MIT's STAMP Research and STPA Applications

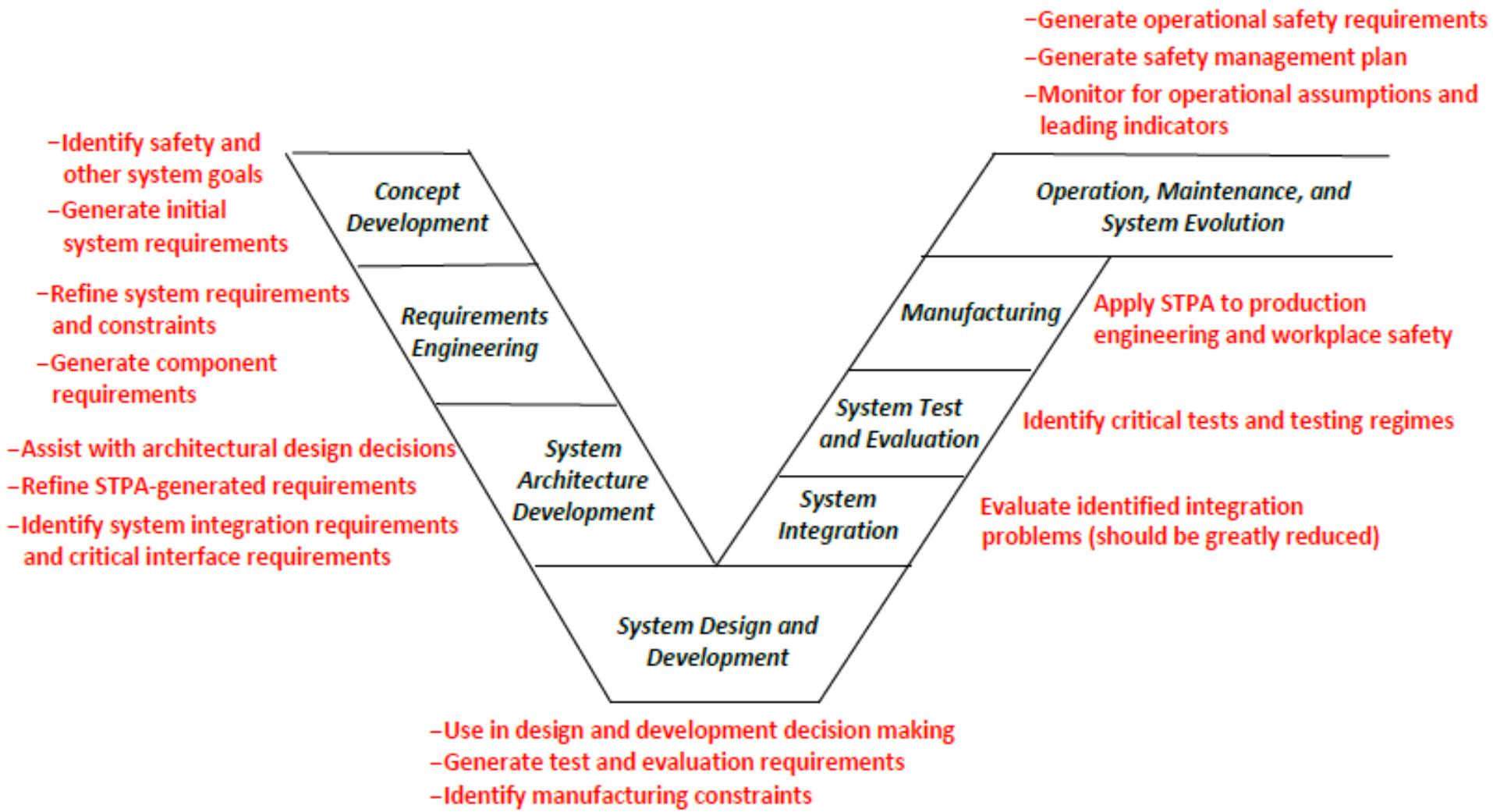
John Thomas

MIT

Some Advances Since Last Year

- Free STPA Handbook (Leveson and Thomas)
  - Free download from: mit.edu/psas
  - 9000 downloads since April 2018
  - Japanese translation available (thanks to JAXA engineers)
  - Translation into Chinese (in progress by CAUC)
- Integration of STPA into industry standards
- More tools to support STPA and its integration into system engineering (XSTAMP, SpecTRM, STAMP Workbench, RM Studio STPA Module) plus some proprietary ones
- New STAMP Conference planned for Brazil in 2020

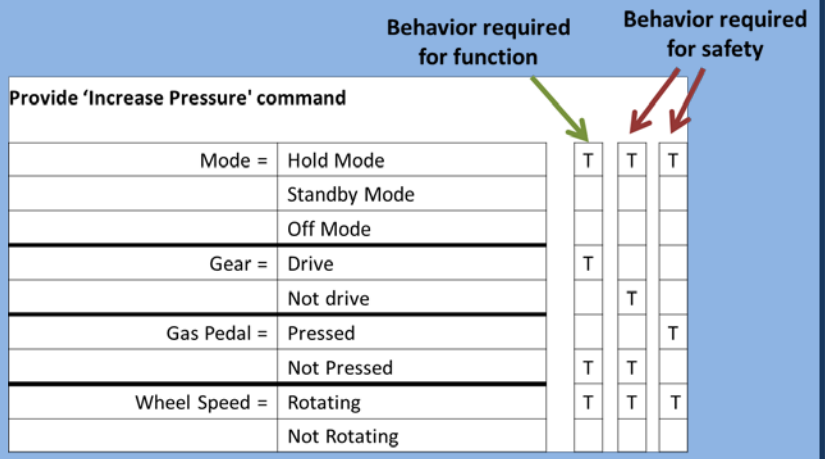
Use of STPA throughout development and operations

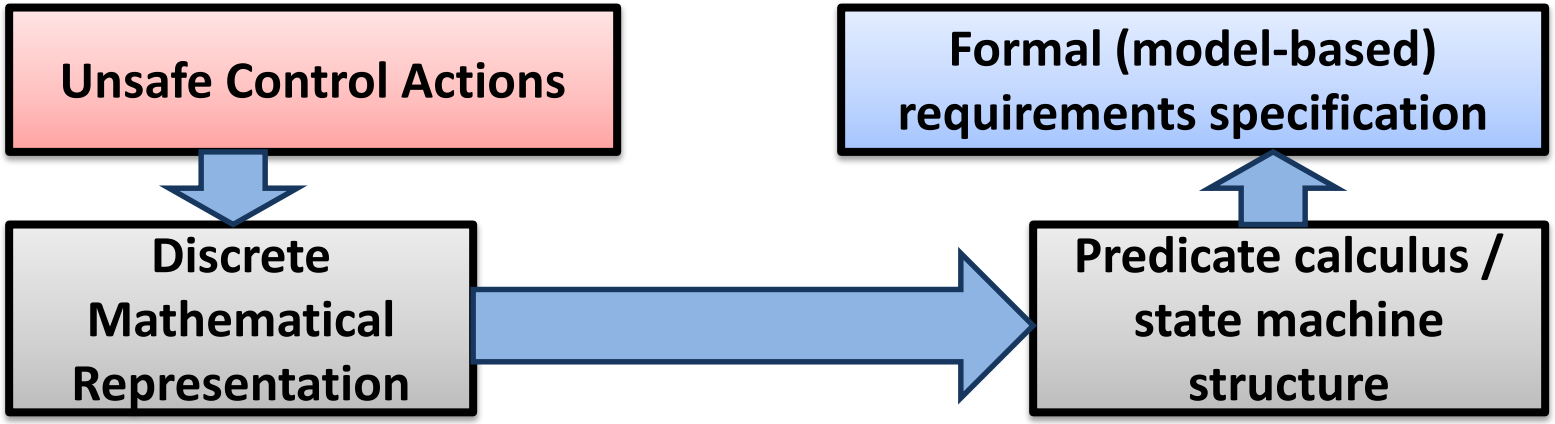


Generating executable requirements from STPA

Unsafe Control Actions
AH provides Increase Pressure command while wheels not rotating
AH provides Increase Pressure command while driver accelerating
AH provides Increase Pressure command too late (more than X sec) after wheels rotating
Etc.

Formal (model-based) requirements specification

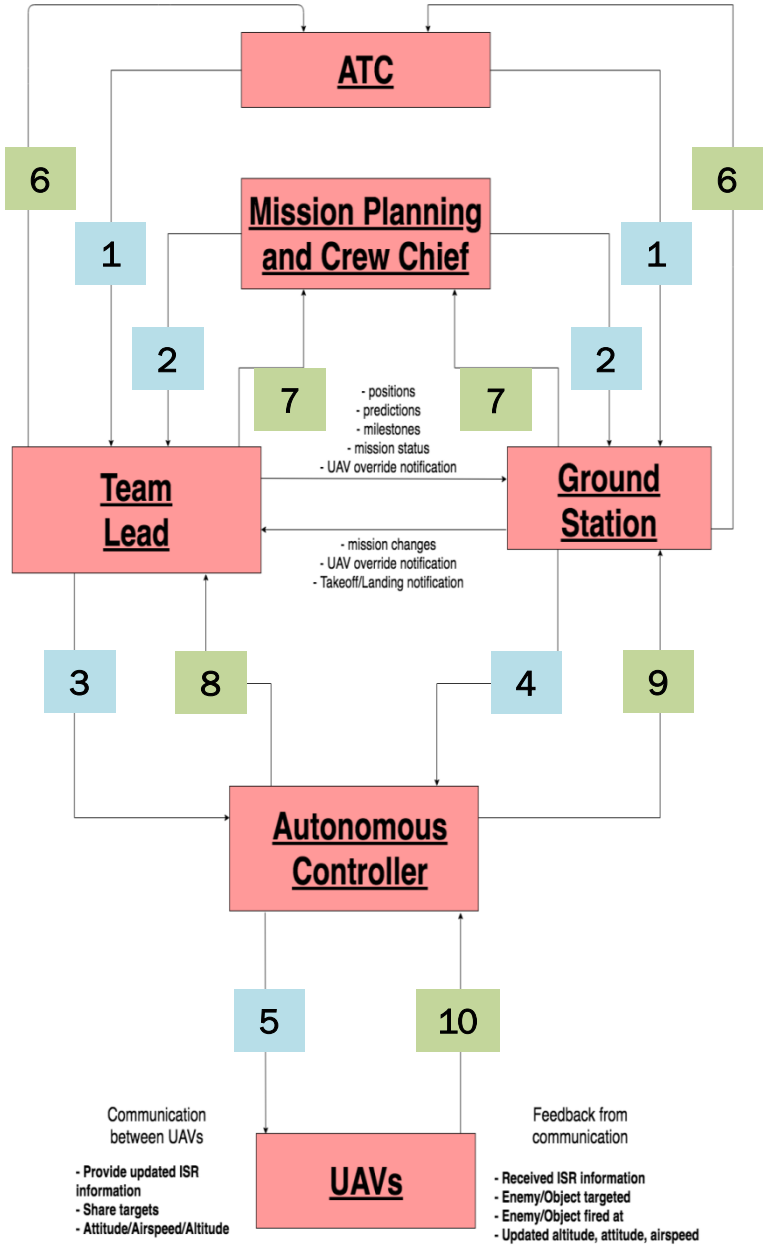




AFRL MUM-T Control Structure (UxAS)

Control Actions

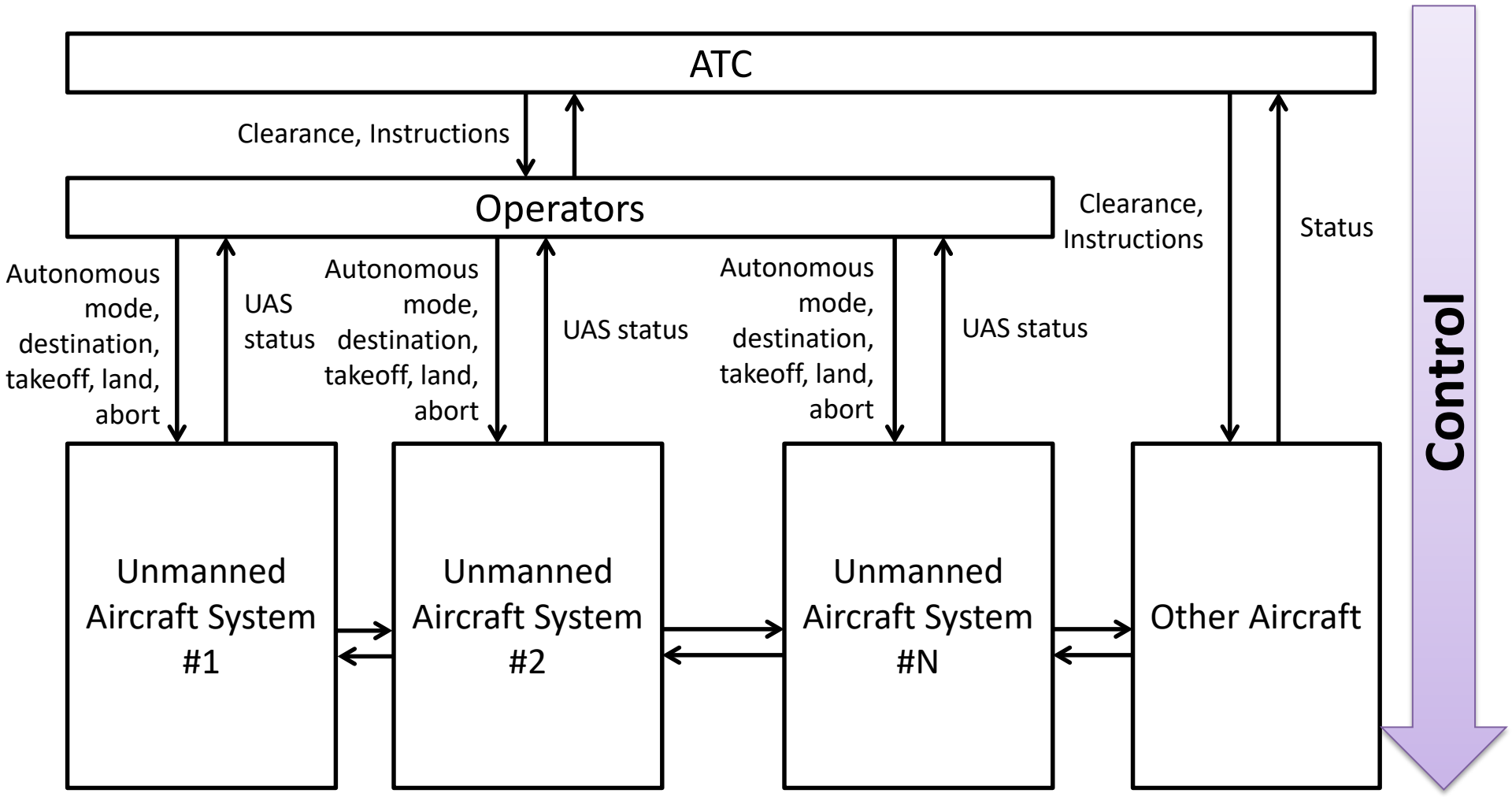
1	Grant clearance Issue ground operation Issue approach/departure instructions
2	Issue mission plan Issue updates/changes
3	Surveil a region Search for a target Identify/Assess target Track target Aim/Fix on target Fire at/Engage target Send formation command Send override command
4	Takeoff Land Send override command Send altitude command Send airspeed command Start engine Stop engine Turn on payload Turn off payload Apply lost link procedure
5	Change altitude Set throttle



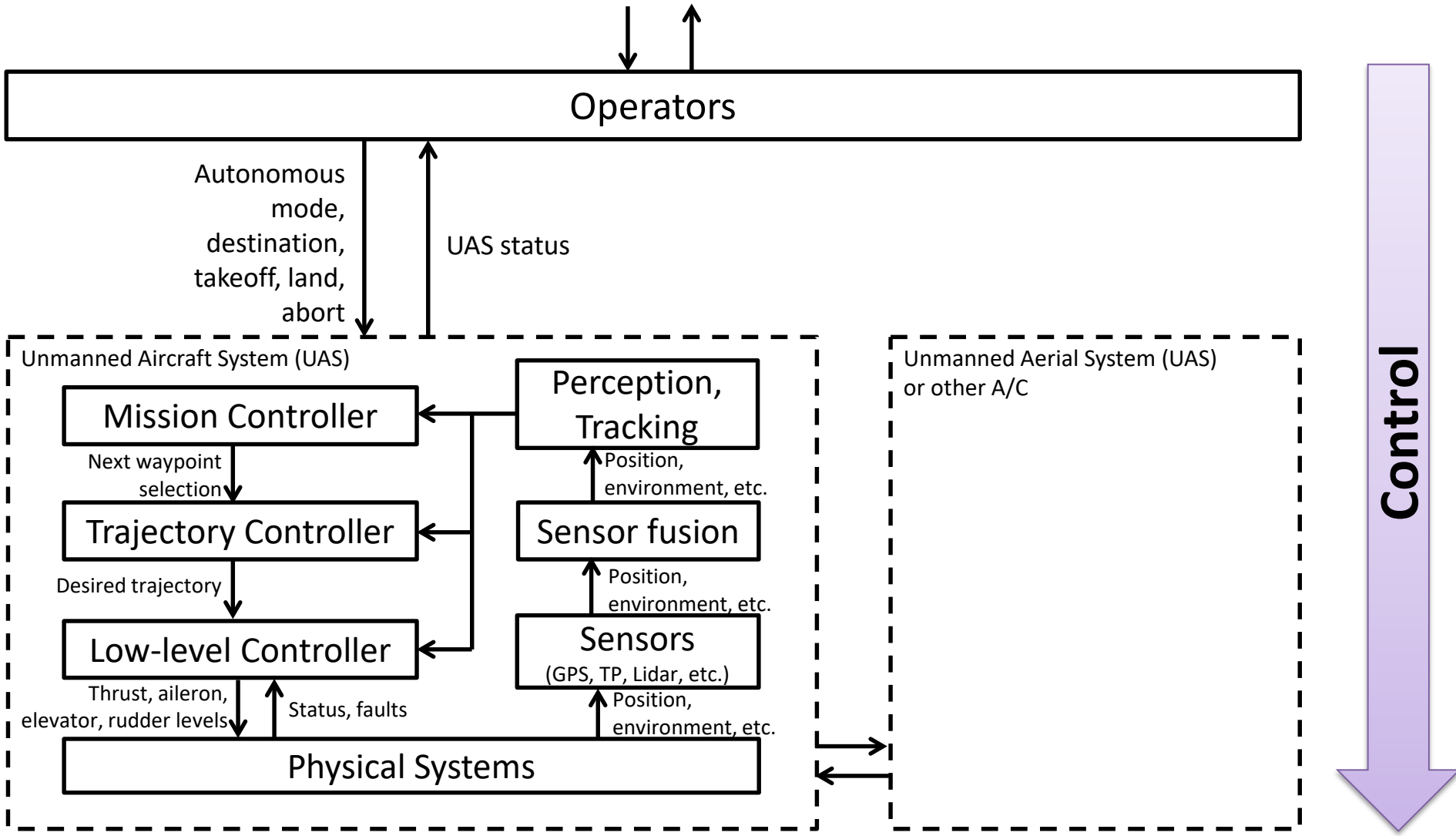
Feedback

6	Request takeoff/landing clearance Request ground clearance Confirm guidance/instructions
7	Mission Status
8	Visual Communication Checks Position Data Mission Progress Updates Waypoint destination Time to destination
9	Engine status Communication checks Current services status + warnings Mission Progress Updates Mission objectives Position Data Aircraft hardware status Waypoint destination Time to destination Unauthorized requests Lost link successful
10	GPS position Altitude Airspeed Fuel level Engine status Warnings/Cautions

UAS Concept


ATC
Clearance, Instructions
Operators
Clearance, Instructions
Status
Autonomous mode, destination, takeoff, land, abort
UAS status
Autonomous mode, destination, takeoff, land, abort
UAS status
Autonomous mode, destination, takeoff, land, abort
UAS status
Control
Unmanned Aircraft System #1
Unmanned Aircraft System #2
Unmanned Aircraft System #N
Other Aircraft

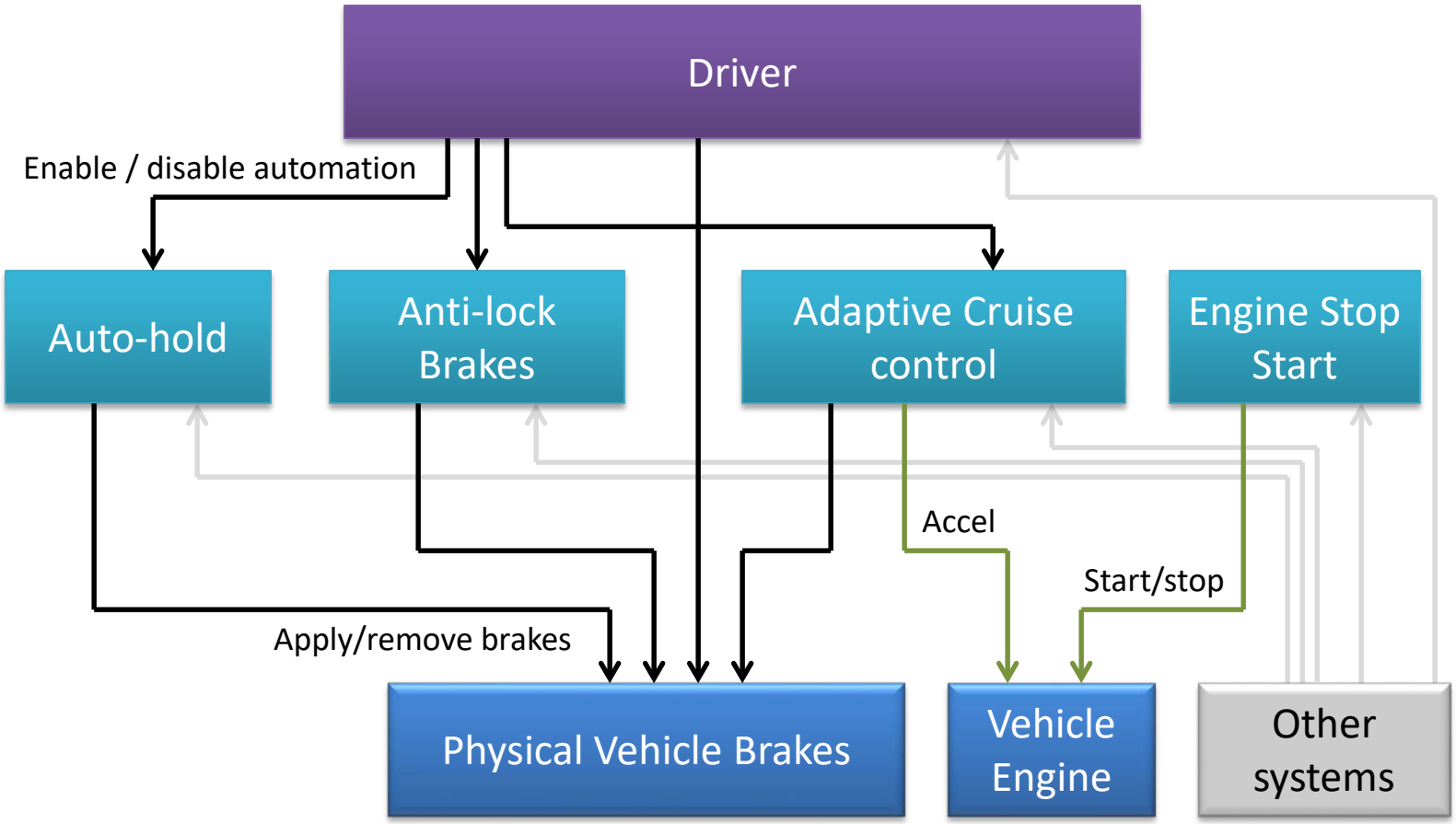
UAS Concept


Operators
Autonomous mode, destination, takeoff, land, abort
UAS status
Unmanned Aircraft System (UAS)
Mission Controller
Next waypoint selection
Trajectory Controller
Desired trajectory
Low-level Controller
Thrust, aileron, elevator, rudder levels
Status, faults
Physical Systems
Perception, Tracking
Position, environment, etc.
Sensor fusion
Position, environment, etc.
Sensors (GPS, TP, Lidar, etc.)
Position, environment, etc.
Unmanned Aerial System (UAS) or other A/C
Control

Is it Practical?

- STPA now being used in a large variety of industries
  - Automobiles (>70% use)
  - Aircraft and Spacecraft (extensive use and growing)
  - Air Traffic Control
  - UAVs (RPAs)
  - Defense systems
  - Medical Devices and Hospital Safety
  - Chemical plants
  - Oil and Gas
  - Nuclear and Electric Power
  - Robotic Manufacturing / Workplace Safety
  - Finance

Feature interactions



Example interaction:

Auto-hold applies brakes

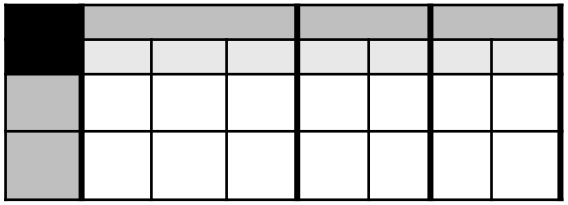
Engine-Stop-Start turns engine off

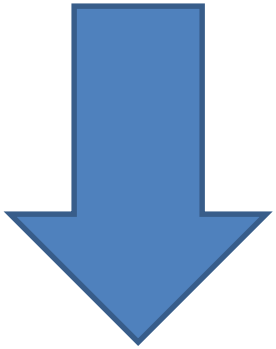
Driver exits vehicle

Brute force approach (incomplete)

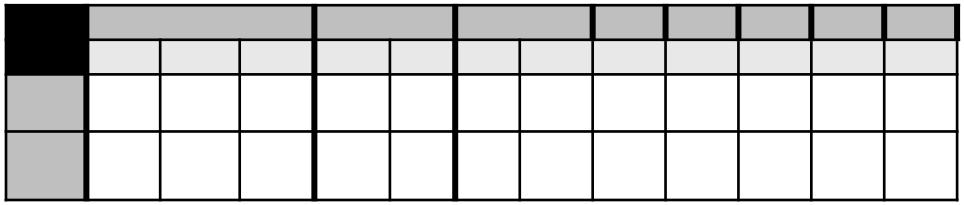
New STPA-based approach for feature interactions

- 3 controllers





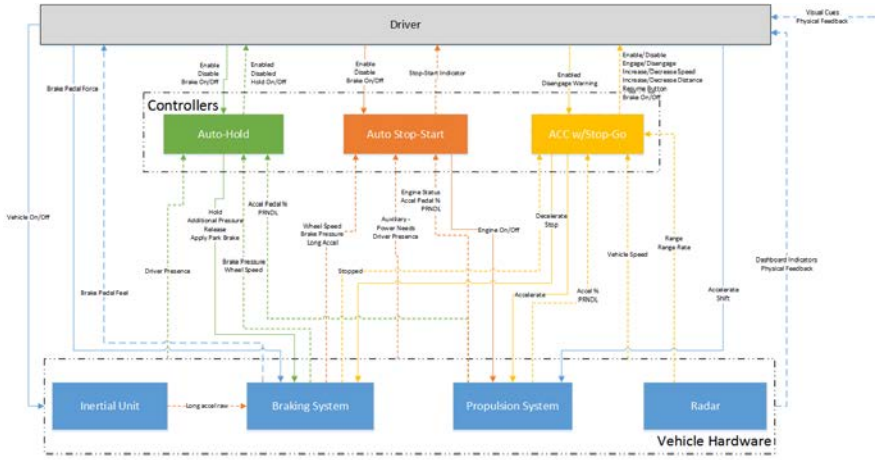
- 6 controllers



Systematically identifying conflicts (e.g. safety vs. regulation)

Context:

- Auto-Hold is holding vehicle
- ESS stops engine to save fuel
- Driver shifts to reverse
- Driver steps on gas to back up



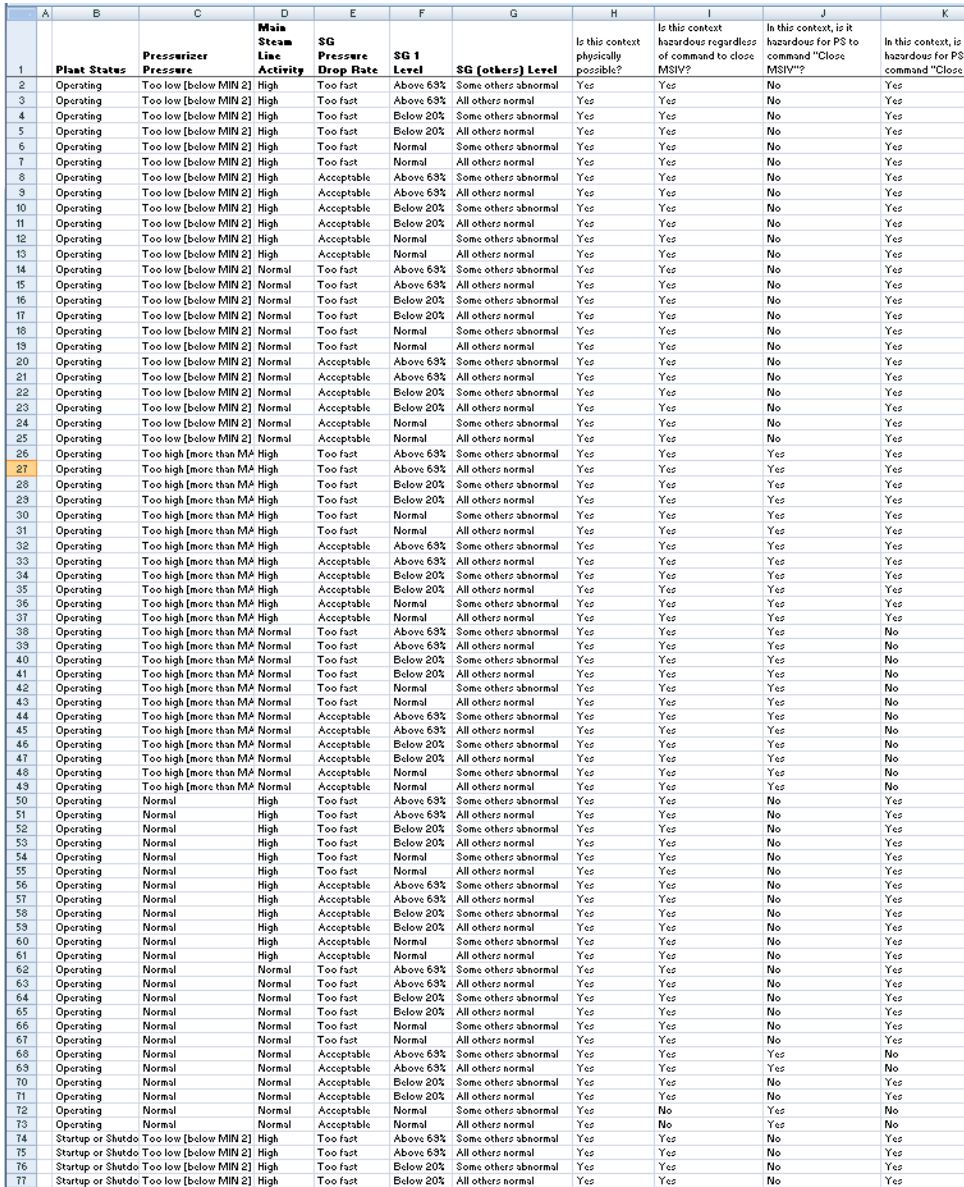
Problem:

- ESS cannot *Start* the engine (prevented by FMVSS 102)
- AH cannot *Release* (insufficient engine torque)

Potential Solutions / Requirements?

Managing complexity

- Gigantic tables?
- Solution: start with simpler analysis, then add more detail.
- But how?



	A	B	C	D	E	F	G	H	I	J	K
1		Plant Status	Pressurizer Pressure	Main Steam Line Activity	SG Pressure Drop Rate	SG 1 Level	SG (others) Level	Is this context physically possible?	Is this context hazardous regardless of command to close MSIV?	In this context, is it hazardous for PS to command "Close MSIV"?	In this context, is hazardous for PS command "Close
2		Operating	Too low [below MIN 2]	High	Too fast	Above 63%	Some others abnormal	Yes	Yes	No	Yes
3		Operating	Too low [below MIN 2]	High	Too fast	Above 63%	All others normal	Yes	Yes	No	Yes
4		Operating	Too low [below MIN 2]	High	Too fast	Below 20%	Some others abnormal	Yes	Yes	No	Yes
5		Operating	Too low [below MIN 2]	High	Too fast	Below 20%	All others normal	Yes	Yes	No	Yes
6		Operating	Too low [below MIN 2]	High	Too fast	Normal	Some others abnormal	Yes	Yes	No	Yes
7		Operating	Too low [below MIN 2]	High	Too fast	Normal	All others normal	Yes	Yes	No	Yes
8		Operating	Too low [below MIN 2]	High	Acceptable	Above 63%	Some others abnormal	Yes	Yes	No	Yes
9		Operating	Too low [below MIN 2]	High	Acceptable	Above 63%	All others normal	Yes	Yes	No	Yes
10		Operating	Too low [below MIN 2]	High	Acceptable	Below 20%	Some others abnormal	Yes	Yes	No	Yes
11		Operating	Too low [below MIN 2]	High	Acceptable	Below 20%	All others normal	Yes	Yes	No	Yes
12		Operating	Too low [below MIN 2]	High	Acceptable	Normal	Some others abnormal	Yes	Yes	No	Yes
13		Operating	Too low [below MIN 2]	High	Acceptable	Normal	All others normal	Yes	Yes	No	Yes
14		Operating	Too low [below MIN 2]	Normal	Too fast	Above 63%	Some others abnormal	Yes	Yes	No	Yes
15		Operating	Too low [below MIN 2]	Normal	Too fast	Above 63%	All others normal	Yes	Yes	No	Yes
16		Operating	Too low [below MIN 2]	Normal	Too fast	Below 20%	Some others abnormal	Yes	Yes	No	Yes
17		Operating	Too low [below MIN 2]	Normal	Too fast	Below 20%	All others normal	Yes	Yes	No	Yes
18		Operating	Too low [below MIN 2]	Normal	Too fast	Normal	Some others abnormal	Yes	Yes	No	Yes
19		Operating	Too low [below MIN 2]	Normal	Too fast	Normal	All others normal	Yes	Yes	No	Yes
20		Operating	Too low [below MIN 2]	Normal	Acceptable	Above 63%	Some others abnormal	Yes	Yes	No	Yes
21		Operating	Too low [below MIN 2]	Normal	Acceptable	Above 63%	All others normal	Yes	Yes	No	Yes
22		Operating	Too low [below MIN 2]	Normal	Acceptable	Below 20%	Some others abnormal	Yes	Yes	No	Yes
23		Operating	Too low [below MIN 2]	Normal	Acceptable	Below 20%	All others normal	Yes	Yes	No	Yes
24		Operating	Too low [below MIN 2]	Normal	Acceptable	Normal	Some others abnormal	Yes	Yes	No	Yes
25		Operating	Too low [below MIN 2]	Normal	Acceptable	Normal	All others normal	Yes	Yes	No	Yes
26		Operating	Too high [more than MA	High	Too fast	Above 63%	Some others abnormal	Yes	Yes	Yes	Yes
27		Operating	Too high [more than MA	High	Too fast	Above 63%	All others normal	Yes	Yes	Yes	Yes
28		Operating	Too high [more than MA	High	Too fast	Below 20%	Some others abnormal	Yes	Yes	Yes	Yes
29		Operating	Too high [more than MA	High	Too fast	Below 20%	All others normal	Yes	Yes	Yes	Yes
30		Operating	Too high [more than MA	High	Too fast	Normal	Some others abnormal	Yes	Yes	Yes	Yes
31		Operating	Too high [more than MA	High	Too fast	Normal	All others normal	Yes	Yes	Yes	Yes
32		Operating	Too high [more than MA	High	Acceptable	Above 63%	Some others abnormal	Yes	Yes	Yes	Yes
33		Operating	Too high [more than MA	High	Acceptable	Above 63%	All others normal	Yes	Yes	Yes	Yes
34		Operating	Too high [more than MA	High	Acceptable	Below 20%	Some others abnormal	Yes	Yes	Yes	Yes
35		Operating	Too high [more than MA	High	Acceptable	Below 20%	All others normal	Yes	Yes	Yes	Yes
36		Operating	Too high [more than MA	High	Acceptable	Normal	Some others abnormal	Yes	Yes	Yes	Yes
37		Operating	Too high [more than MA	High	Acceptable	Normal	All others normal	Yes	Yes	Yes	Yes
38		Operating	Too high [more than MA	Normal	Too fast	Above 63%	Some others abnormal	Yes	Yes	Yes	No
39		Operating	Too high [more than MA	Normal	Too fast	Above 63%	All others normal	Yes	Yes	Yes	No
40		Operating	Too high [more than MA	Normal	Too fast	Below 20%	Some others abnormal	Yes	Yes	Yes	No
41		Operating	Too high [more than MA	Normal	Too fast	Below 20%	All others normal	Yes	Yes	Yes	No
42		Operating	Too high [more than MA	Normal	Too fast	Normal	Some others abnormal	Yes	Yes	Yes	No
43		Operating	Too high [more than MA	Normal	Too fast	Normal	All others normal	Yes	Yes	Yes	No
44		Operating	Too high [more than MA	Normal	Acceptable	Above 63%	Some others abnormal	Yes	Yes	Yes	No
45		Operating	Too high [more than MA	Normal	Acceptable	Above 63%	All others normal	Yes	Yes	Yes	No
46		Operating	Too high [more than MA	Normal	Acceptable	Below 20%	Some others abnormal	Yes	Yes	Yes	No
47		Operating	Too high [more than MA	Normal	Acceptable	Below 20%	All others normal	Yes	Yes	Yes	No
48		Operating	Too high [more than MA	Normal	Acceptable	Normal	Some others abnormal	Yes	Yes	Yes	No
49		Operating	Too high [more than MA	Normal	Acceptable	Normal	All others normal	Yes	Yes	Yes	No
50		Operating	Normal	High	Too fast	Above 63%	Some others abnormal	Yes	Yes	No	Yes
51		Operating	Normal	High	Too fast	Above 63%	All others normal	Yes	Yes	No	Yes
52		Operating	Normal	High	Too fast	Below 20%	Some others abnormal	Yes	Yes	No	Yes
53		Operating	Normal	High	Too fast	Below 20%	All others normal	Yes	Yes	No	Yes
54		Operating	Normal	High	Too fast	Normal	Some others abnormal	Yes	Yes	No	Yes
55		Operating	Normal	High	Too fast	Normal	All others normal	Yes	Yes	No	Yes
56		Operating	Normal	High	Acceptable	Above 63%	Some others abnormal	Yes	Yes	No	Yes
57		Operating	Normal	High	Acceptable	Above 63%	All others normal	Yes	Yes	No	Yes
58		Operating	Normal	High	Acceptable	Below 20%	Some others abnormal	Yes	Yes	No	Yes
59		Operating	Normal	High	Acceptable	Below 20%	All others normal	Yes	Yes	No	Yes
60		Operating	Normal	High	Acceptable	Normal	Some others abnormal	Yes	Yes	No	Yes
61		Operating	Normal	High	Acceptable	Normal	All others normal	Yes	Yes	No	Yes
62		Operating	Normal	Normal	Too fast	Above 63%	Some others abnormal	Yes	Yes	No	Yes
63		Operating	Normal	Normal	Too fast	Above 63%	All others normal	Yes	Yes	No	Yes
64		Operating	Normal	Normal	Too fast	Below 20%	Some others abnormal	Yes	Yes	No	Yes
65		Operating	Normal	Normal	Too fast	Below 20%	All others normal	Yes	Yes	No	Yes
66		Operating	Normal	Normal	Too fast	Normal	Some others abnormal	Yes	Yes	No	Yes
67		Operating	Normal	Normal	Too fast	Normal	All others normal	Yes	Yes	No	Yes
68		Operating	Normal	Normal	Acceptable	Above 63%	Some others abnormal	Yes	Yes	Yes	No
69		Operating	Normal	Normal	Acceptable	Above 63%	All others normal	Yes	Yes	Yes	No
70		Operating	Normal	Normal	Acceptable	Below 20%	Some others abnormal	Yes	Yes	No	Yes
71		Operating	Normal	Normal	Acceptable	Below 20%	All others normal	Yes	Yes	No	Yes
72		Operating	Normal	Normal	Acceptable	Normal	Some others abnormal	Yes	No	Yes	No
73		Operating	Normal	Normal	Acceptable	Normal	All others normal	Yes	No	Yes	No
74		Startup or Shutdo	Too low [below MIN 2]	High	Too fast	Above 63%	Some others abnormal	Yes	Yes	No	Yes
75		Startup or Shutdo	Too low [below MIN 2]	High	Too fast	Above 63%	All others normal	Yes	Yes	No	Yes
76		Startup or Shutdo	Too low [below MIN 2]	High	Too fast	Below 20%	Some others abnormal	Yes	Yes	No	Yes
77		Startup or Shutdo	Too low [below MIN 2]	High	Too fast	Below 20%	All others normal	Yes	Yes	No	Yes

Including more detail with refinement

Solution:

- 1) Define how process model variables are inferred
- 2) …

	1	2	3	4	5
	Control Action	**Condition of Steam Generator Tube**	**Condition of Main Feedwater Pipe**	**Condition of Main Steamline**	**Operation of other support systems**
	Close MSIV				

Condition of Steam Generator Tube inferred to be …

		ruptured when:		*not ruptured* when:
Radioactivity sensor =	Normal			T
	Radioactive	T		
Steam generator water level =	Too low			
	Normal			
	Too high		T	F

Condition of Main Feedwater Pipe inferred to be …

		ruptured when:			*not ruptured* when:
Steam generator pressure drop rate =	More than X	T			F
	Less than X				
Steam generator pressure =	More than Y				
	Less than Y		T		F
Containment pressure =	More than Z			T	F
	Less than Z				

Condition of Main Steam Line inferred to be …

		ruptured when:			*not ruptured* when:
Steam generator pressure drop rate =	More than X	T			F
	Less than X				
Steam generator pressure =	More than Y				
	Less than Y		T		F
Containment pressure =	More than Z			T	F
	Less than Z				

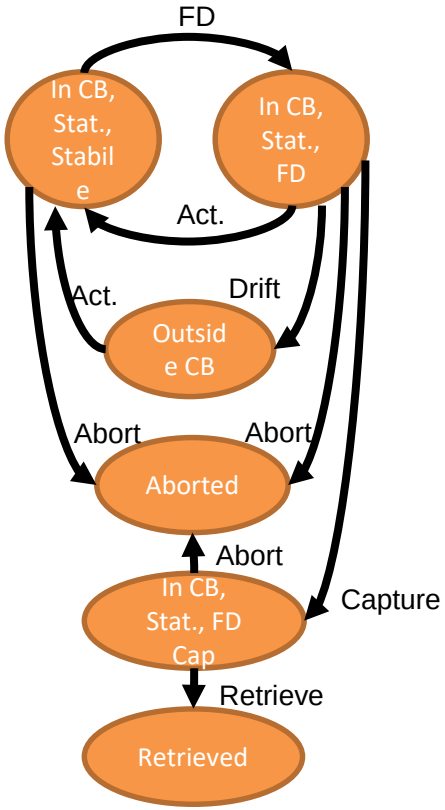
Operation of other support systems inferred to be …

		adequate when:			*not adequate* when:
Safety injection system =	Operating	T			F
	Not operating				
Emergency feedwater system =	Operating		T		F
	Not operating				
Emergency cooling system =	Operating			T	F
	Not operating				

Model-Based System Engineering (MBSE) and Safety Analysis (MBSA)

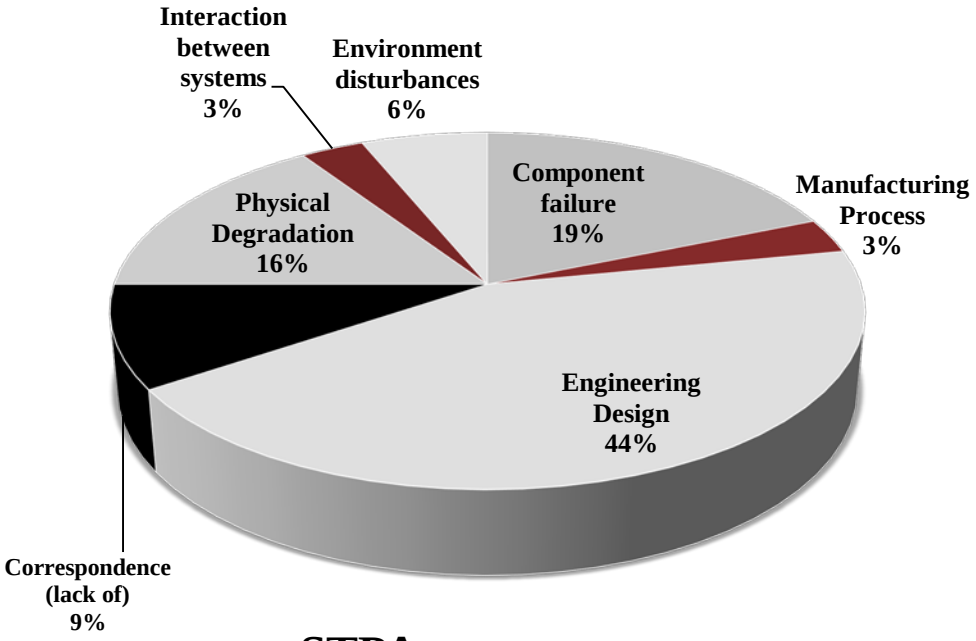
1. Describing hazardous, functional, and required behavior
   - HP(h ∈ H, ca ∈ CA, c ∈ Co)
     - True iff providing command ca in context c will cause hazard h
   - HNP(h ∈ H, ca ∈ CA, c ∈ Co)
     - True iff not providing command ca in context c will cause hazard h
   - FP(f ∈ F, ca ∈ CA, c ∈ Co)
     - True iff providing command ca in context c is necessary to achieve function f
   - R(ca ∈ CA, c ∈ Co)
     - True iff command CA is required to be provided in context c
2. Consistency checks
   - ∀h1 ∈ H,h2 ∈ H ¬ ∃ ca ∈ CA, c ∈ C : HP(h1, ca, c) ^ HNP(h2, ca, c)
     - For every potential context, it must be possible to avoid hazardous control actions/inactions. In other words, if it is hazardous to provide CA then it should be non-hazardous to not provide CA
   - ∀ h ∈ H, f ∈ F ¬ ∃ ca ∈ CA, c ∈ C : HP(h, ca, c) ^ F(f, ca, c)
     - For every potential context, if it is necessary to provide a command to fulfill a function then it must not be hazardous to provide the command in that context
3. Requirements generation (SpecTRM-RL tables)
   - Compute R(ca ∈ CA, c ∈ C) to satisfy the following:
   - ∀h,ca,c: h ∈ H ^ ca ∈ CA ^ c ∈ C → [HP(h, ca, c) → ¬ R(ca, c)]
   - ∀h,ca,c: h ∈ H ^ ca ∈ CA ^ c ∈ C → [R(ca, c) → HNP(h, ca, c)]
   - ∀f,ca,c: f ∈ F ^ ca ∈ CA ^ c ∈ C → [FP(f, ca, c) → R(ca, c)]

Generated requirements / initial model for HTV / ISS crew interaction



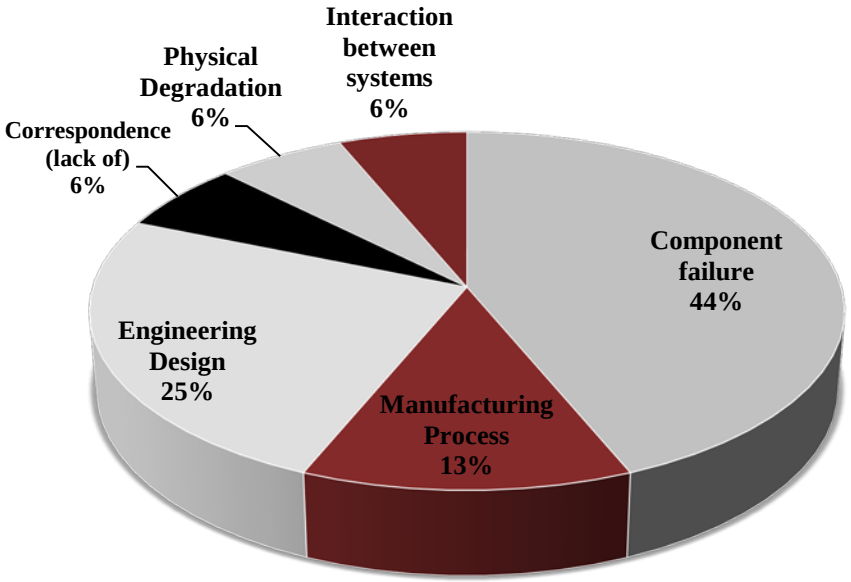
STPA used to automatically generate suitable models

Types of accident causes found by STPA



STPA causes

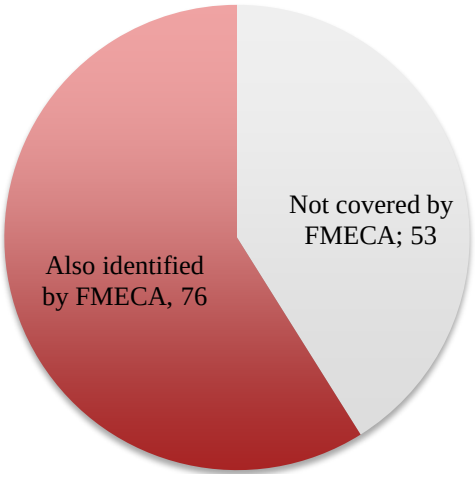
Types of accident causes found by FMECA



FMECA causes

Causes captured by STPA and FMECA

Causes identified in STPA



Examples of causes not captured by FMECA

The method for determining vehicle speed could be incorrect. Relying in one method of measurement (in this case wheel speed) might hazardous if sensor fails.

There is no prioritization for critical operation components if there is low voltage available.

Another controller limits speed when auxiliary assistance is provided (Cruise control).

High friction event is detected at low speed.

Assistance would not be provided because there is a conflict between steering angle and speed signals.

Delayed signal information provided by sensor, or there is a communication error in the BUS

Chime is not laud enough or displayed in a way it is easily noticeable by the driver.

137 vs. 95 total causes found (but there are overlaps)

Using STPA for iterative analysis + design

Iteration #1,2

STPA | **Design**

Initial control structure

STPA Step 1

Revise control structure based on safety constraints

STPA Step 2

Eliminate/mitigate causal factors if possible

Iteration #3

STPA | **Design**

Formal STPA Step 1

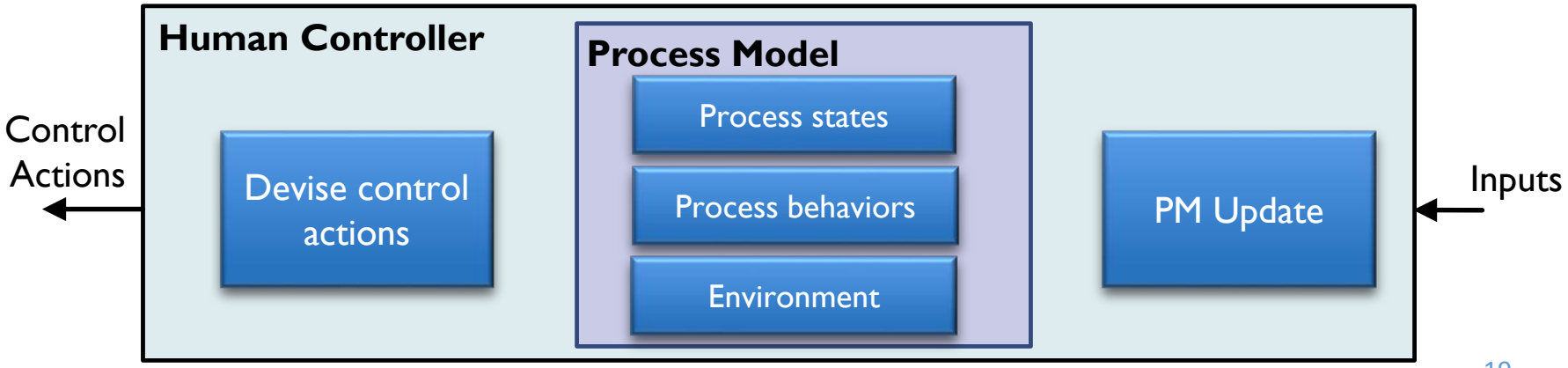
Resolve any new UCAs, conflicts

Detailed STPA Step 2
(for unaddressed scenarios only)

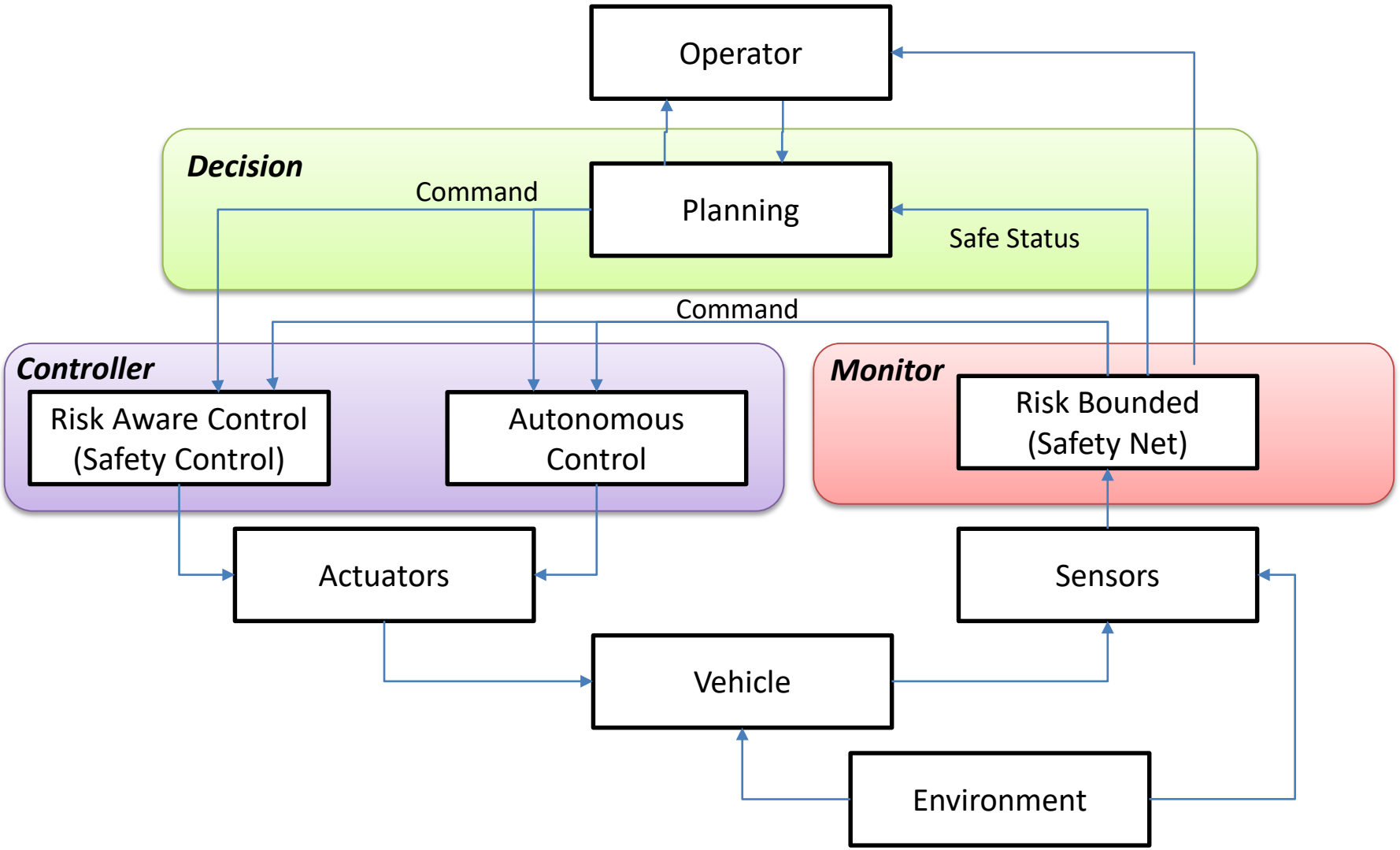
Add controls for new causal factors identified

Human-centric design process

- Human Process Model variables
- Identify unsafe human decisions
- Derive Process Model Flaws
- Identify flaws in Process Model Updates
- Incorporate solutions based on scenario type (missing feedback, conflicting control actions, etc.)



AI-based Autonomous Systems



Regulatory Activity

- FAA internal certification training
- FAA policy
- EASA application: means of compliance
- INTA certification training
- CAAC / CAUC

STPA in Industry Standards

- ISO/PAS 21448: Safety of the Intended Functionality (SOTIF)
  - STPA used assess safety of digital systems
- ASTM WK60748
  - "Standard Guide for Application of STPA to Aircraft"
- SAE AIR6913
  - "Using STPA during Development and Safety Assessment of Civil Aircraft"
- RTCA DO-356A
  - "Airworthiness Security Methods and Considerations"
  - STPA-sec used for cybersecurity of digital systems
- SAE JXXXX
  - "Recommended Practice for STPA in Automotive Safety Critical Systems"
  - GM, Nissan, Ford, Toyota, FCA, Zenuity, Mercedes-Benz, Renesas, Continental, etc.
- MIL-STD-882E
  - STPA used for compliance

For more information

- Website: mit.edu/psas
- Google: “STPA Handbook”
- Next MIT STAMP Conference (March 25-28, 2019)

- Email me! JThomas4@mit.edu