOW/SOO; Contract T&Cs
 - SOW establishes and defines all requirements for contractor efforts (WISE course)
 - SOO establishes and defines a broad description of the government’s required performance objectives (WISE course)
- Dependent upon the quality of the RFP, the safety requirements may be contained in a dedicated paragraph or throughout the documents
 - Either way, review of all documents is required to ensure safety or safety-related requirements are not overlooked
 - Remember, when supporting a proposal effort, Human Factors Engineering requirements also need to be addressed
- Requirements are identified as “SHALL” statements
 - Proposal manager will need to provide direction on responding to “Must”, “Will” or “Should” statements

System Safety 101

Before You Start – RFP – Compliance, Compliance, Compliance

- Each “SHALL” statement is a requirement and must be addressed
 - At beginning of proposal support, generate a Requirements Compliance Matrix (RCM)
 - RCM identifies each requirement (SHALL statement) as a separate entry, don’t place entire paragraph as a single entry
 - RCM identifies where in the proposal response each requirement is addressed
- Trace each requirement and make certain as the proposal is modified, the RCM is maintained
 - It’s OK to combine certain requirements, but make sure the reviewer can easily identify which requirement is being addressed
 - May be helpful to have response in the same order as the requirements

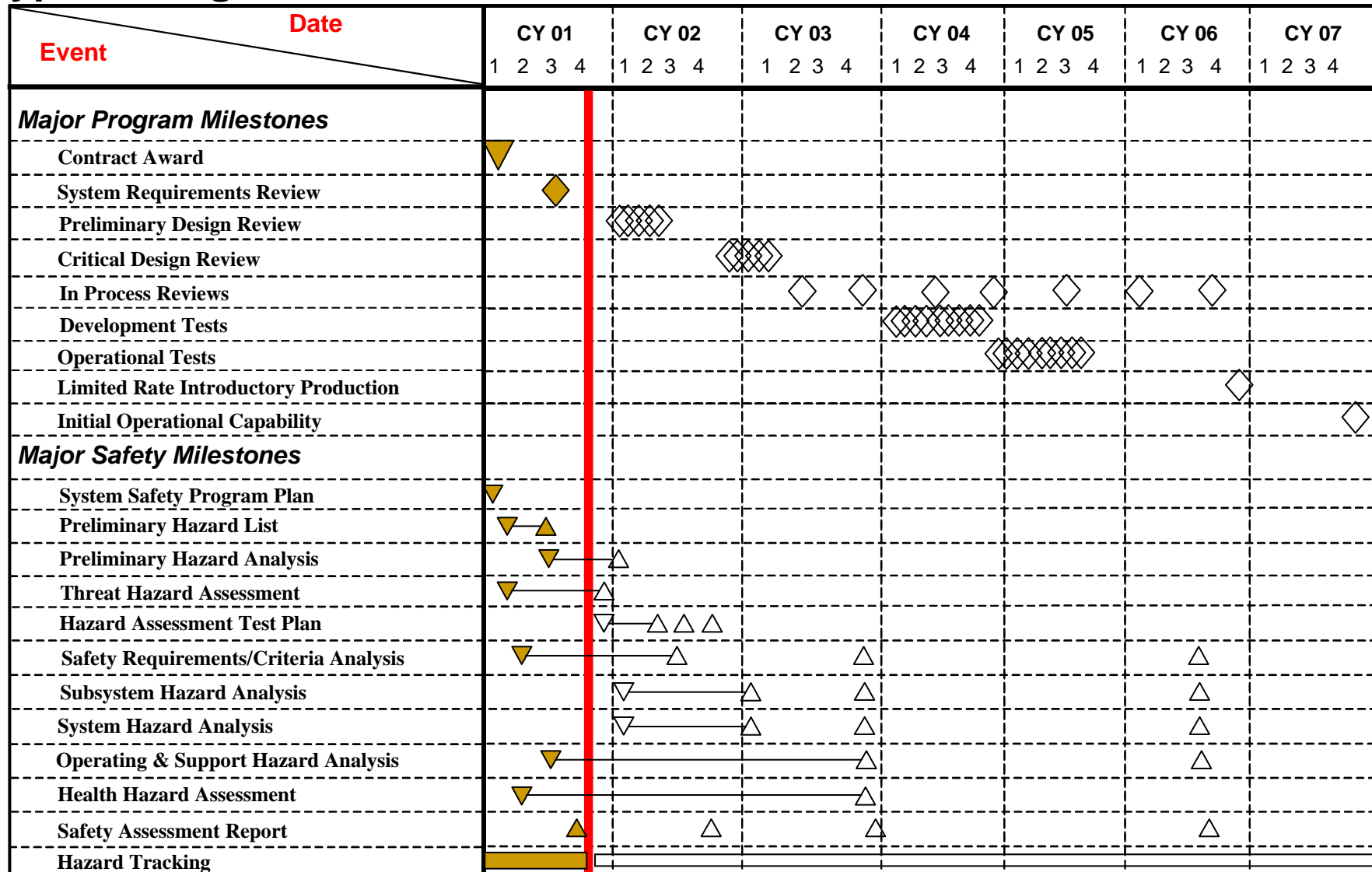
System Safety 101

Before You Start – Understanding the Program

- A key item in support of the proposal is understanding the program schedule and the type of development (spiral or traditional)
 - The program schedule will drive the system safety program schedule
 - The type of development will drive the frequency of deliverables
- A typical schedule is provided

System Safety 101

Typical Program Schedule with Traditional Deliverables



System Safety 101

AGENDA

- **Before You Start**
- **Pre-Preliminary Design Review**
 - **System Safety Program Plan**
 - **Software Safety Program Plan**
 - **Preliminary Hazard List/Preliminary Hazard Analysis**
 - **Threat Hazard Assessment**
 - **Hazard Assessment Test Plan**
 - **Safety Requirements/Criteria Analysis**
 - **Operating & Support Hazard Analysis**
 - **Health Hazard Assessment**
 - **Safety Assessment Report**
 - **Review Authority Evolutions**
 - **Design For Environment Tasks**
 - **Environmental Trade Study**
 - **Hazardous Material Management Program Plan**
 - **Demilitarization and Disposition Program Plan**
 - **Preliminary Demil Assessment**
 - **Design For Environment Analysis**
 - **Design For Demil Analysis**
 - **Hazardous Material Management Program Report**
- **Pre-Critical Design Review**
 - **Subsystem Hazard Analysis**
 - **System Hazard Analysis**
 - **System Safety Engineering Report**
 - **Explosive Ordnance Disposal Data Package**
 - **Explosive Hazard Classification Data Report**
 - **Technical Data for Munitions**
- **Pre-First Flight Test**
 - **Range Safety Data Package**
 - **DM&DP Plan and Report**
- **Other Analyses**
 - **Fault Tree Analysis**
 - **Bent Pin Analysis**
 - **Inadvertent Launch Analysis**
- **Other Topics**
 - **Test Set Safety Process**
 - **Configuration Management**
 - **Engineering Change Proposals, Deviations, Waivers**
 - **Hazard Tracking**
 - **Hazard Action Report**

System Safety Program Plan

System Safety 101

System Safety Program Plan (SSPP)

- Identified as Task #102 in MIL-STD-882
- Specified in Data Item Descriptions DI-SAFT-80100A and DI-SAFT-81626

What Does That Mean?

- The SSPP is the basis of understanding between the contractor and the customer for what will the system safety program be
 - The SSPP tells the “HOW” the safety program will be run and what will be done
- *Vehicle for safety task planning and estimating that describes*
 - *What safety tasks will be performed*
 - *When the safety tasks will be conducted and completed*
 - *Why the safety tasks are to be conducted*
 - *Who will conduct the safety tasks*

System Safety 101

System Safety Program Plan

- Initial SSPP may be performed in support of the proposal
 - Be careful with this delivery – Contents of this SSPP may be considered contractually binding
- Post Contract Award, the SSPP may be updated as a result of customer discussions, or initial delivery may be made
- The SSPP may be periodically updated
 - May be delivered as a Contract Data Requirements List (CDRL) with specified update frequency
 - Should reflect current agreements between you and the customer

System Safety 101

SSPP – What goes in it?

- The SSPP should include the following, at a minimum:
 - Program Scope and Objectives
 - System Safety Organization
 - Schedule
 - Safety Requirement and Criteria
 - Listing of Analyses
 - Safety Data to be Used
 - Safety Verification
 - Safety Audit
 - Training
 - Incident Reporting
 - System Safety Interfaces

Each of these is addressed in the following slides

System Safety 101

SSPP – What goes in it?

- Program Scope and Objectives
 - Description of the overall program
 - Is it a new development program, an upgrade, a modification to an existing program for a new application?
 - Does the program include human factors, nuclear safety, range safety, explosive and ordnance safety, chemical and biological safety, laser safety, etc.?
 - Description of tasks and activities
 - Top level description, including how system safety works with others
 - Applicable documents and references
 - Identify which are directives (those called out in the contract) and which are guidance (all others)
 - Matrix identifying where each contractual requirement is addressed in the SSPP
 - This may include not only requirements, but tasks and responsibilities also

System Safety 101

SSPP – What goes in it?

- System Safety Organization
 - Organizational chart showing where safety fits within the program organization, what are the lines of communications and how safety fits with other functions
 - Organizational chart should include both programmatic and functional legs to show dual reporting paths, if applicable
 - Who's in charge here?
 - Who is the safety lead for the program, including name/number/address/qualifications, what is their authority
 - Described the staffing level
 - Identify how safety requirements are flowed down, subcontractors' efforts are integrated, design reviews/System Safety Working Groups (SSWGs) are supported and hazard analyses are incorporated
 - Identify the decision process for resolving unacceptable/ undesirable hazards

System Safety 101

SSPP – What goes in it?

- Schedule
 - Schedule was shown on slide 16
 - Some items not on the schedule:
 - SSWG support
 - WSESRB/NNMSB/AFSRB (Review Authority) support
 - Engineering Change Proposals (ECPs)/Deviation/Waiver support
 - Insensitive Munitions (IM) testing
 - Code/peer reviews

System Safety 101

SSPP – What goes in it?

- Safety Requirement and Criteria
 - Description of how you will identify hazards and corresponding safety requirements
 - Description of how risk will be categorized
 - Hazard levels, probabilities, control levels
 - Risk/Criticality matrices
 - Assumptions
 - Define Unacceptable/Undesirable
 - Closed loop process for resolving hazards
 - Define criteria used for assessing identified hazards

System Safety 101

SSPP – What goes in it?

- Criteria Used for Assessing Hazards
 - All hazards evaluate the severity of the hazard:
 - I - Catastrophic: Will cause death, system loss, irreversible environmental damage that violates law or regulation or damage to launch platform sufficient to cause loss of combat capability.
 - II - Critical: Will cause severe injury to personnel or major system damage sufficient to cause a reduction in combat capability, reversible environmental damage causing a violation of law or regulation or will require immediate corrective action for personnel or system survival. Severe injury is defined as one which will have a life-long affect on the victim (e.g., severed limb, crushed bones, etc.).
 - III -Marginal: Will cause serious injury to personnel, major system damage or mitigatable environmental damage without violation of law or regulation where restoration activities can be accomplished. Serious injury is defined as one which requires immediate medical attention but will not have a long- term affect (e.g., broken bones which must be set).
 - IV - Negligible: Will result in less than serious personnel injury, system damage or minimal environmental damage not violating law or regulation. A less-than-serious injury is defined as one which may require medical attention but will not have a long-term affect (e.g., bruises, scrapes, etc.).

System Safety 101

SSPP – What goes in it?

- Criteria Used for Assessing Hazards
 - Assessment differs depending upon type of hazard being assessed
 - Hardware uses a qualitative or quantitative probability of occurrence
 - Software uses a Software Control Level
 - Firmware uses Firmware Control Level
 - Each is defined

System Safety 101

SSPP – What goes in it?

- Criteria Used for Assessing Hazards - Hardware
 - Frequent – Level A: Specific Item: Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.
Inventory: Continuously experienced
 - Probable – Level B: Specific Item: Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life
Inventory: Will occur frequently
 - Occasional – Level C: Specific Item: Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life
Inventory: Will occur several times
 - Remote – Level D: Specific Item: Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life
Inventory: Unlikely, but can reasonably be expected to occur
 - Improbable – Level E: Specific Item: So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life
Inventory: Unlikely to occur, but possible

System Safety 101

SSPP – Hardware Risk Index

Hazard Category Frequency	Catastrophic I	Critical II	Marginal III	Negligible IV
A-Frequent	High	High	Medium	Low
B-Probable	High	High	Medium	Low
C-Occasional	High	Medium	Low	Low
D-Remote	Medium	Low	Low	Low
E-Improbable	Low	Low	Low	Low
Legend				
High	High	Unacceptable – CAE Acceptance Required		
Medium	Serious	Undesirable – PEO Acceptance Required		
Low	Medium	Acceptable by PM review		
Low	Low	Acceptable without review		

System Safety 101

SSPP – What goes in it?

- **Criteria Used for Assessing Hazards - Software**
 - Category I: Software exercises autonomous control over potentially hazardous hardware systems, subsystems or components without the possibility of intervention to preclude the occurrence of a hazard. Failure of the software or a failure to prevent an event leads directly to a hazard's occurrence
 - Category IIa: Software exercises control over potentially hazardous hardware systems, subsystems, or components allowing time for intervention by independent safety systems to mitigate the hazard. However, these systems by themselves are not considered adequate
 - Category IIb: Software item displays information requiring immediate operator action to mitigate a hazard. Software failures will allow or fail to prevent the hazard's occurrence
 - Category IIIa: Software item issues commands over potentially hazardous hardware systems, subsystems or components requiring human action to complete the control function. There are several, redundant, independent safety measures for each hazardous event
 - Category IIIb: Software generates information of a safety critical nature used to make safety critical decisions. There are several, redundant, independent safety measures for each hazardous event
 - Category IV: Software does not control safety critical hardware systems, subsystems or components and does not provide safety critical information

SSPP – Software Criticality Matrix

Hazard Category SCL	Catastrophic I	Critical II	Marginal III	Negligible IV
I - Autonomous	1	1	2	4
II - Semi-Autonomous	1	2	3	4
III - Influential	2	3	4	4
IV – No Involvement	3	3	4	4
Legend				
	High	Requirements analysis, design analysis, code analysis and safety specific testing		
	Serious	Requirements analysis, design analysis and in-depth safety specific testing		
	Medium	Requirements analysis and safety specific testing		
	Low	High level safety testing		

System Safety 101

SSPP – What goes in it?

- Criteria Used for Assessing Hazards - Firmware
 - Autonomous – Firmware device exercises autonomous control over potentially hazardous systems, subsystems, or components without the possibility of intervention to preclude the occurrence of a hazard. Failure of firmware outputs lead directly to a hazard occurrence, or a failure of the firmware to prevent an event leads directly to a hazard occurrence. No independent interlocks.
 - Semi-Autonomous (Interlock is Static Random Access Memory {SRAM}/ Electrically Erasable Programmable Read-Only Memory {EEPROM} firmware device) – Firmware device exercises partial control over potentially hazardous systems, subsystems or components. A minimum of one SRAM or EEPROM based firmware device performs remaining control over same system OR acts as a single interlock to mitigate a safety hazard from occurring.
 - Semi-Autonomous (Interlock is Antifuse firmware device or hardware device) – Firmware device exercises partial control over potentially hazardous systems, subsystems or components. A minimum of one Antifuse firmware device or a single hardware device performs remaining control over same system OR acts as a single interlock to mitigate a safety hazard from occurring.
 - Influential – Firmware output commands or provides information to potentially hazardous hardware systems or subsystems. Two or more interlocks exist.

System Safety 101

SSPP – Firmware Criticality Matrix

Hazard Category FCL	Catastrophic I	Critical II	Marginal III	Negligible IV
Autonomous – No Additional Safety Interlock (ASI)	FSCI 1	FSCI 2	FSCI 3	FSCI 4
Semi-Autonomous – One ASI (SRAM/EPROM Device)	FSCI 2	FSCI 3	FSCI 4	FSCI 4
Semi- Autonomous – One ASI (Antifuse or HW)	FSCI 3	FSCI 3	FSCI 4	FSCI 4
Influential – Two or more ASIs	FSCI 4	FSCI 4	FSCI 4	FSCI 4
Legend				
	High	Requires design analysis, requirements analysis, single event upset analysis and extensive testing		
	Serious	Requires design analysis, requirements analysis, single event upset analysis and testing		
	Medium	Requires design analysis, requirements analysis, single event upset analysis and testing		
	Low	Requires requirements analysis and single event upset analysis		

System Safety 101

SSPP – What goes in it?

- One key item to remember:
 - Hazard severity rarely changes
 - Hardware probability of occurrence most likely changes
 - Software Control Level and Firmware Control Level can change based upon system architecture
 - When assessing risk, focus on the most credible scenario
 - May not be the most severe consequence
 - When generating analyses, program may want both most credible and worst-case hazard severity reported
 - Focus on highest risk index

System Safety 101

SSPP – What goes in it?

- Listing of Analyses
 - Identify the specific hazard analyses to be performed
 - Qualitative or quantitative
 - Depth of analysis
 - Format of worksheets
 - Identify the scope of what will be analyzed
 - Non-Development Item (NDI)/Government Furnished Equipment (GFE)?
 - Identify how subcontractors inputs will be incorporated

System Safety 101

SSPP – What goes in it?

- Safety Data to be Used
 - Describe how lessons learned will be collected and used
 - Identify what are your deliverables
 - CDRLs titles and periodicity
 - How will it be delivered – paper, electronically, etc.
 - Identify non-deliverables
 - Describe how results/findings of analyses are flowed up for management/customer review

System Safety 101

SSPP – What goes in it?

- Safety Verification
 - Specify how safety requirements will be verified
 - Inspection – MIL-HDBK-454
 - Demonstration – System abort if out of sequence
 - Test – IM/Restrained firing
 - Simulation – Safe separation
 - Analysis – Careful not to lump everything here
 - Identify how the verification data will be collected and forwarded
 - State how system safety will review test procedures
 - Safe operation of tests
 - Adequate testing of requirements

System Safety 101

SSPP – What goes in it?

- Safety Audit
 - Describe how the safety programs objectives and requirements can be independently verified
 - How are you going to demonstrate you did what you said you'd do

- Training
 - Describe any training system safety will develop for:
 - Maintainers/operators
 - Testers
 - Handlers
 - Software engineers
 - Systems engineers
 - Architects
 - System safety engineers

System Safety 101

SSPP – What goes in it?

- Incident Reporting
 - Identify the process that will be used to notify to customer in the highly unlikely, and probably never to occur, event that a mishap/ incident occurs
 - Identify the thresholds for reporting
 - Specify the timeliness required
 - Work with Environmental Health & Safety (EHS) for common practice

System Safety 101

SSPP – What goes in it?

- System Safety Interfaces
 - Identify how the system safety engineering function working with, reports to or helps guide the following disciplines:
 - Systems
 - Maintainability
 - Reliability
 - Software development
 - Test and evaluation
 - Quality
 - Configuration Management/ Data Management (CM/DM)
 - Mechanical
 - Electronics
 - Architecture
 - EHS

System Safety 101

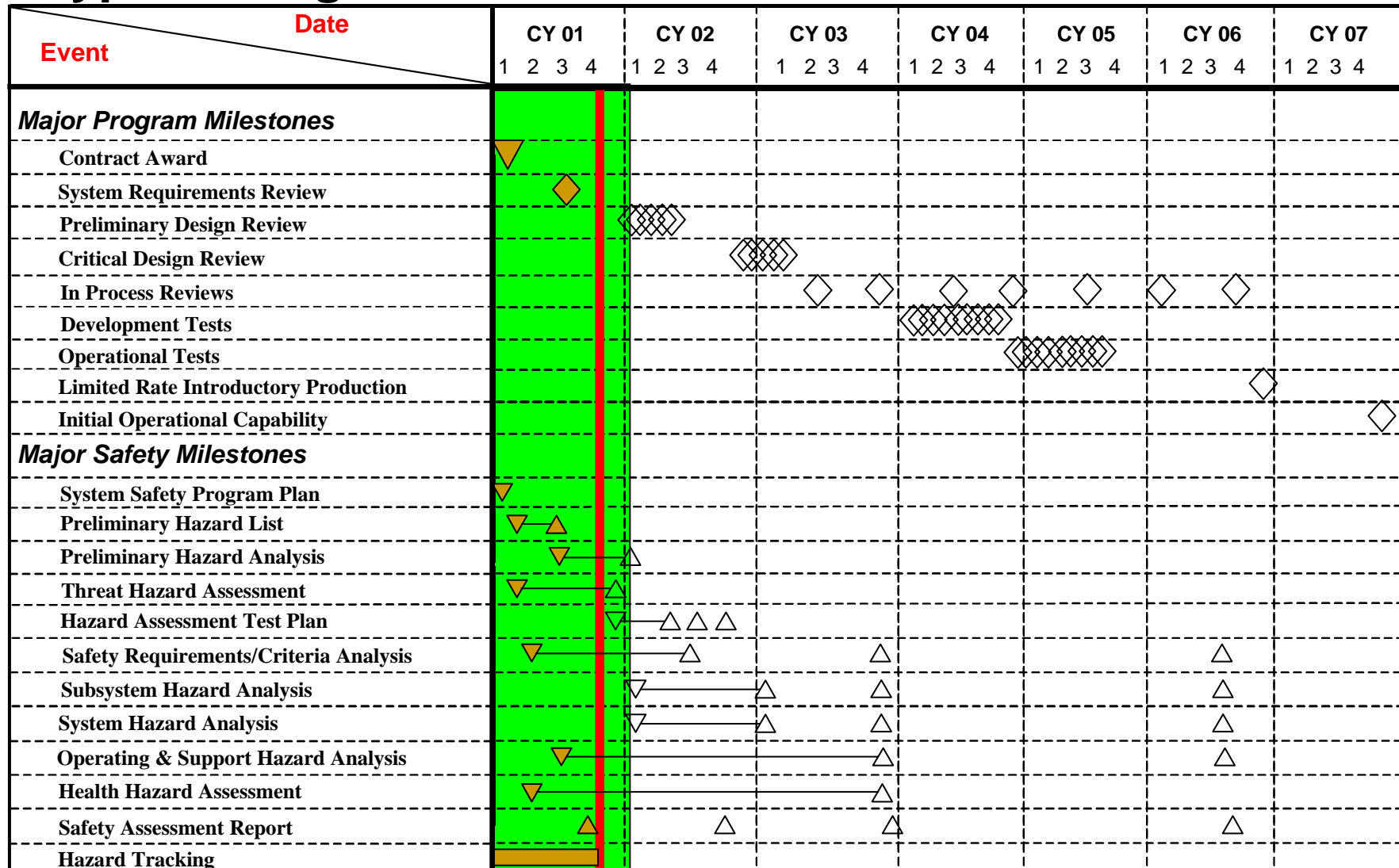
SSPP SUMMARY:

- The SSPP is an agreement between you and the customer
- SSPP can help you bound the scope of your program
- SSPP identifies what your funding level is, so plan accordingly because.....
- What you say, you gotta do

Preliminary Hazard List/ Preliminary Hazard Analysis

System Safety 101

Typical Program Schedule with Traditional Deliverables



System Safety 101

Preliminary Hazard List (PHL)/ Preliminary Hazard Analysis (PHA)

- PHL – Identified as Task 201 in MIL-STD-882
 - Initial assessment, performed extremely early in the program
 - May be performed in support of proposal effort
 - System may be in conceptual form only
 - Identifies areas that will need to be focused on
 - Top level – Radiation hazard, electrical shock, inadvertent detonation, etc.
 - No need to specify system phase or configuration at this time
 - Don't perform the PHL in a vacuum. Involve other engineering disciplines when identifying hazards

System Safety 101

PHL/ PHA

- PHL – Identified as Task 201 in MIL-STD-882
 - When determining listing, consider three items; contractual requirements, lessons learned and generic checklists
 - Contractual requirements may identify concerns
 - WSESRB has issued a fairly comprehensive checklist
 - PHL worksheet requires, at a minimum, three inputs:
 - Brief description of hazard
 - Recommended actions
 - Other applicable information
 - PHL hazards will be expanded in the PHA

System Safety 101

PHL/PHA

- PHA – Identified as Task 202 in MIL-STD-882
 - Identify safety critical areas with the system design
 - Provide an initial assessment of the system's overall safety
 - Used to identify top level hazards
 - Requires a fairly detailed description of the concern in order to reach consensus with the SSWG/PFS
 - From a software perspective, identifies the hazards that will be evaluated
 - Bounds the scope of the software efforts

System Safety 101

PHL/PHA

- PHA – Identified as Task 202 in MIL-STD-882
 - Performed and delivered in support of Preliminary Design Review (PDR)
 - PHA worksheet requires the following inputs:
 - Hazard Number
 - System/Subsystem/Unit
 - System Event Phase
 - Brief Hazard Description
 - Related Safety Critical Factor
 - Effect of Hazard
 - Risk Assessment (Hardware only)
 - Recommended Actions
 - Effects of Recommended Actions
 - Remarks
 - Status

System Safety 101

PHL/PHA – So, what do you really do?

- Best opportunity to derive requirements and get them embedded in the system design
 - This is the time to influence the system design
- Where do the requirements come from?
 - MIL STDs/MIL SPECS
 - Mitigation of identified hazards
 - WSESRB Hazard Analysis Guidelist
 - Lessons learned from similar systems
 - Brain storming
 - Contract/SOW/Performance Spec/talking with co-workers
- Majority of the software effort performed at this time
 - Functional Review
 - Requirements Review
 - Safety Criticality Identification

System Safety 101

PHL/PHA – That’s fine, but what’s expected?

- Two programmatic reviews are typically held during preparation of PHL/PHA
 - System Functional Review {SFR} (Sometimes known as Systems Requirements Review {SRR})
 - PDR
- Reviews have expectations in five key areas:
 - Planning
 - **Requirements Analysis, Review and Verification**
 - **Design Guidance**
 - **Analysis**
 - Budget
- Details of the Requirements Analysis, Review and Verification, Design Guidance and Analysis are provided
 - Planning addresses SSPP and Budget addresses adequate staffing

System Safety 101

PHL/PHA – That’s fine, but what’s expected at SFR/SRR?

- Requirements Analysis, Review and Verification
 - Customer requirements are being analyzed and flowed down/allocated to lower level system components and suppliers. Allocation of requirements between hardware and software is defined
 - Red - Requirements have not been analyzed or flowed down, or allocation of requirements has not been defined between hardware and software
 - Yellow – Requirements have been analyzed but not flowed down, or allocation of requirements between hardware and software has not been determined
 - Green – Requirements have been analyzed and flowed down, and allocation of requirements between hardware and software has been determined
 - Blue – Requirements have been analyzed and flowed down into lower level and suppliers specifications, and allocation of requirements between hardware and software has been reviewed and approved by the SSWG membership with all HIGH risk software contributions eliminated
 - Key analyses and trade studies completed to date have been reviewed to determine if there were opportunities for system safety to influence the design approach
 - Red – Analyses and trade studies have not been completed
 - Yellow – Analyses and trade studies have been completed but have not been reviewed
 - Green – Analyses and trade studies have been completed and internally reviewed
 - Blue - Analyses and trade studies have been completed and reviewed by SSWG membership

System Safety 101

PHL/PHA – That’s fine, but what’s expected at SFR/SRR?

- Design Guidance
 - Development of system safety design guide has been completed and has been distributed to engineering
 - Red – **Safety design guide has not been completed**
 - Yellow – **Safety design guide has been completed but has not been distributed**
 - Green – **Safety design guide has been completed and distributed**
 - Blue – **Safety design guide has been completed, distributed and the details have been incorporated into the applicable hardware and hardware specifications**
- Analysis
 - Verify that any safety related system or subsystem technologies that have not been previously demonstrated have been identified and have been included in a Preliminary Hazard List (or equivalent)
 - Red – **Technologies not previously demonstrated have not been identified or included in the PHL**
 - Yellow – **Technologies not previously demonstrated have been identified but are not included in the PHL**
 - Green – **Technologies not previously demonstrated have been identified and included in the PHL**
 - Blue – **Technologies not previously demonstrated have been identified in the PHL and the review authority concurs with planned mitigation activities**

System Safety 101

PHL/PHA – That’s fine, but what’s expected at PDR?

- Requirements Analysis, Review and Verification
 - Customer requirements have been analyzed and flowed down/allocated to lower level system components and suppliers
 - Red - Requirements have not been analyzed or flowed down
 - Yellow – Requirements have been analyzed but not flowed down
 - Green – Requirements have been analyzed and flowed down into approved lower level and suppliers specifications
 - Blue – Requirements have been analyzed and flowed down into approved lower level and suppliers specifications, and allocation of requirements between hardware and software has been reviewed and approved by the review authority with all HIGH risk software contributions eliminated
 - Verify that identified system safety design opportunities have been flowed down/allocated to lower level system components and suppliers
 - Red – Safety design opportunities have not been identified
 - Yellow – Safety design opportunities have been identified but have not been flowed down
 - Green – Safety design opportunities have been identified and flowed down into lower level and suppliers’ specifications
 - Blue - Safety design opportunities have been identified and flowed down and the review authority concurs their implementation reduces the system risk

System Safety 101

PHL/PHA – That’s fine, but what’s expected at PDR?

- Requirements Analysis, Review and Verification (Continued)
 - Safety critical requirements have been identified in hardware CI and software SI requirement specifications
 - Red - **Safety critical requirements have not been identified**
 - Yellow – **Safety critical requirements have been identified but have not been identified as such in the hardware and software specifications**
 - Green – **Safety critical requirements have been identified and uniquely flagged as such in the hardware and software specifications**
 - Blue – **Safety critical requirements have been identified, reviewed and approved by the review authority and uniquely flagged as such in the hardware and software specifications**
- Design Guidance
 - Compliance to requirements contained in the System Safety design guide are being monitored
 - Red – **Safety design guide requirements are not monitored**
 - Yellow – **Safety design guide requirements are intermittently monitored**
 - Green – **Safety design guide requirements are continuously monitored**
 - Blue - **Safety design guide requirements are continuously monitored and documented via a tracking system**

System Safety 101

PHL/PHA – That’s fine, but what’s expected at PDR?

- Design Guidance (Continued)
 - Hardware and software design checklists completed/initiated and distributed
 - Red – **Hardware and software design checklists are not completed**
 - Yellow – **Hardware and software design checklists are completed but not distributed to all IPTs**
 - Green – **Hardware and software design checklists are completed and distributed to all IPTs**
 - Blue - **Hardware and software design checklists are completed, distributed to all IPTs, and incorporated in the hardware and software specifications**
- Analysis
 - A PHL has been initiated and completed
 - Red – **PHL not completed**
 - Yellow – **PHL completed but not reviewed by SSWG membership**
 - Green – **PHL completed and reviewed by SSWG membership**
 - Blue - **PHL completed and concurred by review authority**
 - A PHA has been initiated and completed
 - Red – **PHA not completed**
 - Yellow – **PHA completed but not reviewed by SSWG membership**
 - Green – **PHA completed and reviewed by SSWG membership**
 - Blue - **PHA completed and concurred by review authority**

What else is done/ expected prior to PDR

Software Safety Process

(The SSPP and SwSPP have been combined into a single document.)

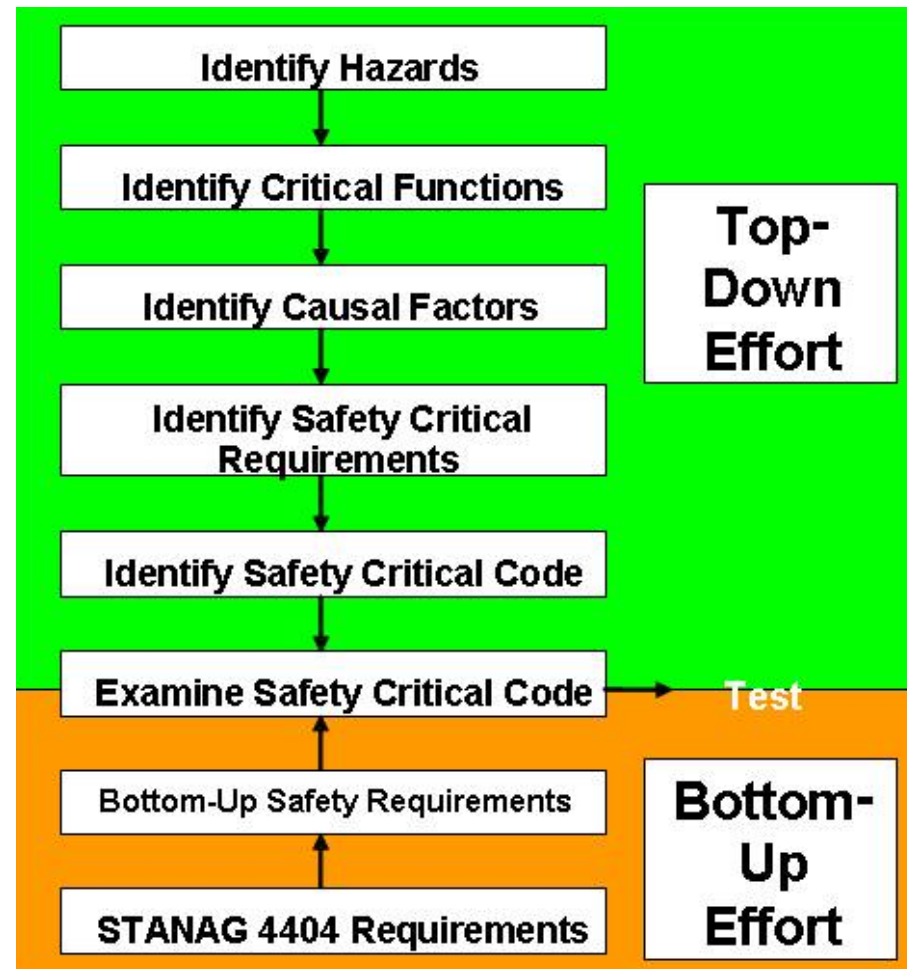
System Safety 101

Software Safety Process -

- Naval Ordnance Safety and Security Activity (NOSSA) (parent group to the WSESRB/SSSTRP) has developed a “WSESRB approved” Software Certification Process
- A generic Software Safety Program Plan (SwSPP) was written to implement the process
 - Took pieces from previously existing SwSPPs
 - Plagiarized from Todd Isaac’s Firmware Process
 - Follows “WSESRB Process”
- SwSPP was distributed to Weavers for review and concurrence
- As a result of Weaver comments, the SwSPP has been embedded into the generic SSPP
- Software process follows

System Safety 101

Dual Effort Software Safety Approach



System Safety 101

Software Safety Process -

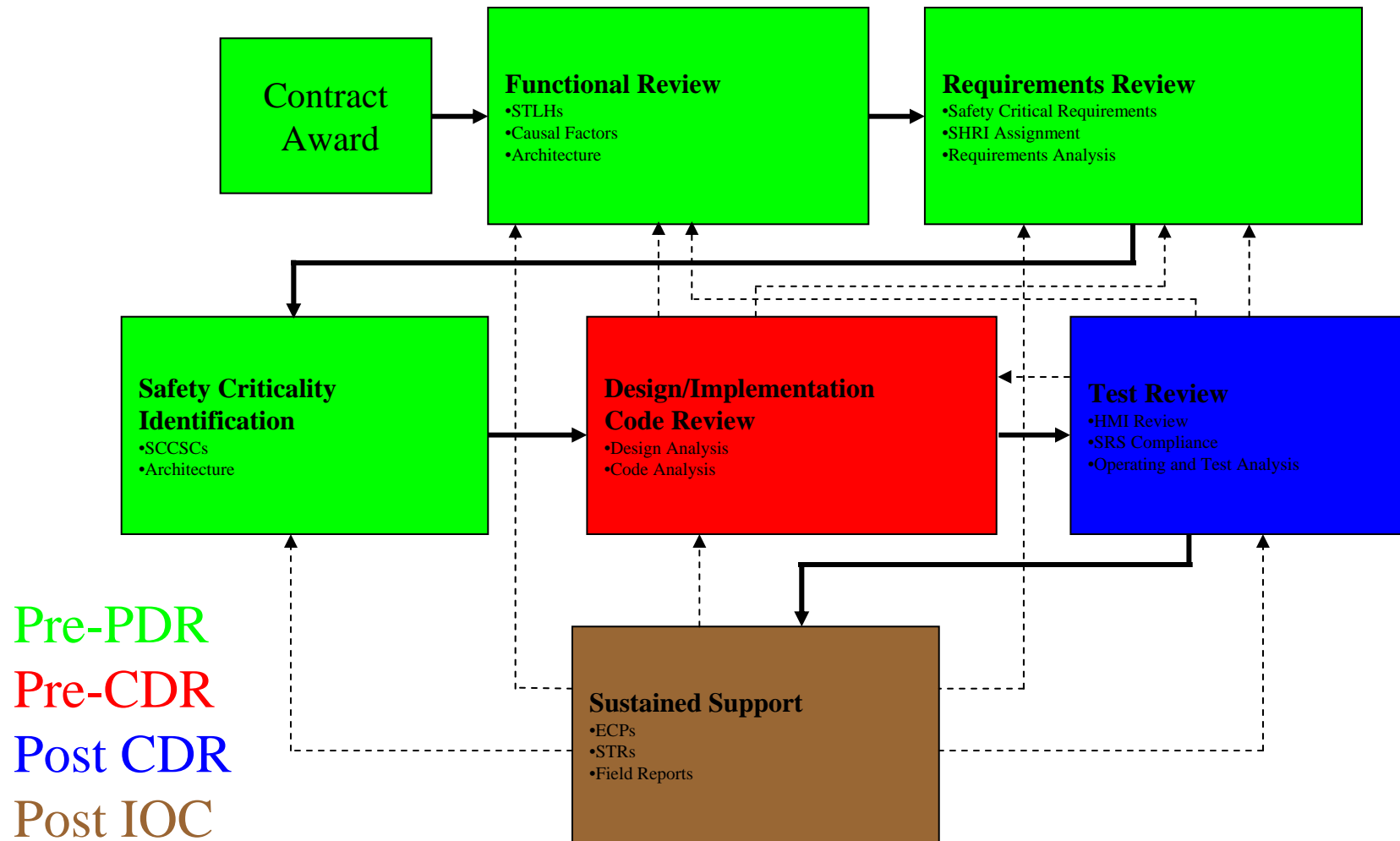
The process described in the software process consists of six main activities:

- Functional Review
- Requirements Review
- Safety Criticality Identification
- Design/Implementation Code Review
- Test Review
- Sustained Support

Each of these is explained in detail

System Safety 101

Software Safety Process



System Safety 101

Software Functional Review

- “Analyzing the system hardware/software from a functional and requirements perspective to determine the Software Top Level Hazards (STLHs), software causal factors associated with the hazards, and architectural alternatives that may reduce the risk associated with the software development”
- What does this mean/how do you do it?

System Safety 101

Software Functional Review

- **Step #1 – Identify Top-Level Hazards (TLHs)**
 - Use usual sources (SOW/Lessons Learned/ConOps/SSWG/co-workers)
 - Work with System Engineer (SE)/Software Engineer (SwE)/Architect
 - Document each TLH in painful detail and present to SSWG/Principal For Safety (PFS) for concurrence
 - TLHs will be scope of the effort
- **Step #2 – For each TLH, identify safety critical functions**
 - Control, eliminate or mitigate a hazard or mishap from occurring
 - Again, document and get SSWG/PFS concurrence
 - Functions will be basis for identifying causal factors

System Safety 101

Software Functional Review

- Step #3 – Review Architecture
 - The allocation of functionality between the hardware and software components as well as operator inputs
 - Work with SE/SwE/Architect
 - (Personal Opinion) This is the best opportunity to impact the design and impact the scope of the software safety effort
 - Perform trade studies on how safety critical functions will be implemented
 - Trade studies documented in Architecture reports

System Safety 101

Software Functional Review

- Step #3...cont... – Review Architecture
 - Identify where firmware will be used in the system
 - Determine functionality associated with these devices
 - Identify each devices technology
 - Determine suitability
 - Perform firmware trade studies and document in the PHA and SHA
 - Identify causal factors associated with each safety critical function
 - Causal factors are used to generate the Safety Critical Requirements
 - Used to determine what is “safety critical code”

System Safety 101

Software Functional Review

- Step #3...cont... – Review Architecture
 - Evaluate *BOTTOM-UP SAFETY REQUIREMENTS* for applicability
 - *Bottom-up Safety Requirements (BUSR)* are derived from STANAG 4404
 - Will be used to examine safety critical code
 - Identify initial *SAFETY CRITICAL REQUIREMENTS*
 - Linked to causal factors
 - Address specific TLH - how will the implementation of the code mitigate the concern
 - Code implementing the safety critical requirement will be “SAFETY CRITICAL CODE”

System Safety 101

Software Functional Review

- Step #3...cont... – Review Architecture
 - Combine initial list of requirements into Safety Requirements/Criteria Analysis (SR/CA)
 - SR/CA will be used to track all requirements thru test
 - Identify where Commercial-Off-The-Shelf (COTS)/NDI will be used in the system
 - Will the COTS/NDI be considered safety critical?
 - What are the safety critical requirements related to the COTS/NDI?
 - What causal factors may be impacted by the COTS/NDI?
 - Are other devices available that can perform the functionality within programmatic schedule, performance and cost limitations?

System Safety 101

Software Functional Review

- Step #4 – Review Test Program
 - Work with SE/SwE/ Test & Evaluation (T&E) personnel to come to common understanding of requirement
 - Requirement is testable
 - Test scenario will address concern
- Step #5 – Determine Initial Criticality (Risk)
 - Based upon severity and control level
 - For software, Software Safety Criticality Index (SSCI) determines level of rigor (High is not Unacceptable)
 - For firmware, Firmware Safety Criticality Index (FSCI) helps define suitability
 - Unlike hardware, SSCIs will not change upon completion of analysis (only architecture change modifying the control level will change SSCI)

SSPP – Hardware Risk Index

Hazard Category Frequency	Catastrophic I	Critical II	Marginal III	Negligible IV
A-Frequent	High	High	Medium	Low
B-Probable	High	High	Medium	Low
C-Occasional	High	Medium	Medium	Low
D-Remote	Medium	Medium	Medium	Low
E-Improbable	Medium	Medium	Medium	Low
Legend				
High	High	Unacceptable – CAE Acceptance Required		
Medium	Serious	Undesirable – PEO Acceptance Required		
Low	Medium	Acceptable by PM review		
Low	Low	Acceptable without review		

SSPP – Software Criticality Matrix

Hazard Category SCL	Catastrophic I	Critical II	Marginal III	Negligible IV
I - Autonomous	1	1	2	4
II - Semi-Autonomous	1	2	3	4
III - Influential	2	3	4	4
IV – No Involvement	3	3	4	4
Legend				
	High	Requirements analysis, design analysis, code analysis and safety specific testing		
	Serious	Requirements analysis, design analysis and in-depth safety specific testing		
	Medium	Requirements analysis and safety specific testing		
	Low	High level safety testing		

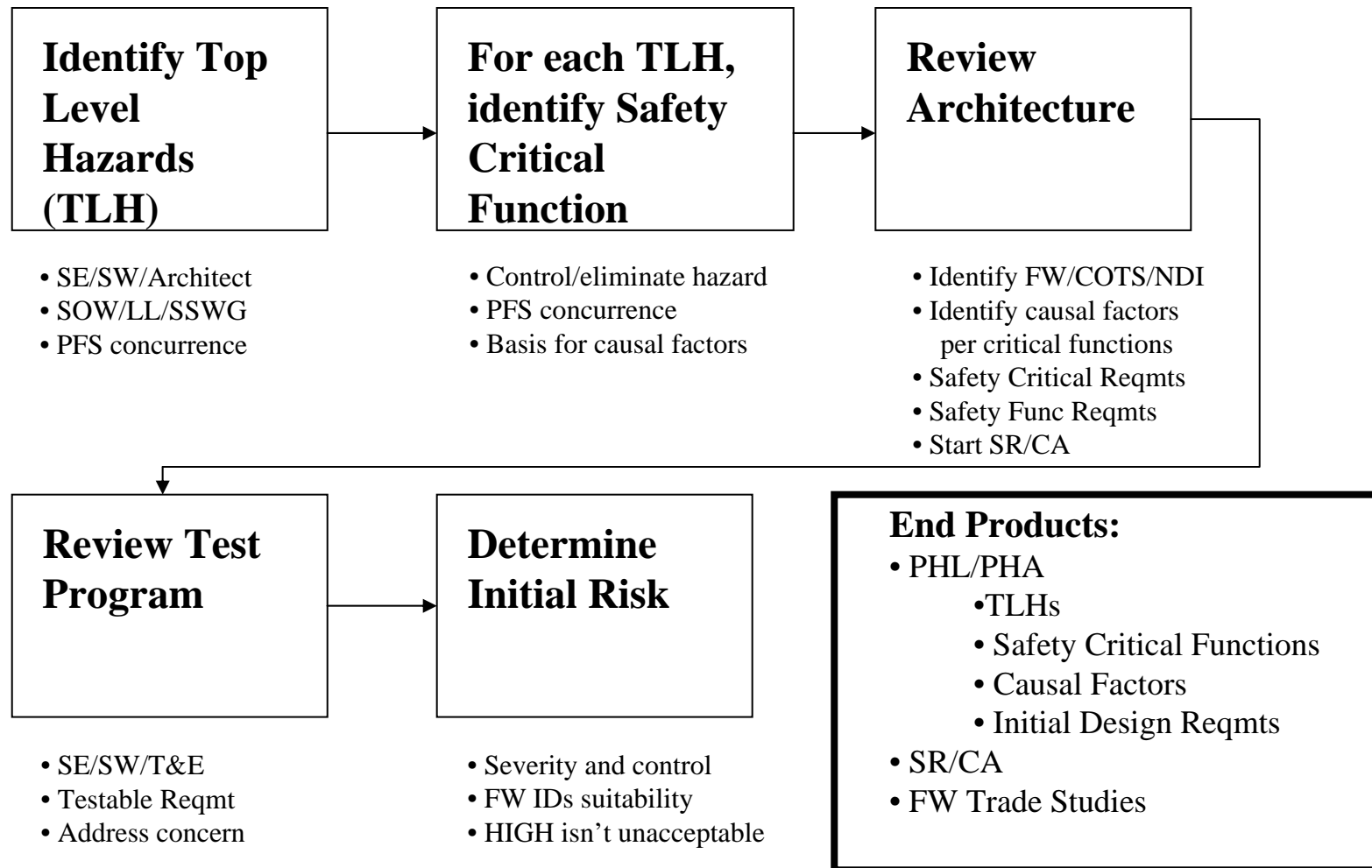
System Safety 101

Software Functional Review – What's documented

- Initial draft of Preliminary Hazard List (PHL)/Preliminary Hazard Analysis (PHA)
 - Listing of TLHs agreed to PFS/SSWG members
 - Identification of Safety Critical Functions
 - Identification of causal factors
 - Initial Safety Critical Requirements
- Initial input of Safety Critical Requirements into SR/CA
- Firmware trade studies, including suitability determination

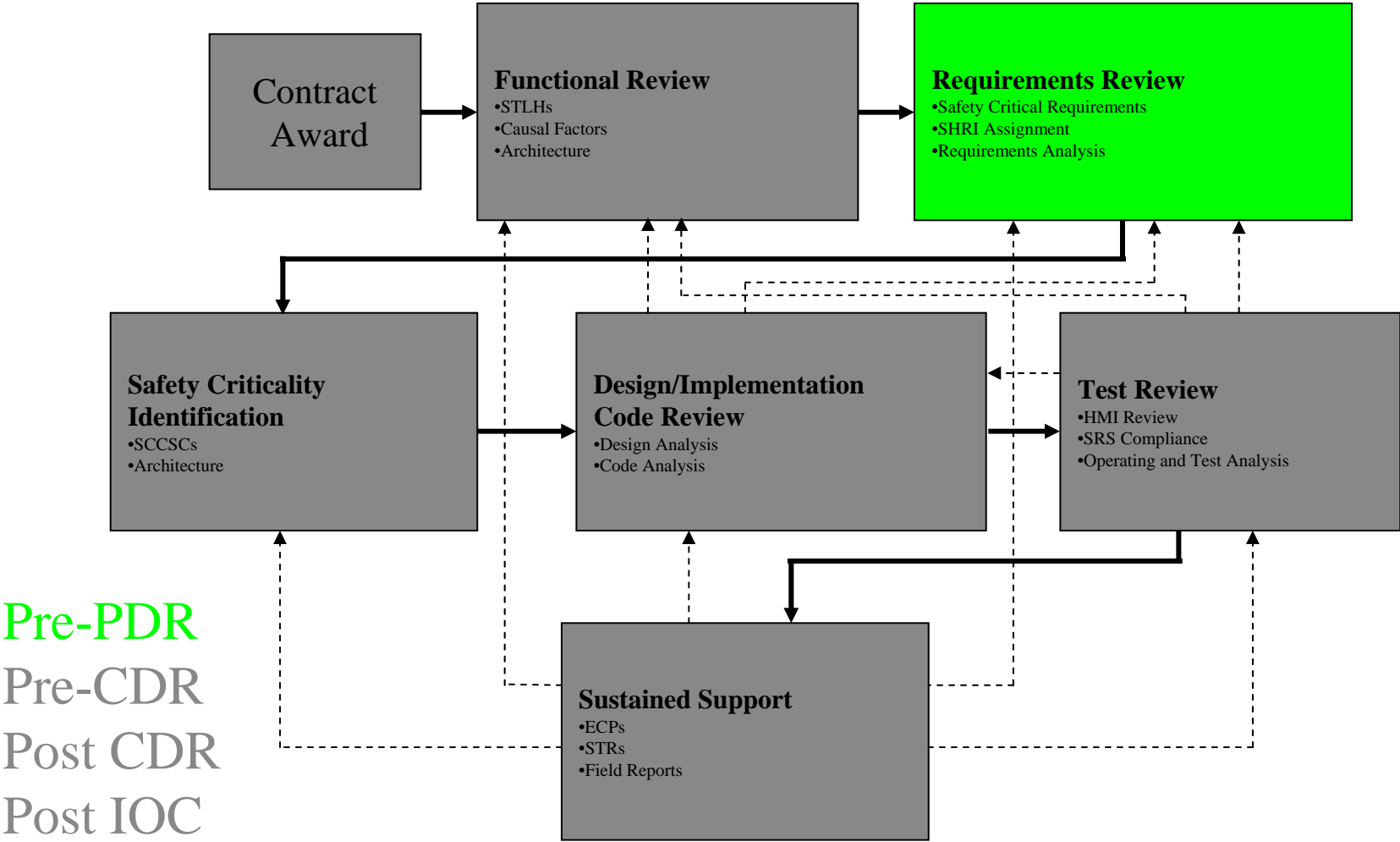
System Safety 101

Functional Review



System Safety 101

Software Safety Process



System Safety 101

Software Requirements Review

“Establishing software safety critical requirements which will eliminate or mitigate the identified hazards for both system software and COTS software products, and determining the SSCI associated with each identified hazard ”

- What does this mean/how do you do it?

System Safety 101

Software Requirements Review

- Step #1 – Review Safety Critical Functions
 - Work with SE/SwE/Architect
 - Verify functions are still applicable
 - Document the logic used for determining them
- Step #2 – Identify causal factors
 - Make sure listing is comprehensive
 - Get PFS/SSWG buy-in
 - Identify roots of causal factors
 - Greater detail in defining causal factors = easier to define the mitigating requirements

System Safety 101

Software Requirements Review

- Step #3 – Review Human/System Interface
 - Human-System Interface Technical Review Panel (HSITRP) coming for USN programs
 - Refer to MIL-STD-1472, paragraph 5.14
 - Ensure software implementation provides:
 - Control and display interactions are clear and concise
 - Improper sequences of control activation are either precluded by making inappropriate controls unavailable or detected by the software with appropriate operator alerts generated
 - The operator has the ability to cancel processing
 - The cancellation of processing places the system into a known safe state

System Safety 101

Software Requirements Review

- Step #4 – Definitize Safety Critical Requirements (SCR)
 - Review Bottom-up Safety Requirements (STANAG 4404), may be SCRs
 - For software, SCRs tend to influence design of code
 - For firmware, SCRs tend to impact architecture (level of control)
 - SCRs will define what is considered Safety Critical Code (and how much needs to be examined)
 - Generate a listing and get Chief Engineer/Program Manager buy-in

System Safety 101

Software Requirements Review

- Step #5 – Review Software Requirements Specification (SRS)/Firmware Specification
 - Work with SwE/Software Configuration Management (SCM) personnel
 - Ensure the requirement says what you want it to say
 - Ensure each SCR is uniquely flagged as such
 - Proper CM controls are in place
- Step #6 – Analyze COTS/NDI Implementation
 - Old subject – new emphasis by WSESRB
 - Need to review and document as part of the process
 - Includes Tools/Environment issues

System Safety 101

Software Requirements Review

- **Step #6 – Analyze COTS/NDI Implementation** (Continued)
 - Determine functionality it performs/supports
 - Determine the causal factors associated with these functions
 - Based upon factors, generate requirements
 - Functionality/requirements form the basis of COTS/NDI analysis
 - Key item is identifying unused functionality and its impact
 - What is the impact if it were activated
 - How is it normally activated
 - Can we limit impact of inadvertent activation
 - Test, test, test, test, test, then test some more

System Safety 101

Software Requirements Review

- **Step #6 – Analyze COTS/NDI Implementation** (Continued)
 - Test COTS/NDI – Rolled into this activity is verifying the tools/test environments used
 - Process for qualifying tools/test environment is requirements-to-test based approach
 - Nominal, stress, fault insertion
 - Classify “safety critical” and place under CM control
 - Test COTS/NDI similar to tools
 - Nominal, stress, fault insertion
 - Ensure failures result in known, safe state

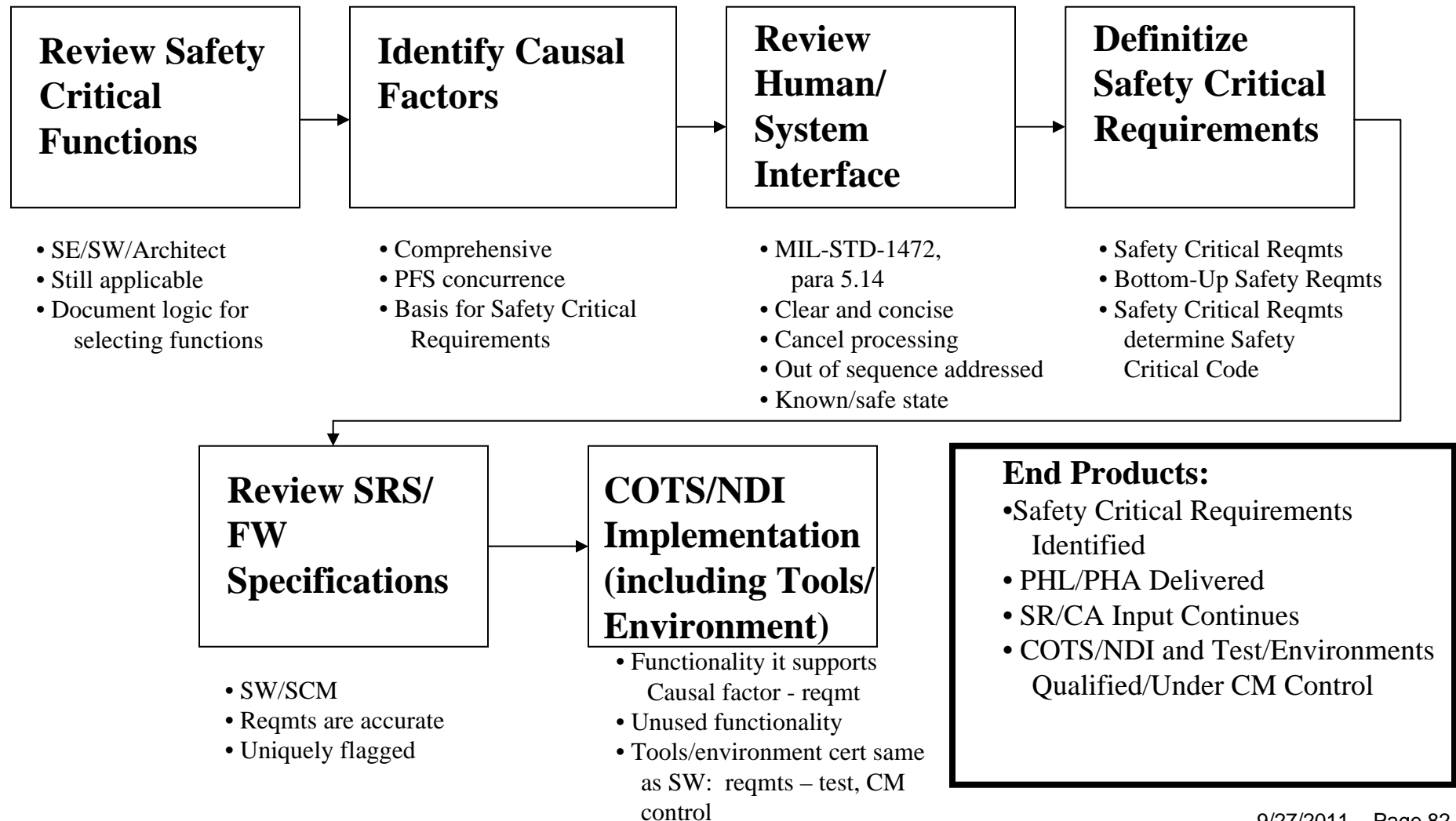
System Safety 101

Software Requirements Review – What's documented

- All Safety Critical Requirements are identified, put in a listing and reviewed/ concurred by chief engineer and Program Manager
- PHL/PHA is delivered
 - Each Safety Critical Requirement is identified as a recommended/corrective action
- Continue inputs into SR/CA
- COTS/NDI and test tools/environments are qualified. Qual reports are appendices to SwHA

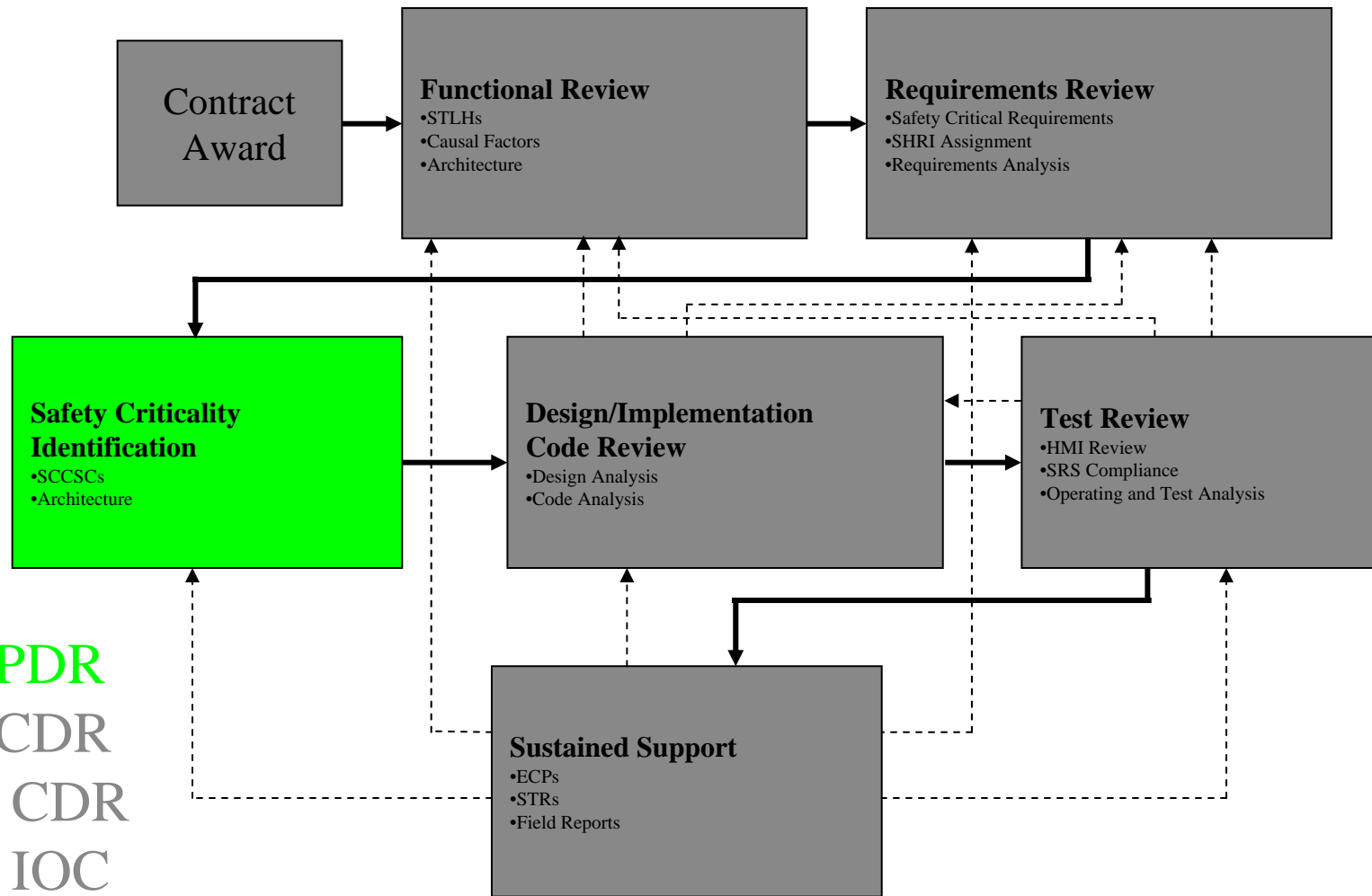
System Safety 101

Requirements Review



System Safety 101

Software Safety Process



Pre-PDR
Pre-CDR
Post CDR
Post IOC

System Safety 101

Safety Criticality Identification

“Identify the Computer Software Configuration Item (CSCI) and Computer Software Component (CSC) which will contain the code associated with the software safety critical requirements. These CSCs shall be classified as Safety Critical Computer Software Components (SCCSCs). ”

- What does this mean/how do you do it?

System Safety 101

Safety Criticality Identification

- Identify CSCIs and SCCSCs
 - Work with SwE/SCM personnel
 - SCM uniquely flags CSCIs and SCCSCs
- Code within SCCSC implements at least one safety critical requirement
 - Changes to ANY code within the SCCSC requires safety review/concurrence per Software Configuration Control Board (SCCB)
 - Re-review software architecture if a CSC only implements a handful of safety critical requirements
 - Limiting number of SCCSCs limits changes requiring review

Safety Criticality Identification

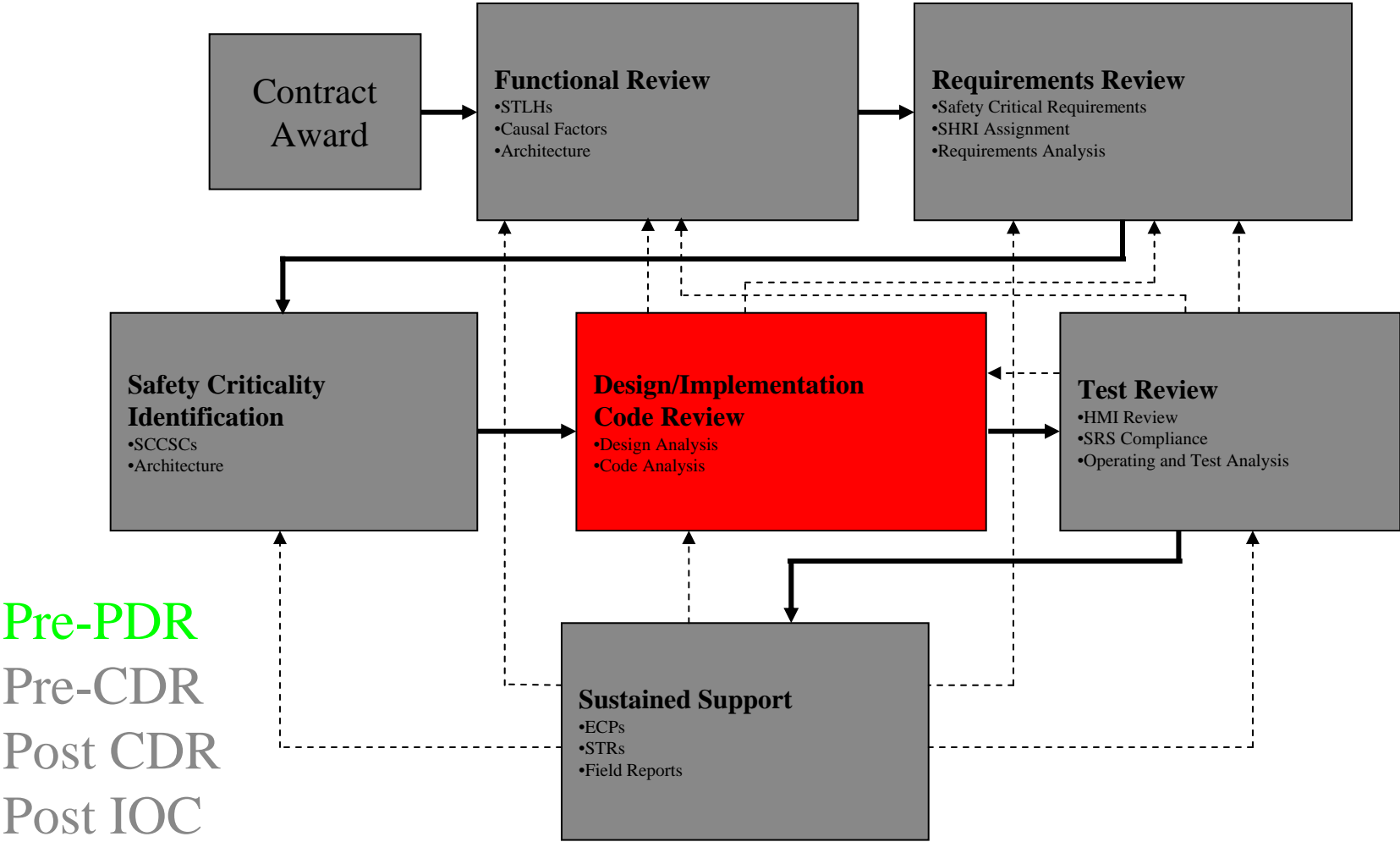


End Products:

- SW Architecture Trade Studies
- Safety Critical Requirements Uniquely Flagged

System Safety 101

Software Safety Process



System Safety 101

Design and Implementation Code Review

“Review the software implementing the software safety critical requirements to ensure the code properly interprets and satisfies the requirement from a safety perspective. In addition, the code contained within the SCCSCs is reviewed for compliance with the bottom-up safety requirements ”

- What does this mean/how do you do it?

System Safety 101

Design and Implementation Code Review

- Step #1 – Review Detailed System Architecture
 - Work with SE/SwE/Architect
 - Ensure analysis reflects CDR architecture
 - Hazard-Function-Causal Factor-Requirement
 - COTS/NDI implementation still the same
 - Firmware use still valid and suitable
 - Perform Single Event Upset (SEU) analysis

System Safety 101

Design and Implementation Code Review

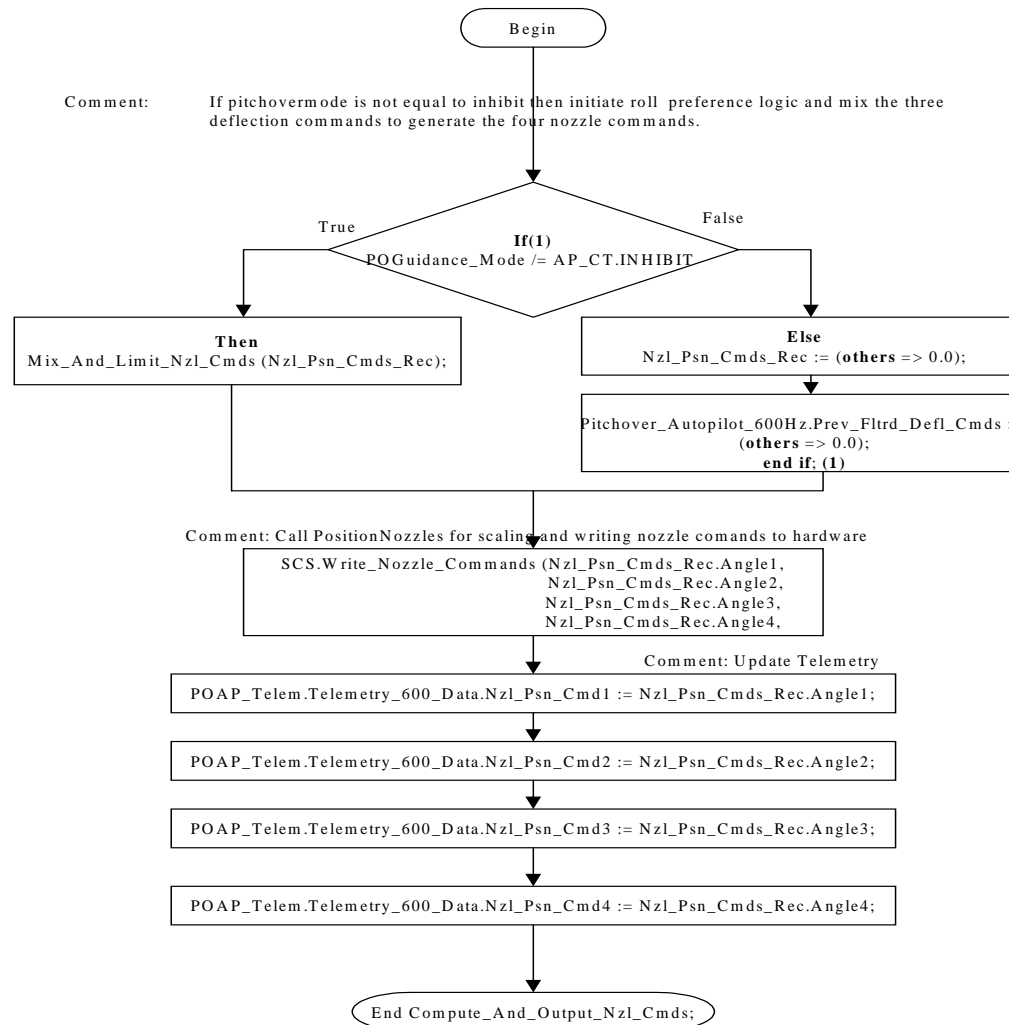
- **Step #2 – Review HSI**
 - Work with SE/SwE/Architect
 - Ensure Human-System Interface (HSI) analysis still valid
- **Step #3 – Analyze Software Implementation**
 - Consists of two parts; top down (requirement implementation) and bottom up safety requirements
 - Top down – Ensure the proper implementation of the safety critical requirements
 - Bottom up – Ensure the code implementing the safety critical requirements complies with the bottom-up safety requirements

System Safety 101

Design and Implementation Code Review

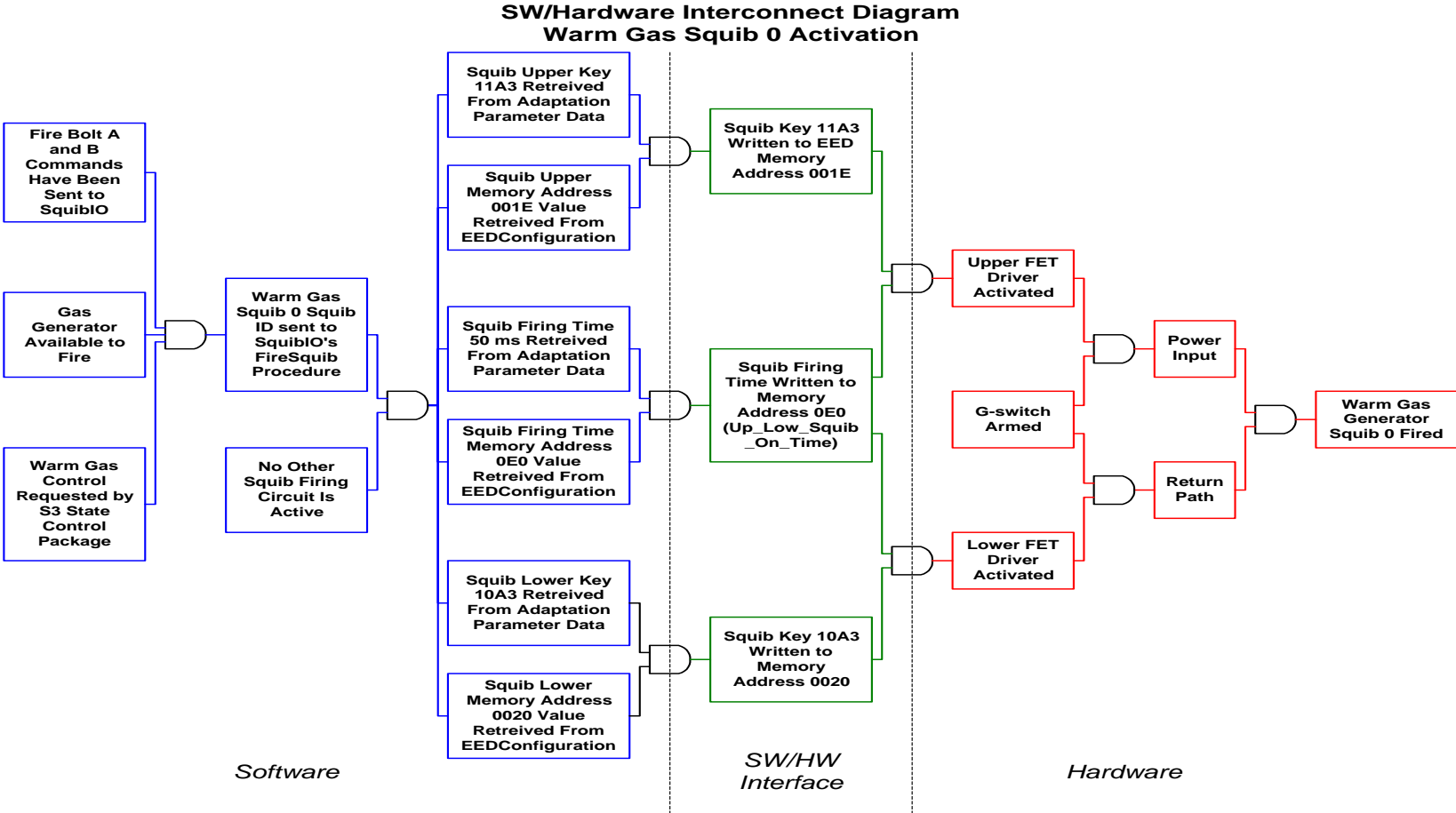
- Step #3 – Analyze Software Implementation Top Down
 - Requires a detailed understanding of what the software is doing
 - Obtained with assistance from SwE
 - Describe interactions with other code with the SCCSC
 - Document understanding in either an event tree or logic diagram
 - Provide rationale as to why the requirement is properly implemented

Logic Diagram



System Safety 101

Event Tree



System Safety 101

Design and Implementation Code Review

- Step #3 – Analyze Software Implementation Bottom Up
 - Safety critical code is identified as part of the Top Down review
 - This code is subjected to “code examination”
 - What does that mean?
 - In addition to implementation, review code for compliance with bottom-up safety requirements
 - Generic derived requirements from STANAG 4404

System Safety 101

Design and Implementation Code Review

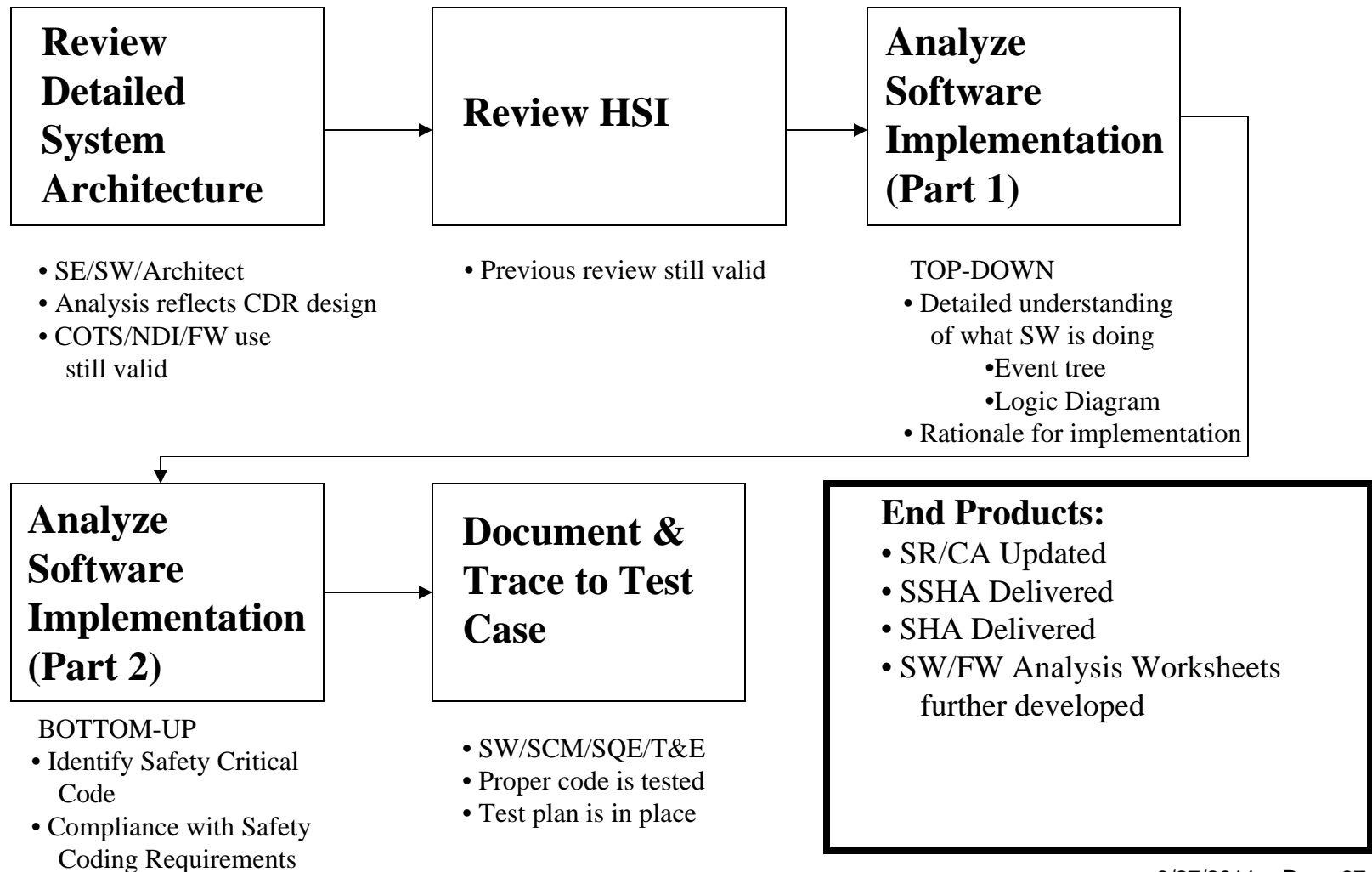
- Step #4 – Document Requirements / Trace to Test Cases
 - Once code has been reviewed, ensure that's the code that will be implemented
 - Work with SCM and SwE and place under CM control
 - Safety critical code is based upon requirement implementation and requirements must be tested, therefore trace code to test
 - Work with the Software Quality Engineering (SQE), SwE and T&E to verify how the requirements will be tested

System Safety 101

Design and Implementation Code Review – What's documented

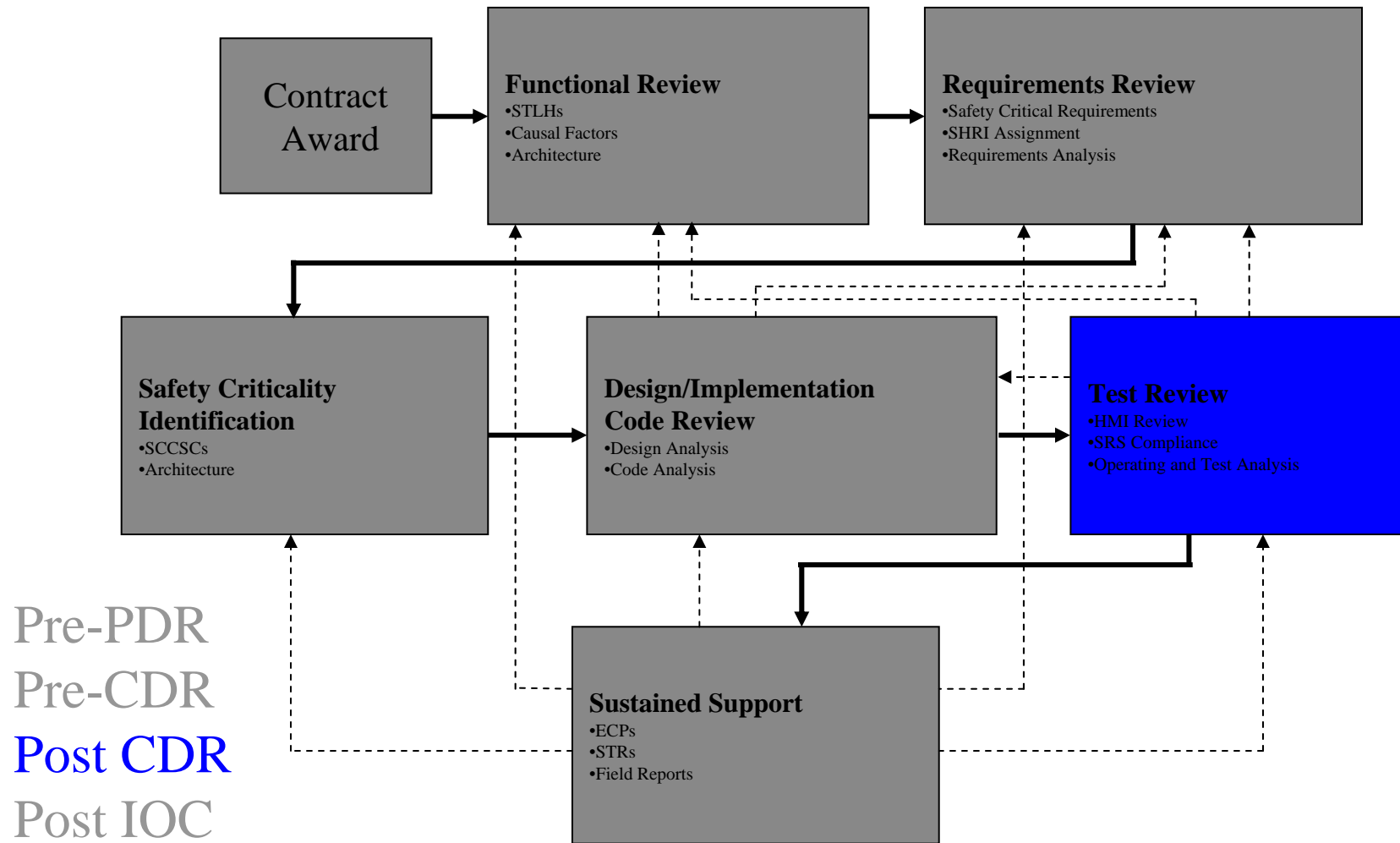
- Subsystem Hazard Analysis (SSHA) is delivered
 - COTS/NDI and firmware use are identified
- System Hazard Analysis (SHA) is delivered
 - Architecture review is documented
- Software analysis worksheets are further developed
 - Diagram and rationale for acceptance
 - Non-compliance with bottom-up safety requirements
- Firmware analysis worksheets are further developed
 - SEU analysis documented
 - Firmware use and suitability identified

Design and Implementation Code Review



System Safety 101

Software Safety Process



System Safety 101

Test Review

“Verifying the safe operation of the software and proper implementation of the requirements via test to the maximum extent possible and where existing test procedures do not adequately address the hazard scenario, modifying the existing procedures. Ensuring the components of the Human System Interface (HSI) (i.e. displays and controls) reduce, or at least do not contribute to, the defined hazards ”

- What does this mean/how do you do it?

System Safety 101

Test Review

(Note that this does not say “Safety Test Review” or “Special Safety Testing”, etc.)

- Step #1 – Trace Safety Critical Requirements to Test Cases
 - Work with SwE/T&E
 - Ensure test scenario address the specific safety critical requirement
- Step #2 - Review Test Case for Thoroughness
 - Ensure test scenario is written to address to concern
 - Verify requirements are “testable” (again, again)

System Safety 101

Test Review

- Step #3 – Ensure Adequacy of Test Environment
 - Work with T&E and CM personnel
 - Verify test set ups are certified or any changes have been reviewed and approved
- Step #4 – Witness Test
 - Per individual program
- Step #5 – Review Test Results
 - Work with T&E and SQE personnel
 - Where results are unexpected and changes are required, may need to regress back to Functional Review

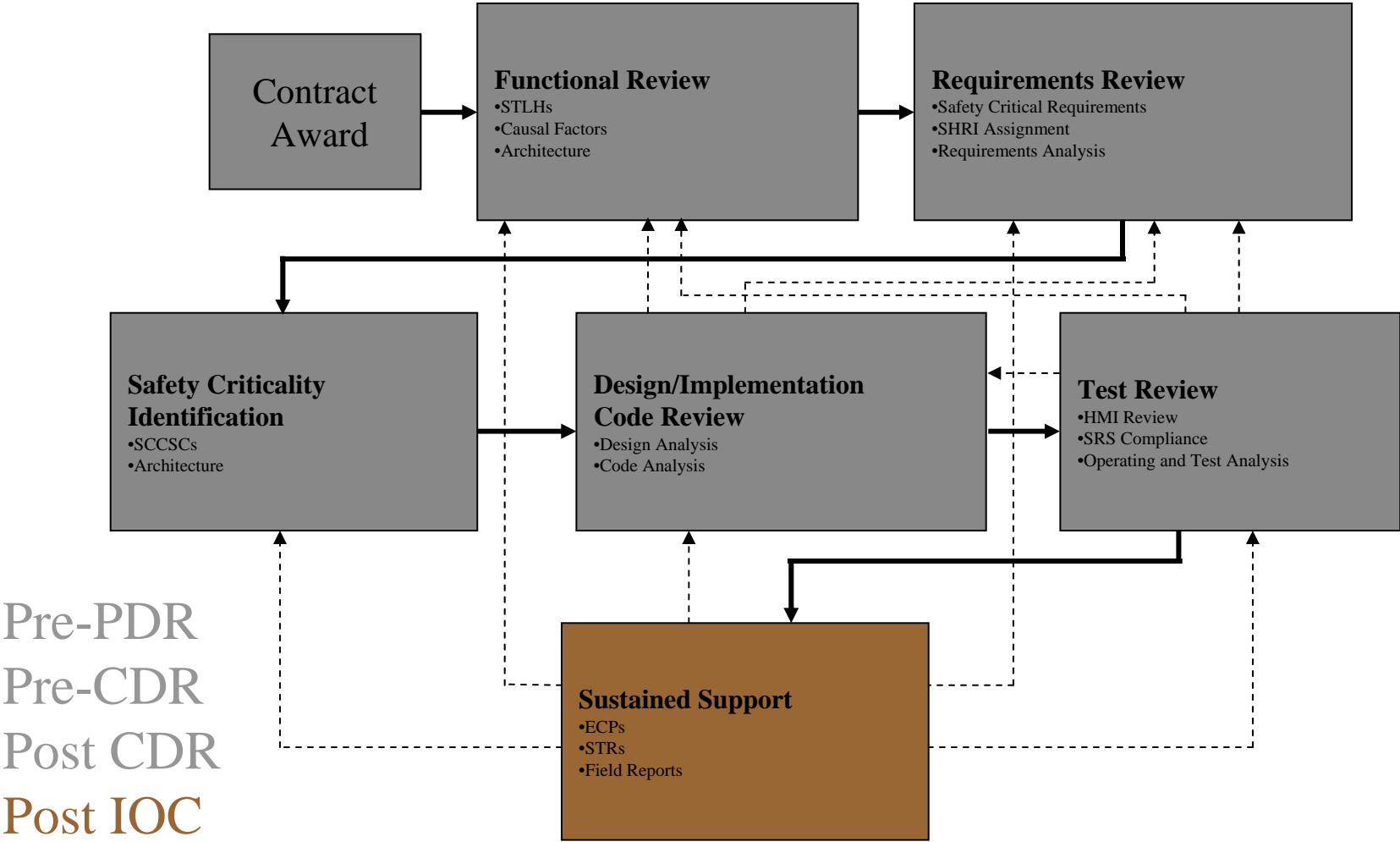
System Safety 101

Test Review – What’s documented

- Results of the test program should flow through all analyses previously submitted (except PHL/PHA)
- Test program will provide justification for closing identified concerns
- Update to at least:
 - SR/CA
 - SSHA
 - SHA
 - Software Analysis Worksheets
 - Firmware Analysis Worksheets

System Safety 101

Software Safety Process



System Safety 101

Sustained Support

“Review proposed changes to the system design, identified field reports, new operating environments and requests for deviations/waivers to ensure the safety of the system is maintained or enhanced. ”

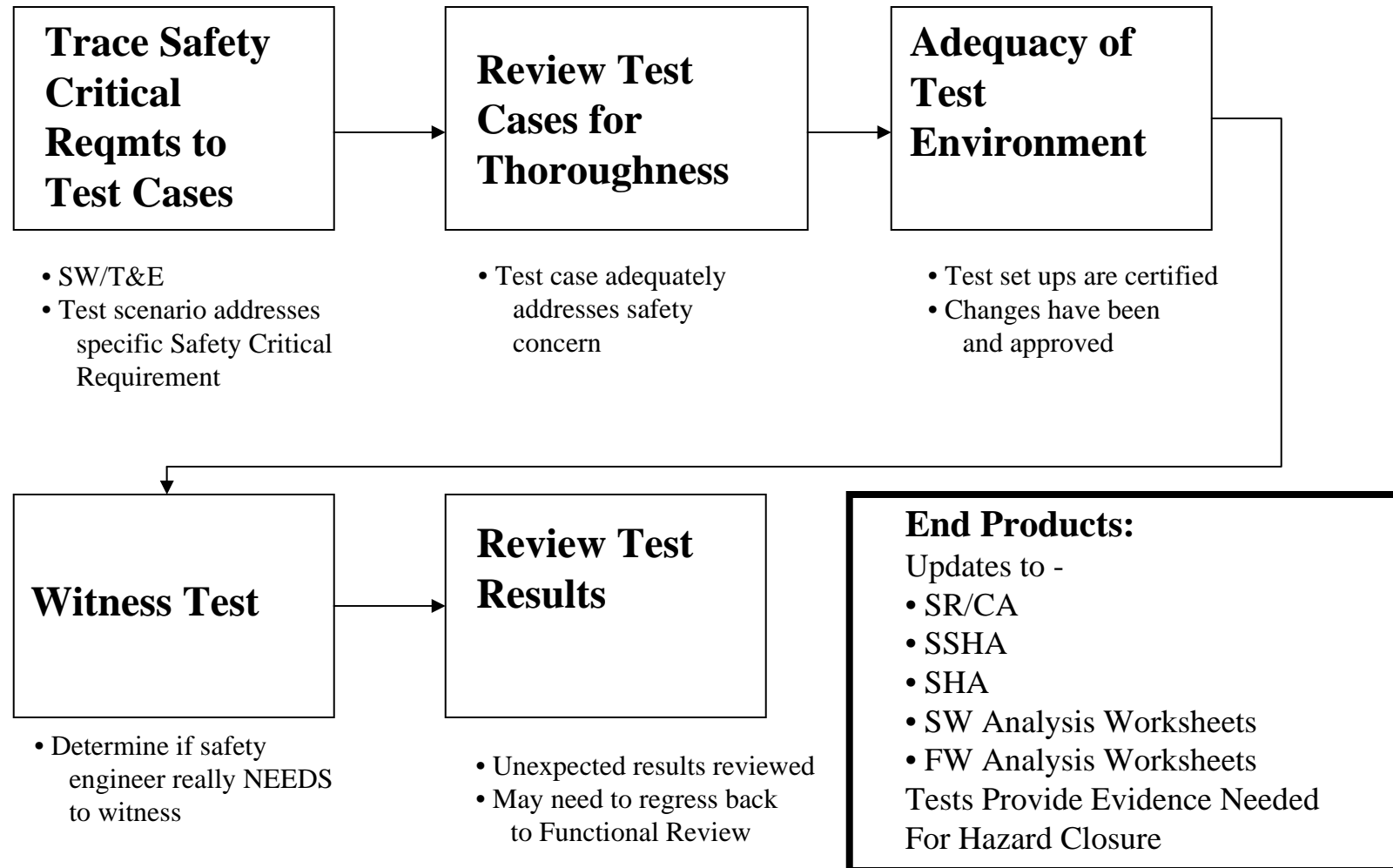
- What does this mean/how do you do it?
 - Changes, changes, changes – expect them
 - Use the same process described, issue is “where do you start?”

System Safety 101

Modification Type	Initiating Review
Design Change	
Hardware – Minor	Design & Implementation Code Review
Hardware – Major	Functional Review
Software/Firmware - Minor	Design & Implementation Code Review
Software/Firmware - Major	Functional Review
Technology Refresh/Insertion	
New Functionality	Functional Review
COTS Operating Environment	Design & Implementation Code Review
COTS Firmware	Design & Implementation Code Review
Modified Use of Configuration	Functional Review
New Language/Compiler	Requirements Review
New Development Paradigm	Design & Implementation Code Review
Change in Operational Environment	
Integration into New SOS	Functional Review
New Operational Environment	Functional Review
New Use or Application	Functional Review
Integration with Higher Order System	Functional Review

System Safety 101

Test Review



Software Safety Process Summary

System Safety 101

Software Hazard Analysis Worksheet

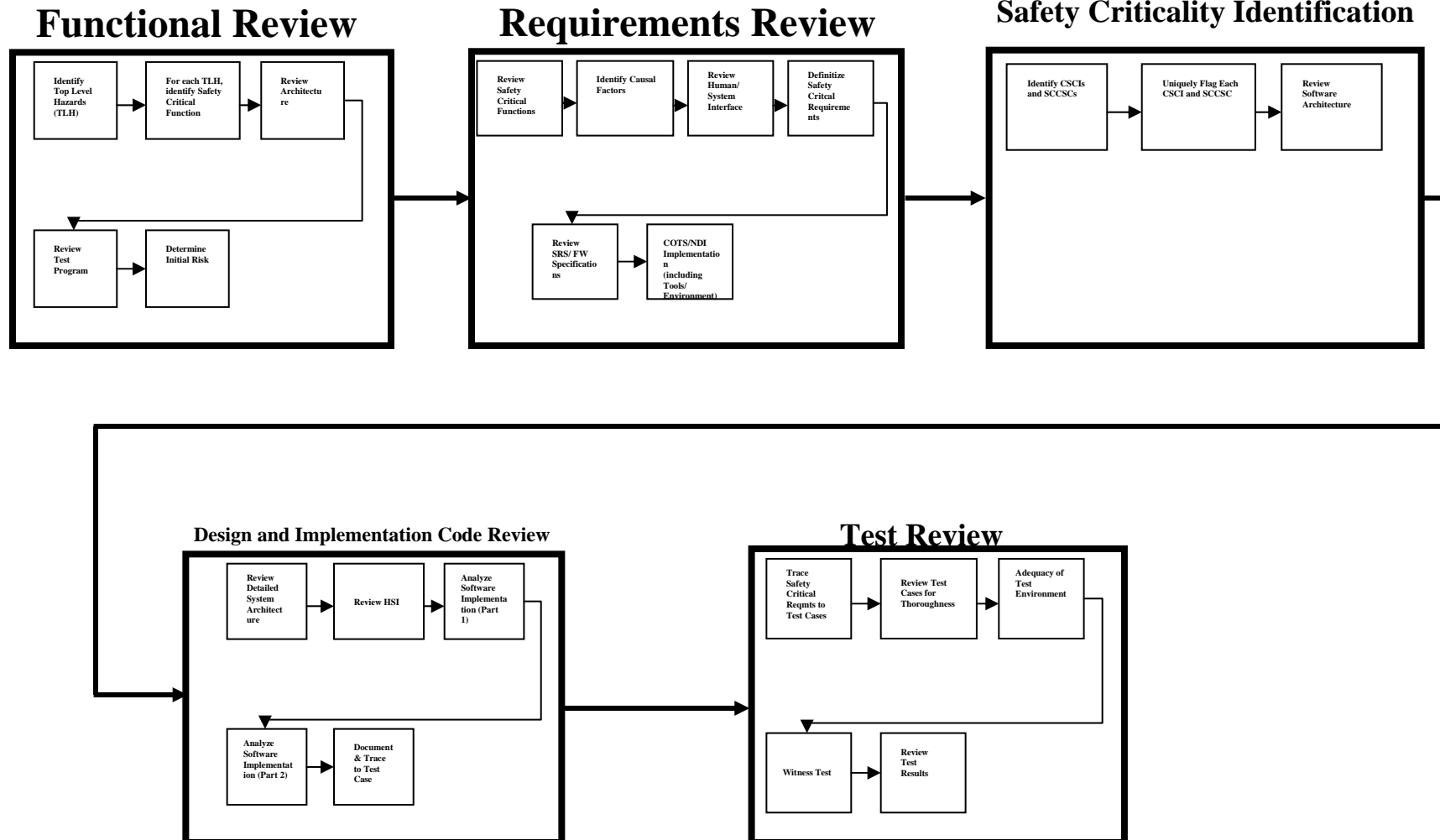
Item Number:	
Title:	
Safety Critical Function:	System State:
Causal Factor:	
System Configuration:	
Safety Critical Requirement (s):	
Software Safety Criticality Index (SSCI):	CM Control:
Code Implementation:	
Code Evaluation:	
Test Case(s):	
Test Results:	
Remarks:	
Status:	

System Safety 101

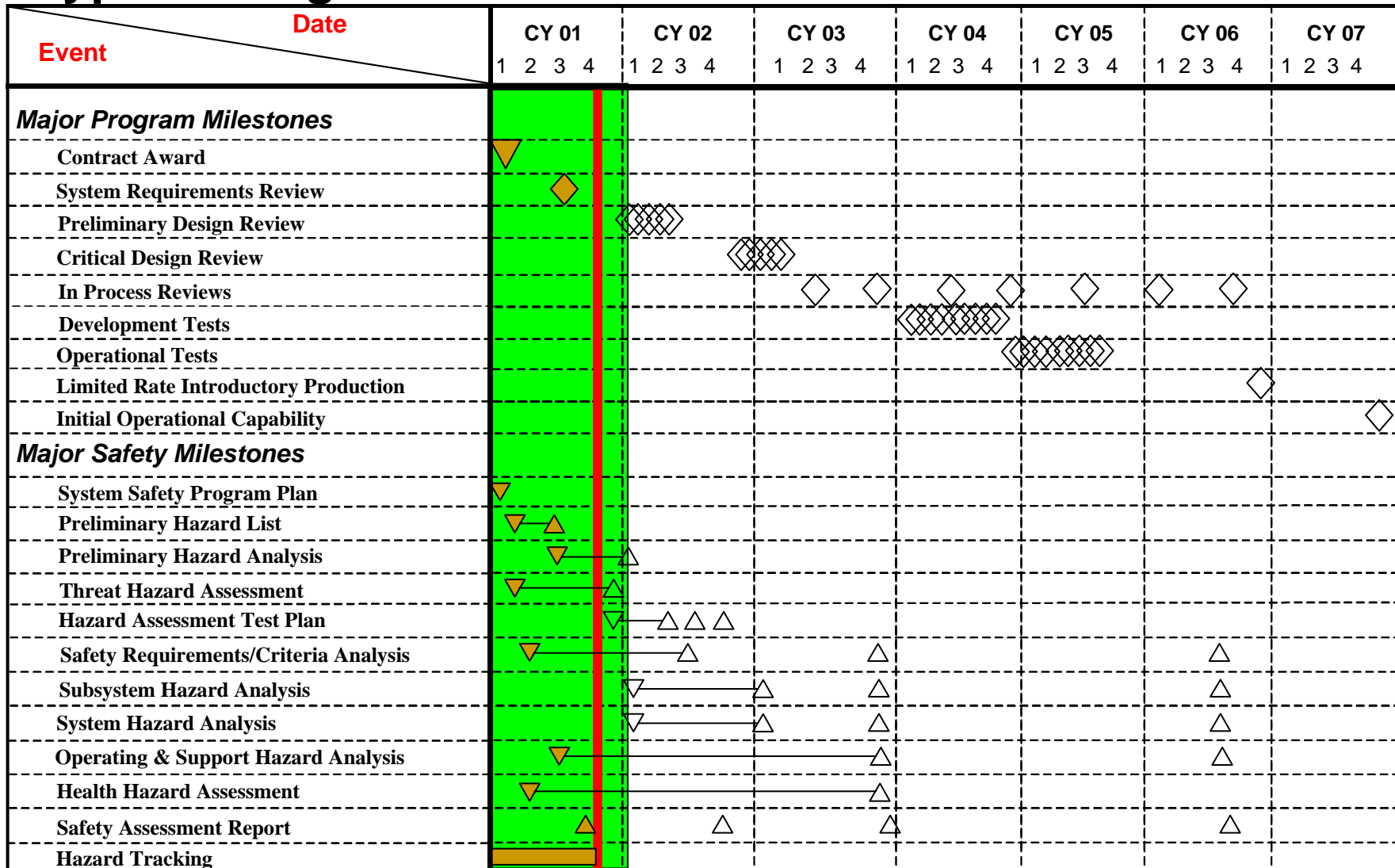
Firmware Hazard Analysis Worksheet

Item #:	Safety Critical: YES <input type="checkbox"/> NO <input type="checkbox"/>	Analyzed Programmable Logic Device (PLD): <i>An example would be U38 CPLD</i>
Safety Critical Function performed by PLD: <i>Explain the safety critical function(s) performed by the PLD</i>		
Causal Factor: A Single Event Upset (SEU) occurs within the PLD which causes a worst-case bit flip within its internal JTAG Scan Mode circuitry. This in-turn may result in all I/Os going into either a HIGH, Low, or Tristate output state. It is also possible for buffered serial streams to be outputted in the correct format required.		
PLD Interlocks: <i>A discussion of the interlocks in the system which prevent a safety mishap given a worst-case failure of this analyzed PLD</i>		
Firmware Safety Criticality Index (FSCI): High <input type="checkbox"/> Serious <input type="checkbox"/> Medium <input type="checkbox"/> Low <input type="checkbox"/> N/A <input type="checkbox"/>		
Level of Rigor / Suitability: High <input type="checkbox"/> High/Moderate <input type="checkbox"/> Moderate <input type="checkbox"/> Low <input type="checkbox"/> N/A <input type="checkbox"/>		
Vendor Part Number:	Technology Type: Antifuse <input type="checkbox"/> EPROM <input type="checkbox"/> SRAM <input type="checkbox"/>	Data Retention? Infinity <input type="checkbox"/> 100 years <input type="checkbox"/> 20 years <input type="checkbox"/> 10 years <input type="checkbox"/> N/A <input type="checkbox"/>
Raytheon Drawing Number:	Physical Location within Design: <i>e.g. GS CCA or PCU2 CCA</i>	Under CM Control: YES <input type="checkbox"/> NO <input type="checkbox"/>
PLD Implementation: <i>Explain what the PLD is doing and how it is operating within your system with special focus shown on the safety critical functions</i>		
PLD Mitigations: <i>Explain the mitigations within this system and to the PLD which prevent safety mishaps due to SEUs, etc... An example would be that "The PLD must output two discrete signals which are of different logic levels in order to activate a safety critical function; JTAG lines are properly terminated, etc..."</i>		
PLD Safety Tests / Test Cases: Recommended minimum tests to be performed to show the stability of safety critical PLDs are as follows: 1) Power-up in known safe state 2) Power-down in known safe state 3) Power-up system with a failed power-on Master Reset circuit to verify the state of the PLDs		
PLD Test Results: TBD		
Remarks: <i>Any information you want to put here that doesn't fit anywhere else. Also, if the analyzed PLD is NOT safety critical use this space to briefly explain why it is not safety critical. Safety Boards are asking for this information!</i>		
Overall Safety Assessment: <i>Make a stand, explain in a short statement whether you think this PLDs use is safe and properly mitigated or not.</i>		
Recommended Status: OPEN <input type="checkbox"/> CLOSED <input type="checkbox"/>		

System Safety 101



Typical Program Schedule with Traditional Deliverables



Threat Hazard Assessment

System Safety 101

What else is done/expected prior to PDR?

- Threat Hazard Assessment – An evaluation of the munition lifecycle environmental profile to determine the threats and hazards to which the munition may be exposed. The assessment includes threats posed by friendly munitions, enemy munitions, accidents, handling, etc. The assessment shall be based on analytical or empirical data to the extent possible

System Safety 101

- **Threat Hazard Assessment – What does that *really* mean?**
 - Determine what credible abnormal environments the weapon might encounter Cradle-to-Grave
 - Limit your credible abnormal environments to those supporting MIL-STD-2105 testing
 - Fast Cook Off
 - Slow Cook Off
 - Bullet Impact
 - Fragment Impact
 - Sympathetic Detonation
 - Shaped Charge Jet
 - Spall Impact

System Safety 101

- **Threat Hazard Assessment – Why is it important/ why do it now?**
 - Determines what tests are credible
 - Determines what system configuration will be used for Insensitive Munitions (IM) testing
 - Determines number of assets required to support each test as well as support assets (e.g., airframes, shipping containers, etc.)
 - You need to inform Program Management ASAP what the needs will be

System Safety 101

- **Threat Hazard Assessment – What do you do with it?**
 - Used to develop the program's Hazard Assessment Test (HAT) Plan
 - Used to justify number of assets and configurations
 - Configuration can both drive huge program cost/schedule risk and technical risk

System Safety 101

Threat Hazard Assessment – What are credible abnormal environments

- Bullet Impact (BI)
- Fragment Impact (FI)
- Fast Cook Off (FCO)
- Slow Cook Off (SCO)
- Shaped Charge Jet (SCJ) Impact
- Sympathetic Detonation
- Spall Impact
- Forty foot drop

Hazard Assessment Test Plan

System Safety 101

What else is done/expected prior to PDR

- Hazard Assessment Test Plan – How are you going to blow things up?
 - Based upon your THA
 - Identifies of how the program plans to test for Insensitive Munitions
 - Develop with assistance from IM Office
 - Get their concurrence with the HAT Plan prior to:
 - Start of testing
 - Going to the Review Authority

System Safety 101

Hazard Assessment Test Plan

- Provides a detailed description of each test case, including
 - Asset configuration
 - Aim points, as applicable
 - Testing requirements
- Facility conducting the test typically prepares the detailed test plans
 - Conducts test
 - Arranges all test site equipment
 - Gather post-test data
 - Generates test report
 - Presents results to Munitions Reaction Evaluation Board (MREB)
 - MREB decides reaction type

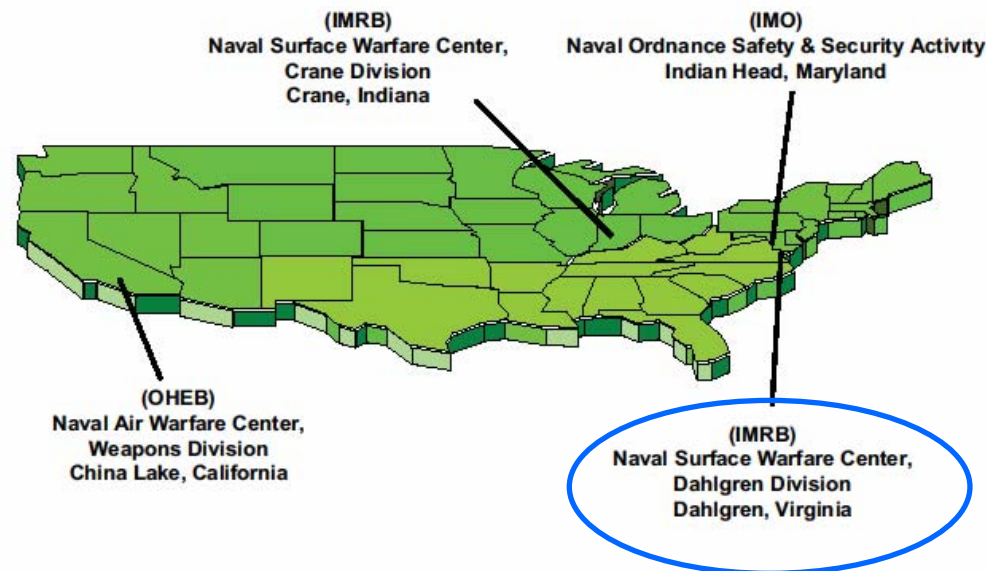
System Safety 101

MREB

-Ordnance Hazards Evaluation Board (OHEB) and Insensitive Munitions Review Boards (IMRB) have been consolidated into one official IM Navy review board called the Munitions Reaction Evaluation Board (MREB).

- MREB reviews and evaluates reactions of munitions that are subjected to unplanned stimuli such as heat, shock, and impact.

- MREB operates under the sponsorship of the Naval Ordnance Safety & Security Advisory (NOSSA), and specifically, its Insensitive Munitions Office (IMO).

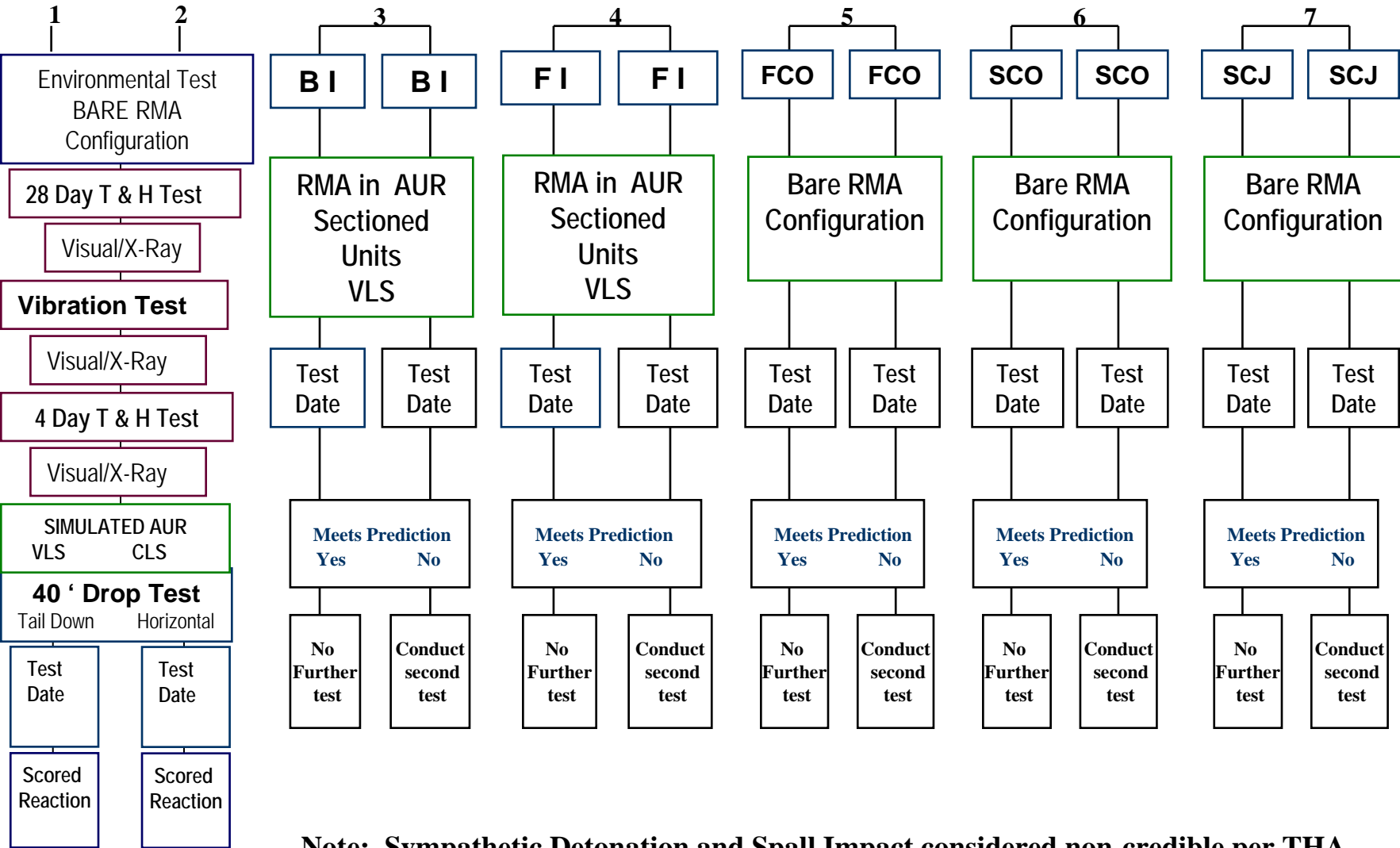


System Safety 101

Hazard Assessment Test Plan

- **Type I (Detonation Reaction).** The most violent type of explosive event. A supersonic decomposition reaction propagates through the energetic material to produce an intense shock in the surrounding medium, air or water for example, and very rapid plastic deformation of metallic cases, followed by extensive fragmentation. All energetic material will be consumed. The effects will include large ground craters for munitions on or close to the ground, holing/plastic flow damage/fragmentation of adjacent metal plates, and blast overpressure damage to nearby structures.
- **Type II (Partial Detonation Reaction).** The second most violent type of explosive event. Some, but not all of the energetic material reacts as in a detonation. An intense shock is formed; some of the case is broken into small fragments; a ground crater can be produced, adjacent metal plates can be damaged as in a detonation, and there will be blast overpressure damage to nearby structures. A partial detonation can also produce large case fragments as in a violent pressure rupture (brittle fracture). The amount of damage, relative to a full detonation, depends on the portion of material that detonates.
- **c. Type III (Explosion Reaction).** The third most violent type of explosive event. Ignition and rapid burning of the confined energetic material builds up high local pressures leading to violent pressure rupturing of the confining structure. Metal cases are fragmented (brittle fracture) into large pieces that are often thrown long distances. Unreacted and/or burning energetic material is also thrown about. Fire and smoke hazards will exist. Air shocks are produced that can cause damage to nearby structures. The blast and high velocity fragments can cause minor ground craters and damage (breakup, tearing, gouging) to adjacent metal plates. Blast pressures are lower than for a detonation.
- **d. Type IV (Deflagration Reaction).** The fourth most violent type of explosive event. Ignition and burning of the confined energetic materials leads to nonviolent pressure release as a result of a low strength case or venting through case closures (loading port/fuze wells, etc.). The case might rupture but does not fragment; closure covers might be expelled, and unburned or burning energetic material might be thrown about and spread the fire. Propulsion might launch an unsecured test item, causing an additional hazard. No blast or significant fragmentation damage to the surroundings; only heat and smoke damage from the burning energetic material.
- **e. Type V (Burning Reaction).** The least violent type of explosive event. The energetic material ignites and burns, non-propulsively. The case may open, melt or weaken sufficiently to rupture nonviolently, allowing mild release of combustion gases. Debris stays mainly within the area of the fire. This debris is not expected to cause fatal wounds to personnel or be a hazardous fragment beyond 15 m (49 ft)

System Safety 101



Note: Sympathetic Detonation and Spall Impact considered non-credible per THA

System Safety 101

MIL-STD-2105C



Fuel fire such as on a carrier flight deck.

Heat or conflagration in an adjacent compartment.

Low velocity gunfire threats.

High velocity fragments from high performance warheads.

Propensity for mass detonation of adjacent rounds.

Shaped charge weapon attack (with calibers from 40mm upwards).

Pass	V	Burning reaction (FCO, SCO, BI, FI) or no propagation (SD) or no detonation (SCJ)
Fail	IV	Deflagration or propulsive reaction
Fail	III	Explosion
Fail	I / II	Detonation

Safety Requirements/ Criteria Analysis

System Safety 101

What else is done/expected prior to PDR

- Safety Requirements/Criteria Analysis (SR/CA) - Identified as Task 203 in MIL-STD-882 (Initial delivery)
 - Relates the hazards identified to the system design and identifies or develops design requirements to eliminate or reduce the risk of the identified hazards to an acceptable level

System Safety 101

Safety Requirements/Criteria Analysis (SR/CA)

- Documents the safety design requirements/ design criteria for the system
- Requirements can be derived or imposed from several sources
 - Contractually imposed requirements
 - Generic safety requirements, such as MIL-STD-1901A, MIL-STD-1472, MIL-STD-2105, etc.
 - Requirements derived from the PHL and/or PHA
- The SR/CA is the device to ensure requirements are clearly identified and tracked through closure

System Safety 101

SR/CA – So, what do you do?

- Combine the requirements from the contract, PHL/PHA and generic sources into a single listing
- Categorize each requirement into one of the following three groups:
 - Detailed requirements: These are detailed design requirements, such as “The ignition system shall not be capable of being manually armed”
 - Procedural requirements: These are requirements, typically from PHL/PHA/Operating & Support Hazard Analysis (O&SHA), that are procedural addressed, such as “Personnel shall visually verify the device is in the SAFE position prior to installation”
 - Task/Analysis requirements: These are requirements that require a task or analysis be performed, such as “In order to preclude unintended or premature ignition system arming or initiation, the ignition system shall not be susceptible to common-mode failures”

System Safety 101

SR/CA – So, what do you do?

- After each identified hazard has been listed and categorized, map each requirement, procedure and task to the top level hazards identified in the PHL/PHA
 - Many will be fairly straight forward, such as mapping a procedure to de-energize components prior to performing system maintenance to a personnel death/injury hazard
 - Several will require some imagination, such as a task “A safety program shall be established in accordance with MIL-STD-882”
 - Although the intent is to map each requirement to a specific hazard, it may be necessary to map one to several/many hazards
 - Another issue is mapping all requirements to a single hazard, such as “Personnel injury/death”

System Safety 101

SR/CA – So, when do you do it?

- The SR/CA is a living document
- Initial efforts associated with the SR/CA can begin during the proposal phase, but should definitely start no later than completion of PHL
- The initial SR/CA is delivered prior to Critical Design Review (CDR)
 - Updated prior to both pre-Flight Test and pre-LRIP Review Authority meetings

Remember – The SR/CA is updated throughout the lifecycle

System Safety 101

SR/CA – So, how do you close it

Individual requirements can be closed out based upon their grouping:

- Detailed requirements: These are contained in the SRS/Unit specs and should be closed no later than at the completion of Verification Testing
- Procedural requirements: These are incorporated into maintenance procedures, operating procedures, Tech Manuals, Maintenance Requirement Cards (MRCs), training, etc. They are typically closed after completion of Flight Test when all procedures are completed
- Task/Analysis requirements: These are follow-on activities. The timing of their closure is dependent upon the task/analysis identified

System Safety 101

SR/CA – What’s documented?

SR/CA document format is as follows:

- Front matter, including a forward, table of contents, scope, purpose, system description, summary of results, methodology, recommendations, and conclusions
- Appendix A will contain the worksheets
- Appendix B will contain the combined listing of requirements/recommendations
- Appendix C will contain the list of hazards
- Appendix D will contain a mapping of requirements/procedures/tasks to each hazard

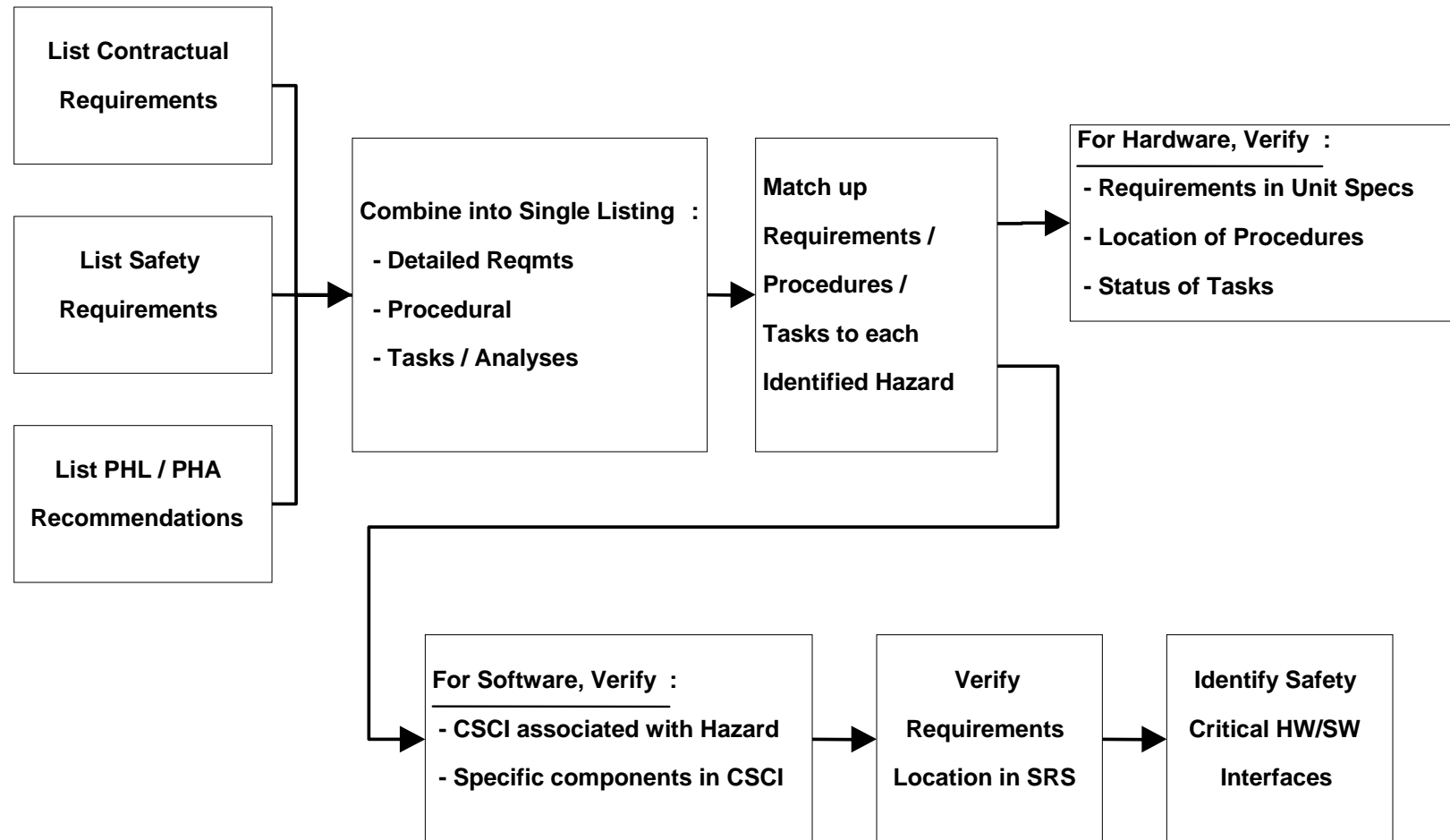
System Safety 101

SR/CA – What’s documented in the worksheets?

- Hazard Number: C-
- Brief Hazard Description:
- Related PHL/PHA Hazard Number:
- Recommended Action(s)/Requirements:
- Location in Documentation:
- Associated Task/Analysis:
- Identified Safety Critical Interfaces:
- Identified SCCSC:

System Safety 101

SR/CA Process Flow



Operating & Support Hazard Analysis

System Safety 101

What else is done/expected prior to PDR

- Operating & Support Hazard Analysis (O&SHA) - Identified as Task 206 in MIL-STD-882
 - Evaluates activities for hazards or risks introduced into the system by operational and support procedures and to evaluate adequacy of operational and support procedures used to eliminate, control, or abate identified hazards or risks

System Safety 101

O&SHA – What do you do?

- Introduce the operator into the analysis loop
- Although the O&SHA isn't typically delivered until prior to start of flight tests, activities start prior to PDR.

Considerations include

- Initiate Human-System Interface (HSI) activities
- Start logging and tracking procedural requirements identified as part of the SR/CA
- Identify system architecture from a hardware/software/human intent perspective
- Review planned configuration/state at each phase
- Identify planned concurrent tasks/operations

System Safety 101

O&SHA – What do you do?

- Considerations include
 - The ranges of all planned environments
 - Tools and support equipment required
 - Contractually imposed health requirements or material limitations
 - Test equipment, including software
 - Review sequence of operations
 - Review should include end-user input
 - Potential for human error during operations
 - Review of operating/maintenance/support procedures
 - O&SHA is the vehicle to ensure all WARNING and CAUTION notes are implemented in the proper documents
 - Document how you can close out the procedural requirements called out in the SR/CA

System Safety 101

O&SHA – What’s documented

- Typical of any hazard analysis, provide front matter
 - Executive Summary
 - Table of Contents
 - Scope/Purpose/Acronyms
 - Summary of Results
 - System Description/Operation
 - Analysis Methodology
 - Hazard Risk Index
 - Data Sources
 - Analysis Results
 - Conclusion/Recommendations
 - Worksheets

System Safety 101

O&SHA – What’s documented in the worksheets?

- Hazard Number: O-
- System Phase/Component:
- System Operation Description:
- Detailed Hazard Description:
- Related PHL/PHA Hazard Number:
- Hazard Identification/Indication:
- Effect of Hazard:
- Risk Assessment:
- Recommended Action:
- Effect of Recommended Action:
- Remarks:
- Status:
- Caution and Warning Notes:

Health Hazard Assessment

System Safety 101

What else is done/expected prior to PDR

- Health Hazard Assessment (HHA) - Identified as Task 207 in MIL-STD-882
 - Also known as Occupational and Health Hazard Assessment (OHHA)
 - Identifies health hazards and proposes protective measures to reduce the associated risk
 - HHA is not limited to the use of hazardous materials and how they contribute to a health issue, but also need to consider biological, physical, ergonomic and chemical aspects of the system

System Safety 101

HHA – What do you do?

- Introduces materials and environments into the analysis loop
- As with the O&SHA, the HHA isn't delivered until prior to start of flight tests, but activities start prior to PDR
- Prior to starting the HHA, determine who or if a Programmatic Environmental, Safety, and Health Evaluation (PESHE, AKA Programmatic Environmental, Safety, and Occupational Health {ESOH} Evaluation) will be performed for the program
 - Align the HHA data with data required to support PESHE preparation

System Safety 101

HHA – How do you do it?

- Start with the Approved Parts List (APL) or equivalent
 - Identify all components used within the system design
 - Where applicable, gather Material Safety Data Sheets (MSDSs)
 - Identify the materials used in the parts to the maximum extent practical
 - Review any issues relative to compatibility
 - Work with Environmental, Health and Safety (EHS) organization, if available
 - Create an Appendix to HHA to document Approved Parts List (APL) review

System Safety 101

HHA – How do you do it?

- Review the Concept of Operations (ConOps) to see how the system will be used
- This is done in concert with the O&SHA preparation and includes:
 - System layout
 - Operating environments
 - Temperature, acoustical, radiation, etc.
 - Required operator actions
 - Planned maintenance
 - Make sure maintainers can access
 - Try to locate components with a relatively low Mean Time Between Failures (MTBF) in accessible areas
 - Unplanned maintenance

System Safety 101

HHA – What do you do with the data?

- Considerations include
 - Chemical hazards (e.g., hazardous materials that are flammable; corrosive; toxic; carcinogens or suspected carcinogens; systemic poisons; asphyxiants, including oxygen deficiencies; respiratory irritants; etc.) {SSHA}
 - Physical hazards (e.g., acoustical energy, heat or cold stress, ionizing and non-ionizing radiation) {O&SHA}
 - Biological hazards (e.g., bacteria, fungi, etc.) {SSHA}
 - Ergonomic hazards (e.g., lifting requirements, task saturation, etc.) {O&SHA}
 - Other hazardous, or potentially hazardous, materials that may be formed by the introduction of the system. or by the manufacture, test, maintenance or operation of the system (e.g., pure tin parts, etc.) {SSHA}

System Safety 101

HHA – What do you do with the data?

- HHA data will directly contribute to several areas:
 - Hazardous Material Management Program (HMMP) plan and subsequent reports
 - Demil/Disposal Plan
 - O&SHA
 - PESHE
- Again, organize HHA data to support other documents and avoid duplication of effort

Safety Assessment Report

System Safety 101

What else is done/expected prior to PDR

- Safety Assessment Report (SAR) - Identified as Task 301 in MIL-STD-882
 - Documents a comprehensive evaluation of the mishap risk being assumed prior to test or operation of a system, prior to the next contract phase or at contract completion

System Safety 101

SAR – Why discuss SAR during pre-PDR?

- SAR contains data from other sources, such as hazard analyses, ConOps, test plans/reports, etc.
- Initial SAR forms the basis of the Review Authority (RA) data package
- The RA evolutions are addressed in the next briefing topic (so just trust me)
- Preparation of the SAR may begin during pre-PDR based upon four deliveries
 - Pre-PDR
 - Pre-Critical Design Review (CDR)
 - Pre-Flight Test
 - Pre-Low Rate Initial Production (LRIP)

System Safety 101

SAR – What does the SAR contain?

- Define the specific purpose of the requested assessment
- System description
- Safety features of the system design, both hardware and software
- Identified hazards
 - Type of hazard
 - Hardware
 - Software
 - Procedural – Including Cautions and Warnings
 - Environment of each hazard
 - Normal environment
 - Credible Abnormal Environments
 - Recommendations addressing each hazard

Pre-PDR
Pre-Critical Design Review (CDR)
Pre-Flight Test
Pre-Low Rate Initial Production (LRIP)

System Safety 101

SAR – What does the SAR contain?

- Risk/Criticality Index Matrices
 - Approval authority for risk acceptance
- Results of analyses
 - Residual risk
- Results of testing
 - What criteria or requirements were verified
 - Unexpected results
- Hazardous materials
 - Material type, quantity, and potential hazards
 - Safety precautions and procedures necessary during use, packaging, handling, storage, transportation, and disposal
 - MSDSs

Pre-PDR
Pre-Critical Design Review (CDR)
Pre-Flight Test
Pre-Low Rate Initial Production (LRIP)

System Safety 101

SAR – What does the SAR contain?

- Explosive components
 - Explosive Ordnance Disposal (EOD) data
 - Hazard classification data
 - Explosive qualification data
- Post- launch safety-related activity of expendable launch vehicles and their payloads including deployment and operation
- If applicable, orbital safety issues
- Signed statement, by appropriate authority, that all identified hazards have been eliminated or their associated risks controlled to acceptable levels

Pre-PDR
Pre-Critical Design Review (CDR)
Pre-Flight Test
Pre-Low Rate Initial Production (LRIP)

System Safety 101

SAR – What does the SAR **NOT contain?**

- Marketing pamphlets on lab facilities, office space layout, etc.
- Test results from components “just like this”
- System description/front matter from analyses in appendices that replicates SAR data

Review Authority Evolutions

System Safety 101

Review Authority is dependent on the US government customer

- USN/USMC – Weapon System Explosives Safety Review Board (WSESRB)
- USAF – Non-Nuclear Munitions Safety Board (NNMSB)
- USA – Army Fuze Safety Review Board (AFSRB)

This presentation focuses on a typical USN program and assumes the contractor prepares the data package/presentation

System Safety 101

WSESRB

For a typical USN program, plan on a minimum of five WSESRB evolutions

- Introduction – Concurrence with safety program
 - Pre-Critical Design Review – Informational briefing
 - Pre-Flight Test – Concurrence to bring weapons onboard USN platform
 - Pre-LRIP – Concurrence for low rate initial production
 - Pre-FRP – Concurrence for full rate production
-
- Additionally, plan on an evolution five years after introduction to the fleet or after major modifications

System Safety 101

WSESRB

- Each WSESRB evolution may require up to four actual presentations
 - WSESRB {All four}
 - Software Systems Safety Technical Review Panel (SSSTRP) {Pre-CDR, Pre-Test, Pre-LRIP, Pre-FRP}
 - Fuze and Initiation Systems Technical Review Panel (FISTRP) {Pre-CDR, Pre-Test}

System Safety 101

WSESRB

- In addition to formal presentations, other reviews may also occur
 - Technical Interchange Meetings {TIM} (SSSTRP, FISTRP)
 - Executive Briefings (WSESRB)
 - Secretariat Meeting – Urgent review
 - Executive Board – Large visible program prior to fielding
 - Classified Board – Urgent and classified
 - Letter Data Package – Minor changes, test results and response to previously actions/findings

System Safety 101

WSESRB

- Each WSESRB evolution will require a data package and presentation material
- Data package content is dependent upon when the program is presented
- If at all possible, generate a single data package to address all potential reviews within the evolution
 - The following charts provide a notional idea of when certain contents are initially provided and who provides them
 - Customer provided data
 - Introduction
 - Pre-CDR
 - Pre-Flight Test
 - Pre-LRIP/FRP

WSESRB Data Package

Customer provided data
Introduction
Pre-CDR
Pre-Flight Test
Pre-LRIP/FRP

- *Program Background and Overview*
- _____ (1) Table of Content
- _____ (2) Acronym List
- _____ (3) Executive Summary
- _____ (4) Purpose of WSESRB Meeting (*Point in the life cycle at which review is conducted.*)
- _____ (5) Background
- _____ (6) Program Schedule and Milestone Chart
- _____ (7) Technical Support Agency(s)
- _____ (8) Who's Who Programmatically
- _____ (9) Acquisition Category (ACAT) Level
- _____ (10) Past WSESRB Meetings: Comments, Action Items, Recommendations Assigned Status, and Resolution of Action Items

- *System Description*
- _____ (1) Detailed Design Description (*To include assessment of complexity and level of software involvement.*)
- _____ (2) Description of Intended Use and Transport
- _____ (3) Description of Explosive Components
- _____ (4) Description of Production to Target Sequence (*Include Environmental Profile.*)
- _____ (5) Description of Special Facility Requirements
- _____ (6) Description of Hazardous Materials
- _____ (7) Surveillance Program/Plan
- _____ (8) Description of Configuration Management Processes

WSESRB Data Package

Customer provided data

Introduction

Pre-CDR

Pre-Flight Test

Pre-LRIP/FRP

- System Safety Program
- _____ (1) Introduction/Objectives
- _____ (2) Safety Program Milestones in Relation to the Program Acquisition Phases
- _____ (3) Safety Program Management Organization
- _____ (4) Risk Assessment Methodology (*To include HRI*)
- _____ (5) Interpretation of Hazard Analysis Results (*i.e., PHA, SHA, SSHA, O&SHA, SAR, Software Hazard Analysis, etc.*)
- _____ (6) Interpretation of Special Safety Analysis (*i.e., FEMECA, Bent Pin Analysis, Safety Audits, FTAs, Sneak Circuit Analysis, etc.*)
- _____ (7) Safety Related Configuration Control Process
- _____ (8) Demilitarization and Disposal Plan
- _____ (9) Explosive Ordnance Disposal Procedures and Validation Plan
- _____ (10) Hazard Test Program Description and Results
 - Hazard Test Plan and Results
 - Comparison and test limits to environmental profile and safety analysis
 - Special Hazard Test Description and Results
- _____ (11) Explosive Qualification Test Description and Results
- _____ (12) Insensitive Munitions Test Description and Results
- _____ (13) MIL-S-901D Shipboard Shock, Test Plan and Results
- _____ (14) Hazards of Electromagnetic Radiation to Ordnance (HERO), Electrostatic Discharge (ESD) and Lightning Test Plan(s) and Results
- _____ (15) Shipboard Test Results
- _____ (16) Land-Based Test Results
- _____ (17) Explosive Hazard Classification (*Final for Production Approval*)
- _____ (18) Hazardous Material Use and Minimization Efforts for Environmental Concerns

System Safety 101

WSESRB Data Package

- *Summary Safety Assessment*
- _____ (1) Residual Risk Assessment
 - Populated HRI Matrix of Residual System Safety Risk
- _____ (2) Principal For Safety's Safety Assessment
- _____ (3) Conclusion
- *Appendix – Contractor Safety Assessment Report (SAR)*
- *Appendix – System Safety Program Plan*
- *Appendix – Hazard Analysis*
- _____ (1) Preliminary Hazard Analysis (PHA)
- _____ (2) Facilities PHA
- _____ (3) Failure Modes, Effects and Criticality Analysis (FMECA)
- _____ (4) System and Sub-System Hazard Analysis (SHA & SSHA)
- _____ (5) Fault Tree Analysis (FTA)
- _____ (6) Operating and Support Hazard Analysis (O&SHA)
- _____ (7) Software Hazard Analysis
- _____ (8) Analysis of the Integration of the Weapon System with the Platform
- _____ (9) Other Safety Analyses/Assessments
- _____ (10) Hazardous Material/Toxic Substances Material Data Sheets
- _____ (11) Hazard Action Report (HAR) Forms

Customer provided data

Introduction

Pre-CDR

Pre-Flight Test

Pre-LRIP/FRP

System Safety 101

WSESRB Data Package

Customer provided data
Introduction
Pre-CDR
Pre-Flight Test
Pre-LRIP/FRP

- *Appendix – Other Reference Material*
- _____ (1) Safety Related Test Results
- _____ (2) Explosive Qualification Test Results
- _____ (3) Final Type Qualification Test Results
- _____ (4) Final Hazard Classification Test Results
- _____ (5) Insensitive Munitions Test Results
- _____ (6) Hardware Safety Test Results
- _____ (7) Software Safety Test Results
- _____ (8) Performance Oriented Packaging (POP) Test Results
- _____ (9) Vertical Replenishment (VERTREP) Test Results or Comparison Data
- _____ (10) Handling Equipment Design Overload Test Results
- _____ (11) Container Qualification Test Results
- _____ (12) Manuals (pertinent to the assessment of the system's safety including technical training manuals or videos)
- _____ (13) Non-standard Reference Data
- _____ (14) Letters/Memos (pertinent to the assessment of the system's safety)
- _____ (15) Accident/Incident Reports

System Safety 101

WSESRB Data Package

- Emphasis of the data package should be:
 - design,
 - life cycle,
 - safety features, and
 - results of the System Safety Program
- Design description does not require a full set of design drawings
 - Documents such as assembly drawings, explosive loading drawings, draft Navy Munitions Data, explosive specifications, firing circuits, or sketches which describe the system are required
 - Emphasize explosive components and other hardware affecting weapon system safety
 - Describe the interaction of any system software with the safety critical aspects of the system.

System Safety 101

WSESRB Data Package

- Life cycle description include a concise but thorough description of the intended use of the system
 - Address subjects such as usage environment, handling equipment and methods of use, replenishment methods, packaging and transportation methods, launching platform, operational sequence, demilitarization, and disposal methods
 - Include special safety procedures required to respond to potential malfunctions

System Safety 101

WSESRB Data Package

- Safety features report the system's compliance with relevant design safety requirements, standards and specifications and special safety features implemented in the system design
- Results of the safety program include a listing of all hazard tests and analyses conducted, test parameters and results, as well as type and scope of analyses
 - Address the rationale for test and test parameter selection
 - Report anomalies noted during explosives qualification or final type qualification testing
 - Describe all safety devices incorporated in the system as well as precautionary measures to be invoked
 - Review the analyses conducted and their results, noting any unresolved or open hazards

System Safety 101

WSESRB Data Package

Data packages **SHOULD NOT** include:

- Filler
 - 28 xeroxes of circular temp charts
 - 100 pages of data logger output
- Individual formal test reports, each of which has the same 10 page boilerplate system description
- 37 8x10 color photos with circles and arrows and a paragraph of explanation on the back
- Pretty white 3 ring binders
- Colored dividing pages that keep members from throwing it in the recycle bin

Unlike a deli, you don't get paid by the pound

System Safety 101

WSESRB Presentation

- Unfortunately, plan on a separately focused presentation for each review within an evolution
 - WSESRB is top level and programmatic
 - SSSTRP is analysis methodology/results and should include a compliance matrix for STANAG 4404
 - FISTRP is AFD/SAD specific and should include compliance matrices for MIL-STDs-1901/1316/1512

System Safety 101

WSESRB Presentation

- Each presentation procedure is different
 - WSESRB is formal, recorded and 3 or 4 hours
 - Two hour presentation (allow for 30 minutes of questions)
 - One hour caucus
 - Reconvene and distribute preliminary findings
 - SSSTRP is less formal and may last 8 hours of open discussion
 - plan on a 3 or 4 hour presentation
 - FISTRP is less formal and may last 2 hours of open discussion
 - plan on a 2 hour presentation, normally open to “what ifs”, especially during TIMs

System Safety 101

WSESRB Presentation

Some other ideas

- Make sure both the purpose and recommendation match
 - Be very careful of how you state a purpose
- Have multiple dry-runs with the actual presenters
- Limit attendance and establish protocol BEFORE the meeting as far as answering questions

System Safety 101

Design For Environment Tasks

- Environmental Trade Study
- Hazardous Material Management Program Plan
- Demilitarization and Disposition Program Plan
- Preliminary Demil Assessment
- Design For Environment Analysis
- Design For Demil Analysis
- Hazardous Material Management Program Report

System Safety 101

What else is done/expected prior to PDR

- Environmental Trade Study (ETS)
 - ETS performed during the proposal effort to identify potentially hazardous materials/processes and propose alternative methods of complying with the performance requirements
 - The ETS purpose is to begin to identify high profile or targeted for reduction materials that, due to their chemical, physical or biological nature cause safety, public health or environmental concerns that result in an elevated level of management effort

System Safety 101

ETS – What do you do?

- Introduces materials and their alternatives into the analysis loop
- ETS evaluates the materials selected as part of the proposed concept and considers the potential safety risk associated with accepting and using the materials
- ETS identifies each material type, its quantity and potential hazards associated with that material over the product's life cycle

System Safety 101

ETS – What are potentially hazardous materials?

- Materials which may present a hazard during normal customer use, handling and/or servicing of a delivered product
- Materials that require unusual or unique handling during normal disposition of the product
- High profile/targeted materials that are of elevated interest or concern to the customer (specified in contract)
- Materials subject to statutory phase-outs or regulatory use restrictions
- Radioactive material
- Hazardous materials required for field use
- Propulsion fuels, propellants and explosives

System Safety 101

What else is done/expected prior to PDR

- Hazardous Material Management Program (HMMP) Plan
 - The HMMP Plan identifies high risk materials or processes that are of elevated interest or concern to the customer or are targeted for reduction or elimination due to their chemical, physical or biological nature that cause safety, public health or environmental concerns
 - Identified hazardous materials are evaluated in formal and informal trade analysis utilizing the methods and processes described in the HMMP Plan

System Safety 101

What else is done/expected prior to PDR

- Demilitarization and Disposition Program (DM&DP) Plan
 - Purpose of the task is to identify and outline a plan to prepare and submit a Demil plan report for the all up rounds and major system sections
 - Identifies the energetics, classified components, and hazardous materials (EHC) that must be included in the detailed demilitarization plan report

System Safety 101

DM&DP Plan – What do you do?

- Demil plans are prepared and submitted in accordance with the RMS Demilitarization / Disposition Common Process template approved by all services 12/1/2003
- The Demil plan identifies how to disassemble and demilitarize an item or its components in a safe and environmentally acceptable manner
- DM&DP Plan process identifies what type and level of detailed data will be required to determine:
 - Products of combustion
 - Specific impacts of Demil & Disposition (DM&D) processes
 - Analysis of residual materials
 - Characteristics of materials
 - Drawings
 - Disassembly level
 - Plans for end items.

System Safety 101

What else is done/expected prior to PDR

- Preliminary Demil Assessment (PDA)
 - Purpose of the PDA is to perform and document a DM&DP assessment of Explosive, Hazardous and Classified (EHC) components
 - PDA includes specific critical spares and re-usable components

System Safety 101

PDA – What do you do?

- PDA is performed to identify:
 - Risks associated with material demilitarization and disposal
 - Ease of disassembly to access lowest required level
 - Future source of supply and reuse opportunities
 - Cost estimate for DM&DP tasks
- Consists of constructing a disassembly technology tree that identifies labor, processes, materials, and waste streams associated with DM&DP of components and subassemblies
- PDA evaluates, as a minimum, the following DM&D system safety elements:
 - Intractable demil concerns
 - Un-separable energetic components
 - Range sustainability and live fire considerations
 - Residual energetic materials and decontamination concerns
 - Capture and recycle of hazardous materials
 - Preferred demil and disposal processes
 - Human factors and environment release risk
 - Ease of disassembly
 - Materials risk analysis

System Safety 101

What else is done/expected prior to PDR

- Design For Environment (DFE) Analysis
 - DFE process results in configurations, materials, processes, components, technologies, and procured items that are superior from an environmental, health, and safety standpoint
 - Intent of DFE is to identify and minimize potential life cycle safety/environmental risks and costs proactively at the design stage

System Safety 101

DFE Analysis – What do you do?

- The DFE analysis includes conducting both formal and informal trade studies of current materials and processes versus less hazardous alternatives
- Where materials are identified as targeted or prohibited by contract, the task includes flowing down the prohibition(s) and the targeted materials to subcontractors preferably completed via request-for-proposal/bid and purchase documents with the subcontractor
- As part of the DFE process, the safety engineer evaluates whether the materials will require safety precautions or procedures during use, packaging, handling, storage, transportation, and disposal

System Safety 101

What else is done/expected prior to PDR

- Design For Demil (DFD) Analysis
 - The purpose of the task is to identify and conduct safety hazard analysis of DM&DP processes where current design development material or process selections increase the future safety and/or disposal risks
 - DFD tradeoff analysis includes:
 - Review of preferred demil/disposal methods
 - Ammunition Peculiar Equipment (APE)
 - Material selections
 - Assembly methods
 - Design configuration
 - Life cycle cost drivers
 - Re-use potential
 - Secondary markets
 - Spares requirements

System Safety 101

DFD Analysis – What do you do?

- The DFD is performed on identified processes, sections, or sub-assemblies where current design development could result in higher end of life risk or total ownership cost
- DFD may be performed on materials, processes, or hardware identified from the PDA or the HHA
- The DFD evaluates, as a minimum, the following DM&DP elements:
 - Material selections and materials of construction
 - Method of assembly/ease of disassembly
 - Demil and disposal processes
 - Resource recovery
 - Intractable demil concerns
 - Modularity/Reuse opportunities
 - Reliability/maintainability enhancements
 - Materials risk analysis
 - Product secondary highest value use
 - Un-Separable Energetic Components

System Safety 101

What else is done/expected prior to PDR

- HMMP Report
 - HMMP Report documents the elimination or reduction of hazardous materials in deliverable systems, system components and associated support items
 - The HMMP Report documents how we are complying with the requirements established in the HMMP Plan

System Safety 101

AGENDA

- Before You Start
- Pre-Preliminary Design Review
 - System Safety Program Plan
 - Software Safety Program Plan
 - Preliminary Hazard List/Preliminary Hazard Analysis
 - Threat Hazard Assessment
 - Hazard Assessment Test Plan
 - Safety Requirements/Criteria Analysis
 - Operating & Support Hazard Analysis
 - Health Hazard Assessment
 - Safety Assessment Report
 - Review Authority Evolutions
 - Design For Environment Tasks
 - Environmental Trade Study
 - Hazardous Material Management Program Plan
 - Demilitarization and Disposition Program Plan
 - Preliminary Demil Assessment
 - Design For Environment Analysis
 - Design For Demil Analysis
 - Hazardous Material Management Program Report
- Pre-Critical Design Review
 - Subsystem Hazard Analysis
 - System Hazard Analysis
 - System Safety Engineering Report
 - Explosive Ordnance Disposal Data Package
 - Explosive Hazard Classification Data Report
 - Technical Data for Munitions
- Pre-First Flight Test
 - Range Safety Data Package
 - DM&DP Plan and Report
- Other Analyses
 - Fault Tree Analysis
 - Bent Pin Analysis
 - Inadvertent Launch Analysis
- Other Topics
 - Test Set Safety Process
 - Configuration Management
 - Engineering Change Proposals, Deviations, Waivers
 - Hazard Tracking
 - Hazard Action Report

Subsystem Hazard Analysis

System Safety 101

What is done/expected prior to CDR

- Subsystem Hazard Analysis (SSHA) - Identified as Task 204 in MIL-STD-882
 - Verifies subsystem compliance with safety requirements contained in subsystem specifications and other applicable documents
 - Identifies previously unidentified hazards associated with the design of subsystems including component failure modes and critical human error inputs
 - Identifies hazards resulting from functional relationships between components and equipment comprising each subsystem

System Safety 101

SSHA – What do you do?

- Analyze the subsystems almost as a series of black boxes
 - Consider the operator from a human error perspective
- Key emphasis of the SSHA is focusing on failure modes of components within the subsystems
- What's a subsystem?
 - For a missile program, it could be propulsion, electrical, warhead, fuel, guidance, etc
 - Each subsystem can also be broken down further to the component level, such as propulsion
 - Propellant
 - Arm/Fire Device – Can be broken down
 - Case
 - Liner
 - Thrust Vector Control – Can be broken down

System Safety 101

SSHA – What do you do?

- Considerations include
 - Failure modes, failure modes, failure modes
 - Work with Reliability Engineering in determining the Failure Modes, Effects and Criticality Analysis (FMECA) or FMEA guidelines
 - Identify what the credible failure modes are up front
 - Human error should be considered as a failure mode
 - Performance and degradation
 - Determine how the failure can impact system level performance
 - Identify critical timing routines
 - Specify testing environments
 - Ensure top level hazards pertinent to subsystems are adequately addressed
 - Review system level requirements to ensure they are properly implemented

System Safety 101

SSHA – What’s documented

- Front matter similar to other analyses
- Worksheets
 - Hazard Number: SS-
 - Component Failure Mode:
 - System Event Phase:
 - Detailed Hazard Description:
 - Related PHL/PHA Hazard Number:
 - Effect of Hazard:
 - Risk Assessment: (Hardware only)
 - Recommended Action:
 - Effect of Recommended Action:
 - Remarks:
 - Status:

System Hazard Analysis

System Safety 101

What is done/expected prior to CDR

- System Hazard Analysis (SHA) - Identified as Task 205 in MIL-STD-882
 - Verifies system compliance with safety requirements contained in system specifications and other applicable documents
 - Identifies previously unidentified hazards associated with the subsystem interfaces and system functional faults
 - Assesses the risk associated with the total system design
 - Software
 - Subsystem interfaces

System Safety 101

SHA – What do you do?

- Each the subsystems has been analyzed as part of the SSHA, now review the interfaces
 - Fuel tank/bumper/differential housing
- SHA takes a system-level review of the product
 - Ensure all top level hazards can track to the SHA
 - Realize that a “failure” is not necessarily a prerequisite for the mishap to occur
 - Power distribution system provides DC and electronics require AC
 - Altimeter uses meters, landing gear deployment in feet
 - Can be the “catch-all” analysis for system related issues
 - Bent Pin Analysis
 - Inadvertent Launch Analysis
 - Software Hazard Analysis
 - Include a single worksheet in the main SHA and reference the standalone analysis as an appendix

System Safety 101

SHA – What do you do?

- Considerations include
 - Review system level requirements to ensure they are properly implemented
 - Consider incorporating a Requirements Verification Matrix as an appendix to the SHA
 - Common mode failures – Do they have a ripple effect through the system
 - SSHA looks at failure modes within individual subsystems
 - Need to evaluate if multiple subsystems can be impacted by single failure mode and impact system-level safety/performance
 - Fault tree analysis is a helpful tool for determining common mode failures

System Safety 101

SHA – What do you do?

- Considerations include
 - Normal operation of one subsystem impacting the operation of another subsystem or the total system
 - Does heat/radiation/etc. of one subsystem degrade another
 - Interface definition/evaluation
 - Ensure SHA addresses not only hardware subsystem interfaces, but hardware/software interfaces and human-system interfaces as well
 - Evaluate/document system architecture from a safety critical functionality perspective
 - Evaluate/document the tasks required by the operator to ensure the overall safety of the system

System Safety 101

SHA – What's documented

- Front matter similar to other analyses
- Worksheets
 - Hazard Number: S-
 - Subsystem Failure Mode: (Remember, this field may be N/A)
 - System Event Phase:
 - Detailed Hazard Description:
 - Related PHL/PHA Hazard Number:
 - Effect of Hazard:
 - Risk Assessment: (Hardware only)
 - Recommended Action:
 - Effect of Recommended Action:
 - Remarks:
 - Status:

System Safety Engineering Report

System Safety 101

What is done/expected prior to CDR

- System Safety Engineering Report (SSER) - Identified as part of Task 303 in MIL-STD-882
 - SSER evaluates all hardware/software/firmware changes and defects for their potential safety impact
 - SSER determines the hazards associated with the proposed change to ensure the system modification maintains a safety risk level acceptable to the customer

System Safety 101

SSER – What do you do?

- Review the existing hazard analyses
- Ensure existing safety requirements (recommended actions) have not been changed
 - If they have, assess the impact of the change on the residual risk for the system
 - In the event the residual risk has changed, notify the appropriate authority and provide alternatives
- Typically, SSER are only performed after CDR when the system is placed under formal Configuration Management control
 - Certain programs may impose this earlier than CDR

Explosive Ordnance Disposal Data Package

System Safety 101

What is done/expected prior to CDR

- Explosive Ordnance Disposal (EOD) Data Package - Identified as Task 404 in MIL-STD-882
 - Assist EOD personnel in the identification of hazardous or energetic components and provide a basic understanding of the functioning of energetic systems
 - Data may consist of:
 - Source data
 - Test items
 - Training units
 - Recommended render safe procedures
 - Explosive ordnance disposal procedures, if available

System Safety 101

EOD Data –

- Source data
 - System description
 - Schematics of energetic circuitry
 - Drawings
 - Markings
 - Hazardous materials/MSDSs
 - Sensitivity test results
 - Test results to date
 - Net Explosive Weight
 - Battery characteristics
- Test items
 - Batteries

System Safety 101

EOD Data –

- Training units
 - Inert assets
- Recommended render safe procedures
 - If available, all data pertaining to rendering the system safe
 - Procedures developed for production facility
 - System design features, such as mechanical return-to-safe, G switch interlocks, etc.
 - Timing relative to battery bleed down, capacitor discharge
- EOD procedures, if available
 - Similar systems
 - System design details that may influence procedures, such as component locations around energetics

Explosive Hazard Classification Data Report (EHCDR)

System Safety 101

EHCDR

- Why do you need this?
 - Required to obtain classification for transportation and storage
 - Transporting over US roadways
 - Storage at DOD facilities
- Who needs to obtain this?
 - All new ammunition/explosives
 - Existing ammunitions/explosives that have been modified or had its packaging modified
 - If there's a new part number, plan on reclassifying
 - If the explosive component is within a cable cutting device and the cable cutter mechanical structure is modified, plan on obtaining a new hazard classification

System Safety 101

EHCDR

- What are the different classes?
 - Class 1 Explosives
 - 1.1 Mass explosion
 - 1.2 Non-mass explosion, fragment producing
 - 1.3 Mass fire, minor blast, or fragment
 - 1.4 Moderate fire, no blast, or fragment
 - 1.5 Explosive substance, very insensitive (with mass explosion hazard)
 - 1.6 Explosive article, extremely insensitive
 - Class 2 Gases
 - 2.1 Flammable gas
 - 2.2 Non-flammable, non-poisonous compressed gas
 - 2.3 Gas poisonous by inhalation
 - Class 3 Flammable liquids
 - Class 4
 - 4.1 Flammable solid
 - 4.2 Spontaneously combustible material
 - 4.3 Dangerous when wet material
 - Class 5
 - 5.1 Oxidizer
 - 5.2 Organic peroxide
 - Class 6
 - 6.1 Poisonous material
 - 6.2 Infectious substance
 - Class 7 Radioactive material
 - Class 8 Corrosive material
 - Class 9 Miscellaneous hazardous materials

System Safety 101

EHCDR

- What are the different types of classifications?
 - Interim Hazard Classification (IHC)
 - IHC are valid for a maximum of one calendar year
 - Issued during development phase
 - Used for transporting new items to test facilities
 - Quantities of test items sufficient to support tests are normally not available
 - IHC for overseas transport limited to military carriers
 - Final DoD Hazard Classification (FHC)
 - Issued after completion of testing
 - Remember, FHC is only valid for the configuration tested

System Safety 101

EHCDR

- What testing is required?
 - STANAG 4123 and DoD storage hazard classification tests
 - For new items, testing is per UN Test Series 1 through 4
 - Gap Test for Solids and Liquids
 - Internal Ignition Test
 - Slow Cookoff Bomb (SCB) Test
 - Bureau of Explosives Impact Machine Test
 - ABL Friction Test
 - Thermal Stability Test
 - Small-Scale Burning Test
 - For Class 1 (explosives, 1.1-1.4), testing is per UN Test Series 6
 - Single Package Test
 - Stack Test
 - External Fire (Bonfire) Test

Technical Data For Munitions

System Safety 101

What is done/expected prior to CDR

- Technical Data For Munitions (TDM)
 - Provide information necessary for the safe storage, maintenance, inspection and transportation of ammo and explosives at test ranges
 - TDM is applicable to all research and development munitions requiring storage by military personnel

System Safety 101

Finally, you're ready for CDR!

- As with the SFR/PDR previously discussed, the CDR typically has expectations in five key areas:
 - Planning
 - Requirements Analysis, Review and Verification
 - Design Guidance
 - Analysis
 - Budget
- Details of the Requirements Analysis, Review and Verification, Design Guidance and Analysis are provided
 - Planning addresses SSPP and Budget addressed adequate staffing

System Safety 101

Finally, you're ready for CDR!

- Requirements Analysis, Review and Verification
 - Ensure that compliance matrix addresses all system safety requirements such that all system safety requirements will be achieved through analysis, demonstration, simulation, test, or inspection
 - Red - Compliance matrix is not in place to address safety requirements or all safety requirements are identified as being verified via analysis
 - Yellow – Compliance matrix is in place to address safety requirements but not all requirements have been assigned a verification method
 - Green – Compliance matrix is in place and all requirements have been assigned a verification method
 - Blue – Compliance matrix is in place, all requirements have been assigned a verification method and the matrix has been reviewed and agreed to by the SSWG members

System Safety 101

Finally, you're ready for CDR!

- Design Guidance
 - Verify compliance to requirements contained in the System Safety design guide
 - Red – Requirements contained in the design guide were not achieved
 - Yellow – Safety design guide requirements were not fully achieved, but work-around plans or rationale for non-compliance is provided
 - Green – Requirements contained in the design guide were fully achieved
 - Blue – Safety design guide requirements were fully achieved and concurred by review authority
- Analysis
 - PHL and PHA Hazards have been transferred to next level of analysis (SHA, SSHA)
 - Red – PHL/PHA hazards have not been transferred to the SSHA/SHA
 - Yellow – PHL/PHA hazards have been partially transferred to the SSHA/SHA
 - Green – PHL/PHA hazards have been transferred to the SSHA/SHA
 - Blue – PHL/PHA hazards have been transferred to the SSHA/SHA and the SSWG membership concurs with the closure of all PHL/PHA hazard worksheets

System Safety 101

Finally, you're ready for CDR!

- Analysis
 - SRCA/Subsystem/System/HHA hazard analyses submitted. This includes any explosive/ordnance related analyses
 - Red – SRCA/SSHA/SHA/HHA have not been submitted
 - Yellow – SRCA/SSHA/SHA/HHA have not all been submitted
 - Green – SRCA/SSHA/SHA/HHA have been submitted
 - Blue – SRCA/SSHA/SHA/HHA have been submitted and the SSWG membership concurs with the closure of the SR/CA
 - Hazard controls (risk mitigations) have been implemented in the design
 - Red – Risk mitigations have not been implemented
 - Yellow – Risk mitigations have been partially implemented
 - Green – Risk mitigations have been fully implemented
 - Blue – Risk mitigations have been fully implemented and the majority of the SSHA/SHA worksheets have been reviewed and closed by the SSWG membership

System Safety 101

AGENDA

- Before You Start
- Pre-Preliminary Design Review
 - System Safety Program Plan
 - Software Safety Program Plan
 - Preliminary Hazard List/Preliminary Hazard Analysis
 - Threat Hazard Assessment
 - Hazard Assessment Test Plan
 - Safety Requirements/Criteria Analysis
 - Operating & Support Hazard Analysis
 - Health Hazard Assessment
 - Safety Assessment Report
 - Review Authority Evolutions
 - Design For Environment Tasks
 - Environmental Trade Study
 - Hazardous Material Management Program Plan
 - Demilitarization and Disposition Program Plan
 - Preliminary Demil Assessment
 - Design For Environment Analysis
 - Design For Demil Analysis
 - Hazardous Material Management Program Report
- Pre-Critical Design Review
 - Subsystem Hazard Analysis
 - System Hazard Analysis
 - System Safety Engineering Report
 - Explosive Ordnance Disposal Data Package
 - Explosive Hazard Classification Data Report
 - Technical Data for Munitions
- Pre-First Flight Test
 - Range Safety Data Package
 - DM&DP Plan and Report
- Other Analyses
 - Fault Tree Analysis
 - Bent Pin Analysis
 - Inadvertent Launch Analysis
- Other Topics
 - Test Set Safety Process
 - Configuration Management
 - Engineering Change Proposals, Deviations, Waivers
 - Hazard Tracking
 - Hazard Action Report

What is done/expected prior to first flight test

Range Safety Data Package

System Safety 101

What is done/expected prior to first flight test - Range Safety Data Package (RSDP)

- RSDP is similar to the SAR previously discussed in that it provides a comprehensive evaluation of the system design prior to test operations
- Plan on delivery approximately 120 days prior to test operations
- Ensure the RSDP description and date is applicable for the system configuration being tested
 - May be difficult to meet 120 day threshold with dynamic systems

System Safety 101

Range Safety Data Package (RSDP)

- RSDP format and content will be dependent upon the specific range
- Regardless of test range, RSDP should provide detailed data relative to:
 - Safety features implemented in the design
 - Command Destruct (CD)/ Self Destruct (SD)/ Flight Termination System (FTS)
 - EMI/EMC/E³

Demilitarization & Disposition Plan and Report

System Safety 101

What is done/expected prior to first flight test – DM&DP Plan and Report

- The DM&DP is the reporting vehicle for providing status of the DM&DP program
- Helps identify and document:
 - products of combustion
 - specific impacts of DM&D processes
 - analysis of residual materials
 - characteristics of materials
 - Drawings
 - disassembly level
 - plans for end items

System Safety 101

AGENDA

- Before You Start
- Pre-Preliminary Design Review
 - System Safety Program Plan
 - Software Safety Program Plan
 - Preliminary Hazard List/Preliminary Hazard Analysis
 - Threat Hazard Assessment
 - Hazard Assessment Test Plan
 - Safety Requirements/Criteria Analysis
 - Operating & Support Hazard Analysis
 - Health Hazard Assessment
 - Safety Assessment Report
 - Review Authority Evolutions
 - Design For Environment Tasks
 - Environmental Trade Study
 - Hazardous Material Management Program Plan
 - Demilitarization and Disposition Program Plan
 - Preliminary Demil Assessment
 - Design For Environment Analysis
 - Design For Demil Analysis
 - Hazardous Material Management Program Report
- Pre-Critical Design Review
 - Subsystem Hazard Analysis
 - System Hazard Analysis
 - System Safety Engineering Report
 - Explosive Ordnance Disposal Data Package
 - Explosive Hazard Classification Data Report
 - Technical Data for Munitions
- Pre-First Flight Test
 - Range Safety Data Package
 - DM&DP Plan and Report
- Other Analyses
 - Fault Tree Analysis
 - Bent Pin Analysis
 - Inadvertent Launch Analysis
- Other Topics
 - Test Set Safety Process
 - Configuration Management
 - Engineering Change Proposals, Deviations, Waivers
 - Hazard Tracking
 - Hazard Action Report

Other Analyses

- Fault Tree Analysis
 - Bent Pin Analysis
- Inadvertent Launch Analysis

Fault Tree Analysis

System Safety 101

Fault Tree Analysis (FTA)

- FTA is a graphical analysis technique that identifies the possible combinations of events required in order for the undesired event to occur
- Why would you want to do an FTA?
 - Undesired event (AKA Top Event) may be a major concern/high impact scenario requiring detailed assessment
 - “Inadvertent Warhead Detonation”
 - System may be extremely complex with multiple potential contributors
 - “Space Shuttle Fails to Lift Off”
 - A quantitative assessment may be required
 - “Inadvertent Launch of a CaseyKyle Missile”
 - Root cause determination
 - “Restrained Firing of a CaseyKyle Missile on the USS GW Bush”

System Safety 101

Fault Tree Analysis (FTA)

- Topics on FTA
 - Top Event
 - Main Gate Types
 - Main Event Types
 - Cutsets
 - FTA Iteration
 - Other Gate and Event Types
 - Some Do's and Don't's

System Safety 101

Fault Tree Analysis (FTA)

- Top Event
 - Each fault tree begins with a single top event
 - Don't use FTA to assess multiple scenarios
 - Top events may be contractually identified or as a result of hazard analyses
 - Be careful of statements such as “All identified catastrophic and critical hazards/mishaps will have fault tree analyses performed”
 - Review previous programs
 - Bound the scope of the FTA
 - Good: “Inadvertent Warhead Detonation During Storage”
 - Not so good: “Warhead Kills People and Damages Stuff”

System Safety 101

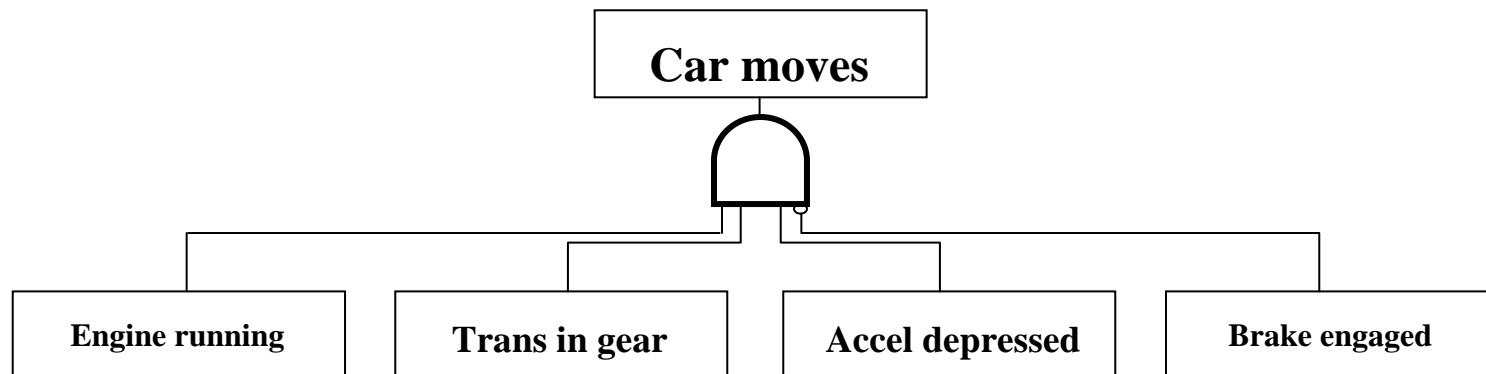
Fault Tree Analysis (FTA)

- What does that mean?
 - Graphical analysis technique: The FTA is comprised of gates, events and transfers that describe all potential failure modes, inputs and contributors to the top event
 - Inputs do not necessarily need to be failures
 - Dependent upon the FTA criteria, events may be further developed
 - Major gates/events are described

System Safety 101

FTA Gates

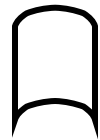
- There are traditionally two main gates used in the preparing a fault tree, AND gate and OR gate
 - Other gates will be addressed later
- AND gate: Output is satisfied if all inputs to the gate are satisfied
 - Example: For a car to move, it requires the engine be running, transmission in gear, accelerator depressed, and brake system not engaged (Example only)



System Safety 101

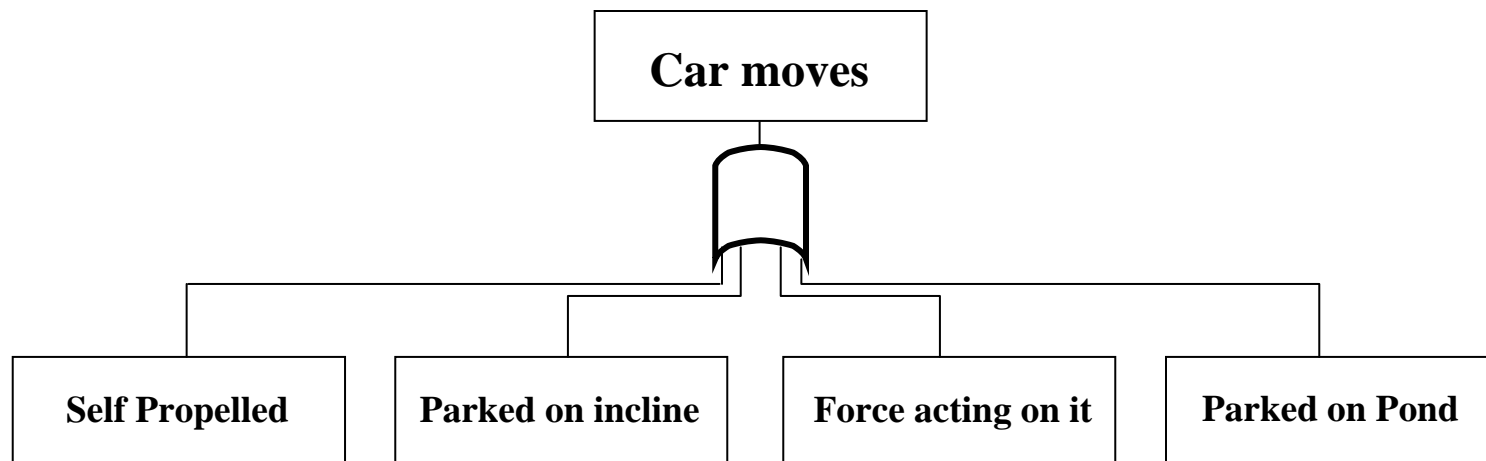
FTA Gates

- The second main gate used is the OR gate



– OR gate: Output is satisfied if any inputs to the gate is satisfied

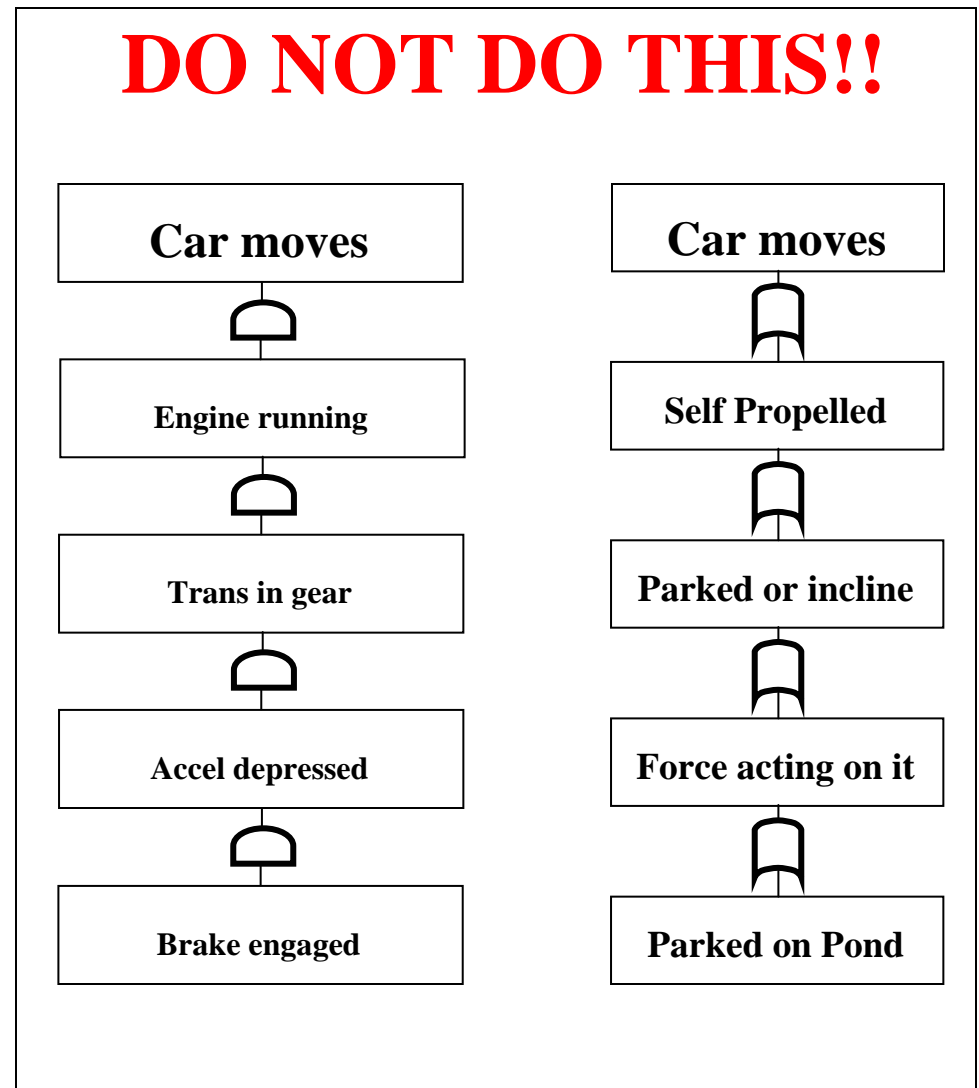
- Example: For a car to move, it may be self-propelled, parked on an incline, have a force acting on it or parked on a frozen pond



System Safety 101

FTA Gates

- Some rules for gates:
 - Require multiple inputs
 - Most FTA programs won't allow this type of tree to be built



System Safety 101

FTA Events

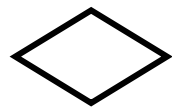
- There are three main event types normally used beyond the Top Event; Basic Event, Undeveloped Event and Normal Event

- – Basic Event: An initiating fault, failure or occurrence that isn't developed any further
 - Typically the end of the line as far as the level of detail for the analysis
 - Make sure the terminology is identical if this event occurs in multiple locations
 - Relay A32 Fails Closed vs. Relay (A32) Fails Closed
 - This event may be further developed in future iterations of the analysis
 - Dependent upon cutsets and common mode failures

System Safety 101

FTA Events

- Main event types



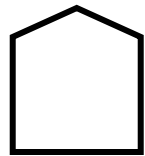
– Undeveloped Event: An event that isn't developed any further

- Similar to a basic event, but may not be further developed in future iterations of the analysis
- This may be an event external to what is being evaluated
 - Rocket motor ignition requires a signal from a combat control system
- Used for operator actions

System Safety 101

FTA Events

- Main event types



- Normal (House) Event: An event that is normally expected to occur
- House events impact different gates differently
 - OR gates are satisfied as are all OR gates above it until an AND gate is reached
 - AND gates should have all house events deleted when determining acceptability of risk
 - Depending upon software tool, house events may or may not appear in cutsets
- As you go through different system states, certain events become house events

System Safety 101

FTA Cutsets

- Cutsets are the minimal of events that must occur in order for the top event to be satisfied
- Cutsets can be used for getting either qualitative results (a minimum of 3 simultaneous independent failures must occur) or quantitative probabilities (probability the the top event occurring is 1×10^{-59})
- Review cutsets to make sure they're reasonable
- Review cutsets to determine if the tree needs to be developed further (this is addressed in the iteration discussion)

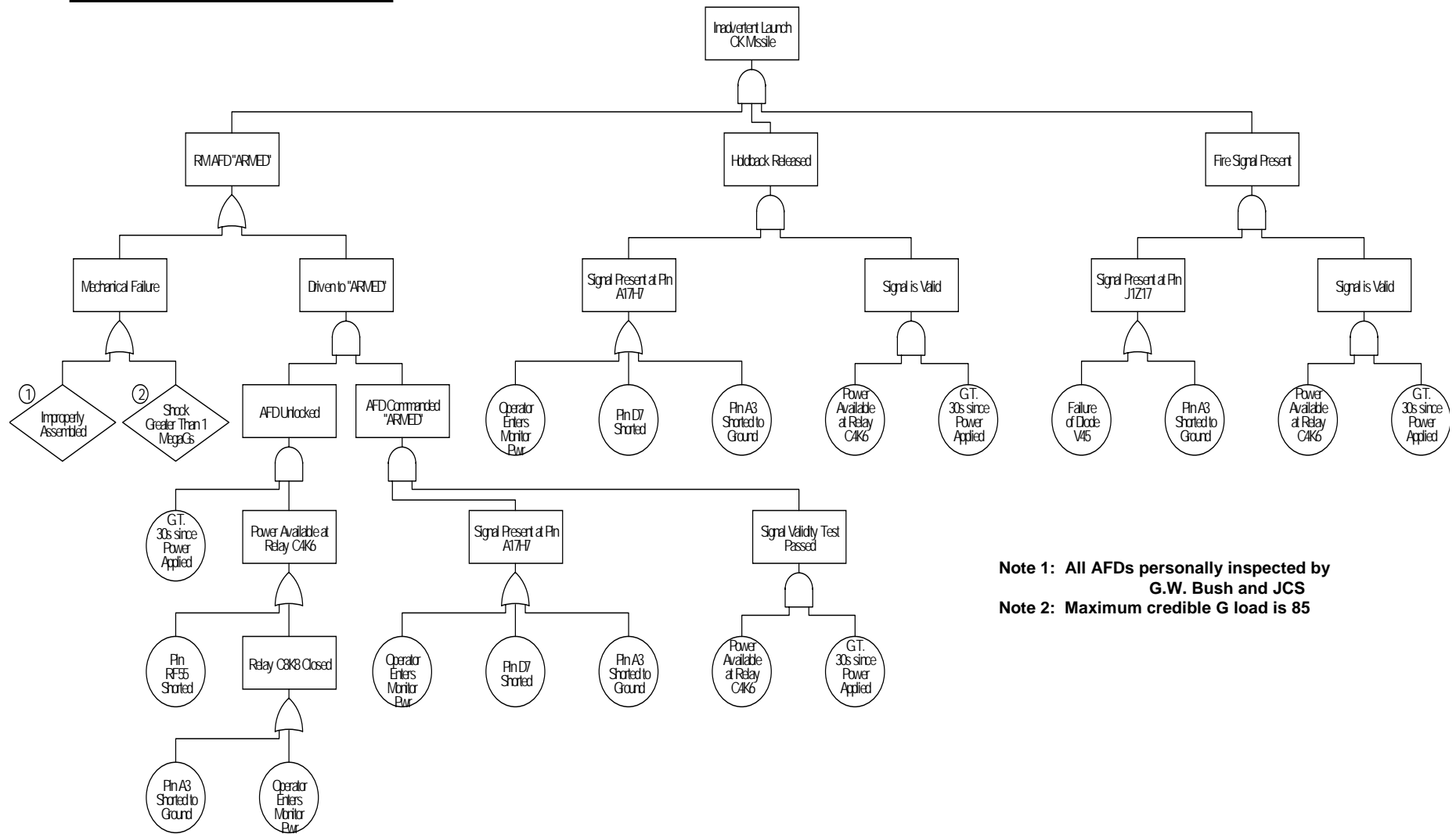
System Safety 101

FTA Iteration

- Once cutsets are generated, review them to determine if the tree needs to be developed further
 - Look at the events in minimum cutsets
 - Determine if “similar” events are present
 - Further develop those events for common mode failures
- Depending upon system state, many trees will need to be further developed as the system withdraws from the top event state or pruned as the system approaches the top event state
 - As the system approaches the top event state, many basic or undeveloped events become house events
 - Need to re-determine the cutsets based upon the system state

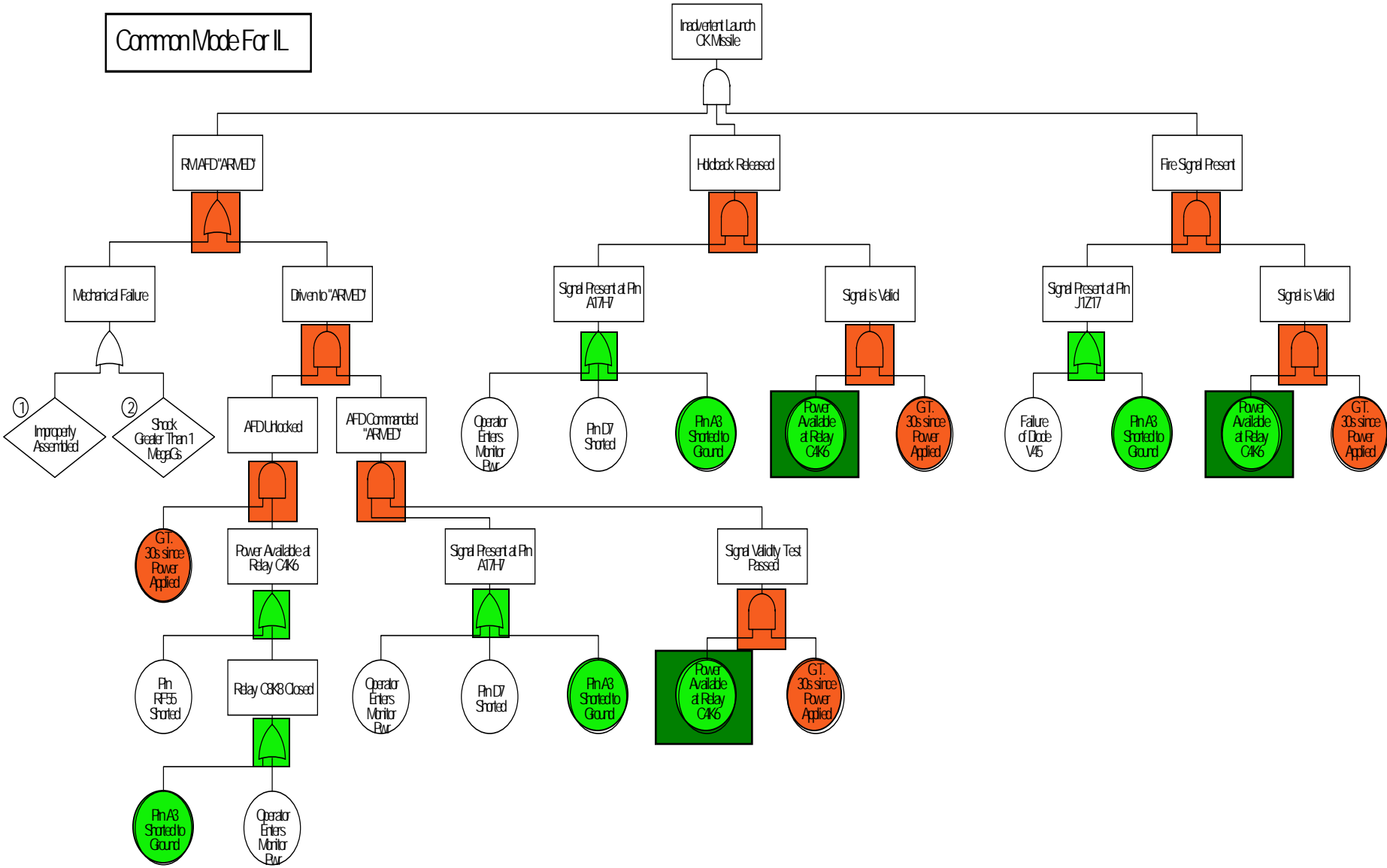
System Safety 101

Inadvertent Launch of Casey Kyle Missile

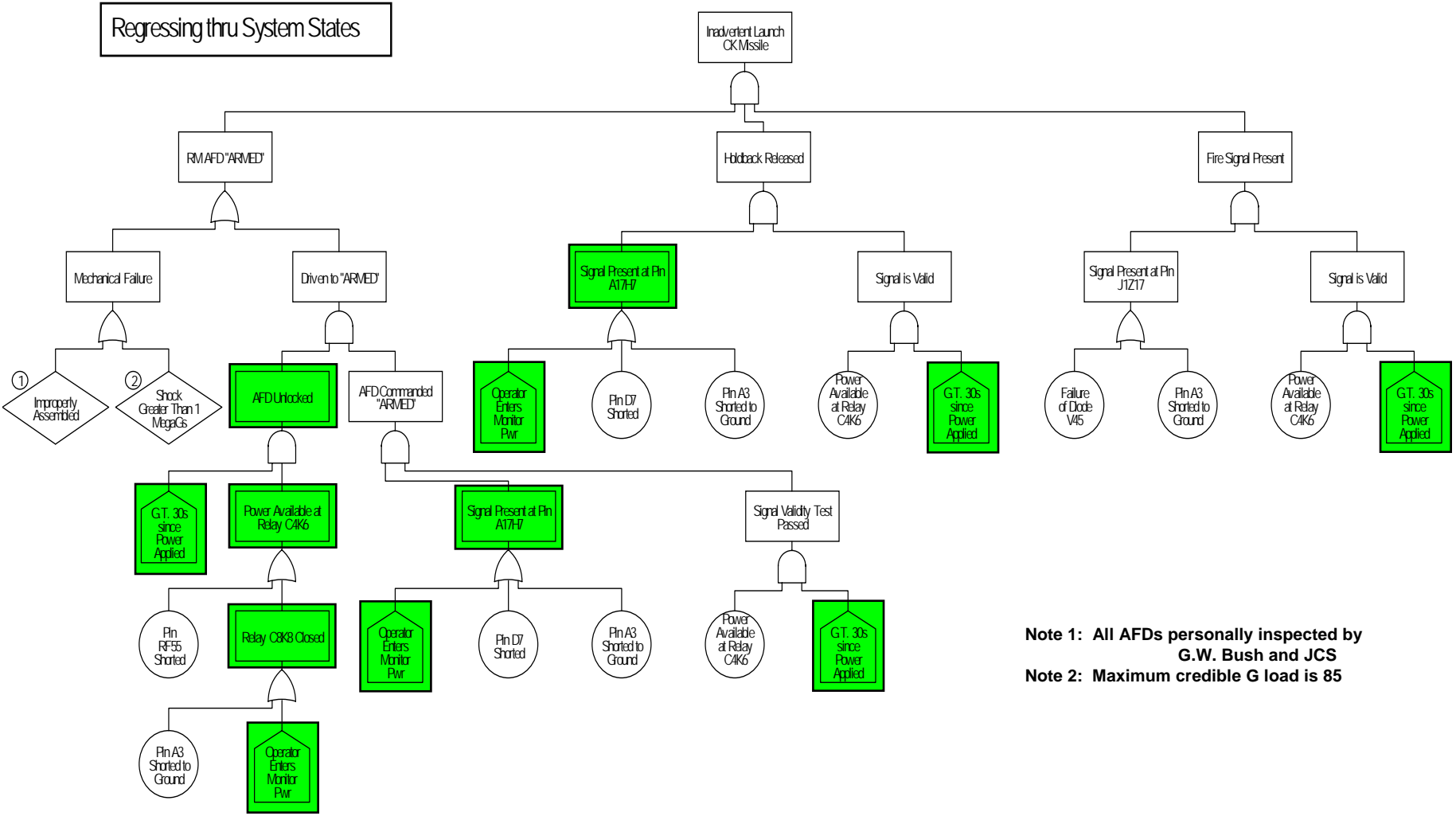


Note 1: All AFDs personally inspected by G.W. Bush and JCS
Note 2: Maximum credible G load is 85

System Safety 101



System Safety 101

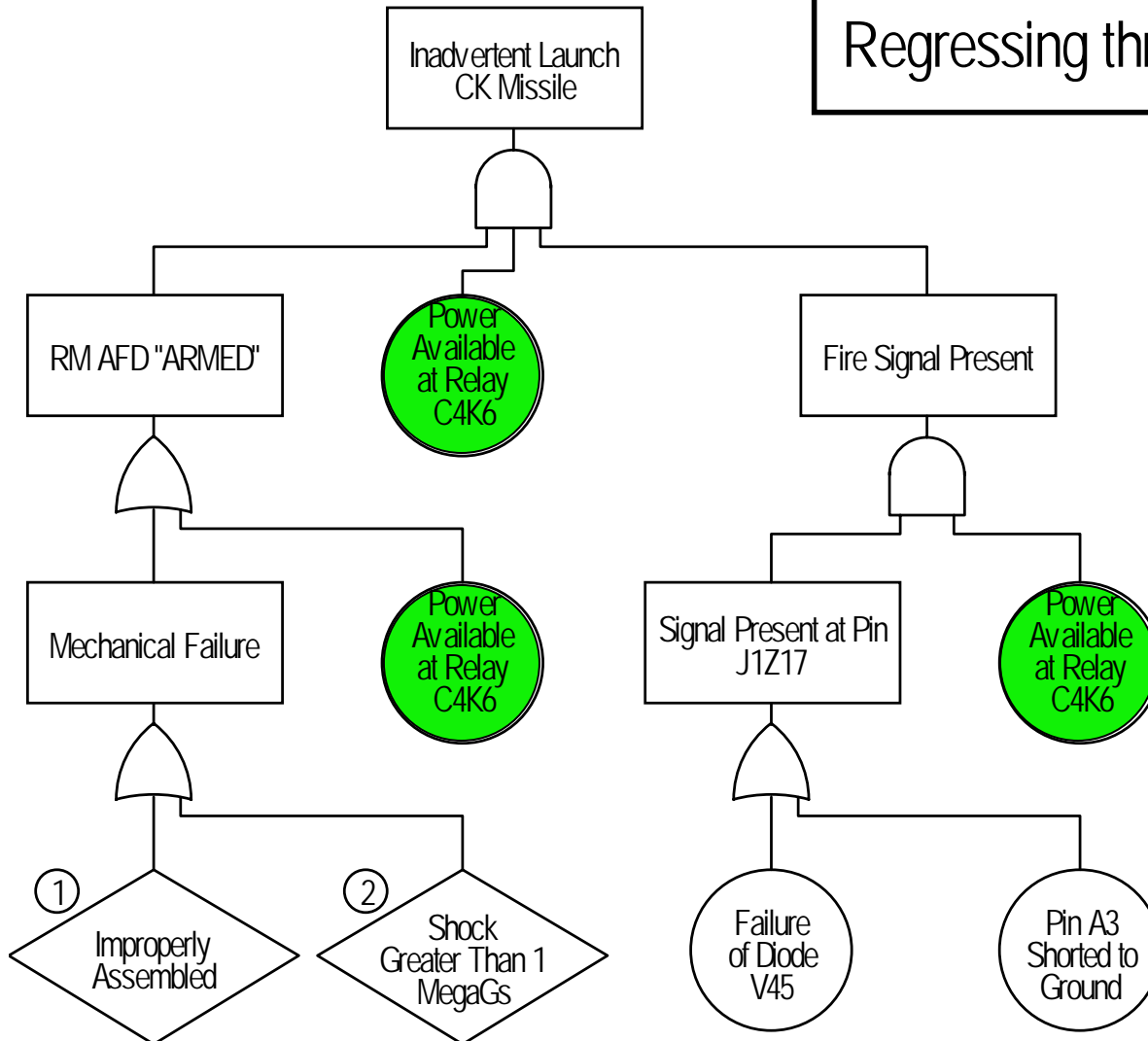


Note 1: All AFDs personally inspected by G.W. Bush and JCS
Note 2: Maximum credible G load is 85

Assume monitor power has been applied and operator is awaiting further orders

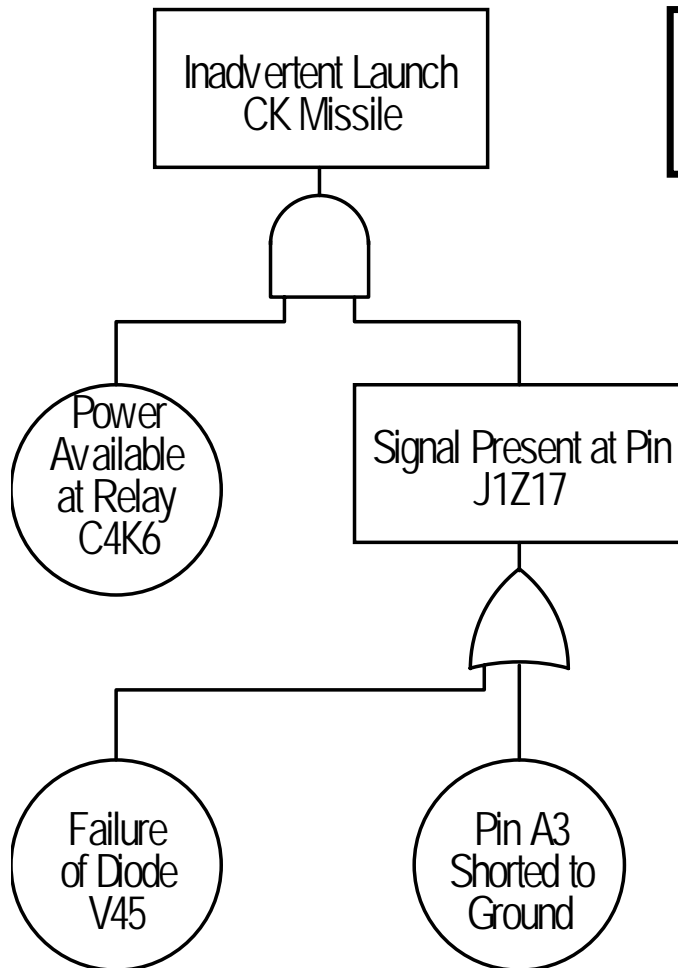
System Safety 101

Regressing thru System States



System Safety 101

Regressing thru System States



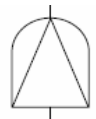
System Safety 101

FTA – Other Gate and Event Types

- Most trees can be built with the two gates and three/four events described, but others do exist



– Transfer: Used when the fault tree is too large for a single screen or the leg of the tree also occurs elsewhere



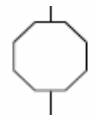
– Priority AND Gate: Output is satisfied if inputs to the gate are satisfied in a pre-determined order



– Exclusive OR Gate: Output is satisfied if one, but only one input to the gate is satisfied



– Mutually Exclusive OR Gate: Output is satisfied if any one input to the gate is satisfied, therefore, all other inputs are prevented



– Inhibit Gate: Output is satisfied if input to the gate occurs while a conditioning event is present

System Safety 101

FTA – Some Do's and Don'ts

- DO
 - Review the tree when you're done to see if it truly represents how the system operates
 - Normal system operation should flow out of the tree
 - Keep careful track of the naming convention
 - Review cutsets for potential common mode issues
 - Triggers include physical location, same power source, device technology, etc
 - Evaluate house events on their impact to the top event
- DON'T
 - Worry about how the tree looks
 - Give a top event to 10 people and you'll get 10 different looking trees (or someone cheated)
 - Cutsets should be the same
 - Have single inputs into gates
 - Include house events into the minimal cutsets

Bent Pin Analysis

System Safety 101

Bent Pin Analysis (BPA)

- Why do a BPA?
 - The BPA will help determine the susceptibility of the system to bent pins within a connector from inadvertently generating commands
 - Assists in the connector layouts
 - Intent of the BPA is not to evaluate multiple connectors simultaneously
- What connectors should you do a BPA on?
 - **STRONG RECOMMENDATION: LIMIT THE BPA TO CONNECTORS THAT ARE NOT POST-MATE TESTED**
 - This methodology was developed in support of the SSN688 Class Submarine Combat System
 - This may assist in deriving testing requirements

System Safety 101

Bent Pin Analysis (BPA)

- How do you do a BPA?
 - Four items are required to perform a BPA:
 - Physical connector configuration
 - Length and diameter of all pins
 - Bending radius of each pin
 - Functional and signal characteristics of each pin
 - Tools may be available to determine bent pin possibilities
 - Otherwise, scaled drawings and a compass will work

System Safety 101

Bent Pin Analysis (BPA)

- How do you do a BPA?
 - Typically, focus on the safety critical functions within the connector, such as Rocket Motor ARM or Rocket Motor IGNITION
 - Don't be concerned with the critical function pin being bent, rather, determine if any adjacent pins can physically come into contact with the safety critical function pin
 - Determine each bent pin that can potentially come into contact with a safety critical function pin
 - Determine the effect of each bent pin, considering
 - Signal characteristics
 - Timing

System Safety 101

Bent Pin Analysis (BPA)

- How do you do a BPA?
 - Document the connector, physical configuration and each safety critical function pin in the connector
 - For each safety critical function pin
 - Identify each pin that could potentially come in contact
 - State the system effect should a bent pin occur
 - In the event the system effect is undesirable or unacceptable, determine alternative pin assignments
 - The BPA can be added as an appendix to the SHA with the bent pin scenario addressed as a single SHA worksheet

Inadvertent Launch Analysis

System Safety 101

Inadvertent Launch Analysis (ILA)

- Who does an ILA?
 - This is a weapon system specific analysis
 - Typically, the ILA is an integrated analysis involved both the weapon control system as well as the weapon itself
- Why do an ILA?
 - Determine the susceptibility of the system to an inadvertent launch of a weapon system
 - Review from both a probability and perception standpoint
- How do you do an ILA?
 - Use FTA methodology
 - Key item to keep in mind is system state and FTA iteration

System Safety 101

Inadvertent Launch Analysis (ILA)

- System State and the ILA
 - This is a key aspect of the ILA
 - Evaluating the susceptibility of the system while in a dormant stage doesn't really prove much
 - Almost all systems will contain a single point failure (last operator action) dependent upon system state
 - Susceptibility of the system may be determined by evaluating from the worst case scenario and working backwards through system states
 - Convenient method is to base the system state upon operator actions

System Safety 101

Inadvertent Launch Analysis (ILA)

- System State and the ILA
 - Determine the operating procedures for the system under review
 - Develop FTA based upon last required action
 - The fault tree will be relatively simple at this time
 - Majority of the system design interlocks will be house events
 - Determine the susceptibility for this system state
 - If FTA shows “adequate” level of protection at this state, declare victory
 - If FTA does not show an adequate level of protection, step back to the previous operator action
 - » Several events previously classified as house events will now need to be further developed
 - Continue the process until the FTA demonstrates an adequate level of protection
 - » May identify the need to incorporate additional interlocks (e.g., additional operator actions)

System Safety 101

AGENDA

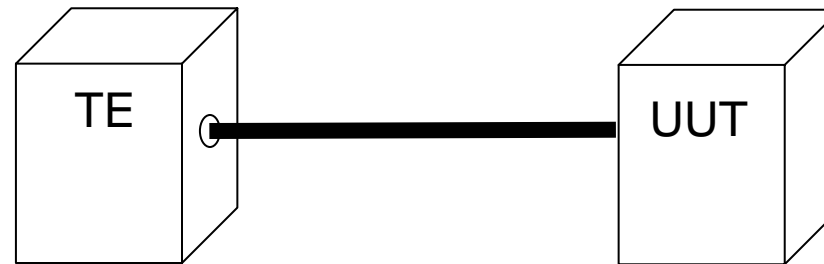
- Before You Start
- Pre-Preliminary Design Review
 - System Safety Program Plan
 - Software Safety Program Plan
 - Preliminary Hazard List/Preliminary Hazard Analysis
 - Threat Hazard Assessment
 - Hazard Assessment Test Plan
 - Safety Requirements/Criteria Analysis
 - Operating & Support Hazard Analysis
 - Health Hazard Assessment
 - Safety Assessment Report
 - Review Authority Evolutions
 - Design For Environment Tasks
 - Environmental Trade Study
 - Hazardous Material Management Program Plan
 - Demilitarization and Disposition Program Plan
 - Preliminary Demil Assessment
 - Design For Environment Analysis
 - Design For Demil Analysis
 - Hazardous Material Management Program Report
- Pre-Critical Design Review
 - Subsystem Hazard Analysis
 - System Hazard Analysis
 - System Safety Engineering Report
 - Explosive Ordnance Disposal Data Package
 - Explosive Hazard Classification Data Report
 - Technical Data for Munitions
- Pre-First Flight Test
 - Range Safety Data Package
 - DM&DP Plan and Report
- Other Analyses
 - Fault Tree Analysis
 - Bent Pin Analysis
 - Inadvertent Launch Analysis
- Other Topics
 - Test Set Safety Process
 - Configuration Management
 - Engineering Change Proposals, Deviations, Waivers
 - Hazard Tracking
 - Hazard Action Report

Other Topics

- Test Set Safety Process
- Configuration Management
- Engineering Change Proposals, Deviations/Waivers
 - Hazard Tracking
- Hazard Assessment Report

System Safety 101

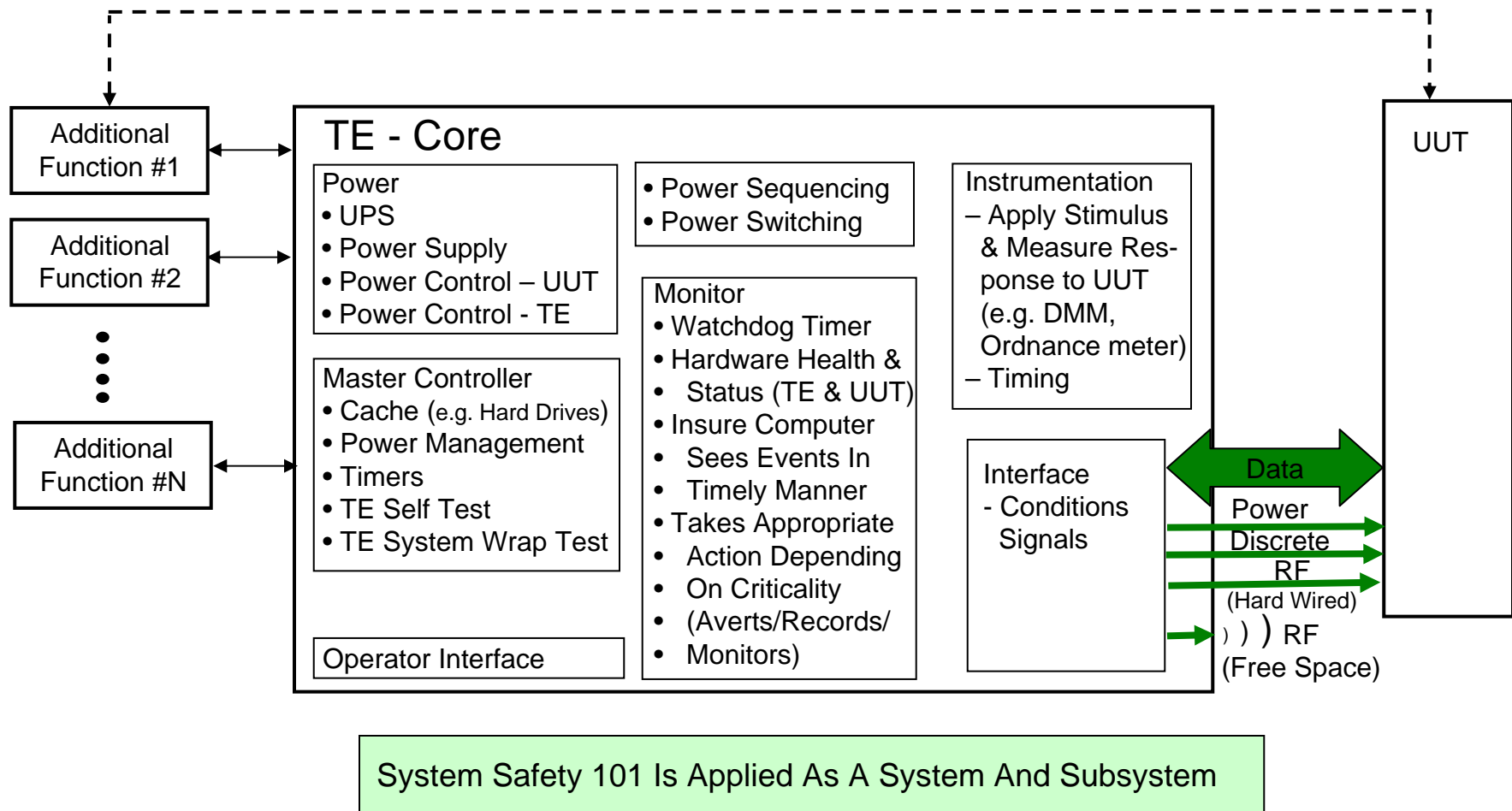
Test Set Safety Process - Applicability of System Safety 101 to TE Systems



- Apply System Safety 101 to Unit
 - Typically Complete Before TE System Analysis Is Started
- 1. Define Environment (e.g. cell, proximity) to determine if previous Unit analysis is outside its intended environment
- 2. Apply System Safety 101 to “Stand-Alone” TE
- 3. Analyze TE With UUT

System Safety 101

Test Set Safety Process - Test Equipment System (Generic) Definition



System Safety 101

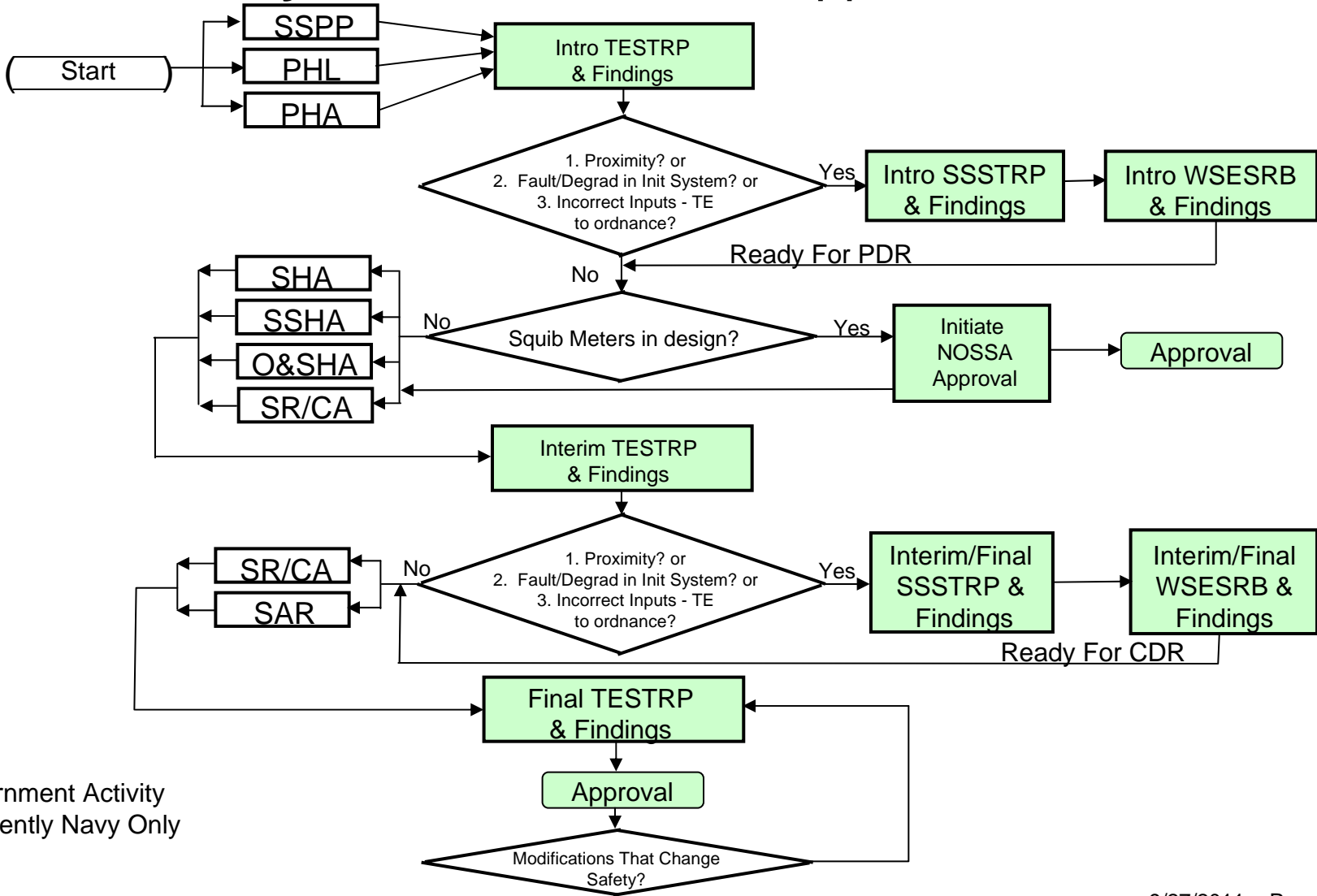
Test Set Safety Process - Comparison of Safety Analysis Approach for Test Equipment Systems to Units

Test Equipment System	Unit
System Definition - TE alone and TE interaction with UUT	- Unit only
Environment - Unit May Be Used In A Different Environment (e.g. Proximity, Cell)	- Used In Intended Environment (e.g. subsystem)
Software - Purpose Centers Around Checking Hardware - Not Tacitcal (STTO, Self-test) - Primarily Continuity Checks - Evaluating Pcodes; Fewer Safety Critical Operations	- Purpose Is Checking Unit functions - Tactical and Built In Test - Checking to See if Timeline happens - Typically More Safety Critical Software
Governing Standards - Test Set Unique Stds (OP5, OP3347)	- Safety Analysis Does Not Take Into Account Test Set Stds
Life Cycle - Test Sequences Analyzed (e.g. STTO - C&R, Power Verify)	- Phases Analyzed (e.g. Disposal)

Approach Is The Same As System Safety 101 But Some Different Considerations Need To Be Addressed

System Safety 101

Test Set Safety Process - Test Set Approval Process



System Safety 101

Configuration Management (CM)

- What does CM do?
 - CM provides an orderly establishment and documentation of functional, performance, and physical attributes of a system as defined by the system specification
 - Manages changes to those attributes,
 - Collects and retrieves of key information essential to the development of the system, and
 - Verifies the product against the required attributes
- What does that mean?
 - CM is responsible for knowing and maintaining the system baseline taking into account Engineering Change Proposals (ECPs), Block/Mod upgrades, Deviations/waivers, software builds
 - CM is responsible for maintaining the total system baseline, including hardware, software and firmware

System Safety 101

Configuration Management (CM)

- Why does system safety care about CM?
 - CM maintains the system baseline
 - Safety should be aware of current baseline by participate as a member of the Configuration Control Board (CCB)
 - Safety analyses and assessments should be made against the current baseline
 - CM is responsible for uniquely flagging safety critical requirements
 - CM process should preclude modifications without safety review and concurrence

Bottom Line – You need to know what it is you're looking at

System Safety 101

Engineering Change Proposals (ECPs), Deviations and Waivers

- What is an ECP?
 - Proposed engineering change and the documentation in which the change is described, justified, and submitted to the customer
- Each ECP will typically be assigned a classification
 - Class I ECP: Directly impacts the form/fit/function or *safety* of the existing system
 - Class II ECP: Does not change the form/fit/function or *safety*
 - Class I ECP normally requires additional documentation be submitted and thereby drives cost
- Who determines the classification of the ECP?
 - That's a key issue: The correct answer is "System safety should determine whether the safety of the system is impacted"

System Safety 101

ECPs, Deviations and Waivers

- How do you determine the safety impacts?
 - Process is essentially the same for ECPs as for deviations and waivers
 - Review existing analyses for the proposed area of change
 - Are requirements being changed?
 - Is the implementation of safety requirements being changed?
 - Is the architecture being modified?
 - Is the operating environment being altered?
 - Are materials being change?
 - Based upon this data, review the SSHA, SHA, HHA, FTA, BPA
 - ECPs don't necessarily have a negative impact on safety
- Document results in System Safety Engineering Report (SSER)

System Safety 101

Hazard Tracking

- What is a Hazard Tracking System (HTS)?
 - HTS is a method or procedure to document and track hazards and their controls thus providing an audit trail of hazard resolutions
 - Make sure identified hazards don't fall through the cracks
 - HTS is identified as a “Hazard Log” and can be either manual or automated
- When do you start developing the HTS?
 - Development of an HTS begins during the pre-PDR phase and continues throughout
 - Hazards are initially identified during the preparation of the PHL/PHA

System Safety 101

Hazard Tracking

- What goes into the HTS?
 - Description of each hazard including the associated risk (hardware) or criticality (software/firmware) index
 - Status of each hazard and control
 - Traceability of resolution for each hazard from the time it was identified to the time the associated risk was reduced to a level acceptable or the software/firmware testing and analysis is complete
 - Identification of residual risk, if applicable
 - Action person(s) and organizational element
 - The recommended controls to reduce the risk to an acceptable level (hardware) or the planned testing and analysis (software/firmware)
 - The signature of the Managing Activity (MA) accepting the risk or verifying completion of analysis/test and thus effecting closure of the Hazard Log item.

System Safety 101

Hazard Action Reports

- What is a Hazard Action Report (HAR)?
 - A HAR (AKA: SAM, SHAR, CAR, SAR, etc.) has traditionally been used to either:
 - Document a newly identified hazard that is not in existing hazard analyses
 - Identify where special emphasis needs to be given
 - Used to identify the main areas of concern within a program
 - HARs have a signature block for MA concurrence
 - Example of a HAR form provided
- What is a HAR **NOT** to be used as?
 - Don't use the HAR to document all identified hazards
 - Even if your program has zero deliverables per Acquisition Reform, use HAR for TLHs with identified hazards as causal factor reports
- Who can generate a HAR?
 - Anyone with knowledge of a potential hazard

System Safety 101

HAZARD NO.	SUBMITTAL DATE
CASEYKYLE WEAPON SYSTEM HAZARD ACTION REPORT	
HAZARD RISK ASSESSMENT:	PRIORITY:
HAZARD DESCRIPTION:	
RECOMMENDED SOLUTION:	
DISPOSITION:	
STATUS:	

System Safety 101

SUMMARY, Finally

- System safety is not magic
 - It's not necessarily easy as there's more to it than generating an analysis 2 weeks prior to CDR
 - Requires planning and an understanding of the processes and the system
- Make sure the safety program is properly planned
 - Majority of the efforts start prior to PDR
 - Playing catch-up can negatively impact your program and cost more
- System safety has processes and procedures in place
 - Examples exist for most analyses/plans/reports
 - If you need assistance, help is available !