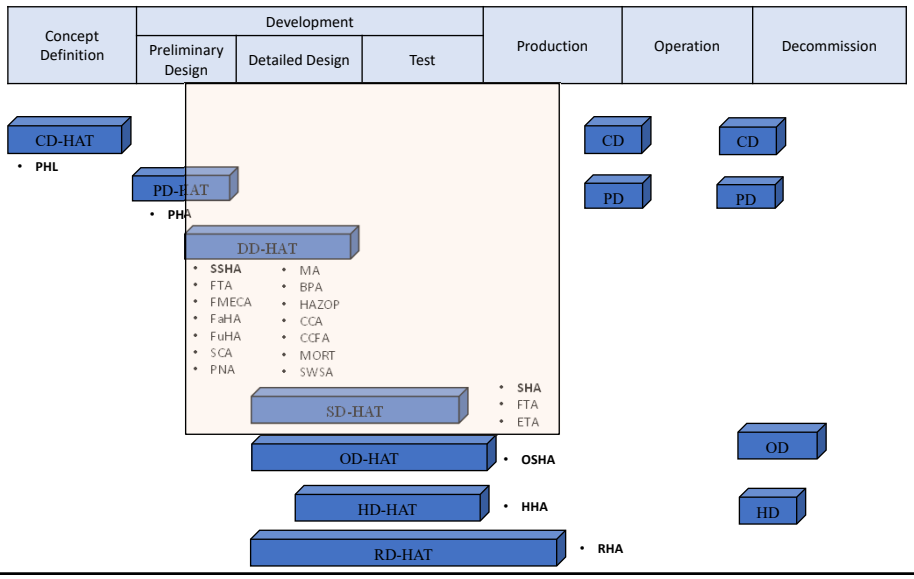
SubSystem Hazard Analysis (SSHA)
Ch 9
System Hazard Analysis (SHA)
Ch 10

1

## System Life Cycle Phase




2

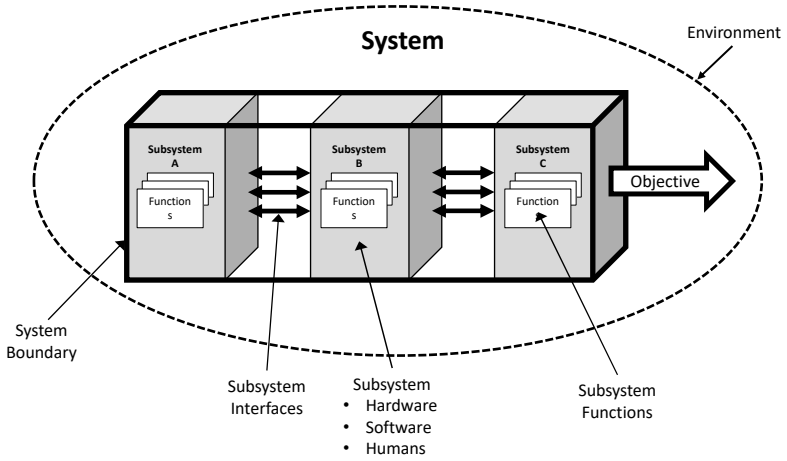
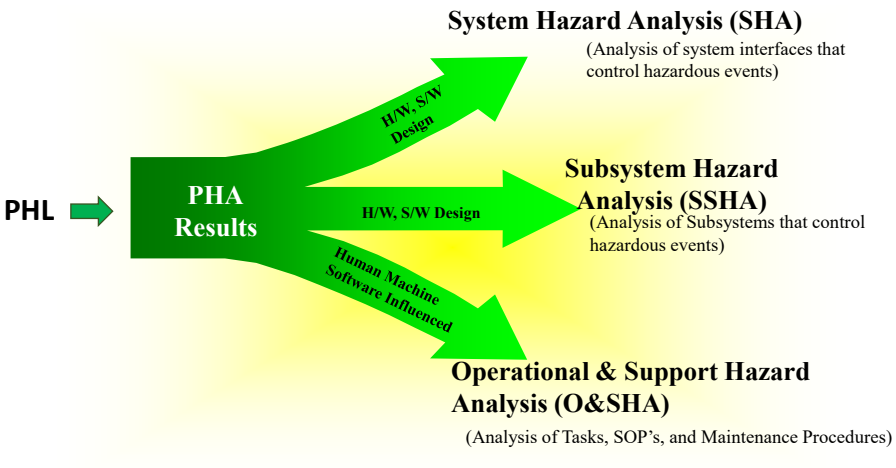



Figure 2.2 System Model -Ericson, C.A., "Hazard Analysis Techniques for System Safety," Wiley, 2005

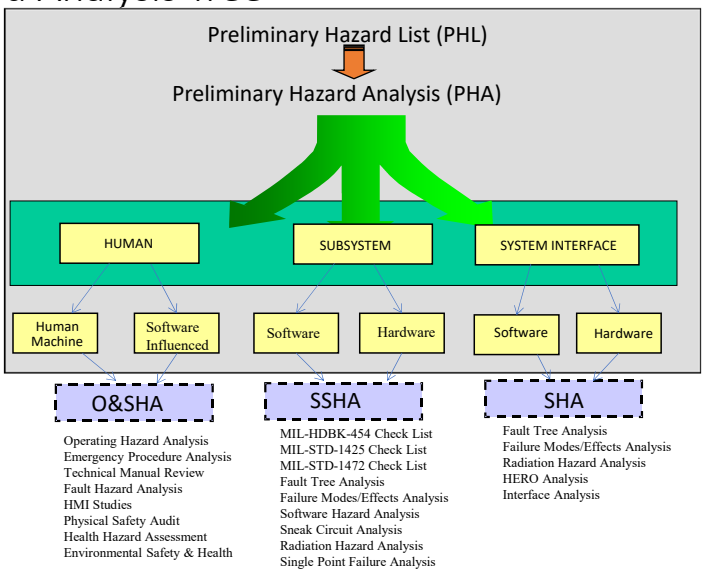
3

## Post PHA-- Analysis Type Determination




4

## Hazard Analysis Tree

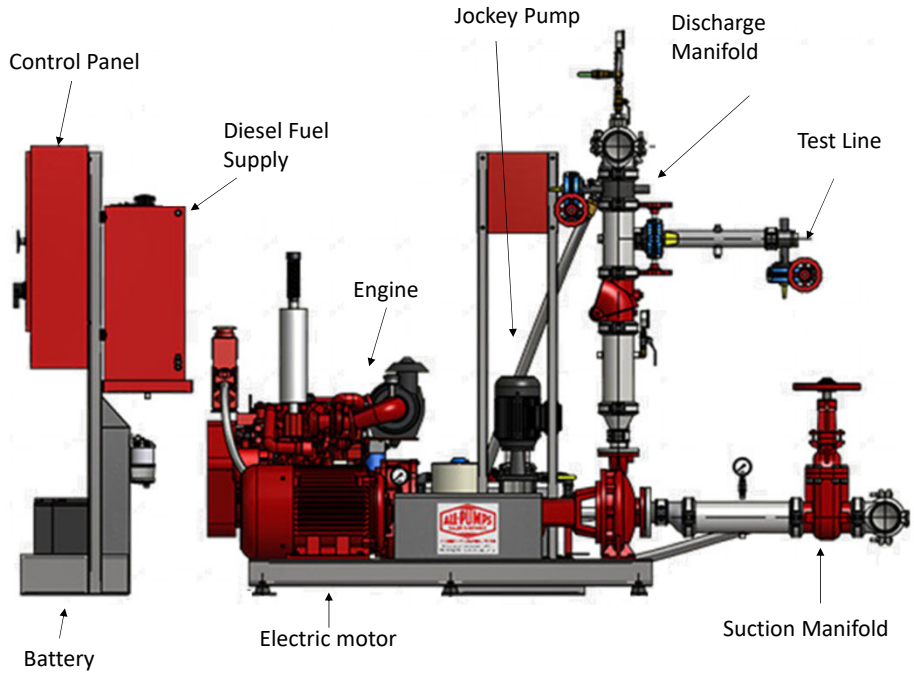



5

## Indentured Equipment

- System components in a hierarchy that defines **dominant and subordinate** relationships between subsystems down to the lowest piece/part level
- The indenture or hierarchy levels progress downward from the more complex high-level system elements to the simpler part/component elements.

6



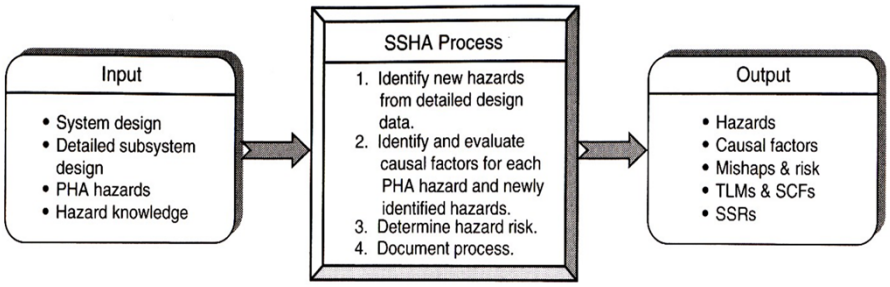

7

## Indentured Equipment List

| No. | Indentured Equipment List | |
|---|---|---|
| 1.0 | Dominant Component (Sub-assembly) | |
| | | 1.1 Subordinate Component |
| | | 1.2 Subordinate Component |
| | | 1.2 Subordinate Component |
| 2.0 | Dominant Component (Subassembly) | |
| | | 2.1 Subordinate Component |
| | | 2.2 Subordinate Component |
| | | 2.3 Subordinate Component |
| 3.0 | Dominant Component (Subassembly) | |
| | | 3.1 Subordinate Component |
| | | 3.2 Subordinate Component |
| | | 3.3 Subordinate Component |

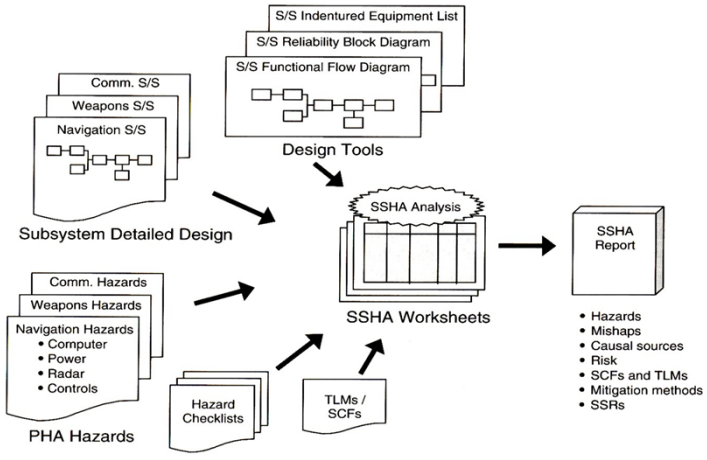
8

## SSHA Overview

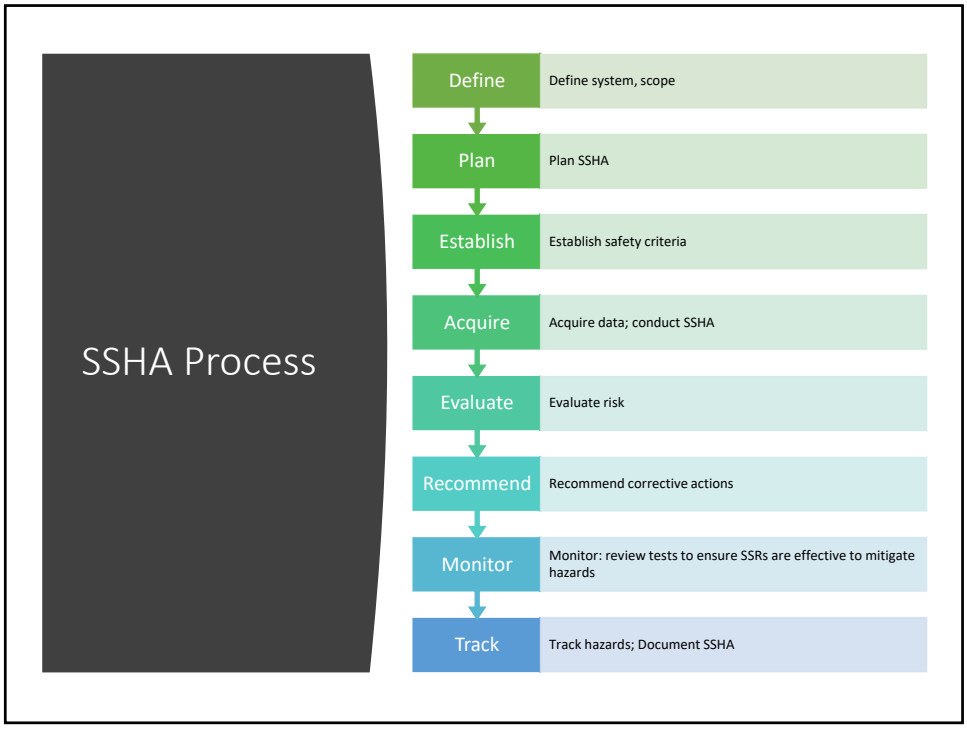



9

## SSHA Methodology




10

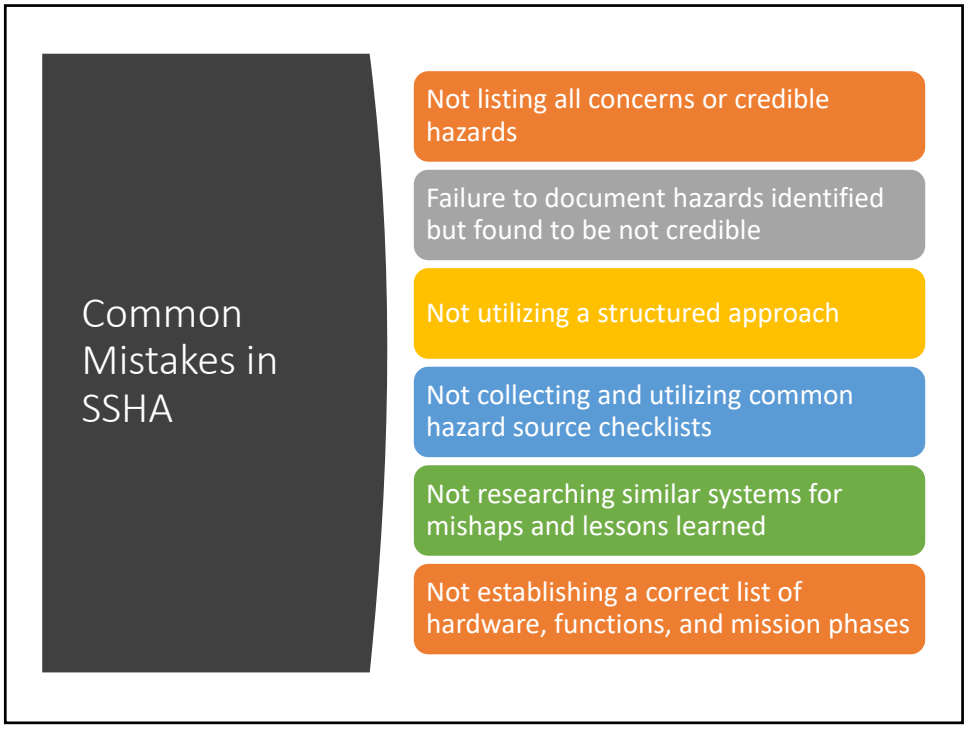



11

## SSHA Worksheet

| System: (1) Subsystem: (2) | | | Subsystem Hazard Analysis | | | | Analyst: (3) Date: (4) | | |
|---|---|---|---|---|---|---|---|---|---|
| No. | Hazard | Causes | Effects | Mode | IMRI | Recommended Action | FMRI | Comments | Status |
| (5) | (6) | (7) | (8) | (9) | (10) | (11) | (12) | (13) | (14) |

12


Common Mistakes in SSHA
Not listing all concerns or credible hazards
Failure to document hazards identified but found to be not credible
Not utilizing a structured approach
Not collecting and utilizing common hazard source checklists
Not researching similar systems for mishaps and lessons learned
Not establishing a correct list of hardware, functions, and mission phases

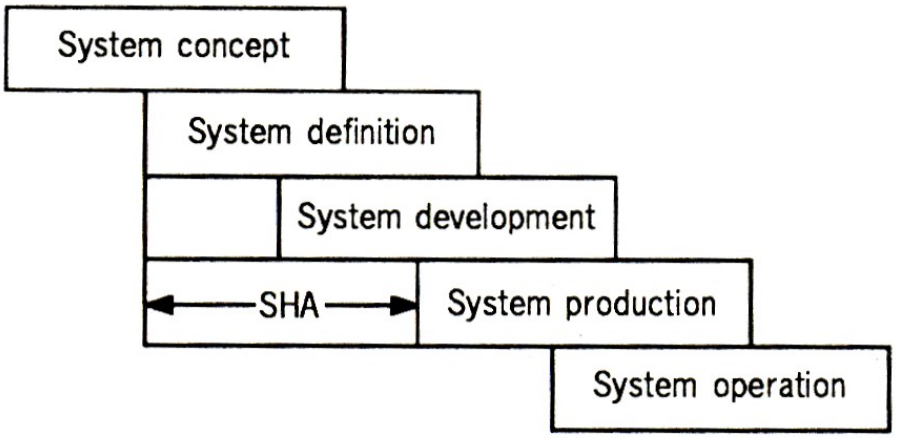
13


Common Mistakes in SSHA
Using too many abbreviations and Acronyms (misunderstanding and confusion)
Inadequately describing the identified hazard
Inadequately describing the causal
Inadequately describing the hazard mishap risk index
Providing recommended hazard mitigation methods that do not address the actual causal factor(s).
Incorrectly closing the hazard.
Not establishing and utilizing a list of TLMs and SCFs.

14

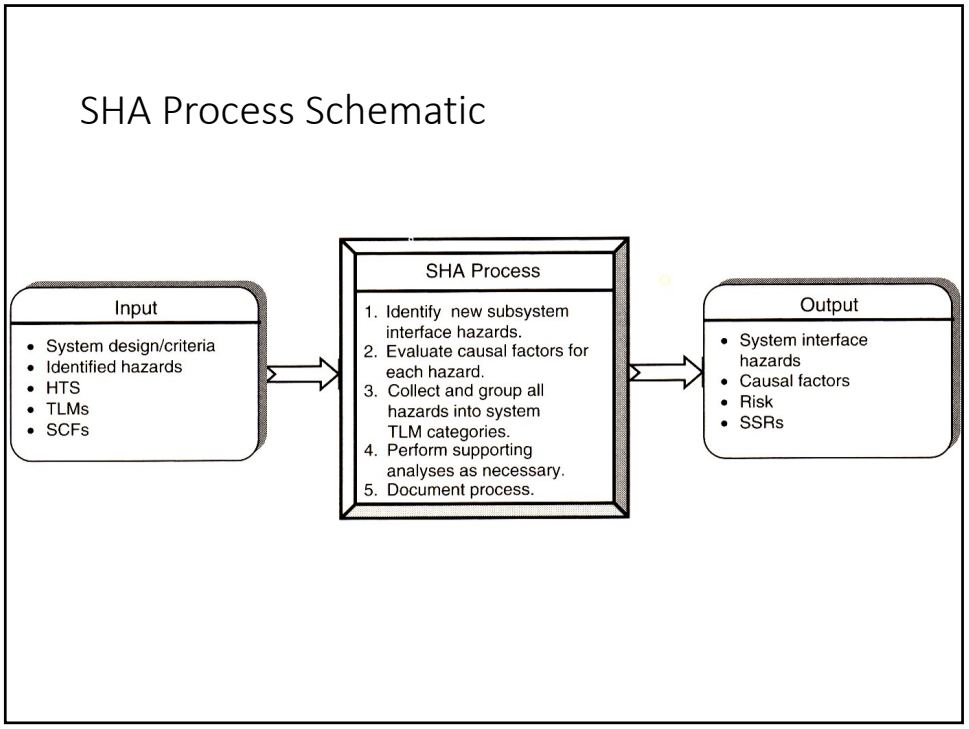
# System Hazard Analysis (SHA)
# Chapter 10

15

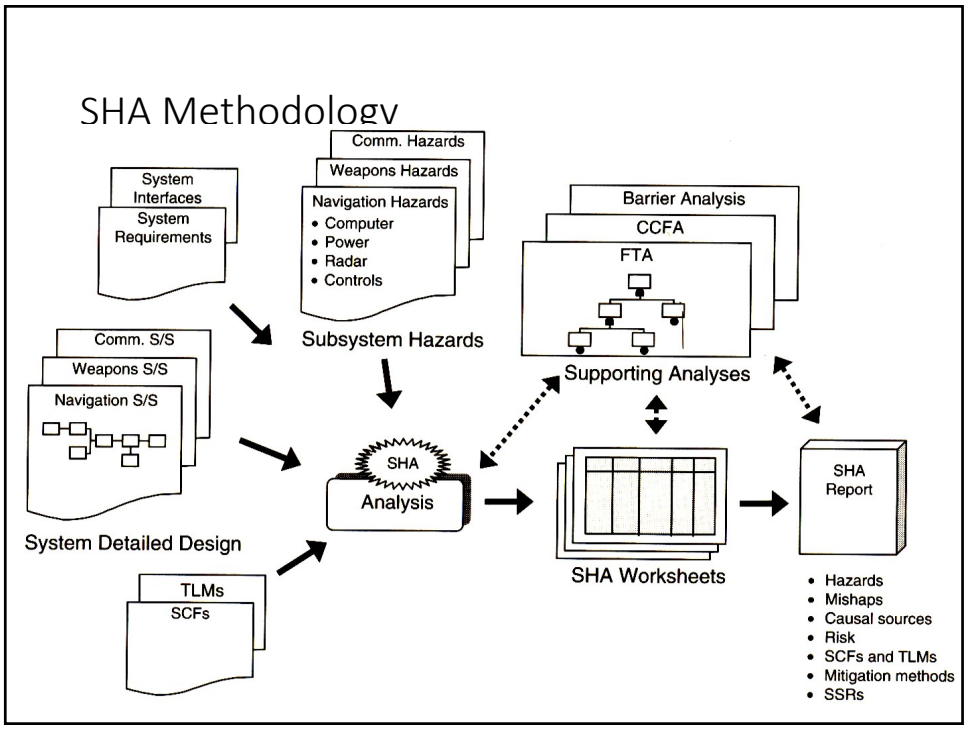



Roland, H.E. and Moriarty, B., "System Safety Engineering and Management," 2nd ed., Wiley, 1990

16


SHA Process Schematic
Input
• System design/criteria
• Identified hazards
• HTS
• TLMs
• SCFs
SHA Process
1. Identify new subsystem interface hazards.
2. Evaluate causal factors for each hazard.
3. Collect and group all hazards into system TLM categories.
4. Perform supporting analyses as necessary.
5. Document process.
Output
• System interface hazards
• Causal factors
• Risk
• SSRs

17


SHA Methodology
System Interfaces
System Requirements
Comm. Hazards
Weapons Hazards
Navigation Hazards
• Computer
• Power
• Radar
• Controls
Subsystem Hazards
Barrier Analysis
CCFA
FTA
Supporting Analyses
Comm. S/S
Weapons S/S
Navigation S/S
System Detailed Design
SHA
Analysis
SHA Worksheets
SHA Report
TLMs
SCFs
• Hazards
• Mishaps
• Causal sources
• Risk
• SCFs and TLMs
• Mitigation methods
• SSRs

18

## SHA Process

| | |
|---|---|
| Define | Define system, boundaries, mission |
| Plan | Plan SHA, goals, worksheets, schedule |
| Establish | Establish safety criteria, SCFs |
| Review | Review TLMs from identified hazards and SCFs |
| Identify | Identify system interface hazards |
| Evaluate | Evaluate risk for each hazard (before/after mitigation) |
| Recommend | Recommend corrective action, SSRs, evaluate tests |
| Track | Track new hazards |
| Document | Document SHA, corrective actions |

19

## SHA Worksheet

System: (1) **System Hazard Analysis** Analyst: (2) Date: (3)

| No. | TLM / SCF | Hazard | Causes | Effects | IMRI | Recommended Action | FMRI | Status |
|---|---|---|---|---|---|---|---|---|
| (4) | (5) | (6) | (7) | (8) | (9) | (10) | (11) | (12) |

20

## SHA Advantages

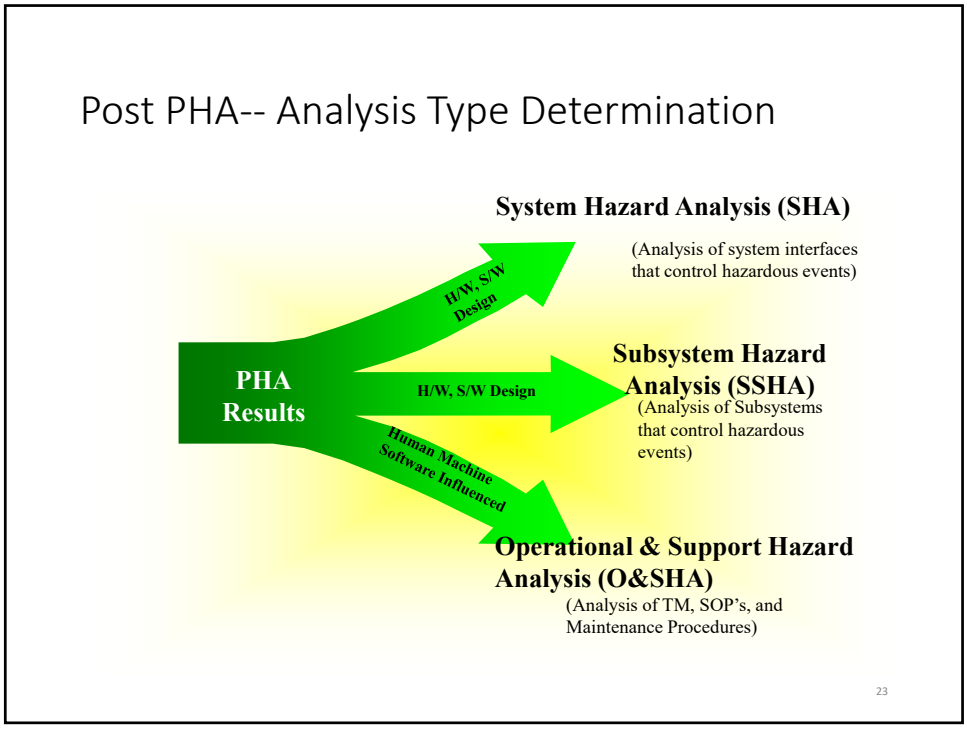
- Identifies System interface-type hazards
- Consolidates hazards to ensure that causal factors are thoroughly investigated and mitigated
- Identifies critical system-level hazards that must be evaluated in more detail through the use of other analysis techniques.
- Provides the basis for making an assessment of overall system risk.

21

## Common Mistakes

- Not thoroughly investigating causal factors
- Risk Index doesn't match identified effects
- Closing hazards prematurely without complete causal factor analysis
- Failure to analyze common cause events and dependent events
- Using Fault Trees in place of SHA

22


Post PHA-- Analysis Type Determination
System Hazard Analysis (SHA)
(Analysis of system interfaces that control hazardous events)
H/W, S/W Design
PHA Results
H/W, S/W Design
Subsystem Hazard Analysis (SSHA)
(Analysis of Subsystems that control hazardous events)
Human Machine Software Influenced
Operational & Support Hazard Analysis (O&SHA)
(Analysis of TM, SOP's, and Maintenance Procedures)
23

23