

**system design and
management**

Applying Systems Approach to Business Process Re-Engineering



**Scott Peterein, USCG
SDM '14**

Presentation Outline

- USCG Financial Management (FM)
- Business Process Reengineering (BPR)
- Thesis Research Focus
- Application of STPA & SafetyHAT
- Hazard Mitigation
- Discussion



USCG Photographs

The United States Coast Guard

- Worldwide Operations 24/7/365
 - Missions
 - People
 - Equipment
 - Activities



Systems are characterized by the interaction of hardware, software, data, humans, processes & procedures

FM System Improvement & Business Process Re-engineering

- USCG Core Accounting System (CAS)
 - Primary FM software application
 - Used to record (and report) full-range of FM transactions
 - Significant reliability, supportability & auditability issues
 - Goal: replace owned/hosted w/ commercial off the shelf system (COTS)
- Business Process Re-engineering
 - Enhance delivery of mission support services
 - Align “mission support” and “operational” models
 - Improve internal controls of funds/resources
 - Sustain unqualified audit opinion

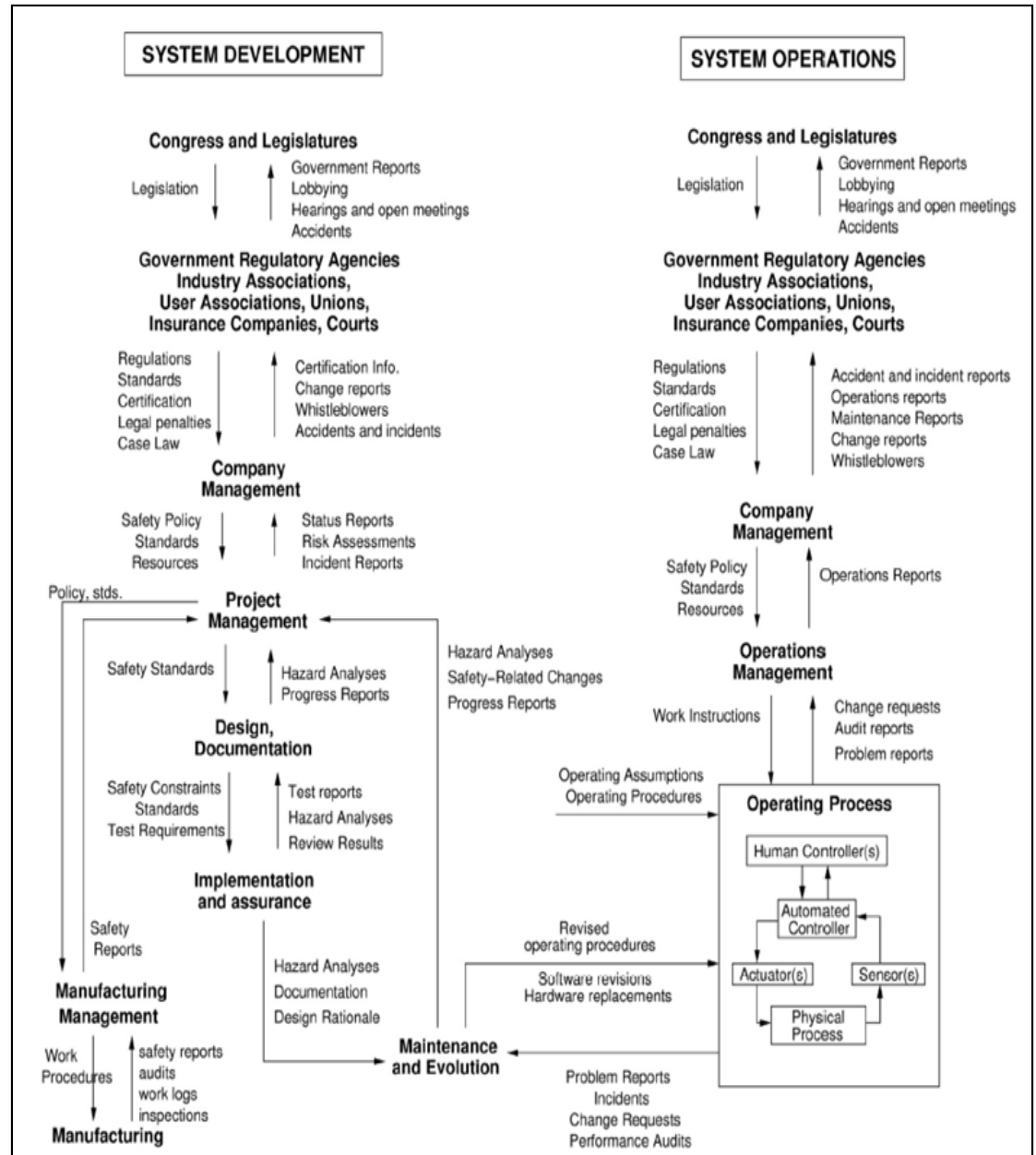
Thesis Research Questions

- What challenges will the USCG's new FM software application and re-engineered business processes create for front-line operating units?
- What system analysis methods may help identify the causal factors that create the challenges, and mitigate or abate them in the new USCG FM system?

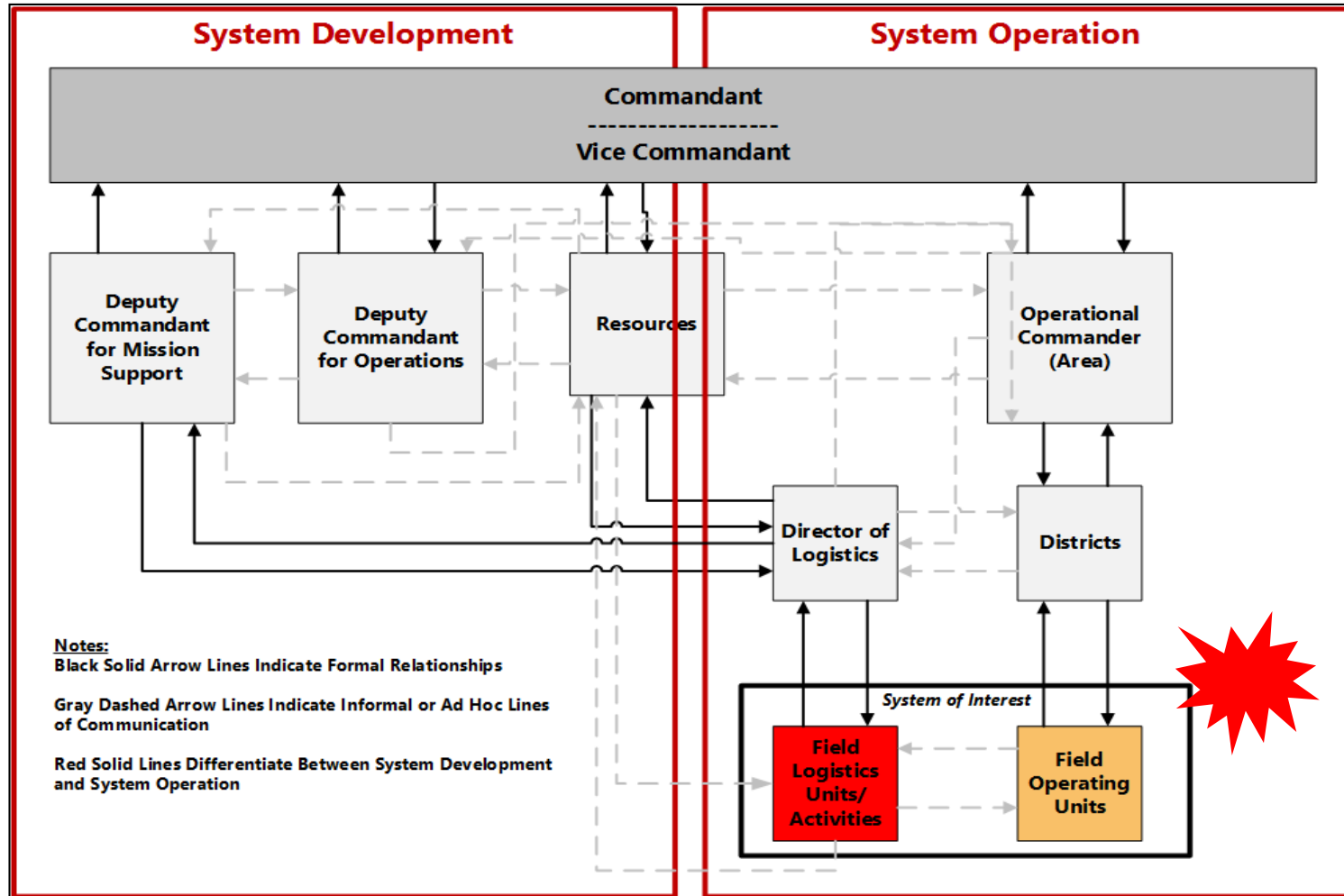
Research focused on evaluation of front-line operational unit procurement activities

Why STPA?

- MIT-SDM curriculum
- Applicability to USCG FM System
- Availability of SafetyHAT

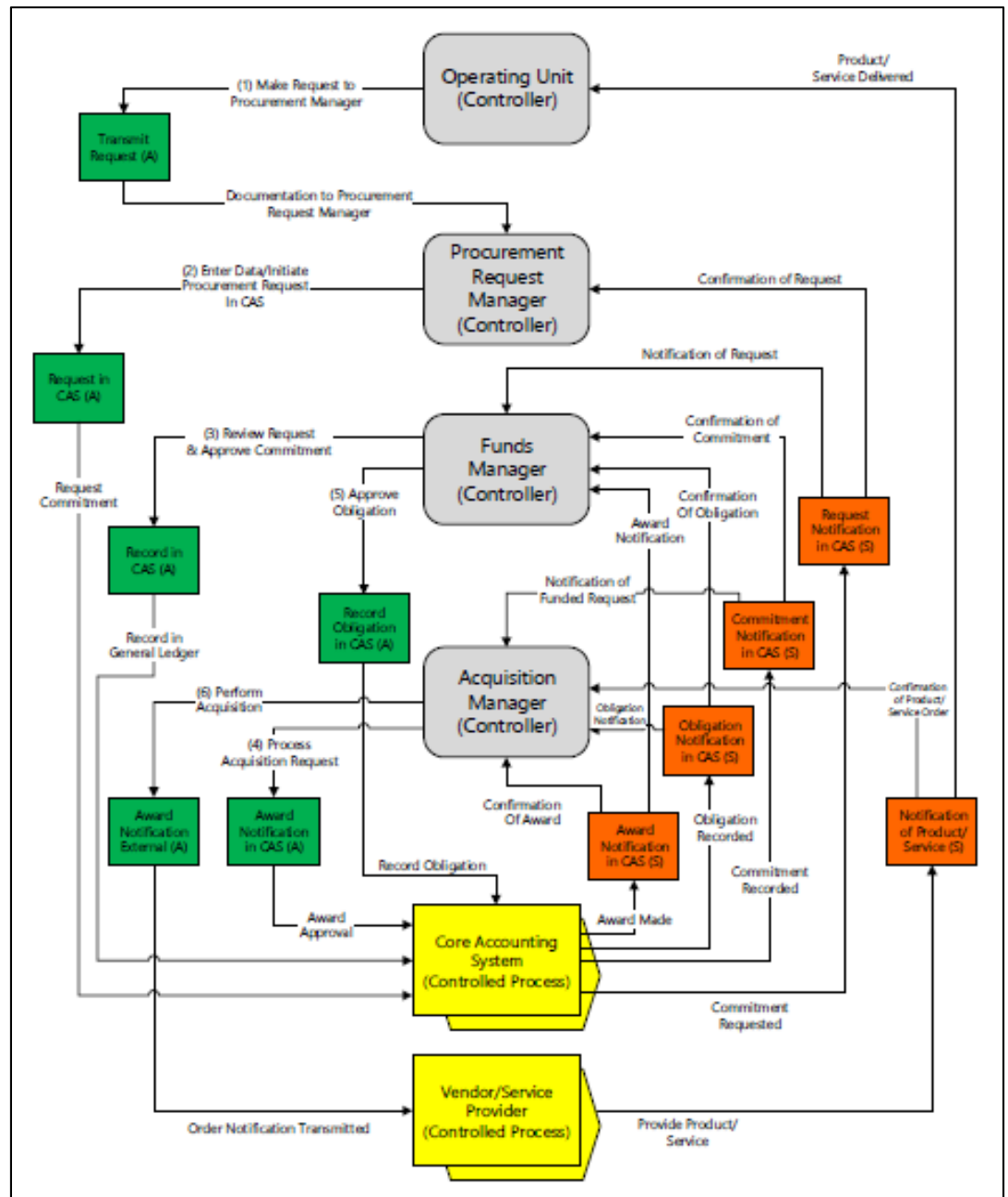
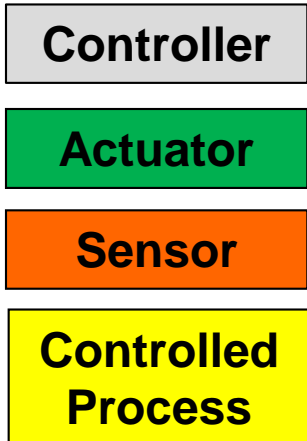


Generalized USCG Control Structure



USCG FM System Control Diagram

Research analyzed a generic product/service procurement transaction



SafetyHAT

Main Menu

Welcome to the Transportation Systems Safety Hazard Analysis Tool (SafetyHAT). This tool will guide you through hazard analysis using the System-Theoretic Process Analysis (STPA) method.

Please complete the Preparatory Steps before accessing the forms below. The Preparatory Steps can be reviewed using the "Review Preparatory Steps" button at the bottom of this screen. A control structure diagram can be uploaded using the "Upload Control Structure Diagram" button at the bottom of this screen.

Complete the forms in the order presented below to ensure a complete analysis.

Enter System Information

- 1. Components** *This form allows you to enter the components of your system.*
- 2. Connections** *This form allows you to enter connections between the components of your system.*
- 3. Control Actions** *This form allows you to enter specific Control Actions issued by controllers in your system.*

Conduct Analysis

- 4. Accidents or Losses** *This form will allow you to enter accidents (or losses) specific to your system.*
- 5. Hazards** *This form will allow you to enter hazards specific to your system.*
- 6. Unsafe Control Action Analysis** *This form will guide you through evaluating Unsafe Control Actions and potentially related system hazards.*
- 7. Causal Factor Analysis** *This form will guide you through evaluating Unsafe Control Actions and potential causal factors.*

Export Analysis

- 8. Export Data** *This will compile the STPA results and export the data to MS Excel.*

Advanced Options

Review Preparatory Steps

Upload Control Structure Diagram

Locate Additional STPA Resources

Volpe The National Transportation Systems Center

STPA

Loss

Hazard

UCA

CF

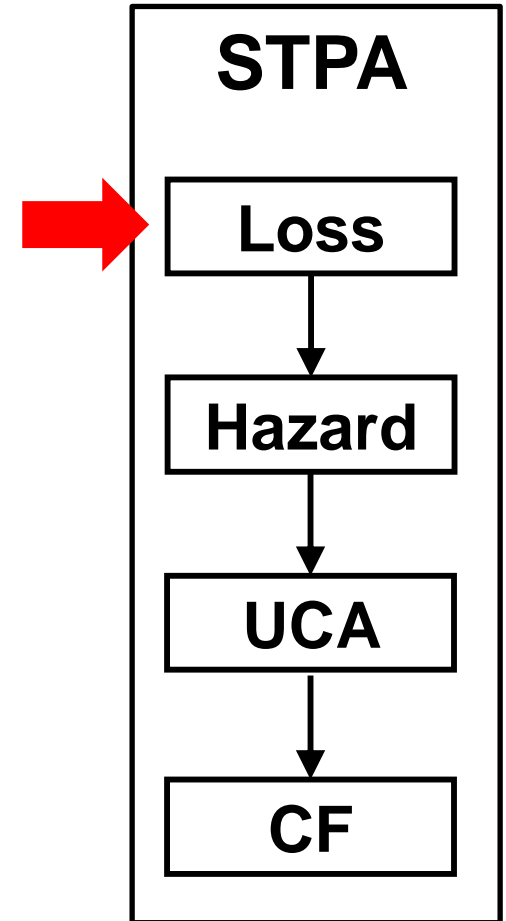


system design and management

USCG System Losses (Accidents)

“Accident: An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.” -Leveson

- Operating Unit cannot meet operational requirements or commitments.
- Violation of USCG Financial Management Laws and/or policies.



SafetyHAT Input Form (Step 4)

Accident (or Losses) Input Form Step: 1 2 3 **4** 5 6 7 8

Review Existing System Accidents or Losses

Existing System Accidents (or Losses) Sort: Order Entered ▼ ▲ A-Z ▼ ▲

- Operating Unit cannot meet operational requirements or commitments
- Violation of USCG Financial Management Laws and/or policies

Add New System Accident or Losses

Enter System Accident (or Loss):
Operating Unit cannot meet operational requirements or commitments

Enter Detailed Description of the Accident (or Loss):
A break-down in the financial management/procurement system results in the inability of the front-line operating unit to perform its missions.

[Delete Existing](#) [Modify Existing](#) [Save As New](#)


[Return to Main Menu](#)

[Step 3: Control Actions](#)

[Step 5: System Hazards](#)

[View Control Structure Diagram](#)

[Close Form](#)

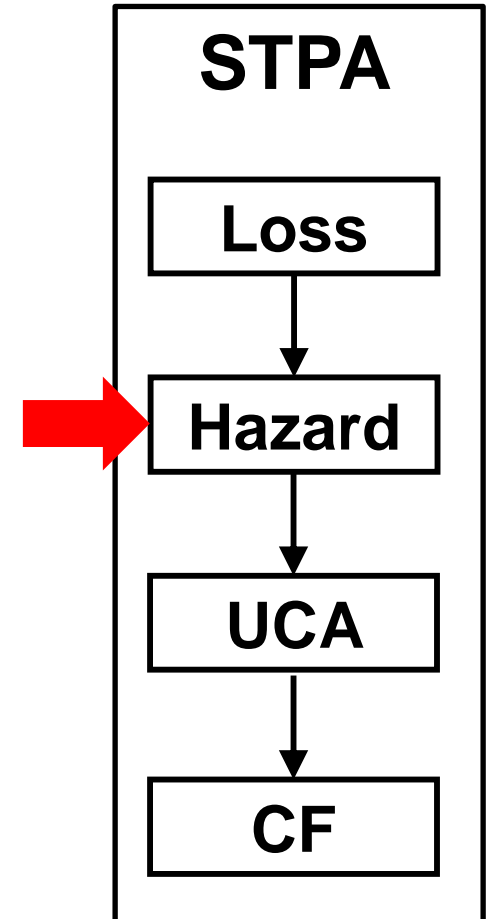
 **Volpe** The National Transportation Systems Center

[Form Guidance](#)

USCG System Hazards

“Hazard: A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss).” -Leveson

- Commitments or obligations are not in line with USCG financial policy
- Commitments or obligations are recorded in excess of funding limitations
- Operating unit has missing and/or inoperable equipment, services, or supplies; or lacks qualification
- USCG contracts are executed prior to sufficient funds being appropriated or committed



SafetyHAT Input Form (Step 5)

Hazard Input Form

Step: 1 2 3 4 5 6 7 8

Review Existing System Hazards

Existing System Hazards Sort: Order Entered ▼ ▲ A-Z ▼ ▲

Commitments or obligations are not in line with USCG financial policy, spend plans, or congressional appropriations

Commitments or obligations are recorded in excess of funding limitations

Financial commitments or obligations are inaccurately or improperly recorded in the financial statements

Operating unit has missing and/or inoperable equipment, services, supplies; or lacks qualified personnel

USCG contracts are executed prior to sufficient funds being appropriated or committed

Add New System Hazard

Enter System Hazard:
Operating unit has missing and/or inoperable equipment, services, supplies; or lacks qualified personnel

Enter Detailed Description of Hazard:
The procurement of products/services did not occur in a manner that enabled the operating unit to obtain supplies or services to repair assets or maintain a required state of readiness and/or crew qualification.

Select Associated Accident(s):
Operating Unit cannot meet operational requirements or commitments
Violation of USCG Financial Management Laws and/or policies

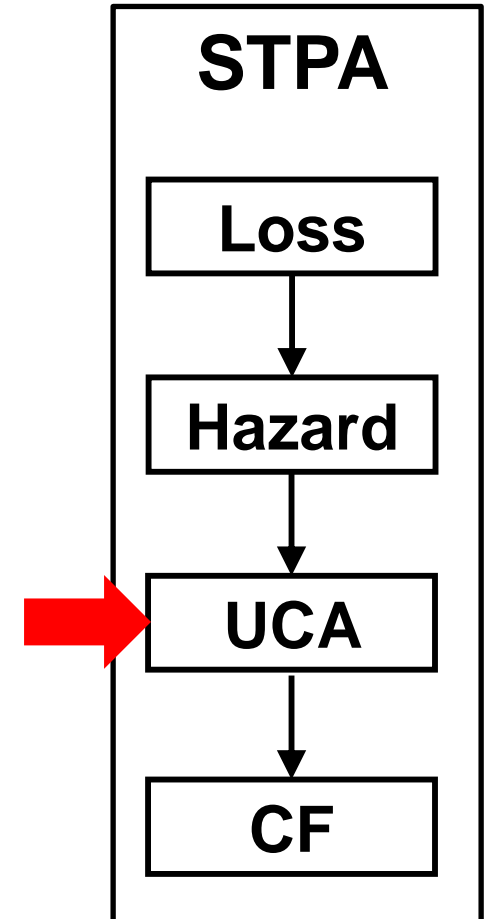
Delete Existing Modify Existing Save As New

Return to Main Menu Step 4: System Accidents or Losses Step 6: Unsafe Ctl Action Analysis View Control Structure Diagram Close Form

Volpe The National Transportation Systems Center Form Guidance

USCG Unsafe Control Action (example)

- The request was initiated in the financial management system, but contained data errors, or possibly incorrect routing for transmittal to the next level
- The product/service requested is incorrect--i.e. wrong vendor, incorrect funding level, wrong quantity, incorrect unit cost or total amount, or incorrect accounting information



SafetyHAT Input Form (Step 6)

Unsafe Control Action (UCA) Analysis

Step: 1 2 3 4 5 6 7 8

Current Control Action

Select Controller
Procurement Request Manager

Control Action: 1 of 1
Initiate Procurement Request (PR) in CAS

Control Action Analysis Completed

Previous Control Action Next Control Action

Existing Unsafe Control Actions

Select Unsafe Control Action Category Complete Add Note
Provided, but executed incorrectly

Existing UCAs for Selected Control Action and UCA Category
The request was initiated in the financial management system, but contained data errors, or p

Unsafe Control Action Analysis

Enter or Select a Detailed Description for UCA
The request was initiated in the financial management system, but contained data errors, or possibly incorrect routing for transmittal to the level

(All UCAs for Selected Controller)

Select Relevant Hazards (if applicable)
Operating unit has missing and/or inoperable equipment, services, supplies; or lacks quali
Commitments or obligations are recorded in excess of funding limitations
Financial commitments or obligations are inaccurately or improperly recorded in the finan
Commitments or obligations are not in line with USCG financial policy, spend plans, or con
USCG contracts are executed prior to sufficient funds being appropriated or committed

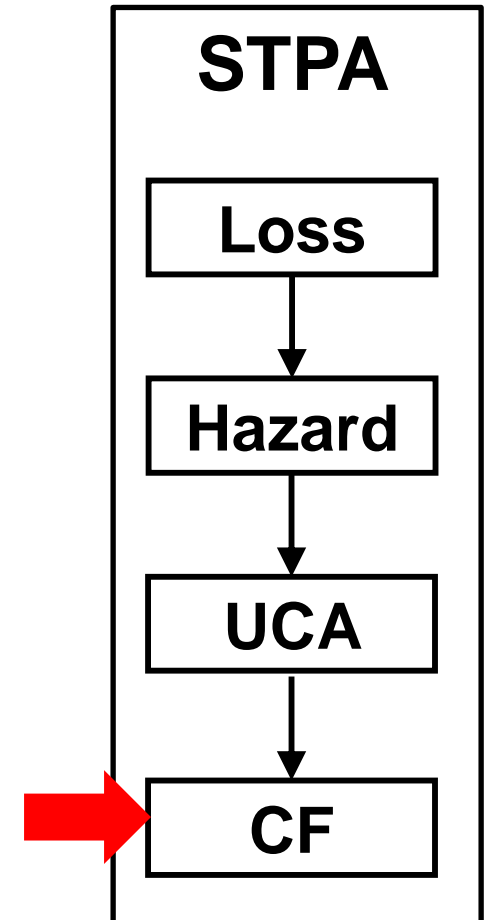
Delete Existing Modify Existing Save As New

Return to Main Menu Step 5: System Hazards Step 7: Causal Factor Analysis View Control Structure Diagram Close Form

Volpe The National Transportation Systems Center Form Guidance

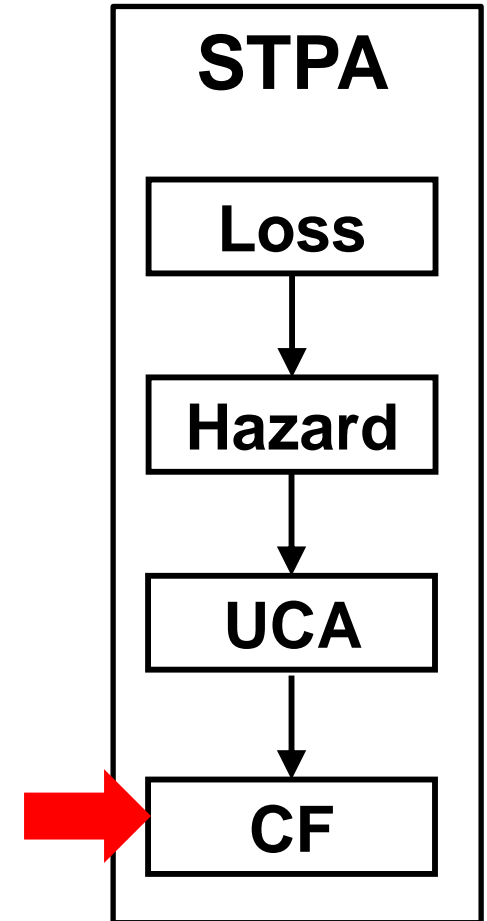
Causal Factors

- STPA with SafetyHAT revealed 205 causal factors
- SafetyHAT data export used to generate requirements & assign responsibility for hazard mitigation in the FM system
- Some causal factors related to changes over time; System Dynamics modeling used to quantify negative system impacts



Causal Factors (examples)

- Excessive workload, job pressure, or distraction could prevent the funds manager from recording the obligation in CAS in a timely manner. (External Disturbances)
- Lack of training, poor job performance, improper prioritization of tasks, or lack of feedback regarding the status of the system prevented the service from being ordered within the required time. (Process Model)



SafetyHAT Causal Factor Analysis (Step 7)

Causal Factor Analysis
Step: 1 — 2 — 3 — 4 — 5 — 6 — 7 — 8

Unsafe Control Action Details

Controller 4 of 4

Description 4 of 4

UCA Analysis Completed

Associated Hazards:
 Operating unit has missing and/or inoperable equipment, services, sup

Previous Controller
Previous Record
Next Record
Next Controller
Add Note

Existing Causal Factor Analyses

Sort: Order Entered ▼ ▲ Component Name A-Z ▼ ▲

Existing Causal Factors for Selected Unsafe Control Action

Causal Factor	Component Name or Connection From	Connection To
External disturbances	Procurement Request	
Process model or calibration incomplete or inc	Procurement Request	
Actuator inadequate operation, change over tim	Request in CAS (A)	
Controlled component failure, change over tim	Core Accounting System	
Sensor inadequate operation, change over tim	Request Notification in	
Sensor to controller signal inadequate, missing	Request Notification in	Funds Manager

Causal Factor Analysis

Select: Component or Connection

Component ▼

Causal Component

Component Type ▼

Select the Appropriate Causal Factor

External disturbances ▼

Enter or Select a Causal Factor Description

(All Causal Factor Descriptions for Selected Component / Connection and Causal Factor)

▼

Delete Existing
Modify Existing
Save As New

Return to Main Menu
Step 6: Unsafe Ctl Action Analysis
Step 8: Export Data
View Control Structure Diagram
Close Form

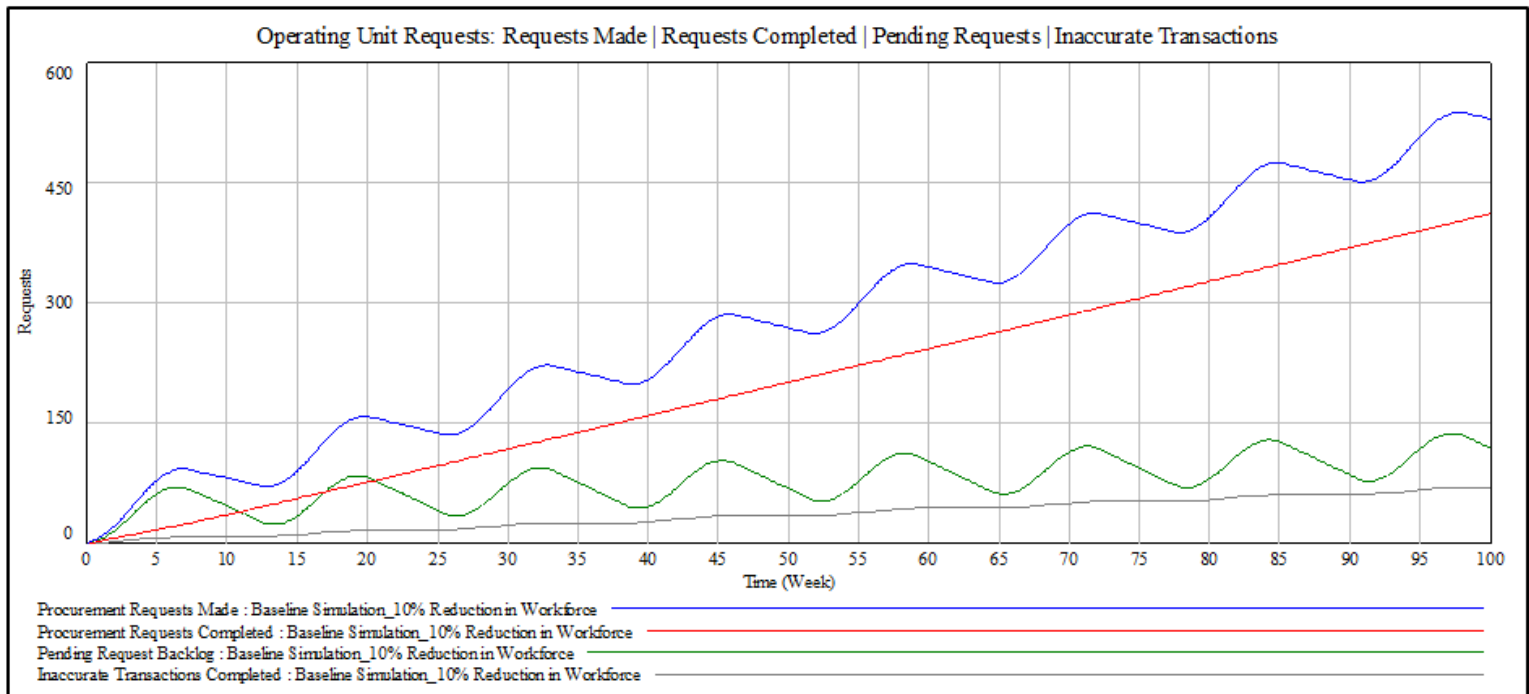
The National Transportation Systems Center
Causal Factor Diagram
Form Guidance

SafetyHAT Utility & Future Research

- SafetyHAT facilitated a very thorough review of a complex socio-technical system
 - Intuitively guides users through STPA
 - Easy to analyze results using Excel data export
 - Traceable requirements generation

SafetyHAT Utility & Future Research (con' t)

- Causal Factor guidewords can be modified to analyze systems in other domains or applications
- Thesis research, including system dynamics modeling, will help inform the implementation of USCG FM application & BPR



Question & Discussion

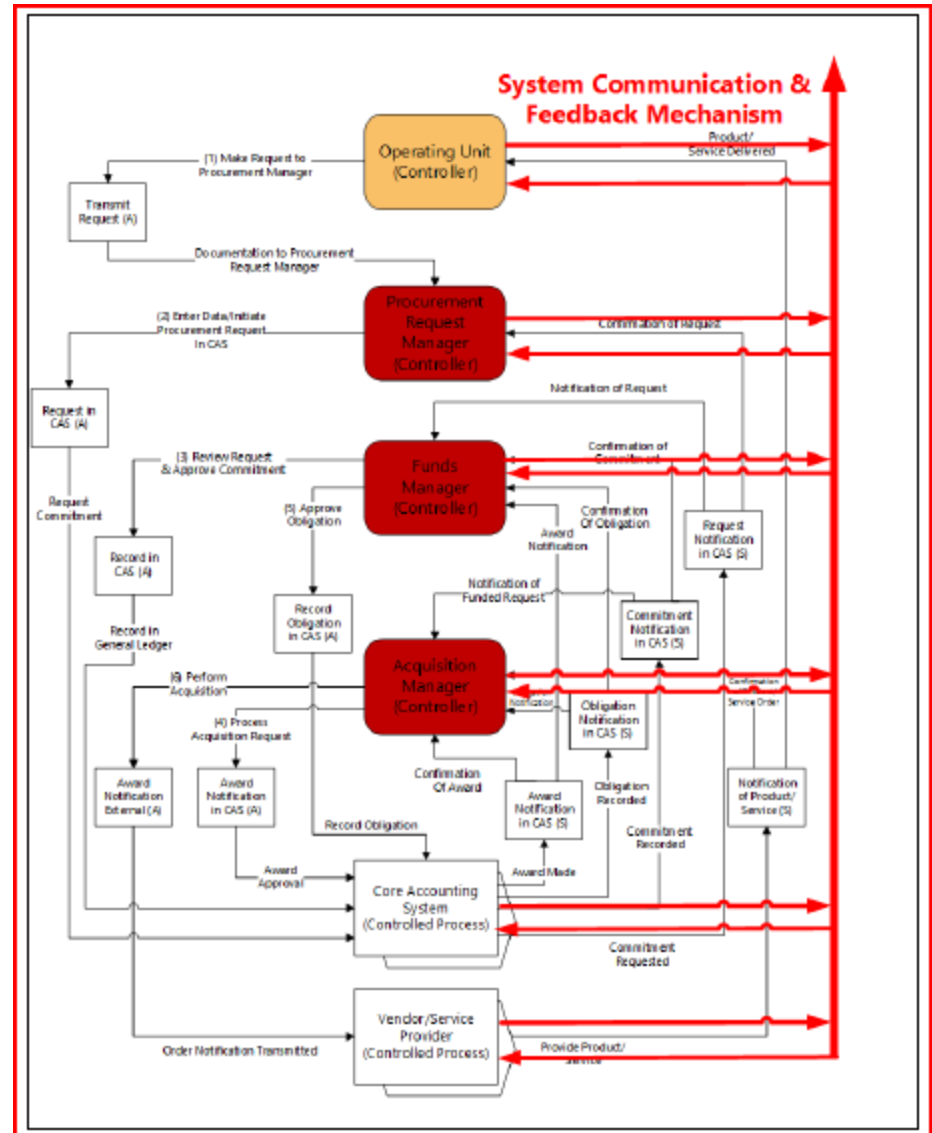
Background

Generalized Findings

- Hazard Analysis methodology proved useful for ID'ing deficiencies in a complex socio-technical systems
- Simulations provide valuable insight into system behavior
 - Informs design & resource allocation decisions
- Strong sponsorship critical to prepare the system for the changes that are needed
 - There must be a common understanding of the problem and consensus on how to resolve it
- The re-engineered CG system must have robust channels for feedback & communication

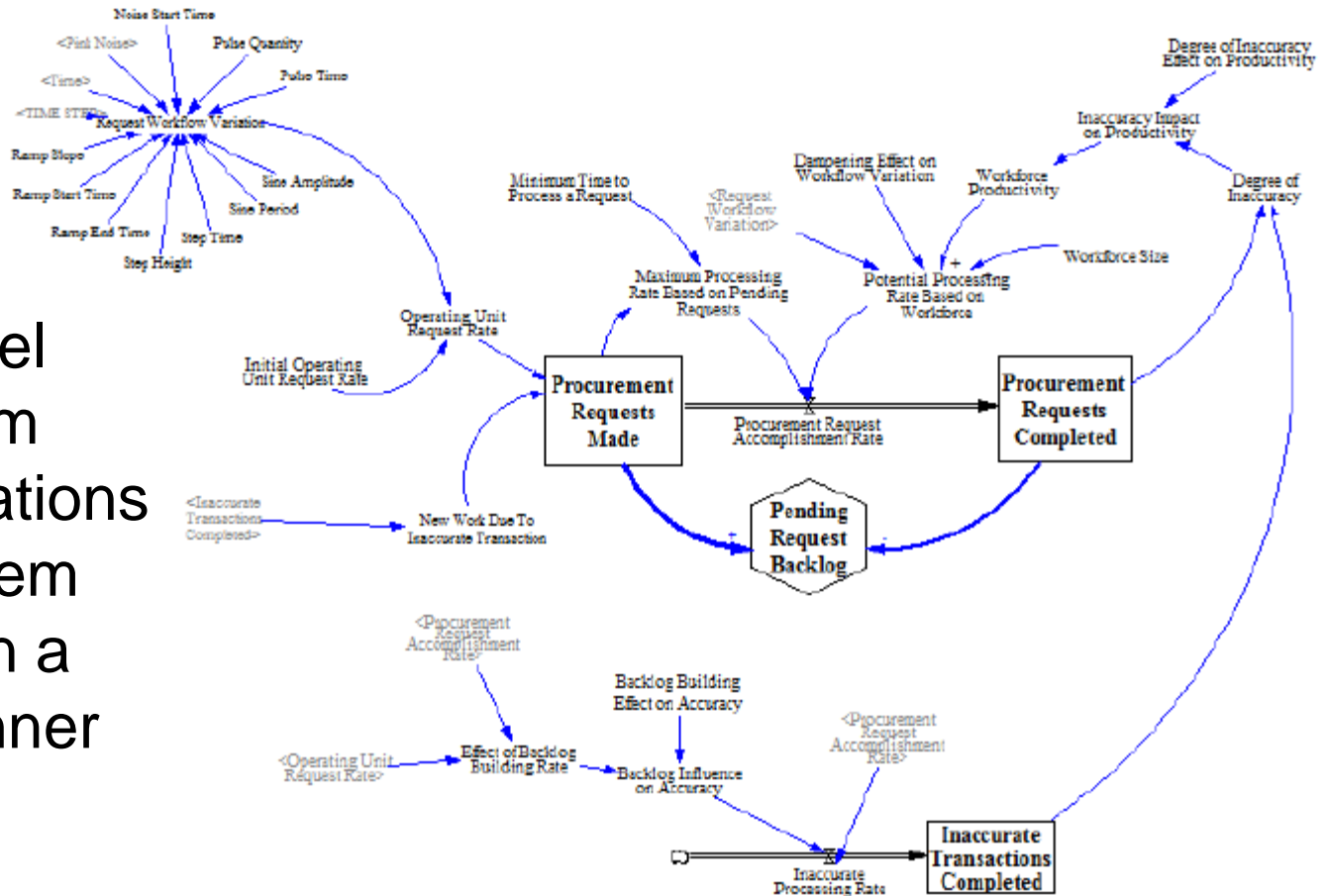
System Feedback

A robust communication & feedback mechanism is critical to achieve desirable system performance



System Dynamics Model

Basic SD Model used to perform multiple simulations to access system performance in a predictive manner



Discussion Topics

Most significant challenges of the current state?

- System limitations
- Liabilities
- Inefficient processes /work-arounds
- Other.....?

Perceived hazards that exist in the “to-be” state?

- Resource constraints (workforce capacity, IT/network, BI)
- DOI Solution
- System feedback & communication mechanism
- Training (OFF and/or business processes)
- Metrics
- Other.....?

Most significant challenges regarding implementation of the “to-be” state?