Extending Systems-Theoretic Safety Analyses for Coordination

Kip Johnson, PhD

29 Mar 2017, MIT, Cambridge, MA

Presentation derived from:

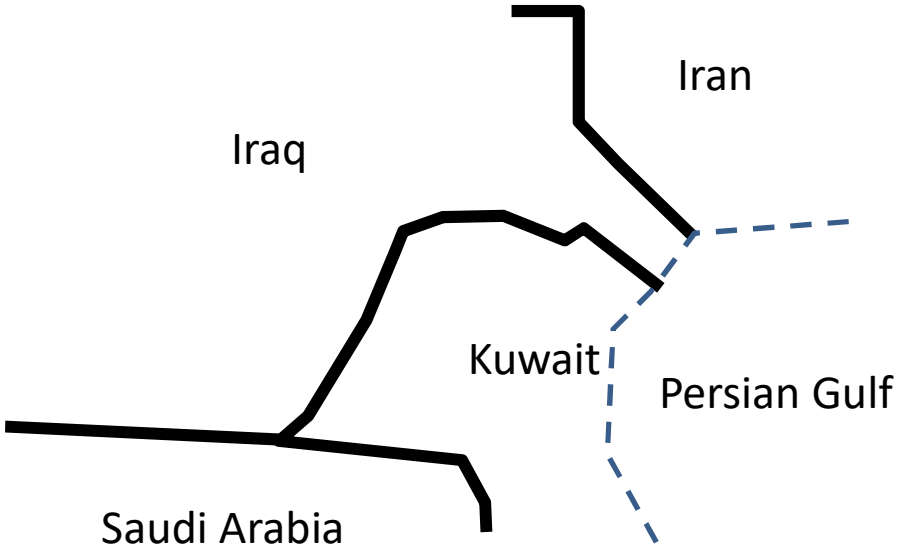
Johnson, Kip (2017). *Extending Systems-Theoretic Safety Analyses for Coordination*. MIT PhD Dissertation.

DISCLAIMER:
This material is based upon work supported by the Department of the Air Force under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the Department of the Air Force, Department of Defense, or the US Government.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.
(Edwards AFB, CA Public Affairs Release No. 17139)

Impact of Flawed Coordination

- Operation Iraqi Freedom
  - Mar 2003, British GR-4 returning to base, Kuwait
  - Patriot classified British GR-4 as a hostile missile
  - Patriot crew engaged GR-4, shot down aircraft, and two aircrew killed



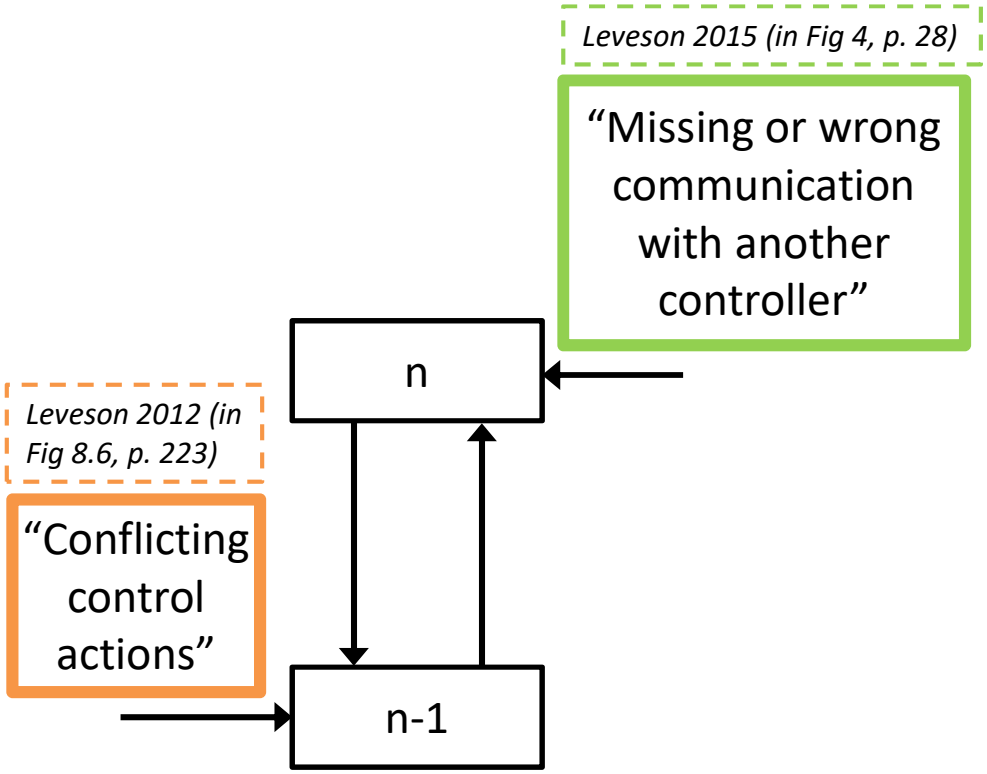
- Accident investigation recommendation: (UK Ministry of Defence 2004, p. 6)
  - "Closer **co-ordination** is implemented between planning and operations organisations regarding airspace usage"


history.redstone.army.mil (public domain)

Motivation: Towards the prevention of flawed coordination related accidents through safety analysis and design.

Systems Approach to Safety Leveson 2012

- **STPA** (System-Theoretic Process Analysis)
  - Identify unsafe control actions (step 1) and why they occur (step 2)
  - Inadequate coordination may lead to unsafe control actions (Leveson 2004)
- **CAST** (Causal Analysis using STAMP)
  - Accident analysis
  - Step 7. "Examine overall coordination" (Leveson 2012, p. 351)



Research Approach

- **Proposition**: To address safety in complex work domains, coordination between decision units is essential.
- **Problem**. The concept of coordination has limited operationalization for use in safety analysis methods, from safety engineering methods through accident investigation.
- **Overall Objective**: Develop extensions to state-of-the-art safety analyses to accommodate and guide examination of flawed coordination between multiple interdependent decision units.

A Coordination Framework

Johnson 2017

Purpose:

- Provide explanatory power and semantics for observation of and analysis of coordination in sociotechnical systems
- Bridge between theory and engineering applications

- **Decision Systems**
  - A functional model, decision behavior
  - Relate coordination with individual decisions/actions
- **Coordination Decomposed**
  - Descriptive power for analysis
  - Expand definition

- **Fundamental Coordination Relationships**
  - Analysis structure
  - Identify where analysis of coordination applies
- **Coordination Perspectives**
  - A means to operationalize the coordination framework for analysis

Decision System

Purpose: Functional model relating coordination to individual decisions and actions

- Sociotechnical System
  - Goal-directed behaviors
- Decision System
  - Decision behavior
  - Boundary defined by common output: action & coordination info
  - Component coordination
- Coordination Behavior
  - *Within* and *Between* decision system
  - Vertical and lateral coordination

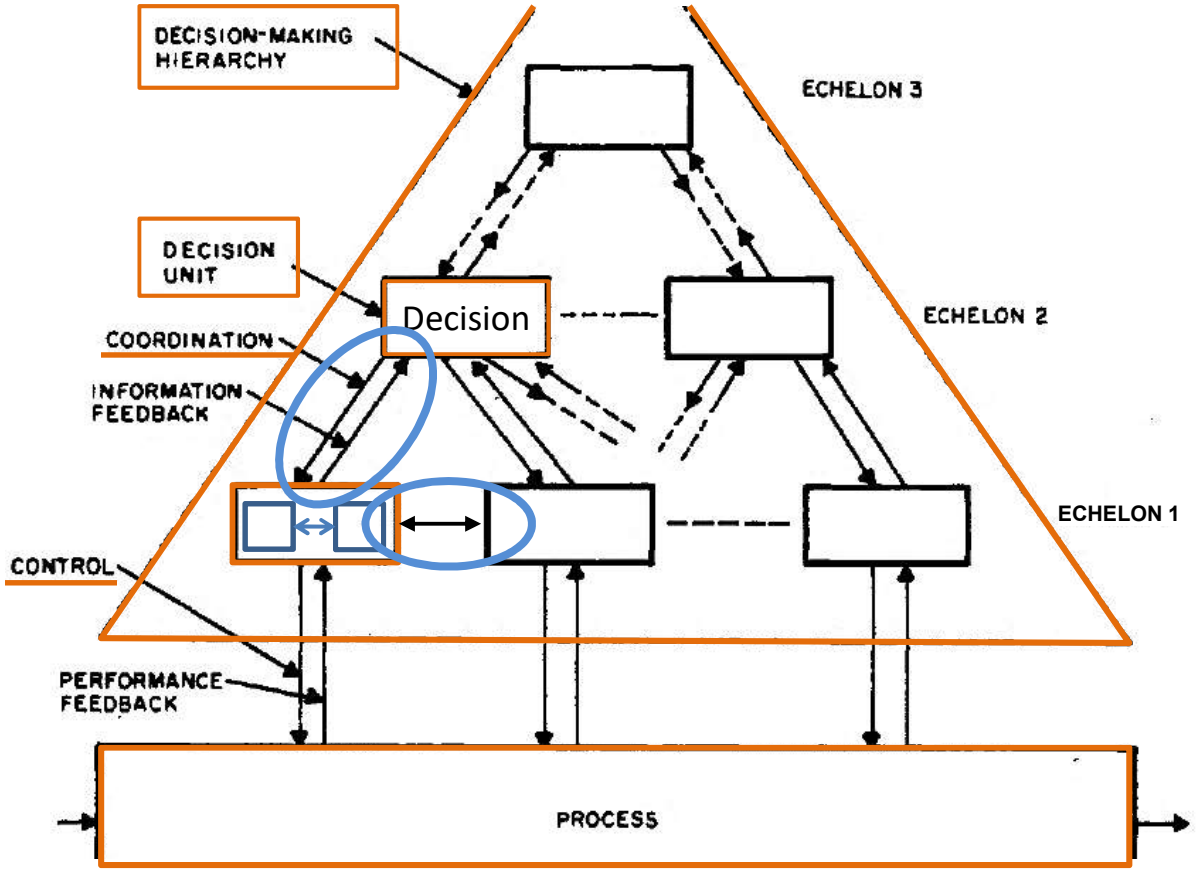


Figure ©1970 IEEE. Reprinted, with permission, from (Mesarović 1970), p 114

Coordination Elements

Purpose: Descriptive power for coordination behavior

- ***What*** is coordination?

Inspired by (Malone & Crowston 1990)

  - Components

Coordination Components

1. Coordination Goals
   - Overarching guidance for systems
2. Coordination Strategy
   - Planned set of behaviors among two or more decision units, pre-planned to dynamic
3. Decision Systems
   - Basic units that carry out coordination behavior

Coordination Elements

Purpose: Descriptive power for coordination behavior

- ***What*** is coordination?

Inspired by (Malone & Crowston 1990)

  - Components
  - Processes

Coordination Processes

4. Communications
   - Capabilities and protocols to exchange information
5. Group Decision-Making
   - Processes to determine and evaluate alternatives
6. Observation of Common Objects
   - Content and protocols of observation

Coordination Elements

Purpose: Descriptive power for coordination behavior

- What is coordination?
  - Components
  - Processes
- ***How*** is coordination accomplished?
  - Enabling conditions

Inspired by (Okhuysen & Bechky 2009)

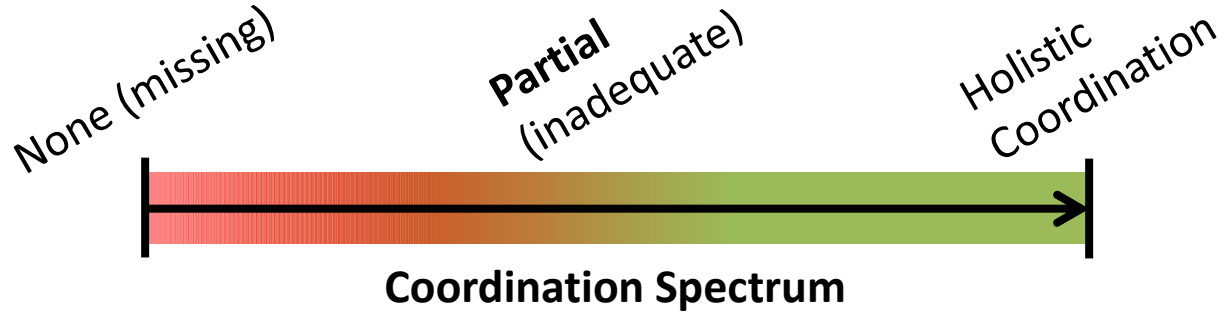
Coordination Enabling Conditions

7. Authority, Responsibility, Accountability
   - Properties needed to ensure coordination strategy is executed as intended
8. Common Understanding
   - A shared perspective the coordination problem and solution
9. Predictability
   - Knowledge of future behavior and the ability to anticipate

Partial Coordination

Holistic

Categories	Coordination Elements
Coordination Components	1. Coordination Goals
	2. Coordination Strategy
	3. Decision Units / Systems
Enabling Processes	4. Communications
	5. Group Decision-Making
	6. Observation of common objects
Enabling Conditions	7. ARA (Authority, Responsibility, Accountability)
	8. Common understanding
	9. Predictability



Decision System | Coordination Decomposed | Coordination Relationships | Coordination Perspectives

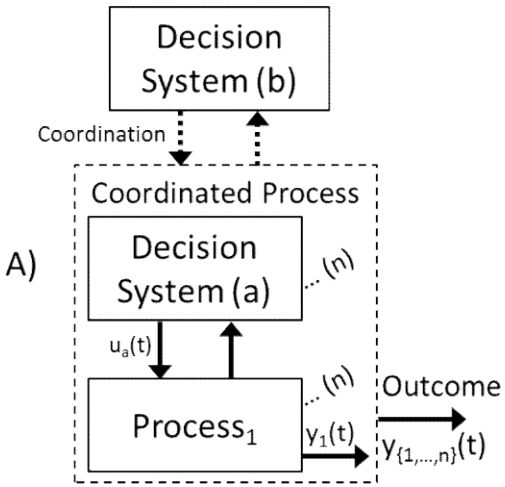
Coordination Definition

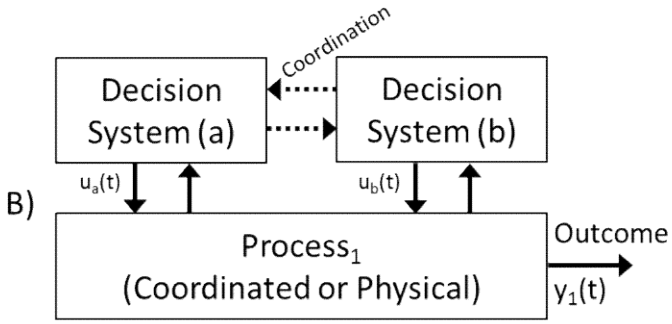
- **Coordination is:**
  - **The management of…**
    - (1) Goals
    - (2) Strategy
    - (7) Authority, Responsibility, Accountability
    - (8) Common understanding
    - (9) Predictability
  - **and processes needed…**
    - (4) Communications
    - (5) Group decision-making
    - (6) Observation of common objects
  - **to integrate interdependent entities.**
    - (3) Decision systems

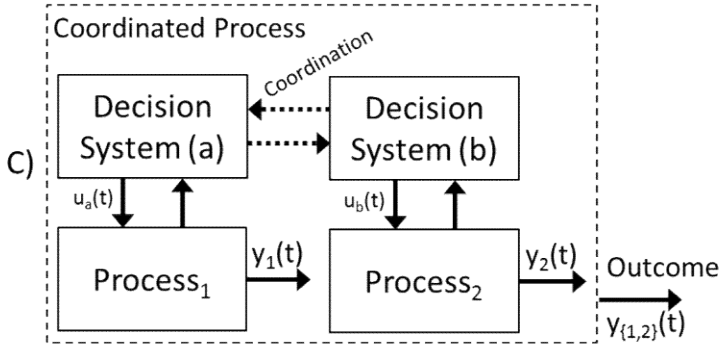
Fundamental Coordination Relationships

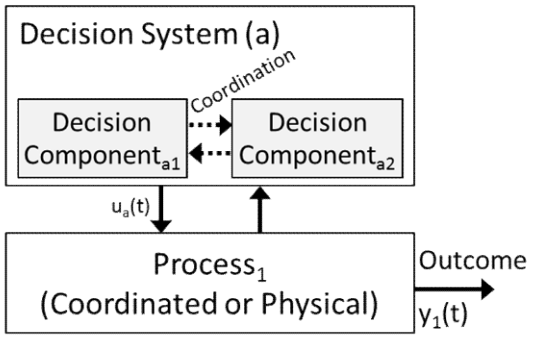
Purpose: Analysis structure

Coord Relationships	Vertical	Lateral
Between Dec'n System	A	B C
Within Dec'n System	--	D







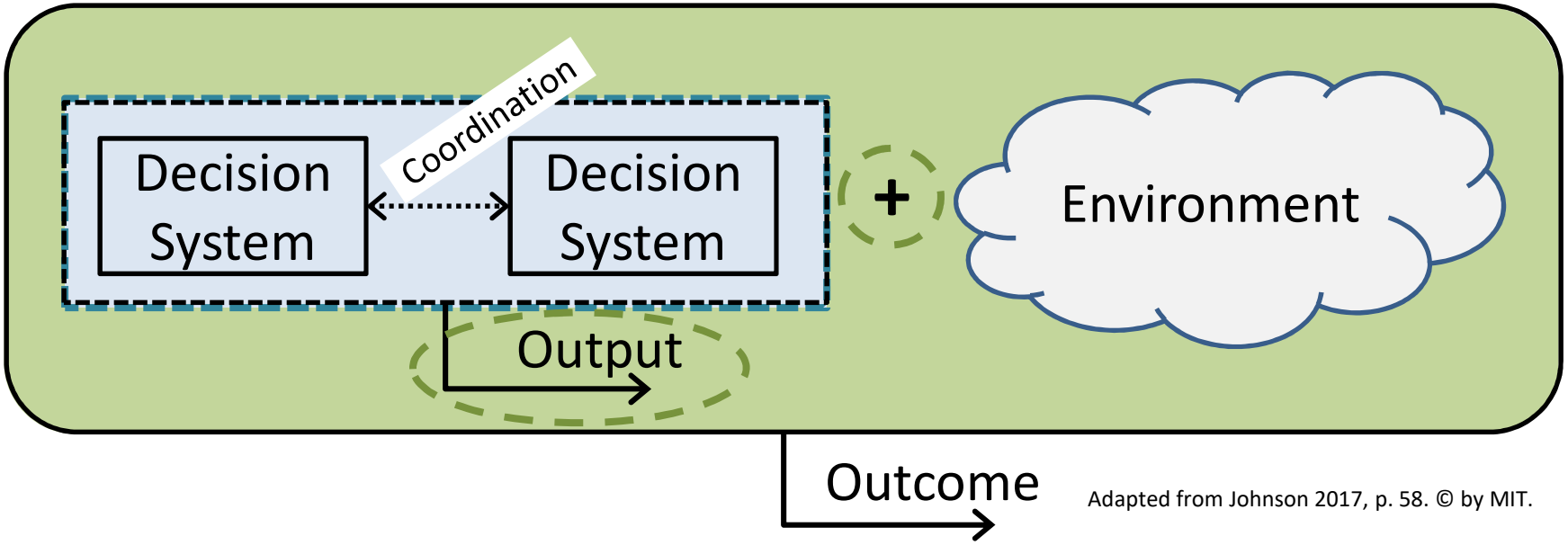


Figures adapted from Johnson 2017, p. 55. © by MIT.

Perspectives on Coordination

Purpose: Perspectives that can be operationalized for analysis

- Internal Perspective: coordination elements
- External Perspective: coordination strategy acceptable (e.g. safe)
  - Coordinated output
  - Coordinated output and environment



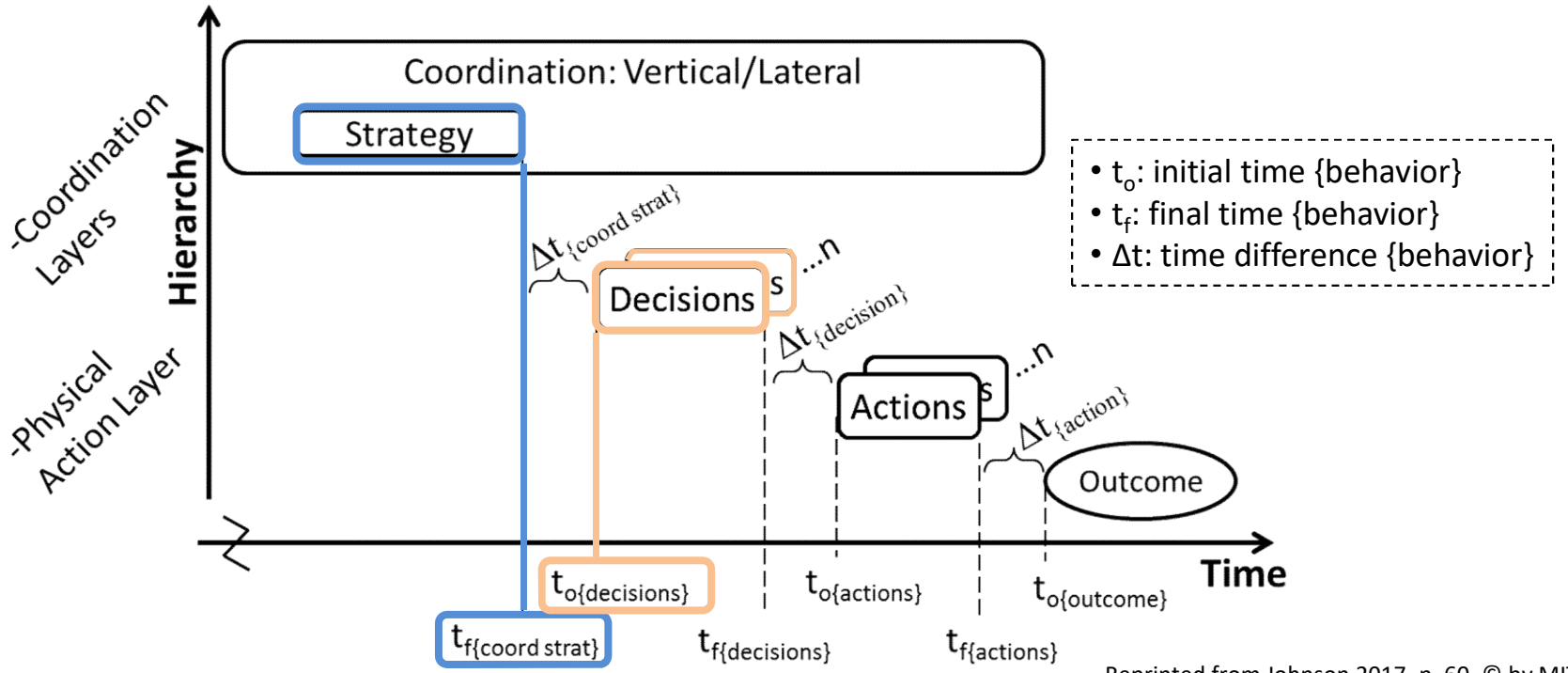
Adapted from Johnson 2017, p. 58. © by MIT.

Decision System | Coordination Decomposed | Coordination Relationships | Coordination Perspectives

Perspectives on Coordination

Purpose: Perspectives that can be operationalized for analysis

- Internal Perspective: coordination elements
- External Perspective: coordination in dynamic systems
  - Coordination strategy established to influence outcome



Reprinted from Johnson 2017, p. 60. © by MIT.

Extended STPA for Coordination

System-Theoretic Process Analysis (Leveson 2012, p. 213)

Step 1: "Identify the potential for inadequate control of the system that could lead to a hazardous state"

Step 2: "Determine how each potentially hazardous control action identified in step 1 could occur"

a) "examine the parts of the control loop to see if they could cause" the unsafe control action

b) "For multiple controllers of the same component or safety constraint, identify conflicts and potential coordination problems"

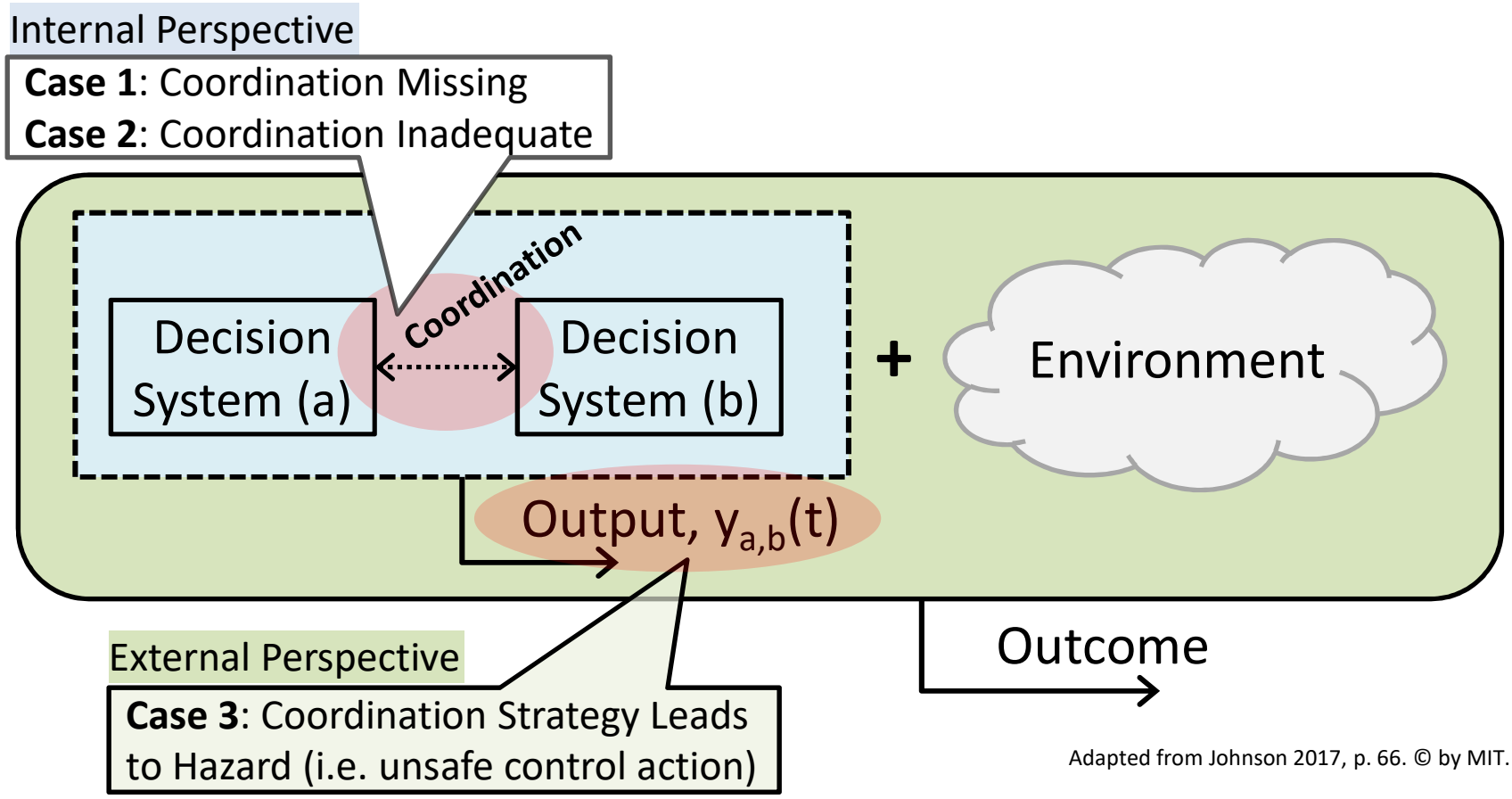
Extended (Johnson 2017)

b) **STPA-Coordination**. For multiple controller processes or coordinated decision-making.
- i) Identify the interdependency
- ii) Identify the fundamental coordination relationship
- iii) Identify coordination scenarios that can lead to unsafe control using the flawed coordination guidance

c) "Consider how the designed controls could degrade over time and build in protection"

Flawed Coordination Guidance

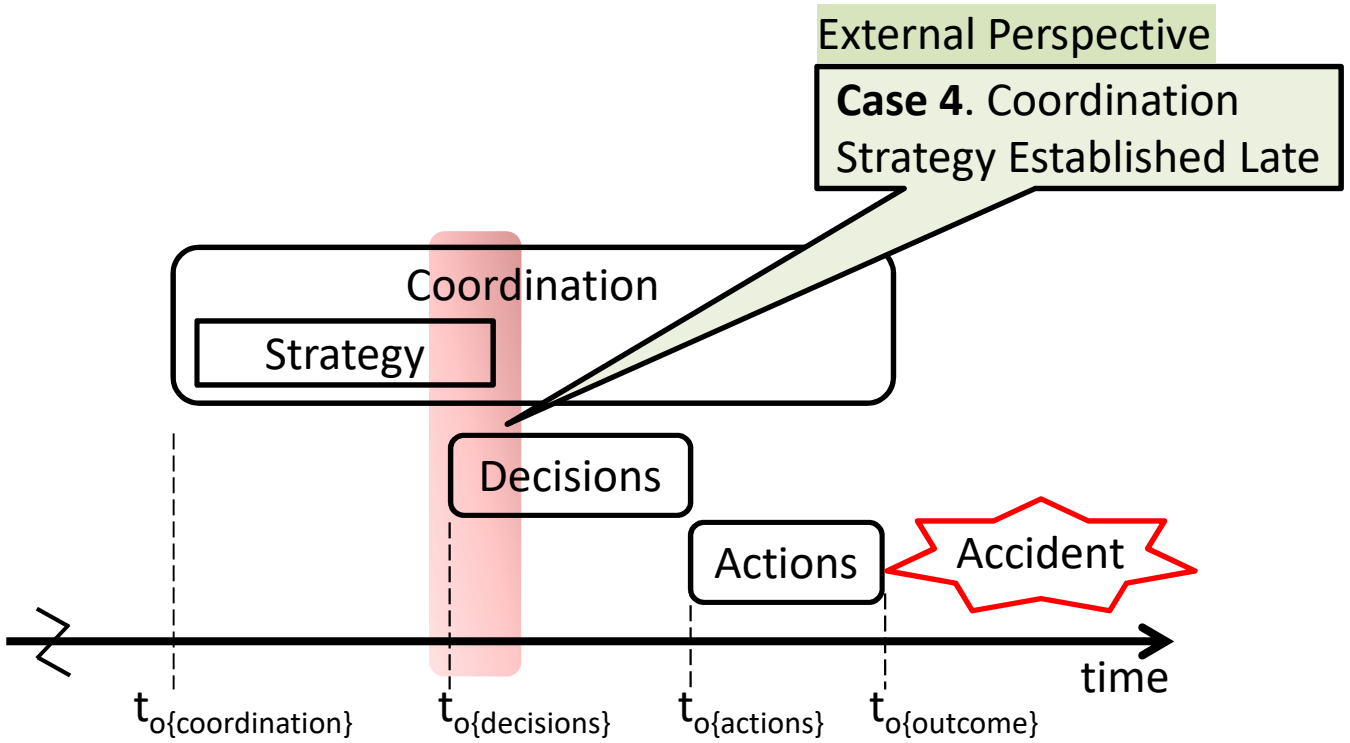
Purpose: Operationalize coordination framework for flawed coordination guidance



Adapted from Johnson 2017, p. 66. © by MIT.

Flawed Coordination Guidance

Purpose: Operationalize coordination framework for flawed coordination guidance



Adapted from Johnson 2017, p. 66. © by MIT.

Flawed Coordination Guidance

- *Flawed Coordination Cases* are unique

Table adapted from Johnson 2017, p. 66. © by MIT.

Unique Cases	Perspective: Internal	Perspective: External
Coord Strategy: None	Case 1	Case 4
Coord Strategy: Exists	Case 2	Case 3

Flawed Coordination Cases	Description
Case 1. Coord missing	Coord missing w/ interdependent conditions
Case 2. Coord inadequate	Coord elements missing or inadequate
Case 3. Coord strategy leads to UCAs	Coord strategy is unacceptable or infeasible
Case 4. Coord strategy established late	Coord strategy established late to influence safe outcome

Flawed coordination cases guide STPA in identifying coordination scenarios that may lead to unsafe control actions

Flawed Coordination Guidance

- Additional flawed coordination guidance using coordination elements

Table adapted from Johnson 2017, p. 68. © by MIT.

Coordination Elements: Missing or Inadequate	Flawed Coord Cases Lead to UCAs			
	1	2	3	4
(1) Coordination Goals	x	x		x
(2) Coordination Strategy	x	x	x	x
(3) Decision Systems		x		x
(4) Communications		x		x
(5) Group Decision-Making	x	x		x
(6) Observation of Common Objects		x		x
(7) Authority, Responsibility, Accountability		x		x
(8) Common Understanding		x		x
(9) Predictability		x		x

Case 2 Guidance:
Expanded next slide

Flawed Coordination Cases Refined

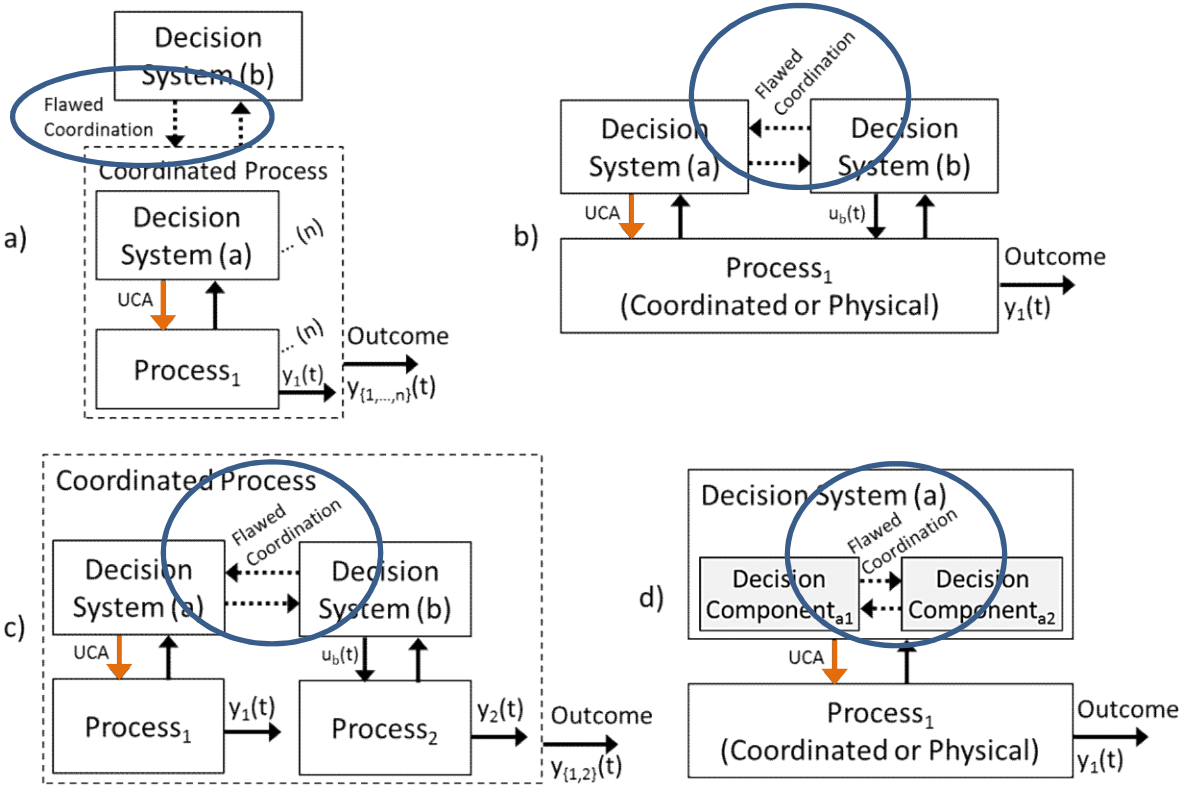
- Coordination elements used for flawed coordination guidance
  - Examples, Case 2 (see Johnson 2017, p. 69, Table 16 for more guidance)

Case 2. Coordination inadequate (strategy exists)
Coordination Components
1. Coordination goals: inconsistent 2. Coordination strategy: do not address interdependent conditions; ambiguous; alternative strategies unknown or incompatible 3. Decision Systems: missing, inadequate aptitude or training
Coordination Enabling Processes
4. Communication channels: missing; inadequate (bandwidth, noise, etc.) 5. Group DM: inadequate (protocols, value functions, problem solving framework, etc.) 6. Observation of common objects: missing; different objects; inadequate (resolution, delays, update rates, information, etc.)
Coordination Enabling Conditions
7. Authority, Responsibility, Accountability: missing; inadequate (observation, update rates, assignment of roles & responsibilities, confidence in other decision systems, etc.); decision systems not coordinable (by design or by organization)
8. Common understanding: missing (process modes, states); inadequate (geo-physical or time reference, local or holistic model, system states, strategy, other decision units, etc.) 9. Predictability: missing; inadequate (models, not familiar with task, time constraints, etc.)

Extended STPA Summary

STPA-Coordination

i. Identify interdependency
ii. Identify coordination relationships
iii. Use flawed coordination guidance to identify scenarios that can lead to unsafe control actions
   - Flawed Coord Cases x4
   - Coord Elements x9



Case Study: UAS Integration

Purpose: Towards validation of STPA-Coordination

Image © DARPA
(www.darpa.mil/news-events/2016-03-31)

- Background
  - UAS integration with military and civilian flight operations
  - RTCA standards efforts (SC-203, SC-228) over a decade old (2004 beginning)
  - Assessing safety a challenge, ongoing

- Systems Engineering Baseline
  - Goal: Safe flight operations
  - Accidents (A) to avoid:
    - A1. Mid-air collisions.
    - A2. Collisions with terrain and ground obstacles.
  - Hazards (H):
    - H1. Violation of aircraft minimum separation. (←A1)
    - H2. Controlled flight into terrain. (←A2)
    - H3. Lack of aircraft controlled flight. (←A1, A2)

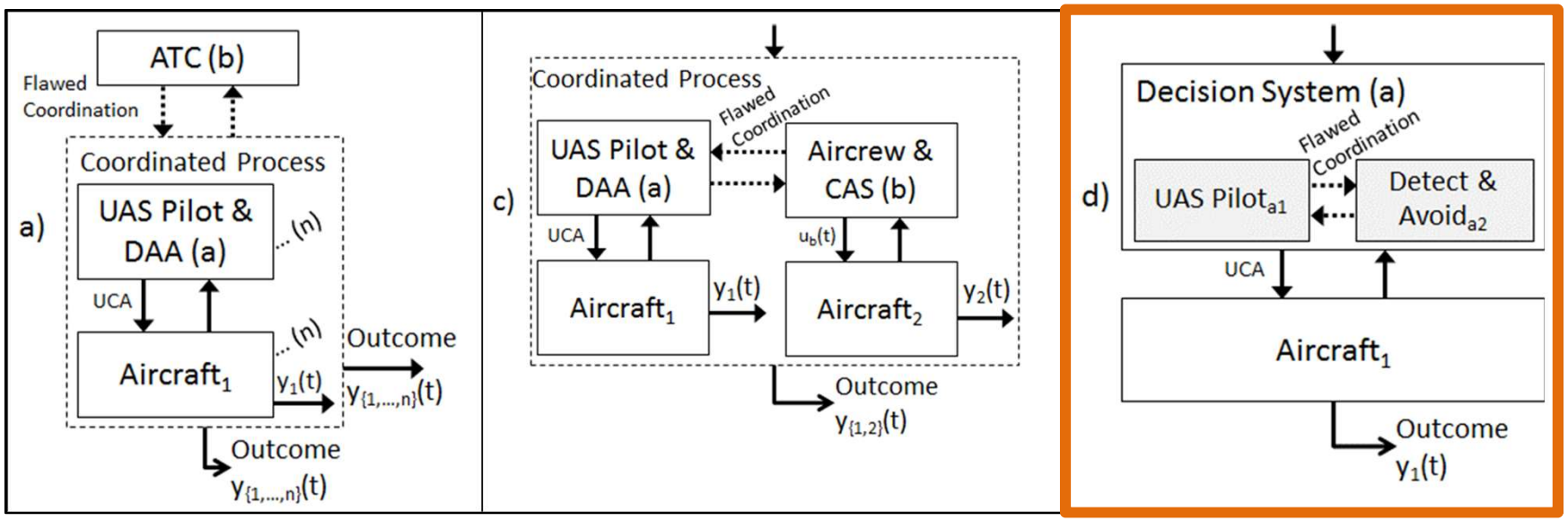
STPA-Coordination Applied

i) Identify the interdependency

- Shared goals. Accident free operations, collision avoidance
- Shared resources. Airspace for aircraft navigation

ii) Identify the coordination relationships

UCA. Unsafe Control Action; DAA. Detect-and-Avoid; CAS. Collision Avoidance System



Reprinted from Johnson 2017, p. 89. © by MIT.

iii) Using flawed coordination guidance, identify scenarios that can lead to UCAs

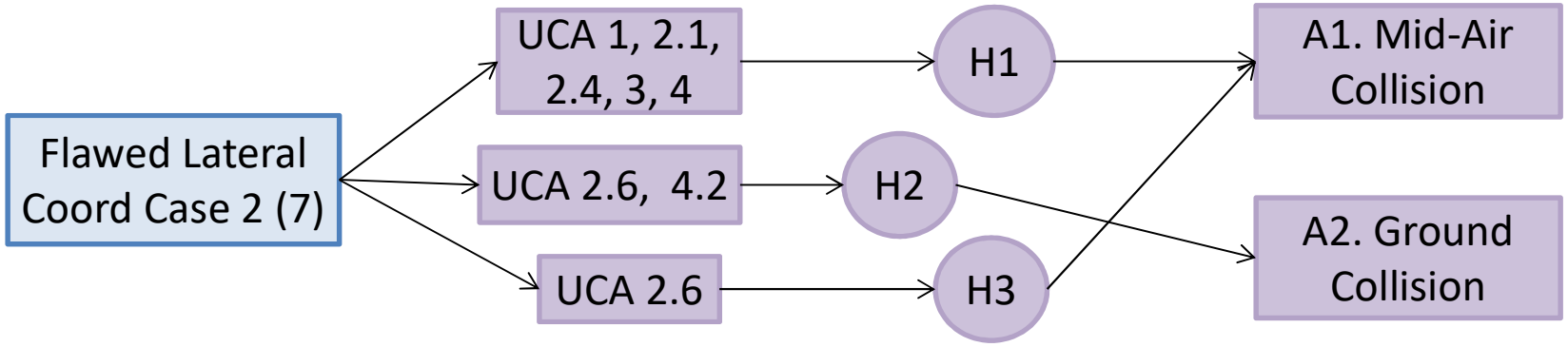
Next: Within decision system STPA-Coordination excerpt

Lateral Coordination Example

UCA. Unsafe Control Action; DAA. Detect-and-Avoid; CAS. Collision Avoidance System

Table adapted from Johnson 2017, p. 99. © by MIT.

Case 2: Inadequate, (7) Accountability	UCAs	Safety Recommendations
• (within Decision System) The DAA does not have means to establish accountability for lateral coordination.	1, 2.1, 2.4, 2.6, 3, 4	• The DAA/CAS shall provide means to establish lateral coordination accountability.
○ Decision systems do not confirm receipt of DAA/CAS cooperative maneuver strategy and they actually did not receive the maneuver guidance.		○ UAS decision systems shall confirm receipt of DAA derived maneuver strategy
○ Decision systems do not acknowledge agreement with DAA/CAS maneuver guidance and one or more actually disagree with guidance.		○ UAS decision systems shall confirm agreement with maneuver strategy



Comparison to Functional Hazard Analysis

- UAS Integration Safety & Performance Standards, DO-344 (RTCA SC-203, 2013)

Table adapted from Johnson 2017, p. 132. © by MIT.

Coordination Elements	Hazardous Coordination Scenarios	
	DO-344	STPA-Coordination
1. Coordination Goals	0	3
2. Coordination Strategy	0	46
3. Decision Systems	0	3
4. Communications	1	16
5. Group Decision-Making	0	12
6. Observation of Common Objects	7	18
7. Authority, Responsibility, Accountability	0	23
8. Common Understanding	30	46
9. Predictability	10	27
Total Hazardous Coordination Scenarios	**48**	**194**

Observations include:

- STPA-Coord identified hazardous scenarios related to 9 elements, vs 4 in FHA
- ~6% of STPA-Coord scenarios due to failure modes, vs 100% for FHA. 94% of STPA-Coord scenarios are potentially *designed* flawed interactions (i.e. not failing)

Comparison to Requirements Analysis

- UAS Integration Safety & Performance Standards, DO-344 (RTCA SC-203, 2013)

Table adapted from Johnson 2017, p. 136. © by MIT.

Coordination Elements	Coordination Recommendations	
	DO-344	STPA-Coordination
1. Coordination Goals	0	2
2. Coordination Strategy	4	53
3. Decision Systems	0	2
4. Communications	2	22
5. Group Decision-Making	0	13
6. Observation of Common Objects	4	25
7. Authority, Responsibility, Accountability	0	33
8. Common Understanding	19	37
9. Predictability	3	29
Total Coordination Recommendations	**32**	**216**

Observations include:

- STPA-Coord recommendations addressed a holistic set of 9 elements, vs 5 using ad-hoc methods
- STPA-Coord had 53 recommendations for coordination strategy, vs 4

CAST-Coordination

CAST (Causal Analysis w/ STAMP)

(Leveson 12)

1-2. Systems engineering baseline. Identify accidents, hazards, safety constraints

3. Document the safety control structure, including roles and responsibilities

4. Identify proximate events

5. Identify unsafe controls, failures, and interactions at the physical system level

6. Identify why higher levels allowed or contributed to an accident. Document context for decisions.

7. "Examine overall coordination and communication contributors to the loss" (Leveson 2012, p. 351)

8. Determine if migration towards unsafe behaviors was a factor

9. Generate recommendations

Extended

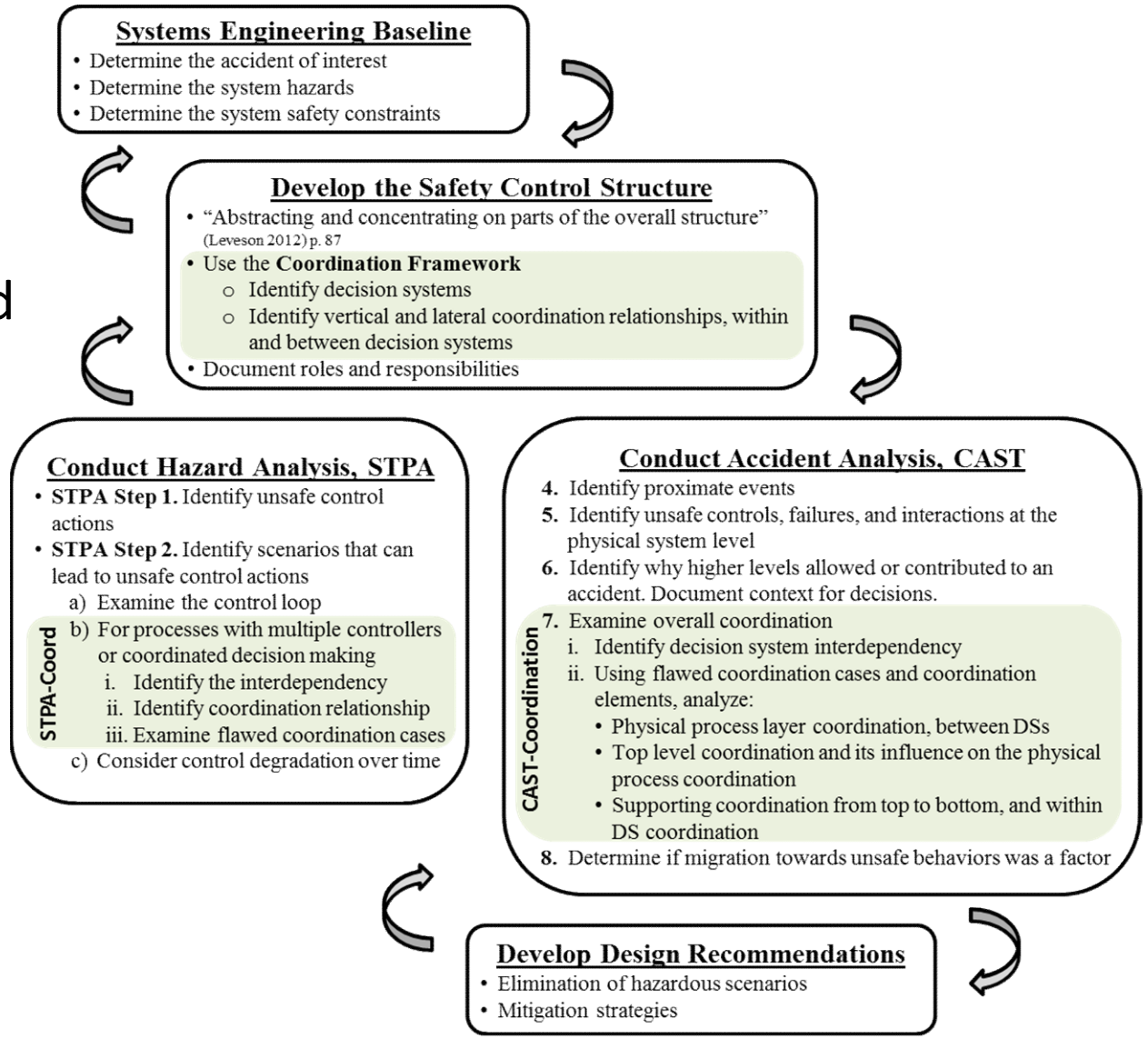
CAST-Coordination (Step 7)

(Johnson 2017)

- Identify decision systems with interdependency
- Use flawed coordination guidance to analyze:
  - Physical process level coordination
  - Top level coordination and its influence on the physical process coordination
  - Supporting coordination. Decision-making hierarchy coordination from top to bottom and within decision system coordination

Systems approach to safety, a coordination focus:

- Coordination framework with four points
- Extended STPA and CAST analysis methods
- Flawed coordination guidance
- Design recommendations that lead to safe coordination



Reprinted from Johnson 2017, p. 183. © by MIT.

Acknowledgements

- Prof. Nancy Leveson
- Committee: Prof. Sheila Widnall, Prof. John Flach, Dr. Roland Weibel
- Dr. John Thomas
- Readers: Prof. Leia Stirling, Prof. Cody Fleming
- Lab mates at MIT, MIT Lincoln Lab, Beaverworks

Bibliography

- United Kingdom Ministry of Defence, 2004. *Aircraft Accident to Royal Air Force Tornado GR MK4A ZG710*, London, UK.
- Johnson, K.E., 2017. *Extending Systems-Theoretic Safety Analyses for Coordination*. MIT PhD Dissertation.
- Leveson, N.G., 2004. A New Accident Model for Engineering Safer Systems. *Safety Science*, 42(4), pp. 237-270.
- Leveson, N.G., 2012. *Engineering a Safer World: Systems Thinking Applied to Safety*, Cambridge, MA: The MIT Press.
- Leveson, N.G., 2015. A systems approach to risk management through leading safety indicators. *Reliability Engineering and System Safety*, 136, pp.17–34.
- Malone, T.W. & Crowston, K., 1990. What is Coordination Theory and How Can It Help Design Cooperative Work Systems? In *Proceedings of the 1990 ACM Conference on Computer-Supported Cooperative Work*. Los Angeles, CA: ACM, pp. 357–370.
- Mesarović, M.D., 1970. Multilevel Systems and Concepts in Process Control. *Proceedings of the IEEE*, 58(1), pp.111–125.
- Okhuysen, G.A. & Bechky, B.A., 2009. Coordination in Organizations: An Integrative Perspective. *The Academy of Management Annals*, 3(1), pp.463–502.