Student Handout
NSWCDD-PN-14-00294

FUNCTIONAL HAZARD ANALYSIS TUTORIAL

International System Safety Training Symposium
Saint Louis, MO
5 August 2014
### Session 2 - 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>

VIPPS is a Mock System used for training purposes only
### Session 2 - Task 1c  
**F.4 Function Descriptions**

<table>
<thead>
<tr>
<th>Function</th>
<th>Function Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.4.2</td>
<td>Sense</td>
<td>Sense, track, and communicate the detection of potential objects of interest to the VIPPS mission</td>
</tr>
<tr>
<td>F.4.5</td>
<td>Lethally Engage</td>
<td>Control the lethal effectors to engage selected target(s)</td>
</tr>
<tr>
<td>F.4.1.3</td>
<td>Transition State/Mode</td>
<td>Assess current State and Mode and allowed transitions, then transition the State and Mode of the VIPPS to the commanded State and Mode or reject the transition</td>
</tr>
</tbody>
</table>
Session 2 - Task 1c
F.4 Operate System

Control States and Modes F.4.1

OR

Sense F.4.2

OR

Evaluate F.4.3

OR

Warn F.4.4

OR

Lethally Engage F.4.5
Session 2 - Task 1c
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 2 - Task 1c
For Reference Use Only

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

#### 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.
Intentionally Left Blank
### Session 4 – Task 2
**Worksheet**

<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>

VIPPS is a Mock System used for training purposes only.
Session 4 – Task 2
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
Session 4 – Task 2
Functional Thread

Training Functional Thread . . .

- System Status
  - Mode Change Request
    - “READY TACTICAL”
    - “READY TRAINING”

- Detection Location

- Transition State/Mode
  - “READY TACTICAL”

- Perform Surveillance
  - State/Mode Change Alert
    - “READY TACTICAL”

- 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)
Session 4 – Task 2
Functional Thread (cont.)

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

Lethal Engagement Order → Select Zone and Lethal Effector → Lethal Engagement Plan → Aim/Target → Visual Target Confirmation → Authorized Lethal Engagement Plan → Activate Lethal Effector

Non-Lethal Energy → Lethal Energy

VIPPS is a Mock System used for training purposes only.
Intentionally Left Blank
### Session 5 Task 4 Worksheet

#### State/Mode | Function | Functional Failure | Hazard Description | Mishap | Effect(s) | System Item(s) | Existing Mitigations | Recommended Mitigations
--- | --- | --- | --- | --- | --- | --- | --- | ---
Ready Tactical | F.4.1.3 Transition State/Mode | 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)

Ready Tactical | F.4.1.3 Transition State/Mode | 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 | | |

---

Reference VIPPS SSS Sections 4.1.1 and 4.1.2 System States and Modes to derive Existing Mitigations.
Session 5 Task 4
Mitigation Type Definitions

- **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