International System Safety Training Symposium

Functional Hazard Analysis (FHA) Tutorial

5 August 2014

Mr. Adam Scharl
NSWCDD, 540-653-7940
adam.scharl@navy.mil

Mr. Rani Kady, Ph.D.
NSWCDD, 540-653-2409
rani.kady@navy.mil

Mr. Kevin Stottlar
NSWCDD, 540-653-7301
kevin.stottlar@navy.mil

Mr. Michael Ingram
NOSSA, 301-744-6750
michael.o.ingram@navy.mil
FHA Tutorial Agenda

SESSION 1
• 0800-0850 What’s an FHA, FHA Tutorial Goals and Objectives, System Architecture and Architecture Framework

SESSION 2
• 0900-0950 Interpreting System Architecture Data

SESSION 3
• 1030-1120 Evaluating Functional Failures

SESSION 4
• 1330-1420 Evaluating Functional Failures (Cont’d), Tracing Functions to Subsystems

SESSION 5
• 1430-1520 Identifying Existing and Recommended Hazard Mitigations

SESSION 6
• 1600-1650 Decomposing Functions to Components, Identifying Risk Levels, Determining SwCI and Documenting FHA results
FHA Tutorial Goals

• The Tutorial shall:
  – Describe the relationship of an FHA to the overall system safety program
  – Identify Systems Engineering (SE) artifacts that can be used to conduct an FHA
  – Define the processes associated with the conduct of an FHA
  – Describe the output of an FHA
FHA Tutorial Learning Objectives

• Understand the relationship between the FHA and other safety analyses

• Familiarization with Department of Defense Architecture Framework (DoDAF) version 2.0 views and their relationship to the FHA
  – Including tracing functions to physical components and interfaces

• Understand the process for identifying
  – Functional hazards
  – Safety-Significant Functions (SSFs)
  – Safety-Significant Items (SSIs)

• Gain exposure to system requirements and design options that mitigate functional hazards

• Understand the considerations for documenting the process and results of the FHA
What is an FHA and why is it important?

- It is an analysis which focuses on identifying and classifying system functions and the safety, environmental, and health-related consequences associated with functional failure or malfunction.
- While performing an FHA consider the following to identify and evaluate functions:
  - Decomposition of the system and its major subsystems to the major component level
  - A functional description of each subsystem and component identified
  - A functional description of interfaces between subsystems and components
  - Hazards associated with loss of function, degraded function, malfunction, functioning out of time, or out of sequence

- PER MIL-STD-882E, Task 208, at a minimum, the analysis shall identify:
  - An assessment of the risk associated with each identified failure of a function
  - An assessment of whether the functions identified are to be implemented in the design hardware, software, or human control interfaces. The assessment should map the functions to their implementing components.
  - An assessment of the Software Control Category (SCC) for each SSF implemented by software
  - A Software Criticality Index (SwCI) for each SSF implemented by software mapped to the design architecture
  - A list of requirements and constraints that, when successfully implemented, will eliminate the hazard or reduce the risk. These could be in the form of fault tolerance, detection, isolation, annunciation, or recovery.
FHA in Acquisition Life Cycle

SYSTEM SAFETY MANAGEMENT PLAN
Guidelines for coordination/conduct of large system safety programs

SYSTEM SAFETY PROGRAM PLAN
Specifics detailing system safety methods, efforts, tasks and milestones

SAFETY TEST PLANING

SAFETY TESTING

PHL
FHA
PHA

PESHE
SRHA
SRVM
SSH A
SHA
O&SHA
HHA

CHANGE REVIEW & ANALYSIS
Hazard Tracking Database

Safety Assessment Reports and Formal WSESRB Reviews

Introductory
Pre-CDR
Pre-Low Rate Initial Production (LRIP)
As-occurring, prior to at-sea testing
Pre-Deployment
Pre-Full Rate Production (FRP)
Conceptual System Design

- Problem Definition and Need Identification
- System Operational Requirements
  - Mission Definition
  - Performance and Physical Parameters
  - Operational Deployment or Distribution
  - Operational Life Cycle
  - Utilization Requirements
  - Effectiveness Factors
  - Environment
- Maintenance and Support Concept
- Technical Performance Measures (TPMs)
- *Functional Analysis and Allocation*
- System Trade-Off Analysis
- System Specification

*B&F, Systems Engineering and Analysis, Chapter 3*
Functional Analysis

• An essential activity in early conceptual and preliminary design is the development of a functional description of the system
• [Functions] may ultimately be accomplished through the use of equipment, software, people, facilities, data, or various combinations thereof
• The objective is to specify the what’s and not the how’s; that is, what needs to be accomplished versus how it is to be done
• Constitutes an iterative process of breaking down system-level requirements into successive levels of detail
  – Should include coverage of all activities throughout the system life cycle
  – Should be concerned with what is required before looking at how it should be accomplished
  – Should be flexible to allow for expansion if additional definition is required or reduction if too much detail is presented
• The objective is to progressively and systematically work down to the level where resources can be identified with how a task should be accomplished

B&F, Systems Engineering and Analysis,
Chapter 3
**Key FHA Terms and Definitions**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function</td>
<td>A task, action, or activity that must be accomplished to achieve a desired outcome or provide a desired capability (Kossiakoff and Sweet, Systems Engineering Principles and Practice, 2003). A <strong>verb</strong> with known (and unknown) outcomes. Examples: <strong>Protect, Communicate, Sense, Eat.</strong></td>
</tr>
<tr>
<td>Functional Analysis</td>
<td>An activity in early conceptual design, undertaken to develop a functional description of the system. The objective is to specify the what's and not the how's; that is, what needs to be done versus how it is to be done.</td>
</tr>
<tr>
<td>Architecture</td>
<td>The structure of components, the relationships between components, and the principles and guidelines governing them. Includes functions, requirements, components, capabilities, data, lines of communication, and more.</td>
</tr>
<tr>
<td>Architecture Framework</td>
<td>A tool that provides a method for designing a system in terms of common building blocks and the ways those building blocks fit together.</td>
</tr>
<tr>
<td>DoD Architecture Framework (DoDAF v 2.0)</td>
<td>DoD’s architecture framework. It defines a common approach for describing, presenting, and comparing DoD architectures, ensuring that architectures can be compared across organizational boundaries.</td>
</tr>
<tr>
<td>Viewpoint</td>
<td>A representation of the system or architecture from the perspective of a specific set of concerns.</td>
</tr>
<tr>
<td>View</td>
<td>One view within a viewpoint.</td>
</tr>
</tbody>
</table>

VIPPS is a Mock System used for training purposes only.
System Architecture
and Architecture Framework
Architecture Model

• Documents system functions and their relationships (among other things)
• Helps ensure traceability of operational requirements and system functions
• Identifies necessary internal and external interfaces
• Allows for initial verification and validation planning
Architecture and Architecture Framework

- System architecture information is required to conduct the FHA
- Architecture is the structure of components, the relationships between components, and the principles and guidelines governing them
  - Includes functions, requirements, components, capabilities, data, lines of communication, operators, and more
- Architecture Framework is a tool to provide a set of common building blocks for designing system architecture
  - DoDAF v 2.0 is the DoD’s architecture framework
    - Defines a common approach for describing, presenting, and comparing DoD architectures
    - Facilitates the use of common principles, assumptions, and terminology
    - Ensures that architecture descriptions can be compared and related across organizational boundaries
Overarching aspects of architecture context that relate to all views

<table>
<thead>
<tr>
<th>Viewpoint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Viewpoint</td>
<td>Articulate the applicable Operational, Business, Technical, and Industry policy, standards, guidance, constraints, and forecasts.</td>
</tr>
<tr>
<td>Data and Information Viewpoint</td>
<td>Articulate the data relationships and alignment structures in the architecture environment.</td>
</tr>
<tr>
<td>Standards Viewpoint</td>
<td>Articulate the applicable Operational, Business, Technical, and Industry policy, standards, guidance, constraints, and forecasts.</td>
</tr>
<tr>
<td>Capability Viewpoint</td>
<td>Articulate the capability requirement, delivery timing, and deployed capability.</td>
</tr>
<tr>
<td>Operational Viewpoint</td>
<td>Articulate operational scenarios, process, activities and requirements.</td>
</tr>
<tr>
<td>Services Viewpoint</td>
<td>Articulate the performers, activities, services, and their exchanges providing for, or supporting, DoD functions.</td>
</tr>
<tr>
<td>Systems Viewpoint</td>
<td>Articulate the legacy systems or independent systems, their composition, interconnectivity, and context providing for, or supporting, DoD functions.</td>
</tr>
<tr>
<td>Project Viewpoint</td>
<td>Describe the relationships between operational and capability requirements and the various projects being implemented. Details dependencies between capability management and the Defense Acquisition System process.</td>
</tr>
</tbody>
</table>

- There are dozens of views in DoDAF that a program may use, but the architecture information needed to conduct an FHA is contained in just a few views
  - OV-1: High Level Operational Concept Graphic
  - SV-4: Systems Functionality Description
  - SV-5: Operational Activity to Systems Traceability Matrix
• OV-1’s main role is to give context and aid discussion about the system

• OV-1 describes the mission or scenario, including:
  – Main operations (what the system is supposed to do)
  – Interactions with environment and external systems, organizations, or actors
  – System boundary

• OV-1 can be for just one smaller component or element of a larger system or system of systems

• OV-1 use and purpose still applies, even at lower levels
Very Important Person Protection System (VIPPS) OV-1

VIPPS is a Mock System used for training purposes only.

NSWCDD-PN-14-00294 is approved for Distribution Statement A: Approved for Public Release; distribution is unlimited.
# Systems Viewpoint

<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SV-1 Systems Interface Description</td>
<td>The identification of system, system items, and their interconnections.</td>
</tr>
<tr>
<td>SV-3 Systems-Systems Matrix</td>
<td>The relationship among systems in a given Architecture Description. It can be designed to show relationships of interest.</td>
</tr>
<tr>
<td>SV-4 Systems Functionality Description</td>
<td>The functions (activities) performed by systems and the system data flows among system functions (activities).</td>
</tr>
<tr>
<td>SV-5a Operational Activity to Systems Function Traceability Matrix</td>
<td>A mapping of system functions back to operational activities.</td>
</tr>
<tr>
<td>SV-5b Operational Activity to Systems Traceability Matrix</td>
<td>A mapping of systems back to capabilities or operational activities.</td>
</tr>
<tr>
<td>SV-6 Systems Resource Flow Matrix</td>
<td>Provides details of system resource flow elements being exchanged between systems and the attributes of that exchange.</td>
</tr>
<tr>
<td>SV-7 Systems Measures Matrix</td>
<td>The measures (metrics) of Systems Model elements of the appropriate timeframe(s).</td>
</tr>
<tr>
<td>SV-8 Systems Evolution Description</td>
<td>The planned incremental steps toward migrating a suite of systems to a more efficient suite, or toward evolving a current system to a future implementation.</td>
</tr>
<tr>
<td>SV-9 Systems Technology and Skills Forecast</td>
<td>The emerging technologies, software/hardware products, and skills that are expected to be available in a given set of time frames and that will affect future system development.</td>
</tr>
<tr>
<td>SV-10a Systems Rules Model</td>
<td>One of three models used to describe system functionality. It identifies constraints that are imposed on systems functionality due to some aspect of system design or implementation.</td>
</tr>
<tr>
<td>SV-10b Systems State Transition Description</td>
<td>One of three models used to describe system functionality. It identifies responses of systems to events.</td>
</tr>
<tr>
<td>SV-10c Systems Event-Trace Description</td>
<td>One of three models used to describe system functionality. It identifies system-specific refinements of critical sequences of events described in the Operational Viewpoint.</td>
</tr>
</tbody>
</table>
VIPPS SV-4 (Functional Hierarchy)

Provide VIPPS Capability
F.0

- Produce System
  F.1
- Handle/Transport System
  F.2
- Install System
  F.3
- Operate System
  F.4
- Maintain System
  F.5
- Dispose of System
  F.6

VIPPS is a Mock System used for training purposes only.
VIPPS SV-4 (Functional Hierarchy)
VIPPS SV-4 (Functional Hierarchy)

Provide VIPPS Capability
F.0

- Produce System
  F.1

- Handle/Transport System
  F.2

- Install System
  F.3

- Operate System
  F.4

- Maintain System
  F.5

- Dispose of System
  F.6

Control States and Modes
F.4.1

- Sense
  F.4.2

- Evaluate
  F.4.3

- Warn
  F.4.4

- Lethally Engage
  F.4.5

- Initialize
  F.4.1.1

- Perform BIT
  F.4.1.2

- Transition State/Mode
  F.4.1.3

- Log State/Mode Data
  F.4.1.4
VIPPS SV-4 (Functional Hierarchy)

Provide VIPPS Capability
F.0

- Produce System F.1
- Handle/Transport System F.2
- Install System F.3
- Operate System F.4
- Maintain System F.5
- Dispose of System F.6

Control States and Modes F.4.1

- Initialize F.4.1.1
- Perform BIT F.4.1.2
- Transition State/Mode F.4.1.3
- Log State/Mode Data F.4.1.4

- Detect F.4.2.1
- Generate Track F.4.2.2
- Perform Surveillance F.4.2.3
- Correlate/Maintain Tracks F.4.2.4
- Log Sensor Data F.4.2.5

- Sense F.4.2

- Evaluate F.4.3

- Identify F.4.3.1
- Provide Operator SA F.4.3.3
- Log Assessment Data F.4.3.4
- Reassess F.4.3.5

- Warn F.4.4

- Select Zone and Non-Lethal Effector F.4.4.1
- Activate Non-Lethal Effector F.4.4.3
- Log Non-Lethal Event Data F.4.4.4

- Lethally Engage F.4.5

- Select Zone and Lethal Effector F.4.5.1
- Verify Intent to Engage F.4.5.2
- Activate Lethal Effector F.4.5.3
- Log Lethal Engagement Data F.4.5.4
- Aim/Target F.4.5.5
VIPPS SV-4 (Functional Hierarchy)

Provide VIPPS Capability
F.0

- Produce System
  F.1
- Handle/Transport System
  F.2
- Install System
  F.3
- Operate System
  F.4
- Maintain System
  F.5
- Dispose of System
  F.6

- Control States and Modes
  F.4.1
  - Initialize
    F.4.1.1
  - Perform BIT
    F.4.1.2
  - Transition State/
    Mode
    F.4.1.3
  - Log State/Mode Data
    F.4.1.4

- Sense
  F.4.2
  - Detect
    F.4.2.1
  - Generate Track
    F.4.2.2
  - Perform Surveillance
    F.4.2.3
  - Correlate/Maintain
    Tracks
    F.4.2.4
  - Log Sensor Data
    F.4.2.5

- Evaluate
  F.4.3
  - Identify
    F.4.3.1
  - Recommend Action
    F.4.3.2
  - Provide Operator SA
    F.4.3.3
  - Log Assessment Data
    F.4.3.4

- Warn
  F.4.4
  - Select Zone and Non-
    Lethal Effector
    F.4.4.1
  - Verify Intent to Warn
    F.4.4.2
  - Activate Non-Lethal
    Effector
    F.4.4.3
  - Log Non-Lethal Event
    Data
    F.4.4.4

- Lethally Engage
  F.4.5
  - Select Zone and Lethal Effector
    F.4.5.1
  - Verify Intent to Engage
    F.4.5.2
  - Activate Lethal
    Effector
    F.4.5.3
  - Log Lethal Engagement Data
    F.4.5.4
  - Aim/Target
    F.4.5.5
VIPPS is a Mock System used for training purposes only.

VIPPS SV-4
(Functional Flow Block Diagram)
VIPPS SV-4 (Functional Hierarchy)

Provide VIPPS Capability F.0

- Produce System F.1
- Handle/Transport System F.2
- Install System F.3
- Operate System F.4
- Maintain System F.5
- Dispose of System F.6

Control States and Modes F.4.1

- Initialize F.4.1.1
- Perform BIT F.4.1.2
- Transition State/Mode F.4.1.3
- Log State/Mode Data F.4.1.4

- Sense F.4.2
- Generate Track F.4.2.2
- Perform Surveillance F.4.2.3
- Correlate/Maintain Tracks F.4.2.4
- Log Sensor Data F.4.2.5

- Evaluate F.4.3
- Identify F.4.3.1
- Recommend Action F.4.3.2
- Provide Operator SA F.4.3.3
- Log Assessment Data F.4.3.4
- Reassess F.4.3.5

- Warn F.4.4
- Select Zone and Non-Lethal Effector F.4.4.1
- Verify Intent to Warn F.4.4.2
- Activate Non-Lethal Effector F.4.4.3
- Log Non-Lethal Event Data F.4.4.4

- Lethally Engage F.4.5
- Select Zone and Lethal Effector F.4.5.1
- Verify Intent to Engage F.4.5.2
- Activate Lethal Effector F.4.5.3
- Log Lethal Engagement Data F.4.5.4
- Aim/Target F.4.5.5
F.4.1 - Control States and Modes

- Initialize F.4.1.1
- Perform BIT F.4.1.2
- Transition State/Mode F.4.1.3
- Log State/Mode Data F.4.1.4
Session 1 Summary

- The FHA provides early insight to safety aspects of the system during conceptual system design
- System Architecture Model provides source material for conducting an FHA
  - Architecture frameworks provide commonality between various system architecture models
  - Operational and functional architecture provides starting point for the FHA
FHA Tutorial Agenda

SESSION 1
• 0800-0850 What’s an FHA, FHA Tutorial Goals and Objectives, System Architecture and Architecture Framework

SESSION 2
• 0900-0950 Interpreting System Architecture Data

SESSION 3
• 1030-1120 Evaluating Functional Failures

SESSION 4
• 1330-1420 Evaluating Functional Failures (Cont’d), Tracing Functions to Subsystems

SESSION 5
• 1430-1520 Identifying Existing and Recommended Hazard Mitigations

SESSION 6
• 1600-1650 Decomposing Functions to Components, Identifying Risk Levels, Determining SwCI and Documenting FHA Results
FHA process is used to identify and classify the system functions and safety hazards, environmental, and health-related consequences associated with functional failure or malfunction; i.e., hazards

- Identifies the relationships between functions and hazards, thereby identifying the SSFs of the system as well as the hazards associated with that functionality
- This identification provides a foundation for the safety program to scope additional safety analyses and Level of Rigor (LOR) verification of the system’s SSFs
- Provides the safety engineer a perspective with which to participate in functional definition of the system under analysis
- Starts the mitigation solution discussion
FHA Process Flow

1. Gather and Interpret System Architecture Data

2. Evaluate Functional Failures for Hazards

3. Identify Safety Significant Subsystems and Interfaces

4. Identify Existing and Recommended Mitigations

5. Decompose SSFs to Components

6. Identify Risk Levels, SwClIs, and Follow-On Actions

7. Document Analysis
FHA Process Flow

1. Gather and Interpret System Architecture Data
2. Evaluate Functional Failures for Hazards
3. Identify Safety Significant Subsystems and Interfaces
4. Identify Existing and Recommended Mitigations

5. Decompose SSFs to Components
6. Identify Risk Levels, SwCIs, and Follow-On Actions
7. Document Analysis
Task 1b

• Task 1: Gather and interpret design data
  – Task 1.b: Evaluate DoDAF views for use case coverage
    • Trace functions to capabilities and identify gaps
  – Task 1.c: Identify inputs/outputs and flow of functions
    • For the selected functions, identify the inputs and outputs of each and determine whether the function occurs continuously
1. The Very Important Person Protection System (VIPPS) should detect and track threats approaching the VIP’s house. It should characterize the movements of those threats and aid the operator in recognizing hostile actions and intent. The intrusion should cause an alert at the operator’s console and provide the operator an approach bearing on the threat. The VIPPS will track the threat via video and allow ID assignments. Based on hostile intent and distance from the home, the operator will engage within the warning zone with an Unambiguous Warning Device (UWD), consisting of a loudspeaker and/or high intensity spotlight. If the intruder continues toward the home with determined hostile intent, the operator shall employ lethal effectors to neutralize the intruder before they enter the house.
VIPPS CONOPS as a Use Case

VIPPS is a Mock System used for training purposes only.

VIPPS Detects and Tracks Threat
VIPPS Characterizes Threat
VIPPS Determines Course of Action
VIPPS Warns Threat
VIPPS Lethally Engages Threat

Threat Enters Detection Zone

Sensor/device coverage

Assessment Zone

NSWCDD-PN-14-00294 is approved for Distribution Statement A: Approved for Public Release; distribution is unlimited.
1. The Very Important Person Protection System (VIPPS) should **detect** and track **threats** approaching the VIP’s house. It should characterize the movements of those threats and aid the operator in recognizing hostile actions and intent. The intrusion should cause an alert at the operator’s console and provide the operator an approach bearing on the threat. The VIPPS will track the threat via video and allow ID assignments. Based on hostile intent and distance from the home, the operator will engage within the warning zone with an Unambiguous Warning Device (UWD), consisting of a loudspeaker and/or high intensity spotlight. If the intruder continues toward the home with determined hostile intent, the operator shall employ lethal effectors to neutralize the intruder before they enter the house.
VIPPS Functional Hierarchy

Provide VIPPS Capability
F.0

- Produce System  F.1
  - Control States and Modes  F.4.1
    - Initialize  F.4.1.1
    - Perform BIT  F.4.1.2
    - Transition State/Mode  F.4.1.3
    - Log State/Mode Data  F.4.1.4
  - Detect  F.4.2.1
    - Perform BIT  F.4.2.2
    - Perform Surveillance  F.4.2.3
    - Correlate/Maintain Tracks  F.4.2.4
    - Log Sensor Data  F.4.2.5
  - Generate Track  F.4.2.2
  - Generate Track  F.4.2.2
  - Generate Track  F.4.2.2

- Handle/Transport System  F.2
  - Sense  F.4.2
    - Identify  F.4.3.1
    - Recommend Action  F.4.3.2
    - Provide Operator SA  F.4.3.3
    - Log Assessment Data  F.4.3.4
    - Reassess  F.4.3.5
  - Generate Track  F.4.2.2
  - Generate Track  F.4.2.2
  - Generate Track  F.4.2.2

- Install System  F.3
  - Evaluate  F.4.3
    - Select Zone and Non-Lethal Effector  F.4.4.1
    - Verify Intent to Warn  F.4.4.2
    - Activate Non-Lethal Effector  F.4.4.3
    - Log Non-Lethal Event Data  F.4.4.4
  - Log Non-Lethal Event Data  F.4.4.4
  - Log Non-Lethal Event Data  F.4.4.4

- Operate System  F.4
  - Warn  F.4.4
    - Select Zone and Lethal Effector  F.4.5.1
    - Verify Intent to Engage  F.4.5.2
    - Activate Lethal Effector  F.4.5.3
    - Log Lethal Engagement Data  F.4.5.4
  - Aim/Target  F.4.5.5

- Maintain System  F.5
  - Dispose of System  F.6
1. The Very Important Person Protection System (VIPPS) should **detect** threats.

2. and track threats approaching the VIP’s house. It should characterize

**From VIPPS CONOPS**

<table>
<thead>
<tr>
<th>Source</th>
<th>Capability</th>
<th>Function No.</th>
<th>Function Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONOPS line 1-2</td>
<td>Detect threats</td>
<td>F.4.2.1</td>
<td>Detect</td>
</tr>
</tbody>
</table>
Task 1b Example (Cont’d)

VIPPS ICD

From VIPPS Initial Capabilities Document (ICD)

MCT 5.1.1.2 - Provide Telephone Communications (Page 5)
Function Context

Provide VIPPS Capability
F.0

- Produce System
  F.1
- Handle/Transport System
  F.2
- Install System
  F.3
- Operate System
  F.4
- Maintain System
  F.5
- Dispose of System
  F.6

Control States and Modes
F.4.1

- Initialize
  F.4.1.1
- Perform BIT
  F.4.1.2
- Transition State/ Mode
  F.4.1.3
- Log State/Mode Data
  F.4.1.4

Sense
F.4.2

- Detect
  F.4.2.1
- Generate Track
  F.4.2.2
- Perform Surveillance
  F.4.2.3
- Correlate/Maintain Tracks
  F.4.2.4
- Log Sensor Data
  F.4.2.5

Evaluate
F.4.3

- Identify
  F.4.3.1
- Recommend Action
  F.4.3.2
- Provide Operator SA
  F.4.3.3
- Log Assessment Data
  F.4.3.4

Warn
F.4.4

- Select Zone and Non-Lethal Effector
  F.4.4.1
- Verify Intent to Warn
  F.4.4.2
- Activate Non-Lethal Effector
  F.4.4.3
- Log Non-Lethal Event Data
  F.4.4.4

Lethally Engage
F.4.5

- Select Zone and Lethal Effector
  F.4.5.1
- Verify Intent to Engage
  F.4.5.2
- Activate Lethal Effector
  F.4.5.3
- Log Lethal Engagement Data
  F.4.5.4
- Aim/Target
  F.4.5.5
### Task 1b Example (Cont’d)

<table>
<thead>
<tr>
<th>Source</th>
<th>Capability</th>
<th>Function No.</th>
<th>Function Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONOPS line 1-2</td>
<td>Detect threats</td>
<td>F.4.2.1</td>
<td>Detect</td>
</tr>
<tr>
<td>ICD Page 5</td>
<td>Provide Telephone communications</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**MCT 5.1.1.2 - Provide Telephone Communications (Page 5)**

**From VIPPS Initial Capabilities Document (ICD)**
### Table: Source, Capability, Function No., Function Name

<table>
<thead>
<tr>
<th>Source</th>
<th>Capability</th>
<th>Function No.</th>
<th>Function Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONOPS line 1 and 2</td>
<td>Detect threats</td>
<td>F.4.2.1</td>
<td>Detect</td>
</tr>
<tr>
<td>ICD Page 5</td>
<td>Provide Telephone communications</td>
<td>None Identified</td>
<td>None Identified</td>
</tr>
<tr>
<td>CONOPS line 2</td>
<td>Track threats</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. The Very Important Person Protection System (VIPPS) should **detect**
2. and **track threats** approaching the VIP’s house. It should characterize
1. The Very Important Person Protection System (VIPPS) should detect and **track threats** approaching the VIP’s house. It should characterize...
### Task 1b Exercise

<table>
<thead>
<tr>
<th>Source</th>
<th>Capability</th>
<th>Function No.</th>
<th>Function Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONOPS line 1-2</td>
<td>Detect threats</td>
<td>F.4.2.1</td>
<td>Detect</td>
</tr>
<tr>
<td>CONOPS line 2</td>
<td>Track threats</td>
<td>F.4.2.2</td>
<td>Generate Track</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.2.4</td>
<td>Correlate/Maintain Tracks</td>
</tr>
<tr>
<td>CONOPS line 3-4</td>
<td>Aid operator in recognizing hostile actions and intent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CONOPS line 11</td>
<td>Employ lethal effectors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICD Page 5</td>
<td>Provide Telephone communications</td>
<td>None Identified</td>
<td>None Identified</td>
</tr>
<tr>
<td>ICD Page 5</td>
<td>Provide Single Channel Radio Communications</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Task 1b Exercise

<table>
<thead>
<tr>
<th>Source</th>
<th>Capability</th>
<th>Function No.</th>
<th>Function Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONOPS line 1-2</td>
<td>Detect threats</td>
<td>F.4.2.1</td>
<td>Detect</td>
</tr>
<tr>
<td>CONOPS line 2</td>
<td>Track threats</td>
<td>F.4.2.2</td>
<td>Generate Track</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.2.4</td>
<td>Correlate/Maintain Tracks</td>
</tr>
<tr>
<td>CONOPS line 3-4</td>
<td>Aid operator in recognizing hostile actions and intent</td>
<td>F.4.3.1</td>
<td>Identify</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.3.3</td>
<td>Provide Operator SA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.3.5</td>
<td>Reassess</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.3.2</td>
<td>Recommend Action</td>
</tr>
<tr>
<td>CONOPS line 11</td>
<td>Employ lethal effectors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICD Page 5</td>
<td>Provide Telephone communications</td>
<td>None Identified</td>
<td>None Identified</td>
</tr>
<tr>
<td>ICD Page 5</td>
<td>Provide Single Channel Radio Communications</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Task 1b Exercise**

<table>
<thead>
<tr>
<th>Source</th>
<th>Capability</th>
<th>Function No.</th>
<th>Function Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONOPS line 1-2</td>
<td>Detect threats</td>
<td>F.4.2.1</td>
<td>Detect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.2.2</td>
<td>Generate Track</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.2.4</td>
<td>Correlate/Maintain Tracks</td>
</tr>
<tr>
<td>CONOPS line 2</td>
<td>Track threats</td>
<td>F.4.2.2</td>
<td>Generate Track</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.3.3</td>
<td>Provide Operator SA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.3.5</td>
<td>Reassess</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.3.2</td>
<td>Recommend Action</td>
</tr>
<tr>
<td></td>
<td>Aid operator in recognizing hostile actions and intent</td>
<td>F.4.3.1</td>
<td>Identify</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.3.3</td>
<td>Provide Operator SA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.3.5</td>
<td>Reassess</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.3.2</td>
<td>Recommend Action</td>
</tr>
<tr>
<td>CONOPS line 3-4</td>
<td>Detect threats</td>
<td>F.4.2.1</td>
<td>Detect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.2.2</td>
<td>Generate Track</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.2.4</td>
<td>Correlate/Maintain Tracks</td>
</tr>
<tr>
<td></td>
<td>Track threats</td>
<td>F.4.2.2</td>
<td>Generate Track</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.2.4</td>
<td>Correlate/Maintain Tracks</td>
</tr>
<tr>
<td></td>
<td>Aid operator in recognizing hostile actions and intent</td>
<td>F.4.3.1</td>
<td>Identify</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.3.3</td>
<td>Provide Operator SA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.3.5</td>
<td>Reassess</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.3.2</td>
<td>Recommend Action</td>
</tr>
<tr>
<td>CONOPS line 11</td>
<td>Employ lethal effectors</td>
<td>F.4.5.1</td>
<td>Select Zone and Lethal Effector</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.5.2</td>
<td>Verify Intent to Engage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.5.5</td>
<td>Aim/Target</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.5.3</td>
<td>Activate Lethal Effector</td>
</tr>
<tr>
<td>ICD Page 5</td>
<td>Provide Telephone communications</td>
<td>None Identified</td>
<td>None Identified</td>
</tr>
<tr>
<td>ICD Page 5</td>
<td>Provide Single Channel Radio Communications</td>
<td>None Identified</td>
<td>None Identified</td>
</tr>
</tbody>
</table>
### Task 1b Exercise

<table>
<thead>
<tr>
<th>Source</th>
<th>Capability</th>
<th>Function No.</th>
<th>Function Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONOPS line 1-2</td>
<td>Detect threats</td>
<td>F.4.2.1</td>
<td>Detect</td>
</tr>
<tr>
<td>CONOPS line 2</td>
<td>Track threats</td>
<td>F.4.2.2</td>
<td>Generate Track</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.2.4</td>
<td>Correlate/Maintain Tracks</td>
</tr>
<tr>
<td>CONOPS line 3-4</td>
<td>Aid operator in recognizing hostile actions and intent</td>
<td>F.4.3.1</td>
<td>Identify</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.3.3</td>
<td>Provide Operator SA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.3.5</td>
<td>Reassess</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.3.2</td>
<td>Recommend Action</td>
</tr>
<tr>
<td>CONOPS line 11</td>
<td>Employ lethal effectors</td>
<td>F.4.5.1</td>
<td>Select Zone and Lethal Effector</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.5.2</td>
<td>Verify Intent to Engage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.5.5</td>
<td>Aim/Target</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F.4.5.3</td>
<td>Activate Lethal Effector</td>
</tr>
<tr>
<td>ICD Page 5</td>
<td>Provide Telephone communications</td>
<td>None Identified</td>
<td>None Identified</td>
</tr>
<tr>
<td>ICD Page 5</td>
<td>Provide Single Channel Radio Communications</td>
<td>None Identified</td>
<td>None Identified</td>
</tr>
</tbody>
</table>
Task 1c

• Task 1: Gather and interpret design data
  – Task 1.b: Evaluate DoDAF views for use case coverage
  • Trace functions to capabilities and identify gaps
  – Task 1.c: Identify inputs/outputs and flow of functions
  • For the selected functions, identify the inputs and outputs of each and determine whether the function occurs continuously
NSWCDD-PN-14-00294 is approved for Distribution Statement A: Approved for Public Release; distribution is unlimited.

VIPPS is a Mock System used for training purposes only
Task 1c Example (Cont’d)

1. Identify F.4.3.1
2. Provide Operator SA F.4.3.3
3. Recommend Action F.4.3.2
4. Log Assessment Data F.4.3.4
5. Reassess F.4.3.5

Provide VIPPS Capability F.0

NSWCDD-PN-14-00294 is approved for Distribution Statement A: Approved for Public Release; distribution is unlimited.

VIPPS is a Mock System used for training purposes only.
**Task 1c Example (Cont’d)**

<table>
<thead>
<tr>
<th>Function</th>
<th>Function Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.4.3</td>
<td>Evaluate</td>
<td>Evaluate sensor objects of interest and communicate the assessments</td>
</tr>
<tr>
<td>F.4.3.1</td>
<td>Identify</td>
<td>Evaluate the potential object of interest against a comparison library to determine if threatening, and communicate the evaluation</td>
</tr>
<tr>
<td>F.4.3.2</td>
<td>Recommend Action</td>
<td>Recommend a course of action to the operator for each track based upon location, identification results, and any previous engagements</td>
</tr>
<tr>
<td>F.4.3.3</td>
<td>Provide Operator SA</td>
<td>Provide the operator with the tactical picture, including tracks, identification status, and recommended actions</td>
</tr>
<tr>
<td>F.4.3.4</td>
<td>Log Assessment Data</td>
<td>Log the track positions, identification results, and recommended actions</td>
</tr>
<tr>
<td>F.4.3.5</td>
<td>Reassess</td>
<td>Reassess tracks based on logged history</td>
</tr>
</tbody>
</table>
Task 1c Example (Cont’d)

<table>
<thead>
<tr>
<th>Function Number</th>
<th>Function Name</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
</table>
| F.4.3.1         | Identify      | 1. Object(s) of Interest  
2. Comparison Library | 1. Threat evaluation  
2. Object(s) of Interest |

F.4.3.1 Identify Evaluate the potential object of interest against a comparison library to determine if threatening, and communicate the evaluation.

VIPPS is a Mock System used for training purposes only.
Task 1c Example (Cont’d)

NSWCDD-PN-14-00294 is approved for Distribution Statement A: Approved for Public Release; distribution is unlimited.
Task 1c Example (Cont’d)

F.0 - Provide VIPPS Capability
### Task 1c Example (Cont’d)

<table>
<thead>
<tr>
<th>Function</th>
<th>Function Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.0</td>
<td>Provide VIPPS Capability</td>
<td>Provide all of the required functionality necessary for the VIPPS to deploy and complete its mission</td>
</tr>
<tr>
<td>F.1</td>
<td>Produce System</td>
<td>Provide the necessary functionality to produce the VIPPS and all of its support, maintenance, and disposal equipment</td>
</tr>
<tr>
<td>F.2</td>
<td>Handle/Transport System</td>
<td><strong>Provide the functionality to handle, package, transport, store, and unpack the VIPPS and all of its support equipment</strong></td>
</tr>
<tr>
<td>F.3</td>
<td>Install System</td>
<td>Provide the functionality required to install the complete VIPPS in its operating location</td>
</tr>
<tr>
<td>F.4</td>
<td>Operate System</td>
<td>Provide the functionality required for VIPPS to provide VIP protection in the defined environment</td>
</tr>
<tr>
<td>F.5</td>
<td>Maintain System</td>
<td>Provide the functionality required to keep the VIPPS supported and fully operational</td>
</tr>
<tr>
<td>F.6</td>
<td>Dispose of System</td>
<td>Provide the functionality required to remanufacture, recycle, or dispose of the VIPPS items at the end of their useful life</td>
</tr>
</tbody>
</table>
### Task 1c Example (Cont’d)

<table>
<thead>
<tr>
<th>Function Number</th>
<th>Function Name</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
</table>
| F.4.3.1         | Identify                       | 1. Object(s) of Interest  
2. Comparison Library | 1. Threat evaluation  
2. Object(s) of Interest |
| F.2             | Handle/Transport System        | 1. Produced System  
2. Transportation/Handling Equipment and Packaging Materials  
3. Fuel | 1. System at Installation Site  
2. Used Transportation/Handling Equipment  
3. Used Packaging Materials  
4. Fuel Emissions |

**F.2 Handle/Transport System**

Provide the functionality to handle, package, transport, store, and unpack a produced VIPPS and all of its support equipment at the installation site.

![Task Flow Diagram](diagram.png)
## Task 1c

**Function Inputs and Outputs Identification Worksheet**

Compare selected Functions with the SV-4s and determine inputs, and outputs

<table>
<thead>
<tr>
<th>Function Number</th>
<th>Function Name</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.4.2</td>
<td>Sense</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.5</td>
<td>Lethally Engage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.1.3</td>
<td>Transition State/Mode</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Discussion of Task 1c Exercise Results
## Task 1c

### Function Inputs and Outputs Identification Worksheet

Compare selected Functions with the SV-4s and determine inputs, and outputs

<table>
<thead>
<tr>
<th>Function Number</th>
<th>Function Name</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
</table>
| F.4.2           | Sense                  | 1. Appropriate State/Mode Confirmation  
2. Evaluated Track  
3. Warned Track  
4. Lethally Engaged Track | 1. Object(s) of Interest (Track) for Evaluation                        |
| F.4.5           | Lethally Engage        | 1. Selected Target/Track                                               | 1. Lethal energy  
2. Lethally Engaged Track                                         |
| F.4.1.3         | Transition State/Mode  |                                                                        |                                                                         |
# Task 1c Answer Key

## Function Inputs and Outputs Identification Worksheet

Compare selected Functions with the SV-4s and determine inputs, and outputs

<table>
<thead>
<tr>
<th>Function Number</th>
<th>Function Name</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.4.2</td>
<td>Sense</td>
<td>1. Appropriate State/Mode Confirmation &lt;br&gt;2. Evaluated Track &lt;br&gt;3. Warned Track &lt;br&gt;4. Lethally Engaged Track</td>
<td>1. Object(s) of Interest (Track) for Evaluation</td>
</tr>
<tr>
<td>F.4.5</td>
<td>Lethally Engage</td>
<td>1. Selected Target/Track</td>
<td>1. Lethal energy &lt;br&gt;2. Lethally Engaged Track</td>
</tr>
</tbody>
</table>
Gather and Interpret Design Data

- Associated some VIPPS capabilities to Functions
- Using SV-4 functional flows, we determined functional inputs and outputs for only a few functions
Session 2 Summary – Interpret System Architecture

• Establish assumptions and understandings to carry forward into assessment of functional failures
• Brainstorm “safety” use cases with which to evaluate functional architecture
• Consider all life-cycle phases, activities, and states/modes
SESSION 1
• 0800-0850  What’s an FHA, FHA Tutorial Goals and Objectives, System Architecture and Architecture Framework

SESSION 2
• 0900-0950  Interpreting System Architecture Data

SESSION 3
• 1030-1120  Evaluating Functional Failures

SESSION 4
• 1330-1420  Evaluating Functional Failures (Cont’d), Tracing Functions to Subsystems

SESSION 5
• 1430-1520  Identifying Existing and Recommended Hazard Mitigations

SESSION 6
• 1600-1650  Decomposing Functions to Components, Identifying Risk levels, Determining SwCI and Documenting FHA Results
FHA Process Flow

1. Gather and Interpret System Architecture Data
2. Evaluate Functional Failures for Hazards
3. Identify Safety Significant Subsystems and Interfaces
4. Identify Existing and Recommended Mitigations
5. Decompose SSFs to Components
6. Identify Risk Levels, SwCIs, and Follow-On Actions
7. Document Analysis
Functional Failures

- **Fails to operate**
  - Function does not happen/perform when given the appropriate input

- **Operates at wrong time (early or late)**
  - Function performs earlier or later than it should have; if too late function could be out of sequence

- **Out of sequence**
  - Function occurs in the incorrect order; function occurs without receiving the appropriate inputs

- **Failure to stop operation**
  - Current function continues even though it should move on to the next function

- **Degraded function/malfunction**
  - Function does not finish or only partially completes (only some outputs are provided); function generates improper output

![Functional Failures Diagram]
1. **Activate Non-Lethal Effector** Function *Fails to Operate*
2. **Activate Non-Lethal Effector** Function *Operates at Wrong Time (Late)*
3. **Activate Lethal Effector** Function *Unable to Stop Operation*
4. **Activate Lethal Effector** Function *Out of Sequence*
5. **Detect** Function *Fails to Operate*

- Brainstorming is not always an effective approach when identifying hazards
- Let's explore a more rigorous and structured approach to Functional Hazard Analysis
Energy Trace Barrier Analysis (ETBA) Framework

- Identify energy-release functions
  - Leverage energy sources identified during Preliminary Hazard List (PHL)
  - Consider architecture artifacts, as available
- Consider the impact of functional failure on energy-release functions
  - All system functions must be considered for impact to energy-release functions
Task 2 Example

Provide VIPPS Capability F.0

- Produce System F.1
- Handle/Transport System F.2
- Install System F.3
- Operate System F.4
- Maintain System F.5
- Dispose of System F.6

Control States and Modes F.4.1

- Initialize F.4.1.1
- Perform BIT F.4.1.2
- Transition State/Mode F.4.1.3
- Log State/Mode Data F.4.1.4

Sense F.4.2

- Detect F.4.2.1
- Generate Track F.4.2.2
- Perform Surveillance F.4.2.3
- Correlate/Maintain Tracks F.4.2.4
- Log Sensor Data F.4.2.5

Evaluate F.4.3

- Identify F.4.3.1
- Recommend Action F.4.3.2
- Provide Operator SA F.4.3.3
- Log Assessment Data F.4.3.4
- Reassess F.4.3.5

Warn F.4.4

- Select Zone and Non-Lethal Effector F.4.4.1
- Verify Intent to Warn F.4.4.2
- Activate Non-Lethal Effector F.4.4.3
- Log Non-Lethal Event Data F.4.4.4
- Log Lethal Engagement Data F.4.4.5

Lethally Engage F.4.5

- Select Zone and Lethal Effector F.4.5.1
- Verify Intent to Engage F.4.5.2
- Activate Lethal Effector F.4.5.3
- Aim/Target F.4.5.5
## Task 2 Example

<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
<th>Hazard Description</th>
<th>Mishap</th>
<th>Effect(s)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Fails to operate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Operates at wrong time (early)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Operates at wrong time (late)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Out of sequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Unable to stop operation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Degraded function/ malfunction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Task 2 Example

<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Fails to operate</td>
</tr>
</tbody>
</table>

Fails to operate: Function does not happen/perform when given the appropriate inputs
## Task 2 Example

<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
<th>Hazard Description</th>
<th>Mishap</th>
<th>Effect(s)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Fails to operate</td>
<td>Failure to perform maintenance results in component failure and unintended release of energy</td>
<td>Personnel, equipment, or the environment exposed to unintended release of energy</td>
<td>Death, injury, equipment/environmental damage</td>
<td>This is really a causal factor that impacts hazards in the operating activity</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Operates at wrong time (early)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Operates at wrong time (late)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Out of sequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Unable to stop operation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Degraded function/malfunction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

VIPPS is a Mock System used for training purposes only
Task 2 Example

<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Operates at wrong time (early)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Operates at wrong time (Late)</td>
</tr>
</tbody>
</table>

Operates at wrong time: Function performs earlier or later than it should have; if too late function could be out of sequence

---

Equipment / Supplies

Maintenance Requirement Cards

Installed System

Operate System

Used System

Maintain System

Repaired System

Operate System

Supplies

Tactics

Installed System

Operate System

Used System

Maintain System

Repaired System

Operate System

Supplies

Tactics

Installed System

Operate System

Used System

Maintain System

Repaired System

Operate System

Supplies

Tactics
<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
<th>Hazard Description</th>
<th>Mishap</th>
<th>Effect(s)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Fails to operate</td>
<td>Failure to perform maintenance results in component failure and unintended release of energy</td>
<td>Personnel, equipment, or the environment exposed to unintended release of energy</td>
<td>Death, injury, equipment/environmental damage</td>
<td>This is really a causal factor that impacts hazards in the operating activity</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Operates at wrong time (early)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Not safety - system is maintained</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Operates at wrong time (late)</td>
<td>Failure to perform maintenance results in component failure and unintended release of energy</td>
<td>Personnel, equipment, or the environment exposed to unintended release of energy</td>
<td>Death, injury, equipment/environmental damage</td>
<td>Same as maintenance failing to happen</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Out of sequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Unable to stop operation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Degraded function/malfunction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Task 2 Example

<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Out of Sequence</td>
</tr>
</tbody>
</table>

Operates out of sequence: Function occurs in the incorrect order; function occurs without receiving the appropriate inputs
<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
<th>Hazard Description</th>
<th>Mishap</th>
<th>Effect(s)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Fails to operate</td>
<td>Failure to perform maintenance results in component failure and unintended release of energy</td>
<td>Personnel, equipment, or the environment exposed to unintended release of energy</td>
<td>Death, injury, equipment/environmental damage</td>
<td>This is really a causal factor that impacts hazards in the operating activity</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Operates at wrong time (early)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Not safety - system is maintained</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Operates at wrong time (late)</td>
<td>Failure to perform maintenance results in component failure and unintended release of energy</td>
<td>Personnel, equipment, or the environment exposed to unintended release of energy</td>
<td>Death, Injury, equipment/environmental damage</td>
<td>Same as maintenance failing to happen</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Out of sequence</td>
<td>Use of incorrect procedures and/or equipment/supplies results in component damage and/or inadvertent release of energy and/or exposure</td>
<td>Personnel, equipment, or the environment exposed to unintended release of energy</td>
<td>Death, injury, equipment/environmental damage</td>
<td>Failure to follow appropriate procedures would be a function occurring without the proper inputs; could include use of wrong tool, failure to use PPE etc.</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Unable to stop operation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Degraded function/malfunction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Task 2 Example

<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Unable to stop operation</td>
</tr>
</tbody>
</table>

**Failure to stop operation:** Current function continues even though it should move on to the next function.
### Task 2 Example

<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
<th>Hazard Description</th>
<th>Mishap</th>
<th>Effect(s)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Maintaining Off</td>
<td>F.5 Maintain System</td>
<td>Fails to operate</td>
<td>Failure to perform maintenance results in component failure and unintended release of energy</td>
<td>Personnel, equipment, or the environment exposed to unintended release of energy</td>
<td>Death, injury, equipment/environmental damage</td>
<td>This is really a causal factor that impacts hazards in the operating activity</td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining Off</td>
<td>F.5 Maintain System</td>
<td>Operates at wrong time (early)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Not safety - system is maintained</td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining Off</td>
<td>F.5 Maintain System</td>
<td>Operates at wrong time (late)</td>
<td>Failure to perform maintenance results in component failure and unintended release of energy</td>
<td>Personnel, equipment, or the environment exposed to unintended release of energy</td>
<td>Death, injury, equipment/environmental damage</td>
<td>Same as maintenance failing to happen</td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining Off</td>
<td>F.5 Maintain System</td>
<td>Out of sequence</td>
<td>Use of incorrect procedures and/or equipment/supplies results in component damage and/or inadvertent release of energy/exposure</td>
<td>Personnel, equipment, or the environment exposed to unintended release of energy</td>
<td>Death, injury, equipment/environmental damage</td>
<td>Failure to follow appropriate procedures would be a function occurring without the proper inputs; could include use of wrong tool, failure to use PPE etc.</td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining Off</td>
<td>F.5 Maintain System</td>
<td>Unable to stop operation</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Unable to perform operations - not safety issue</td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining Off</td>
<td>F.5 Maintain System</td>
<td>Degraded function/malfunction</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NSWCDD-PN-14-00294 is approved for Distribution Statement A: Approved for Public Release; distribution is unlimited.
Task 2 Example

Degraded function/malfunction: Function does not finish or only partially completes (only some outputs are provided); function generates improper output

<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Maintaining Off</td>
<td>F.5 Maintain System</td>
<td>Degraded function/malfunction</td>
<td></td>
</tr>
</tbody>
</table>

- **Installed System**
  - Operate System
  - Supplies
  - Tactics

- **Used System**
  - Operate System
  - Maintain System
  - Equipment / Supplies
  - Maintenance Requirement Cards

- **Repaired System**
  - Maintain System
  - Repaired System
  - Tactics
  - Supplies

- **Used System**
  - Operate System
  - Supplies
  - Tactics

VIPPS is a Mock System used for training purposes only.
### Task 2 Example

<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
<th>Hazard Description</th>
<th>Mishap Description</th>
<th>Effect(s) Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Fails to operate</td>
<td>Failure to perform maintenance results in component failure and unintended release of energy</td>
<td>Personnel, equipment, or the environment exposed to unintended release of energy</td>
<td>Death, injury, equipment/environmental damage</td>
<td>This is really a causal factor that impacts hazards in the operating activity</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Operates at wrong time (early)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Not safety - system is maintained</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Operates at wrong time (late)</td>
<td>Failure to perform maintenance results in component failure and unintended release of energy</td>
<td>Personnel, equipment, or the environment exposed to unintended release of energy</td>
<td>Death, injury, equipment/environmental damage</td>
<td>Same as maintenance failing to happen</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Out of sequence</td>
<td>Use of incorrect procedures and/or equipment/supplies results in component damage and/or inadvertent release of energy/exposure</td>
<td>Personnel, equipment, or the environment exposed to unintended release of energy</td>
<td>Death, injury, equipment/environmental damage</td>
<td>Failure to follow appropriate procedures would be a function occurring without the proper inputs; could include use of wrong tool, failure to use PPE etc.</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Unable to stop operation</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Unable to perform operations - not safety issue</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Degraded function/malfunction</td>
<td>Improper maintenance results in hazardous materials being released during maintenance operations</td>
<td>Personnel, equipment, and/or environment exposed to hazardous materials</td>
<td>Death, injury, equipment/environmental damage</td>
<td>Not following procedures during maintenance operations results in hazardous materials being exposed to the environment and/or personnel</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Maintaining</td>
<td>Off</td>
<td>F.5 Maintain System</td>
<td>Degraded function/malfunction</td>
<td>Failure to perform maintenance results in component failure and unintended release of energy</td>
<td>Personnel, equipment, or the environment exposed to unintended release of energy</td>
<td>Death, injury, equipment/environmental damage</td>
<td>This is really a causal factor that impacts hazards in the operating activity</td>
</tr>
</tbody>
</table>

**NSWCDD-PN-14-00294 is approved for Distribution Statement A:** Approved for Public Release; distribution is unlimited.

VIPPS is a Mock System used for training purposes only.
Task 2 Example

Provide VIPPS Capability
F.0

- Produce System
  F.1
  - Control States and Modes
    F.4.1
    - Initialize
      F.4.1.1
    - Perform BIT
      F.4.1.2
    - Transition State/Mode
      F.4.1.3
    - Log State/Mode Data
      F.4.1.4
  - Log Sensor Data
    F.4.2.5
  - Detect
    F.4.2.1
  - Perform Surveillance
    F.4.2.3
  - Correlate/Maintain Tracks
    F.4.2.4
  - Generate Track
    F.4.2.2

- Install System
  F.3

- Operate System
  F.4
  - Identify
    F.4.3.1
  - Recommend Action
    F.4.3.2
  - Provide Operator SA
    F.4.3.3
  - Log Assessment Data
    F.4.3.4
  - Reassess
    F.4.3.5
  - Log Non-Lethal Event Data
    F.4.4.4
  - Log Lethal Engagement Data
    F.4.5.4
  - Aim/Target
    F.4.5.5

- Maintain System
  F.5
  - Select Zone and Non-Lethal Effector
    F.4.4.1
  - Verify Intent to Warn
    F.4.4.2
  - Activate Non-Lethal Effector
    F.4.4.3
  - Select Zone and Lethal Effector
    F.4.5.1
  - Verify Intent to Engage
    F.4.5.2
  - Activate Lethal Effector
    F.4.5.3
  - Log Non-Lethal Event Data
    F.4.4.4

- Dispose of System
  F.6
  - Lethally Engage
    F.4.5.5

Safety-Significant Function
Session 3 Summary

• Assess functional failures for all system functions to identify hazards
• Functional failures culminating in a hazard are SSFs
SESSION 1

• 0800-0850 What’s an FHA, FHA Tutorial Goals and Objectives, System Architecture and Architecture Framework

SESSION 2

• 0900-0950 Interpreting System Architecture Data

SESSION 3

• 1030-1120 Evaluating Functional Failures

SESSION 4

• 1330-1420 Evaluating Functional Failures (Cont’d), Tracing Functions to Subsystems

SESSION 5

• 1430-1520 Identifying Existing and Recommended Hazard Mitigations

SESSION 6

• 1600-1650 Decomposing Functions to Components, Identifying Risk levels, Determining SwCI and Documenting FHA Results
1. Gather and Interpret System Architecture Data

2. Evaluate Functional Failures for Hazards

3. Identify Safety Significant Subsystems and Interfaces

4. Identify Existing and Recommended Mitigations

5. Decompose SSFs to Components

6. Identify Risk Levels, SwCIs, and Follow-On Actions

7. Document Analysis
REFRESHER

• Fails to operate
  – Function does not happen/perform when given the appropriate input

• Operates at wrong time (early or late)
  – Function performs earlier or later than it should have; if too late function could be out of sequence

• Out of sequence
  – Function occurs in the incorrect order; function occurs without receiving the appropriate inputs

• Failure to stop operation
  – Current function continues even though it should move on to the next function

• Degraded function/malfunction
  – Function does not finish or only partially completes (only some outputs are provided); function generates improper output
Task 2 Exercise

Provide VIPPS Capability

- Produce System F.1
- Handle/Transport System F.2
- Install System F.3
- Operate System F.4
- Maintain System F.5
- Dispose of System F.6

Control States and Modes F.4.1

- Initialize F.4.1.1
- Generate Track F.4.2.2
- Perform Surveillance F.4.2.3
- Correlate/Maintain Tracks F.4.2.4
- Log State/Mode Data F.4.1.4
- Log Sensor Data F.4.2.5

Sense F.4.2

- Detect F.4.2.1
- Perform BIT F.4.1.2
- Perform Surveillance F.4.2.3
- Log Sensor Data F.4.2.5

Evaluate F.4.3

- Identify F.4.3.1
- Recommend Action F.4.3.2
- Provide Operator SA F.4.3.3
- Log Assessment Data F.4.3.4
- Reassess F.4.3.5

Warn F.4.4

- Select Zone and Non-Lethal Effector F.4.4.1
- Verify Intent to Warn F.4.4.2
- Identify F.4.3.1
- Provide Operator SA F.4.3.3
- Log Assessment Data F.4.3.4
- Reassess F.4.3.5

Lethally Engage F.4.5

- Select Zone and Lethal Effector F.4.5.1
- Verify Intent to Engage F.4.5.2
- Activate Lethal Effector F.4.5.3
- Log Lethal Engagement Data F.4.5.4
- Aim/Target F.4.5.5

Safety-Significant Function

VIPPS is a Mock System used for training purposes only

NSWCDD-PN-14-00294 is approved for Distribution Statement A: Approved for Public Release; distribution is unlimited.
Ready Tactical Functional Thread

Current System State/Mode

SAFE

Mode Change Request READY TACTICAL

Detection Location

Generate Track

Track Location

Correlate/ Maintain Tracks

Track Picture

Identify

Search Params

Perform Surveillance

“READY TACTICAL”

Transition State/Mode

Recommend Action

Lethal/Non-Lethal Engagement Order (next slide)

Detection

ID’d Track

NSWCDD-PN-14-00294 is approved for Distribution Statement A: Approved for Public Release; distribution is unlimited.
Ready Tactical Functional Thread

Non-Lethal Engagement Order → Select Zone and Non-Lethal Effector → Verify Intent to Warn → Activate Non-Lethal Effector

Recommend Action → Non-Lethal Engagement Plan → Authorized Non-Lethal Engagement Plan → Non-Lethal Energy

Lethal Engagement Order → Select Zone and Lethal Effector → Aim/Target → Visual Target Confirmation → Authorize Lethal Effector

Lethal Engagement Order → Verify Intent to Engage → Activate Lethal Effector → Lethal Energy
# Task 2 Exercise

<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
<th>Hazard Description</th>
<th>Mishap</th>
<th>Effect(s)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Operating</td>
<td>Ready Tactical</td>
<td>F.4.1.3 Transition State/Mode</td>
<td>Fails to operate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Operating</td>
<td>Ready Tactical</td>
<td>F.4.1.3 Transition State/Mode</td>
<td>Operates at wrong time (late)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Operating</td>
<td>Ready Tactical</td>
<td>F.4.1.3 Transition State/Mode</td>
<td>Out of sequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Operating</td>
<td>Ready Tactical</td>
<td>F.4.1.3 Transition State/Mode</td>
<td>Unable to stop operation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Operating</td>
<td>Ready Tactical</td>
<td>F.4.1.3 Transition State/Mode</td>
<td>Degraded function/malfunction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

VIPPS is a Mock System used for training purposes only.
“Transition State/Mode”
Ready Tactical to Ready Training Functional Thread

Current System State/Mode

Mode Change Request

Training Functional Thread ...

Transition State/Mode

Perform Surveillance

Detect

Search Params

Generate Track

Track Location

Correlate/ Maintain Tracks

Track Picture

Identify

ID’d Track

Recommend Action

Lethal/Non-Lethal Engagement Order (next slide)

Detection Location

Detect

Ready Tactical

Ready Training

Slide 1 of 2

NSWCDD-PN-14-00294 is approved for Distribution Statement A: Approved for Public Release; distribution is unlimited.

VIPPS is a Mock System used for training purposes only
“Transition State/Mode”

Ready Tactical to Ready Training Functional Thread

Non-Lethal Engagement Order

Select Zone and Non-Lethal Effector

Non-Lethal Engagement Plan

Verify Intent to Warn

Authorized Non-Lethal Engagement Plan

Activate Non-Lethal Effector

Non-Lethal Energy

Recommend Action

Select Zone and Lethal Effector

Lethal Engagement Order

Select Zone and Lethal Effector

Lethal Engagement Plan

Aim/Target

Visual Target Confirmation

Authorized Lethal Engagement Plan

Activate Lethal Effector

Lethal Energy

NSWCDD-PN-14-00294 is approved for Distribution Statement A: Approved for Public Release; distribution is unlimited.

VIPPS is a Mock System used for training purposes only
## Task 2 Exercise

<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
<th>Hazard Description</th>
<th>Mishap</th>
<th>Effect(s)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Operating</td>
<td>Ready Tactical</td>
<td>F.4.1.3 Transition State/Mode</td>
<td>Fails to operate</td>
<td>System remains in tactical mode when transition is attempted, causing the operator to perform training operations with the system in tactical mode and an unintended release of energy</td>
<td>Personnel, equipment, and the environment exposed to unintended release of energy</td>
<td>Death, injury, equipment damage, environmental damage</td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Operating</td>
<td>Ready Tactical</td>
<td>F.4.1.3 Transition State/Mode</td>
<td>Operates at wrong time (late)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Operating</td>
<td>Ready Tactical</td>
<td>F.4.1.3 Transition State/Mode</td>
<td>Out of sequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Operating</td>
<td>Ready Tactical</td>
<td>F.4.1.3 Transition State/Mode</td>
<td>Unable to stop operation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Operating</td>
<td>Ready Tactical</td>
<td>F.4.1.3 Transition State/Mode</td>
<td>Degraded function/ malfunction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Task 2 Exercise Instructions

• Task 2: Evaluate functional failures to identify hazards
  – Task 2.b: Assess each functional failure for one or more hazards
    • Perform initial assessment of every row in FHA worksheet
  – Task 2.c: Document hazard description, mishap(s), and effect(s)
    • Refine and capture initial assessment in appropriate fields of FHA worksheet
Task 2 Exercise Instructions

Session 4 – Task 2

<table>
<thead>
<tr>
<th>Activity</th>
<th>Function of Failure</th>
<th>Hazard Description</th>
<th>Misstep</th>
<th>Effect(s)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transition State/Mode</td>
<td>System remains in tactical mode when transition is attempted, causing the operator to perform training operations with the system in tactical mode and an unintended release of energy</td>
<td>Personnel, environment exposed to unintended release of energy</td>
<td>Death, injury, equipment damage, environmental damage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transition State/Mode</td>
<td>Unable to stop operation</td>
<td>Operator training interruption</td>
<td>Operator training interruption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transition State/Mode</td>
<td>Degraded function/ Malfunction</td>
<td>Operator training interruption</td>
<td>Operator training interruption</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

VIPPS is a Mock System used for training purposes only.
Discussion of Task 2 Exercise Results
## Task 2 Exercise Answer Key

<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Function Failure</th>
<th>Hazard Description</th>
<th>Mishap</th>
<th>Effect(s)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Operating</td>
<td>Ready Tactical</td>
<td>F.4.1.3 Transition State/Mode</td>
<td>Fails to operate</td>
<td>System remains in tactical mode when transition is attempted, causing the operator to perform training operations with the system in tactical mode and an unintended release of energy</td>
<td>Personnel, Equipment and the environment exposed to unintended release of energy</td>
<td>Death, Injury, Equipment Damage, Environmental Damage</td>
<td></td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Operating</td>
<td>Ready Tactical</td>
<td>F.4.1.3 Transition State/Mode</td>
<td>Operates at wrong time (late)</td>
<td>System remains in tactical mode when transition is attempted, causing the operator to perform training operations with the system in tactical mode and an unintended release of energy</td>
<td>Personnel, Equipment and the environment exposed to unintended release of energy</td>
<td>Death, Injury, Equipment Damage, environmental damage</td>
<td>Early State/Mode transitions are not deemed to have safety implications</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Operating</td>
<td>Ready Tactical</td>
<td>F.4.1.3 Transition State/Mode</td>
<td>Out of sequence</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>System mode transition out of tactical during a tactical engagement (without request for mode transition) would impact the operational effectiveness of the system, but not produce a safety concern.</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Operating</td>
<td>Ready Tactical</td>
<td>F.4.1.3 Transition State/Mode</td>
<td>Unable to stop operation</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>System state becomes unstable, system mode is unknown, and system is unable to perform additional functions. There is no clear hazard associated with this function failing to stop operating.</td>
</tr>
<tr>
<td>Operation and Support</td>
<td>Operating</td>
<td>Ready Tactical</td>
<td>F.4.1.3 Transition State/Mode</td>
<td>Degraded function/ Malfunction</td>
<td>System partially transitions to training, maintaining tactical control of components while allowing the conduct of training operations and subsequent unintended release of energy</td>
<td>Personnel, Equipment and the environment exposed to unintended release of energy</td>
<td>Death, Injury, Equipment Damage, environmental damage</td>
<td></td>
</tr>
</tbody>
</table>
NSWCDD-PN-14-00294 is approved for Distribution Statement A: Approved for Public Release; distribution is unlimited.

VIPPSS is a Mock System used for training purposes only.
Identify Safety Significant Functions

Provide VIPPS Capability
F.0

- Produce System
  F.1
  - Handle/Transport System
    F.2
  - Install System
    F.3
  - Operate System
    F.4
  - Maintain System
    F.5
  - Dispose of System
    F.6

  - Control States and Modes
    F.4.1
    - Initialize
      F.4.1.1
    - Perform BIT
      F.4.1.2
    - Transition State/Mode
      F.4.1.3
    - Log State/Mode Data
      F.4.1.4

  - Sense
    F.4.2
    - Detect
      F.4.2.1
    - Generate Track
      F.4.2.2
    - Perform Surveillance
      F.4.2.3
    - Correlate/Maintain Tracks
      F.4.2.4
    - Log Sensor Data
      F.4.2.5

  - Evaluate
    F.4.3
    - Identify
      F.4.3.1
    - Recommend Action
      F.4.3.2
    - Provide Operator SA
      F.4.3.3
    - Log Assessment Data
      F.4.3.4

  - Warn
    F.4.4
    - Select Zone and Non-Lethal Effector
      F.4.4.1
    - Verify Intent to Warn
      F.4.4.2
    - Activate Non-Lethal Effector
      F.4.4.3
    - Log Non-Lethal Event Data
      F.4.4.4
    - Aim/Target
      F.4.5.5

  - Lethally Engage
    F.4.5
    - Select Zone and Lethal Effector
      F.4.5.1
    - Verify Intent to Engage
      F.4.5.2
    - Activate Lethal Effector
      F.4.5.3
    - Log Lethal Engagement Data
      F.4.5.4
FHA Process Flow

1. Gather and Interpret System Architecture Data
2. Evaluate Functional Failures for Hazards
3. Identify Safety Significant Subsystems and Interfaces
4. Identify Existing and Recommended Mitigations
5. Decompose SSFs to Components
6. Identify Risk Levels, SwClis, and Follow-On Actions
7. Document Analysis
Task 3 Instructions

• Task 3: Identify Safety Significant Items and Interfaces
  – Use VIPPS SV-5 to identify subsystems associated with functional hazards
  – Document allocated items in “System Item(s)” field of FHA worksheet
VIPPS Physical Architecture

VIPPS is a Mock System used for training purposes only.

Assumptions

Interior Equipment

Exterior Equipment

VIPPS Physical Architecture Diagram:
- Battery Backup
- Gun Support System
  - AMMO Supply
  - Fire Control Interface
  - Optics Suite
- High Intensity Spotlight
- Hailer
- Data Recording Device
- Command and Control (C2) Computer
  - Computer
  - Operator Console
- Sensor/Motion Detect Subsystem
- Assumptions
- Power
- Data
<table>
<thead>
<tr>
<th>View</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SV-1 Systems Interface Description</td>
<td>The identification of system, system items, and their interconnections.</td>
</tr>
<tr>
<td>SV-3 Systems-Systems Matrix</td>
<td>The relationship among systems in a given Architecture Description. It can be designed to show relationships of interest.</td>
</tr>
<tr>
<td>SV-4 Systems Functionality Description</td>
<td>The functions (activities) performed by systems and the system data flows among system functions (activities).</td>
</tr>
<tr>
<td><strong>SV-5a Operational Activity to Systems Function Traceability Matrix</strong></td>
<td>A mapping of system functions back to operational activities.</td>
</tr>
<tr>
<td><strong>SV-5b Operational Activity to Systems Traceability Matrix</strong></td>
<td>A mapping of systems back to capabilities or operational activities.</td>
</tr>
<tr>
<td>SV-6 Systems Resource Flow Matrix</td>
<td>Provides details of system resource flow elements being exchanged between systems and the attributes of that exchange.</td>
</tr>
<tr>
<td>SV-7 Systems Measures Matrix</td>
<td>The measures (metrics) of Systems Model elements of the appropriate timeframe(s).</td>
</tr>
<tr>
<td>SV-8 Systems Evolution Description</td>
<td>The planned incremental steps toward migrating a suite of systems to a more efficient suite, or toward evolving a current system to a future implementation.</td>
</tr>
<tr>
<td>SV-9 Systems Technology and Skills Forecast</td>
<td>The emerging technologies, software/hardware products, and skills that are expected to be available in a given set of time frames and that will affect future system development.</td>
</tr>
<tr>
<td>SV-10a Systems Rules Model</td>
<td>One of three models used to describe system functionality. It identifies constraints that are imposed on systems functionality due to some aspect of system design or implementation.</td>
</tr>
<tr>
<td>SV-10b Systems State Transition Description</td>
<td>One of three models used to describe system functionality. It identifies responses of systems to events.</td>
</tr>
<tr>
<td>SV-10c Systems Event-Trace Description</td>
<td>One of three models used to describe system functionality. It identifies system-specific refinements of critical sequences of events described in the Operational Viewpoint.</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td>F.4.1. Control States and Modes</td>
<td>X</td>
</tr>
<tr>
<td>F.4.1.1. Initialize</td>
<td></td>
</tr>
<tr>
<td>F.4.1.2. Perform BIT</td>
<td></td>
</tr>
<tr>
<td>F.4.1.3. Transition State/Mode</td>
<td></td>
</tr>
<tr>
<td>F.4.1.4. Log State/Mode Data</td>
<td></td>
</tr>
<tr>
<td>F.4.2. Sense</td>
<td>X</td>
</tr>
<tr>
<td>F.4.3. Evaluate</td>
<td></td>
</tr>
<tr>
<td>F.4.3.1. Identify</td>
<td></td>
</tr>
<tr>
<td>F.4.3.2. Recommend Action</td>
<td></td>
</tr>
<tr>
<td>F.4.3.3. Provide Operator SA</td>
<td></td>
</tr>
<tr>
<td>F.4.3.4. Log Data Assessment</td>
<td></td>
</tr>
<tr>
<td>F.4.3.5. Reassess</td>
<td>X</td>
</tr>
<tr>
<td>F.4.4. Warn</td>
<td>X</td>
</tr>
<tr>
<td>F.4.4.1. Select Zone and Non-Lethal Effector</td>
<td></td>
</tr>
<tr>
<td>F.4.4.2. Verify Intent to Warn</td>
<td></td>
</tr>
<tr>
<td>F.4.4.3. Activate Non-Lethal Effector</td>
<td>X</td>
</tr>
<tr>
<td>F.4.4.4. Log Non-Lethal Event Data</td>
<td>X</td>
</tr>
<tr>
<td>F.4.5. Lethally Engage</td>
<td>X</td>
</tr>
</tbody>
</table>

Note: VIPPS is a Mock System used for training purposes only.
### Task 3 Example

<table>
<thead>
<tr>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
<th>Hazard Description</th>
<th>Mishap</th>
<th>Effect(s)</th>
<th>System Item(s)</th>
<th>Existing Mitigations</th>
<th>Recommended Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ready Tactical</td>
<td>F.4.1.3 Transition State/Mode</td>
<td>Fails to operate</td>
<td>System remains in tactical mode when transition is attempted, causing the operator to perform training operations with the system in tactical mode and an unintended release of energy</td>
<td>Personnel and equipment exposed to unintended release of energy</td>
<td>Death, injury, equipment damage</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

VIPPS is a Mock System used for training purposes only.
### Task 3 Example - VIPPS SV-5

<table>
<thead>
<tr>
<th>Task 3 Example</th>
<th>Lethal Effectors</th>
<th>Sensor Subsystem</th>
<th>C2 Computer</th>
<th>UWD (Light)</th>
<th>Operator Console</th>
<th>Operator</th>
<th>UWD (Hailer)</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.4. Operate</td>
<td>X X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.1. Control States and Modes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.1.1. Initialize</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.1.2. Perform BIT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>F.4.1.3. Transition State/Mode</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.1.4. Log State/Mode Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.2. Sense</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.3. Evaluate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.3.1. Identify</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.3.2. Recommend Action</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.3.3. Provide Operator SA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.3.4. Log Data Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.3.5. Reassess</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.4. Warn</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.4.1. Select Zone and Non-Lethal Effector</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.4.2. Verify Intent to Warn</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.4.3. Activate Non-Lethal Effector</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.4.4. Log Non-Lethal Event Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4.5. Lethally Engage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**
- VIPPS is a Mock System used for training purposes only.
- Approved for Public Release; distribution is unlimited.

**References:**
- NSWCDD-PN-14-00294
### Task 3 Example (Cont’d)

<table>
<thead>
<tr>
<th>State/Mode</th>
<th>Function</th>
<th>Functiona l Failure</th>
<th>Hazard Description</th>
<th>Mishap</th>
<th>Effect(s)</th>
<th>System Item(s)</th>
<th>Existing Mitigations</th>
<th>Recommended Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ready Tactical Transition State/Mode</td>
<td>F.4.1.3</td>
<td>Fails to operate</td>
<td>System remains in tactical mode when transition is attempted, causing the operator to perform training operations with the system in tactical mode and an unintended release of energy</td>
<td>Personnel and equipment exposed to unintended release of energy</td>
<td>Death, injury, equipment damage</td>
<td>C2, Operator Console, Operator</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VIPPS Physical Architecture

Battery Backup

GSS
- AMMO Supply
- Fire Control Interface
- Optics Suite

High Intensity Spotlight

Hailer

Data Recording Device

PWR

Operator Console

Command and Control (C2) Computer

Power

Data

Power

Data

Power

Data

Power

Data

Power

Data

Power

Data

Power

Data

Power

Data

Power

Data

Sensor/Motion Detect Subsystem

Assumptions

Interior Equipment

Exterior Equipment
Session 4 Summary

• Evaluate failures of all system functions to identify hazards
• Those functions whose failure(s) constitute a hazard are SSFs
• Consider the sequence of events that may influence an energy-release function
• Trace safety significant functions to subsystems
FHA Tutorial Agenda

SESSION 1
• 0800-0850  What’s an FHA, FHA Tutorial Goals and Objectives, System Architecture and Architecture Framework

SESSION 2
• 0900-0950  Interpreting System Architecture Data

SESSION 3
• 1030-1120  Evaluating Functional Failures

SESSION 4
• 1330-1420  Evaluating Functional Failures (Cont’d), Tracing Functions to Subsystems

SESSION 5
• 1430-1520  Identifying Existing and Recommended Hazard Mitigations

SESSION 6
• 1600-1650  Decomposing Functions to Components, Identifying Risk levels, Determining SwCl and Documenting FHA Results
FHA Process Flow

1. Gather and Interpret System Architecture Data
2. Evaluate Functional Failures for Hazards
3. Identify Safety Significant Subsystems and Interfaces
4. Identify Existing and Recommended Mitigations
5. Decompose SSFs to Components
6. Identify Risk Levels, SwCIs, and Follow-On Actions
7. Document Analysis
Task 4 Instructions

- **Task 4: Identify existing and recommended mitigations**
  - Evaluate system design and hazard information to identify existing mitigations and document in “Existing Mitigations” field
    - Detection
    - Tolerance
    - Isolation
    - Annunciation
    - Recovery
  - Provide recommendations for additional functional hazard mitigations in “Recommended Mitigations” field
Existing Mitigations

- Existing Mitigations
  - Identified in system artifacts under development
  - Used to identify gaps in functional mitigations
  - Contribute to Initial Mishap Risk assessment
  - Consider the following types:

  - **Detection**
    - System can detect fault conditions and alert operator or take other action to preclude propagation into a mishap (may initiate further mitigation)

  - **Tolerance**
    - System can tolerate a fault condition to prevent propagation into a mishap

  - **Isolation**
    - System can detect and isolate a fault condition to prevent propagation into a mishap

  - **Recovery**
    - System can recover from a fault condition through one or more mechanism

  - **Annunciation**
    - Visual and/or audio cuing to system operator of a faulty condition. System relies on operator intervention to preclude propagation into a mishap.
Recommended Mitigations

• If insufficient existing mitigations, try to eliminate hazards through design selection
• If elimination is not feasible, reduce the severity and/or the probability of the mishap by recommending mitigations
• Consider system safety design order of precedence
  – Design alteration (*Tolerance, Detection, Isolation, Recovery*)
  – Incorporate engineered features or devices (*Detection, Isolation*)
  – Provide warning devices (*Detection, Annunciation*)
  – Incorporate signage, procedures, training, and personal protection equipment (PPE) (*Annunciation, Recovery, Isolation, Tolerance*)
• Provided to developer for inclusion in design

Opportunity for Safety to Directly Influence System Design and Eliminate/Reduce Risk
## Task 4 Example

<table>
<thead>
<tr>
<th>State/Mode</th>
<th>Function</th>
<th>Functiona Failure</th>
<th>Hazard Description</th>
<th>Mishap</th>
<th>Effect(s)</th>
<th>System Item(s)</th>
<th>Existing Mitigations</th>
<th>Recommended Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ready</td>
<td>F.4.1.3</td>
<td>Transition State/Mode</td>
<td>Fails to operate System remains in tactical mode when transition is attempted, causing the operator to perform training operations with the system in tactical mode and an unintended release of energy</td>
<td>Personnel and equipment exposed to unintended release of energy</td>
<td>Death, injury, equipment damage</td>
<td>C2, Operator Console, Operator</td>
<td>Detection</td>
<td>Tolerance</td>
</tr>
<tr>
<td>Tactical</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Isolation</td>
<td>Annunciation</td>
</tr>
</tbody>
</table>

VIPPS is a Mock System used for training purposes only
4.1  **System States and Modes**

For the purposes of this specification, the following definitions apply:

- System state - A physical or operational condition that characterizes the status of the system at a point in time.

  [4.1.a] All VIPPS operating stations shall provide a clear and unambiguous indication of the current VIPPS State.
### Task 4 Example (Cont’d)

<table>
<thead>
<tr>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
<th>Hazard Description</th>
<th>Mishap</th>
<th>Effect(s)</th>
<th>System Item(s)</th>
<th>Existing Mitigations</th>
<th>Recommended Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ready</td>
<td>F.4.1.3</td>
<td>Fails to operate</td>
<td>System remains in</td>
<td>Personnel and equipment exposed to unintended release of energy</td>
<td>Death, injury, equipment damage</td>
<td>C2, Operator Console, Operator</td>
<td>All VIPPS operating stations shall provide a clear and unambiguous indication of the current VIPPS State (SSS 4.1.a) (detection, annunciation)</td>
<td>• Provide hardware-based power control (recovery) • Audio and visual mode transition failure alert (annunciation)</td>
</tr>
</tbody>
</table>

#### Detection & Tolerance
- **Isolation**
- **Annunciation**
- **Recovery**
Task 4 Exercise Instructions

- Task 4: Identify existing and recommended mitigations
  - Evaluate system design and hazard information to identify existing mitigations and document in “Existing Mitigations” field
    - Detection
    - Tolerance
    - Isolation
    - Annunciation
    - Recovery
  - Provide recommendations for additional functional hazard mitigations in “Recommended Mitigations” field
Discussion of Task 4 Exercise Results
<table>
<thead>
<tr>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
<th>Hazard Description</th>
<th>Mishap</th>
<th>Effect(s)</th>
<th>System Item(s)</th>
<th>Existing Mitigations</th>
<th>Recommended Mitigations</th>
</tr>
</thead>
</table>
| Ready     | F.4.1.3  | Fails to operate  | System remains in tactical mode when transition is attempted, causing the operator to perform training operations with the system in tactical mode and an unintended release of energy | Personnel, Equipment and the environment exposed to unintended release of energy | Death, Injury, Equipment Damage, Environmental Damage | C2, Operator Console, Operator | • System state is displayed to operator (SSS 4.1.a) (detection) | • Provide hardware-based power control (recovery)  
• Alert the operator to failed mode transitions (annunciation) |
| Tactical  | Transition|                    |                                                                                   |                                                                        |                               |                        |                                                            |                                                             |
| Ready     | F.4.1.3  | Degraded function/ Malfunction | System partially transitions to training, maintaining tactical control of components while allowing the conduct of training operations and subsequent unintended release of energy | Personnel, Equipment and the environment exposed to unintended release of energy | Death, Injury, Equipment Damage, Environmental damage | C2, Operator Console, Operator | • System must transition to safe state from ready tactical (SSS 4.1.2.b)  
• The system shall exist in only one state at any point in time (SSS 4.1.1.b)  
• VIPPS shall only allow operators to control sensors and weapons that are in the same State of operation as the operator console (i.e., Safe, Ready Test, Ready Tactical, or Ready Training) (SSS 4.1.1.1.c) | • Monitor for mixed-mode conditions (detection)  
• Provide alert for mode mismatch conditions (annunciation)  
• Transition to SAFE State if mixed states/modes are detected (recovery)  
• System shall prevent communications with lethal and non-lethal subsystems upon detection of a mixed-mode condition (isolation) |
| Tactical  | Transition|                    |                                                                                   |                                                                        |                               |                        |                                                            |                                                             |
Session 5 Summary

• Existing Mitigation Sources:
  – Specification development
  – Operational concepts
  – Standards, Guidance
  – Lessons learned

• Recommended Mitigation Sources:
  – Experience/kgnowledge of similar systems
  – System Safety and System Engineering experts
  – Other Subject Matter Experts

Significant Opportunity for Safety to Impact System Design
SESSION 1

• 0800-0850  What’s an FHA, FHA Tutorial Goals and Objectives, System Architecture and Architecture Framework

SESSION 2

• 0900-0950  Interpreting System Architecture Data

SESSION 3

• 1030-1120  Evaluating Functional Failures

SESSION 4

• 1330-1420  Evaluating Functional Failures (Cont’d), Tracing Functions to Subsystems

SESSION 5

• 1430-1520  Identifying Existing and Recommended Hazard Mitigations

SESSION 6

• 1600-1650  Decomposing Functions to Components, Identifying Risk levels, Determining SwCI and Documenting FHA Results
FHA Process Flow

1. Gather and Interpret System Architecture Data
2. Evaluate Functional Failures for Hazards
3. Identify Safety Significant Subsystems and Interfaces
4. Identify Existing and Recommended Mitigations
5. Decompose SSFs to Components
6. Identify Risk Levels, SwCIs, and Follow-On Actions
7. Document Analysis
Decompose SSFs to Components

Safety-Significant Function

VIPPS is a Mock System used for training purposes only.
FHA Process Flow Step 5

• Task 5.a: Evaluate component-level functional failures
  – Describe functional failures in terms of function under assessment in “Functional Failure” field
  – Use updated system architecture artifacts to assess potential safety impact of each functional failure and document safety rationale in Comments field
  – If failure considered safety, fill in Hazard Description, Mishap, and Effect(s) fields
  – If failure not considered safety, enter “N/A” in Hazard Description, Mishap, and Effect(s) fields

• Task 5.b: Identify safety significant components and interfaces
  – Use updated system architecture artifacts to identify components and interfaces associated with functional failures assessed as safety
  – Enter associated components and interfaces in System Item field for those functional failures assessed as safety

• Task 5.c: Identify existing and recommended mitigations at subsystem and component level design
  – Use existing system artifacts to identify existing mitigations
  – Consider functional mitigation types to recommend additional mitigations
Functional Decomposition

Transition State/Mode

Perform Surveillance

Detect

Search Params

Generate Track

Correlate/Maintain Tracks

Identify

Track Location

ID'd Track

Lethal/Non-Lethal Engagement Order (next slide)

Recommend Action

Select Zone and Non-Lethal Effector

Non-Lethal Engagement Plan

Verify Intent to Warn

Activate Non-Lethal Effector

Authorized Non-Lethal Engagement Plan

Non-Lethal Energy

Recommend Action

Select Zone and Lethal Effector

Lethal Engagement Plan

Aim/Target

Activate Lethal Effector

Authorized Lethal Engagement Plan

Lethal Energy

VIPPS is a Mock System used for training purposes only

NSWCDD-PN-14-00294 is approved for Distribution Statement A:
Approved for Public Release; distribution is unlimited.
F.4.1.3 Transition State/Mode

Mode Change Request

Receive Mode Transition Request

Mode Change Order

Mode Change Authorization

Evaluate Mode Transition Request

Mode Change Prohibition

System Status

READY TRAINING

OR

Transition Mode

Current State/Mode

Report System Mode

State/Mode Change

“READY TACTICAL”

State/Mode Display

VIPPS is a Mock System used for training purposes only

NSWCDD-PN-14-00294 is approved for Distribution Statement A: Approved for Public Release; distribution is unlimited.
### F.4.1.3 Subfunction Descriptions

<table>
<thead>
<tr>
<th>Function</th>
<th>Function Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.4.1.3.1</td>
<td>Receive Mode Transition Request</td>
<td>C2 receives operator request to transition the system to a particular system mode</td>
</tr>
<tr>
<td>F.4.1.3.2</td>
<td>Evaluate Mode Transition Request</td>
<td>C2 evaluates the current system status (i.e. active threats, active threat engagement) for readiness to transition to the requested system mode</td>
</tr>
<tr>
<td>F.4.1.3.3</td>
<td>Transition Mode</td>
<td>If allowed, C2 transitions the entire system to the requested mode</td>
</tr>
<tr>
<td>F.4.1.3.4</td>
<td>Maintain System Mode</td>
<td>If the transition is disallowed, C2 rejects the requested mode transition and provides a fault code to the operator console</td>
</tr>
<tr>
<td>F.4.1.3.5</td>
<td>Report System Mode</td>
<td>Upon completion of acting (or not acting) on the requested mode transition, C2 reports the current system mode to the operator console for display</td>
</tr>
</tbody>
</table>
## FHA Task 5.a Example

<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Hazard Description</th>
<th>Mishap</th>
<th>Effect(s)</th>
<th>System Item(s)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Operating Ready Training</td>
<td>F.4.1.3.3 Transition Mode</td>
<td>Fails to operate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Diagram:

- **Mode Change Request**
- **Receive Mode Transition Request**
- **Mode Change Order**
- **Evaluate Mode Transition Request**
- **System Status READY TRAINING**
- **Mode Change Authorization**
- **OR**
- **Transition Mode**
- **Maintain System Mode**
- **Report System Mode**
- **Current State/Mode**
- **Current State/Mode**
- **State/Mode Display**

**F.4.1.3.3 Transition Mode**

If allowed, C2 transitions the entire system to the requested mode.

"READY TACTICAL"
FHA Task 5.a Example (Cont’d)

<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
<th>Hazard Description</th>
<th>Mishap</th>
<th>Effect(s)</th>
<th>System Item(s)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Operating Ready Training</td>
<td>F.4.1.3.3 Transition Mode</td>
<td>Degraded function/malfunction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

F.4.1.3.3 Transition Mode If allowed, C2 transitions the entire system to the requested mode

```
Mode Change Request
REEADY TACTICAL
```

```
Receive Mode Transition Request
```

```
Mode Change Authorisation
```

```
Evaluate Mode Transition Request
```

```
System Status READY TRAINING
```

```
Transition Mode
```

```
Report System Mode
```

```
Maintain System Mode
```

```
Mode Change Prohibition
```

```
Current State/Mode
```

```
State/Mode Display
```

```
“READY TACTICAL” State/Mode Change
```

```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
FHA Process Flow Task 5b

• Task 5.a: Evaluate component-level functional failures
  – Describe functional failures in terms of function under assessment in “Functional Failure” field
  – Use updated system architecture artifacts to assess potential safety impact of each functional failure and document safety rationale in Comments field
  – If failure considered safety, fill in Hazard Description, Mishap, and Effect(s) fields
  – If failure not considered safety, enter “N/A” in Hazard Description, Mishap, and Effect(s) fields

• Task 5.b: Identify safety significant components and interfaces
  – Use updated system architecture artifacts to identify components and interfaces associated with functional failures assessed as safety
  – Enter associated components and interfaces in System Item field for those functional failures assessed as safety

• Task 5.c: Identify existing and recommended mitigations at subsystem and component level design
  – Use existing system artifacts to identify existing mitigations
  – Consider functional mitigation types to recommend additional mitigations
C2 Software Architecture

- Human Computer Interface (HCI)
  - Sensor Controller (SC)
  - Track Manager (TM)
  - Energy Controller (EC)
- Common Services (CS)
- Operating Environment (OE)
### C2 Function/Item Matrix

<table>
<thead>
<tr>
<th>C2 Function</th>
<th>C2 Software Component</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OE</td>
</tr>
<tr>
<td>F.4.1.3.1</td>
<td></td>
</tr>
<tr>
<td>Receive Mode Transition Request</td>
<td></td>
</tr>
<tr>
<td>F.4.1.3.2</td>
<td></td>
</tr>
<tr>
<td>Evaluate Mode Transition Request</td>
<td></td>
</tr>
<tr>
<td>F.4.1.3.3</td>
<td></td>
</tr>
<tr>
<td>Transition Mode</td>
<td></td>
</tr>
<tr>
<td>F.4.1.3.4</td>
<td></td>
</tr>
<tr>
<td>Maintain System Mode</td>
<td></td>
</tr>
<tr>
<td>F.4.1.3.5</td>
<td></td>
</tr>
<tr>
<td>Report System Mode</td>
<td></td>
</tr>
</tbody>
</table>

**OE** Operating Environment  
**CS** Common Services  
**SC** Sensor Controller  
**TM** Track Manager  
**EC** Energy Controller  
**HCI** Human Computer Interface
## FHA Task 5.b Example

<table>
<thead>
<tr>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
<th>Hazard Description</th>
<th>Mishap</th>
<th>Effect(s)</th>
<th>System Item(s)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation and Support</td>
<td>Operating</td>
<td>Ready Training</td>
<td>F.4.1.3.3 Transition Mode</td>
<td>Degraded function/malfunction</td>
<td>C2 performs partial mode transition, leaving some applications in Training while some have transitioned to Tactical. Mixed mode operations may contribute to the operator tactically engaging a training track, which may be a friendly and result in unintentional death or injury.</td>
<td>Engagement of friendly</td>
<td>Death, injury, equipment damage</td>
<td></td>
<td>Partial transition of system out of ready training</td>
</tr>
</tbody>
</table>

### C2 Function vs C2 Software Component

<table>
<thead>
<tr>
<th>C2 Function</th>
<th>C2 Software Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.4.1.3.1</td>
<td><strong>OE</strong></td>
</tr>
<tr>
<td>Receive Mode Transition Request</td>
<td>X</td>
</tr>
<tr>
<td>Evaluate Mode Transition Request</td>
<td></td>
</tr>
<tr>
<td>Transition Mode</td>
<td>X</td>
</tr>
<tr>
<td>Maintain System Mode</td>
<td></td>
</tr>
<tr>
<td>Report System Mode</td>
<td></td>
</tr>
</tbody>
</table>
FHA Process Flow Step 5c

- **Task 5.a: Evaluate component-level functional failures**
  - Describe functional failures in terms of function under assessment in “Functional Failure” field
  - Use updated system architecture artifacts to assess potential safety impact of each functional failure and document safety rationale in Comments field
  - If failure considered safety, fill in Hazard Description, Mishap, and Effect(s) fields
  - If failure not considered safety, enter “N/A” in Hazard Description, Mishap, and Effect(s) fields

- **Task 5.b: Identify safety significant components and interfaces**
  - Use updated system architecture artifacts to identify components and interfaces associated with functional failures assessed as safety
  - Enter associated components and interfaces in System Item field for those functional failures assessed as safety

- **Task 5.c: Identify existing and recommended mitigations at subsystem and component level design**
  - Use existing system artifacts to identify existing mitigations
  - Consider functional mitigation types to recommend additional mitigations
FHA Process Flow

1. Gather and Interpret System Architecture Data
2. Evaluate Functional Failures for Hazards
3. Identify Safety Significant Subsystems and Interfaces
4. Identify Existing and Recommended Mitigations
5. Decompose SSFs to Components
6. Identify Risk Levels, SwCIs, and Follow-On Actions
7. Document Analysis
FHA Task 6

• For all identified functional hazards, assess for:
  – Mishap severity
  – Mishap probability of occurrence
• For safety functions implemented by software:
  – Derive SwCI
  – Execute appropriate Level of Rigor
    • Covered in the Software Safety Analysis Tutorial
  – Determine risk level of identified causal factors
• Identify required follow-on actions
FHA Task 7

• Reference or provide system architecture
• Discuss FHA methodology
• Summarize results and recommendations
  – Provide detailed results and recommendations in FHA Worksheet as appendix to report
## FHA Worksheet

<table>
<thead>
<tr>
<th>Hazard ID #</th>
<th>Life-Cycle Phase</th>
<th>Activity</th>
<th>State/Mode</th>
<th>Function</th>
<th>Functional Failure</th>
<th>Hazard Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**System Item(s)**

- **Causal Factor Description**
- **Mishap(s)**
- **Effect(s)**
- **Existing Mitigations**
- **Software Control Category**
- **Initial MRI**

**Software Criticality Index**

- **Target MRI**
- **Causal Factor Risk Level**
- **Recommended Mitigations**
- **Comments**
- **Follow-On Actions**

**NSWCDD-PN-14-00294** is approved for Distribution Statement A: Approved for Public Release; distribution is unlimited.
FHA Tutorial Summary

• Communicate with SE in the same language

• Establish comprehensive foundation for future, more detailed, safety analyses
  – Evaluation of all system functions
  – SSFs and SSIs allow the program to focus on high-risk areas of the architecture

• Provide mitigation recommendations early in system development