

3rd European STAMP Workshop

Using STPA to Investigate Test Safety



Massachusetts
Institute of
Technology

Dan Montes, Ph.D. Student
Systems Engineering Research Lab

6 October 2015

Disclaimer

The views expressed in this document are those of the author



<http://www.museumofflight.org/>

Overview

- Motivation
- Work & Study Project
- Results

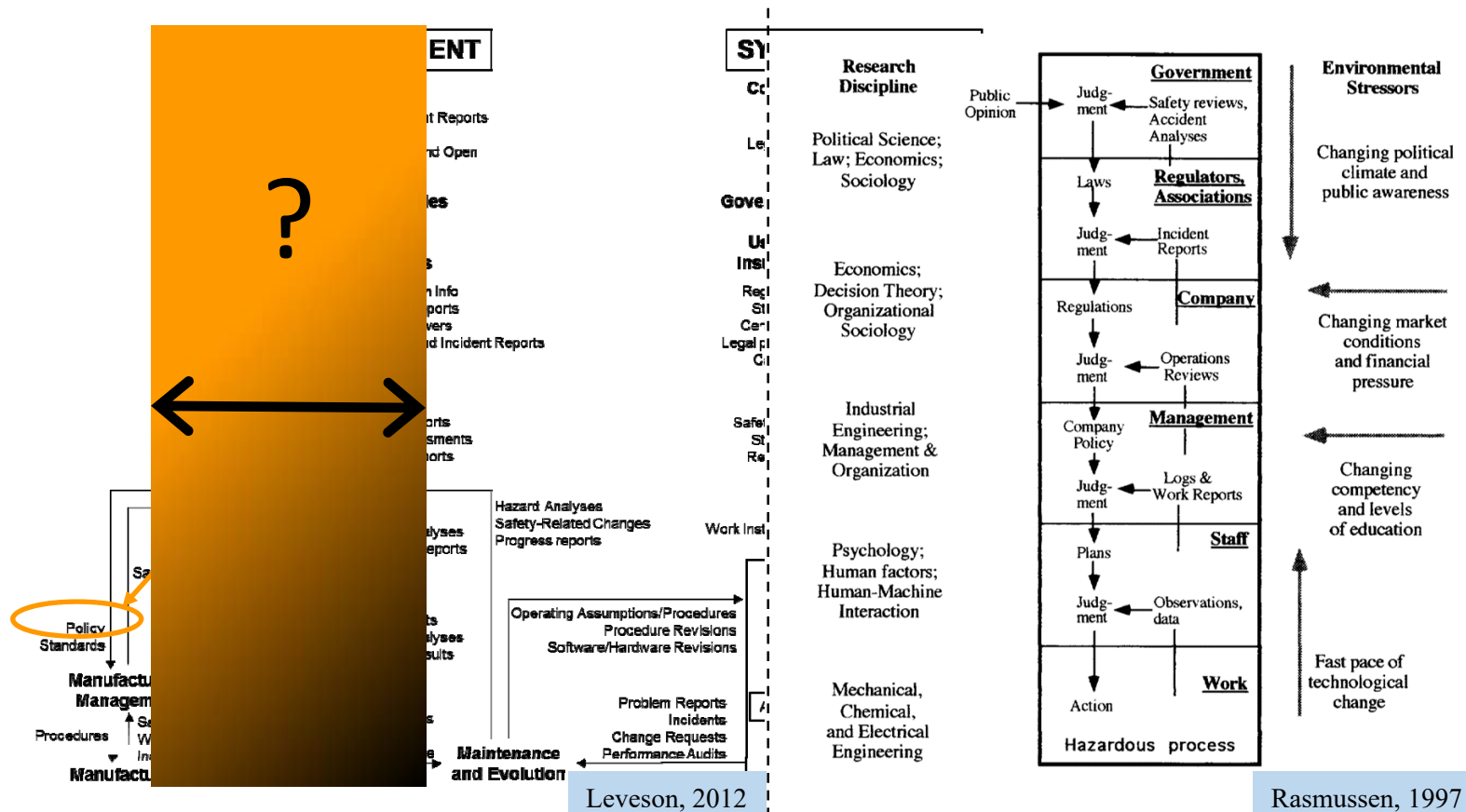
Research Objective

Motivation

Provide a common framework for test-safety planning that addresses both the safety of the test process and inherent system safety

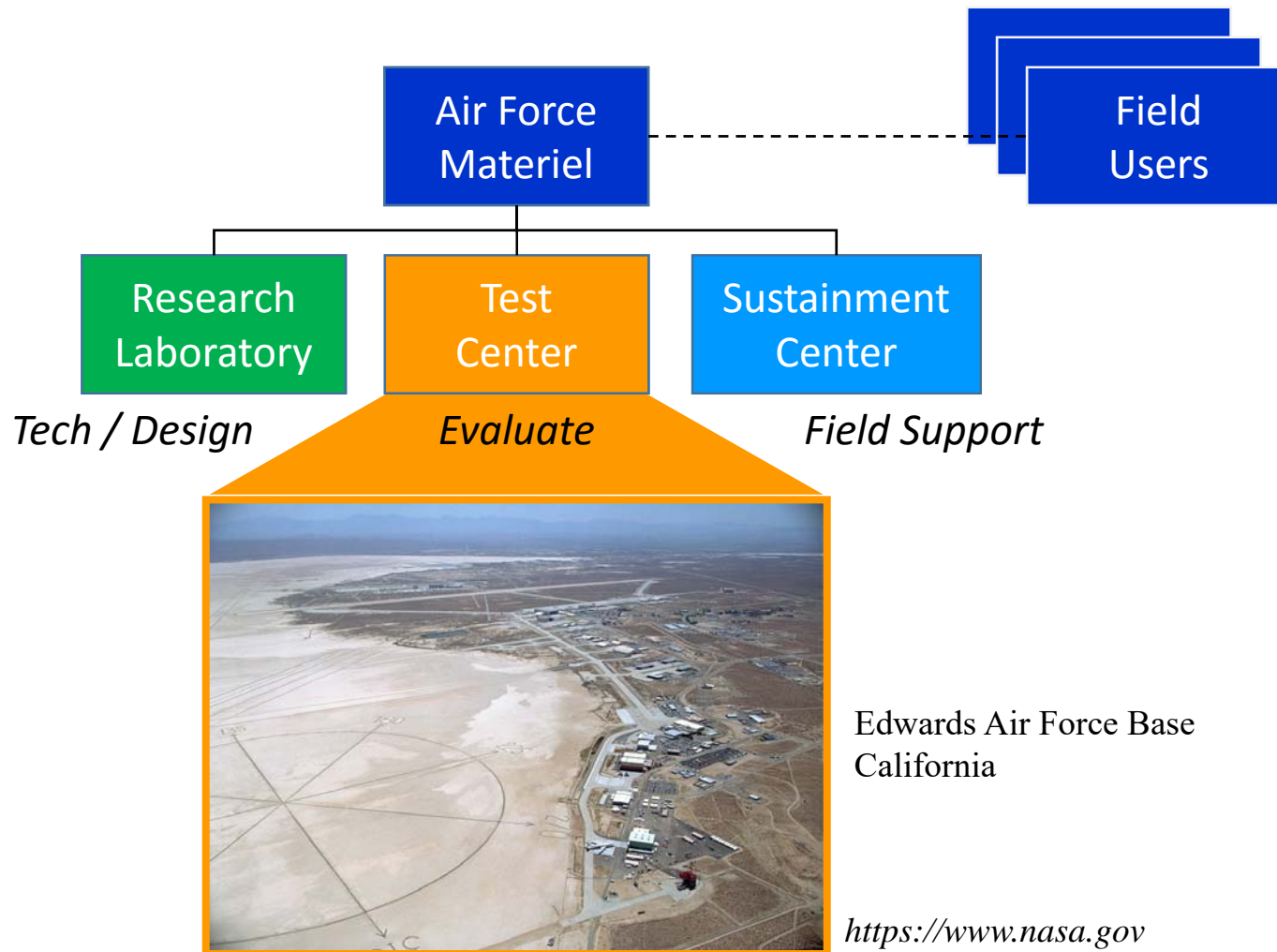
Organizational Example

Motivation



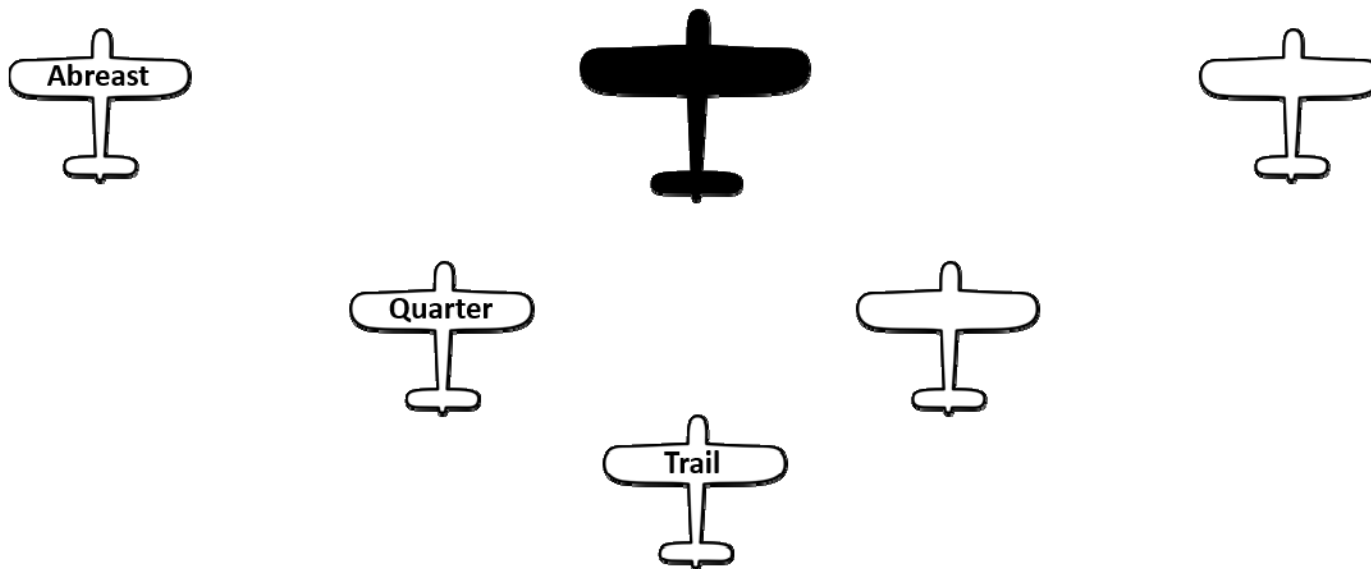
Test Enterprise Use Case

Motivation



Autonomous Wingman

Motivation



Safety Goals During Test

Motivation

a) Safety of the system as designed and intended for use

SYSTEM SAFETY

- Confirmation of design intent
- Risk reduction when no models available (e.g., humans, software)

b) Safety of the test conduct

TEST SAFETY

- Techniques, configuration, test environment
- Buildup approach when models are inaccurate or nonexistent

MIL-STD-882E

Expert Knowledge

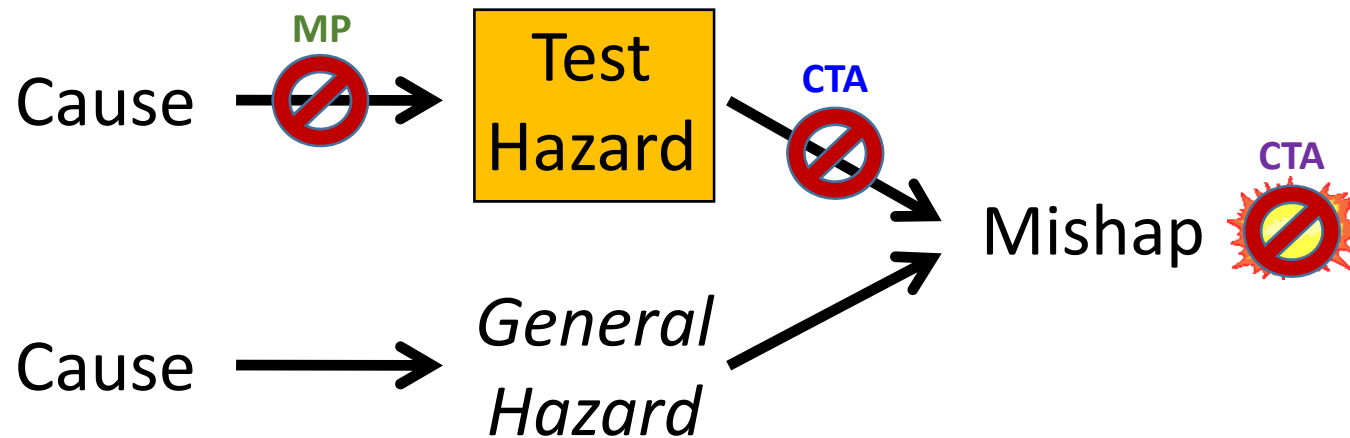
Motivation



Event Chain (Test)

Motivation

TEST SAFETY



Test Hazards (THAs)

Identify specific test hazards during the analysis and the cause(s) of each

Determine effect (mishap) and severity (consequence)

Minimizing Procedures (MP): break the chain of cause

- Directives / Considerations
- Can be pre-mission or during operations

Corrective Actions (CTAs): break chain after hazard

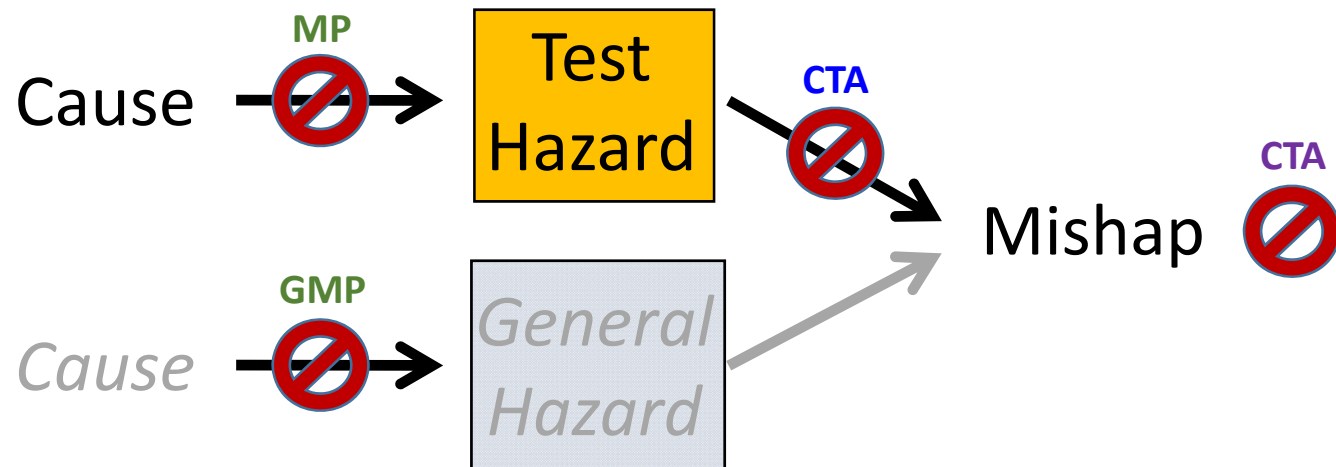
Corrective Actions (CTAs): reduce effect of mishap

ASSIGN
RISK

View of Hazard Analysis

Motivation

TEST SAFETY




Traditionally, hazards must be test-specific to be acknowledged in formal analysis...

e.g. “Mid-air collision during formation maneuvers”

Traditional Approach

Motivation

TEST SAFETY



“Use system safety-techniques, prior experience, legacy system research, and overall engineering judgment” to identify hazards and populate the risk matrix

– *AF Test Safety Policy*

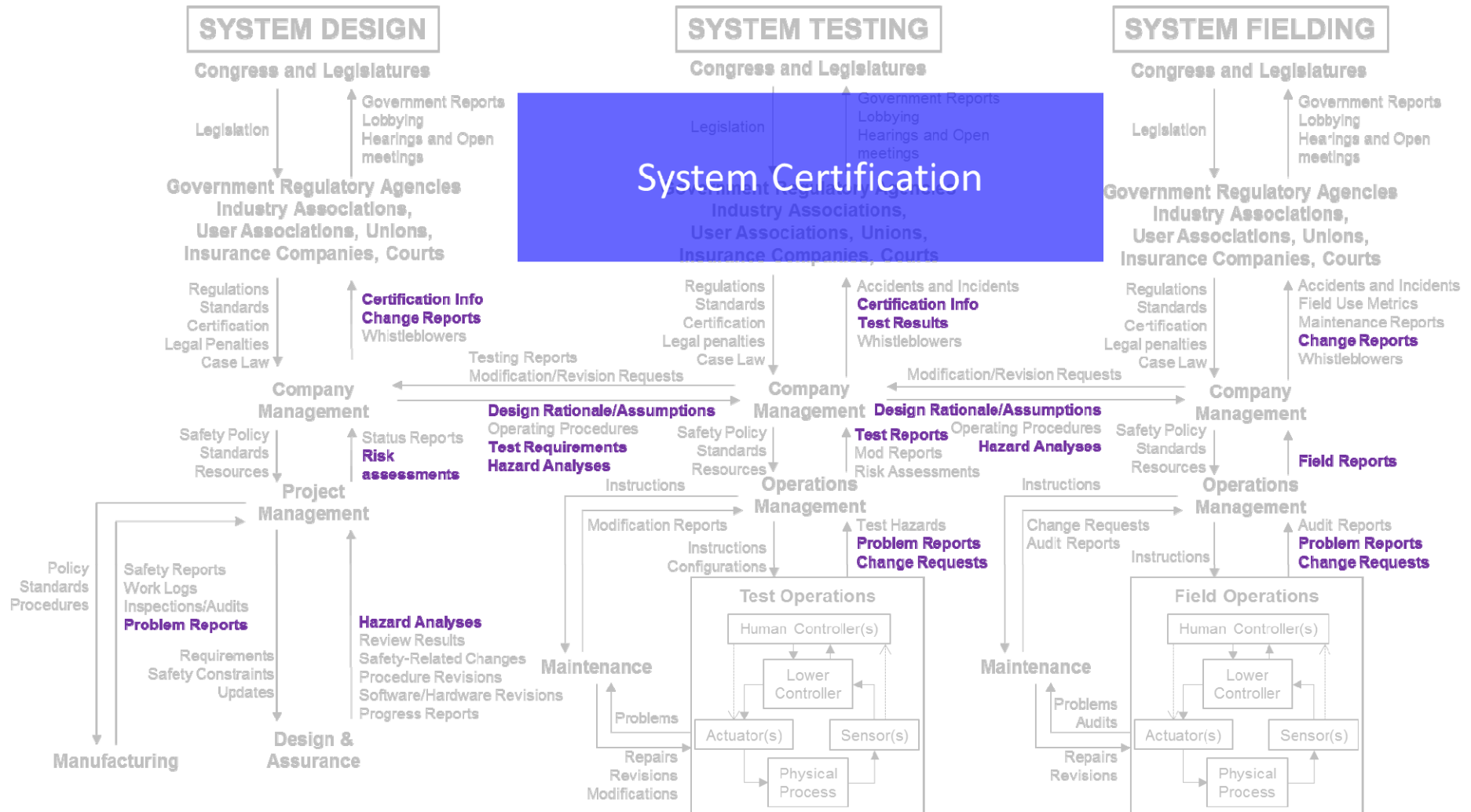
Research Tasks

Work

- Update Organizational Control Structure Example
 - Systems View of Testing
 - *New Inclusion Criteria*
- Develop Test-Safety Planning Method
 - Systems Perspective of Test Planning
 - *Proposed Document Format*
- Comparison with Flight-Test Study

Updated Org Example

Work

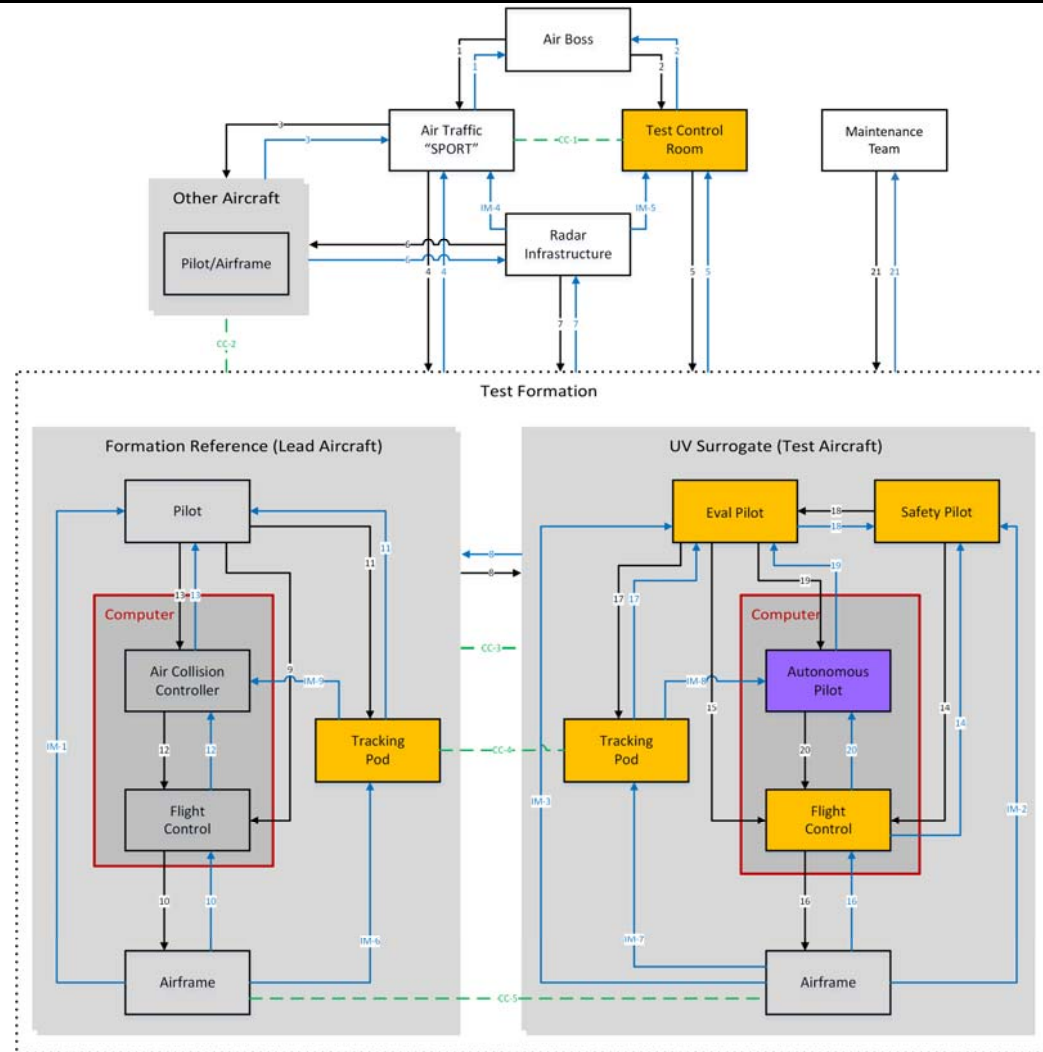


Flight Test Study

Work



Control Structure (Operating Process) *Work*



Process Behavior

Work

System
Behavior

contribute



Hazard



Mishap

*Design
Use / Test*

System Boundary

SYSTEM

ENVIRONMENT

Process Control

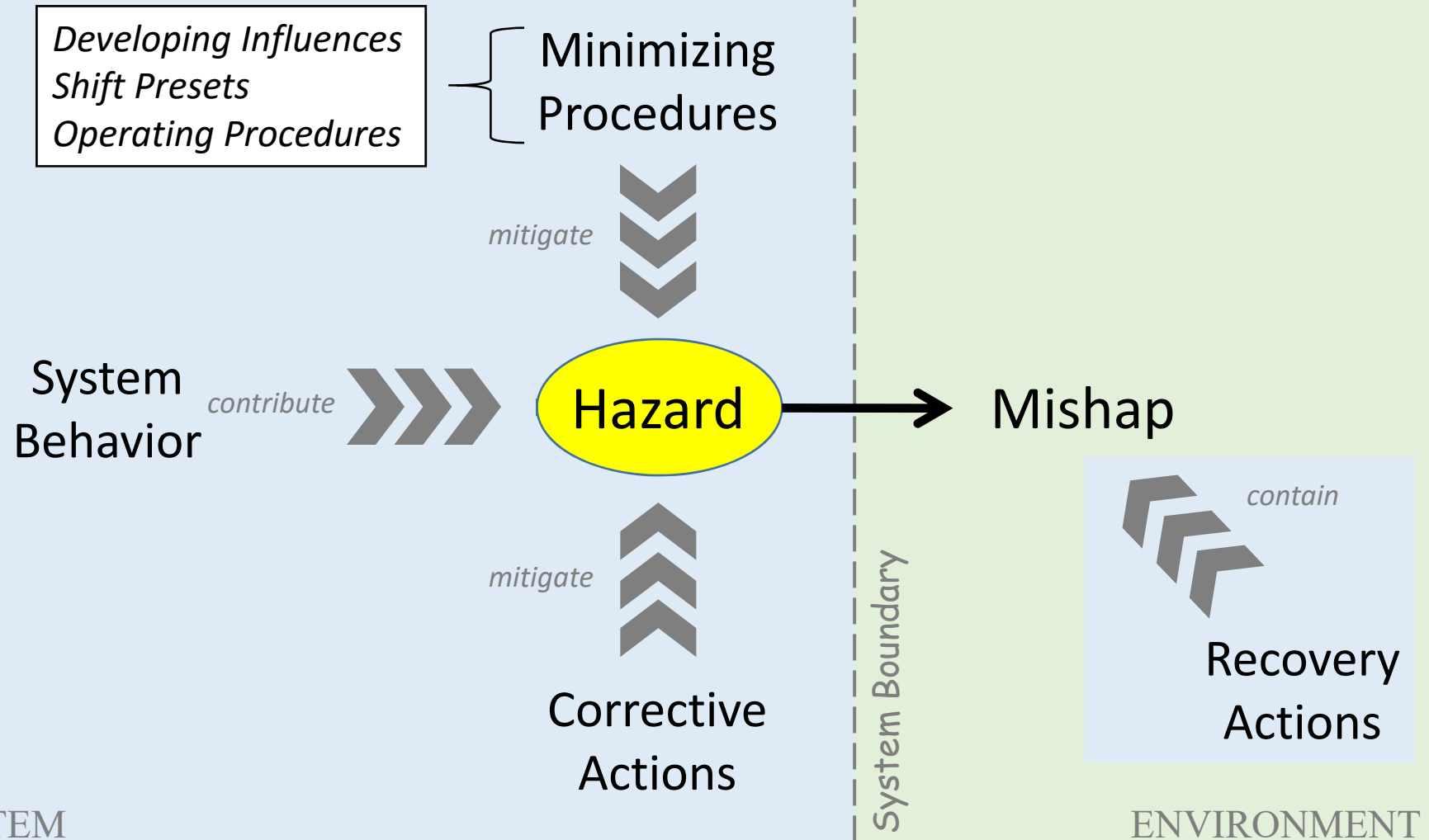
Work

- 1) Redesign to Eliminate Hazard
- 2) Reduce Hazard Likelihood
- 3) Control Hazard Exposure
- 4) Lessen Damage Severity

❖ MIL-STD-882E: “No amount of doctrine, training, warning, caution, or Personal Protective Equipment (PPE) can [eliminate a hazard]” (p. 11)

Process Control

Work



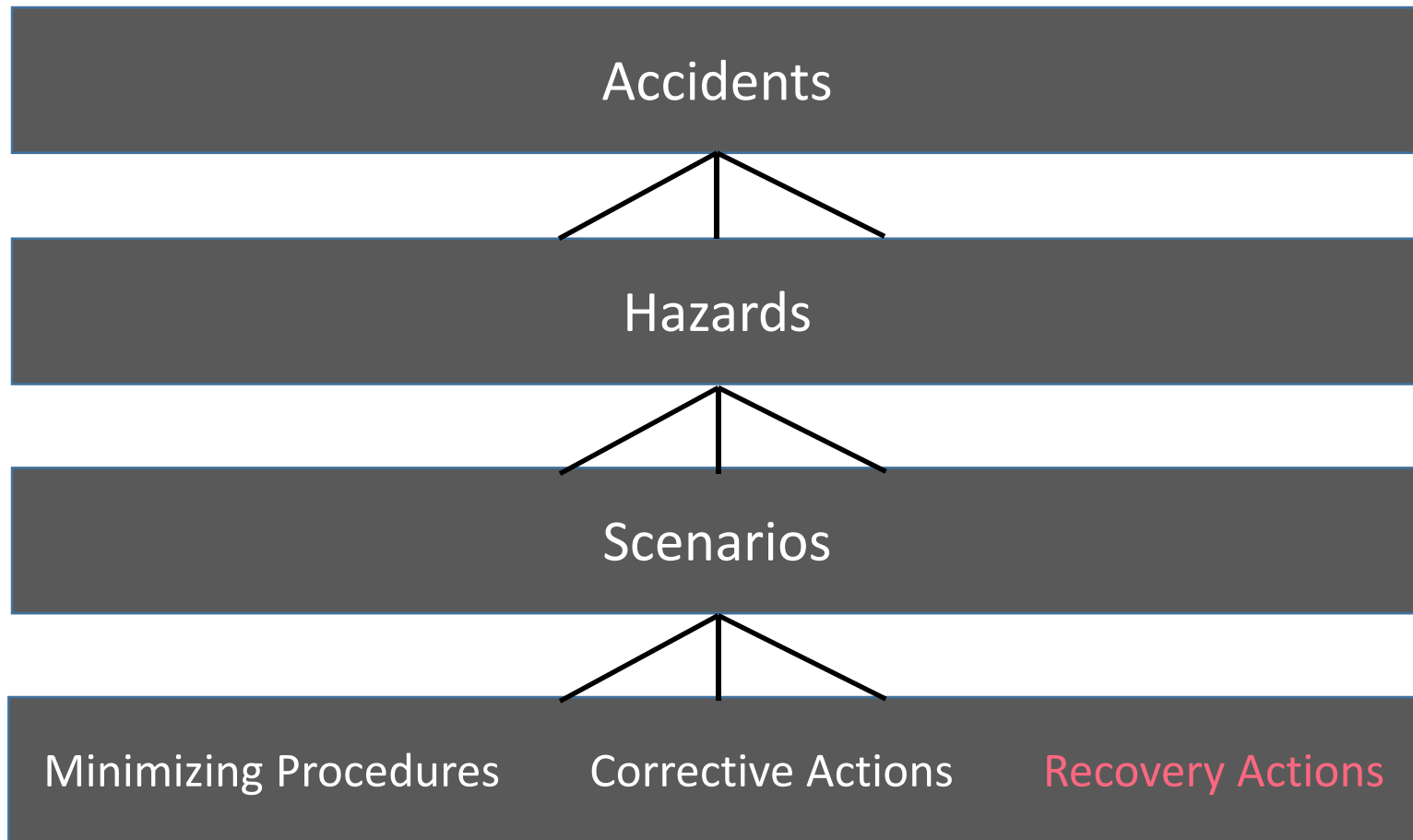
Minimizing Procedures

Work

- Developing Influences
 - *Test/Safety Planning*
 - *Training and Qualifications*
 - *Flight and Test Manuals*
- Shift Presets
 - *Test Card Requirements*
 - *Briefing Requirements*
 - *Instrumentation and Item Configurations*
 - *Operations and Maintenance*
 - *Personal Risk Management / Physiological Prep*
- Operating Procedures

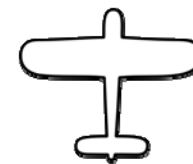
Top Down Planning

Work



Study Findings

Results



Objective Findings - Analysis *Results*

Traditional	STPA
2 Effects	6 Accidents
1 Test Hazard (actually a mishap)	4 System Hazards
3 Causes	392 Unsafe Control Actions
13 Minimizing Procedures - 8 <i>THA minimizing procedures</i> - 5 <i>general minimizing procedures</i>	46 Minimizing Procedures - 14 <i>developing influences</i> - 10 <i>shift presets</i> - 22 <i>operating procedures</i>
<i>Nothing identified to control hazard exposure (test hazard was a mishap)</i>	8 Corrective Actions
1 Accident-Corrective Action	7 Recovery Actions

Objective Findings - Hours

Results

	Author	Expert (est.)
<i>Control Structure</i>	5	2
<i>Hazard Analysis</i>	40	30
<i>Report Writing</i>	15	8
<i>Total</i>	60	40

Total hours for traditional safety plan: **10**

Total time for software certification (including FMEA): 4,000 hours and 8 months

Subjective Findings

Results

Intelligibility

The accessibility of information in the document, the ease of comprehending that information, and the intuitiveness of how the information was presented in the structure of the document.

Informativeness

The document's ability to convey information about hazards, the causal scenarios that might contribute to the hazards, and safety mitigations.

Implementability

The ease and willingness of planners to construct (or modify for use) new diagrams, ease of identifying hazards, causal scenarios, and mitigations, and perceived ability to brief, implement, and track risk mitigation strategies.

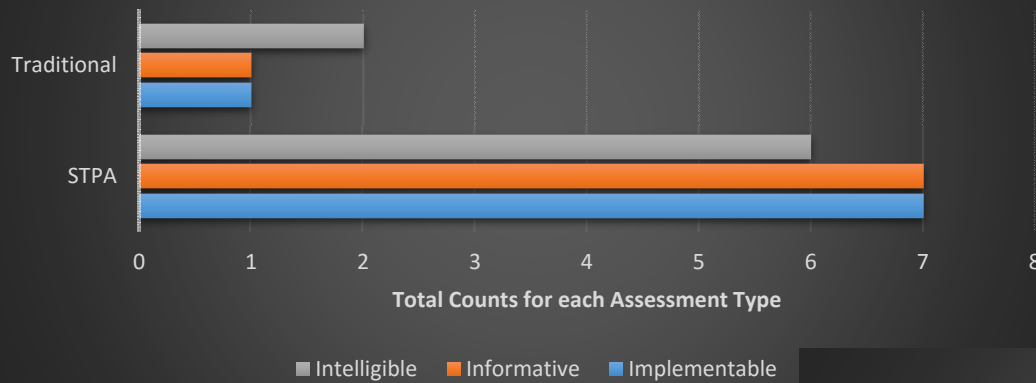
3 General Forced-Choice Questions → Traditional or STPA

20 Detailed Questions → Traditional, STPA, Both, Neither

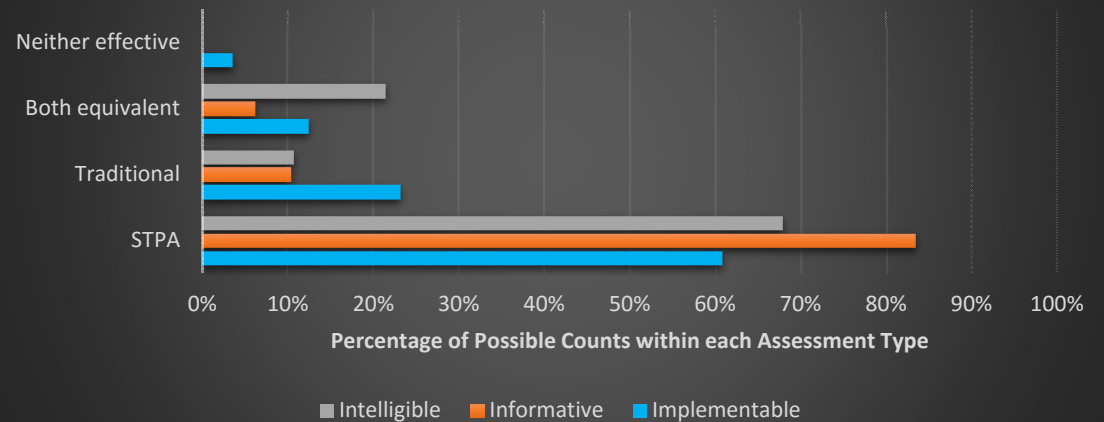
Trends

Results

Preferences Totaled from Forced-Choice Questions; all Eight Subjects



Preferences Totaled from Detailed Questions; all Eight Subjects



Systematic Preferences

Results

Question	Response	
Which of the Safety Plans did you find MOST Intelligible?	TWO choices	
Easy to quickly reference desired information	FOUR choices	
Easy to read and comprehend	FOUR choices	
Easy to find the "bottom line"	FOUR choices	
Consistency of formatting across multiple similar entries (e.g., hazardous behaviors)	FOUR choices	>> Reject: χ^2 (3, n = 8) = 9.33, p < 0.05
Easier to mentally visualize the system	FOUR choices	
Easy to understand what portions of the system are upgraded / being evaluated	FOUR choices	>> Reject: χ^2 (3, n = 8) = 8.00, p < 0.05
Easy to understand which equipment and personnel are part of only the testing (but not the intended field use)	FOUR choices	>> Reject: χ^2 (3, n = 8) = 8.00, p < 0.05
Which of the Safety Plans did you find MOST Informative?	TWO choices	>> Reject: χ^2 (1, n = 8) = 4.50, p < 0.05
Informative presentation of hazards (and unsafe actions, if applicable)	FOUR choices	>> Reject: χ^2 (3, n = 8) = 13.33, p < 0.01
Informative presentation of causes / causal scenarios	FOUR choices	>> Reject: χ^2 (3, n = 8) = 13.33, p < 0.01
Informative presentation of minimizing procedures / considerations	FOUR choices	
Informative presentation of corrective actions	FOUR choices	
Traceability of causes / causal scenarios to hazards / behaviors	FOUR choices	>> Reject: χ^2 (3, n = 8) = 13.33, p < 0.01
Traceability of minimizing procedures / considerations to causes / causal scenarios	FOUR choices	>> Reject: χ^2 (3, n = 8) = 8.67, p < 0.05
Which of the Safety Plans would you consider the MOST Implementable?	TWO choices	>> Reject: χ^2 (1, n = 8) = 4.50, p < 0.05
Ease of performing the hazard analysis	FOUR choices	
Ease of constructing the safety plan document	FOUR choices	
Ability for the format and information in the document to be used as a template for future documents	FOUR choices	
Easy to teach the method to someone	FOUR choices	
Perceived ability of analysis outputs to inform risk mitigation activities during test planning	FOUR choices	>> Reject: χ^2 (3, n = 8) = 9.33, p < 0.05
Perceived ability of analysis outputs to aid pre-mission briefs	FOUR choices	
Perceived ability to implement changes to the safety planning as lessons are learned during test activities	FOUR choices	>> Reject: χ^2 (3, n = 8) = 9.33, p < 0.05
What do you like the best about each method?	Short answer	
What do you like the least about each?	Short answer	
How much time would you recommend to someone for learning the basics of each?	Short answer	
Which method would you prefer to use for your next test project, and why?	Short answer	
Do you have any suggestions for the formatting and information ordering in the STPA planning document?	Short answer	
Additional Comments	Short answer	

Where STPA Shone

Results

INTELLIGIBILITY: *generally inconclusive*

- Consistency of formatting
- Easy to understand what portions of the system are being evaluated
- Easy to understand what portions of the system are part of the test framework

INFORMATIVENESS: *systematic STPA preference in general*

- Hazards clear
- Hazardous behavior (UCAs) clear
- Traceability between hazardous behavior and hazards
- Traceability between mitigations and hazards

IMPLEMENTABILITY: *systematic STPA preference in general*

- Ability to use the method to identify mitigations
- Ability to implement changes to safety plan as lessons are learned

Short Answer Responses

Results

	Traditional	STPA
+	<ul style="list-style-type: none"> • It is <u>more familiar</u> and hence more comfortable • It is <u>fast and convenient</u>, especially from reusing of old planning documents to aid in writing new ones • Test hazards, as defined traditionally, are test-specific and easy to brief and keep in mind during a mission • Easier for decision-makers to visualize test-specific hazards and <u>qualify risk</u> 	<ul style="list-style-type: none"> • Investigates contributions to hazards inherent in the <u>entire system</u> (not just items under test); better for determining <u>true risk</u> • <u>Description of the system</u> and boundary are more <u>accurate</u> and explicit, and the distinction between accidents and hazards is clearer • The structure is <u>more straightforward and easy to follow</u>, and traceability of hazardous behaviors and mitigations is built-in
-	<ul style="list-style-type: none"> • It encourages <u>laziness</u> in the analysis <u>without a full understanding</u> of the system, due to the ease of copying old safety plans as well as <u>duplicating test-hazard sheets</u> and mitigating procedures • It <u>relies on experienced reviewers</u> to catch any holes that were missed by planners • During mission briefings, repeated reviews of multiple test-hazard sheets with <u>overlapping information</u> tends to cause practitioners to tune the information out • It is unclear what belongs in the technical plan and then the safety plan, often resulting in <u>repeated information</u> in both 	<ul style="list-style-type: none"> • It requires an intricate control analysis and <u>more time to perform</u> appropriately • It can be difficult to navigate for larger projects with a wealth of information, especially with the traceability expressed as parenthetical references • It requires <u>more management involvement</u> in terms of system definition, standardization of terms and formats, maintenance of repositories, and teaching of the new method

Limitations

Results

Author's Analysis

- Dissimilar access to simulators, technical data, and designer input
- Traditional approach is not as formal as those usually examined for comparisons

Survey Study

- Non-parametric (lack of statistical power) – 8 participants
- Volunteers recruited by convenience; no exact match to population demographic
- Predisposition/apprehension
- Demand characteristic potential; no blinding possible (single or double)

Take Aways

Results

- STPA planning document 40 percent longer than traditional
- 60 percent of the language in the STPA document was original
- 60 percent of the minimizing procedures in the STPA document were original
- 300 percent more time invested (STPA) yielded 330 percent more mitigations
- STPA mitigations were organized by influences, presets, and operating procedures
...while traditional mitigations were organized by scenarios (and can repeat)
- Two types of issues found with STPA that affect system in the *field*
 - *Some data-entry interfaces were not optimal*
 - *Lack of feedback to lead's pilot that wingman had received certain commands*
- STPA requires paradigm adj (e.g., control structure and re-ordered mitigations)

Questions?



<http://stealth-ai.wikia.com/>

Backups

Event Chain Model

Motivation

TEST SAFETY

Cause → Hazard → Mishap

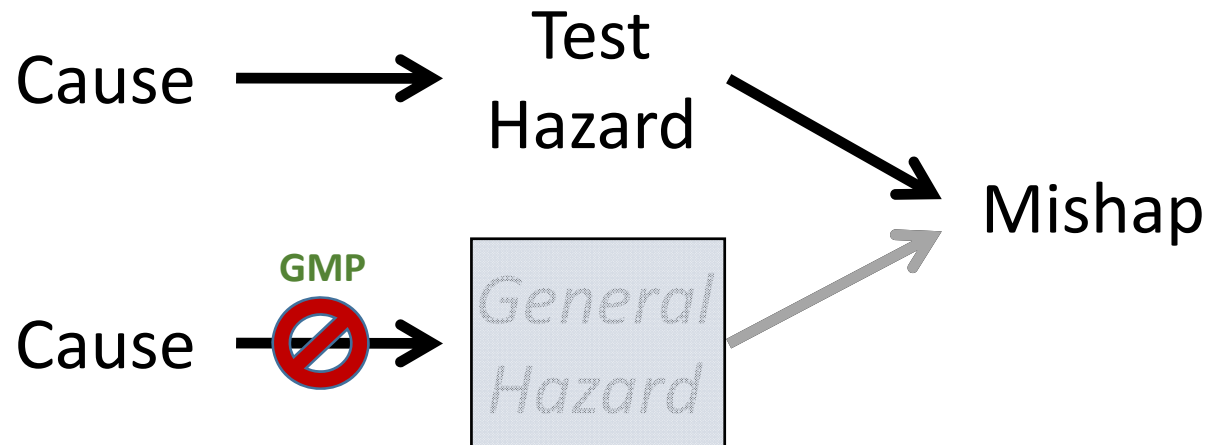
PROBABILISTIC RISK ASSESSMENT (PRA)

1. Identify hazards that precede mishaps
2. Determine consequences of each mishap (e.g., I, II)
3. Build chain(s) of causality for each hazard (root cause analysis)
 - Event Trees, Fish Bones, etc.
4. Determine mishap probability
 - *Calculated*: Fault Tree Analysis, (FTA), Failure Mode and Effects Analysis (FMEA)
 - *Estimated*: Preliminary Hazard Analysis (PHA), Test Hazard Analysis (THA)
5. Apply mitigations (when applicable) and update probability
6. Put an X on the risk chart

Event Chain (Test)

Motivation

TEST SAFETY



General Hazards

No specific identification of general hazards or causes

No mishap reference

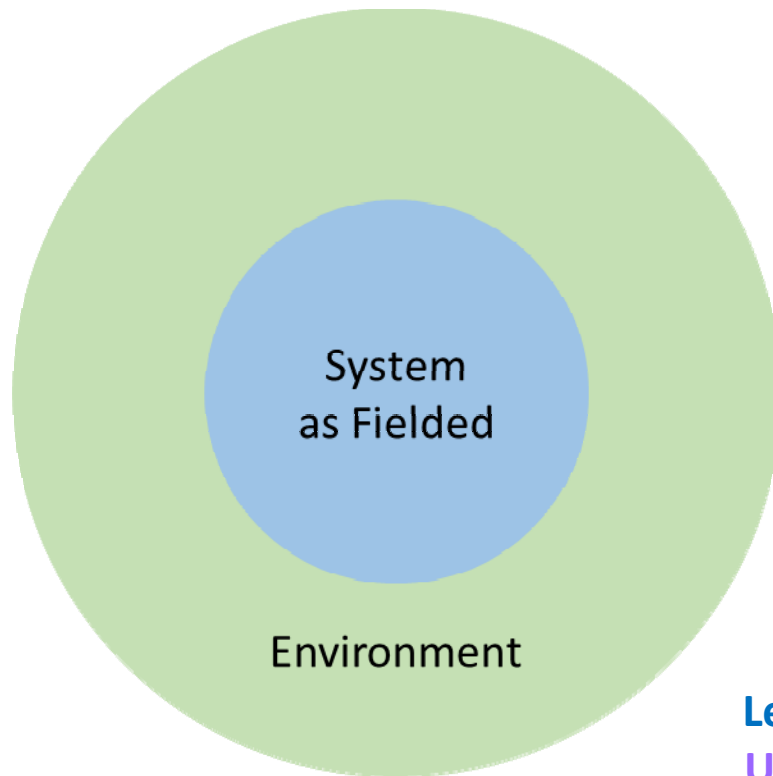
General Minimizing Procedures (GMP)

- Directives / Considerations
- Can be pre-mission or during operations

Ends there (no corrective actions)

Systems View

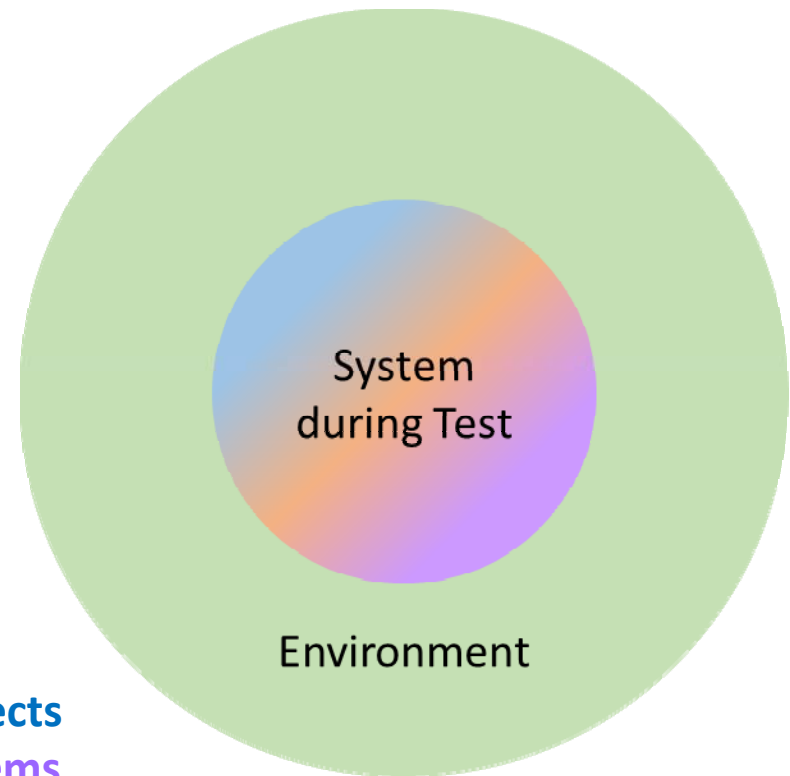
Work



Environment

System
as Fielded

Legacy Aspects
Updated Items
Test Framework



Environment

System
during Test

Modern

Systems Perspective

Work

Hazard → Mishap

System Boundary

SYSTEM

ENVIRONMENT

Identify Accidents (Mishaps)

Work

An undesired or unplanned event that results in a loss, including a loss of human life or human injury, property damage, environmental pollution, mission loss, etc.

Organizational Stakeholders establish these

- A1: Ground personnel are killed or injured
- A2: Ground assets are damaged or destroyed
- A3: Flight personnel are killed or injured
- A4: Flight assets are damaged or destroyed
- A5: Asset enters prohibited airspace or range
- A6: Test data are lost or destroyed

SYSTEM

ENVIRONMENT

Hazards, Not “Test” Hazards Work

Hazard Analysis is the heart of any system safety program

Hazards are specific insofar as the domain / industry / technology sector

Hazards should not be design- or test*-specific

**unless testing a brand new technology that cannot be generalized by other hazards*

Identify Hazards

Work

A system state or set of conditions that, together with a particular set of environmental conditions, will lead to an accident.

Safety Office standardizes these

H1: Aircraft violates minimum separation distance to other flying objects (A1-A4, A6)

H2: Aircraft violates terrain closure limits (A1-A4, A6)

H3: Aircraft departs aerodynamically stable flight (A1-A4)

H4: Aircraft exits allowable testing area (A5, A6)

SYSTEM

System B

ENVIRONMENT

Traditional “Test” Hazards

All THA worksheets as of June 2014

30%

System
Behavior

40%

Hazard

30%

Mishap

Loss of landing gear steering
Ice buildup on control surfaces
Inadvertent activation of [item]
Display failure
Wrong procedure used
[Test item] fails
Electrical bus fails
Flameout

Exceeding structural limits
Overheating
Exposure to laser / radiation
Exposure to chemicals
Approach/depart a boundary
Deep stalls / Loss of control
Degraded flying qualities
Hung or loose stores

Midair collision
Collision with ground
Collision with people
Weapon impacts outside range
Explosion
Structural failure
Test item destruction
Physiological incident

Updated Inclusion Criteria

- 1) Is the actor/entity/component responsible for or involved in defining requirements, criteria, and metrics for test enterprise capabilities and test-project schedule priority?
- 2) Is the actor/entity/component capable of influencing the allocation of resources (e.g. funding, staffing) throughout the enterprise?
- 3) Is the actor/entity/component capable of hiring/firing controllers within the system?
- 4) Is the actor/entity/component responsible for enforcing schedule pressure, budgets, and/or resource requirements (especially safety requirements) for systems during test?
- 5) Is the actor/entity/component responsible for defining test standards, practices, and processes (especially safety-related standards and processes)? If so, does it have enforcement power?
- 6) Is the actor/entity/component capable of changing the requirements, standards, procedures, or waivers for test operations or influencing others to do so?
- 7) Does the actor/entity/component perform a significant amount of work on activities such as safety analyses, system maintenance, system integration, and/or quality assurance?
- 8) Is the actor/entity/component responsible for, or heavily involved in system modifications for test?
- 9) Is the actor/entity/component responsible for, or heavily involved in, system certification renewal or review?
- 10) Does the actor/entity/component have the authority to request a delay or stop in production when problems arise?
- 11) Is the actor/entity/component an important contractor of the system, providing a significant portion of the system hardware or technical and operating personnel?
- 12) Would the actor/entity/component be impacted in the event of an accident?

Dulac, 2007
Stringfellow, 2011

Proposed Plan Format

Work

I – Planning Summary

1. Summary of Changes (if not initial)

2. Overview of Findings

test objectives / methods / techniques

of hazards

of scenarios

of minimizing procedures (MPs)

hazard corrective actions (HCAs)

mishap recovery actions (MRAs)

3. Remarks

Proposed Plan Format

Work

II – Project Description

1. Background
2. Mishap Responsibilities
3. Test Objectives

Proposed Plan Format

Work

II – Project Description (continued)

4. Description of System

- *System Model (Control Structure)*
- *Updated Items*
- *Legacy Aspects: Modifications / Configurations*
- *Test Facilities / Test Instrumentation (Framework)*
- *Control Discussion*
 - *Control modes*
 - *Required and Desired Assets and Channels*

5. System Maturity / Limitations / Readiness

6. Predicted / Expected Results

Proposed Plan Format

Work

III – Safety Implementation

1. Safety Requirements

Accidents, Hazards

2. Types of Tests*

Aspect being evaluated

Methods / Techniques

Expected Results

Hazardous Behaviors (UCAs, scenarios)

**Include an entry for transitions between test points*

Proposed Plan Format

Work

III – Safety Implementation (continued)

3. Safety Mitigations

MINIMIZING
PROCEDURES

System Notes and Restrictions

Testing Restrictions

Developing Influences

Shift Presets

Operating Procedures

Hazard Corrective Actions

Mishap Recovery Actions

Pre-Mission Influences

Work

