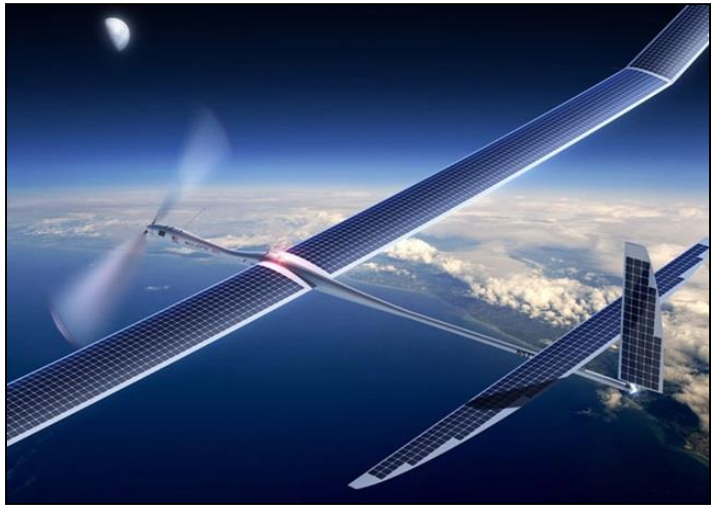
Deriving safety constraints for Unmanned Aircraft Systems (UAS)



Yusuke URANO

Candidate of Master of Science in Technology and Policy 2016, MIT

Massachusetts Institute of Technology

Overview of my research

- **Research Objective:**

  Derive safety constraints for integration of unmanned aircraft systems (UAS) into the national airspace (NAS)

- **Methodology:**

  Application of "Systems-Theoretic Early Concept Analysis (STECA)" to concept of operation (ConOps) of integration of UAS into NAS

Contents

- Integration of UAS into NAS
- Current approach
- What is STECA, Why STECA
- ConOps
- Application of STECA

Civil Unmanned Aircraft Systems

Agriculture

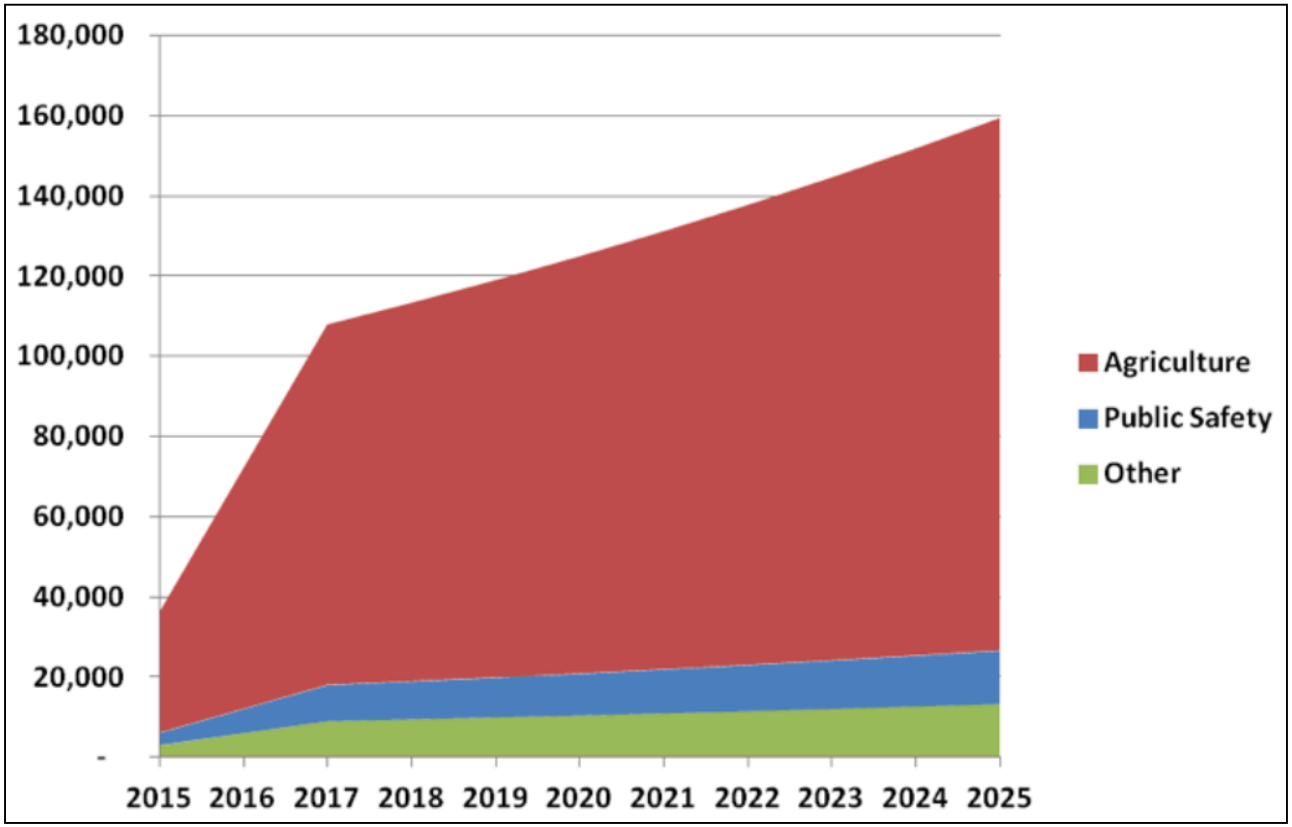
Package delivery

Surveillance, Inspection, media

Internet delivery

Freighter

Market Impact: Annual Sales forecast



Association for Unmanned Vehicle Systems International (AUVSI) estimates it will create more than 100,000 jobs and the economic impact of approximately $82 billion in the next decade

source: http://robohub.org/_uploads/AUVSI_New_Economic_Report_2013_Full.pdf

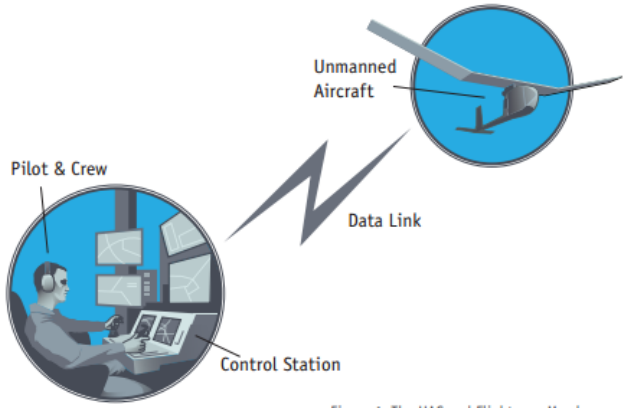
Lack of regulatory structure

- In the US: In 2012, the congress has passed the FAA Modernization and Reform Act, which encouraged FAA to accelerate the integration of UAS into the national airspace
- In the international context: In 2014, ICAO established RPASP (Remotely Piloted Aircraft Systems Panel) to develop regulatory concept and associated guidance materials to support the regulatory process

Source: http://www.wyvernltd.com/wp-content/uploads/2015/05/ICAO-10019-RPAS.pdf

Major concerns of integration of UAS into NAS

- Effect of having a ground control station instead of having a cockpit
  - **Sense and avoid / Detect and avoid**: In a manned aircraft, pilots see and avoid collision. How about unmanned aircraft?
  - **C2 (command and control) link**: In a manned aircraft, cockpit is on the airplane and it is physically connected. If the control station is on the ground, what is the effect of having a communication/control link?
  - Other concern: Interaction between air traffic control (ATC), pilot training (license?), airworthiness of the aircraft, operational consideration, etc.



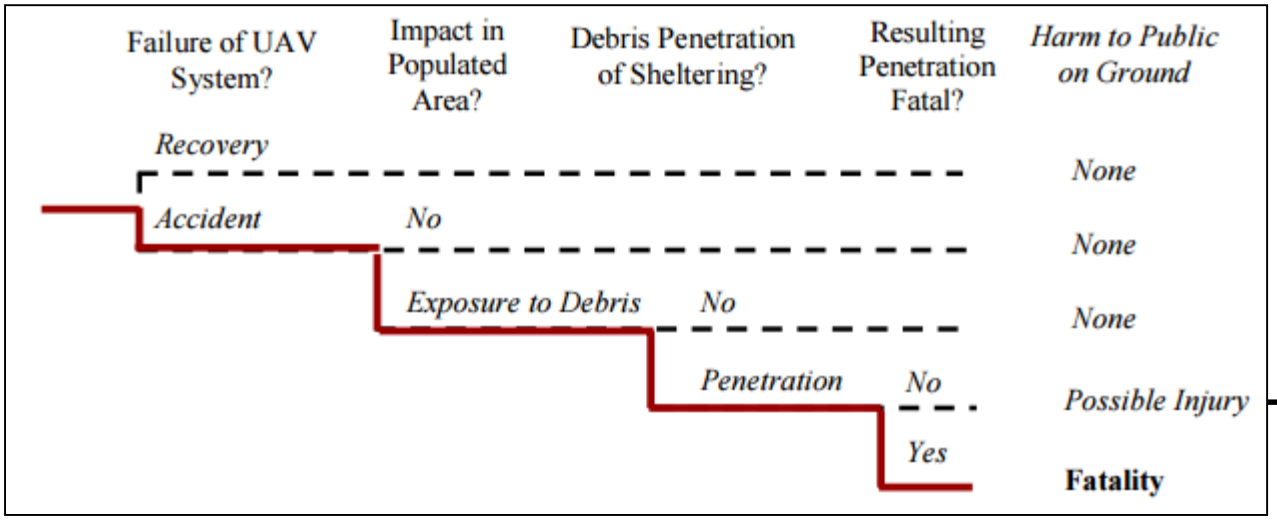
Souce: http://www.faa.gov/uas/media/uas_roadmap_2013.pdf

Contents

- ✓ Integration of UAS into NAS
- Current approach
- What is STECA, Why STECA
- ConOps
- Application of STECA

Current approach to assess risk

- Assesses risk based on probability (e.g. model is based on event tree and assess probability of each event)
- Pros: These type of research made progress on quantifying risks and helping to determine the "target level of safety."
- Cons: These type of research heavily rely on statistical assumptions, which does not take into account of additional complexity typical to UAS. In addition, quantifying numbers itself does not solve problem.

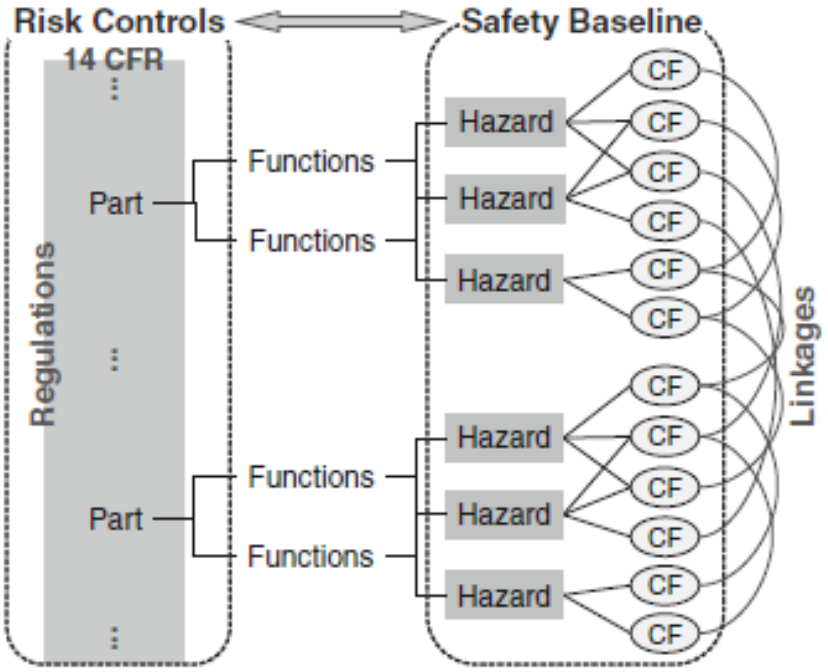


Adapted from Roland E. Weibel and R. John Hansman, Jr."Safety Considerations for Operation of Different Classes of UAVs in the NAS"

http://dspace.mit.edu/bitstream/handle/1721.1/34955/Acr2113645.pdf?seq

FAA's approach (Regulatory-based Causal Factor Framework (RCFF))

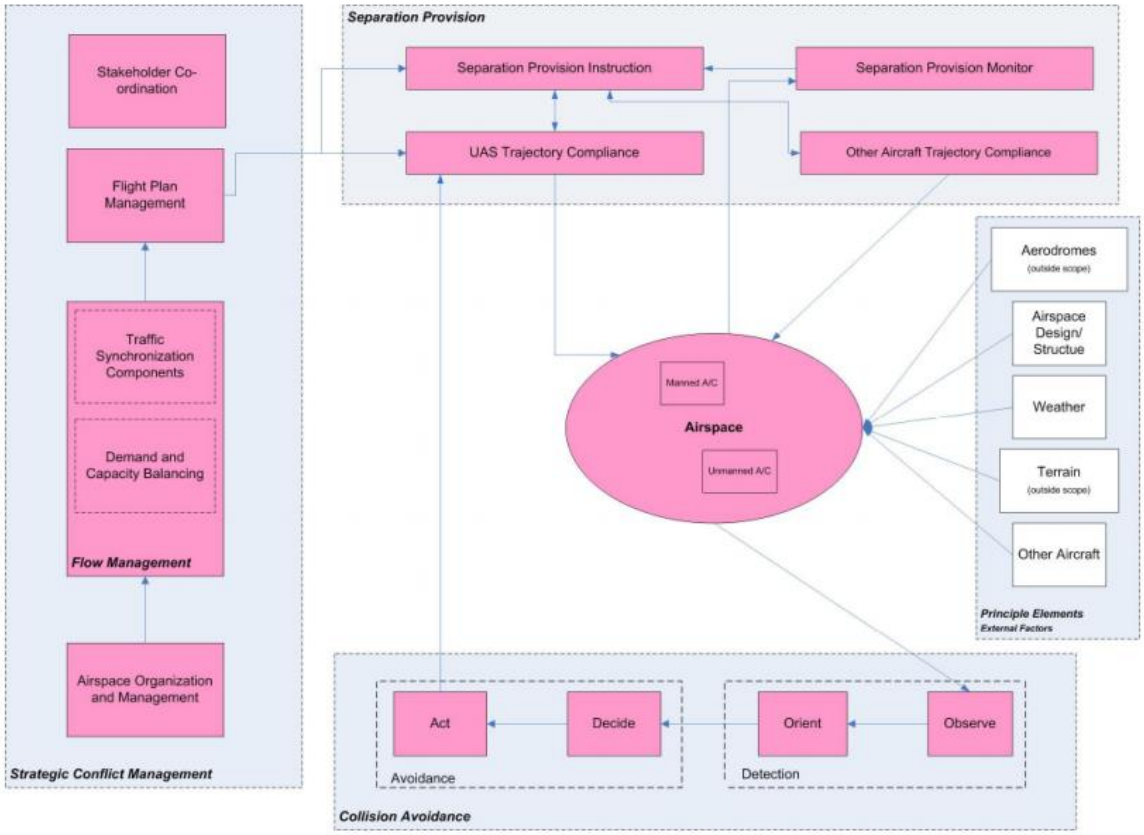
- FAA has proposed a qualitative analysis methodology that identifies hazards and associated causal factors on the basis of the established regulation.
- Pros: This approach has potential to derive comprehensive safety constraints necessary for operation in NAS.
- Cons: RCFF is not intended to create UAS specific regulation, and therefore, UAS specific concern is not treated in this framework as well.



Adapted from Ahmet Oztekin · Cynthia Flass · Xiaogong Lee "Development of a Framework to Determine a Mandatory Safety Baseline for Unmanned Aircraft Systems"
Source: http://link.springer.com/article/10.1007/s10846-011-9578-0

Functional hazard analysis

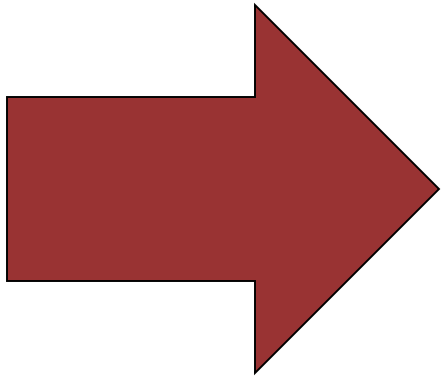
- Eurocontrol Agency has conducted functional hazard analysis for unmanned aircraft system in 2009 for establishing ATM safety requirement.
- Pros: Understand the risk by identification of hazardous scenarios from the functional model
- Cons: Did not identify UAS specific hazardous scenarios.



Adapted from EUROCONTROL "Functional Hazard Assessment (FHA) Report for Unmanned Aircraft Systems"
Source: https://www.eurocontrol.int/sites/default/files/content/documents/single-sky/uas/library/safety-uasfha-report-v2-ebeni.pdf

Summary of challenges

- Lack of understanding and enforcement of UAS specific safety constraints. UAS specific safety constraints can be derived from
  - Identification of UAS specific hazardous scenarios
  - Identification of causal factors of UAS specific hazardous scenarios



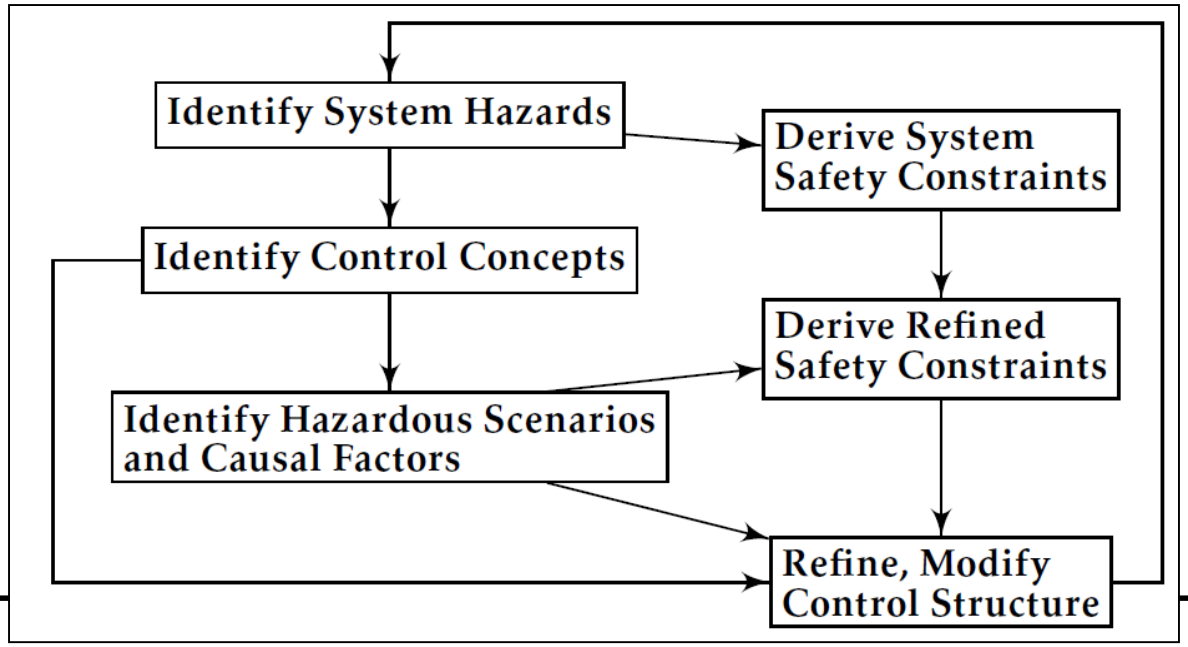
Need STAMP

Contents

- ✓ Integration of UAS into NAS
- ✓ Current approach
- What is STECA, Why STECA
- ConOps
- Application of STECA

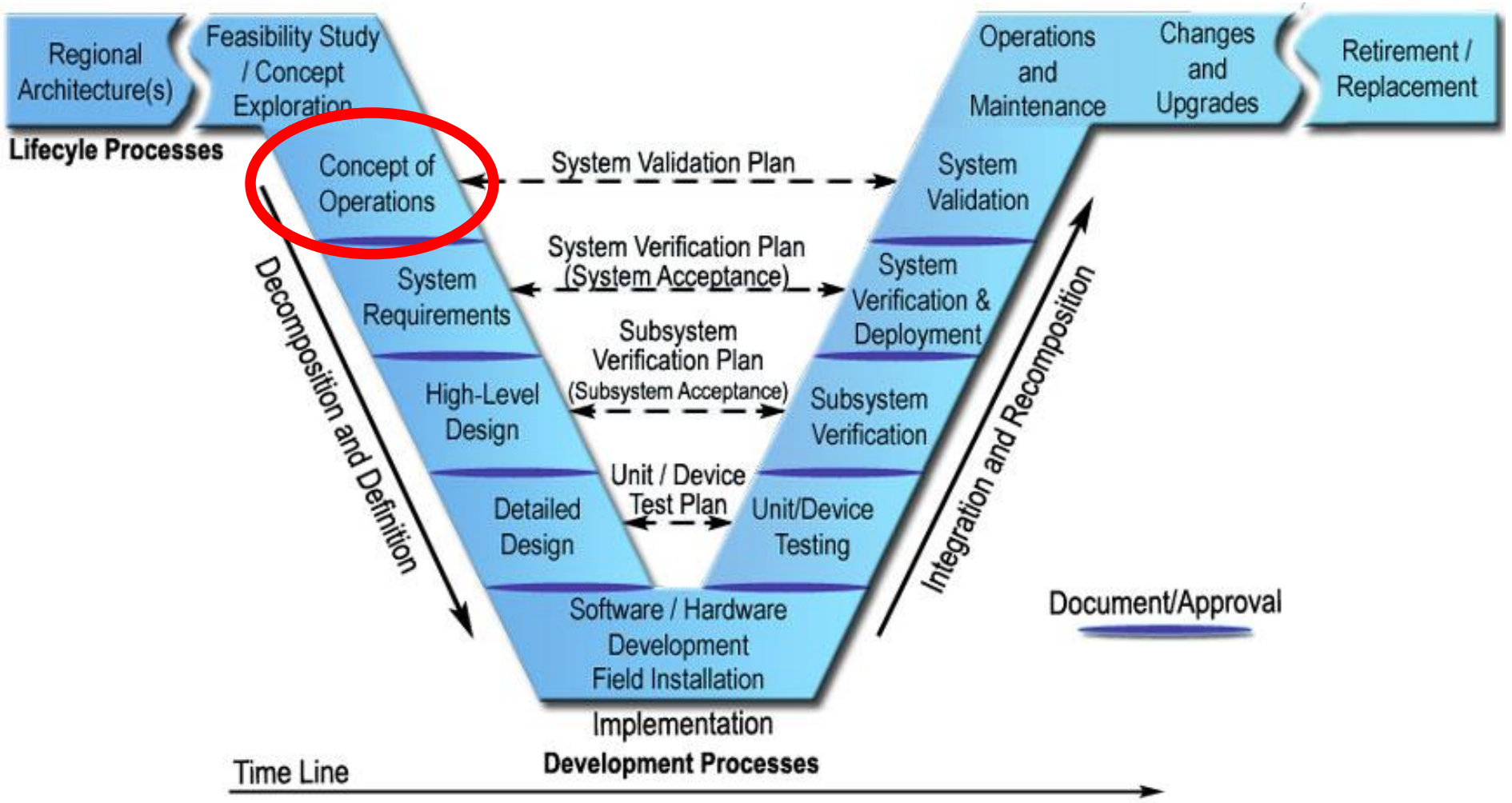
STECA

- STECA (Systems-Theoretic Early Concept Analysis): Technique to analyze concept of future system based on STAMP
- The goal of STECA: derive safety constraints by identifying potential hazardous scenarios and associated systemic factors
- The process of STECA:



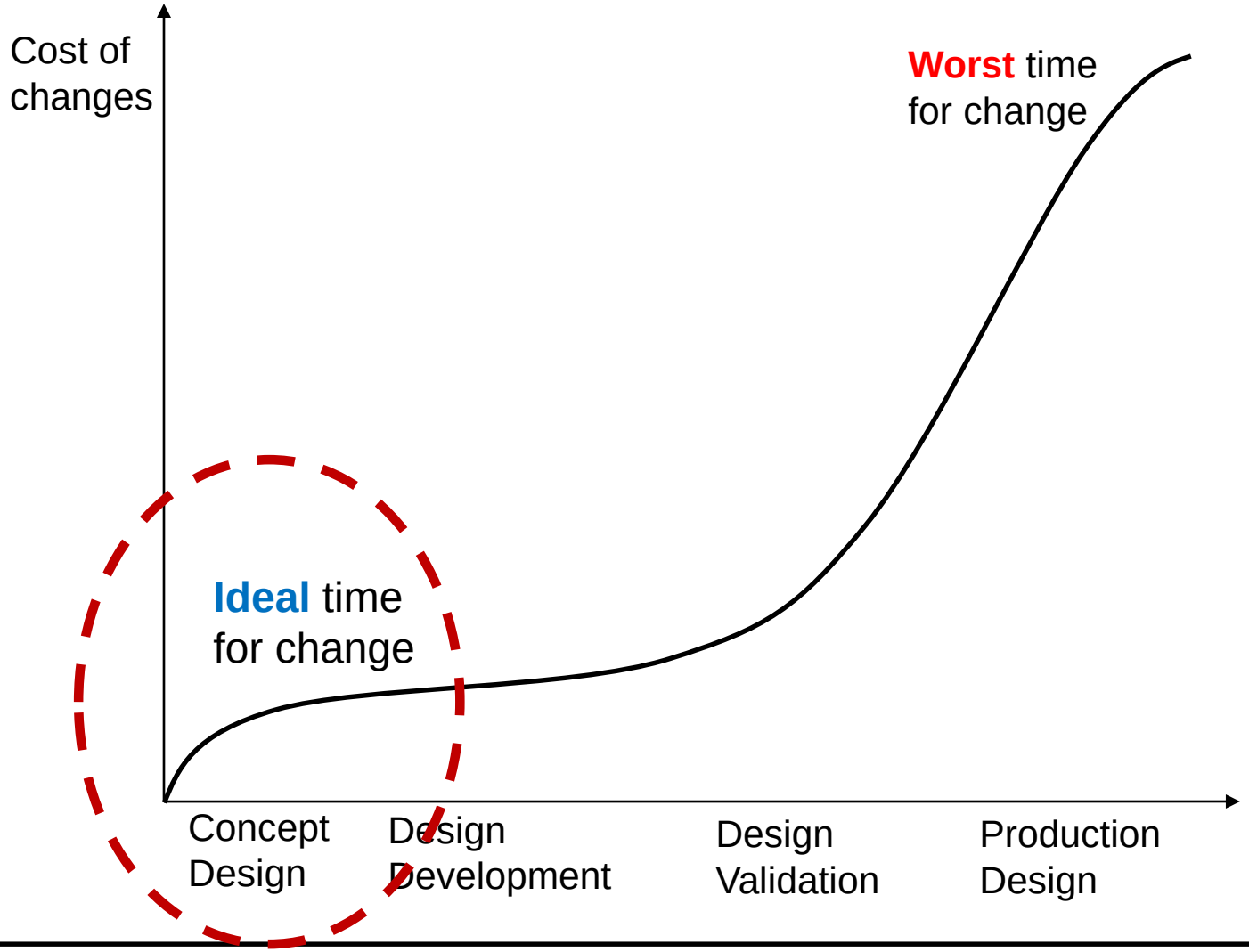
Source: "Safety-driven early concept analysis and development" Fleming

"V" model in systems engineering



source: adapted from "Systems Engineering for Intelligent Transportation Systems" US Department of Transportation
http://ops.fhwa.dot.gov/publications/seitsguide/section3.htm

Cost advantage of STECA

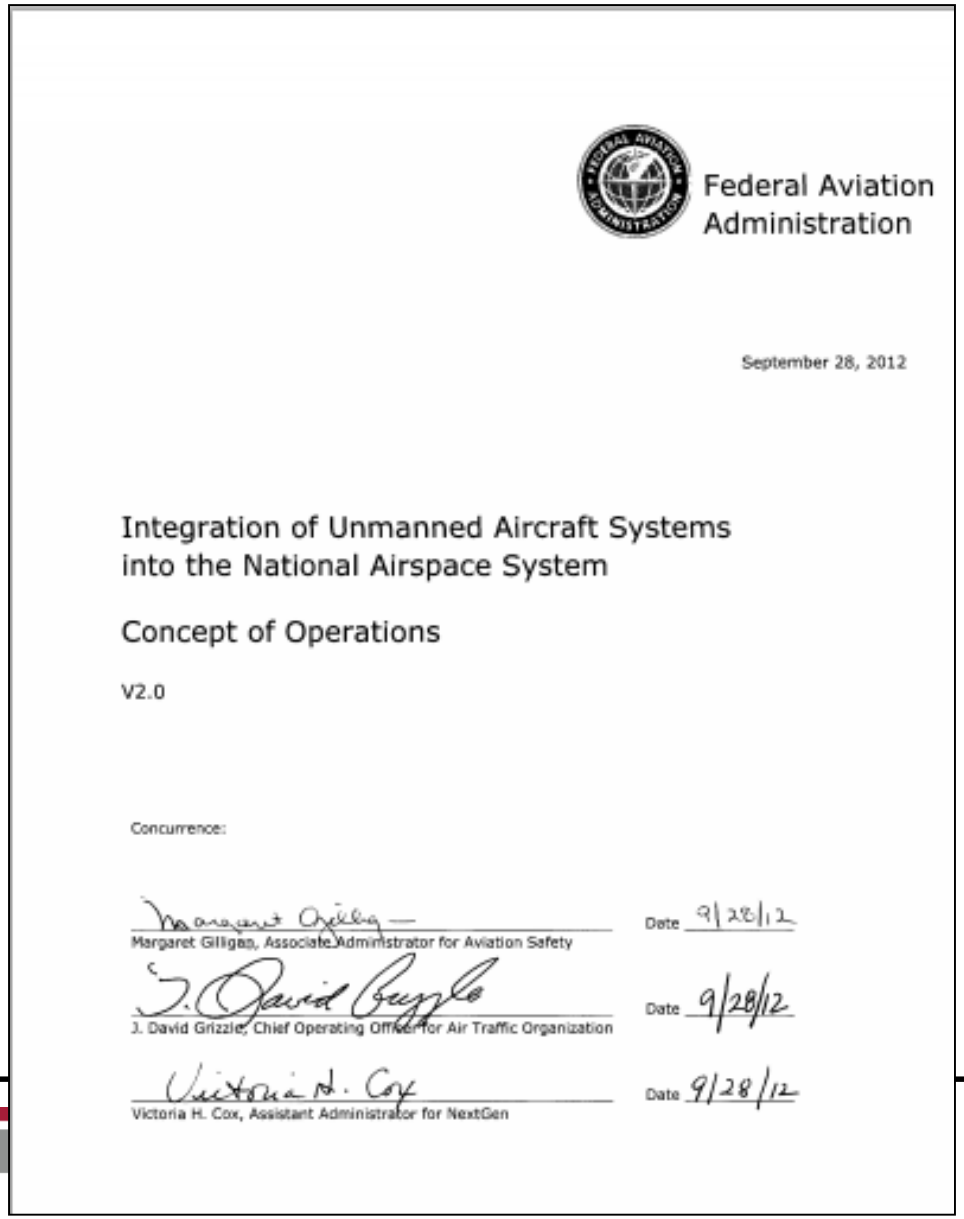


Source: Adapted from Cost of change in each phase of system development (adapted from "Concurrent Engineering" (Harley 1992))

Contents

- ✓ Integration of UAS into NAS
- ✓ Current approach
- ✓ What is STECA, Why STECA
- ConOps
- Application of STECA

FAA ConOps



Federal Aviation Administration

September 28, 2012

Integration of Unmanned Aircraft Systems into the National Airspace System

Concept of Operations

V2.0

Concurrence:

Margaret Gilligan, Associate Administrator for Aviation Safety — Date 9/28/12

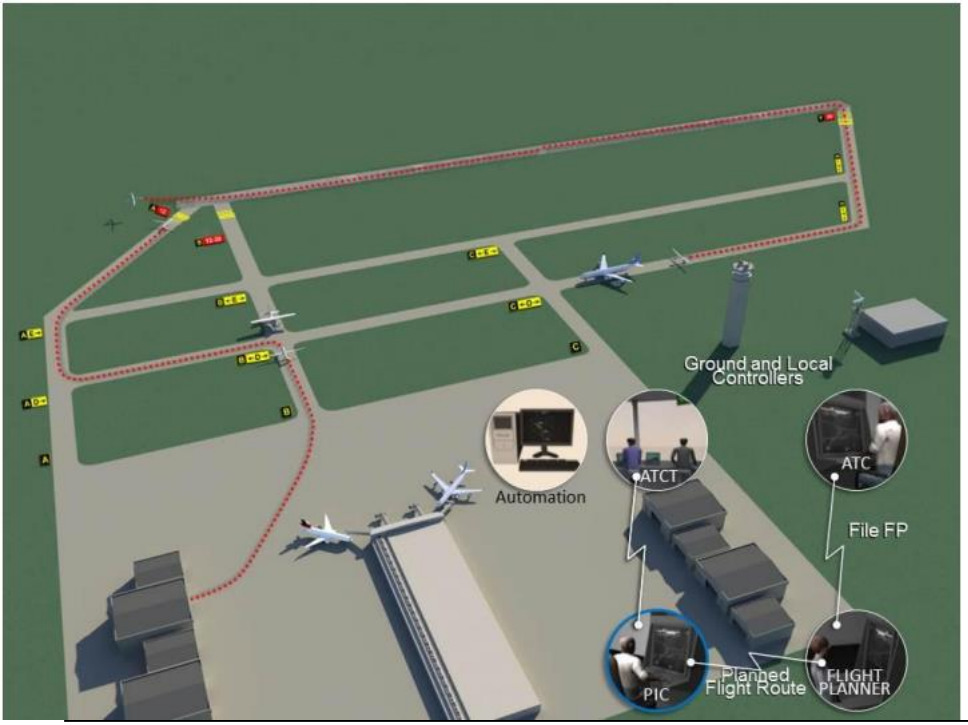
J. David Grizzle, Chief Operating Officer for Air Traffic Organization — Date 9/28/12

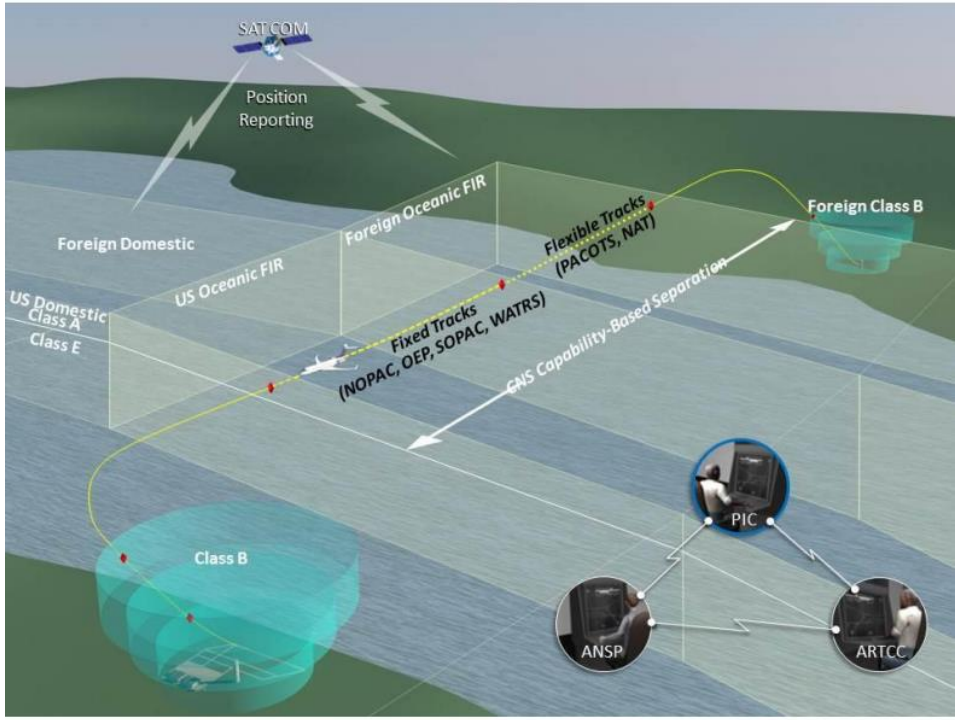
Victoria H. Cox, Assistant Administrator for NextGen — Date 9/28/12

Source: "Integration of Unmanned Aircraft Systems into the National Airspace System " FAA http://www.suasnews.com/wp-content/uploads/2012/10/FAA-UAS-Conops-Version-2-0-1.pdf

Scope of analysis

- Analysis are conducted for “Surface Operations” and “Oceanic point-to-point” scenario within ConOps
- Aircraft used are unmanned Boeing 747 (cargo)



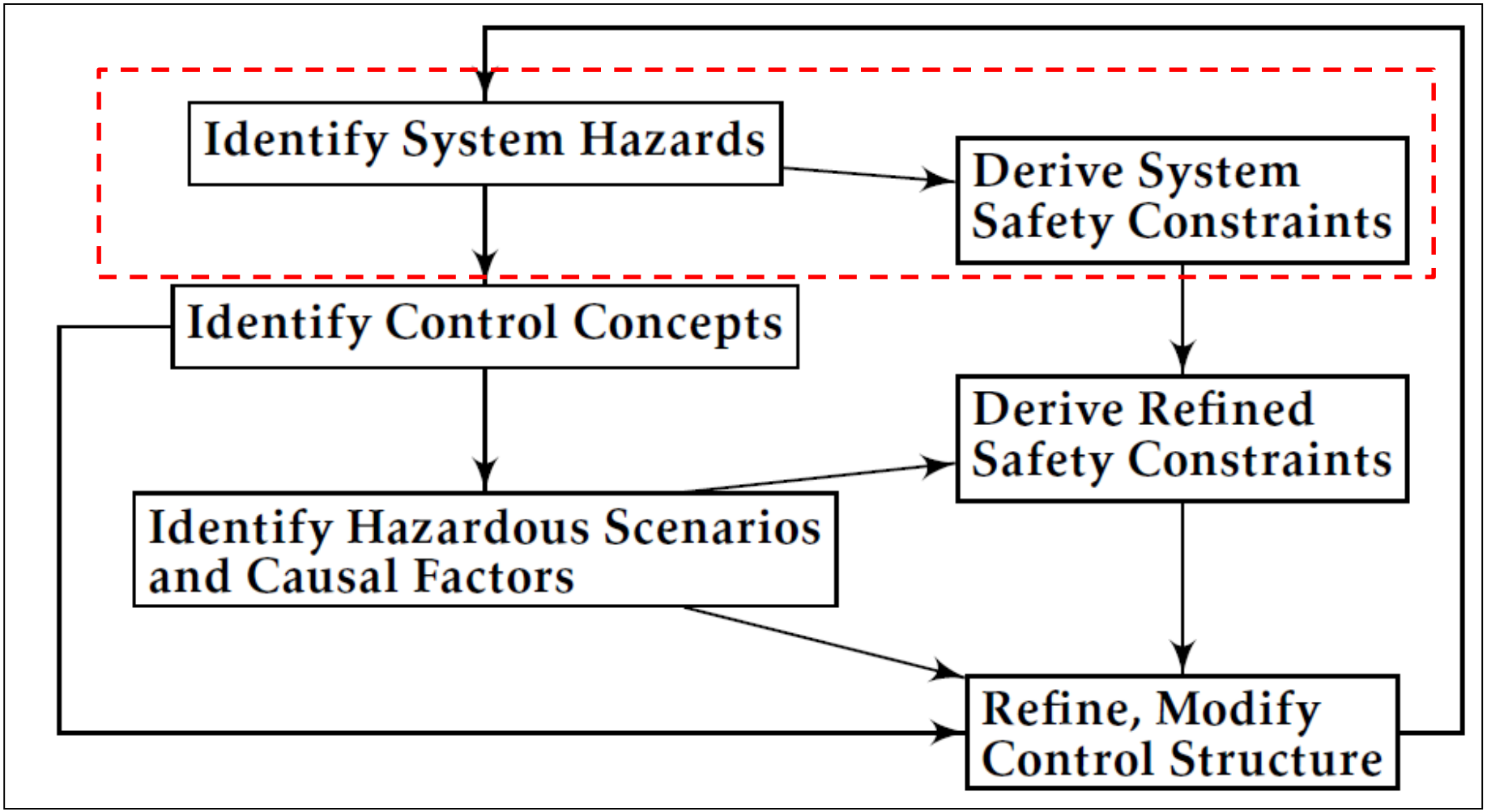


Source: “Integration of Unmanned Aircraft Systems into the National Airspace System ” FAA http://www.suasnews.com/wp-content/uploads/2012/10/FAA-UAS-Conops-Version-2-0-1.pdf

Contents

- ✓ Integration of UAS into NAS
- ✓ Current approach
- ✓ What is STECA, Why STECA
- ✓ ConOps
- Application of STECA

Process of STECA



Source: "Safety-Driven Early Concept Analysis and Development" Cody Fleming

High level system hazards and safety constraints

Hazards

[H-1] Aircraft violate minimum separation with other aircraft

[H-2] Aircraft loses its control or loses airframe integrity

[H-3] Aircraft performs controlled maneuver into ground or into obstacles on ground

[H-4] Aircraft on the ground comes too close to other objects or leaves the paved area

[H-5] Aircraft enters a runway with no clearance

Safety Constraints

[SC-1] Aircraft must maintain separation with other aircraft

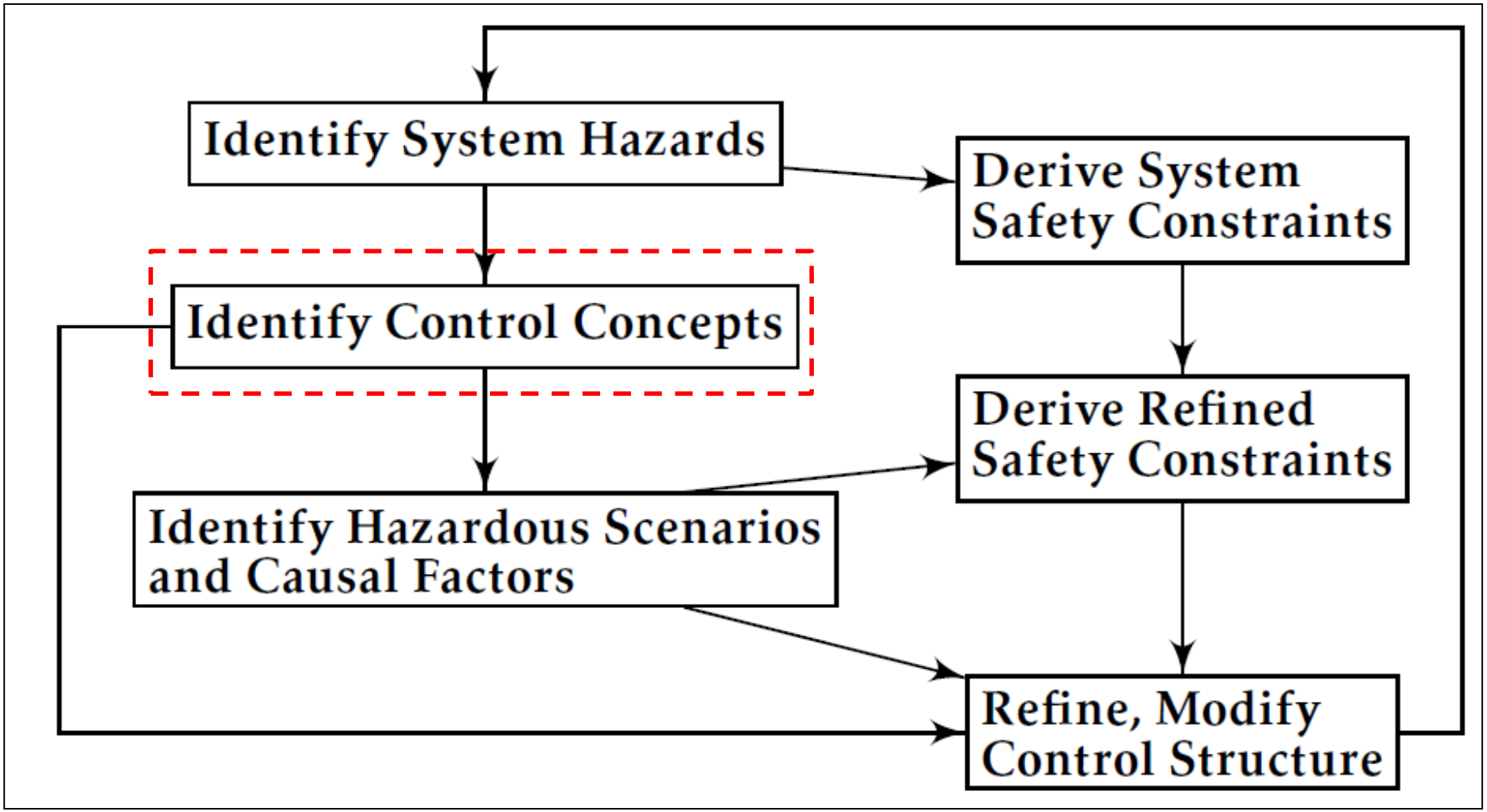
[SC-2] Aircraft must maintain its control and maintain airframe integrity

[SC-3] Aircraft must maintain separation with ground or obstacles on ground

[SC-4] Aircraft on ground must maintain separation with other objects and must not leave the paved area

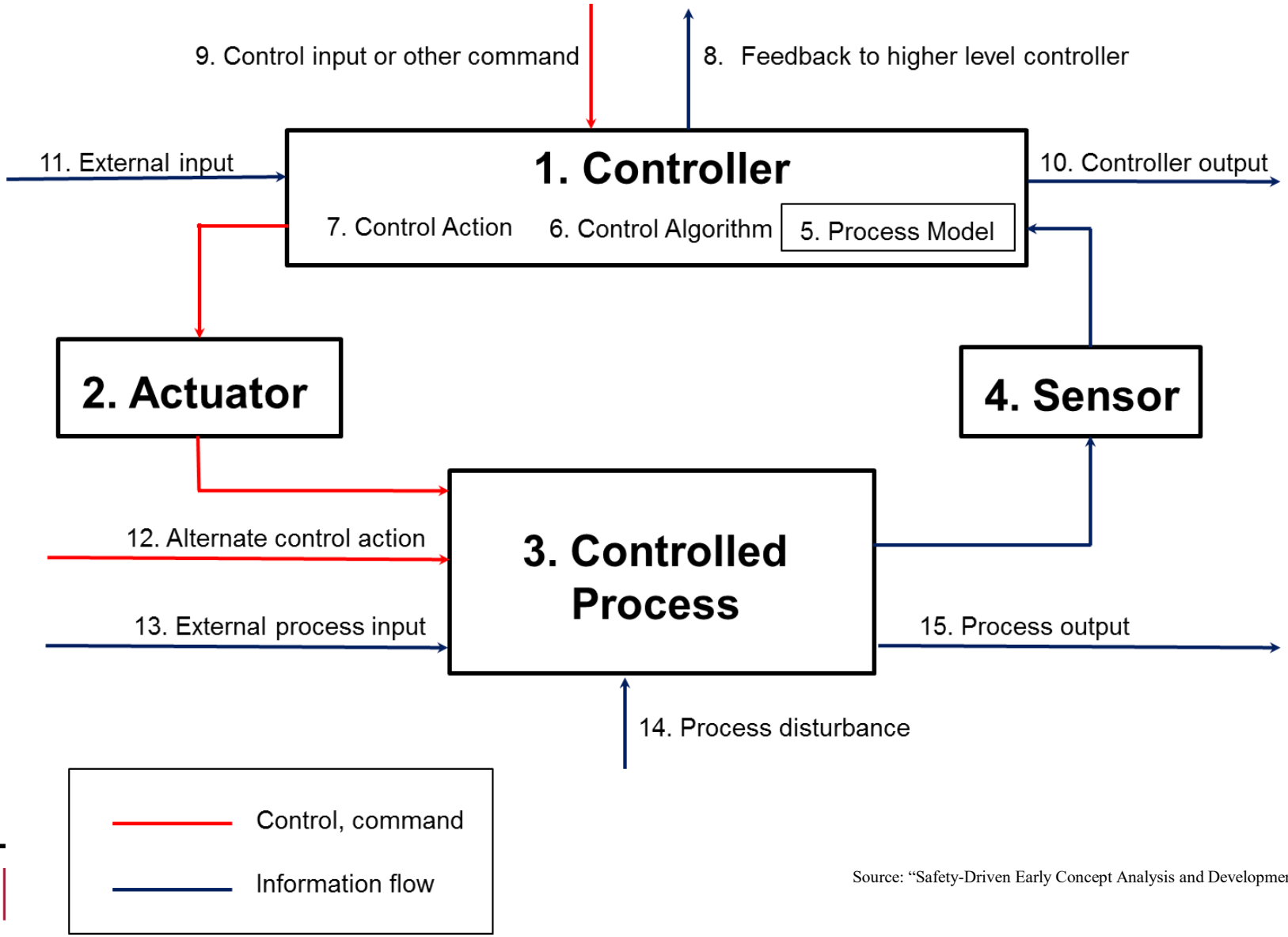
[SC-5] Aircraft must not enter a runway without clearance

Process of STECA



Source: "Safety-Driven Early Concept Analysis and Development" Cody Fleming

Generic role in the control loop



Source: "Safety-Driven Early Concept Analysis and Development" Cody Fleming

Example of allocation of role

- “To initiate taxi, the PIC contacts ATC ground to request taxi to the active runway via two-way communications. ATC ground identifies the aircraft standing-by on the non-movement area, visually inspects the desired taxi route for any potential conflicts, and approves the UAS to taxi to the active runway as filed.”

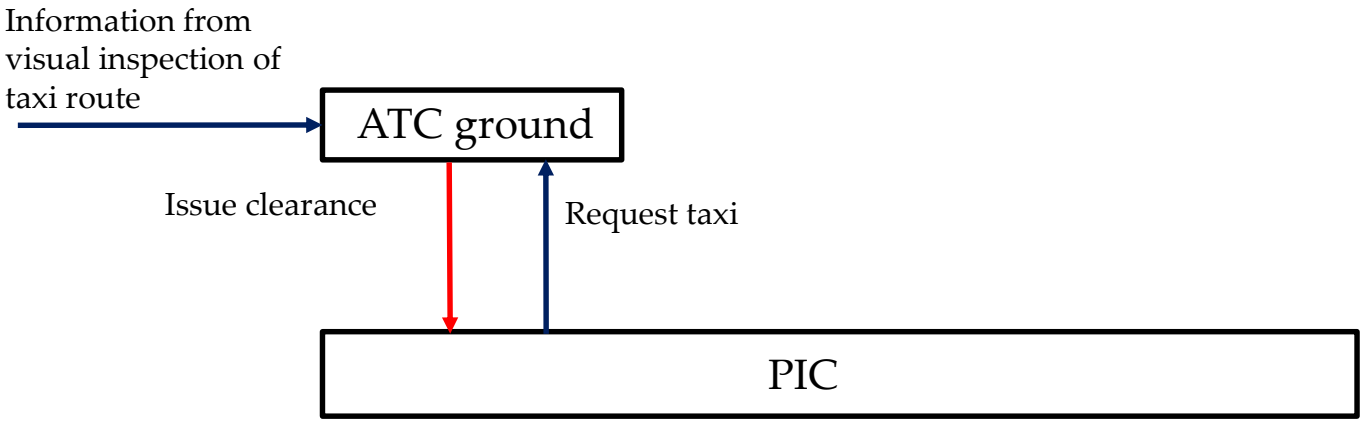
1. Controller	
2. Actuator	
3. Controlled Process	
4. Sensor	
5. Process Model	
6. Control Algorithm	
7. Control Action	

Example of allocation of role

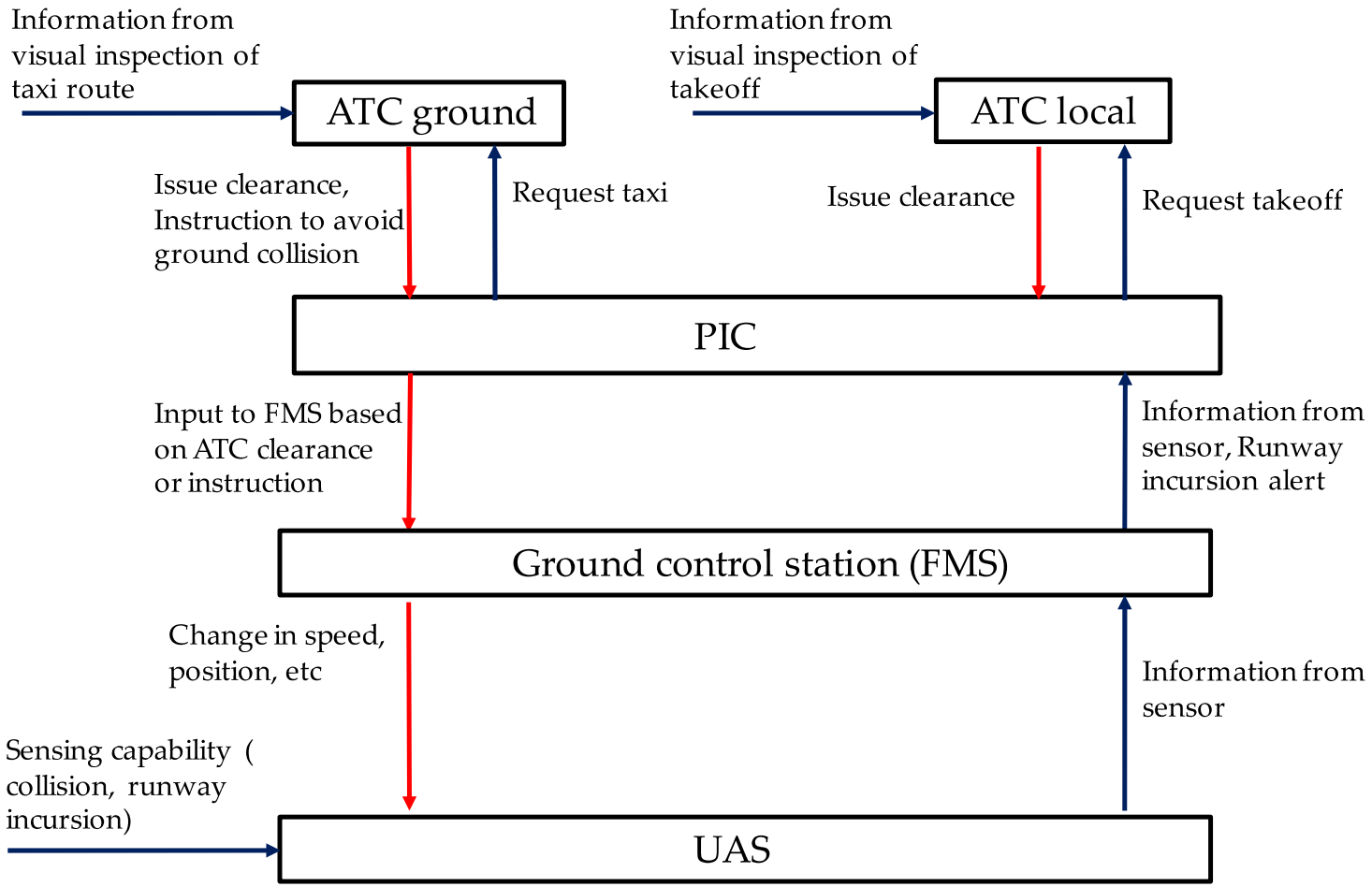
- “To initiate taxi, the PIC contacts ATC ground to request taxi to the active runway via two-way communications. ATC ground identifies the aircraft standing-by on the non-movement area, visually inspects the desired taxi route for any potential conflicts, and approves the UAS to taxi to the active runway as filed.”

1. Controller	ATC ground
2. Actuator	Instrument for two-way communications
3. Controlled Process	PIC initiating taxi
4. Sensor	Instrument for two-way communications, visual inspection
5. Process Model	Information from visual inspection or two-way communicaiton
6. Control Algorithm	If there is no potential conflicts, ATC issues clearance for UAS to taxi to the active runway.
7. Control Action	Issues clearance

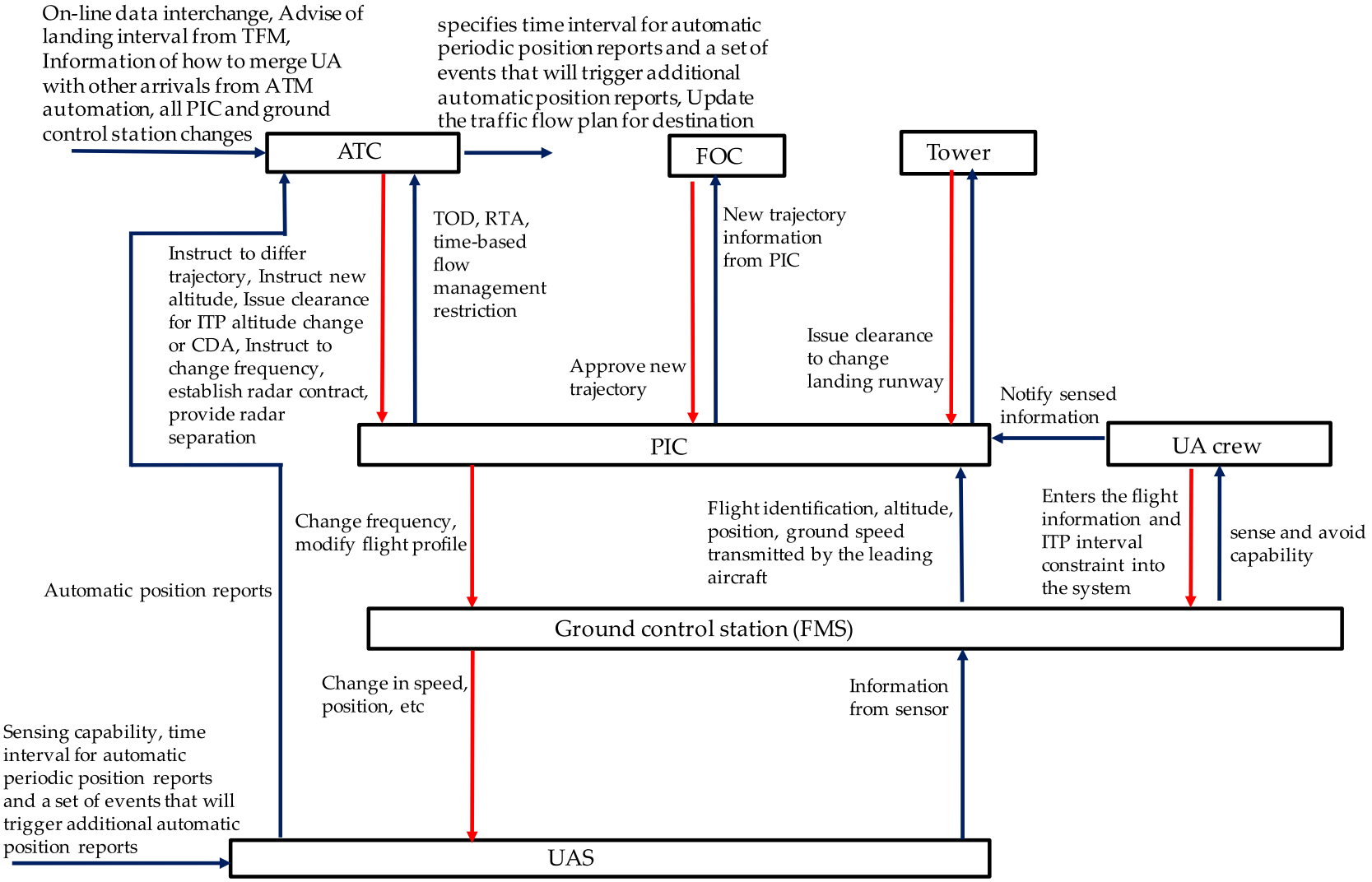
PIC initiating taxi



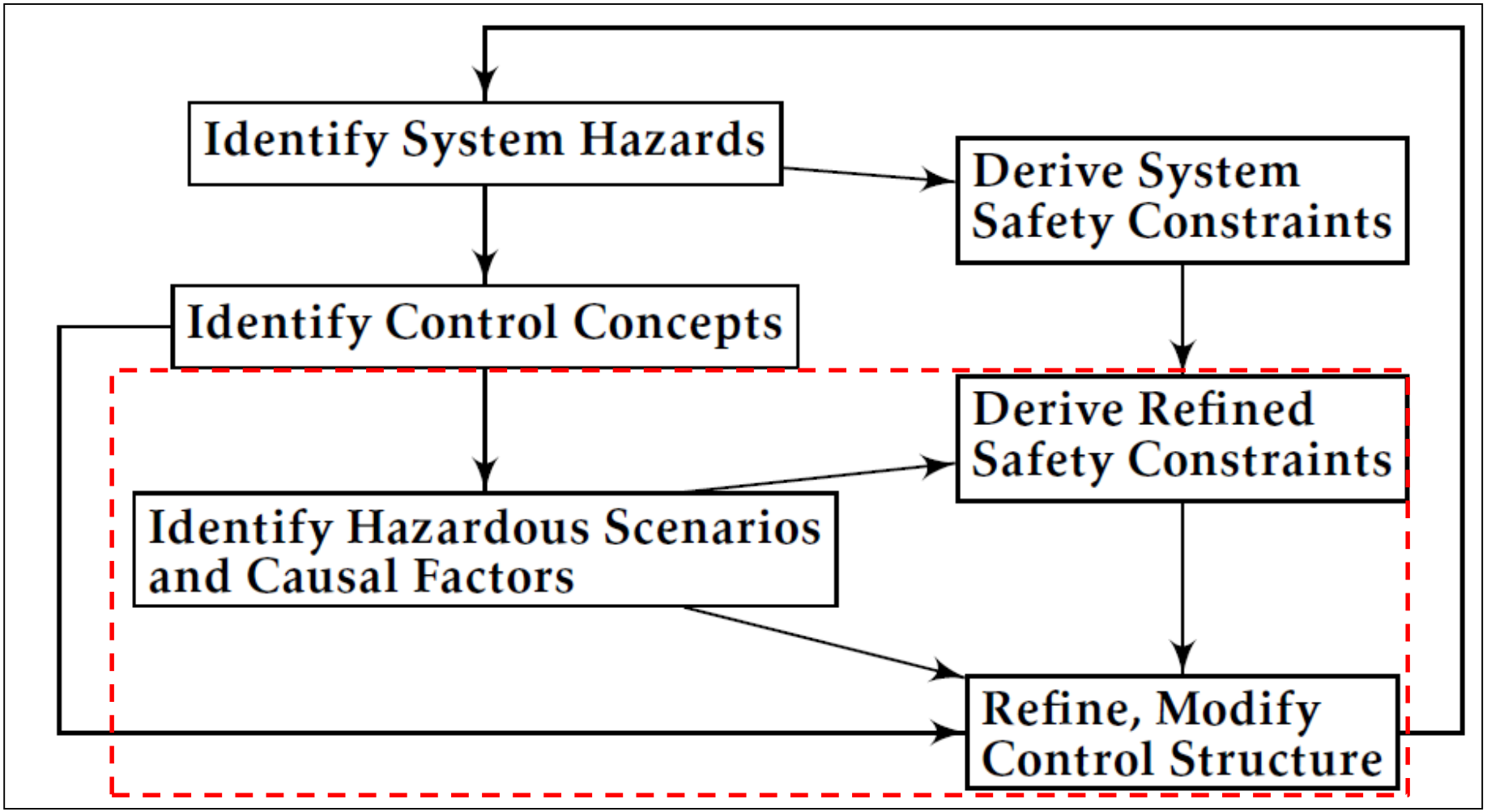
Control concept of “Surface Operations” scenario



Control concept of “Oceanic Point-to-Point” scenario

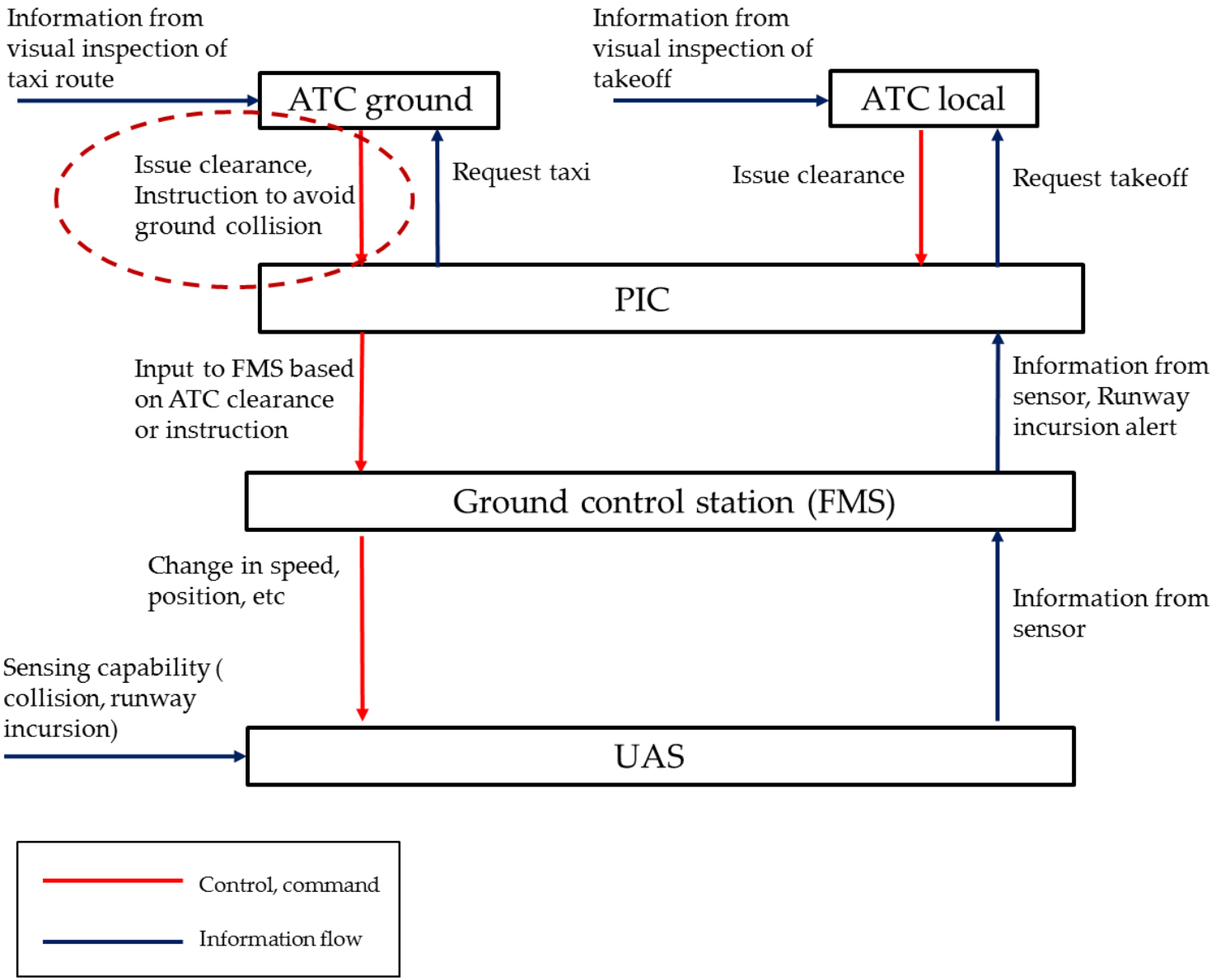


Process of STECA



Source: "Safety-Driven Early Concept Analysis and Development" Cody Fleming

Example of identified hazardous scenario



Framework proposed for the analysis

"Completeness"

"1. Are the control loops complete? That is, does each control loop satisfy a Goal Condition, Action Condition, Model Condition, and Observability Condition?

- (a) Goal Condition – what are the goal conditions? How can the goals violate safety constraints and safety responsibilities?
- (b) Action Condition – how does the controller affect the state of the system? Are the actuators adequate or appropriate given the process dynamics?
- (c) Model Condition – what states of the process must the controller ascertain? How are those states related or coupled dynamically? How does the process evolve?
- (d) Observability Condition – how does the controller ascertain the state of the system? Are the sensors adequate or appropriate given the process dynamics?

"Safety Related Responsibilities"

2. Are the system-level safety responsibilities accounted for?

3. Do control agent responsibilities conflict with safety responsibilities?

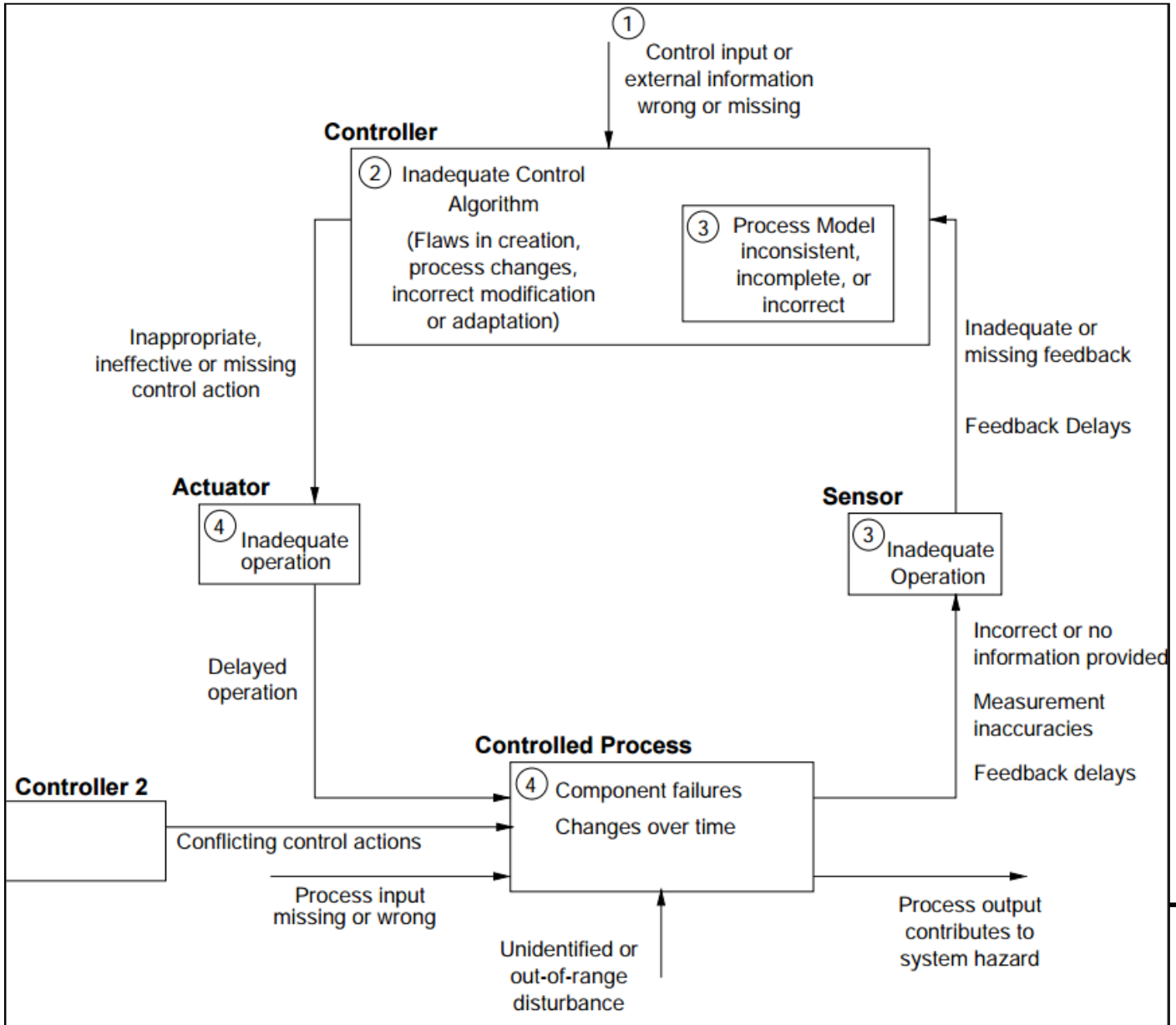
"Coordination and Consistency"

4. Do multiple control agents have the same safety responsibility(ies)?

5. Do multiple control agents have or require process model(s) of the same process(es)?

6. Is a control agent responsible for multiple processes? If so, how are the process dynamics (de)coupled?"

Identification of causal factors

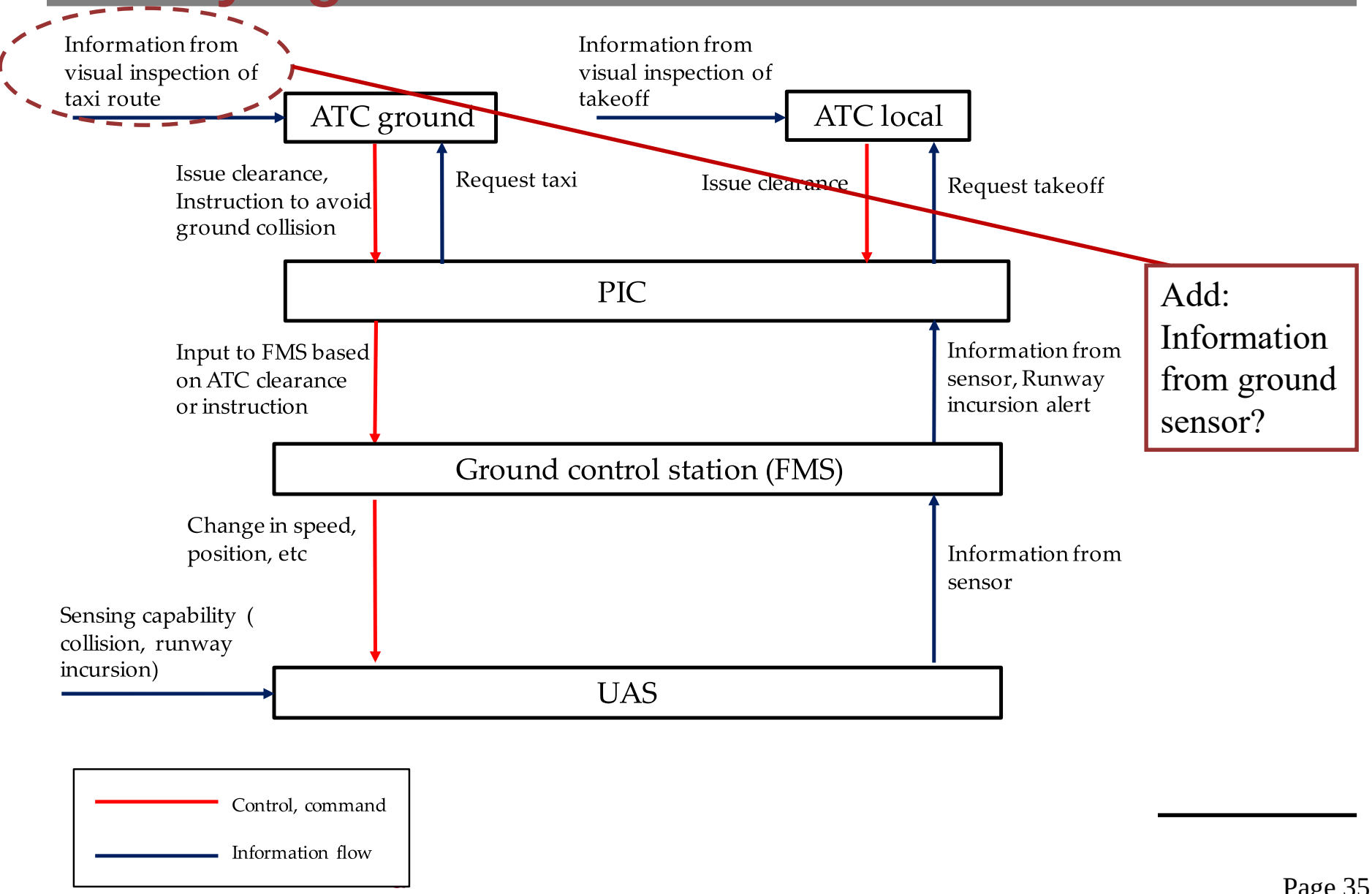


Source: "Engineering a Safer World" Nancy Leveson

Example of identified hazardous scenario

- Scenario a.1: ATC ground does not instruct to avoid ground collision.
  - Scenario a.1.1: ATC ground believes that there is no risk of ground collision.
  - Associated causal factors include:
    - ATC ground is incapable of acquiring sufficient information from visual inspection (in bad weather or in night)
    - (continue)
- Refined safety constraints:
  - SC.a.1.1.1: ATC ground must acquire sufficient information from visual inspection in any weather or in night so that ATC ground can instruct PIC to avoid ground collision. If ATC ground cannot acquire sufficient information from visual inspection, ATC ground must use other sensors to gather information to avoid ground collision.
  - SC.a.1.1.2: (continue)

Modifying control structure



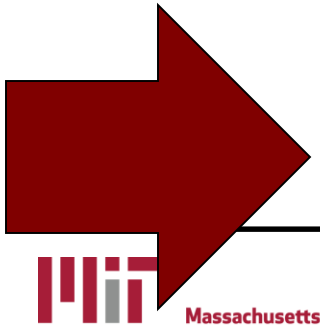
Implication for technology and policy

- From the following safety constraint,

"SC.a.1.1.1: ATC ground must acquire sufficient information from visual inspection in any weather or in night so that ATC ground can instruct PIC to avoid ground collision. If ATC ground cannot acquire sufficient information from visual inspection, ATC ground must use other sensors to gather information to avoid ground collision."

implication would be…

- Engineer: developing sensor to assist ATC ground in any weather or in night
- Regulator: consider sensing requirement for UAS ground operation



Safety constraints should be reviewed by the stakeholders. This can be achieved by incorporating them in the revision of ConOps or as system requirements

Conclusion

- STECA is a powerful tool that can identify a number of UAS specific hazardous scenarios and associated causal factors.
- STECA rectifies the system in the early stage. This is safer and cheaper.
- Recommendation of STECA can be incorporated in the revision of ConOps or system requirements so that stakeholders can further analyze them.

Future research

- Application of STECA to other scenarios in FAA ConOps or other ConOps:
  - My research focuses on B747 (cargo) ConOps, but UAS have other applications as well, and other scenarios may derive different safety constraints
- Refinement of STECA applied to UAS by experts:
  - STECA may derive more safety constraints if analyzed by experts in related field
- Extension of STECA into emerging areas such as security and/or privacy
- Help managing ConOps and system requirements
  - E.g. Incorporate control structure created in STECA into ConOps

Questions?

Source: http://si.wsj.net/public/resources/images/BN-BV717_0310dr_P_20140310122144.jpg