STAMP Introduction

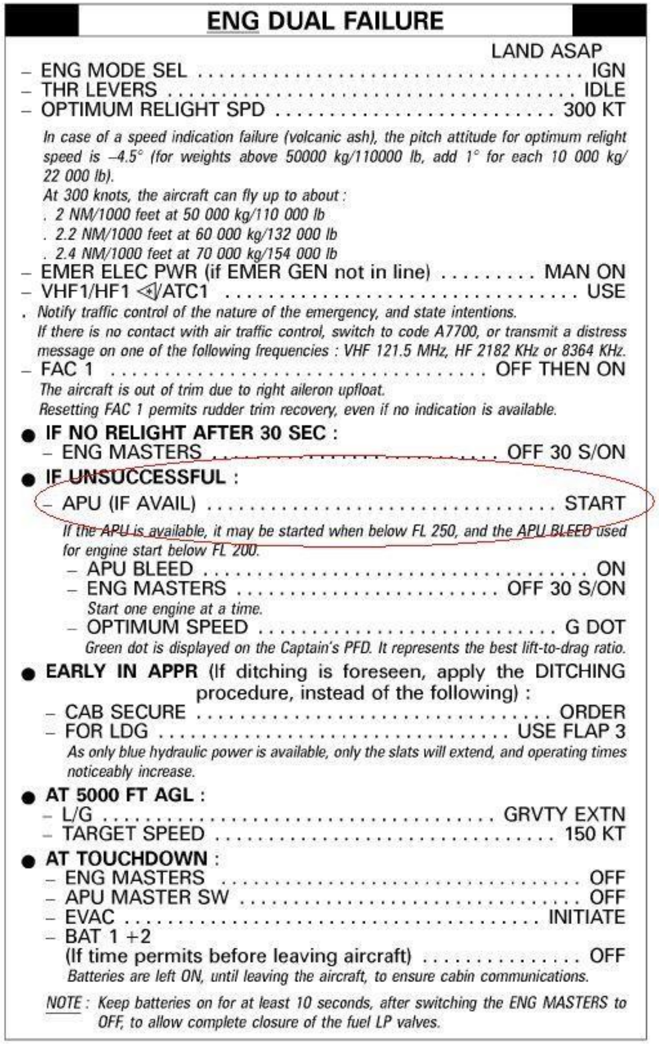
Dr. John Thomas

Success Example: Landing on Hudson River

Cause: Engine Failure (NTSB)

Engine <u>failed</u>, <u>varied</u>, <u>deviated</u> from its function

Dual Engine Failure Planning



ENG DUAL FAILURE

LAND ASAP

- ENG MODE SEL .... IGN
- THR LEVERS .... IDLE
- OPTIMUM RELIGHT SPD .... 300 KT

In case of a speed indication failure (volcanic ash), the pitch attitude for optimum relight speed is –4.5° (for weights above 50000 kg/110000 lb, add 1° for each 10 000 kg/ 22 000 lb).
At 300 knots, the aircraft can fly up to about :
. 2 NM/1000 feet at 50 000 kg/110 000 lb
. 2.2 NM/1000 feet at 60 000 kg/132 000 lb
. 2.4 NM/1000 feet at 70 000 kg/154 000 lb

- EMER ELEC PWR (if EMER GEN not in line) .... MAN ON
- VHF1/HF1 ◁/ATC1 .... USE

. Notify traffic control of the nature of the emergency, and state intentions.
If there is no contact with air traffic control, switch to code A7700, or transmit a distress message on one of the following frequencies : VHF 121.5 MHz, HF 2182 KHz or 8364 KHz.

- FAC 1 .... OFF THEN ON

The aircraft is out of trim due to right aileron upfloat.
Resetting FAC 1 permits rudder trim recovery, even if no indication is available.

● **IF NO RELIGHT AFTER 30 SEC :**
- ENG MASTERS .... OFF 30 S/ON

● **IF UNSUCCESSFUL :**
- APU (IF AVAIL) .... START

If the APU is available, it may be started when below FL 250, and the APU BLEED used for engine start below FL 200.

- APU BLEED .... ON
- ENG MASTERS .... OFF 30 S/ON

Start one engine at a time.

- OPTIMUM SPEED .... G DOT

Green dot is displayed on the Captain's PFD. It represents the best lift-to-drag ratio.

● **EARLY IN APPR** (If ditching is foreseen, apply the DITCHING procedure, instead of the following) :
- CAB SECURE .... ORDER
- FOR LDG .... USE FLAP 3

As only blue hydraulic power is available, only the slats will extend, and operating times noticeably increase.

● **AT 5000 FT AGL :**
- L/G .... GRVTY EXTN
- TARGET SPEED .... 150 KT

● **AT TOUCHDOWN :**
- ENG MASTERS .... OFF
- APU MASTER SW .... OFF
- EVAC .... INITIATE
- BAT 1 +2
(If time permits before leaving aircraft) .... OFF

Batteries are left ON, until leaving the aircraft, to ensure cabin communications.

NOTE : Keep batteries on for at least 10 seconds, after switching the ENG MASTERS to OFF, to allow complete closure of the fuel LP valves.

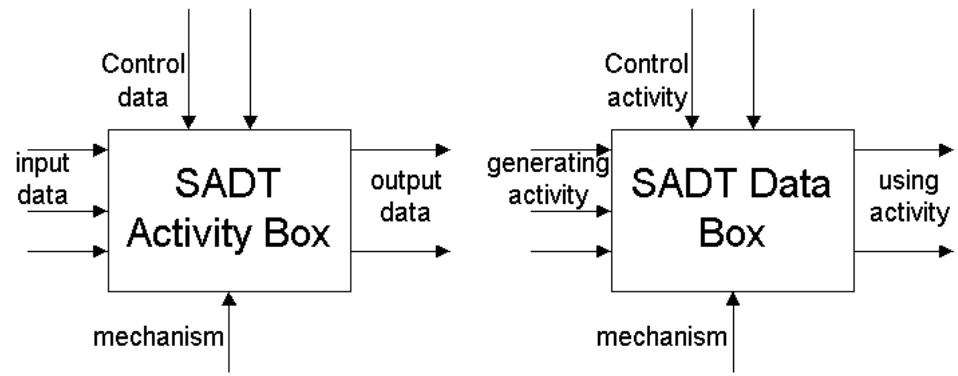
- Design features
  - Software automatically impose limits
  - Ram Air Turbine (RAT)
  - Etc.

Ram Air Turbine

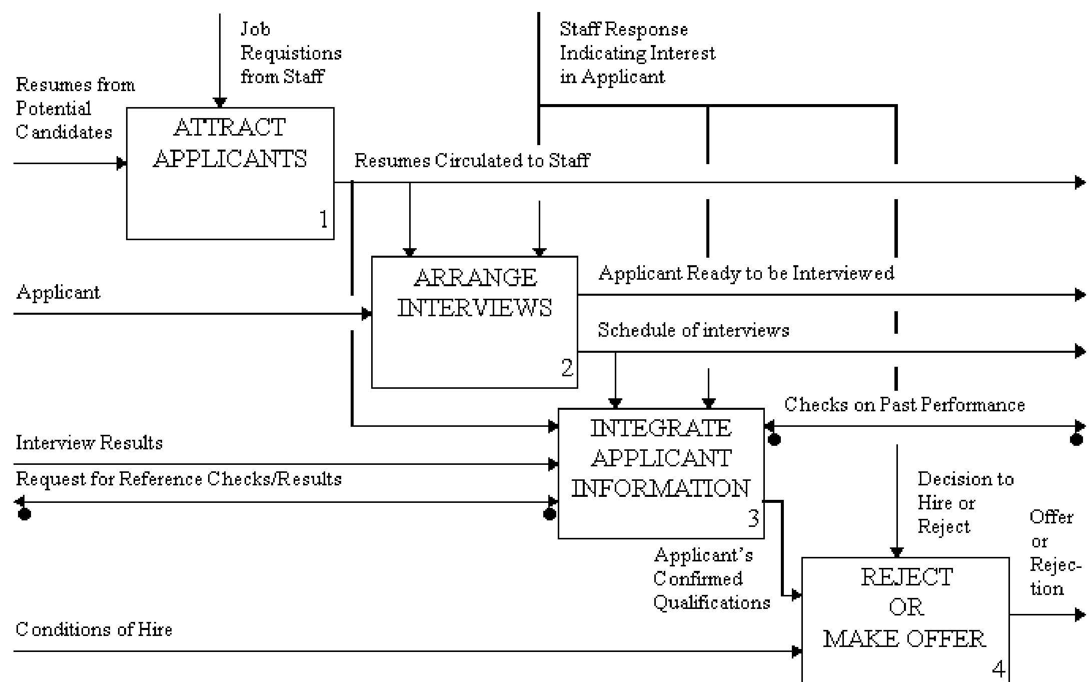
This was anticipated and planned for

Methods to analyze variations and deviations

- HAZOP
- Functional Hazard Analysis
- Fault Tree Analysis
- Failure Modes and Effects Analysis
- Structured Analysis and Design Technique (SADT)
- Parameter diagrams
- Etc.

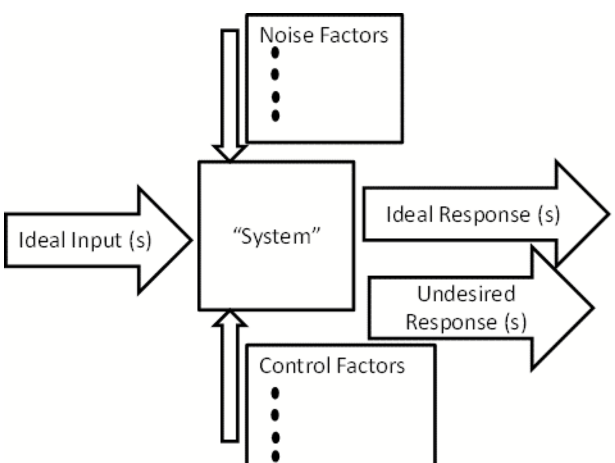


SADT Example (1974)



Example from Pankaj Jain http://p.web.umkc.edu/pjad3/homework5.html

P-diagram Example (1989)



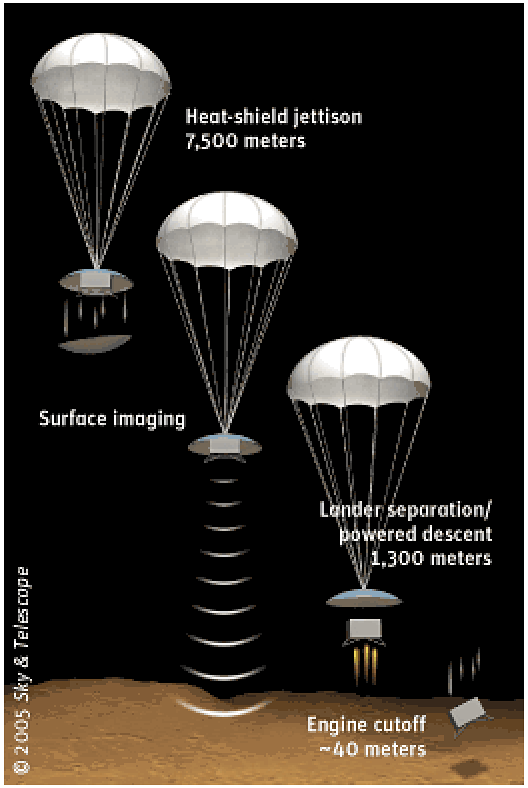
Example from http://themanagersguide.blogspot.jp/2011/01/parameter-diagrams-help-define.html

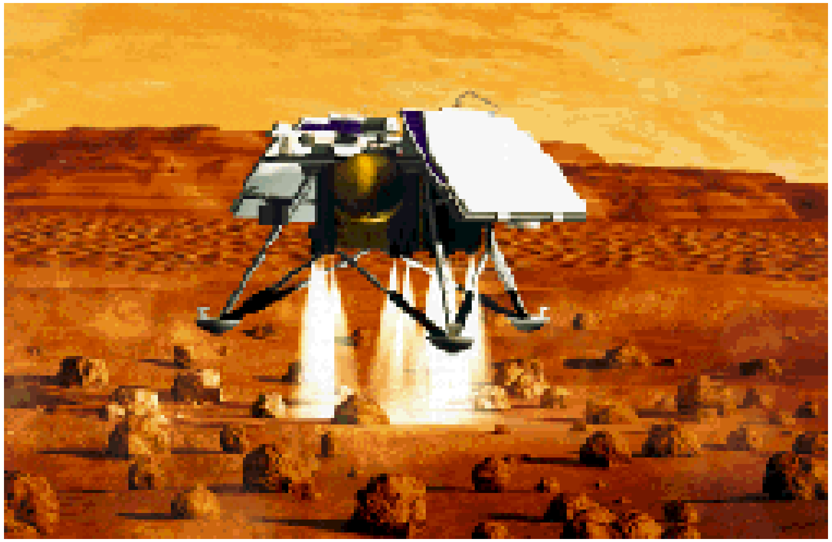
Mars Polar Lander

- During the descent to Mars, the legs were deployed at an altitude of 40 meters.
- Touchdown sensors (on the legs) sent a momentary signal
- The software responded as it was designed to: by shutting down the descent engines.
- The vehicle free-fell and was destroyed upon hitting the surface at 50 mph (80 kph).

There was no component failure, no component deviation!

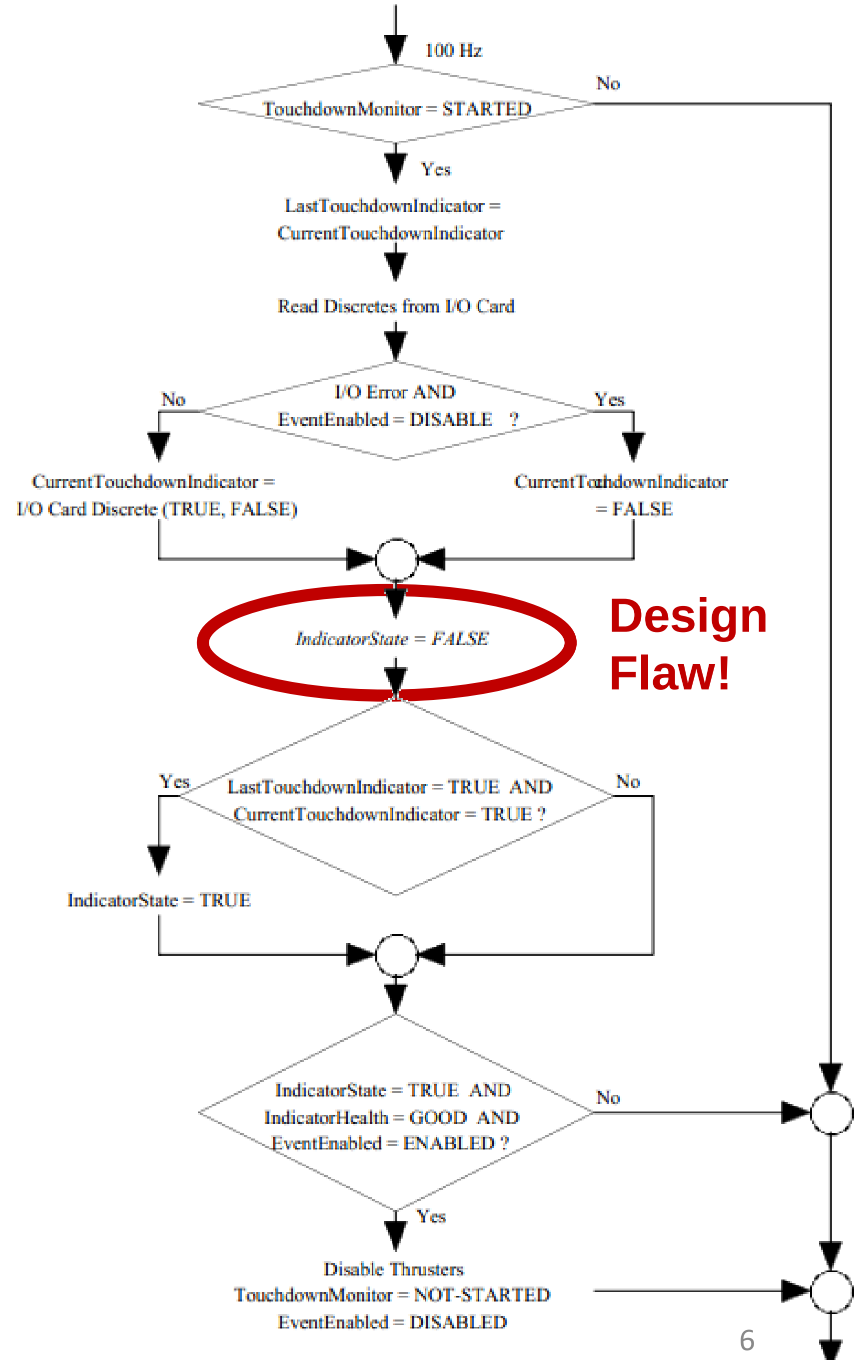
All software and hardware operated exactly as designed!





What was the software problem?

- No variation or deviation
- Didn't eventually "wear out" like hardware
- Software worked exactly as designed
- Requirements were satisfied
- The *design* and *requirements* were flawed from the start!



JPL Special Review Board Report, p115

FLIGHT SOFTWARE REQUIREMENTS

3.7.2.2.4.2 Processing

a. The lander flight software shall cyclically check the state of each of the three touchdown sensors (one per leg) at 100 Hz during EDL.

b. The lander flight software shall be able to cyclically check the touchdown event state with or without touchdown event generation enabled.

c. Upon enabling touchdown event generation, the lander flight software shall attempt to detect failed sensors by marking the sensor as bad when the sensor indicates "touchdown state" on two consecutive reads.

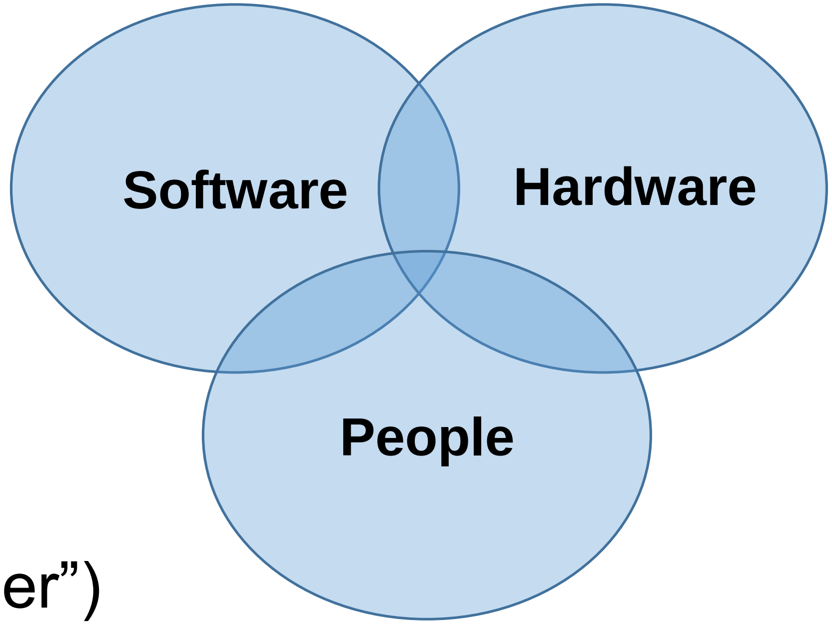
d. The lander flight software shall generate the landing event based on two consecutive reads indicating touchdown from any one of the "good" touchdown sensors.

.

Systems View

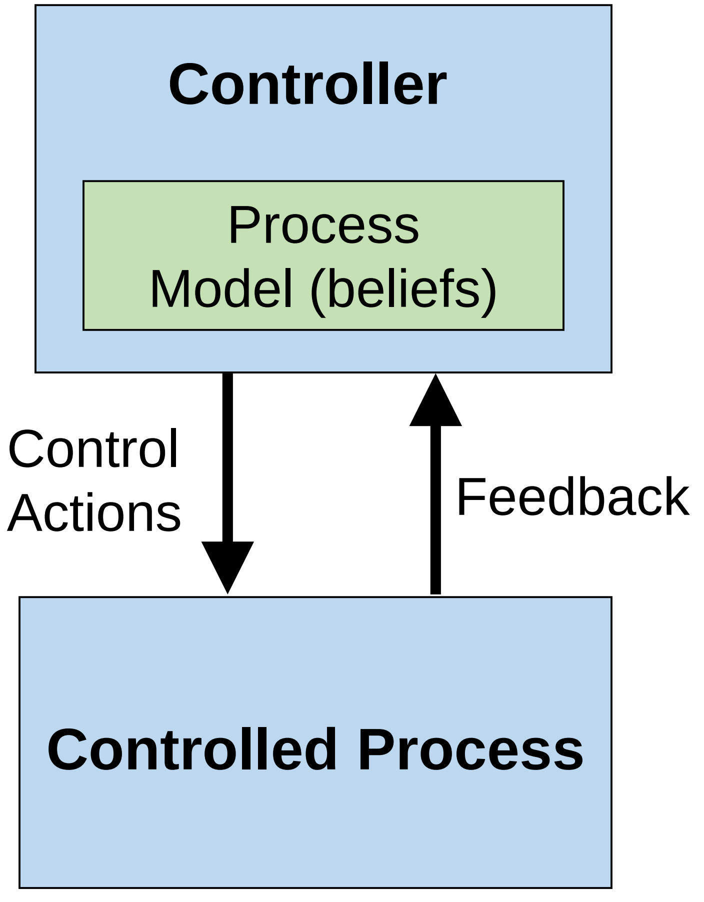
Many different factors were involved:

- Touchdown sensors
- Software implementation
- Software requirements
- Testing
- Engineering reviews
- Communication
- Time pressure
- Culture (“Faster, Better, Cheaper”)
- Etc.



Hard to see the problem by looking at any one part

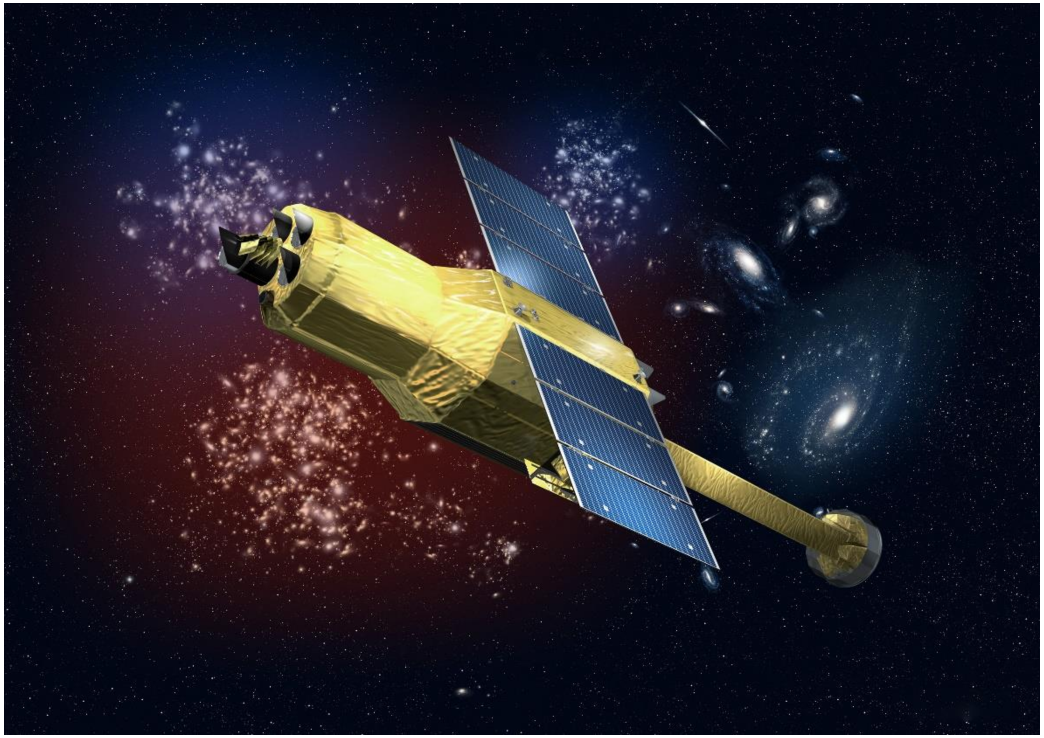
Another way to think about accidents



- Foundation for STAMP

HITOMI Satellite (2016)

- Unexpected software behavior
  - Computer suddenly believed satellite was spinning (incorrect!)
  - Computer commanded faster and faster rotation
  - Satellite destroyed
- Japanese Investigation
  - **Project was lacking an "approach to examine the overall design of the spacecraft"**
- JAXA
  - **"We were unable to let go of our usual methods"**



Components operated exactly as designed!

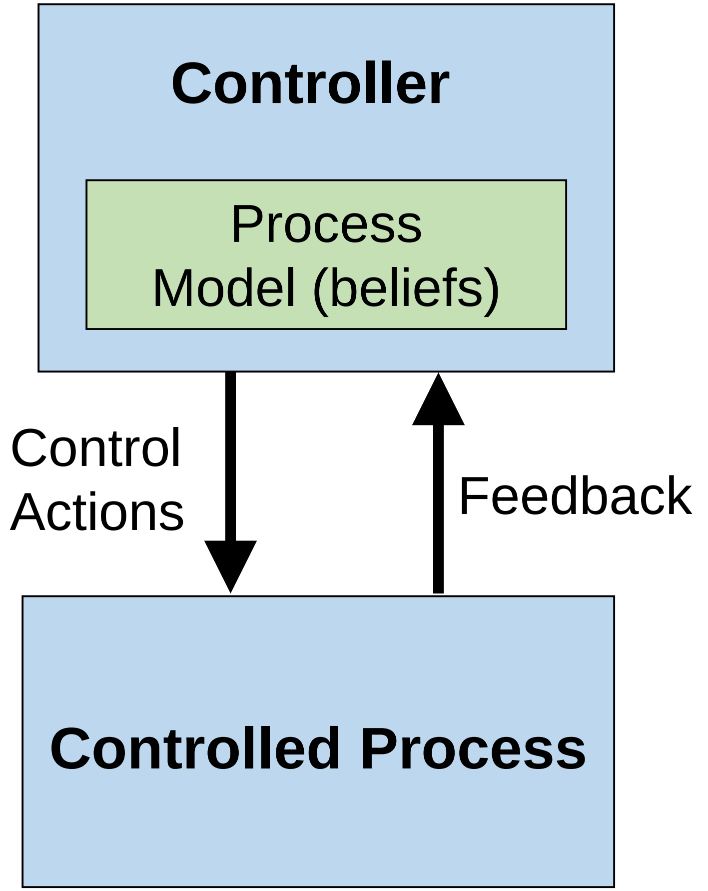
http://www.asahi.com/ajw/articles/AJ201606200006.html

Quote

- “The hardest single part of building a software system is deciding precisely what to build.”
  -- Fred Brooks, *The Mythical Man-Month*

- **ソフトウェアシステム構築の最も困難な部分をひとつあげるとするなら何を構築すべきかを的確に決定することだ**
  -- フレデリック・ブルックス, 人月の神話

Basic STAMP
"Systems Thinking"



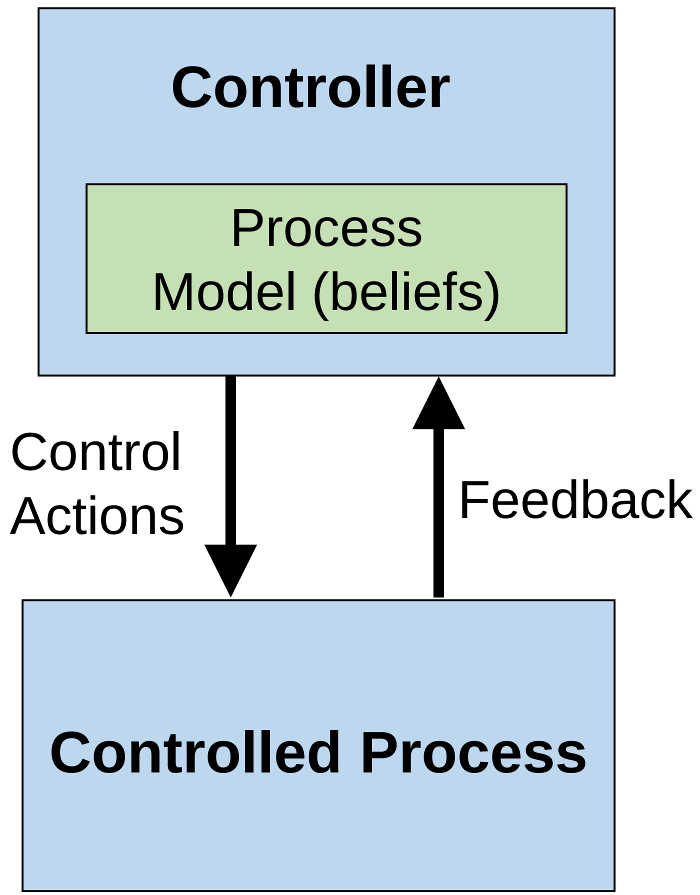
This could have prevented the real HITOMI problem!

Honda Odyssey

- 344,000 minivans recalled
- Stability control software problem
  安定性制御SWの問題
- In certain circumstances, an error in
  ある状況下で
  the software can prevent the system
  あるSWエラーが正確なキャリブレーションを妨害、
  from calibrating correctly, leading to
  これによりブレーキシステムの圧力増大につながる
  pressure building up in the braking system, the National Highway Traffic Safety Administration said.
- If pressure builds to a certain point,
  ある点に圧力が達すると
  "the vehicle may suddenly and
  車は突然予想外の急ブレーキをかけかねず
  unexpectedly brake hard, and
  それはブレーキランプを点灯することもしないため、
  without illuminating the brake lights,
  追突のリスクを高めてしまう
  increasing the risk of a crash from behind," the NHTSA said.
- 2007-2008 models affected
  - Problem discovered in 2013

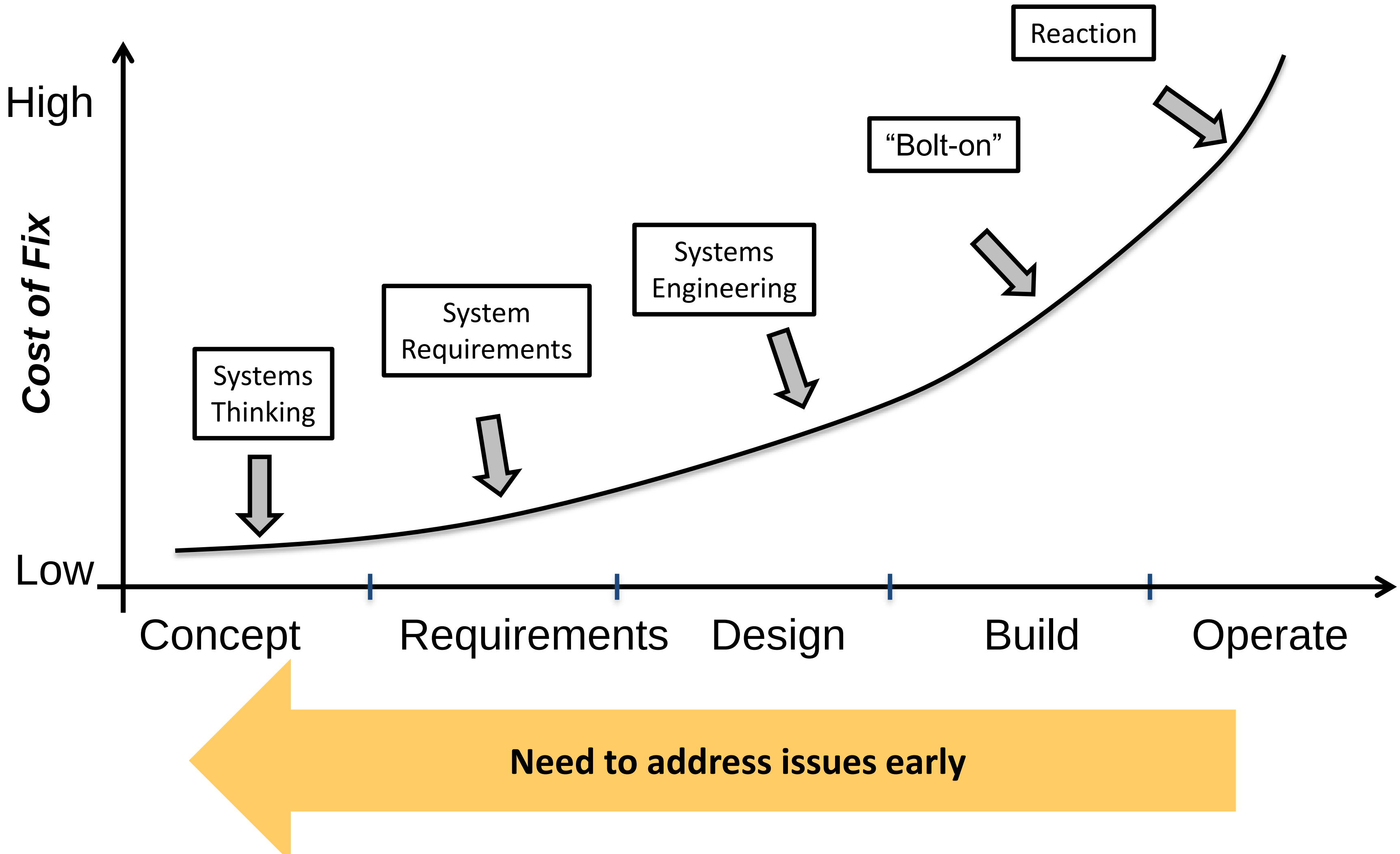
These problems made it through all existing processes: design reviews, testing, etc.
これらの問題はすべての既存のプロセスをすり抜けた：設計、レビュー、テスト、等

Basic STAMP
"Systems Thinking"



This could have anticipated the problem!

Addressing potential issues



STAMP goal: help find problems earlier when least expensive to fix!

Illustration courtesy Bill Young

Recent automotive recalls

- In October 2013, Chrysler announced a recall of 140,800 vehicles to fix a problem in the anti-lock braking **software** that can cause <u>instrument-cluster blackouts</u>
- In September 2014, Ford announced a recall of 692,500 vehicles to fix a **software** problem that could <u>delay airbag deployment</u> in a crash
- In June 2014, GM announced a recall of 392,459 vehicles to fix a problem with **software** that could cause vehicles to [effectively] <u>switch into neutral on their own</u>
- In October 2014, Audi/VW announced a recall of 850,000 vehicles for a **software** glitch that can <u>prevent airbags from deploying</u> in a crash
- In February 2014, Toyota announced a recall of 1.9 million vehicles to fix a **software** problem that could cause the vehicle to <u>power down and come to a stop</u>

http://www.autonews.com/article/20131001/RETAIL05/131009967/chrysler-recalls-142800-pickups-and-suvs-because-of-instrument
http://spectrum.ieee.org/cars-that-think/transportation/safety/ford-recalls-695-000-vehicles-for-airbag-transmission-software-updates
http://www.bloomberg.com/news/2014-06-27/gm-to-recall-about-400-000-pickups-suvs-for-software-fix.html
http://online.wsj.com/articles/audi-recalls-850-000-a4s-for-air-bag-fix-1414071876
http://www.nytimes.com/2014/02/13/business/international/toyota-issues-another-recall-for-hybrids-this-time-over-software-glitch.html?_r=0

Automotive recalls are increasing

Why?

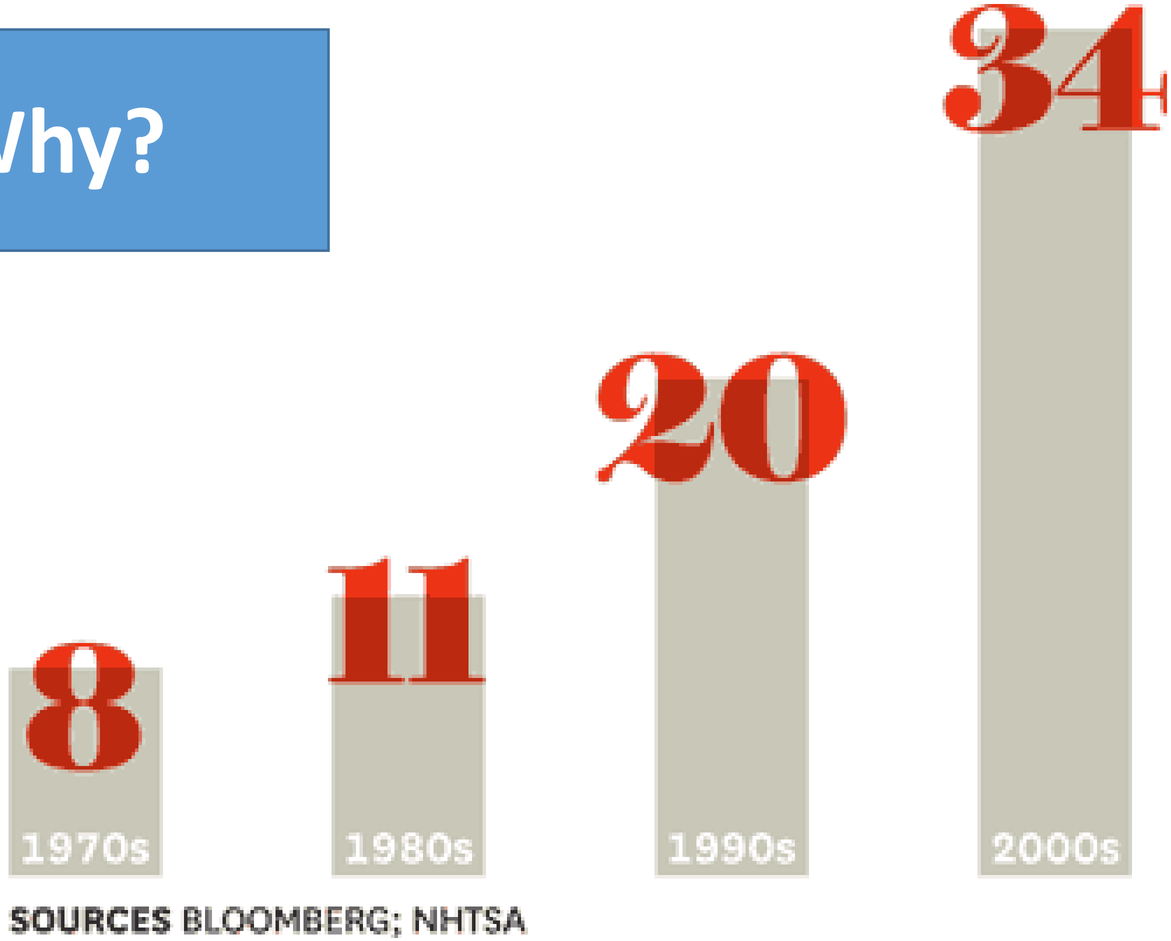
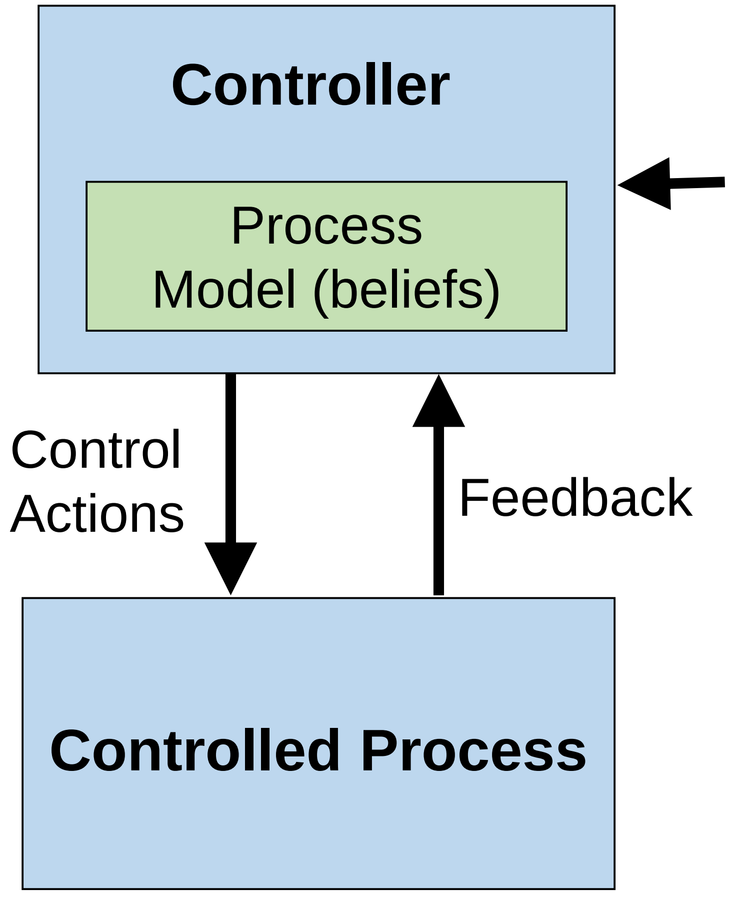


Image: https://hbr.org/2010/06/why-dinosaurs-will-keep-ruling-the-auto-industry/ar/1

Cyber-security example: 2014 Jeep Cherokee

Basic STAMP
"Systems Thinking"



Works very well for security!

Boeing 787 Lithium Battery Fires

- 2013 – 2014
- Reliability analysis
  - Predicted 10 million flight hours between battery failures
  - Careful reviews, testing, certification, etc.
- Actual experience
  - Two fires caused by battery failures in 52,000 flight hours
  - Does not include 3 other less-reported incidents of smoke in battery compartment

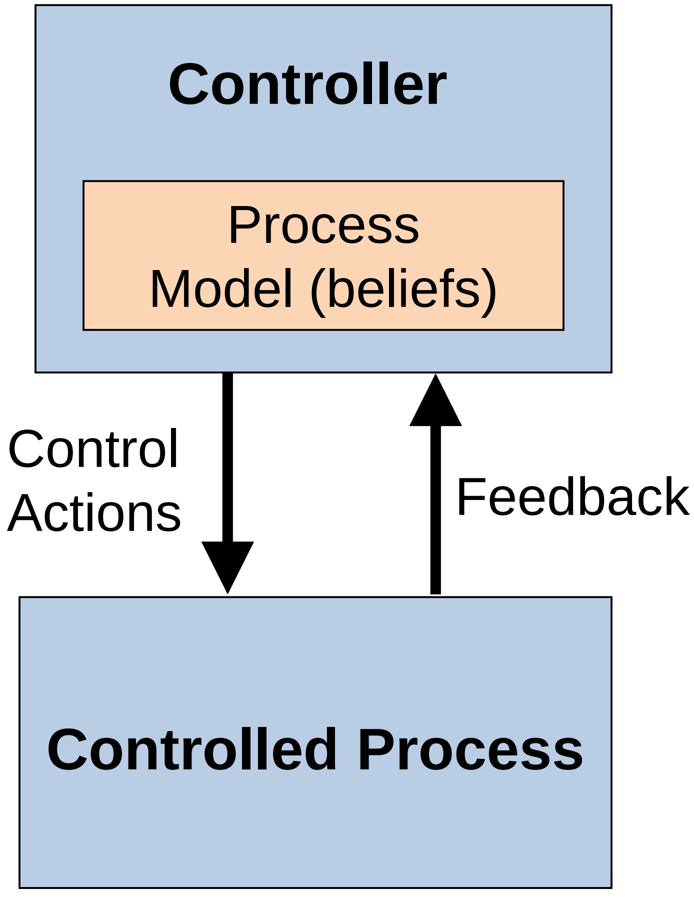
Challenges:
- **Getting accurate failure estimates**
- **Validating results (before an accident)**
- **Did we overlook other problems?**

Boeing 787 Lithium Battery Fires

- A module monitors for smoke in the battery bay, controls fans and ducts to exhaust smoke overboard.
- Power unit experienced low battery voltage, shut down various electronics including ventilation.
- Smoke could not be redirected outside cabin

This flaw passed through every standard process we have today!

A new view



- Provides another way to think about accidents
- Forms foundation for STAMP/STPA
- For each system we discuss, let’s consider how this applies

Bombardier Learjet 60 Accident

- Tires disintegrated on takeoff, pilots tried to abort
- Automation ignored pilot commands for reverse thrusters
  - The tire explosion damaged landing gear sensors
  - Computer believed aircraft in flight
  - Computer <u>increased thrust</u>

Bombardier Learjet 60 Accident

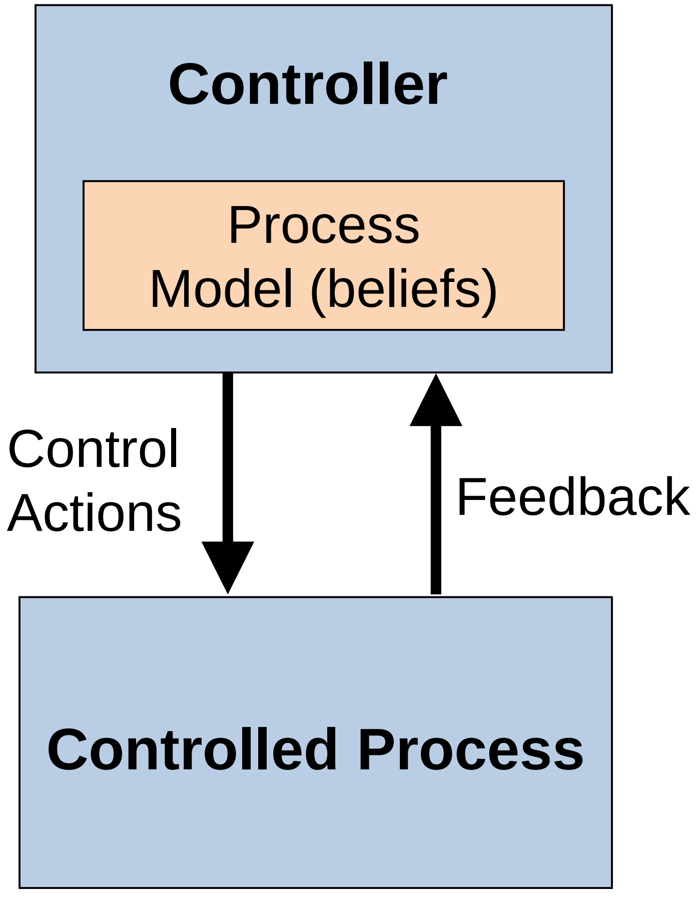
- Tires disintegrated on takeoff, pilots tried to abort
- Automation ignored pilot commands for reverse thrusters
  - The tire explosion damaged landing gear sensors
  - Computer believed aircraft in flight
  - Computer <u>increased thrust</u>

The control system operated exactly as designed!

Bombardier Learjet 60 Accident

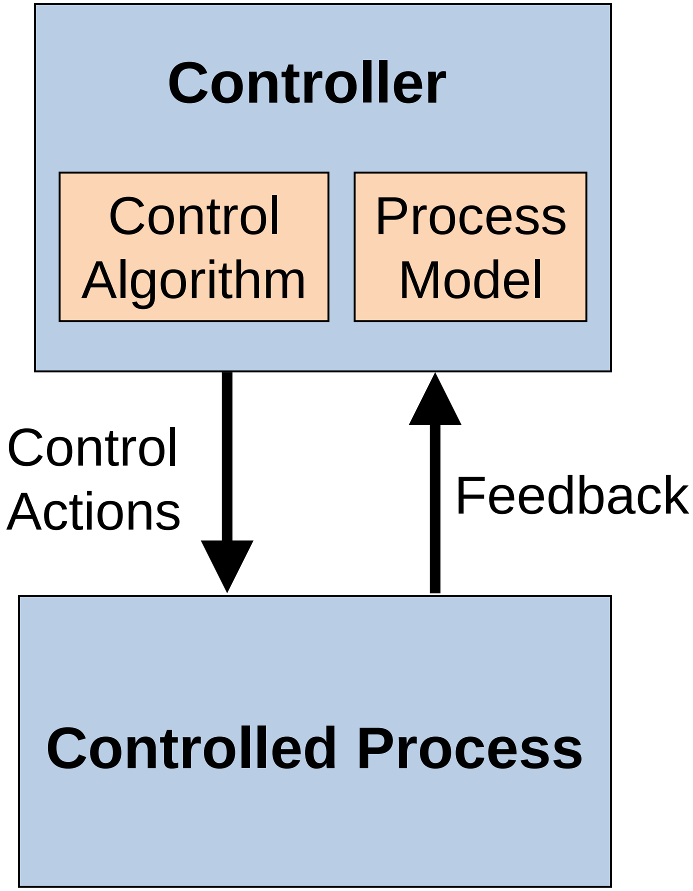
- NTSB Causes include:
  - “Deficiencies in Learjet's design of and the Federal Aviation Administration's (FAA) certification of the Learjet Model 60's thrust reverser system”
  - “The inadequacy of Learjet's safety analysis and the FAA's review of it, which failed to detect and correct the thrust reverser and wheel well design deficiencies after a 2001 uncommanded forward thrust accident”

A new view



- Provides another way to think about accidents
- Forms foundation for STAMP/STPA
- For each system we discuss, let’s consider how this applies

STAMP: basic control loop

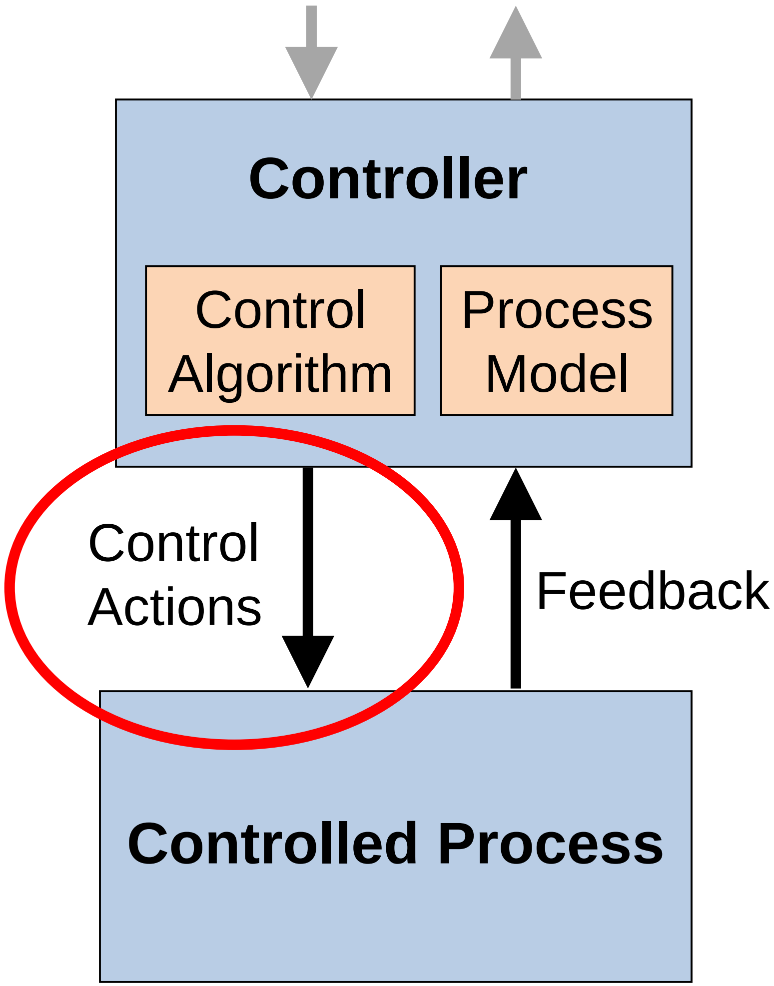


- **Control actions** are provided to affect a controlled process
- **Feedback** may be used to monitor the process
- **Process model** (beliefs) formed based on feedback and other information
- **Control algorithm** determines appropriate control actions given current beliefs

Captures software errors, human errors, flawed requirements,…

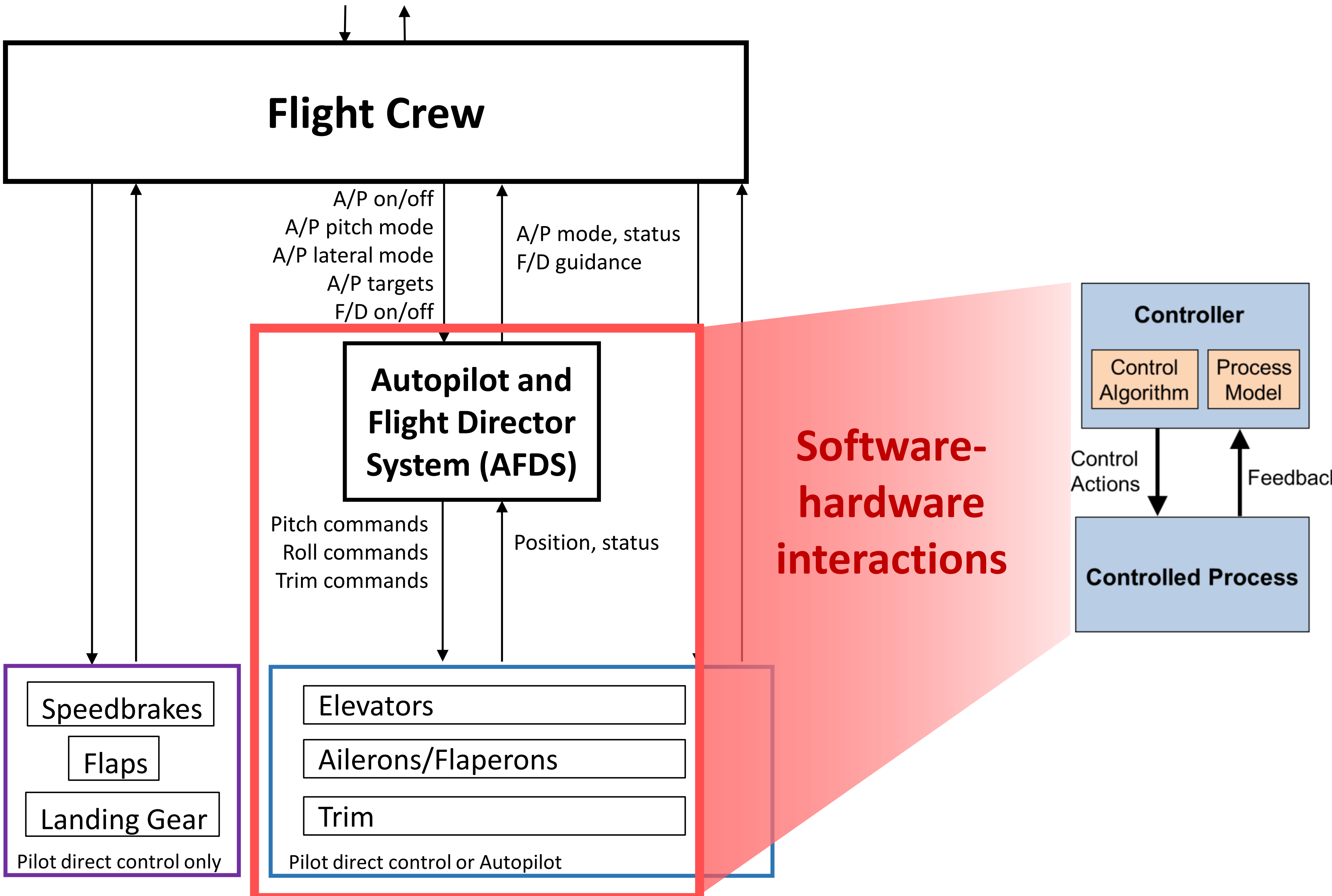
Four types of **unsafe control actions**:

1) Control commands required for safety are not given
2) Unsafe ones are given
3) Potentially safe commands but given too early, too late
4) Control action stops too soon or applied too long



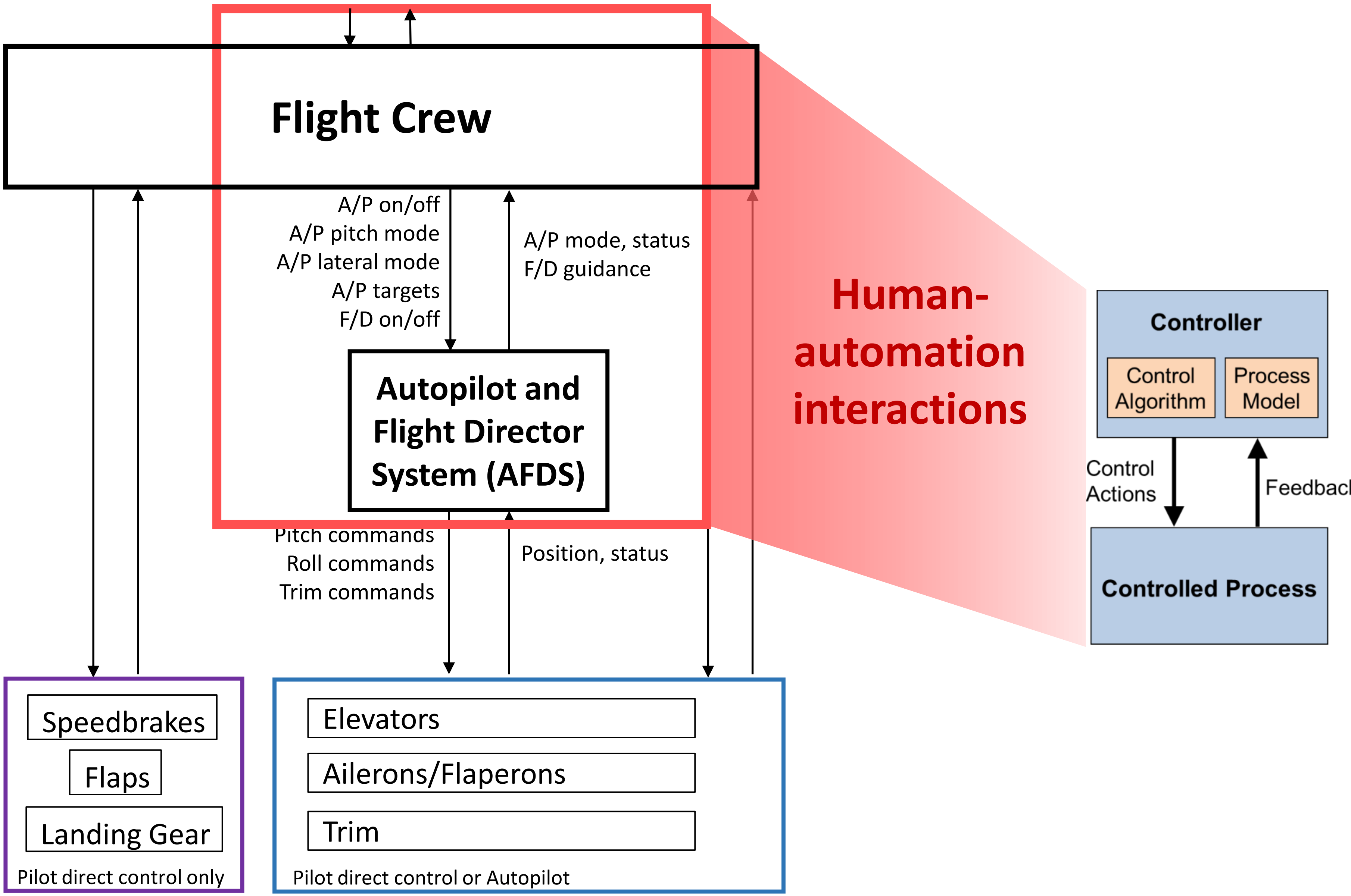
(Leveson, 2012)

STAMP: Control Structure



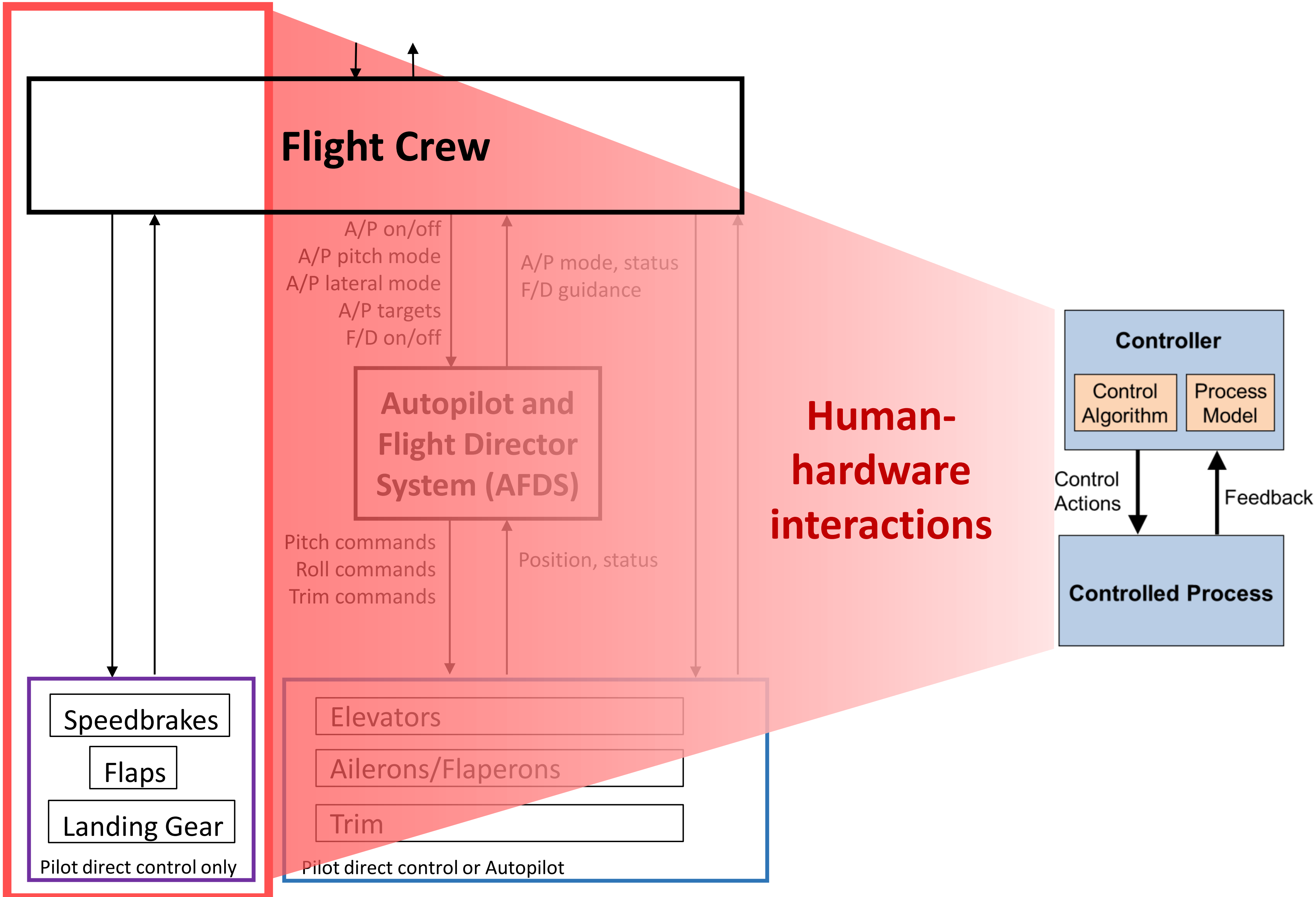
Thomas, 2017

STAMP: Control Structure



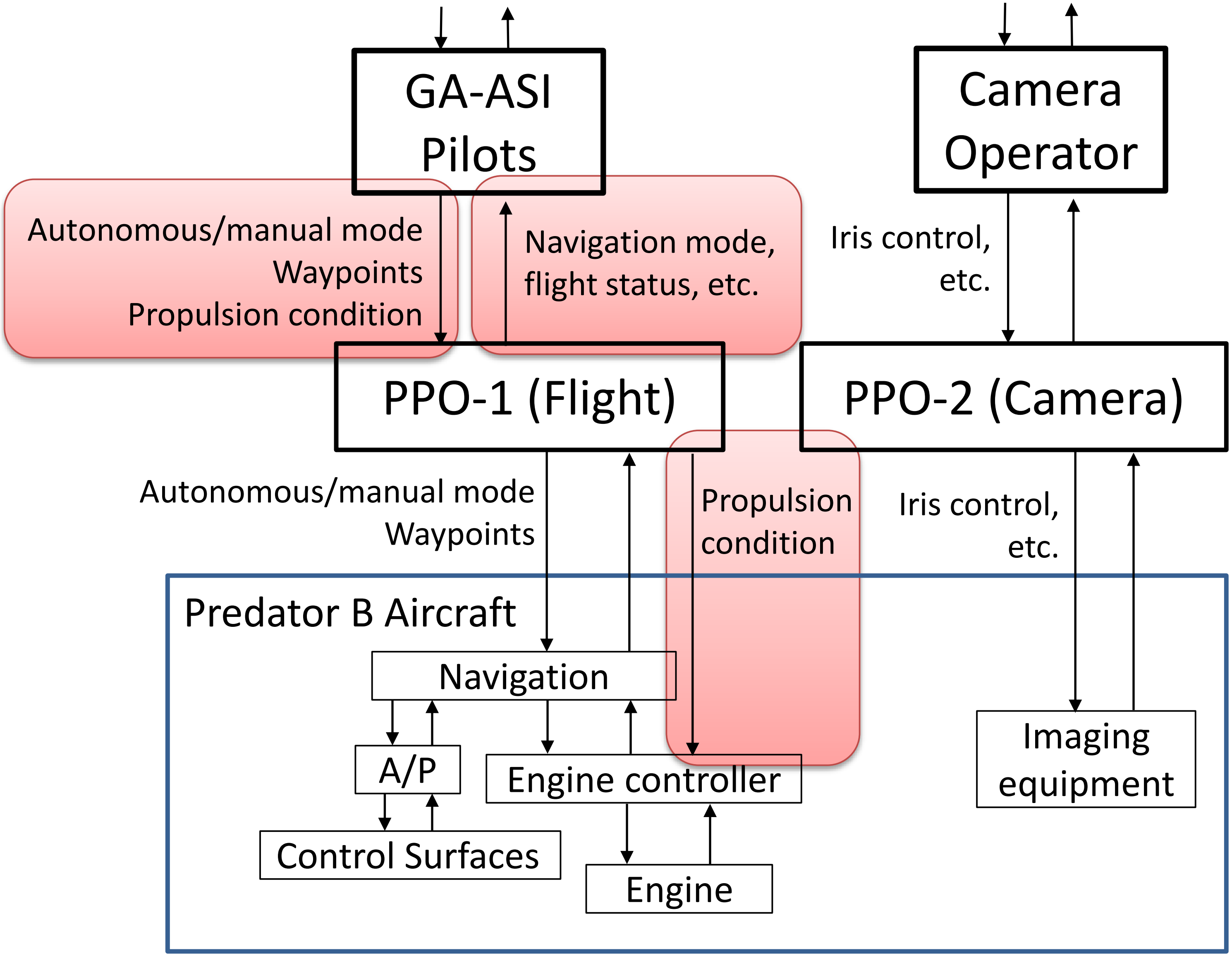
Thomas, 2017

STAMP: Control Structure



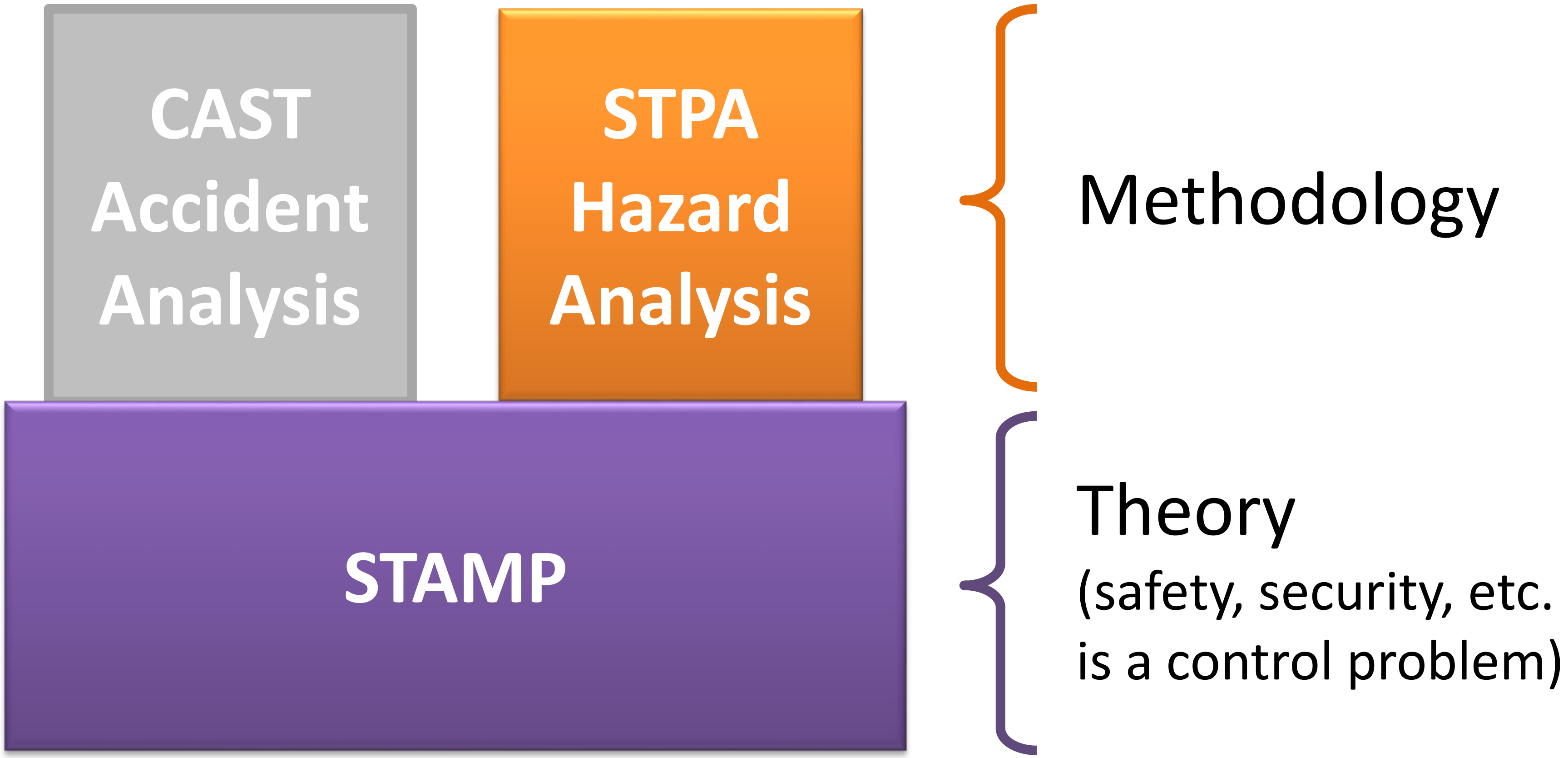
Thomas, 2017

Unmanned Predator-B Crash (US CBP)

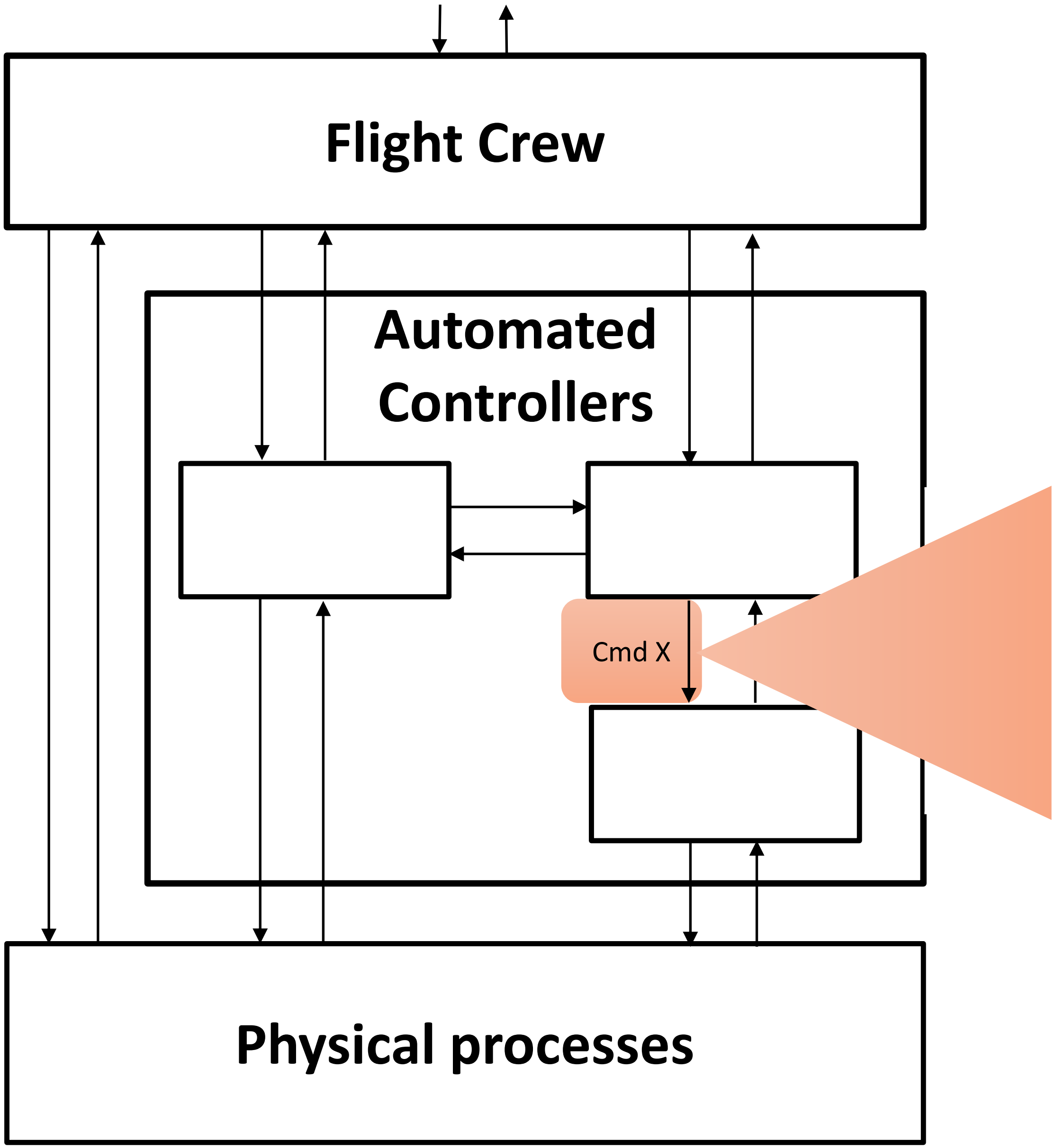


Thomas, 2017

STAMP and STPA



STPA: Unsafe Control Actions (UCA)

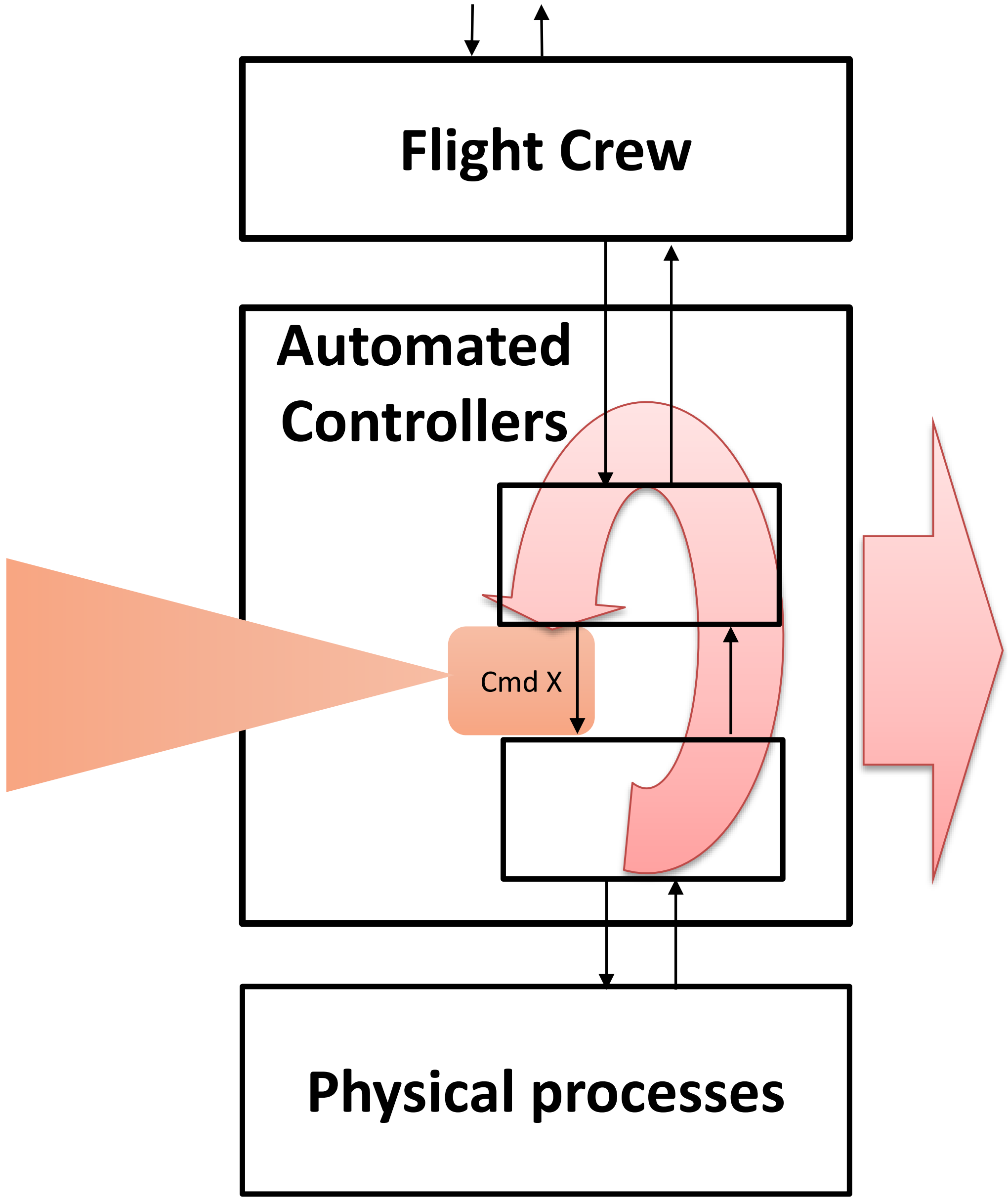


Not provided causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long

Thomas, 2017

STPA: Identify Accident Scenarios

What could cause Unsafe Control Actions?

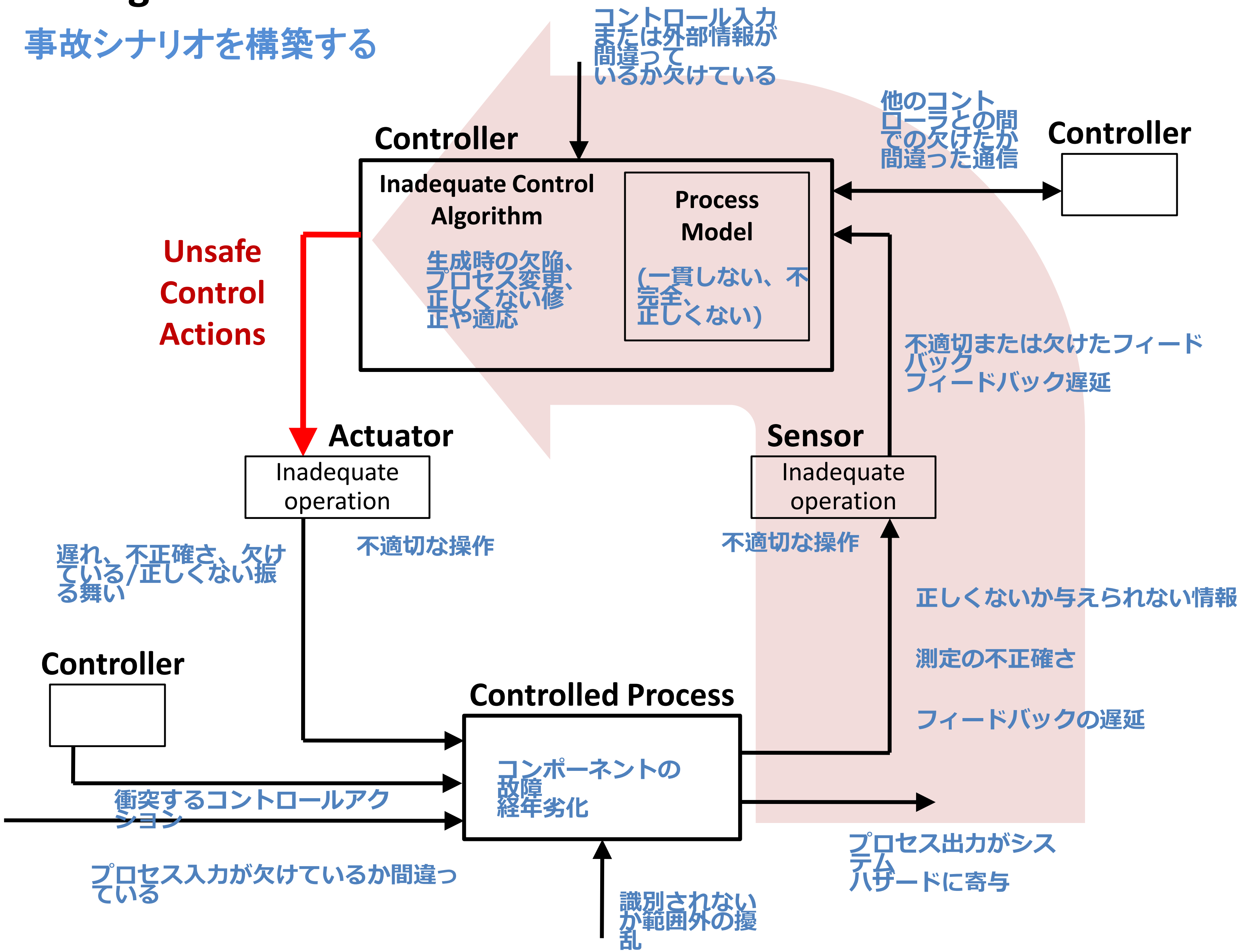


Scenarios
Controller incorrectly believes X because …
Controller control algorithm does not enforce Y because …
Incorrect feedback Z received because …
Sensor failure causes…
Etc.

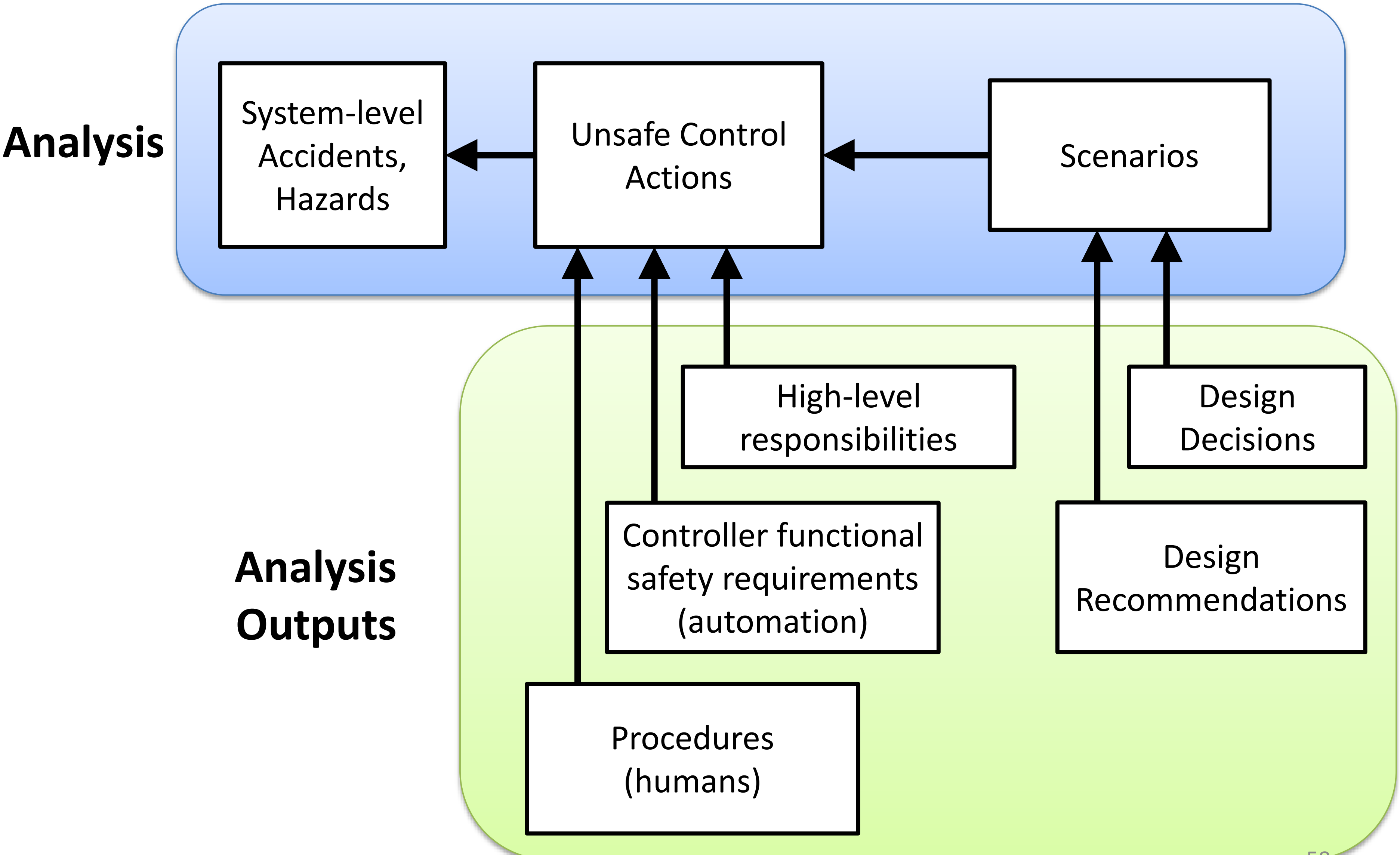
Thomas, 2017

Building Accident Scenarios

事故シナリオを構築する



STPA: Traceability



Thomas, 2017

How does STPA compare?

- MIT: TCAS
  - Existing high quality fault tree done by MITRE for FAA
  - MIT comparison: STPA found everything in fault tree, plus more
- JAXA: HTV
  - Existing fault tree reviewed by NASA
  - JAXA comparison: STPA found everything in fault tree, plus more
- EPRI: HPCI/RCIC
  - Existing fault tree & FMEA overlooked causes of real accident
  - EPRI comparison: Blind study, only STPA found actual accident scenario
- Safeware: U.S. Missile Defense Agency BMDS
  - Existing hazard analysis per U.S. military standards
  - Safeware comparison: STPA found everything plus more
  - STPA took 2 people 3 months, MDA took 6 months to fix problems
- MIT: NextGen ITP
  - Existing fault tree & event tree analysis by RTCA
  - MIT comparison: STPA found everything in fault tree, plus more
- MIT: Blood gas analyzer
  - Existing FMEA found 75 accident causes
  - STPA by S.M. student found 175 accident causes
  - STPA took less effort, found 9 scenarios that led to FDA Class 1 recall

Automotive companies using STAMP/STPA

Other large silicon valley companies*

Annual STAMP Workshops (free)

Industries:
Automotive
Oil and Gas
Space
Aviation
Defense
Nuclear
Healthcare and Healthcare IT
Medical Devices
Academia
Insurance
Academia (Education)
Hydropower
Chemicals
Software/Computing
Government
Industrial Automation
Electric Utility
Security
Think Tank
Transportation
Maritime (security)
Environmental
Pharmaceuticals
Internet

Organizations:
General Motors
Ford
Nissan Motor Company
Toyota
Draper Lab
Volpe National Transportation Research Center
The Boeing Company
Boeing Environment Health and Safety
Boeing Engineering and Operations
Embraer
U.S. Nuclear Regulatory Commission
U.S. Army
GE Aviation
Sikorsky
Thoratec Corporation
University of Alabama in Huntsville
Liberty Mutual Safety Research Institute
ITA (Instituto Tecnologico de Aeronautica)
Jeppesen
Beijing Institute of Technology
TEGMA Gestao Logistica S.A.
Amsterdam University of Applied Sciences
Dutch Safety Agency
University of Stuttgart
BC Hydro
Therapeutic Goods Administration
Institute of Aeronautics and Space (IAE), Brazil
Shell Oil
University of Braunschweig
Stiki
Reykjavik University
National Nuclear Energy Commission, Brazil
FAA
U.S. Department of Transportation
U.S. Air Force
U.S. Navy
IPEV (Institute for Research and Flight Testing), Brazil
Japan Aerospace Exploration Agency (JAXA)
U.S. Department of Energy
Rockwell Automation
Democritus University of Thrace
Dependable Management
ILF Consulting Engineers
JETRO (Japan)
Alliance for Clinical Research Excellence and Safety
Washington CORE
Florida Institute of Technology
U.S. Navy Strategic Systems Programs
IPEN (Institute for Nuclear and Energy Research), Brazil
Duke Energy
Synensis
Japan MOT Society
Tufts University
Southern Company
U.S. Army Aviation Engineering
U.S. Army Corps of Engineers (Kansas City District)
University of Houston, Clear Lake
Lincoln Lab
Hanscom AFB
U.S. Army Research, Development, and Engineering Command
McMaster University
Bechtel
Kyushu University (Japan)
Analog Devices
Cummins
University of Massachusetts Dartmouth
Syracuse Safety Research
National Civil Aviation Agency (ANAC0, Brazil
State Nuclear Power Automation System Engineering Company (China)
Toyota Central R&D Labs
Massachusetts General Hospital
AstraZeneca
STM (Defense Technology Engineering and Trading Corp., Turkey)
Varian Medical Systems
Fort Hill Group
TUBITAK-UZAY (Scientific and Technological Research Council of TURKEY-Space Technologies Research Institute)
Cranfield University (U.K.)
U.S. Air Force Test Pilot School
NASA/Bastion Technologies
U.S. Customs and Border Protection
Second Curve Systems
Vequria
Akamai Technologies
Canadian Dept. of Defense (DND)
University of Virginia
MSAG
Novartis
U.S. Coast Guard
EPRI (Electric Power Research Institute)
Sandia National Laboratories
Lawrence Livermore National Laboratories
Tapestry Solutions
Kansas State University
Systems Planning and Analysis
Zurich University of Applied Sciences
IBM
Lawrence Berkeley National Laboratory (LBNL)
U.S. Navy School of Aviation Safety
JAMSS (Japanese Manned Space Systems)
U.S. Chemical Safety Board

mit.edu/psas

Countries: USA, Brazil, Japan, China, Netherlands, Germany, Canada, Australia, Iceland, Greece, United Kingdom, Turkey, Estonia, Australia

Please contact me!

- JThomas4@mit.edu
- Send me questions or comments!