Systems Theoretic Process Analysis STPA

Developing, Fielding, and Sustaining America's Aerospace Force Safely

STPA Applied to the Air Force Test Safety Process

Capt Michael "T-Rex" Tibbs
419th Flight Test Squadron

Mr. Lowell Bishop
412th Test Wing Test Safety

U.S. AIR FORCE

DISTRIBUTION A
Approved for public release
Distribution is unlimited
412TW-PA-18578

Edwards AFB, CA
9 October 2018

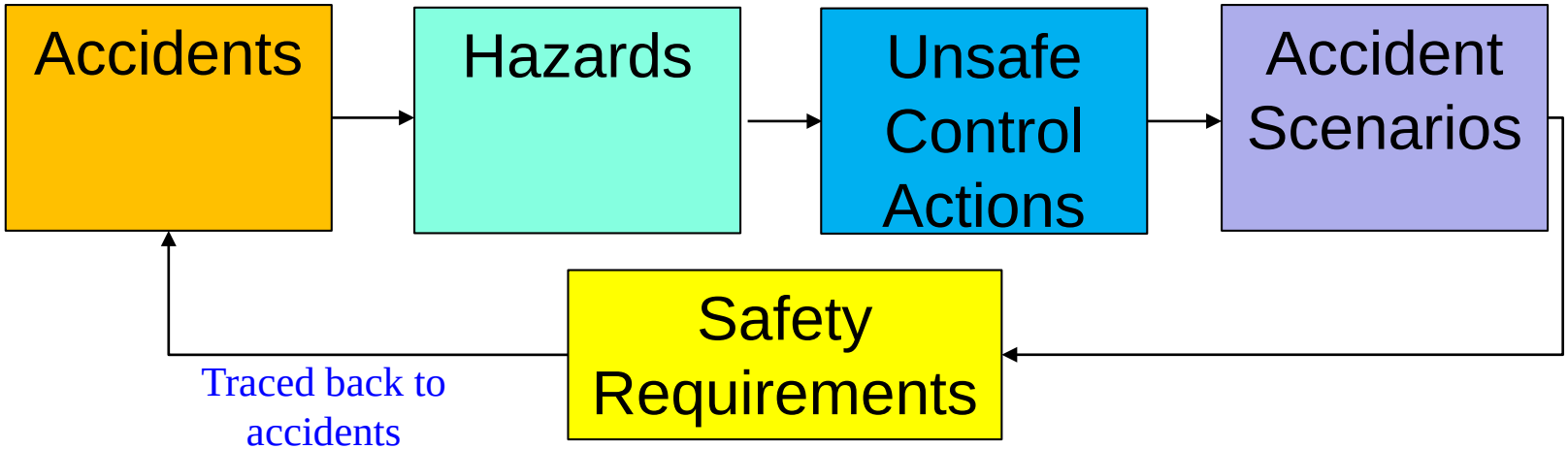
Integrity - Service - Excellence

Overview

- STPA Introduction
- AFTC Trials
- Spoiler Alert!
- STPA Example: B-1B Software Block
- STPA in DoD Acquisition
- STPA Early
- Where are we going?
- STPA Limitations
- STPA Strong Points

STPA Introduction

- Hazard Analysis Technique
- Traceable Mitigations
- Top-down Systems Engineering Approach
- Approach based on control and feedback
- Result = Traceable Safety Requirements



STPA Introduction

Basic Process:

1. Define the system (drives scope of effort)
2. Identify system accidents/hazards
   a) Undesired & Unintended Effects
3. Draw functional control structure
4. Identify unsafe control actions
5. Identify accident scenarios (context)
6. Create Design & Safety Requirements or Constraints

Air Force Test Center (AFTC) Trials

- Hardware Based
  - Edwards F-16 Composite Stabilator
  - Eglin A-10 Wing Loads
- Human Systems Integration
  - Edwards C-17 Pilot Workload
- SW/HW based
  - Edwards B-1B Software Sustainment
  - 704 Test Group Mag Lev Rocket Sled Track
  - Eglin Countermeasures
- Lab/Facility
  - Arnold Alternate Fuel Test, Diffuser Project, Remote Oil Sampling

Spoiler Alert!

- Not a replacement for current process
- Did not identify large gap in traditional test safety planning methods
- STPA could be very powerful and useful, **IF** performed early enough to influence system design and test requirements
  - Expected to be most useful for New Capabilities and Complex Systems

STPA Example: B-1B Software Block (SB)

- Targeting Pod Testing
- Weapons Testing
- Radar Testing
- Datalink Testing

- Communication/Navigation Testing
- Electronic Warfare
- Human Systems Integration

The System Boundary

1. **STPA team became familiar with project**
   - How in-depth does the project need to go?
   - How has the system changed?
   - What are the types of tests?

System Boundary for this test:
Stops at Aircraft and Aircrew

Best choice in hindsight?
Consider: Chase, Control Room, Range?

ID Hazards and Accidents (Mishaps)

Accidents

A1: Loss of life/injury to people
A2: Loss of aircraft
A3: Loss of test asset
A4: Loss of mission

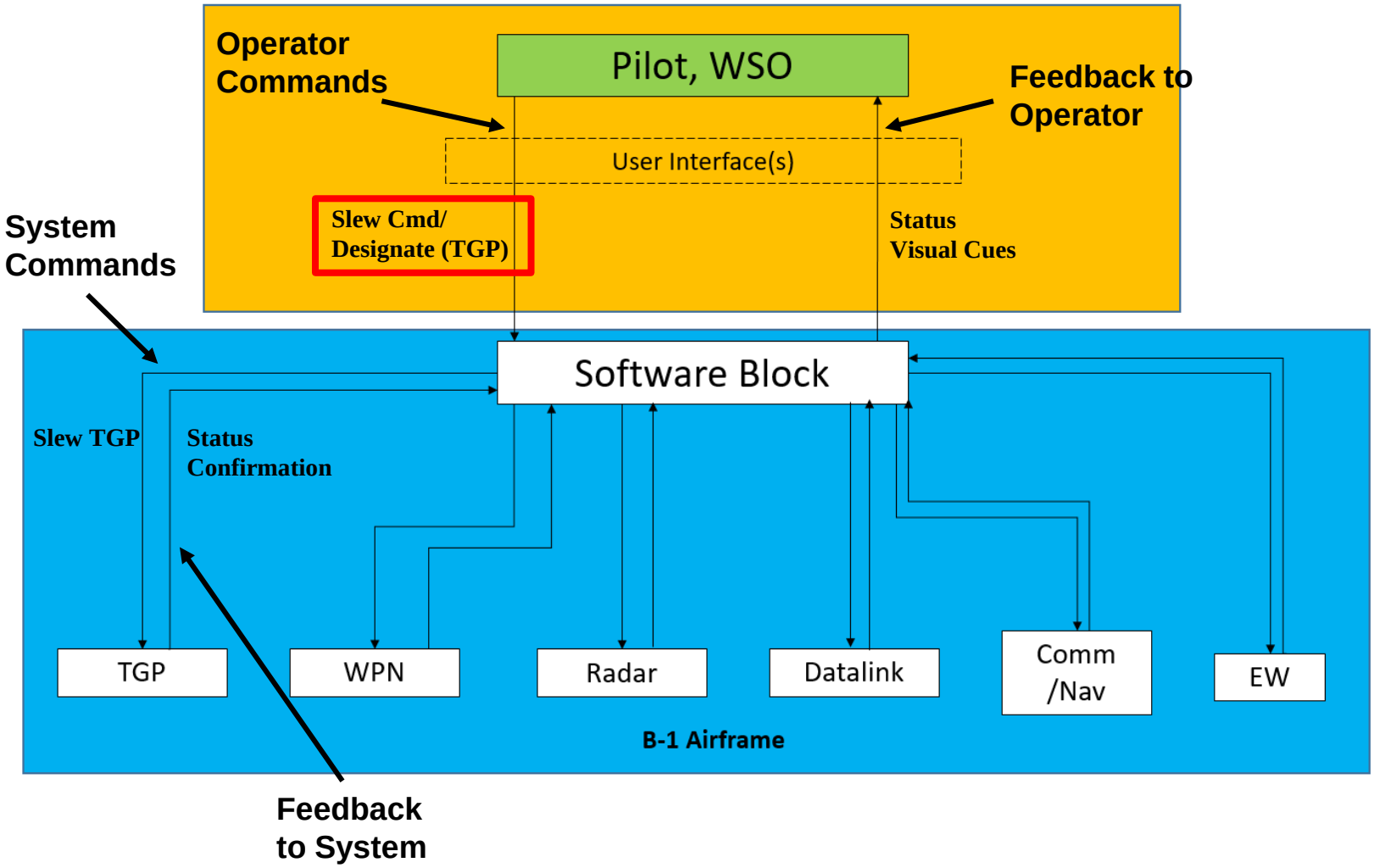
Hazards traceable to accidents

Hazards

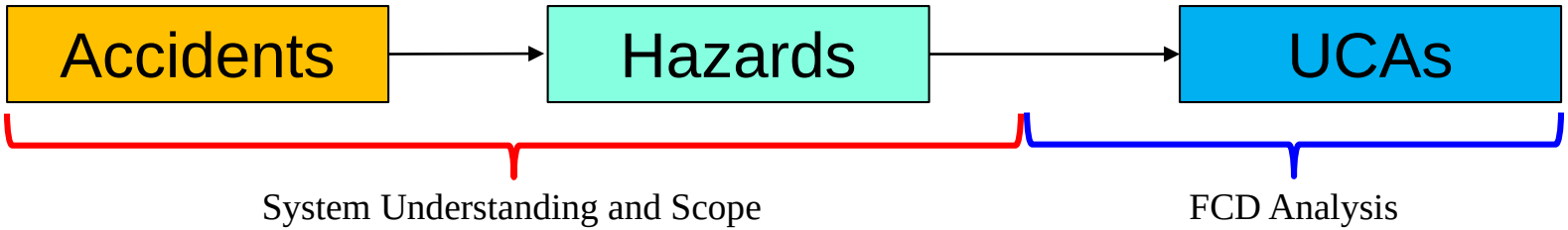
H1: Weapon/Flare/Chaff Impacts wrong place (A1, A2, A3)
H2: Unsafe weapon separation (A1, A2, A3)
H3: System damages aircraft/test asset (A2, A3)
H4: Exceeds minimum aircraft separation (A1, A2, A3)
H5: Exceeds altitude limits (A1, A2, A3)
H6: Exceeds human health limits (A1)

STPA IDs hazards in the beginning resulting in generic, non-test unique hazards with test unique causes
→ **High order hazards drive detailed analysis**

Functional Control Diagram (FCD)



Unsafe Control Actions (UCAs)



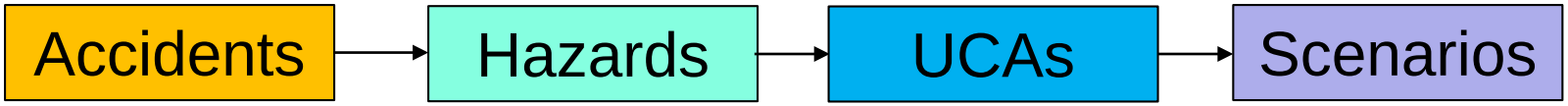
UCAs created for every hazard, controller and command!

UCAs have four categories:

1. Not providing the control causes hazard
2. Providing the control causes hazard
3. Incorrect timing/order of control causes hazard
4. Control applied too long or too short causes hazard

Hazard	Controller	UCA	Not Provide	Provide	Early/Late/ Wrong Order	Too Short/ Too Long
H1: Weapon/Flare/Chaff Impact Wrong Place	Operator	Slew Cmd/Designate (TGP)	1. Operator does not provide slew command while weapon is in transit. 2. Operator does not provide laser (designate) while weapon is in transit.	3. Operator provides erroneous slew command while weapon is in transit. 4. Operator provides designate command while in poor environmental conditions.	5. Operator provides slew command too late while weapon is in transit. 6. Operator provides designate command too late after weapon is in transit.	7. Operator provides designate command too short for proper target parameters.

Accident Scenarios (Causes)

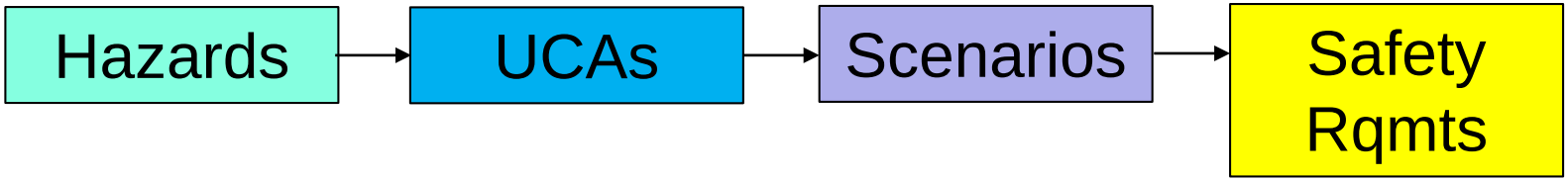


- UCAs now exist for every hazard, controller, and command combination
  - Can **scenarios** be thought of where a UCA would actually occur?
  - Can two "uninformed smart people" really come up with all the scenarios?

Not Provide	Provide	Early/Late/ Wrong Order	Too Short/ Too Long	Scenarios (Causes)
1. Operator does not provide slew command while weapon is in transit. 2. Operator does not provide laser (designate) while weapon is in transit.	3. Operator provides erroneous slew command while weapon is in transit. 4. Operator provides designate command while in poor environmental conditions.	5. Operator provides slew command too late while weapon is in transit. 6. Operator provides designate command too late after weapon is in transit.	7. Operator provides designate command too short for proper target parameters.	1. Operator beileved he was moving the TGP toggle but it was not due to TGP functionality 2. Operator beileved he was pulling the trigger but was not so no lasing occurred 3. same as 1 4. Operator beileved that the environmental conditions were good enough to lock a target, but it was not. 5. Operator believed there was enough time remaing during fliyout for weapon to acquire/reach target 6. Operator releases weapon while lasing, becomes distracted with another task (quits lasing), then renegages lasing 7. Operator pickled too early before weapon process model could update parameters from lasing, causing a large miss distance

Traceability of Scenarios back to UCAs

SB STPA Methodology: Safety Rqmts (Minimizing Procedures)



- What safety requirements are needed to mitigate the scenario?
- Two kinds of safety requirements:
  - Design (D) → Design Change? Regression Tests?
  - Test (T) → What we consider minimizing procedures

Scenarios (Causes)	Safety Rqmts/Constraints
1. Operator beileved he was moving the TGP toggle but it was not due to TGP functionality 2. Operator beileved he was pulling the trigger but was not so no lasing occurred 3. same as 1 4. Operator beileved that the environmental conditions were good enough to lock a target, but it was not. 5. Operator believed there was enough time remaing during fliyout for weapon to acquire/reach target 6. Operator releases weapon while lasing, becomes distracted with another task (quits lasing), then renegages lasing 7. Operator pickled too early before weapon process model could update parameters from lasing, causing a large miss distance	1. (D) Ensure visual feedback of TGP cursor location 2a. (D) Ensure laser detent is acceptable and visual feedback exists for lasing and not lasing 2b. (T) Other Aircrew and MCR personnel ensure proper TGP visual displays are shown during test 4. (T) Ensure environmental conditions are appropriate for respective TGP tests 5. (D) Ensure flyout (TTG) timer is visually displayed to operator 6. (T) Ensure other aircrew and MCR personnel are backing up operator to reduce workload with secondary tasks 7. (T) Have operator wait X seconds after lasing, but before pickling to ensure weapon parameters are updated

Traceable safety requirements mitigate the hazard!

SB STPA Metrics

- Analysis performed on the side in parallel with actual job duties
- Time for pre-safety review board: ~ 80 hrs
  - # of Hazards: 6
  - # of mitigations: 39
- STPA not designed to assess risk, must use current method
- STPA does not discuss corrective actions after a hazard has occurred (future growth?)

Current method takes ~ 8-16 hrs

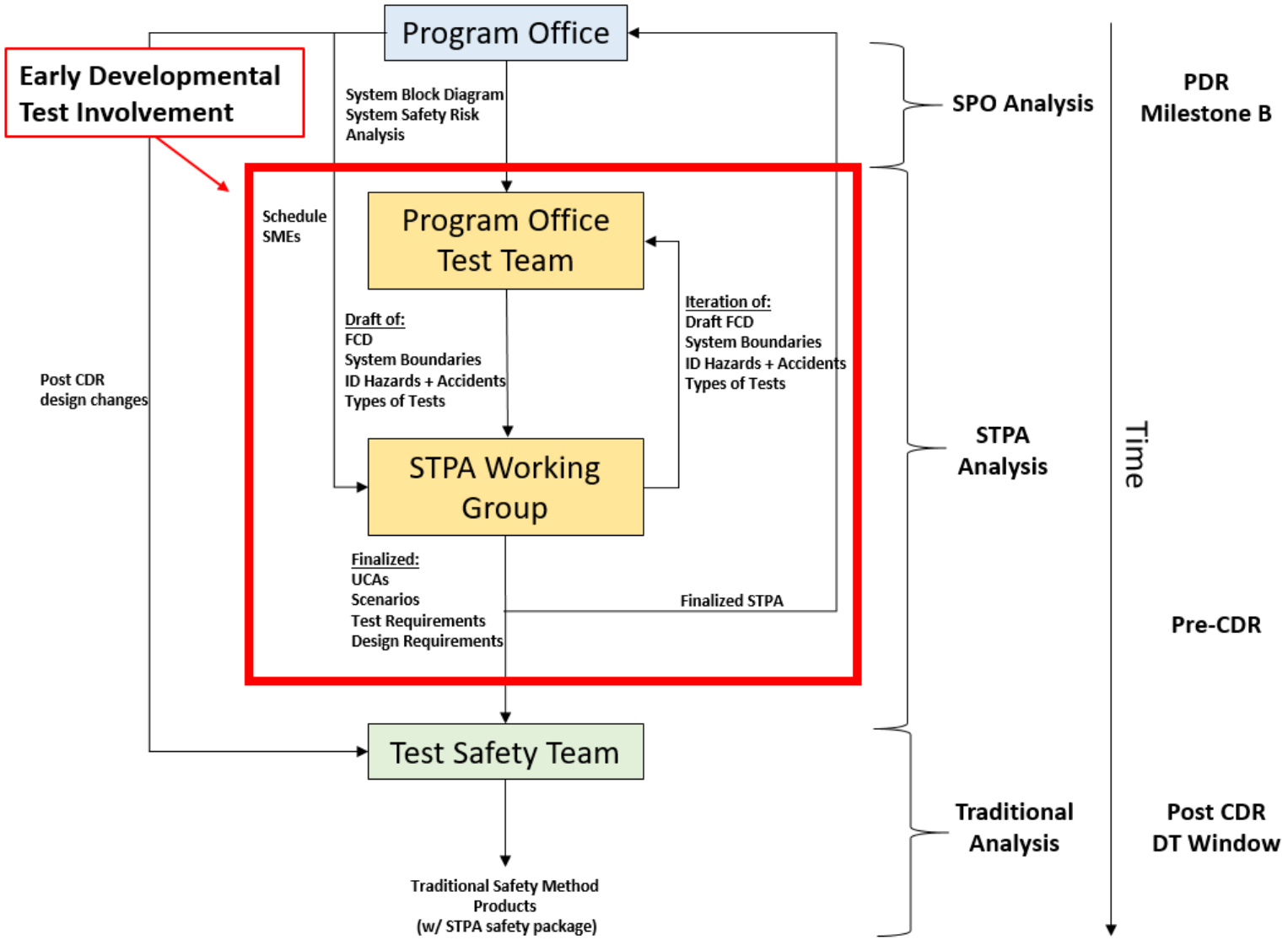
<u>Current method produced similar results in less time!</u>

- B-1 SB has been done many times before…
  - May not be the case for all projects…

- What if we did STPA earlier in the acquisition timeline?

How about an example!

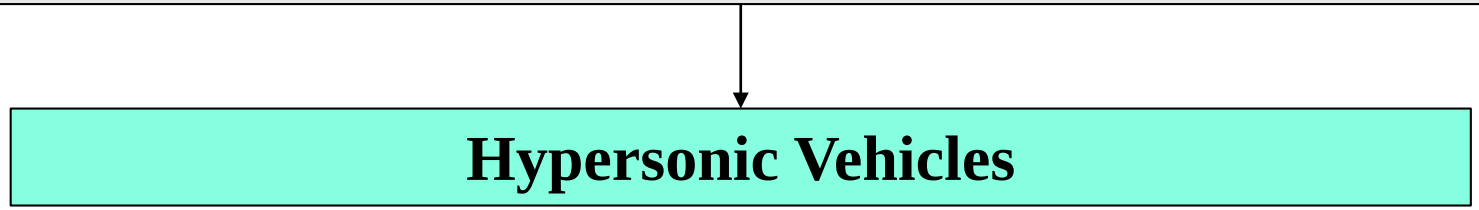
Where should STPA be in the acquisition timeline?



Benefits of doing STPA early

1. Influence system safety early in design
2. Streamline test and safety planning
3. Feed system safety and airworthiness
4. Aids in planning for “never before done” tests

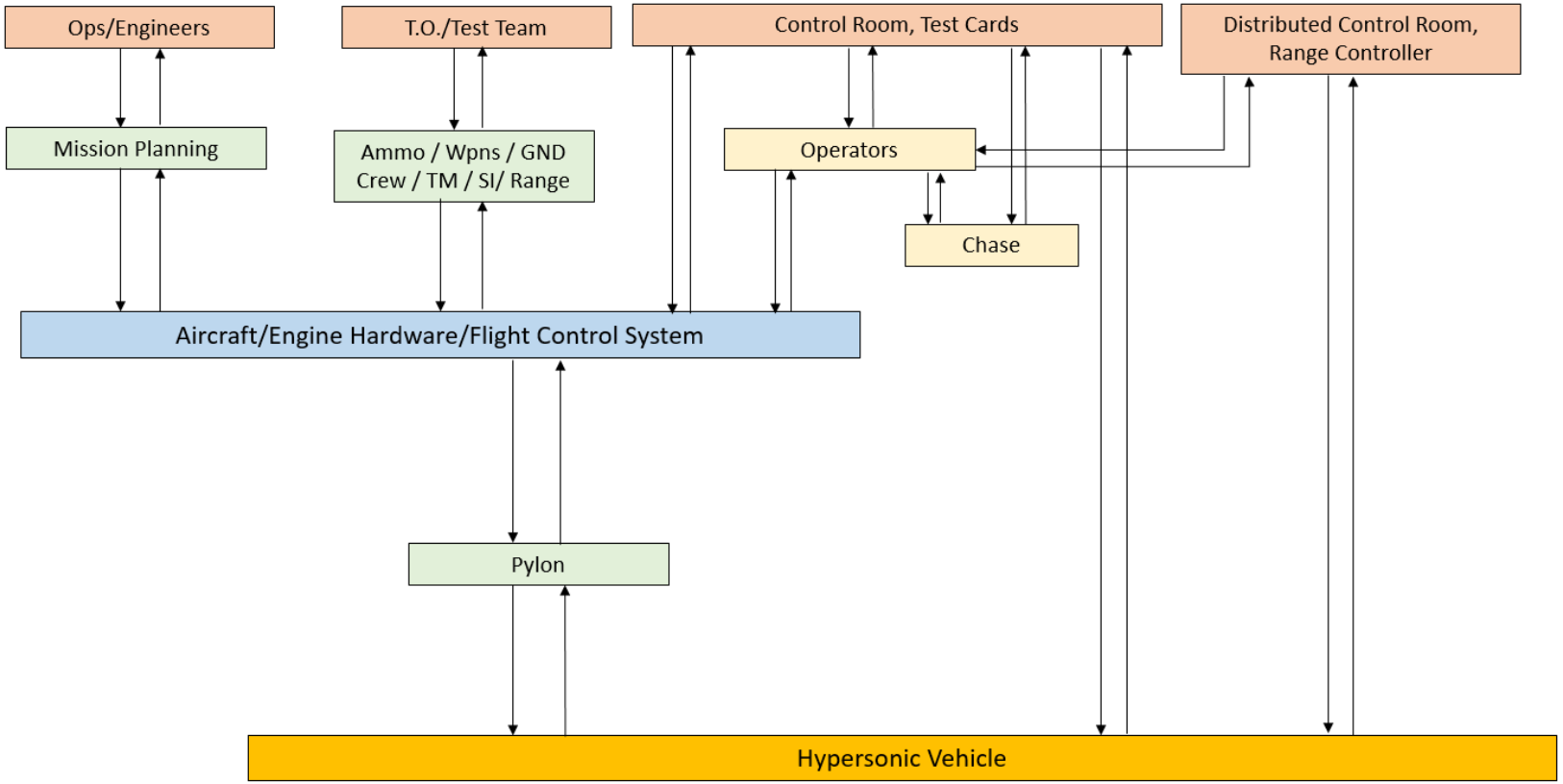
So where is the 412th TW going with this now?



Hypersonics STPA Flight Test System Boundary

- Aircraft + Aircrew
- Hypersonic Vehicle
- Governing Documents
- Pre-Mission Engineers and Ground Crews
- Range Control
- Mission Control
- Chase

Hypersonic Vehicle STPA Functional Control Diagram (FCD)



FCD represents an example hypersonic flight test
- **Built upon lessons learned from previous trials**
- **Hypersonic STPA Working Group!**

STPA Limitations

1. SPTA may not be as powerful without subject matter expert (SME) involvement
2. The FCD is the critical point in analysis
3. Extremely time intensive
4. STPA does not discuss corrective actions
5. STPA does not assess risk

STPA is not a form, fit, function replacement for the current 412th TW safety process!

But STPA had Strong Points!

1. Great traceability from mitigations to accidents
2. The FCD creates an easily understood model
3. No “completed” test plan required
4. STPA also found system design mitigations
5. May be useful for projects that are not well understood

STPA should be used early in the DoD acquisition process to influence system design as well as test safety

Thank You

- **Acknowledgments**
  - **Maj Daniel Montes, USAF TPS**
  - **Mr. Rey Enriquez, AFTC/SE**
  - **Maj Sarah Summers, 772 TS**
  - **Mr. John Thomas, MIT**
  - **Mr. Michael Kopriva, USAF TPS**