Air Force Institute of Technology

Develop America's Airmen Today ... for Tomorrow

U.S. AIR FORCE

Tutorial: STPA-Coordination Introduction

Presented at: 2024 MIT STAMP Workshop

Kip Johnson, Assistant Professor
AF Institute of Technology
4 Jun 2024



Service since 1947: Granting degrees since 1956

Air University: The Intellectual and Leadership Center of the Air Force

Aim High...Fly – Fight – Win

Disclaimer

The views expressed in this presentation are those of the author and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government.

DISTRIBUTION STATEMENT A.
APPROVED FOR PUBLIC RELEASE 88 ABW Case 2024-0431
DISTRIBUTION UNLIMITED

Overview

- **Purpose:**
  - *Introduce* STPA-Coordination;
    - CAST-Coordination uses the same coordination framework, but not a focus of this tutorial.
  - Based on Johnson's 2017 MIT PhD Dissertation
    - http://sunnyday.mit.edu/johnson-dissertation.pdf

- **Agenda**
  - Motivation/Background
  - Coordination Framework
  - STPA-Coordination

Motivation

- **Interdependence**
  - Mutual dependence
  - Outcome depends on each other



Figure 2. Doctors Without Borders Friendly Fire Incident, Kunduz, Afghanistan 2015.
Image from (US Central Command 2015), p. 70. Image in public domain.

Interdependency exists?
Coordination is required to ensure acceptable outcomes



Image in public domain. US Army

Coordination Defined

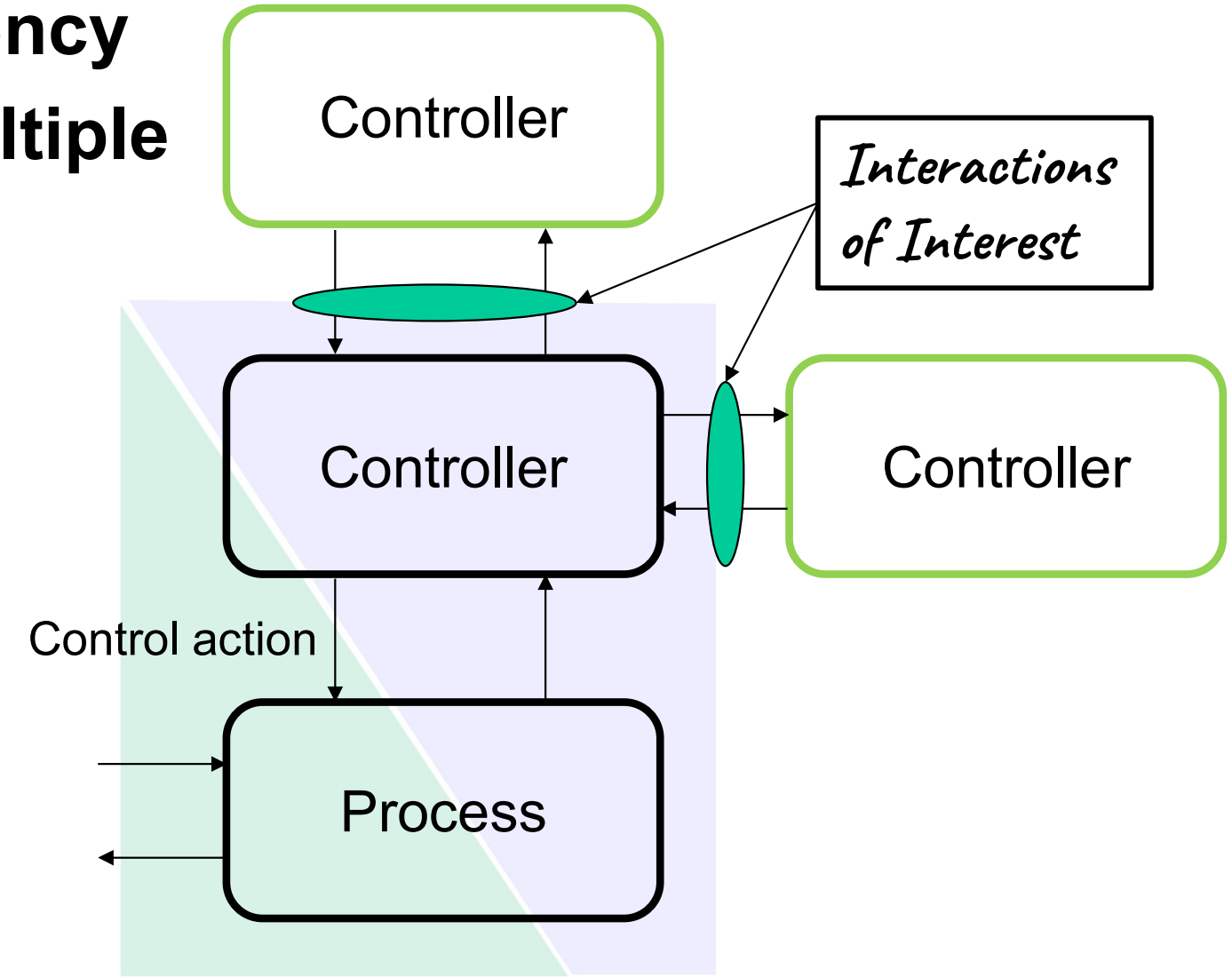
- **Coordination ≠ Communication**

- **Coordination is:**

  "management of and the processes needed to integrate interdependent entities" (Johnson, 2017. p. 33)

Coordination in STPA

- **Interdependency**
- **Focus on multiple controller interactions**
- **Vertical and Horizontal Interactions**



Coordination Framework

- **Providing explanatory power to conduct STPA/CAST for multiple-controller interactions**

Coordination Framework

- **4 Primary Concepts**
  1. Decision System functional model
  2. Coordination elements (9)
  3. Fundamental coordination relationships
  4. Coordination perspectives

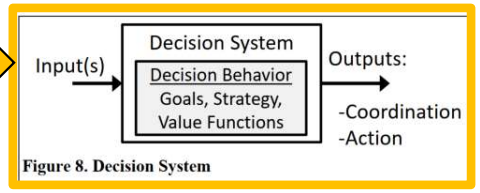


Figure 8. Decision System

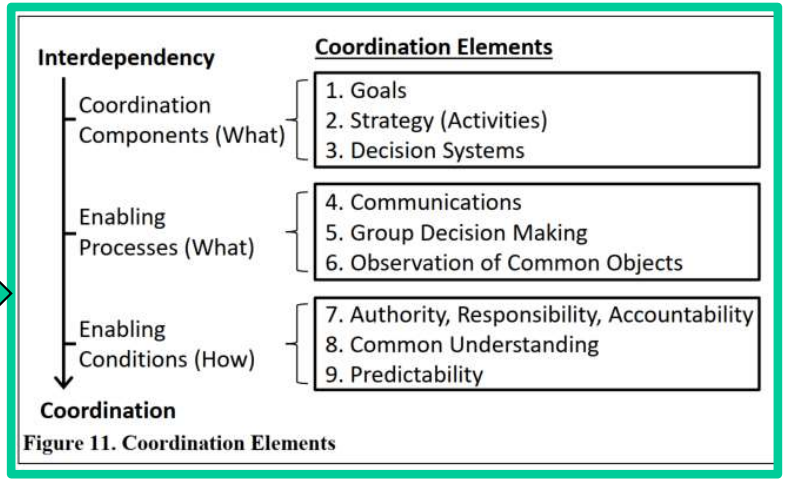


Figure 11. Coordination Elements

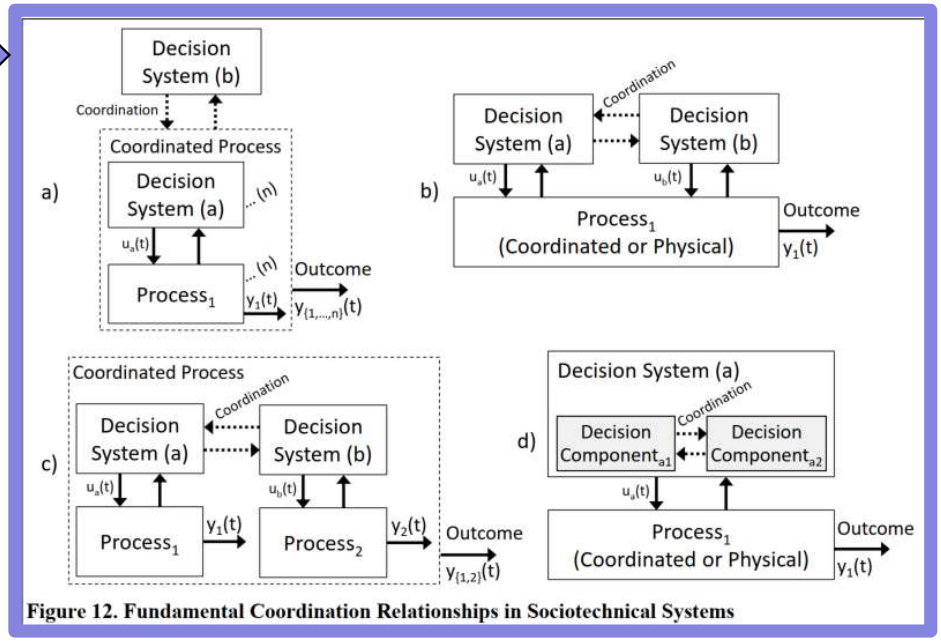


Figure 12. Fundamental Coordination Relationships in Sociotechnical Systems

Coordination Framework

- **Decision System**
  - Behavior
    - Goals
    - Strategy
    - Value Functions
  - Outputs
    - Action → Control mechanisms in STPA
    - Coordination
  - Is a *functional* model
    - Function vs form?
    - Decision component?



Figure 8. Decision System

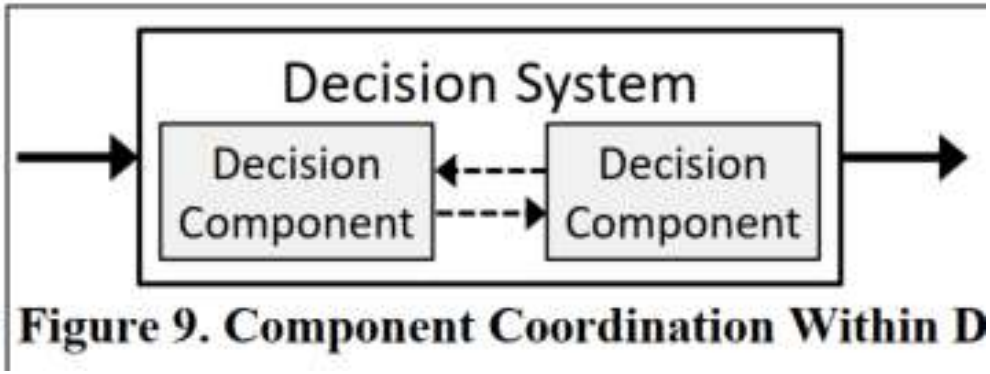


Figure 9. Component Coordination Within D

Coordination Framework

- **4 Primary Concepts**
  1. Decision System functional model
  2. Coordination elements
  3. Fundamental coordination relationships
  4. Coordination perspectives

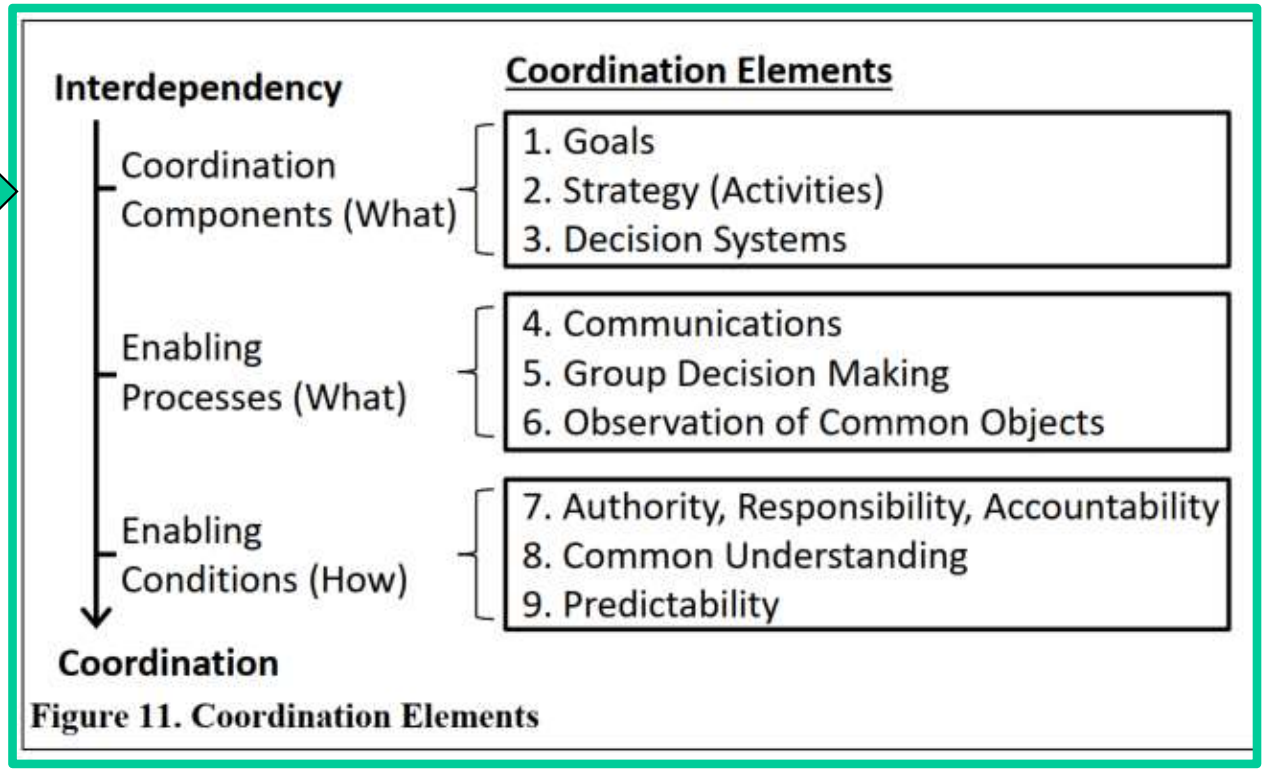


Figure 11. Coordination Elements

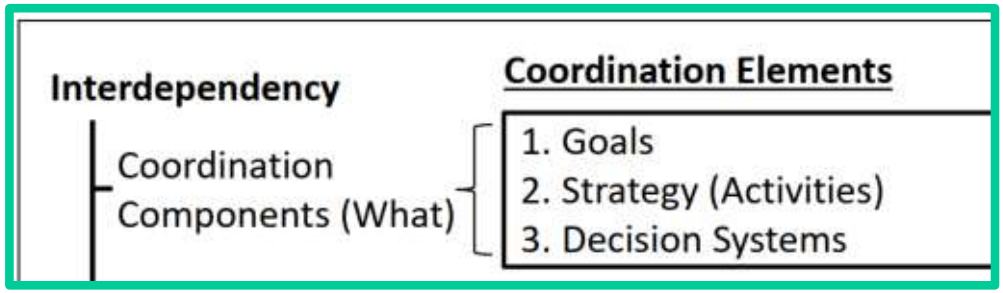
Coordination Framework

- **Coordination elements**
  - Components
    - Coordination Goals

      The minimum interdependency
    - Coordination Strategy

      Planned set of behaviors and activities needed to achieve coordination goals
    - Decision Systems

      e.g. humans, organizations, AI, automation, software



Coordination Framework

- **Coordination elements**
  - Enabling Processes
    - Communications

      Capabilities and protocols to enable information sharing
    - Group Decision Making

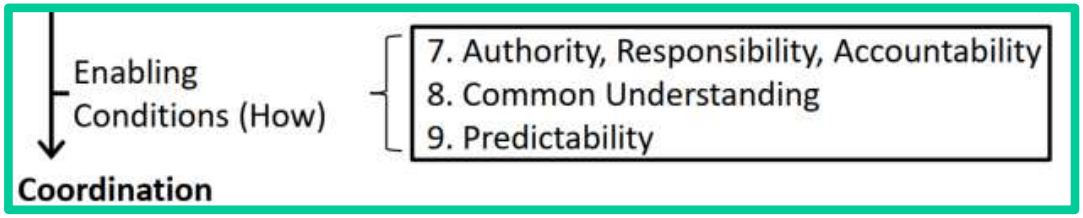
      Processes that enable decision system/component interactions to develop coordination strategies and determine actions
    - Observation of Common Objects

      Process to ensure decision system process models are the same; observation protocols/timing influence this process



Coordination Framework

- **Coordination elements**
  - Enabling Conditions
    - Authority, responsibility, accountability
    - Common Understanding
    - Predictability



Coordination Framework

- **4 Primary Concepts**
  1. Decision System functional model
  2. Coordination elements
  3. Fundamental coordination relationships
  4. Coordination perspectives

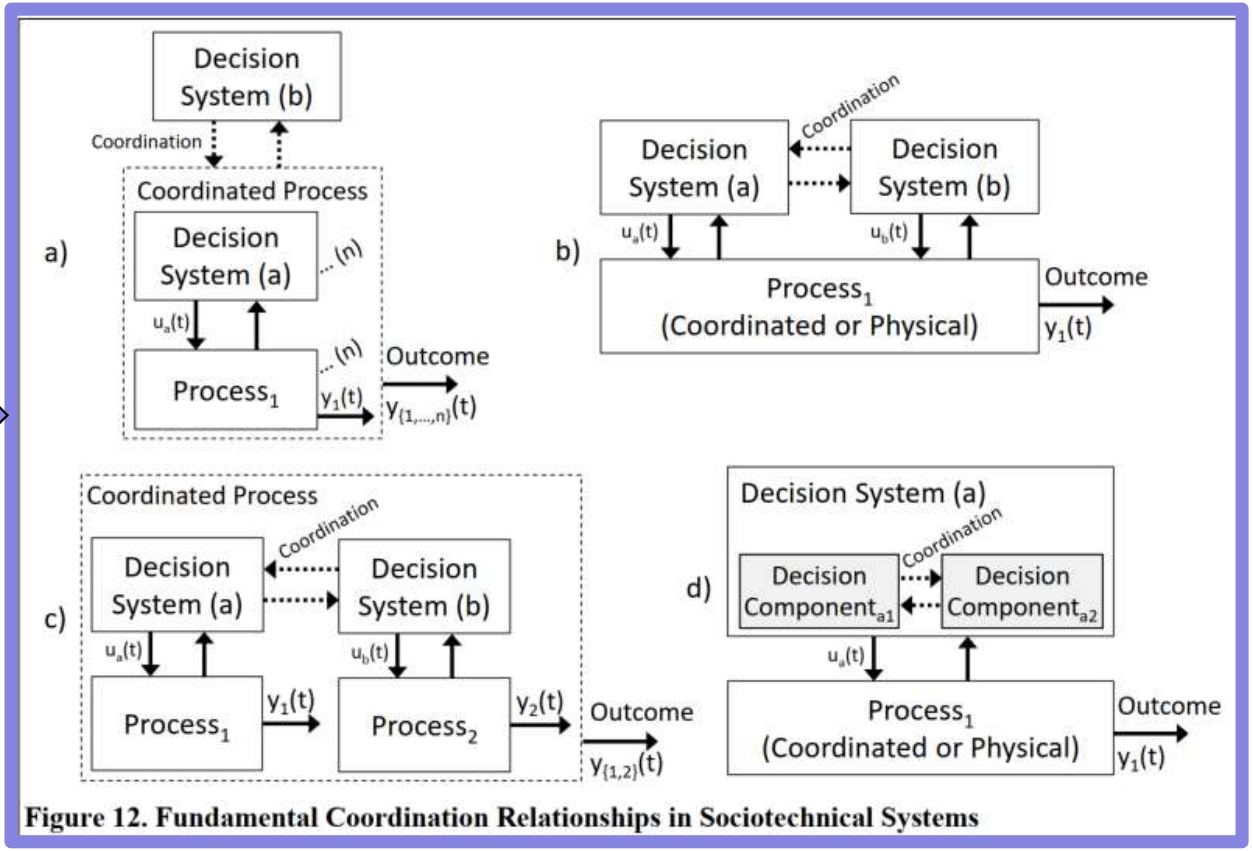


Figure 12. Fundamental Coordination Relationships in Sociotechnical Systems

Coordination Framework

- **Fundamental Coordination Relationships**
  - **Within Decision System coordination**

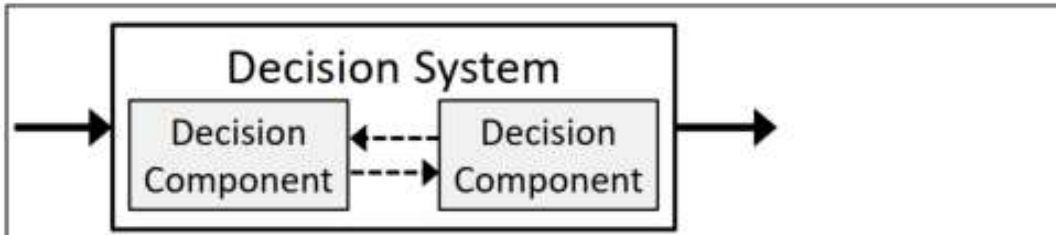


Figure 9. Component Coordination Within Decision System

  - **Between Decision System coordination**

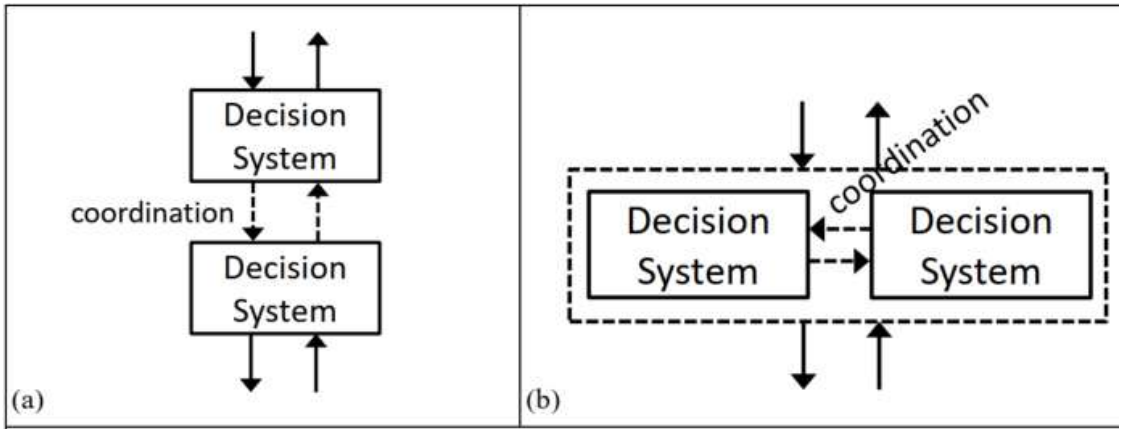


Figure 10. Between Decision System Coordination, (a) Vertical and (b) Lateral

Coordination Framework

- **Fundamental Coordination Relationships**

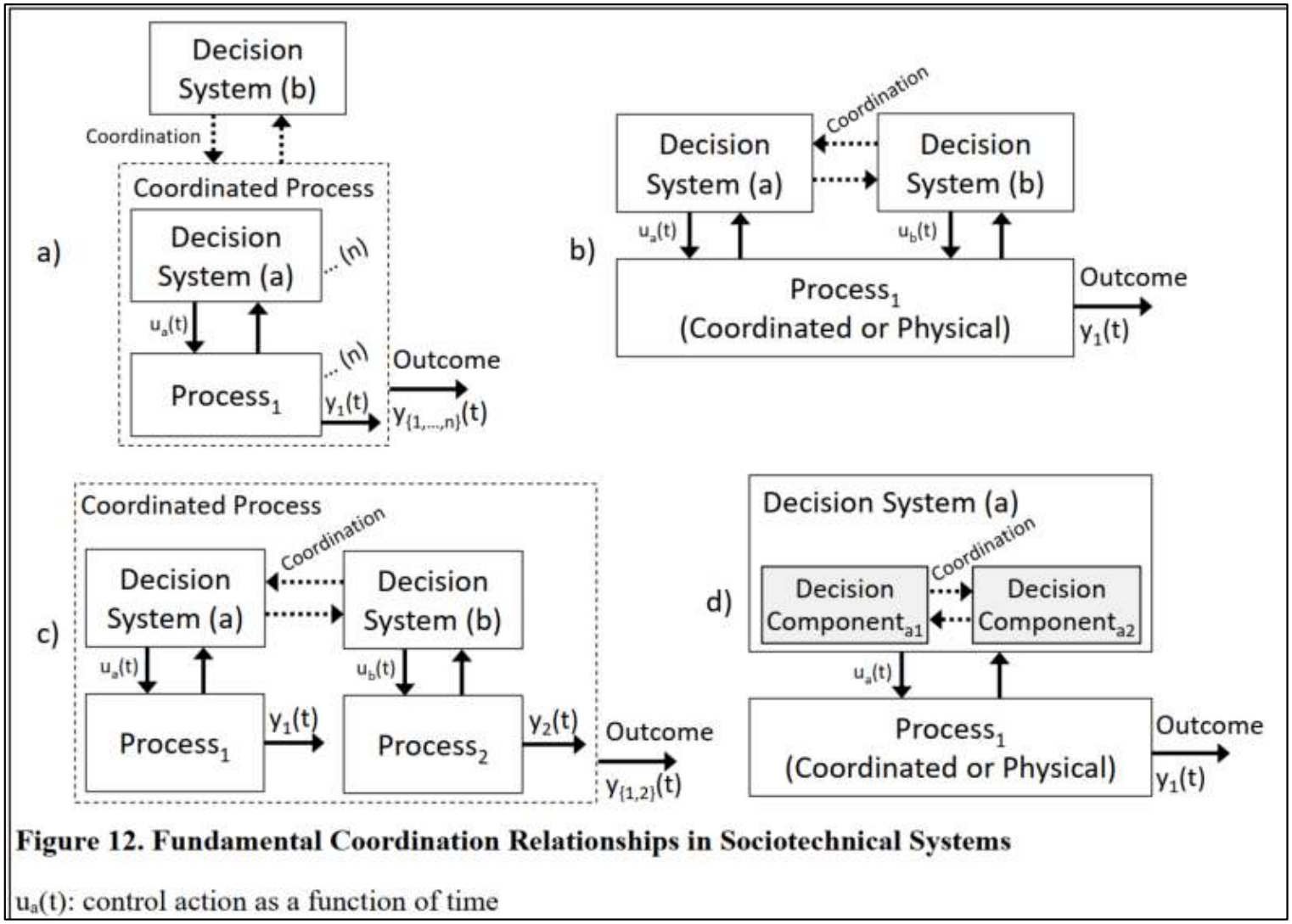


Figure 12. Fundamental Coordination Relationships in Sociotechnical Systems

$u_a(t)$: control action as a function of time

Johnson, 2017

Coordination Framework

- **Perspectives – Hierarchy vs Temporal**
  - Time to develop a coordination strategy
  - Time to make decisions (humans?)
  - Time to execute actions
  - $T_{f\{coord\ strategy\}}$ needs to occur before $t_{o\{decisions\}}$

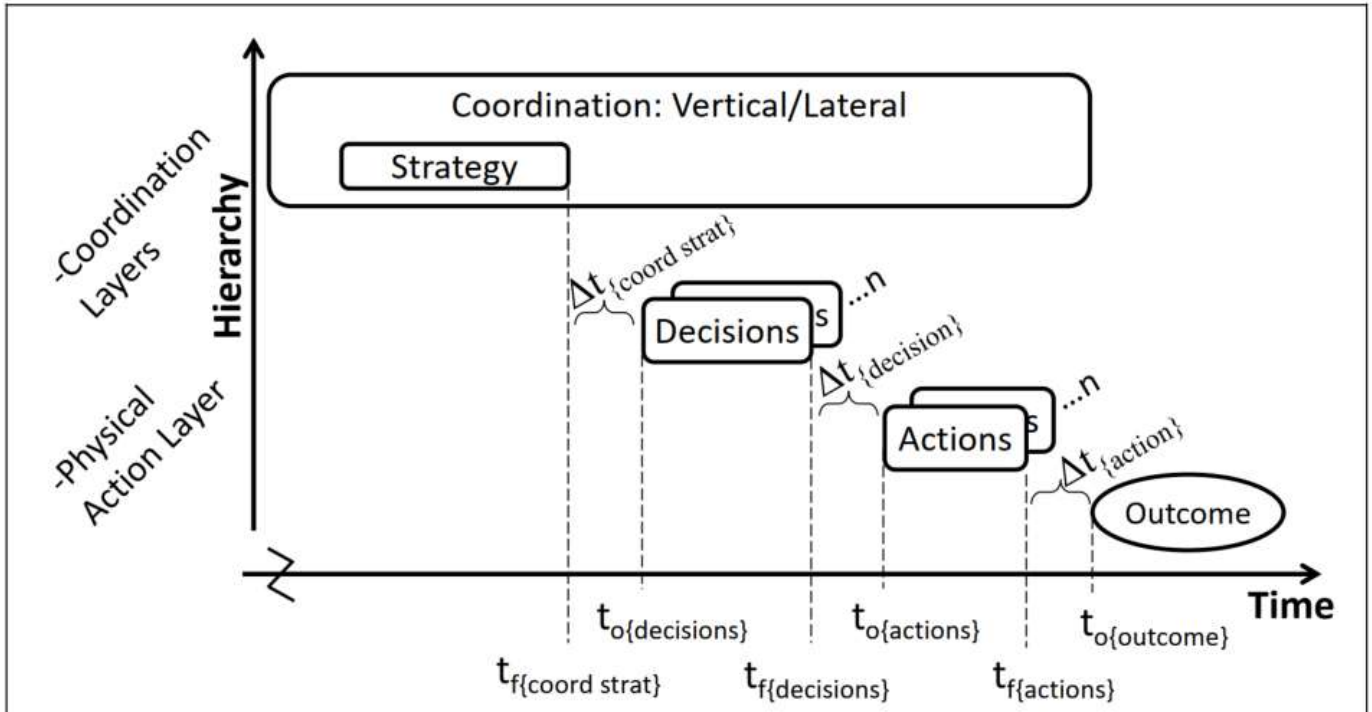


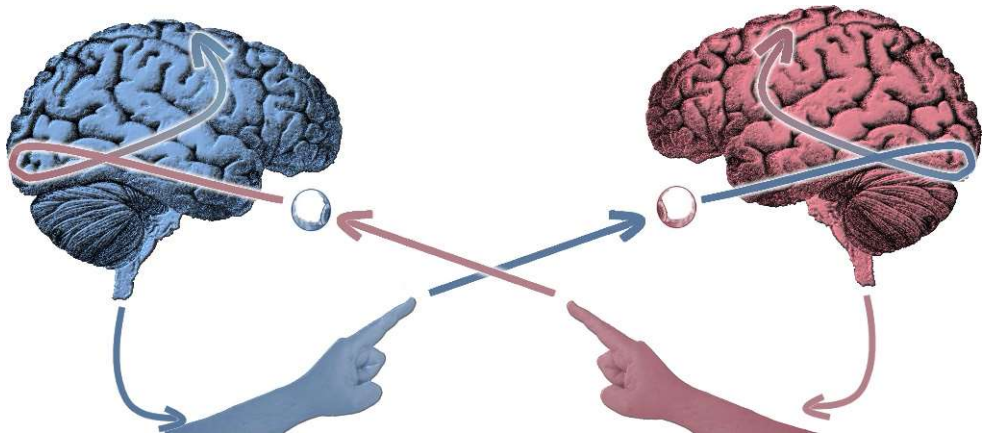
Figure 14. Coordination and Time

$t_{f\{behavior\}}$: finish time of a behavior
$t_{o\{behavior\}}$: initial time of a behavior
Δt: time difference between behaviors

Johnson, 2017

Coordination Framework

- **Provides**
  - Explanatory power for the observation and analysis of coordination behavior in sociotechnical systems
- **Operationalized**
  - For analysis of coordination to ensure safety or other emergent property
  - STPA-Coordination
  - CAST-Coordination



This Photo by Unknown Author is licensed under CC BY



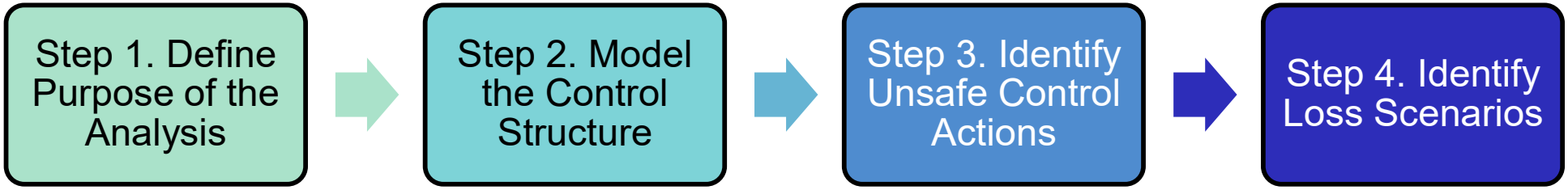
This Photo by Unknown Author is licensed under CC BY-NC-ND

STPA-Coordination

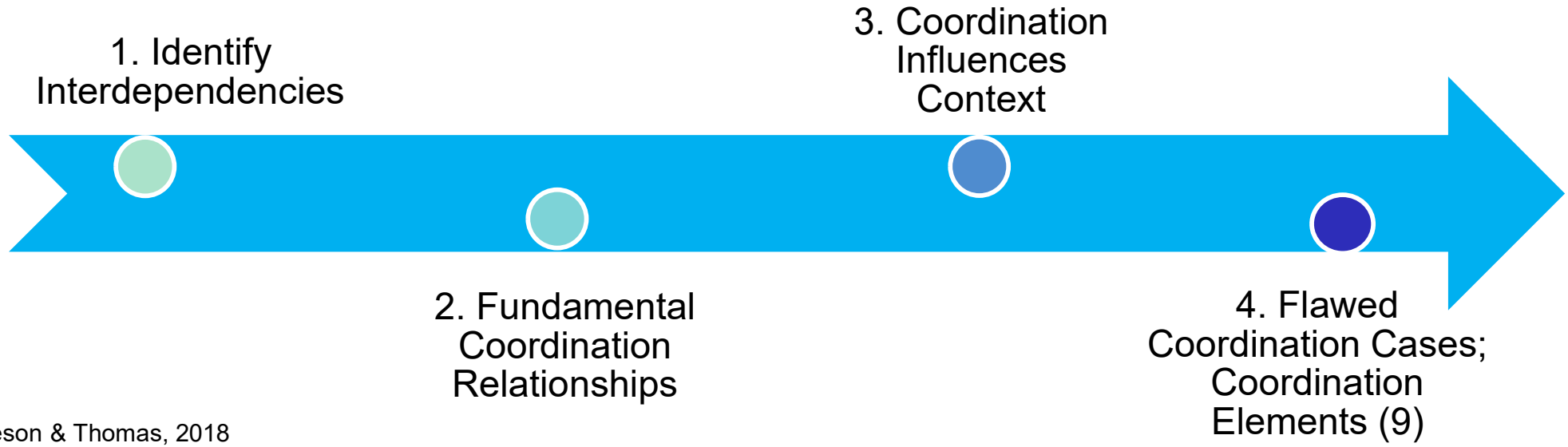
- Introducing, STPA extended for Coordination

STPA-Coordination

STPA



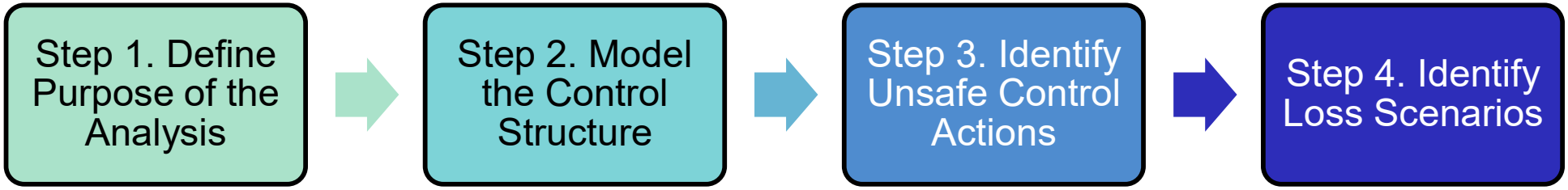
STPA-Coordination



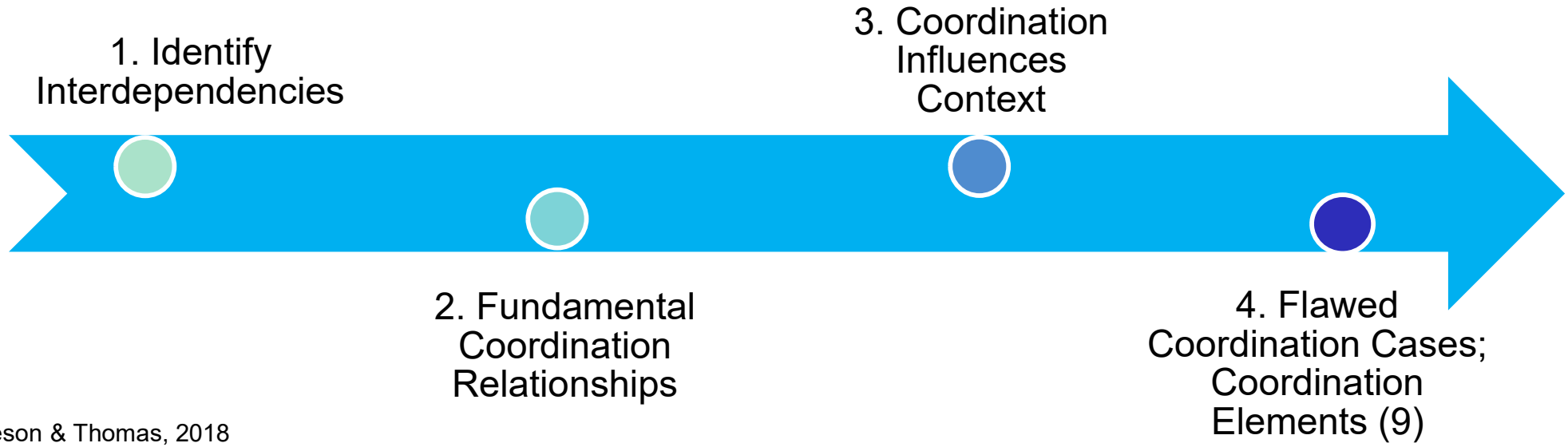
Leveson & Thomas, 2018
Johnson, 2017

STPA-Coordination

STPA



STPA-Coordination



Leveson & Thomas, 2018
Johnson, 2017

STPA-Coordination

1. Identify interdependencies

- Shared Goals: No losses
- Shared Resource: Airspace for UAS integration

2. Identify fundamental coordination relationships

y(t): output or outcome as a function of time
u(t): control signal as a function of time
UCA: unsafe control action
n: additional

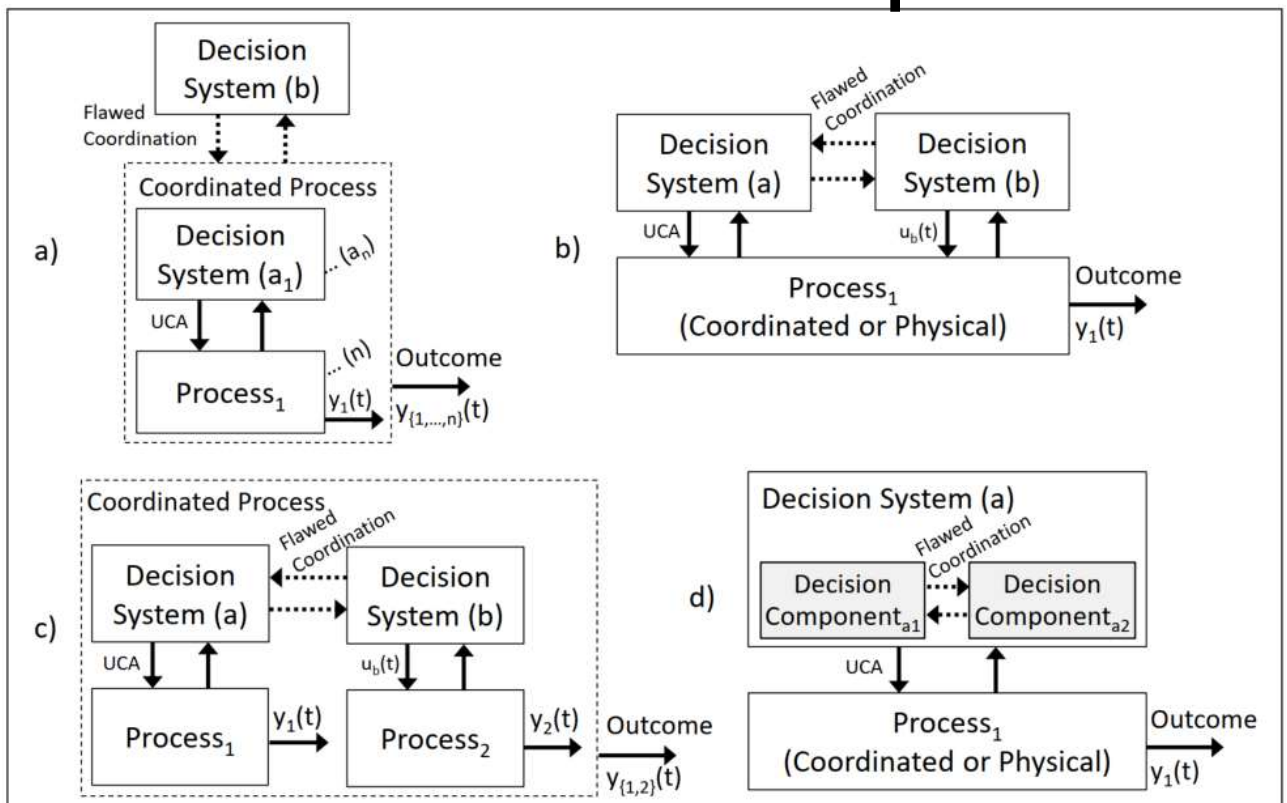


Figure 16. Causal Analysis Diagrams for Coordination

Johnson, 2017

2. Identify fundamental coordination relationships

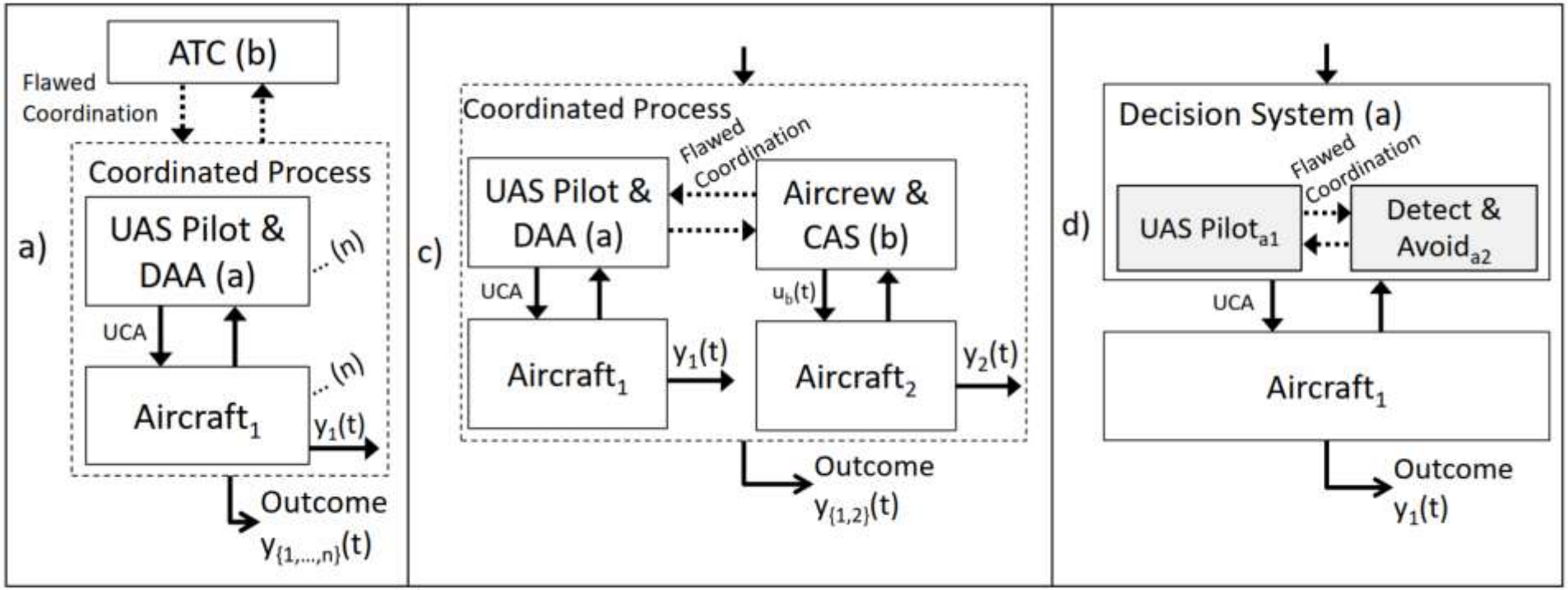


Figure 25. Coordination Relationships for Collision Avoidance

STPA-Coordination

3. UCAs where coordination influences the unsafe context

STPA Step 3. ID Unsafe Control Actions
a. Control action is not provided
b. Control action provided
c. Control action too early, too late, or in the wrong order
d. Control action too long or stopped too soon

<source> <type> <control action> <context> <link hazards>

- UAS Provides (too much) Separation Maneuver when separation violation imminent [structural hazards]
- Autonomous Wingman Does Not Provide Launch Missile when needed to defend themselves, their team, or other assets [flight, mission hazards]

Leveson & Thomas, 2018
Johnson, 2017

STPA-Coordination

4. Examine flawed coordination cases

4. Identify Hazardous Coordination Scenarios
Case 1. Coordination missing
Case 2. Coordination inadequate
Case 3. Coordination strategy leads to UCAs
Case 4. Coordination strategy established late

Leads to

STPA Step 4. Identify Loss Scenarios

a. Why Unsafe Control Actions occurred?
b. Why control not executed or improperly executed, leads to hazards?
-- Coordination strategy correct

Leveson & Thomas, 2018
Johnson, 2017

STPA-Coordination

4. Examine flawed coordination cases

Flawed Coordination Causal Analysis Matrix		1. coord missing	2. coord flawed	3. strategy hazardous	4. strategy late
Coordination Elements: Missing or Flawed	1. Coordination Goals	•	•		•
	2. Coordination Strategy	•	•	•	•
	3. Decision Systems		•		•
	4. Communications		•		•
	5. Group Decision-Making	•	•		•
	6. Observation of Common Objects		•		•
	7. Authority, Responsibility, Accountability		•		•
	8. Common Understanding		•		•
	9. Predictability		•		•

Johnson, 2017

Discussion

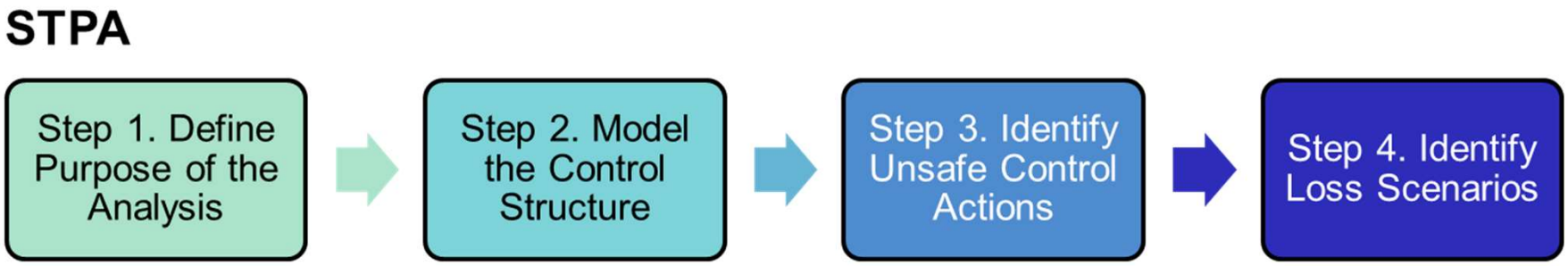
- **Flawed Coord Cases**
  - Case 1. no strategy
    - Not likely in well established scenarios, highly planned
    - UCAs with dynamic/novel context, where a strategy may not exist yet. (e.g. mission ops)
  - Case 4, strategy late
    - Similar concerns as case 1
  - Must lead to identified UCAs in STPA step 3
- **Vertical Coordination**
  - See relationship A.
  - Analyze how coordination may cause UCAs of lower decision system,
  - Or, how coordination from upper to lower decision system was flawed (i.e. control improperly executed)

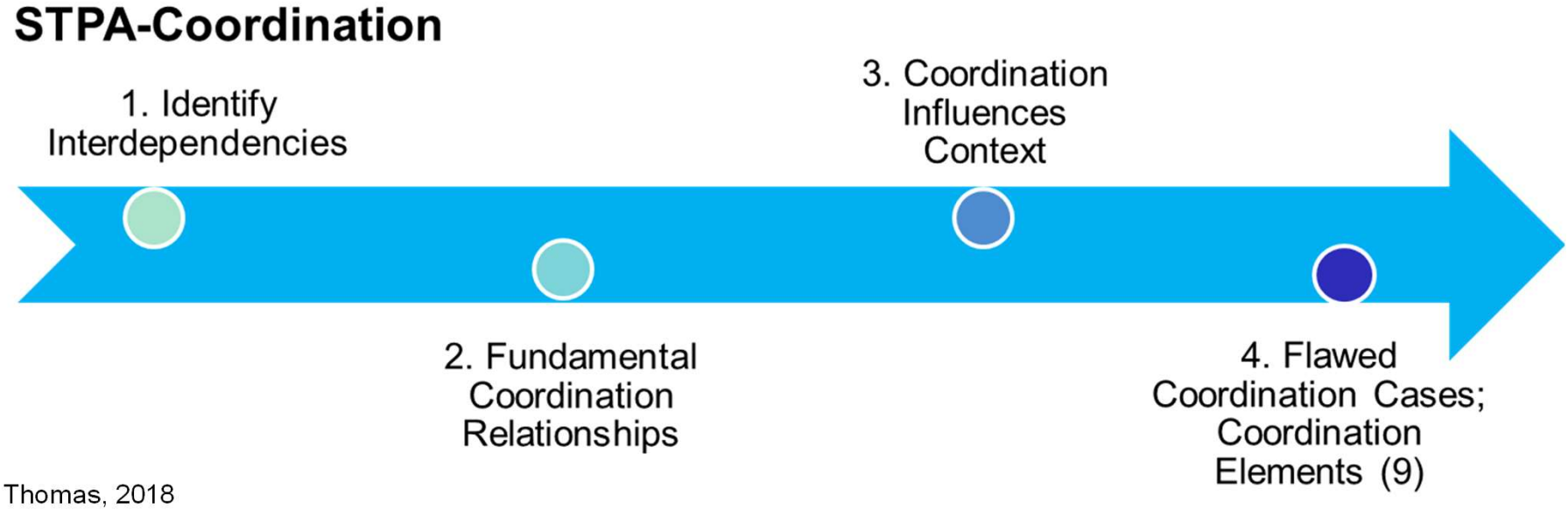
STPA / CAST-Coordination

- **Recommended Examples:**
  - **STPA-Coordination:**
    - **UAS Integration**; Kip Johnson. *Systems-Theoretic Safety Analyses Extended for Coordination* (PhD Dissertation), MIT, 2017. Ch 5.
    - Pennington, Elizabeth. A Model-Based and System Theoretic Approach to Design Advanced Autonomy for Air Dominance Missions: A **Loyal Wingman** Case Study. AFIT MS Thesis, Mar 2024
  - **CAST-Coordination**:
    - **Patriot Friendly Fire**; Kip Johnson. *Systems-Theoretic Safety Analyses Extended for Coordination* (PhD Dissertation), MIT, 2017. Ch 6.
    - "Light Water **Reactor Sustainability** Program. Optimizing **Information Automation** Using a New Method Based on System-Theoretic Process Analysis," US DOE/Office of Nuclear Energy, Jun 2023

STPA-Coordination

- **In-class exercise**





Leveson & Thomas, 2018
Johnson, 2017

Questions?

- **References**

  - Nancy Leveson & John Thomas. *STPA HANDBOOK,* 2018.
  - Kip Johnson. *Systems-Theoretic Safety Analyses Extended for Coordination* (PhD Dissertation), MIT, 2017.