Unmanned Aircraft Integration into the National Airspace: A Cognitive Systems Engineering Framework for Safety Model Development.

Kip Johnson, Maj, USAF
Prof Nancy Leveson, Research Advisor

Presentation approved for public release. Case 88ABW-2015-1073

March 24, 2015
Massachusetts Institute of Technology
Cambridge, MA 02139

Disclaimer

- This material is based upon work supported by the United States Air Force under Contract No. FA8721-05-C-0002.
- Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Air Force.
- Presentation approved for public release.
  - Case 88ABW-2015-1073

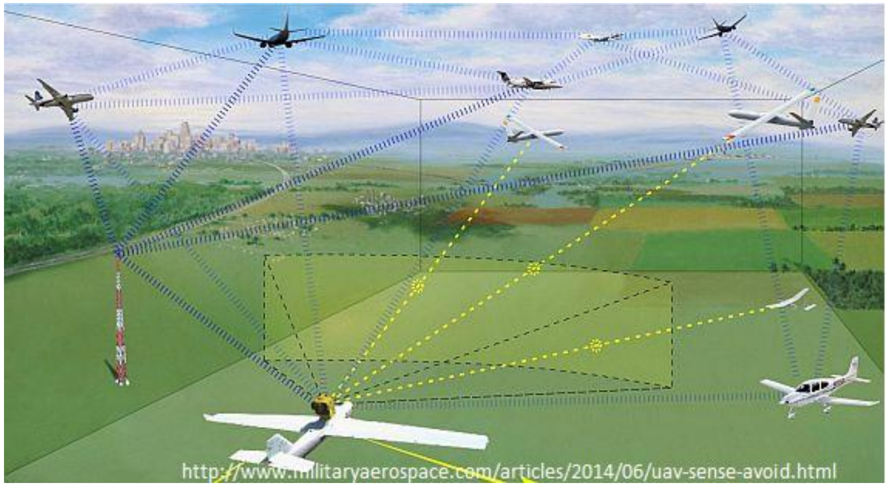
Overview

- **Introduction**
  - **Unmanned Aircraft Systems Integration**
  - **The problems**
  - **The research questions**
- Background
  - What is Cognitive Systems Engineering (CSE)
  - What is the Abstraction Hierarchy
- Results and Discussion
  - Abstraction Hierarchy applied to STAMP-STPA
  - Safety Control Structure development
  - Toward safety model validation
- Conclusions
  - Use of CSE for Complex Sociotechnical System safety design
  - Future research

Introduction

Problem description

- **UAS integration into the Nat'l airspace.**
  - Prevent mid-air and ground collisions.
  - Design the detect-and-avoid technology.
  - Lack a framework for designing safe UAS integration into the NAS.*
- **Challenges.**
  - Early lifecycle phase.
    - Ambiguous architecture.
    - Lack of useful data.
    - Sweeping change for air transportation system.
  - Complex sociotechnical system.
    - Traditional reliability safety methods inadequate.
    - Modeling and simulation limited use for safety design.
  - Human-designed system. Coping with complexity.



*U.S. H.R. 113th Congress, "Report 113-464. Departments of Transportation, and Housing and Urban Development, and Related Agencies Appropriations Bill, 2015," 2014.
*U.S. Department of Transportation, "FAA Faces Significant Barriers to Safely Integrate Unmanned Aircraft Systems into the National Airspace System," Washington, DC, 2014.

Introduction

The question

- How to develop an *adequate* qualitative model, the safety control structure?
  - Propose. Use of Cognitive Systems Engineering, specifically the Abstraction Hierarchy (Rasmussen, 1986) can augment the development of safety models and improve model validation.*

*Rasmussen, J., 1986. *Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering*, New York, NY: North-Holland; Elsevier Science Inc.

Overview

- Introduction
- **Background**
  - **What is Cognitive Systems Engineering**
  - **What is the Abstraction Hierarchy**
- Results and Discussion
- Conclusions

Background

Cognitive Systems Engineering (CSE)

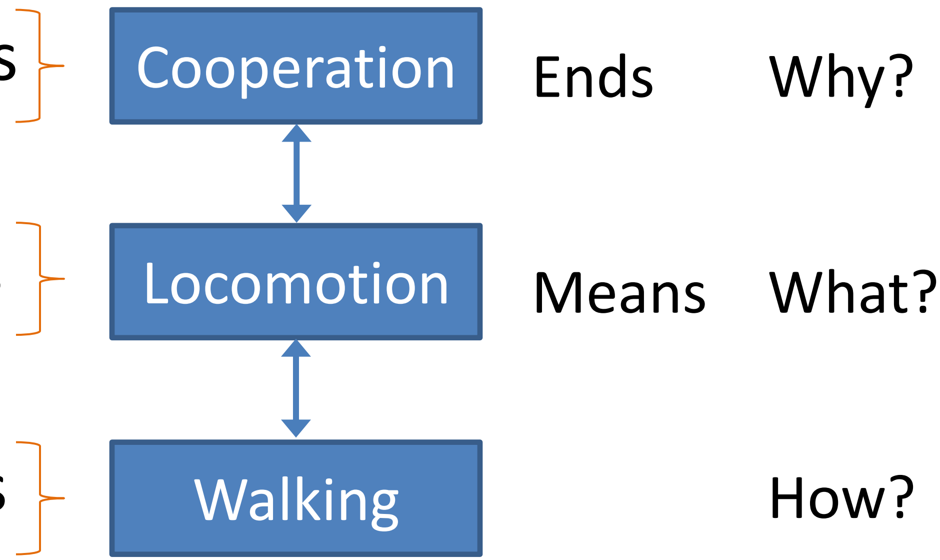
- "The central tenet of CSE is that an MMS [man-machine system] needs to be conceived, designed, analyzed and evaluated in terms of a cognitive system." p. 585*
- Abstraction Hierarchy. Abstraction-decomposition system characterization.**
  - A *framework* to organize information, to cope with complexity in system design.
  - Abstraction levels.
    - Varying hierarchical levels, from system purpose to physical realization.
    - Abstractions related by a means-ends relationship.
  - Decomposition.
    - From whole system to components.

*Hollnagel, E. & Woods, D., 1983. Cognitive Systems Engineering: New Wine in New Bottles. *International Journal of Man-machine Studies*, 18, pp.583–600.
**Rasmussen, J., 1985. The Role of Hierarchical Knowledge Representation in Decisionmaking and System Management. *IEEE Transactions on Systems, Man, and Cybernetics*, SMC-15(2), pp.234–243.

Background

System abstraction hierarchy example*

- Domain purpose
- Abstract Functions
- General Functions
- Physical Processes
- Physical Form



Hierarchy explicit, control implicit

*Rasmussen, J., Pejtersen, A.M. & Goodstein, L.P., 1994. *Cognitive Systems Engineering* M. Helander, ed., New York, NY: John Wiley & Sons, Inc.

Overview

- Introduction
- Background
- **Results and Discussion**
  - **Abstraction Hierarchy applied to STAMP-STPA**
  - **Safety Control Structure development**
  - **Toward safety model validation**
- Conclusions

Results & Discussion

Abstraction Hierarchy applied to Safety Driven Design of complex sociotechnical systems (CSS)

Influences on safety design: Competing priorities (e.g. efficiency), budget, automation trust, etc.

* Ends-Means / Whole-Part	Total System	Subsystem 1	Subsystem 2	Subsystem 3	Component
Functional Purpose -Production flow models, system objectives, constraints, etc.	Safe System				
Abstract function -Causal structure: mass, energy and information flow topology, etc.					
Generalized functions -Standard functions and processes: feedback loops, heat transfer, etc.					
Physical functions -Electrical, mechanical, chemical processes of components and equipment					
Physical form -Physical appearance and anatomy; material and form; locations, etc.					No Accidents

????????????????

*Table adapted from: Rasmussen, J., 1985. The Role of Hierarchical Knowledge Representation in Decisionmaking and System Management. *IEEE Transactions on Systems, Man, and Cybernetics*, SMC-15(2), pp.234–243.

Results & Discussion

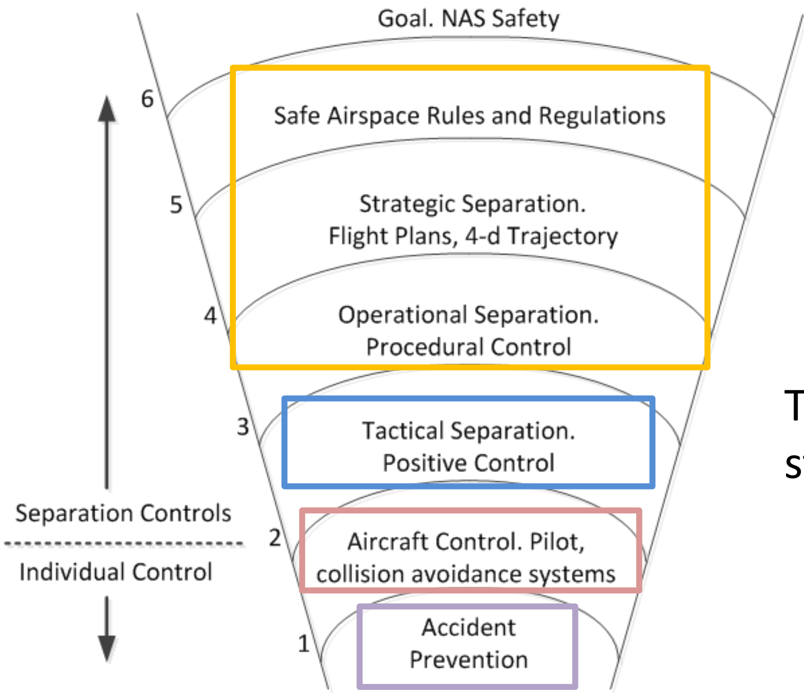
Abstraction Hierarchy applied to Safety Driven Design of the Air Transportation System

Ends-Means / Whole-Part	Total System Nat'l Airspace	Airspace Management	Local airspace control	Individual aircraft control	Component Aircraft
Functional purpose	**System goal.** Safe integrated flight operations; accident free	Safe NAS flight operations	Safe NAS flight operations	Safe aircraft control	Safe encounter
Abstract function	Rules & Regs. NAS req'ts, architecture, operations	Aggregate mass flow	Local mass flow	Aircraft energy control	Mass separation
Generalized functions		4-d flight planning (strategic control)	Communications	Lift, drag, power control	Collision free flight
Physical functions		Procedural control	Air Traffic Control, decision support, communications functions	Pilot/operator, decision support, communications (C2 Link)	Safe aircraft trajectory
Physical form					**No mid-air or ground collisions**

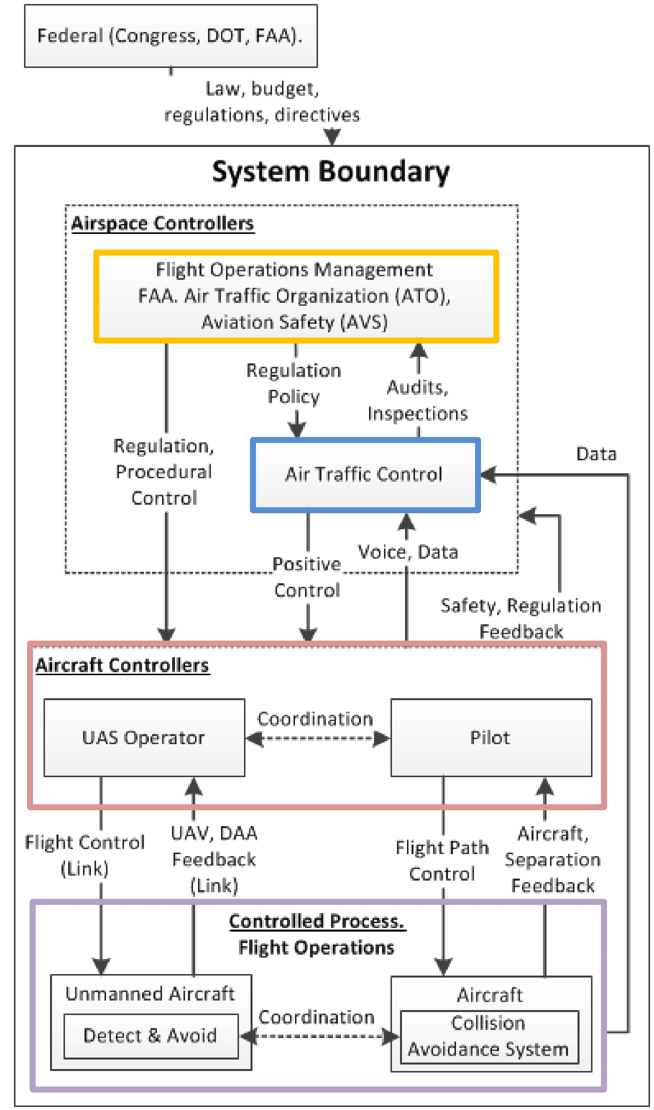
Results & Discussion

Developing the *Safety Control Structure*

- From abstraction hierarchy.



To safety control structure.

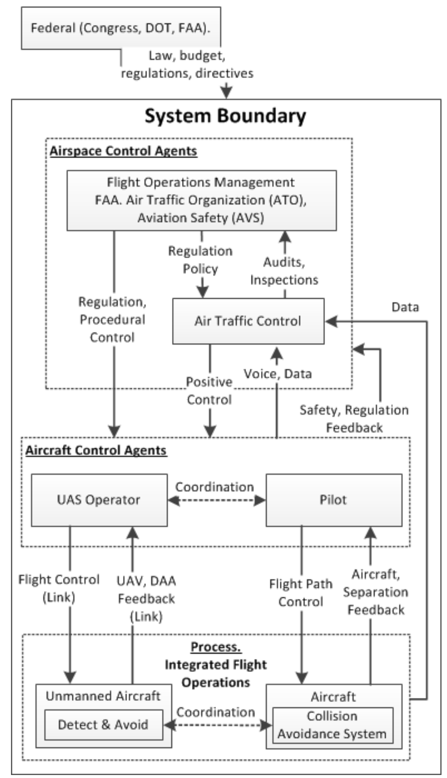


Abstraction Hierarchy maps to Safety Control Structure

Results & Discussion

- Validation. Model is adequate for safety analysis.
  - Does the model represent the intended system?
  - In STAMP. The intended functional control, the controlled process, and interactions represented?

Ends-Means / Whole-Part	Total System Nat'l Airspace	Airspace Management	Local airspace control	Individual aircraft control	Component
Functional purpose	**System goal.** Safe integrated flight operations; accident free	Safe NAS flight operations	Safe NAS flight operations	Safe aircraft control	Safe encounter
Abstract function	Rules & Regs. NAS req'ts, architecture, operations	Aggregate mass flow	Local mass flow	Aircraft energy control	Mass separation
Generalized functions		4-d flight planning (strategic control)	Communications	Lift, drag, power control	Collision free flight
Physical functions		Procedural control	Air Traffic Control, decision support, communications functions	Pilot/operator, decision support, communications (C2 Link)	Safe aircraft trajectory
Physical form					**No mid-air or ground collisions**



Abstraction-hierarchy useful for safety design. Rigorous approach. May improve model validation vs model development alone.

SERL AEROASTRO MIT

Results & Discussion

MIT Lincoln Laboratory

- National Airspace Safety. STAMP-STPA applied to UAS integration.
  - Top-down goal: prevent mid-air and ground collisions.

SYSTEM CONSTRAINTS
UAS operations shall not lead to loss of minimum separation requirements.
UAS operations shall not induce or contribute to a controlled flight into terrain maneuver.
UAS operations shall not induce or contribute to loss of aircraft controlled flight. -Aerodynamic/Structural limits, UAS C2 lost link disruptions

- ~65 High Level NAS safety requirements (STPA Step 1)
- ~68 Detect & Avoid safety/certification requirements (STPA Step 2)
- Draft publication

Overview

- Introduction
- Background
- Results and Discussion
- **Conclusions**
  - Use of cognitive systems engineering for sociotechnical system safety design
  - Future research

S E R L AERO ASTRO MIT

Conclusion

MIT Lincoln Laboratory

- Research question. How to develop an *adequate* qualitative model, the safety control structure?
  - Demonstrated use of Abstraction Hierarchy for understanding the Air Transportation system.
  - Demonstrated the Abstraction Hierarchy mapping to the safety control structure.
- Abstraction Hierarchy able to rigorously guide safety model development; toward model validation.

Future Research

Is the abstraction-decomposition framework useful for designing your sociotechnical system, for coping with complexity?

Influences on safety design: Competing priorities (e.g. efficiency), budget, automation trust

Ends-Means / Whole-Part	Total System Nat'l Airspace	Airspace Management	Local airspace control	Individual aircraft control	Component
Functional purpose	**System goal.** Safe integrated flight operations; accident free	Safe NAS flight operations	Safe NAS flight operations	Safe aircraft control	Safe encounter
Abstract function	Rules & Regs. NAS req'ts, architecture, operations	Aggregate mass flow	Local mass flow	Aircraft energy control	Mass separation
Generalized functions		4-d flight planning (strategic control)	Communications	Lift, drag, power control	Collision free flight
Physical functions		Procedural control	Air Traffic Control, decision support, communications functions	Pilot/operator, decision support, communications (C2 Link)	Safe aircraft trajectory
Physical form					**No mid-air or ground collisions**

Decomposition model

Temporal model

SERL MIT AEROASTRO

Acknowledgements

MIT Lincoln Laboratory

- The authors thank Dr. Roland Weibel, MIT Lincoln Laboratory Technical Staff, for research collaboration and technical insights.

- Contact information:
  - Kip Johnson: johnskip@mit.edu
  - Prof Nancy Leveson: leveson@mit.edu