Welcome to STAMP/STPA 2020 Virtual Workshop

Nancy Leveson (MIT)
John Thomas (MIT)

Attendance

- 2,212 people registered (and growing)
  - Registration for in-person workshop this year was about 550 in March
  - Each year we have grown by at least 25% (in-person attendees)

- Industries represented (largest number first)

Aviation
Automotive
Academia/Universities
Defense
Oil/gas/chemicals
Medical/Healthcare
Power/Energy/Nuclear
Space
Rail
Communications
Software
Robotics

Transportation
Maritime/Ships
Insurance, Financial
Agriculture
Insurance
Financial
Mining
Iron and Steel
Workplace Safety
[Cement, consumer goods, lighting, entertainment, printing and packaging, …]

Countries of Registrants (73) [last year 34]

Argentina	Denmark	Indonesia	Netherlands	Serbia
Australia	Ecuador	Iran	New Zealand	Singapore
Austria	Egypt	Ireland	Nicaragua	South Africa
Bahrain	El Salvador	Israel	Nigeria	South Korea
Bangladesh	England	Italy	Norway	Spain
Belgium	Estonia	Ivory Coast	Oman	Sweden
Brazil	Finland	Japan	Pakistan	Switzerland
Canada	France	Kenya	Peru	Taiwan
Chile	Georgia	Kosovo	Poland	Thailand
China	Germany	Lithuania	Portugal	Tunesia
Colombia	Greece	Luxembourg	Qatar	Turkey
Costa Rica	Hong Kong	Malaysia	Romania	USA
Croatia	Hungary	Mexico	Russia	Vietnam
Cyprus	Iceland	Morocco	Saudi Arabia	
Czech Republic	India	Nepal	Scotland	

Logistics

- Zoom and streaming
- Tapes for workshop: MIT requires captioning

  Akamai is funding professional captioning

- Plans for the future:
  - In-person in March, virtual in the fall

VISION & TEAM MEMBERS

STAMP ENGINEERING SERVICES, LLC

ENGINEERING A SAFER AND MORE SECURE WORLD

DR NANCY LEVESON

MIT PROFESSOR,

STAMP CREATOR

DR JOHN THOMAS

MIT PHD, STPA, TRAINING

BILL YOUNG

MIT PHD,

STPA-SEC

LORI SMITH

COMPLEX SYSTEMS ENGINEERING ANALYSIS

MARC NANCE

TRANSPORTATION, BUSINESS MANAGEMENT

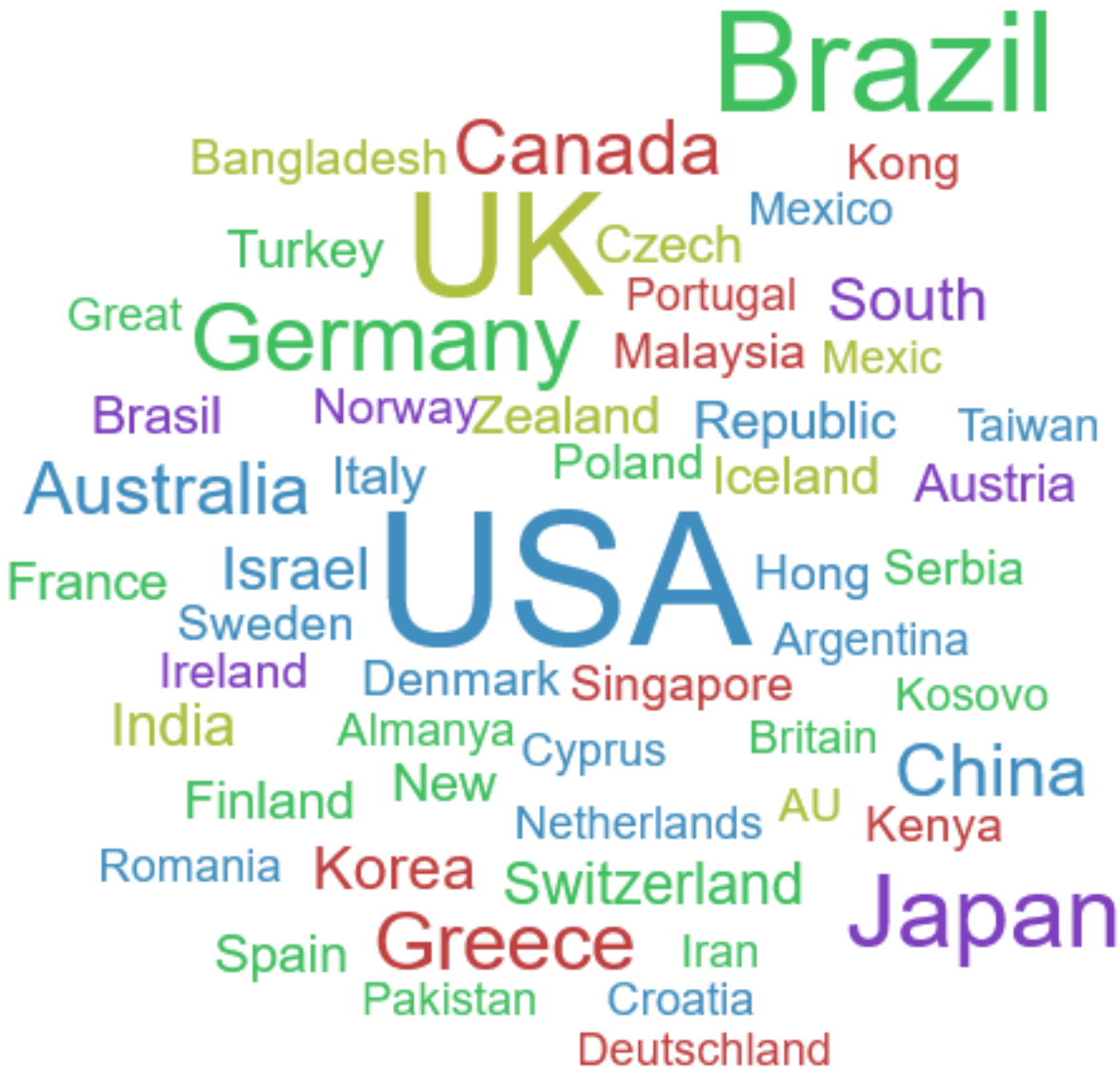
PHIL SPECHT

PRODUCTION ENGINEERING, AUTONOMOUS SYSTEMS

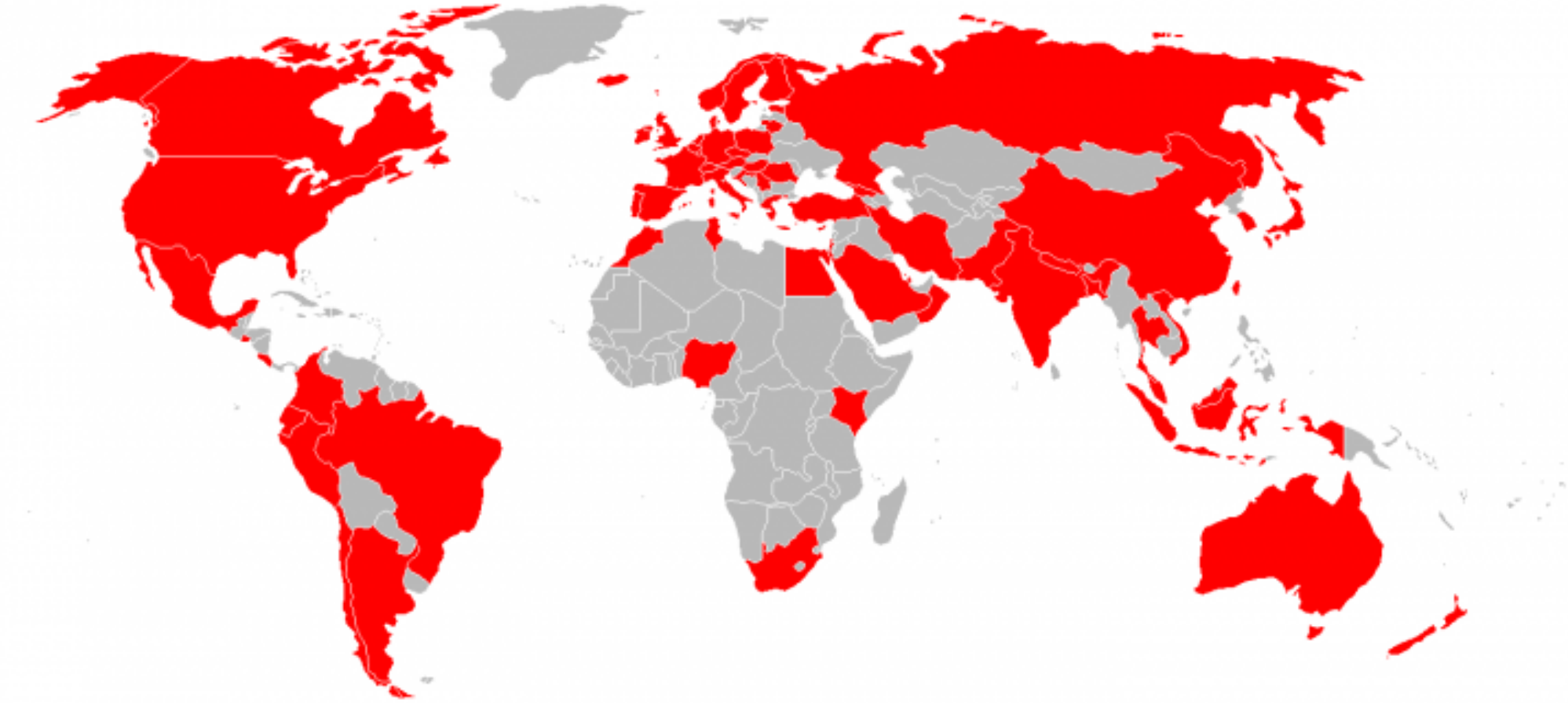
stamp-services.com

info@stamp-services.com

2020 STAMP Workshop
Countries where STAMP/STPA/CAST already being used



2020 STAMP Workshop Countries



Asia:14	45.16%
Africa:6	10.71%
Caribbean:2	9.09%
Europe:28	58.33%
Middle East:8	38.1%
North America:3	75%
Pacific:2	10%
South America:6	46.15%

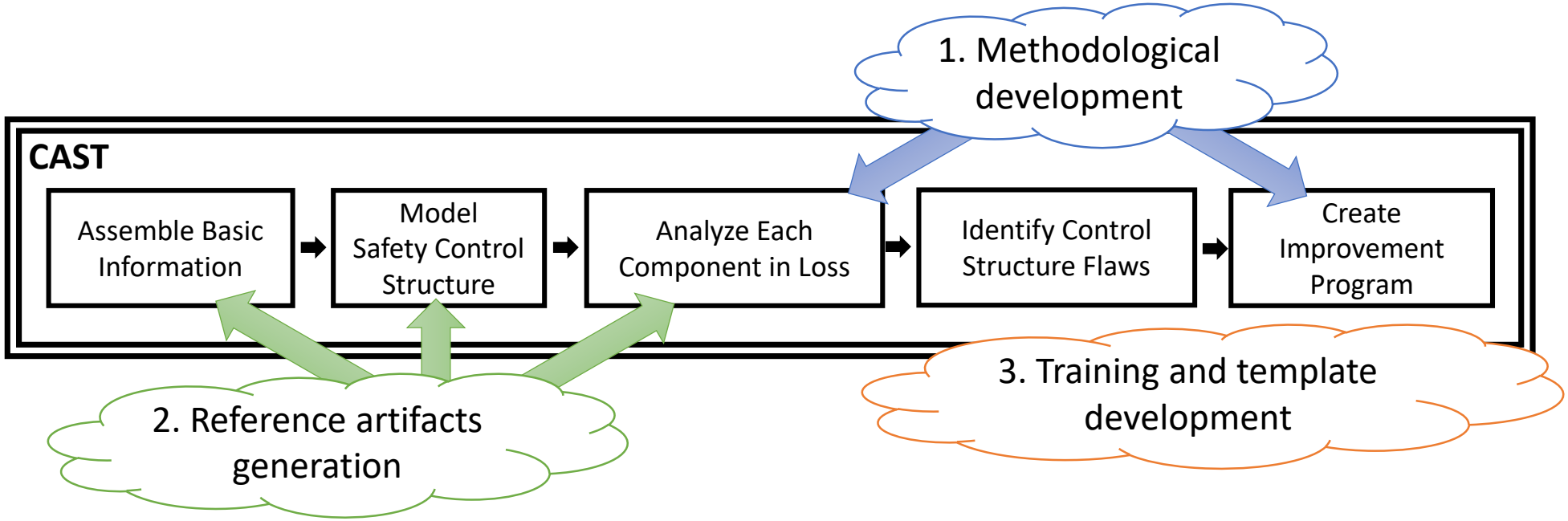
Map generated by: https://traveltip.org/countries_visited.php

MIT STAMP Research Projects

Implementing CAST in Health Care

Lawrence Wong

- Root cause analyses not generating the needed learning for safety improvement
- Structural barriers to CAST implementation: Time and knowledge relatively scarce in health care
- Tailored development to facilitate CAST adoption in health care



A System-Theoretic Approach to Risk Assessment

By Dro Gregorian and Sam Yoo

- Risk matrices used worldwide rely on probability (likelihood) vs severity (consequence)
  - Matrix development is frequently subjective or biased and is often uninformed by a quantifiable deeper analysis
- New research applies results of STPA to inform the standard risk matrix in a repeatable, objective, deeper way

DoD Acquisition Risk Management Guide

Likelihood	1	2	3	4	5
5		IVA		IIA	IA
4		IVB	IIIA IIIB IIIC	IIB	IB
3		IVC	IIID IIIE	IIC	IC
2		IVD		IID IIE	ID
1		IVE			IE

Consequence

MIL-STD-882E

Probability	I	II	III	IV
A				
B				
C				
D				
E				

Severity

Note: MIL-STD-882E includes probability level "F" for "eliminated" ESOH risks that are "incapable of occurrence." ESOH risks with probability level F should not be translated to the DoD Acquisition Risk Management program risk matrix.

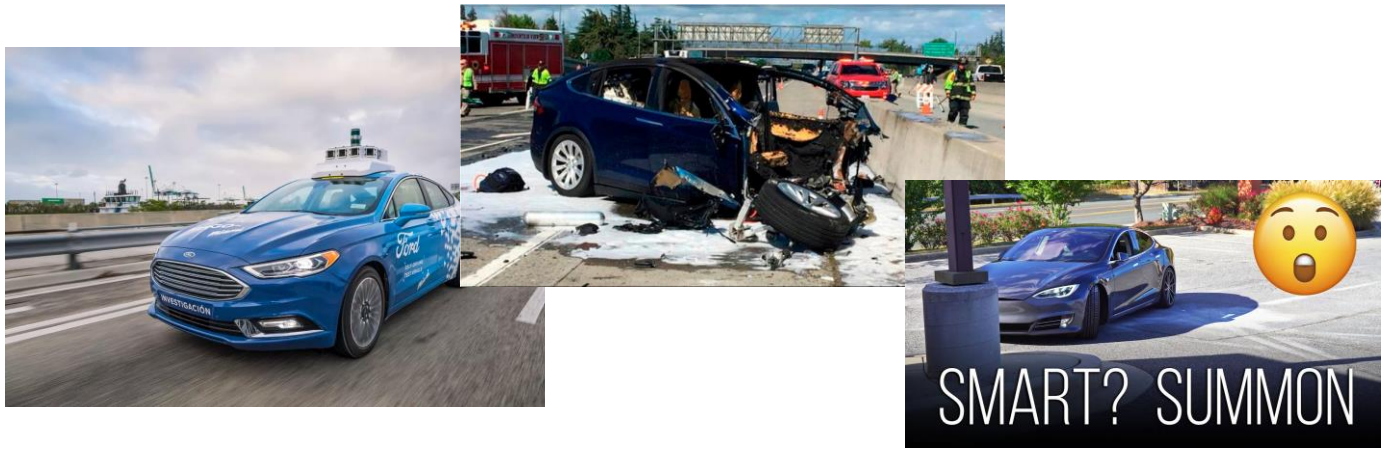
Hazard Analysis for U.S. Army Air Launched Effects Program

STPA for swarms of unmanned aircraft and manned / unmanned teaming

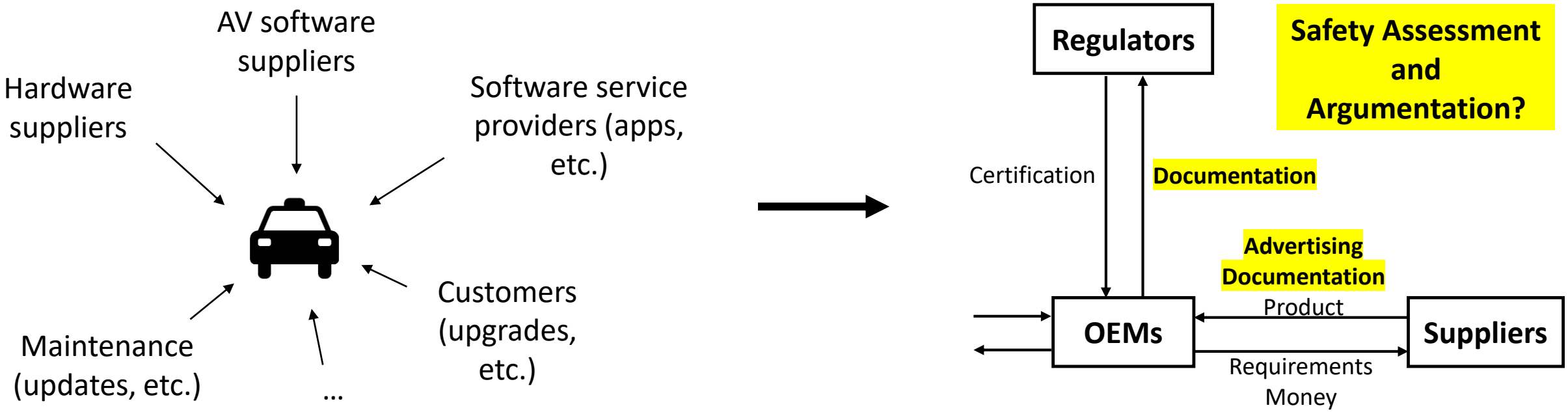
Air Launched Effects: semi- autonomous UAVs launched from rotorcraft and larger UAVs – multi domain missions including recon, decoy, jamming, and kinetic deployments.

STPA and Conceptual Architectural provide impactful information for analysis of alternatives

Michael Schmid – Automation and AI in Automotive



- common factors in accidents
- hazard identification & safety requirements
- regulation & insurance of AVs
- application to regulation & insurance
- Development processes of AI applications



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.

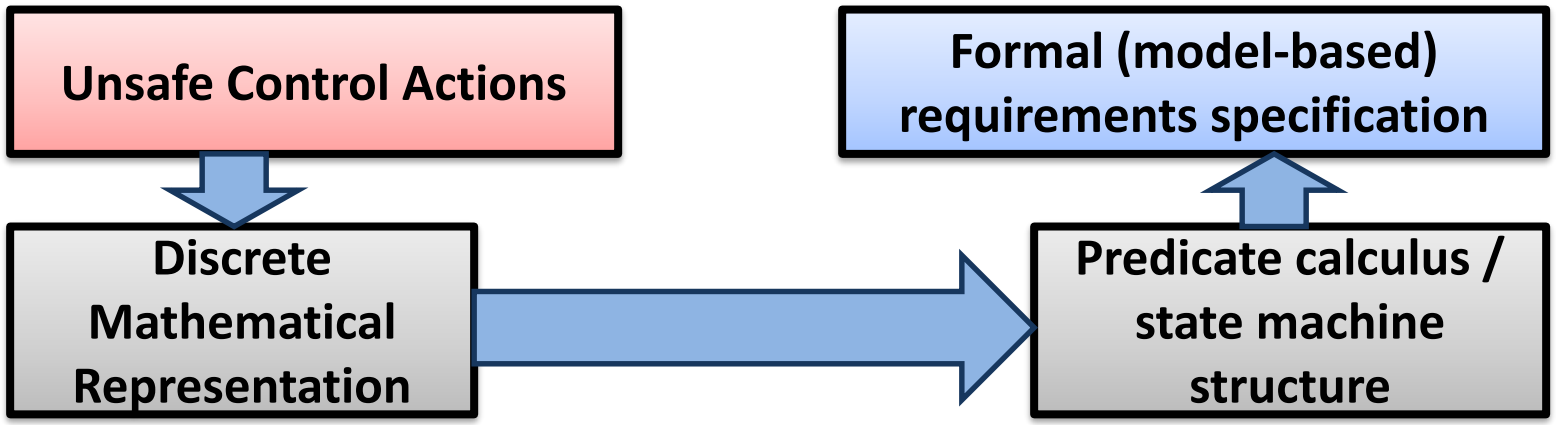
Formal (model-based) requirements specification

Behavior required for function

Behavior required for safety

Provide 'Increase Pressure' command

Mode =	Hold Mode	T	T	T
	Standby Mode			
	Off Mode			
Gear =	Drive	T		
	Not drive		T	
Gas Pedal =	Pressed			T
	Not Pressed	T	T	
Wheel Speed =	Rotating	T	T	T
	Not Rotating			

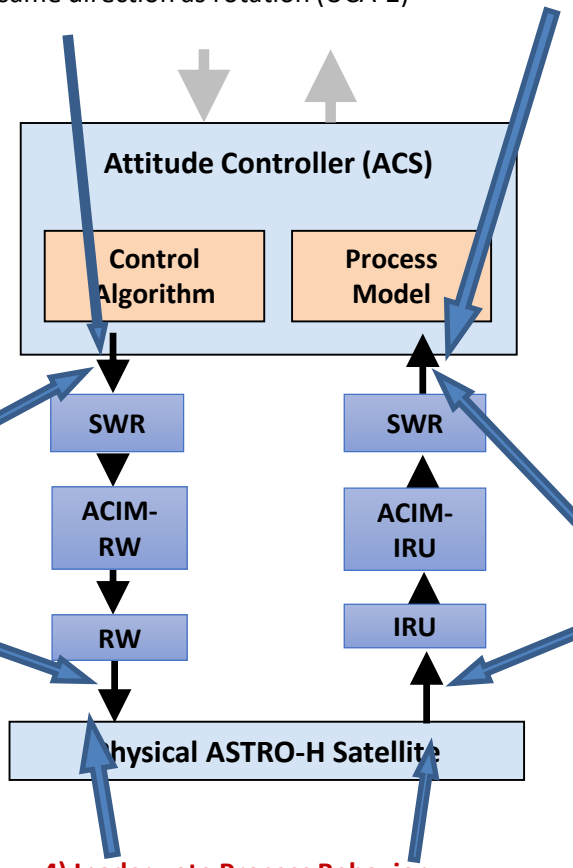


I did STPA, did I miss anything?

Evaluate quality of analysis

Demonstrate coverage

2) Inappropriate Decisions
- ACS receives correct vehicle rotation feedback
- ACS provides attitude maneuver commands in the same direction as rotation (UCA-2)



1) Inadequate Control Execution
- ACS provides attitude maneuver commands
- RW does not respond accordingly

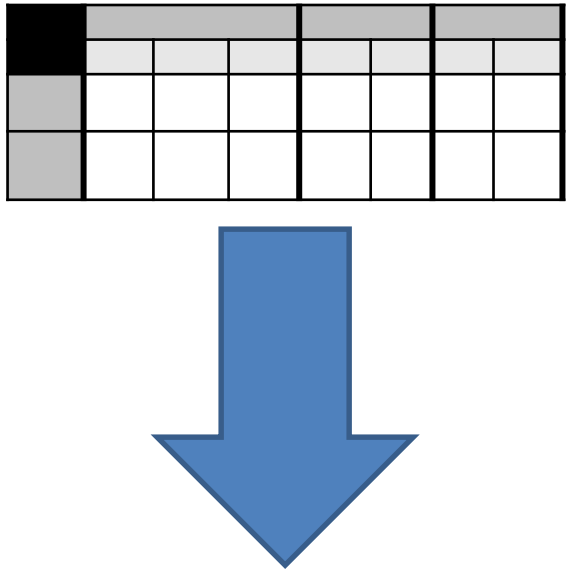
3) Inadequate Feedback & Other Inputs
- ACS receives incorrect feedback that vehicle is rotating
- Vehicle is not rotating

4) Inadequate Process Behavior
- RW momentum changes
- Vehicle attitude does not change accordingly

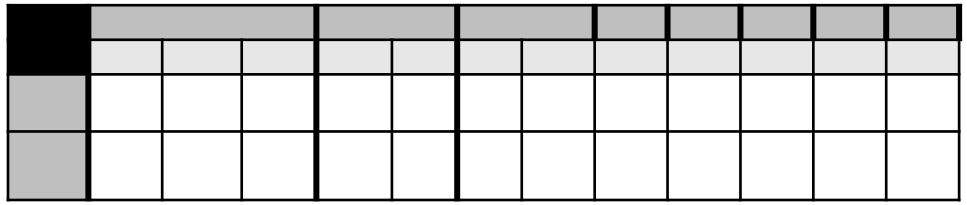
Automatically identify mistakes, inconsistencies

New scalable STPA-based approach for feature interactions

- 3 controllers



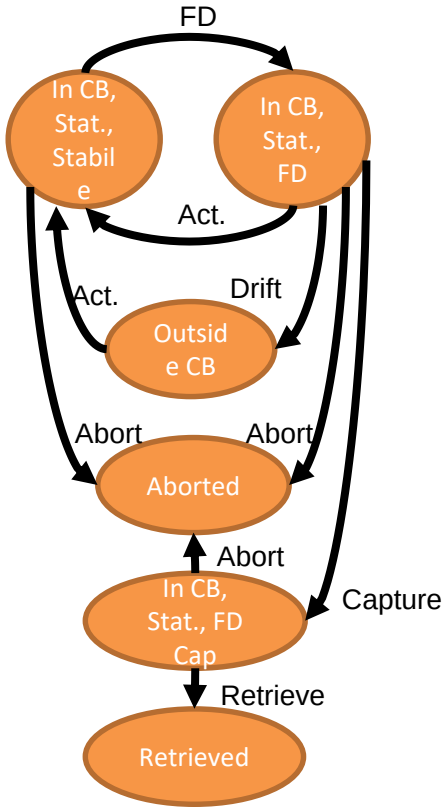
- 6 controllers



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

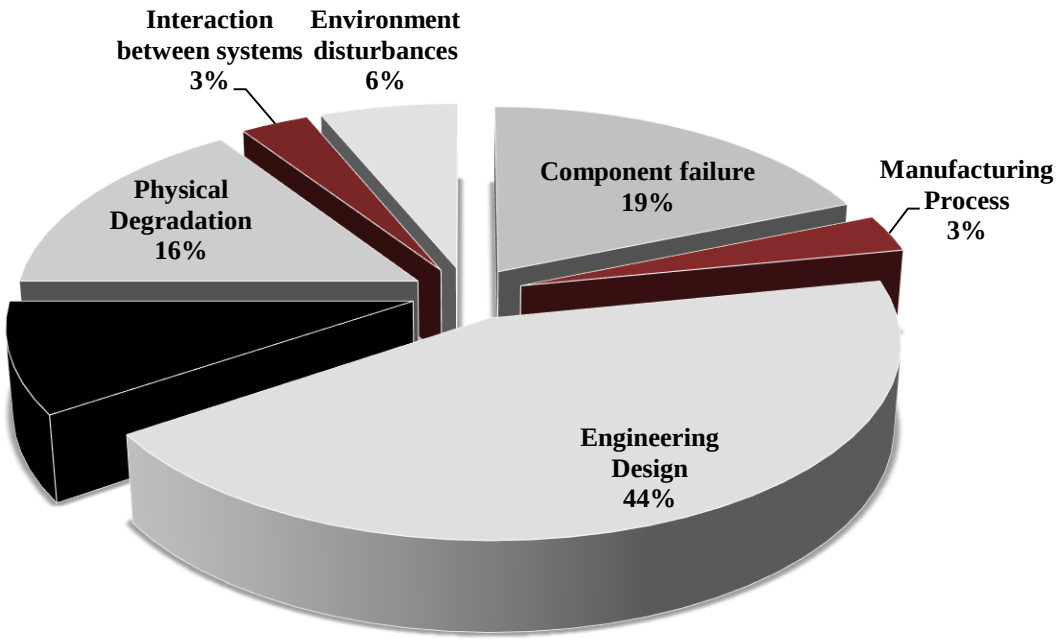
1. Describing hazardous, functional, and required behavior
   - HP(h ∈ H, ca ∈ CA, c ∈ Co)
     - True iff providing command ca in context c will cause hazard h
   - HNP(h ∈ H, ca ∈ CA, c ∈ Co)
     - True iff not providing command ca in context c will cause hazard h
   - FP(f ∈ F, ca ∈ CA, c ∈ Co)
     - 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



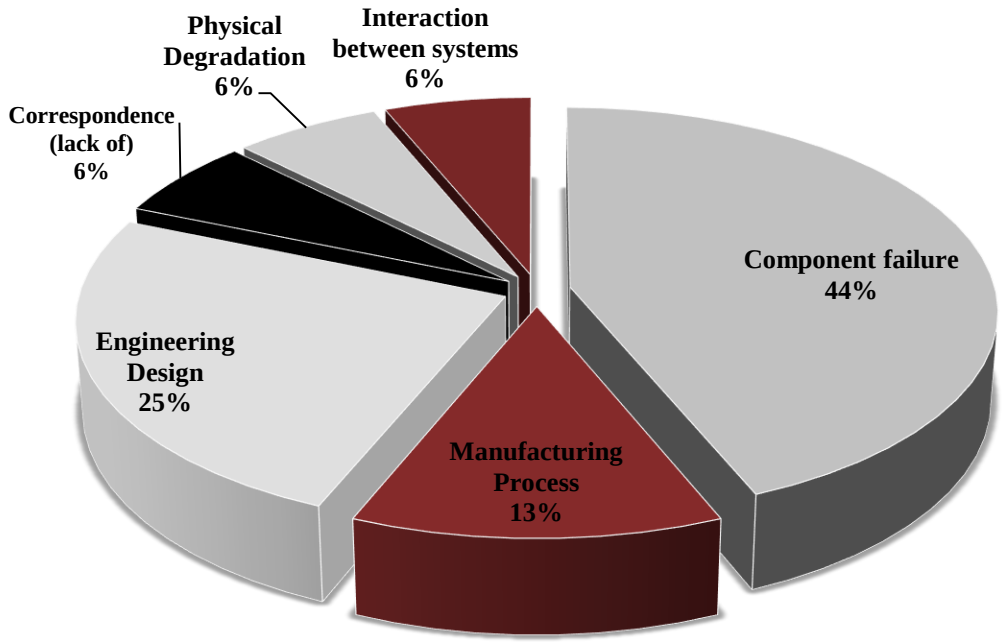
STPA used to automatically generate suitable models

Types of accident causes found by STPA



STPA causes for UCA1

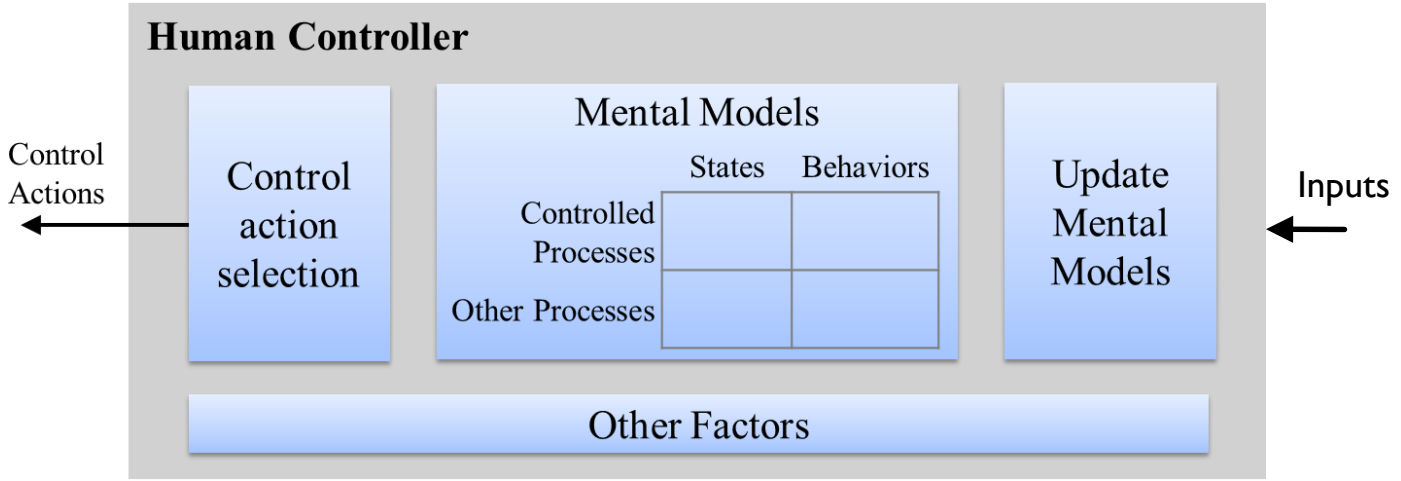
Types of accident causes found by FMECA



FMECA causes for FM1

STPA based human-centric design process

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



MIT-Industry Consortium

- Participate in new STAMP-based research with MIT
- Direct our activities and research

- Network and exchange opportunities
- Participate in the research process
- Provide case studies
- Inclusion as a test site
- Collaboration on company projects

Contact: JThomas4@mit.edu