AWO

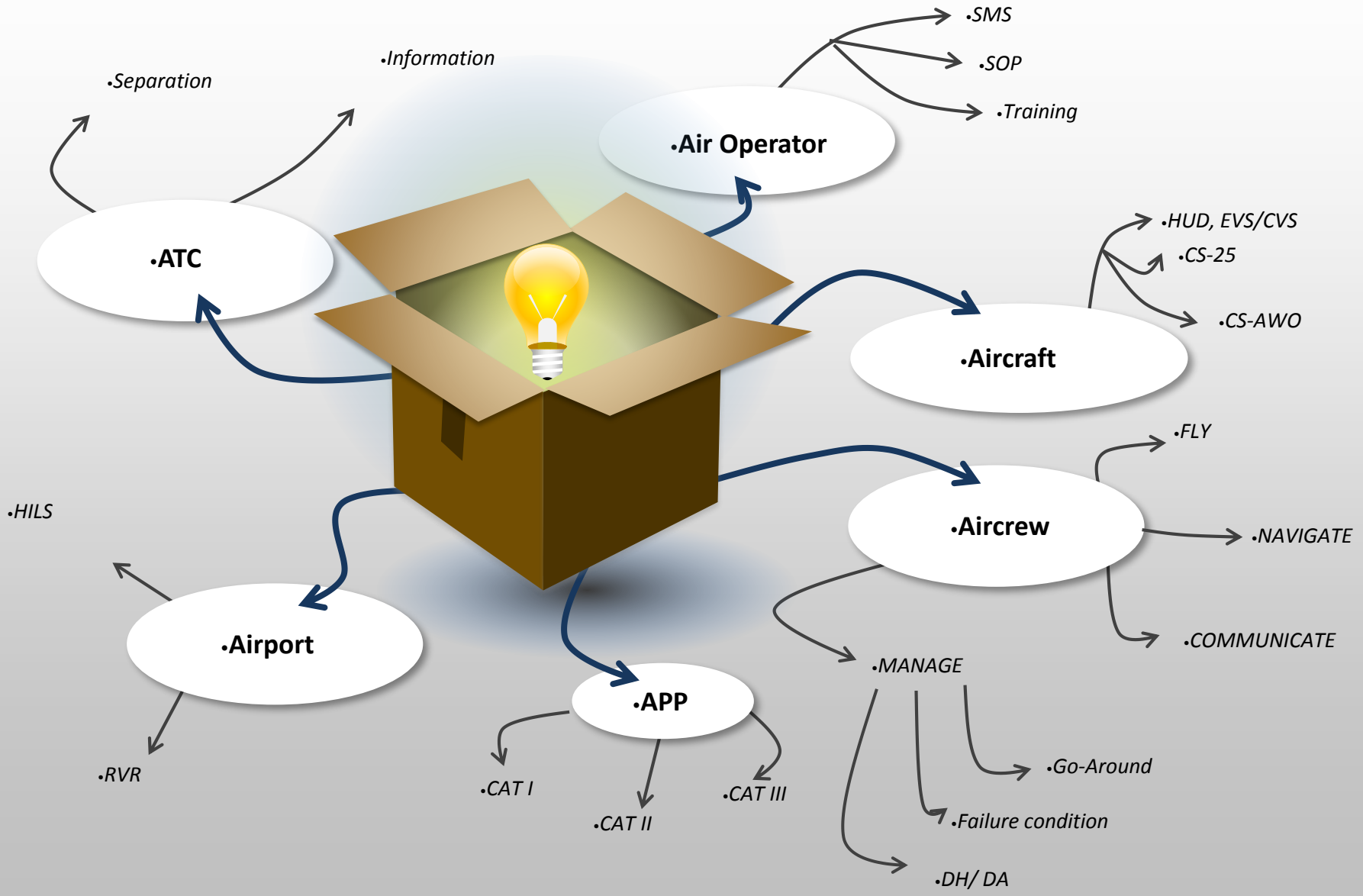
Bernard Bourdon
Aircrew & Medical Progamme Manager, EASA

09 November 2016

Your safety is our mission.

An agency of the European Union

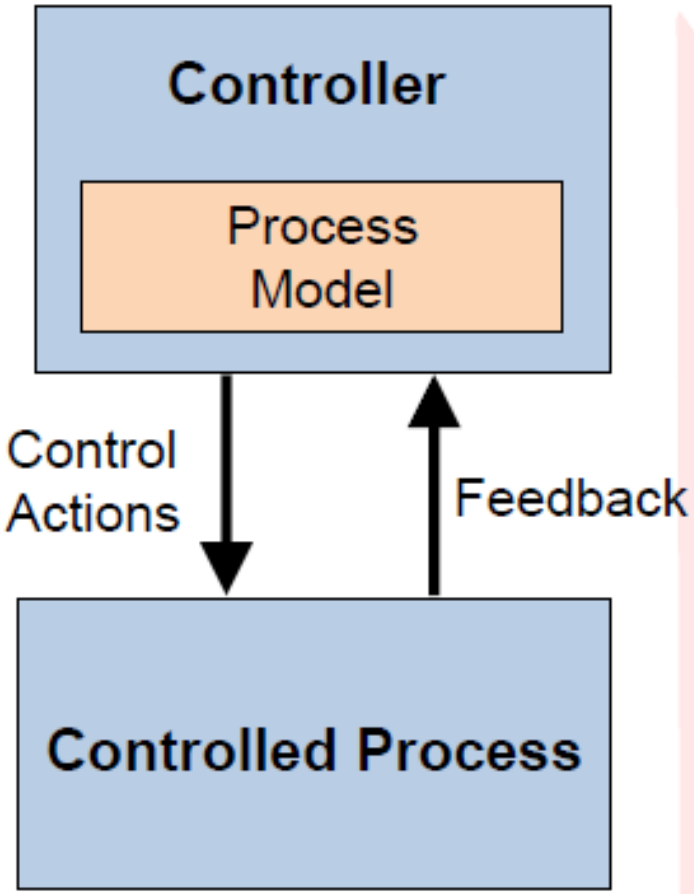
AWO Hazards Assessement

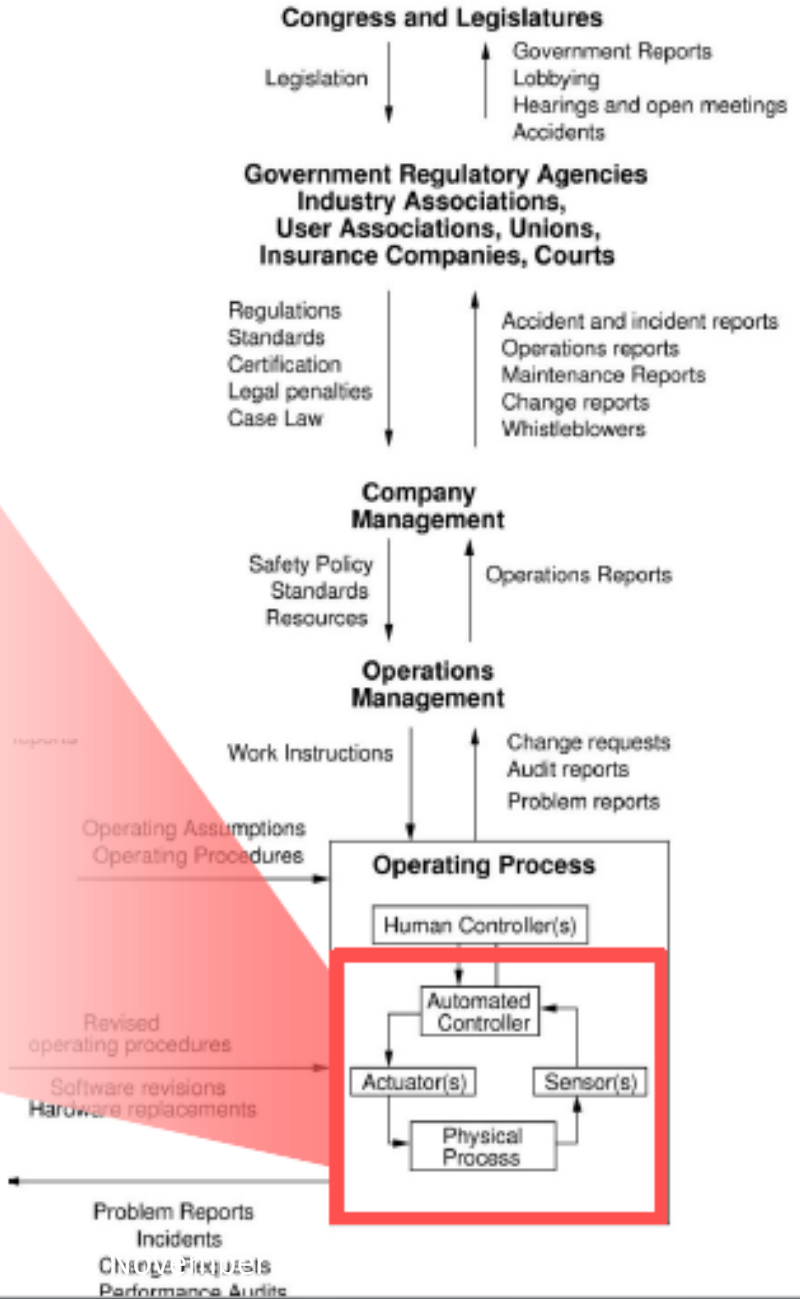


Systems Theory

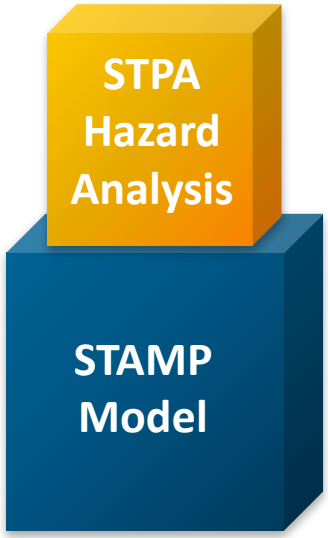
- Developed to handle systems with “organized complexity”
- Focuses on systems taken as a whole, not on parts taken separately
  - Some properties can only be treated adequately in their entirety, taking into account all social and technical aspects
  - These properties derive from relationships among the parts of the system - How they interact and fit together
- Safety is an emergent system property
  - It is NOT a component property
  - It can only be analyzed in the context of the whole

STAMP

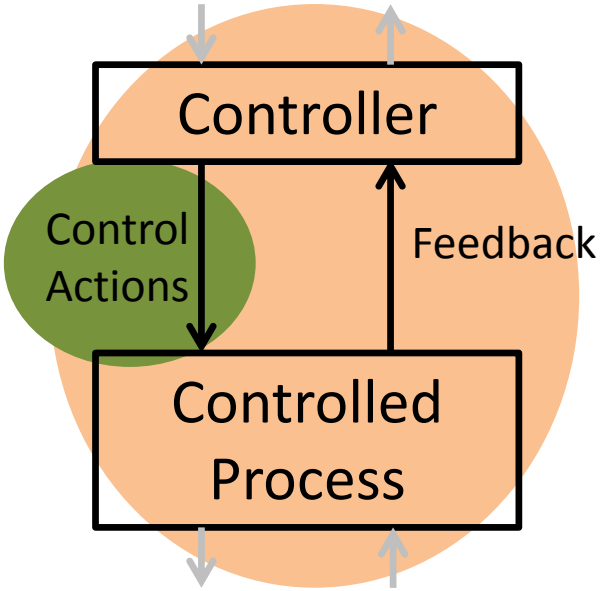

Controller
Process Model
Control Actions
Feedback
Controlled Process


Congress and Legislatures
Legislation
Government Reports
Lobbying
Hearings and open meetings
Accidents
Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts
Regulations
Standards
Certification
Legal penalties
Case Law
Accident and incident reports
Operations reports
Maintenance Reports
Change reports
Whistleblowers
Company Management
Safety Policy
Standards
Resources
Operations Reports
Operations Management
Work Instructions
Change requests
Audit reports
Problem reports
Operating Assumptions
Operating Procedures
Operating Process
Human Controller(s)
Automated Controller
Actuator(s)
Sensor(s)
Physical Process
Revised operating procedures
Software revisions
Hardware replacements
Problem Reports
Incidents
Change Requests
Performance Audits

XSTAMPP



- Identify Hazards and Accidents
- Construct the control structure
- Step 1: Identify Unsafe Control Actions
- Step 2: Identify causal factors and control flaws

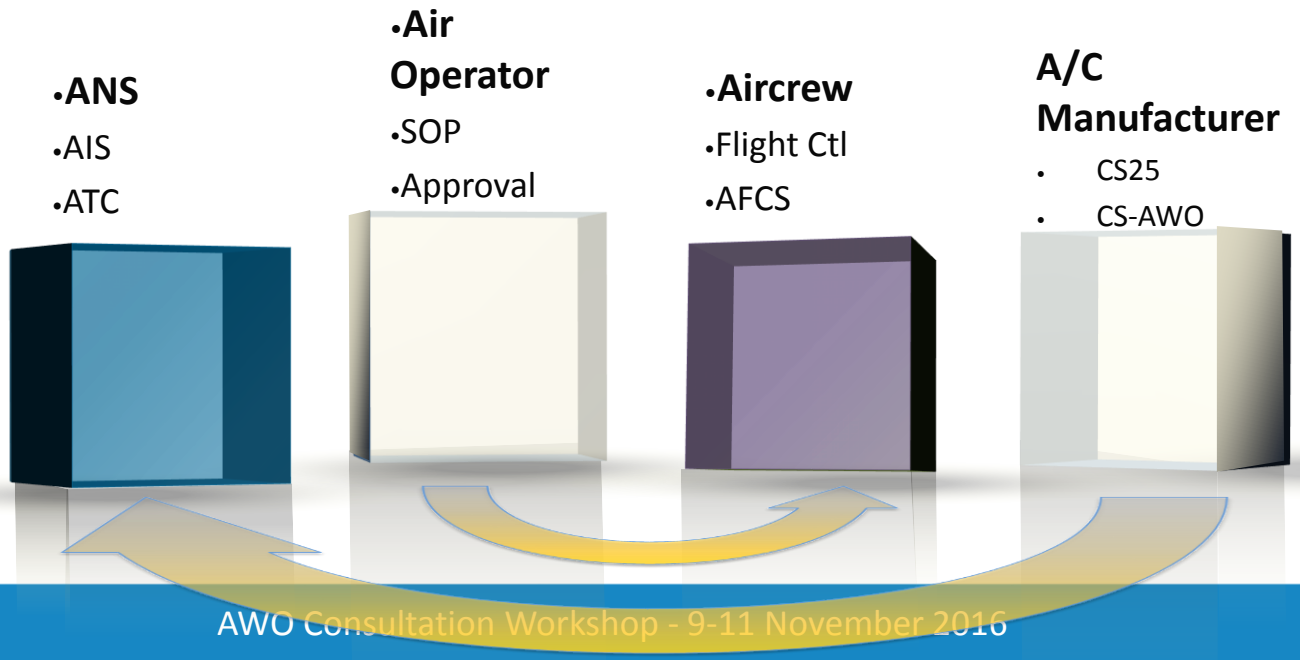


STAMP Process

- 1. Identify Hazards and Accidents
- 2. Construct the control structure
- 3. Identify Unsafe Control Actions
- 4. Identify causal factors and control flaws

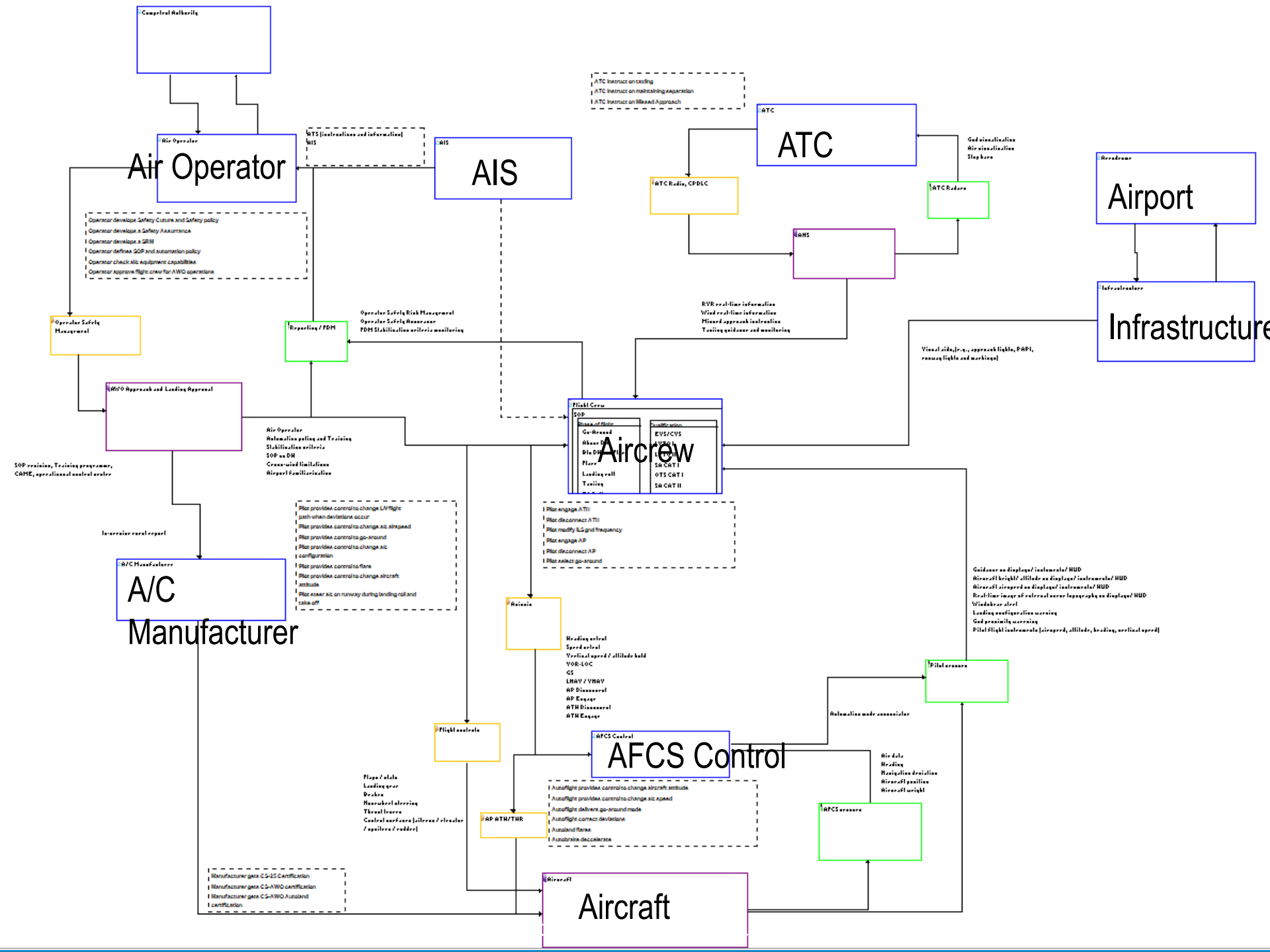
Generalities on the model

- Simplification added
  - Pilot Fly (i.e keep a/c attitude along 3 axis)
  - Pilot Navigate (i.e. correct deviations along 3 axis)
  - Pilot Manage (i.e. drive AFCS, Go-Around…)
  - Pilot Communicate
- Focus on global inter-system relationship <u>in all cases</u>



STAMP Process

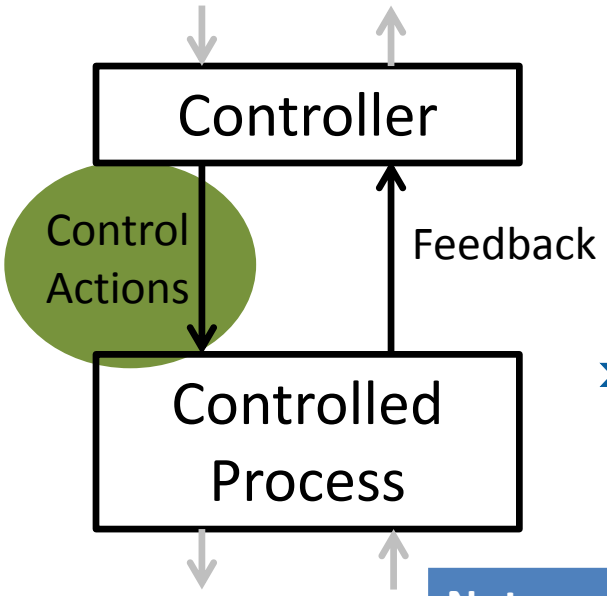
- 1. Identify Hazards and Accidents
- 2. Construct the control structure
- 3. Identify Unsafe Control Actions
- 4. Identify causal factors and control flaws


Air Operator
AIS
ATC
Airport
Infrastructure
Aircrew
A/C Manufacturer
AFCS Control
Aircraft

STAMP Process

- 1. Identify Hazards and Accidents
- 2. Construct the control structure
- 3. Identify Unsafe Control Actions
- 4. Identify causal factors and control flaws

STPA Step 1: Unsafe Control Action (UCA)



- Safety is an emergent property that arises when system components interact with each other within a larger environment
  - A set of constraints related to behavior of system components enforces that property
  - Accidents occur when interactions violate those constraints (a lack of appropriate constraints on the interactions)
  - "Controllers" embody or enforce those constraints
- Events are the result of the inadequate control
  - Result from lack of enforcement of safety constraints by design and operations

	Not providing causes hazard	Providing causes hazard	Incorrect Timong / Order	Stopped too soon / applied too long
Control Action				

STPA Step 1: Unsafe Control Action (UCA)

- Process Model Variables
  - A more rigorous approach

Control Action	Process Model Variable 1	Process Model Variable 1	Hazardous?

Process Model Variables	Values
Qualification	LVP
Qualification	LVTO I
Qualification	LVTO II
Qualification	Type A
Qualification	CAT I
Qualification	SA CAT I
Qualification	OTS CAT I
Qualification	CAT II
Qualification	SA CAT II
Qualification	OTS CAT II
Qualification	CAT III
Qualification	EVS/CVS
Phase of flight	Above DH
Phase of flight	Btn DH and Flare
Phase of flight	Flare
Phase of flight	Landing Roll
Phase of flight	Taxiing
Phase of flight	TO Roll
Phase of flight	Go around

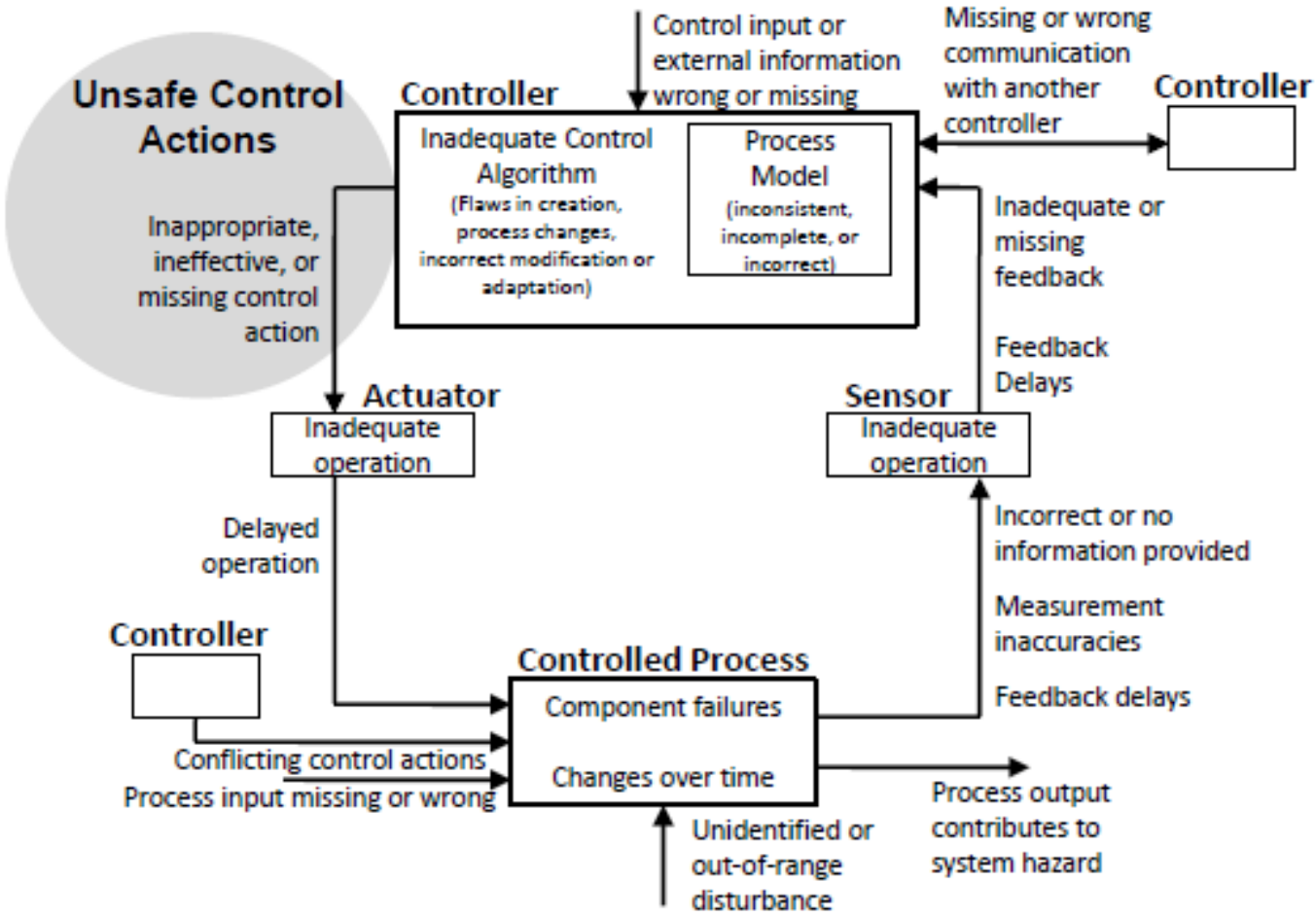
ID_CA	Source	Destination	Control Action	Control Action Type	ID CA	Unsafe Controlled Action	UCA Hazards	Process Model	Hazardous
CA.101	Flight Crew	Flight Controls	Pilote provides control to change L/V flight path when deviations occur	Not providing causes hazard	UCA.101.1	Pilot does not provide control to change L/V flight patch when deviat occurs above DH	[H-2][H-5][H-7][H-4]	Above DH	Y
CA.101	Flight Crew	Flight Controls	Pilote provides control to change L/V flight path when deviations occur	Not providing causes hazard	UCA.101.2	Pilot does not provide control to change L/V flight patch when deviation occurs between DH and flare	[H-2][H-5][H-7][H-4]	Btn DH and Flare	Y
CA.101	Flight Crew	Flight Controls	Pilote provides control to change L/V flight path when deviations occur	Not providing causes hazard	UCA.101.3	Pilot does not provide control to change L/V flight patch when deviat occurs during flare	[H-2][H-5][H-7][H-4]	Flare	Y
CA.101	Flight Crew	Flight Controls	Pilot provides control to change L/V flight path when deviations occur	Not providing causes hazard	UCA.101.4	Pilot does not provide control to change L/V flight path when deviat occurs during landing roll	[H-2][H-5][H-7][H-4]	Landing Roll	Y
CA.101	Flight Crew	Flight Controls	Pilot provides control to change L/V flight path when deviations occur	Not providing causes hazard	UCA.101.5	Pilot does not provide control to change L/V flight patch when deviat occurs during taxi	[H-2][H-5][H-7][H-4]	Taxiing	Y
CA.101	Flight Crew	Flight Controls	Pilot provides control to change L/V flight path when deviations occur	Not providing causes hazard	UCA.101.6	Pilot does not provide control to change L/V flight patch when deviat occurs during take off roll	[H-2][H-5][H-7][H-4]	TO Roll	Y
CA.101	Flight Crew	Flight Controls	Pilot provides control to change L/V flight path when deviations occur	Providing causes hazard	UCA.101.7	Pilot provides control to change L/V flight path when established on flight path before DH	[H-2][H-7][H-5][H-1]	Above DH	Y
CA.101	Flight Crew	Flight Controls	Pilot provides control to change L/V flight path when deviations occur	Providing causes hazard	UCA.101.8	Pilot provides control to change L/V flight path when established on flight path between DH and flare	[H-2][H-7][H-5][H-1]	Btn DH and Flare	Y
CA.101	Flight Crew	Flight Controls	Pilot provides control to change L/V flight path when deviations occur	Providing causes hazard	UCA.101.9	Pilot provides control to change L/V flight path when established on flight path at flare	[H-2][H-7][H-5][H-1]	Flare	
CA.101	Flight Crew	Flight Controls	Pilot provides control to change L/V flight path when deviations occur	Providing causes hazard	UCA.101.10	Pilote provides control to change L/V flight path when established on flight path during landing roll	[H-2][H-7][H-5][H-1]	Landing Roll	Y
CA.101	Flight Crew	Flight Controls	Pilot provides control to change L/V flight path when deviations occur	Providing causes hazard	UCA.101.11	Pilote provides control to change L/V flight path when established on flight path during take off roll	[H-2][H-7][H-5][H-1]	TO Roll	Y
CA.101	Flight Crew	Flight Controls	Pilot provides control to change L/V flight path when deviations occur	Wrong timing or order causes hazard	UCA.101.12	Pilot lagged or provides a wrong change to L/V flight path and increase deviations before DH	[H-7][H-5][H-2]	Above DH	Y
CA.101	Flight Crew	Flight Controls	Pilot provides control to change L/V flight path when deviations occur	Wrong timing or order causes hazard	UCA.101.13	Pilot lagged or provides a wrong change to L/V flight path and increase deviations between DH and flare	[H-7][H-5][H-2]	Btn DH and Flare	Y
CA.101	Flight Crew	Flight Controls	Pilot provides control to change L/V flight path when deviations occur	Wrong timing or order causes hazard	UCA.101.14	Pilot lagged or provides a wrong change to L/V flight path and increase deviations during flare	[H-7][H-5][H-2]	Flare	Y
CA.101	Flight Crew	Flight Controls	Pilot provides control to change L/V flight path when deviations occur	Wrong timing or order causes hazard	UCA.101.15	Pilot lagged or provides a wrong change to L/V flight path and increase deviations during landing roll	[H-7][H-5][H-2]	Landing Roll	Y
CA.101	Flight Crew	Flight Controls	Pilot provides control to change L/V flight path when deviations occur	Wrong timing or order causes hazard	UCA.101.16	Pilot lagged or provides a wrong change to L/V flight path and increase deviations during take off roll	[H-7][H-5][H-2]	TO Roll	Y

STAMP Process

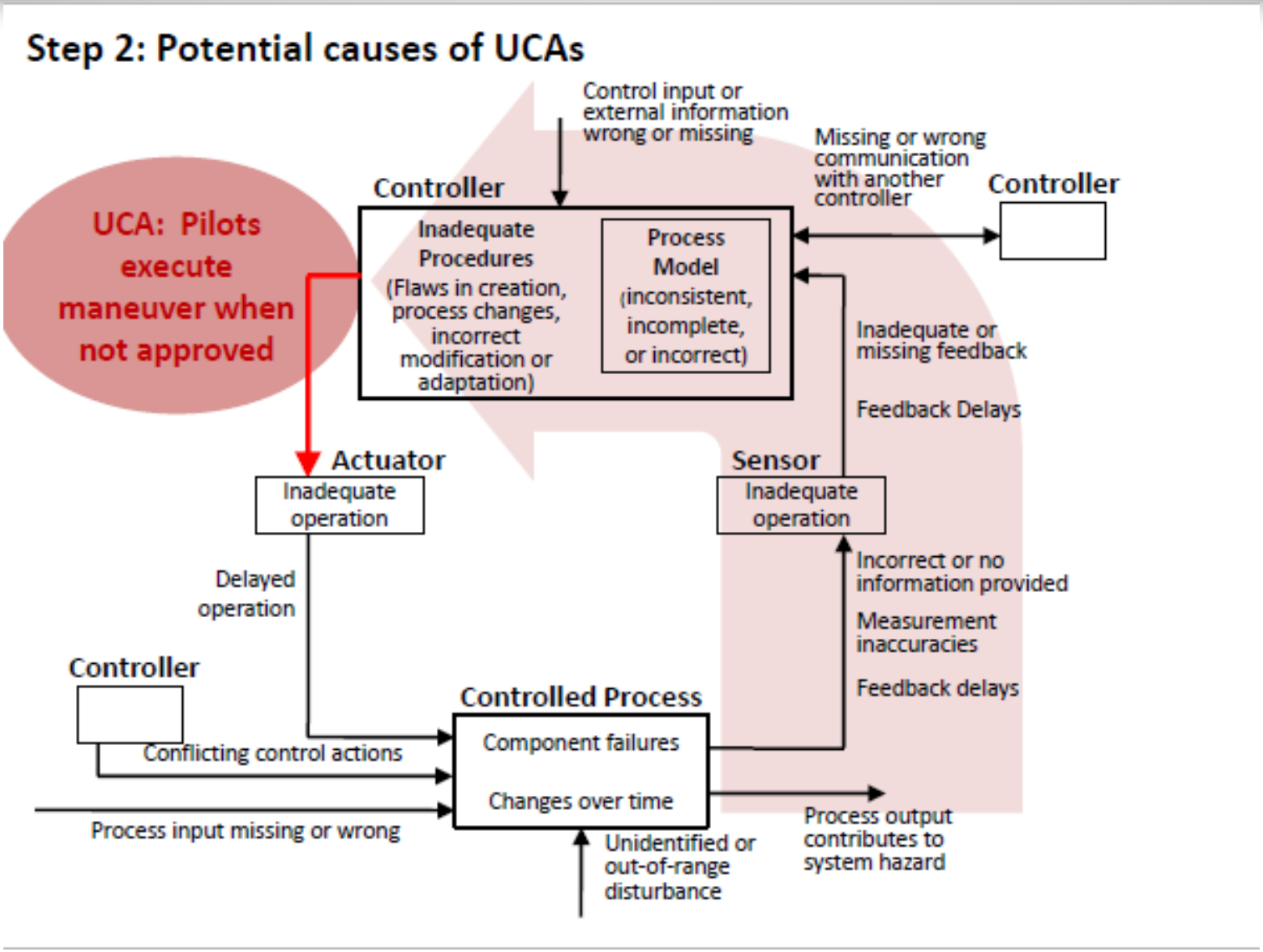
- 1. Identify Hazards and Accidents
- 2. Construct the control structure
- 3. Identify Unsafe Control Actions
- 4. Identify causal factors and control flaws

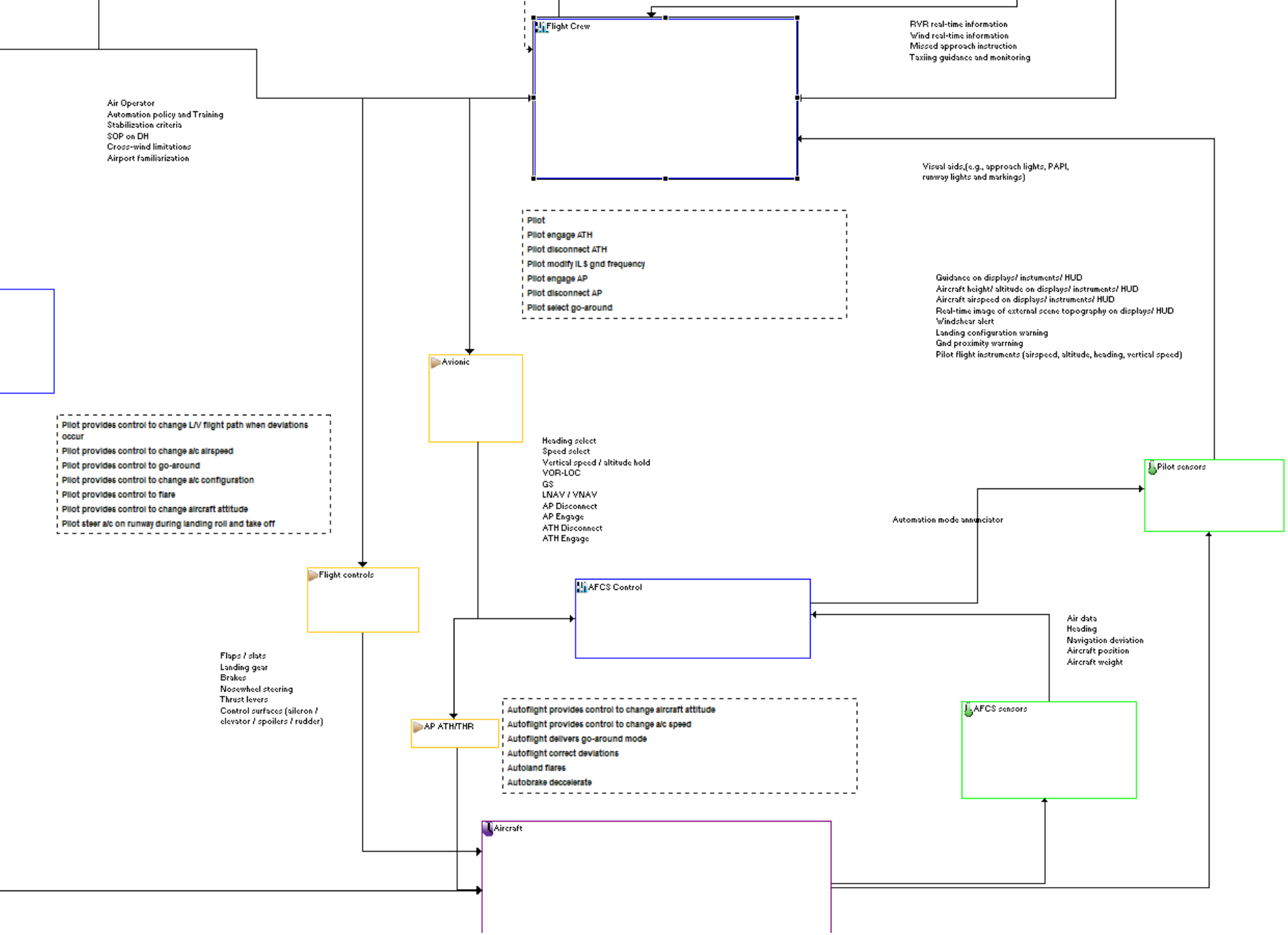
Control Flaws identification

STPA Step 2: Identify Control Flaws



Link UCAs to Control Flaws




Flight Crew
RVR real-time information
Wind real-time information
Missed approach instruction
Taxiing guidance and monitoring
Air Operator
Automation policy and Training
Stabilization criteria
SOP on DH
Cross-wind limitations
Airport familiarization
Visual aids,(e.g., approach lights, PAPI, runway lights and markings)
Pilot
Pilot engage ATH
Pilot disconnect ATH
Pilot modify IL S gnd frequency
Pilot engage AP
Pilot disconnect AP
Pilot select go-around
Guidance on displays/ instruments/ HUD
Aircraft height/ altitude on displays/ instruments/ HUD
Aircraft airspeed on displays/ instruments/ HUD
Real-time image of external scene topography on displays/ HUD
Windshear alert
Landing configuration warning
Gnd proximity warning
Pilot flight instruments (airspeed, altitude, heading, vertical speed)
Avionic
Pilot provides control to change L/V flight path when deviations occur
Pilot provides control to change a/c airspeed
Pilot provides control to go-around
Pilot provides control to change a/c configuration
Pilot provides control to flare
Pilot provides control to change aircraft attitude
Pilot steer a/c on runway during landing roll and take off
Heading select
Speed select
Vertical speed / altitude hold
VOR-LOC
GS
LNAV / VNAV
AP Disconnect
AP Engage
ATH Disconnect
ATH Engage
Pilot sensors
Automation mode annunciator
Flight controls
AFCS Control
Air data
Heading
Navigation deviation
Aircraft position
Aircraft weight
Flaps / slats
Landing gear
Brakes
Nosewheel steering
Thrust levers
Control surfaces (aileron / elevator / spoilers / rudder)
AP ATH/THR
Autoflight provides control to change aircraft attitude
Autoflight provides control to change a/c speed
Autoflight delivers go-around mode
Autoflight correct deviations
Autoland flares
Autobrake decelerate
AFCS sensors
Aircraft

Contol Flaws Identification

Pilot does not provide control to change L/V flight patch when deviation occurs between DH and flare	Btn DH and Flare	Y	UCA.101.2.1	1.Pilot Sensors	Guidance on displays/ instuments/ HUD - Not provided or incorrect.
Pilot does not provide control to change L/V flight patch when deviation occurs between DH and flare	Btn DH and Flare	Y	UCA.101.2.2	1.Pilot Sensors	Aircraft height/ altitude on displays/ instruments/ HUD - Not provided or incorrect
Pilot does not provide control to change L/V flight patch when deviation occurs between DH and flare	Btn DH and Flare	Y	UCA.101.2.3	1.Pilot Sensors	Gnd proximity warning - Not provided or incorrect
Pilot does not provide control to change L/V flight patch when deviation occurs between DH and flare	Btn DH and Flare	Y	UCA.101.2.4	1.Pilot Sensors	Real-time image of external scene topography on displays/ HUD - Misleading
Pilot does not provide control to change L/V flight patch when deviation occurs between DH and flare	Btn DH and Flare	Y	UCA.101.2.5	1.Pilot Sensors	Windshear alert - Not fitted
Pilot does not provide control to change L/V flight patch when deviation occurs between DH and flare	Btn DH and Flare	Y	UCA.101.2.6	2.Air Operator	Automation policy and training - Insufficient
Pilot does not provide control to change L/V flight patch when deviation occurs between DH and flare	Btn DH and Flare	Y	UCA.101.2.7	2.Air Operator	Cross wind limitations - Inadequate
Pilot does not provide control to change L/V flight patch when deviation occurs between DH and flare	Btn DH and Flare	Y	UCA.101.2.8	2.Air Operator	CRM - Insufficient
Pilot does not provide control to change L/V flight patch when deviation occurs between DH and flare	Btn DH and Flare	Y	UCA.101.2.9	3.ANS	RVR real-time information - Not provided
Pilot does not provide control to change L/V flight patch when deviation occurs between DH and flare	Btn DH and Flare	Y	UCA.101.2.10	3.ANS	Wind real-time information - Not provided
Pilot does not provide control to change L/V flight patch when deviation occurs between DH and flare	Btn DH and Flare	Y	UCA.101.2.11	4.Infrastructure	Visual aids - Not provided

Sensor concerned	Inadequate Control flows	Caused by	Safety Requirements / Mitigation
1.Pilot Sensors	Landing configuration warning - Not provided or incorrect.		• stall warning, maximum operation speed/maximum operating mach number, or flap limits, should be displayed to provide the flight crew a quick -glance sense of speed • Pilot flying must cross check aircraft airspeed with other instruments or have pilot not-flying to monitor the aircraft attitude information that is provided to the pilot flying for errors. • There should be a means to detect wrong configuration setting
1.Pilot Sensors	Real-time image of external scene topography on displays/ HUD - Misleading	• Sensor failure • Computation/processing error • Terrain Database Error • Navigational position error due to failure	• The flight crew must be advised of failed aircraft systems or components affecting the decision to continue to use the display/HUD. • Terrain/runway database must be uploaded correctly and integrity checked before use. • Pilot must be informed/alerted to a navigation error or inability of the system to determine position within defined limits.
1.Pilot Sensors			
1.Pilot Sensors			
1.Pilot Sensors			
1.Pilot Sensors			
1.Pilot Sensors			
1.Pilot Sensors			
1.Pilot Sensors			
1.Pilot Sensors			
1.Pilot Sensors			