29th Annual INCOSE international symposium

Orlando, FL, USA
July 20 - 25, 2019

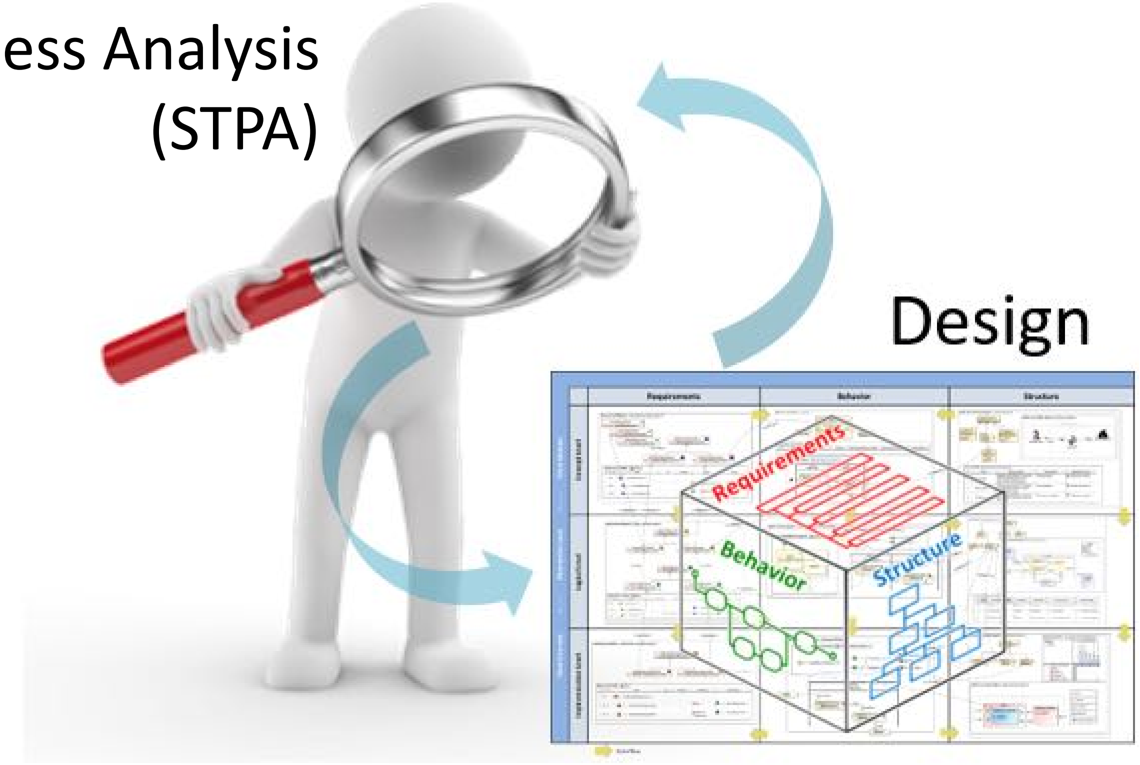
Presenter: Rashmi Hegde

Authors: Rashmi Hegde, Sarra Yako, Kyle Post, Sandro Nuesch

System-Theoretic Process Analysis (STPA) for Layers of System Safety

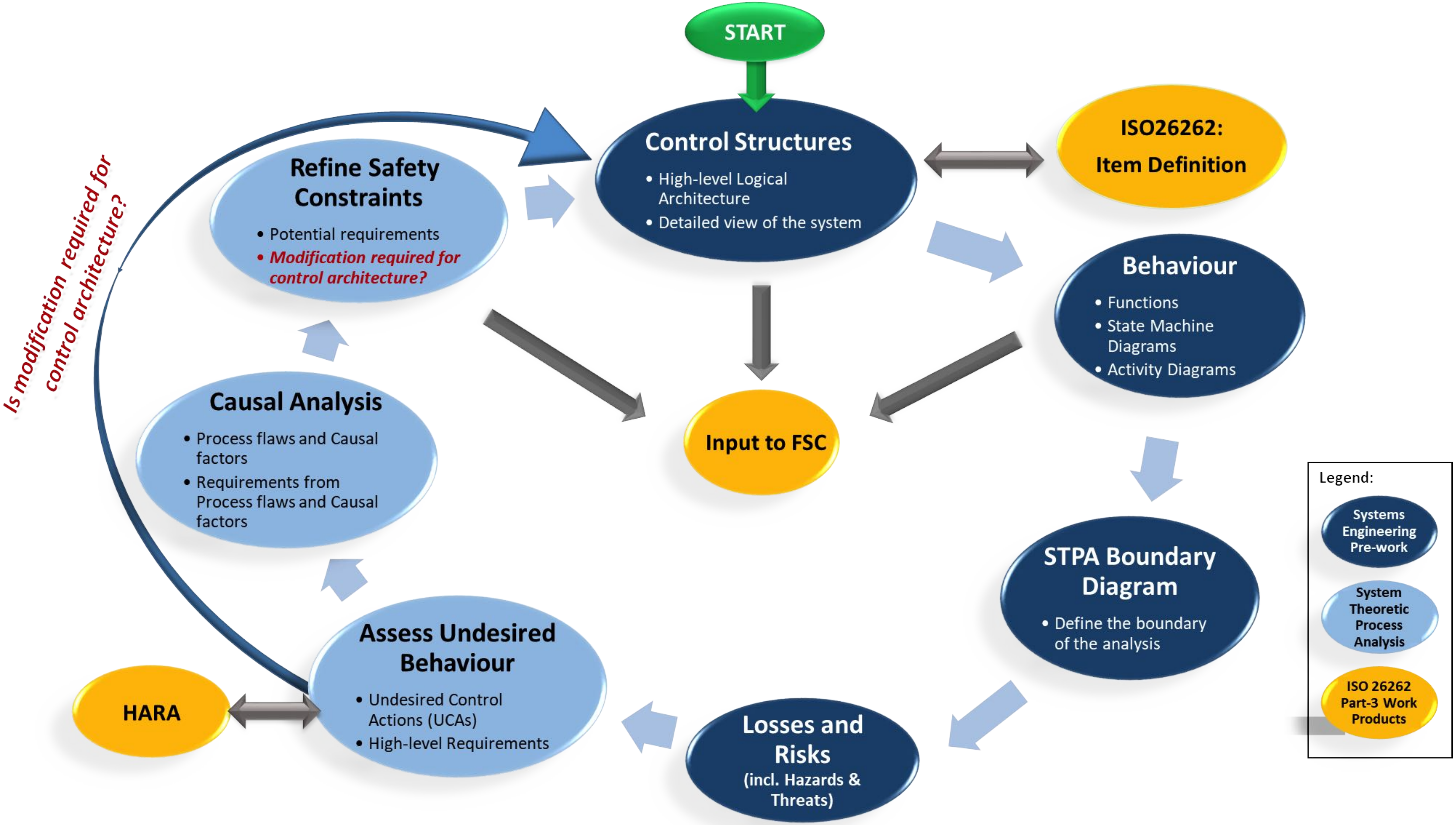
Introduction to STPA

System-Theoretic Process Analysis (STPA)



Adapted from diagram by Matt Meinhart, MBSE Reference Guide

STPA Process Overview



START

Control Structures
- High-level Logical Architecture
- Detailed view of the system

ISO26262: Item Definition

Behaviour
- Functions
- State Machine Diagrams
- Activity Diagrams

STPA Boundary Diagram
- Define the boundary of the analysis

Losses and Risks
(incl. Hazards & Threats)

Assess Undesired Behaviour
- Undesired Control Actions (UCAs)
- High-level Requirements

HARA

Causal Analysis
- Process flaws and Causal factors
- Requirements from Process flaws and Causal factors

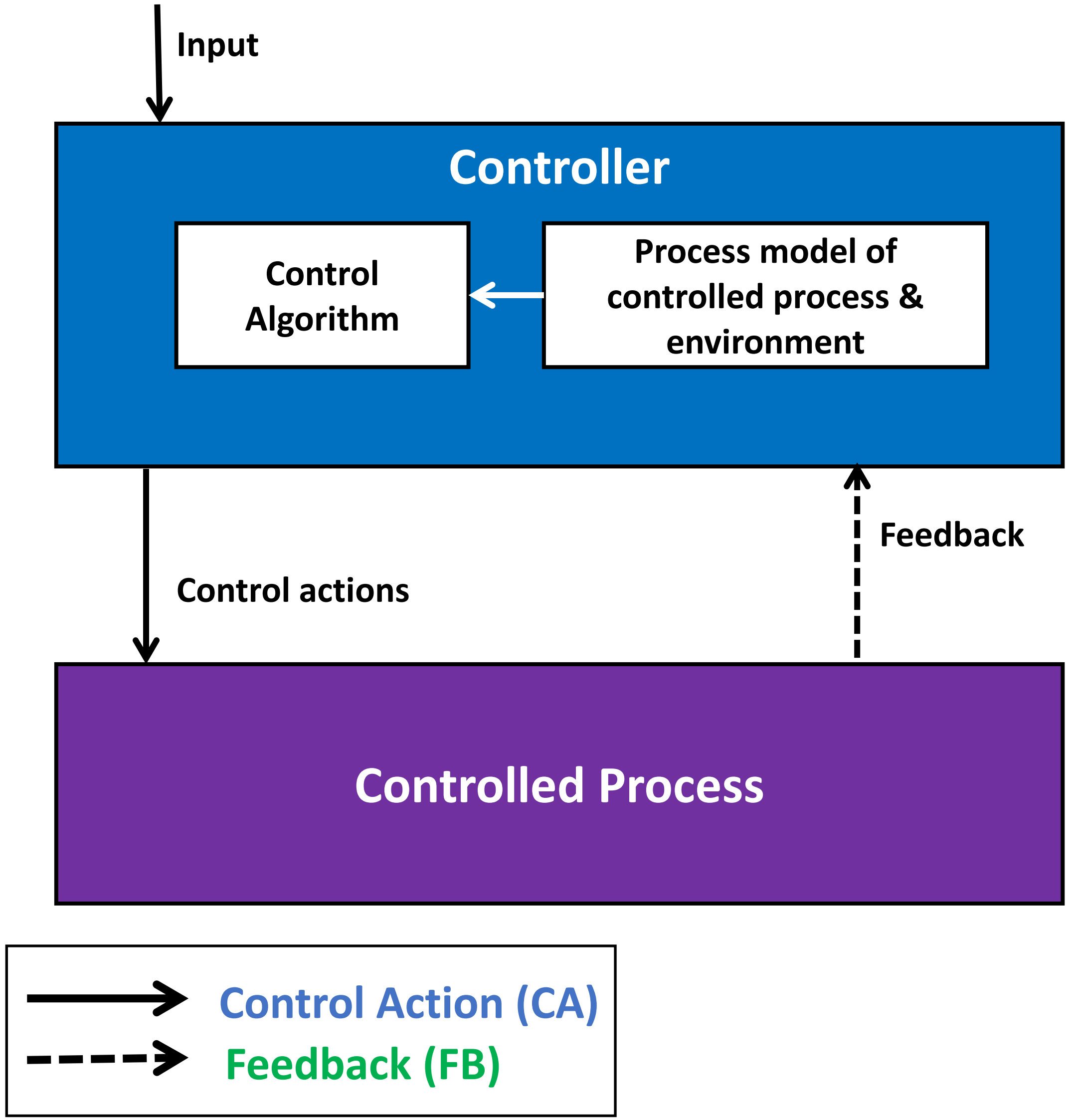
Refine Safety Constraints
- Potential requirements
- *Modification required for control architecture?*

Is modification required for control architecture?

Input to FSC

Legend:
- Systems Engineering Pre-work
- System Theoretic Process Analysis
- ISO 26262 Part-3 Work Products

Hierarchical Control Structure



Input

Controller

Control Algorithm

Process model of controlled process & environment

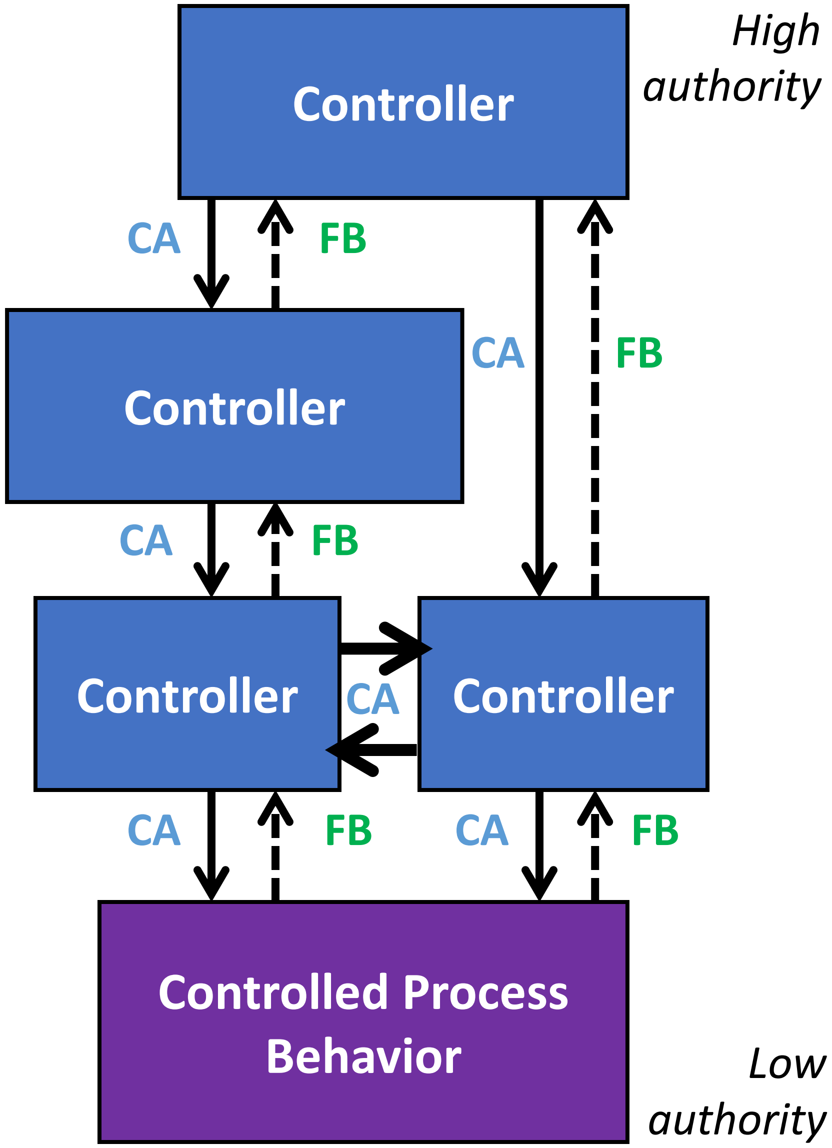
Control actions

Feedback

Controlled Process

Control Action (CA)

Feedback (FB)



High authority

Controller

CA FB

Controller

CA FB

CA FB

Controller

CA

Controller

CA FB

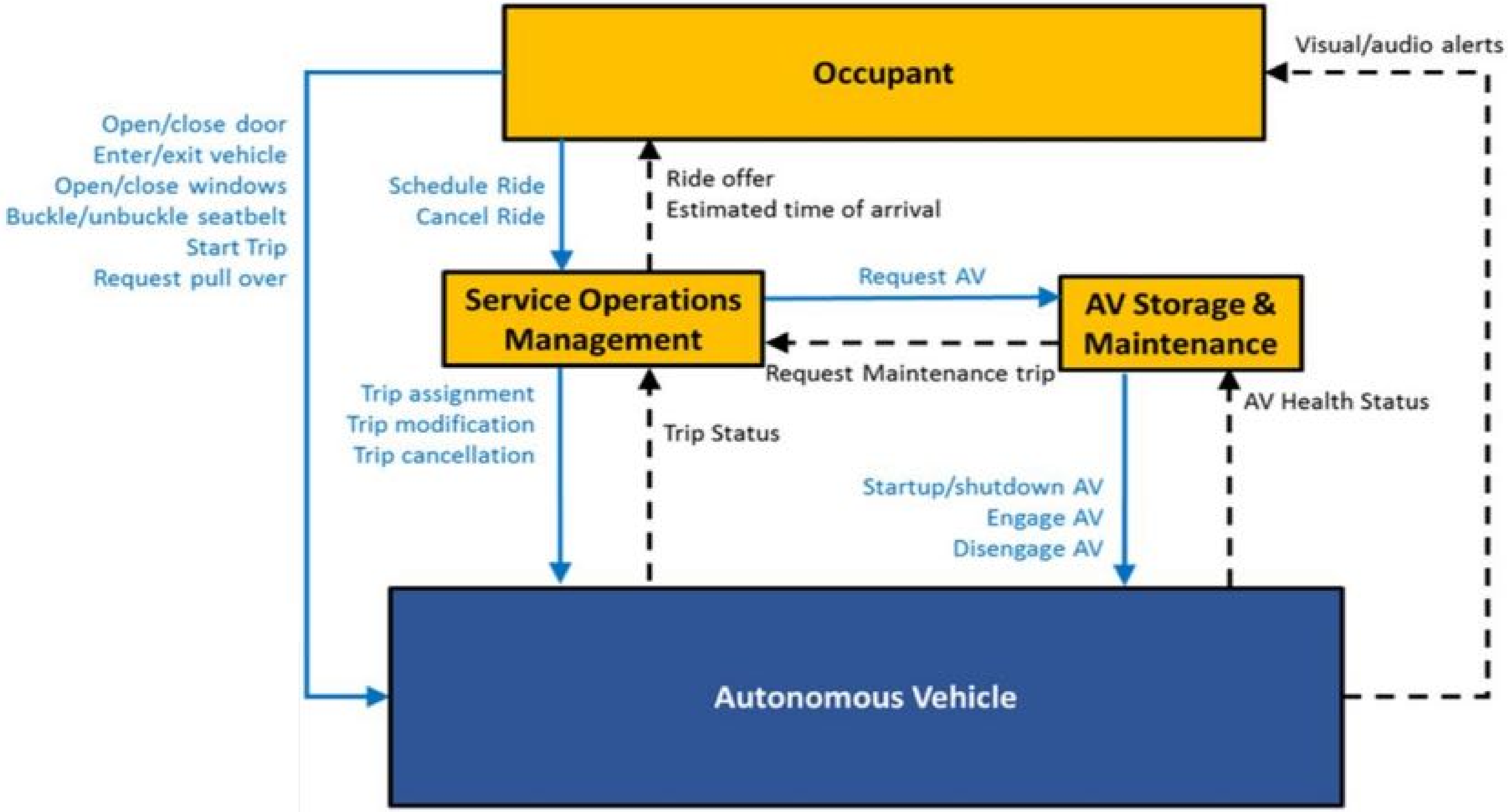
CA FB

Controlled Process Behavior

Low authority

Hierarchical Control Structure – Example

🟨 Controller
🟦 Controlled Process
→ Control Action
- - → Feedback



Occupant

Service Operations Management

AV Storage & Maintenance

Autonomous Vehicle

Open/close door
Enter/exit vehicle
Open/close windows
Buckle/unbuckle seatbelt
Start Trip
Request pull over

Schedule Ride
Cancel Ride

Ride offer
Estimated time of arrival

Visual/audio alerts

Request AV

Request Maintenance trip

Trip assignment
Trip modification
Trip cancellation

Trip Status

Startup/shutdown AV
Engage AV
Disengage AV

AV Health Status

Losses, Risks and Hazards

Loss – is anything unacceptable that should be prevented. Some factors such as environmental conditions may contribute to a loss but are outside our control.

- Loss or injury to human life
- Economic Loss
- Loss of Customer Satisfaction
- Legal Loss

Risk – is a system state or set of conditions that together with a particular set of worst-case environment conditions may lead to a loss

- Vehicle Impedes Traffic
- Inappropriate Fuel or Energy Consumption

Hazard – a system state or set of conditions that together with a particular set of worst-case environment conditions, may lead to a safety-related Loss.

- Vehicle does not maintain separation distance to objects
- Passenger unable to exit the vehicle

Losses, Risks and Hazards – Example

STPA Losses
L-1: Safety Loss
L-2: Operational Loss
L-3: Financial Loss
L-4: Loss of Corporate Reputation, Loss of customer satisfaction

STPA Hazards & Risks	Mapped to Loss
H-1: Vehicle does not maintain separation distance to objects	L-1, L-3, L-4
H-2: Vehicle enters area	L-1, L-3, L-4
Risk-1: Inappropriate passenger pick-up	L-2, L-4
Risk-2: Vehicle availability is impaired	L-2, L-3

Undesired Control Actions (UCAs)

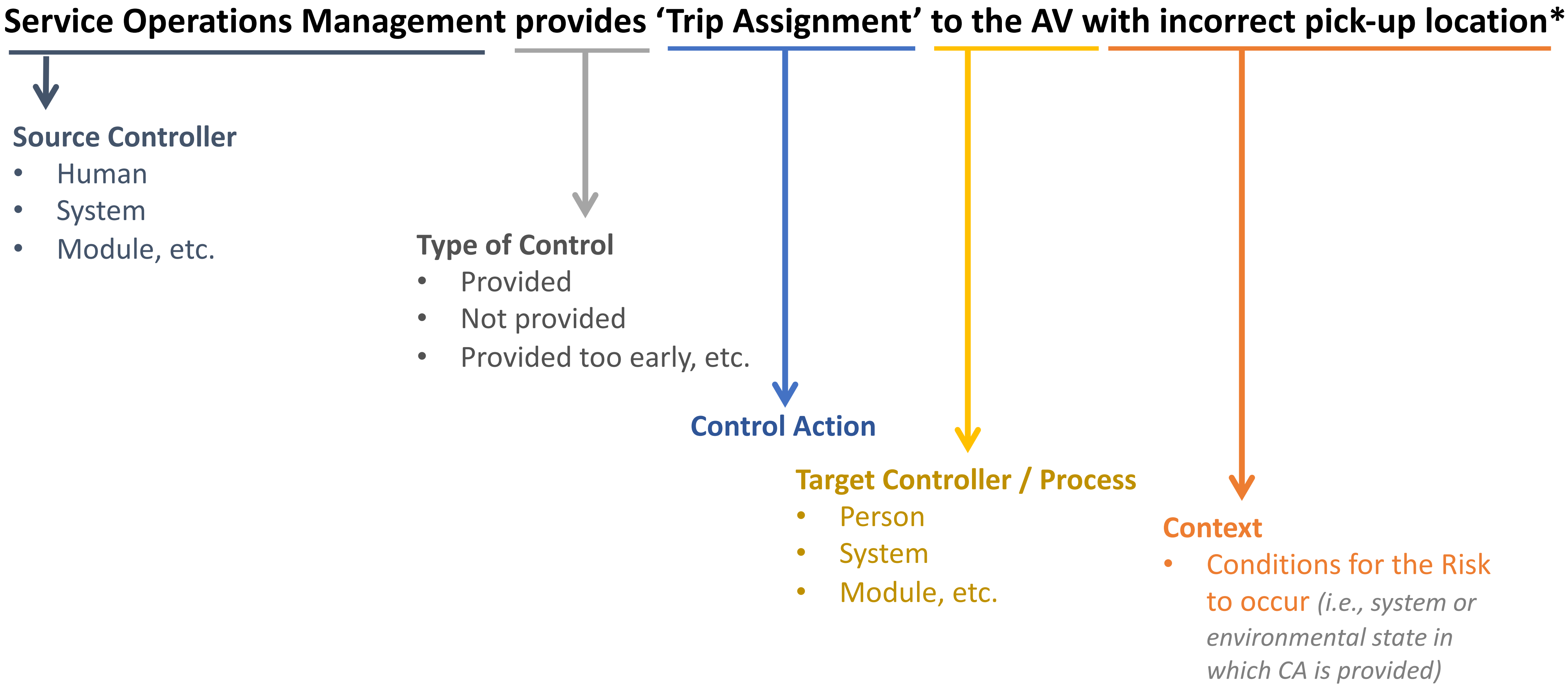
- Unanticipated behavior in the Controller may lead to **Undesired Control Action (UCA)**
- **Definition:** Undesired Control Action is a control action that, in a particular context and worst-case environment, will lead to a hazard

- Systematically identify UCAs for each CA using 4 types:

Not provided causes Hazard	Provided causes Hazard	Provided too early / too late / out of order causes Hazard	Stopped too soon / provided too long causes Hazard
i.e. CA missing	i.e. CA provided in wrong context, incomplete or wrong magnitude	i.e. CA provided too late, too early, or in wrong sequence with other CAs / processes	only relevant for continuous CA

UCA Syntax

Five elements of a UCA:



Service Operations Management provides ‘Trip Assignment’ to the AV with incorrect pick-up location*

Source Controller
- Human
- System
- Module, etc.

Type of Control
- Provided
- Not provided
- Provided too early, etc.

Control Action

Target Controller / Process
- Person
- System
- Module, etc.

Context
- Conditions for the Risk to occur *(i.e., system or environmental state in which CA is provided)*

*This example is for academic purposes only

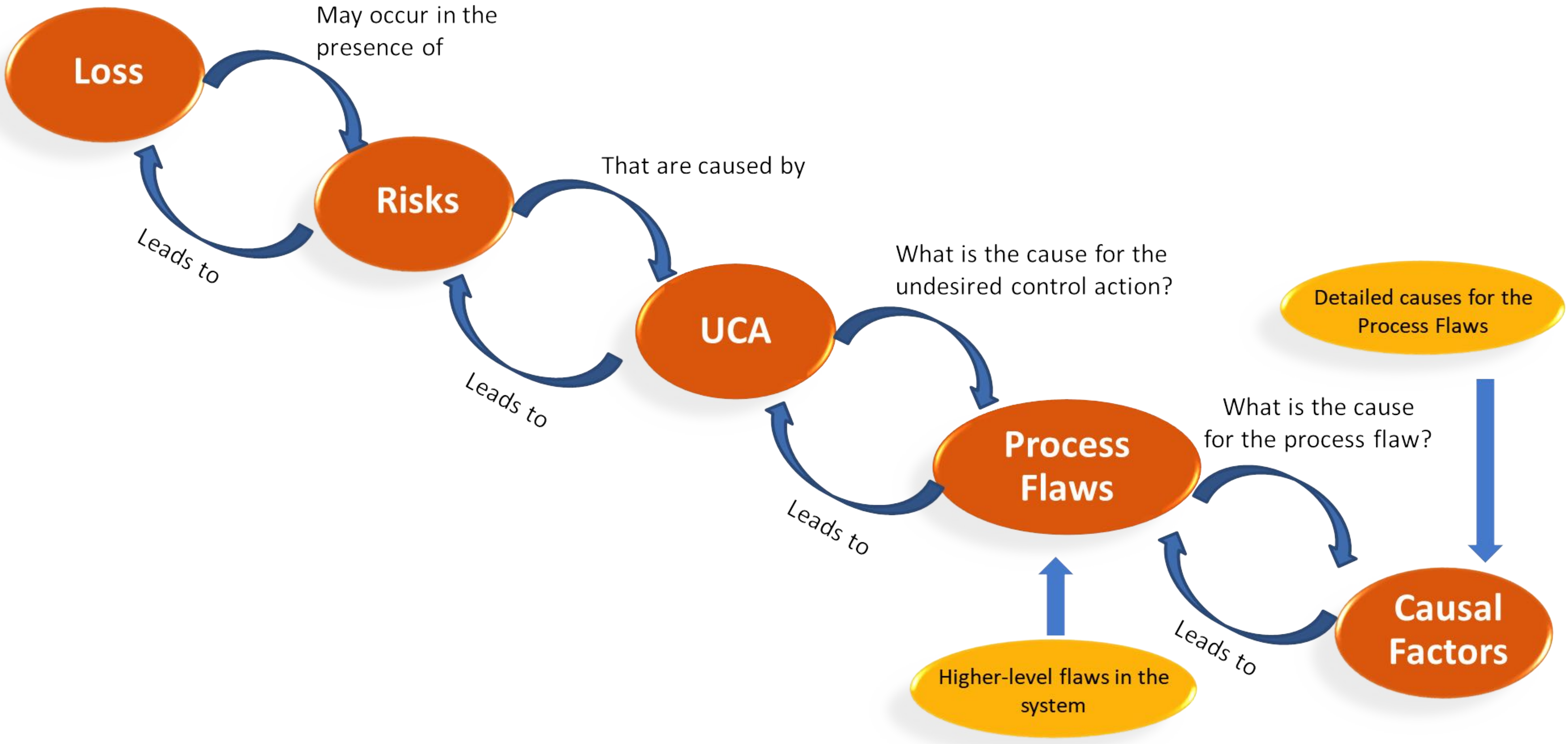
UCA Example

Hazards:
H-1: Vehicle does not maintain separation distance to objects
H-2: Degraded vehicle stability

Risks:
Risk-1: Inappropriate passenger pick-up
Risk-2: Vehicle availability is impaired

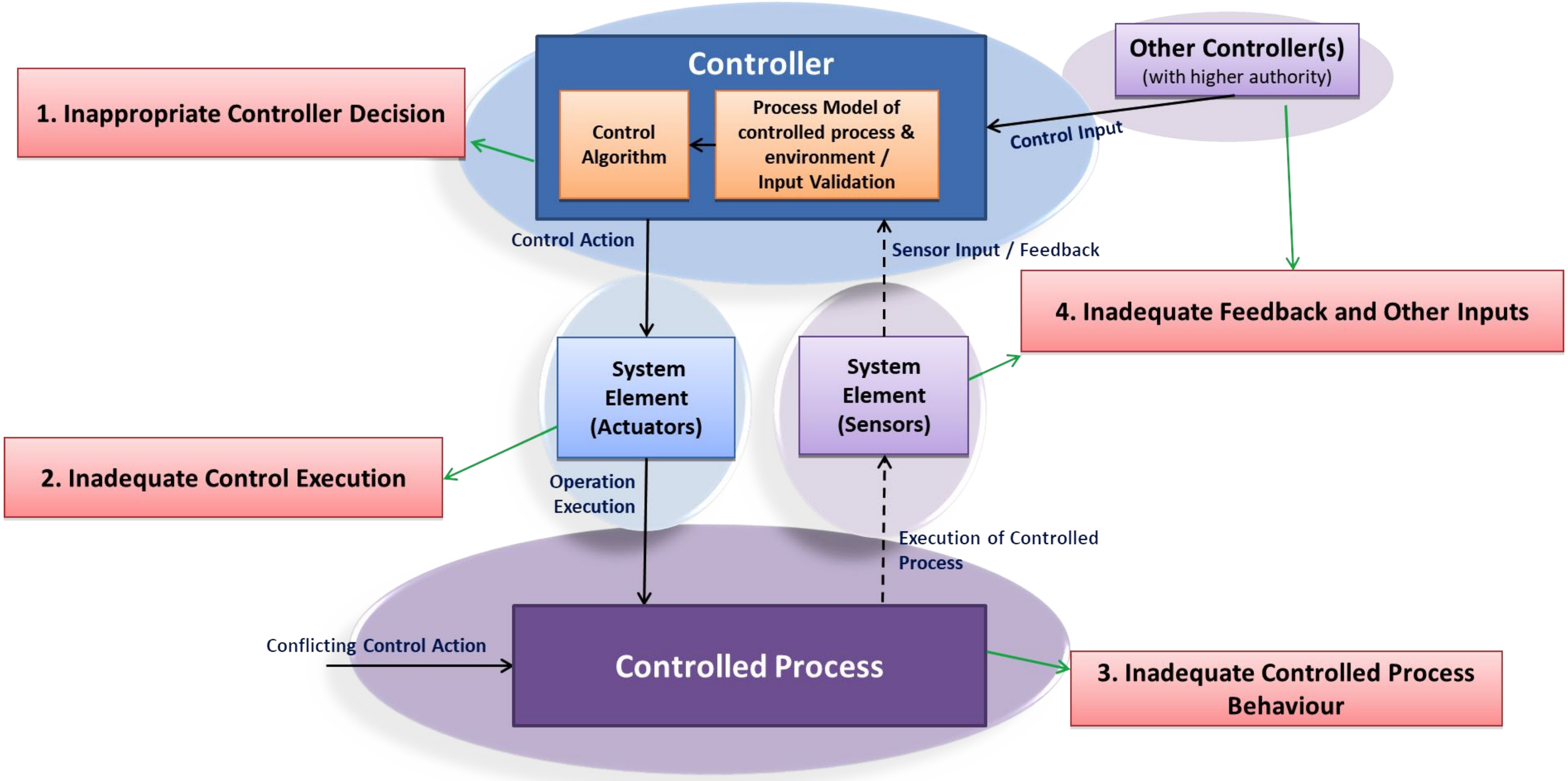
Controller	UCA #	Control Action	UCA Statement	Hazard/Risk
Service Operations Management	UCA-1	Trip Assignment	Service Operations Management provides “Trip Assignment” to AV with incorrect pick-up location	Risk-1
	UCA-2	Trip Assignment	Service Operations Management provides “trip assignment” to AV with hazardous pickup location, route, or destination	H-1

STPA Causal Analysis – Process Flaws & Causal Factors



Loss
May occur in the presence of
Risks
Leads to
That are caused by
UCA
Leads to
What is the cause for the undesired control action?
Process Flaws
Leads to
What is the cause for the process flaw?
Detailed causes for the Process Flaws
Causal Factors
Leads to
Higher-level flaws in the system

STPA Process Flaws


1. Inappropriate Controller Decision
Controller
Control Algorithm
Process Model of controlled process & environment / Input Validation
Other Controller(s)
(with higher authority)
Control Input
Control Action
Sensor Input / Feedback
4. Inadequate Feedback and Other Inputs
System Element (Actuators)
System Element (Sensors)
2. Inadequate Control Execution
Operation Execution
Execution of Controlled Process
Conflicting Control Action
Controlled Process
3. Inadequate Controlled Process Behaviour

Causal Analysis: Type-1 Flaws

UCA-1: Service Operations Management provides “Trip Assignment” to AV with incorrect pick-up location

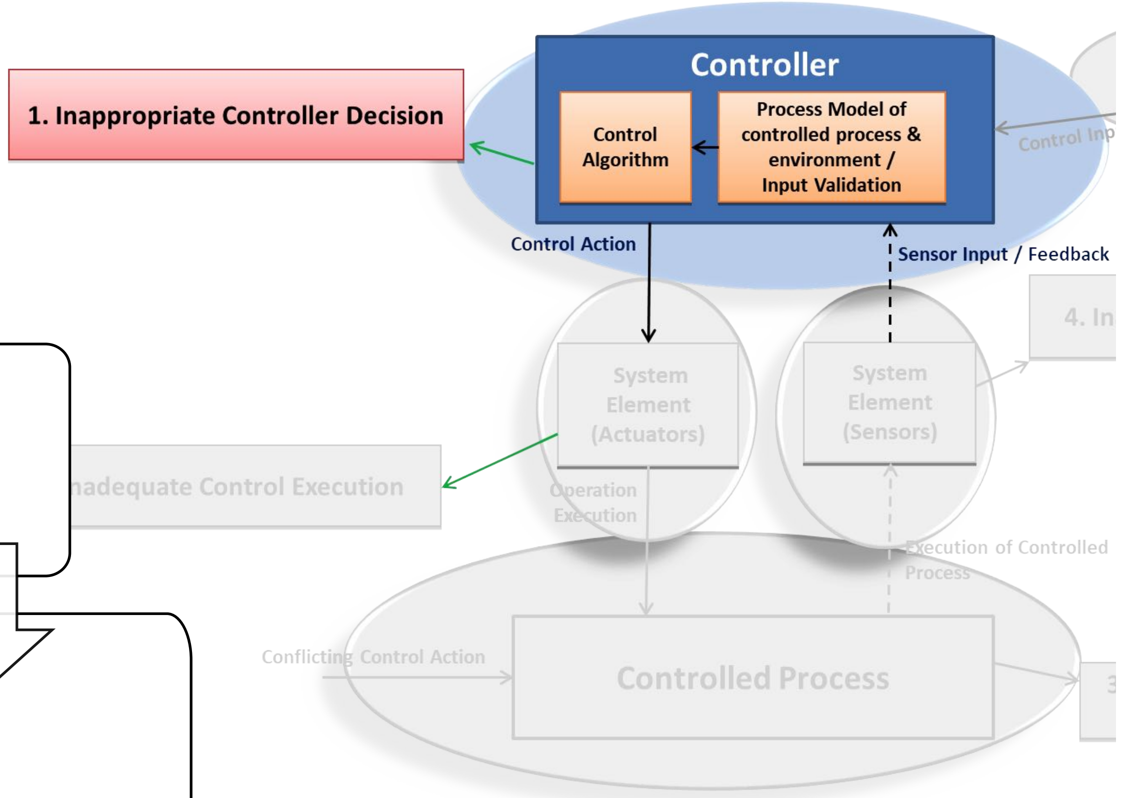
Process Flaws:

PF-1-1: Service Operations Management believes that it is providing the correct pick-up location

Causal Factors:

CF-1-1-1: Service Operations Management receives a high-volume of request simultaneously and is unable to handle it adequately.

CF-1-1-2: Requestor updates the pick-up location, but their service operations management believes the update is invalid and ignores the request.



1. Inappropriate Controller Decision
Controller
Control Algorithm
Process Model of controlled process & environment / Input Validation
Control Inp
Control Action
Sensor Input / Feedback
4. In
System Element (Actuators)
System Element (Sensors)
nadequate Control Execution
Operation Execution
Execution of Controlled Process
Conflicting Control Action
Controlled Process
3

Causal Analysis: Type-2 Flaws

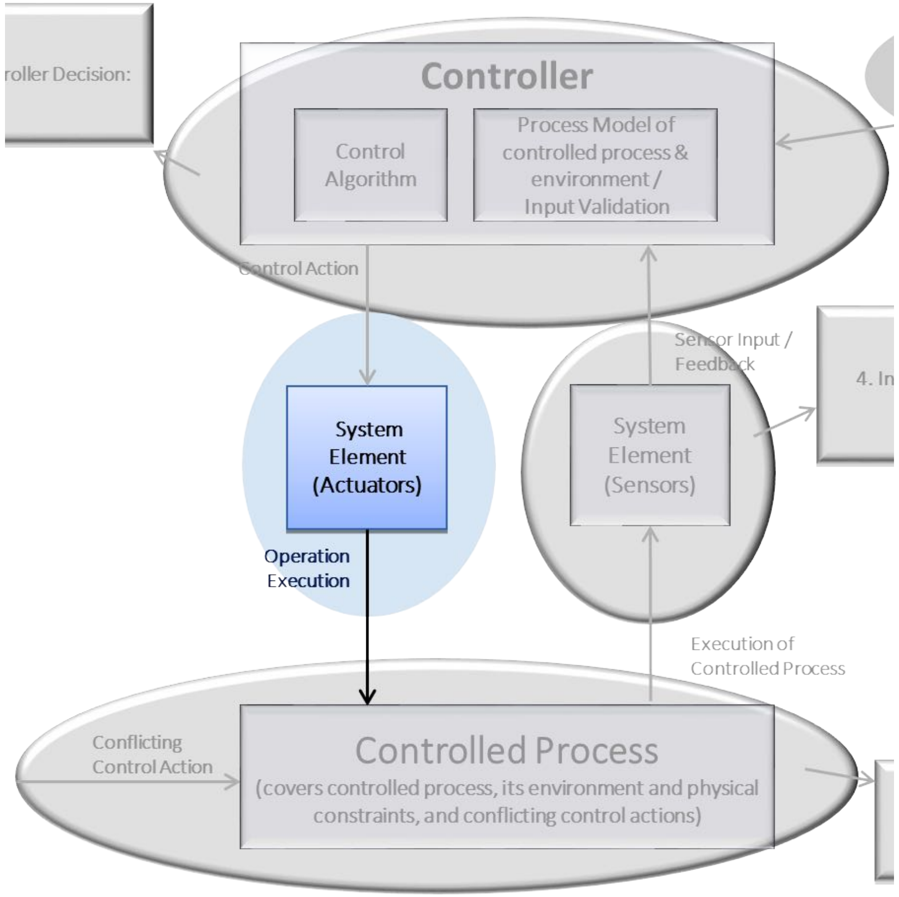
UCA-1: Service Operations Management provides "Trip Assignment" to AV with incorrect pick-up location

Process Flaws:

PF-1-2: Service Operations Management provides "Trip Assignment" with the correct pick-up location, but the AV receives an invalid location

Causal Factor:

CF-1-2-1: The "Trip Assignment" signal is spoofed during transmission from Service Operations Management to AV, leading to an invalid pick-up location



roller Decision:
Controller
Control Algorithm
Process Model of controlled process & environment / Input Validation
Control Action
Sensor Input / Feedback
4. In
System Element (Actuators)
System Element (Sensors)
Operation Execution
Execution of Controlled Process
Conflicting Control Action
Controlled Process
(covers controlled process, its environment and physical constraints, and conflicting control actions)

Causal Analysis: Type-3 Flaws

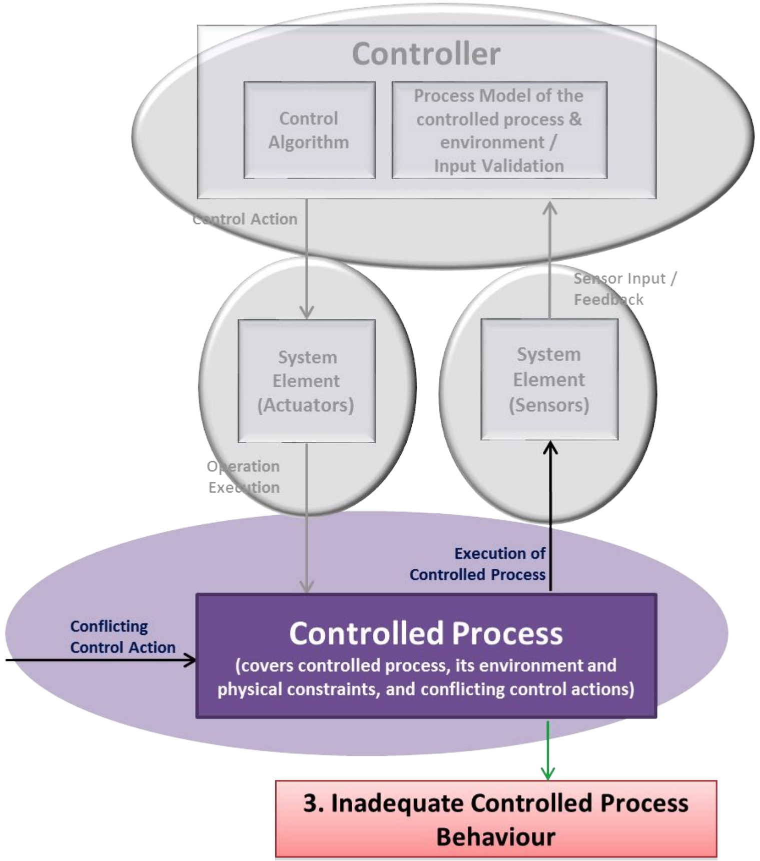
UCA-1: Service Operations Management provides “Trip Assignment” to AV with incorrect pick-up location

Process Flaws:

PF-1-3: Service Operations Management provides “Trip Assignment” with the correct pick-up location and the AV receives proper signal, but the AV fails to reach the pick-up location because the roadway is blocked

Causal Factor:

CF-1-3-1: The AV does not comprehend the situation, and therefore does not send any requests for rerouting to the Service Operations Management. The controller, Service Operations Management, case does not receive any feedback of an issue or failure to re-coordinate a new route or response for the AV.


Controller
Control Algorithm
Process Model of the controlled process & environment / Input Validation
Control Action
Sensor Input / Feedback
System Element (Actuators)
System Element (Sensors)
Operation Execution
Execution of Controlled Process
Conflicting Control Action
Controlled Process
(covers controlled process, its environment and physical constraints, and conflicting control actions)
3. Inadequate Controlled Process Behaviour

Causal Analysis: Type-4 Flaws

UCA-1: Service Operations Management provides “Trip Assignment” to AV with incorrect pick-up location

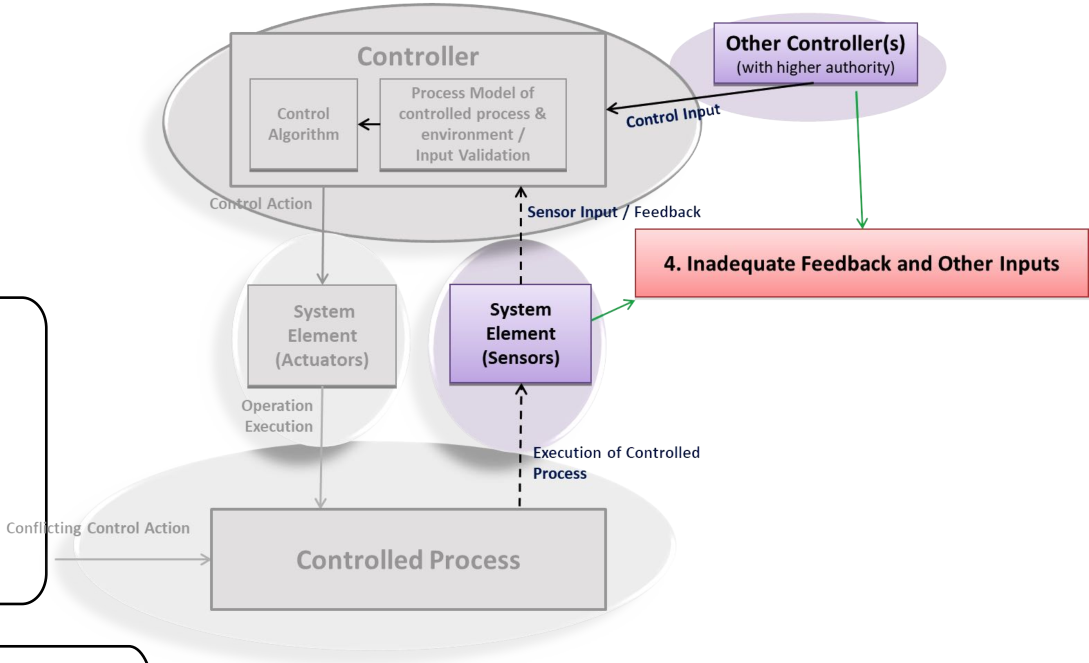
Process Flaws:

PF-1-4: Service Operations Management provides “Trip Assignment” with incorrect pick-up location because it receives a ride schedule request with an invalid location

Causal Factor:

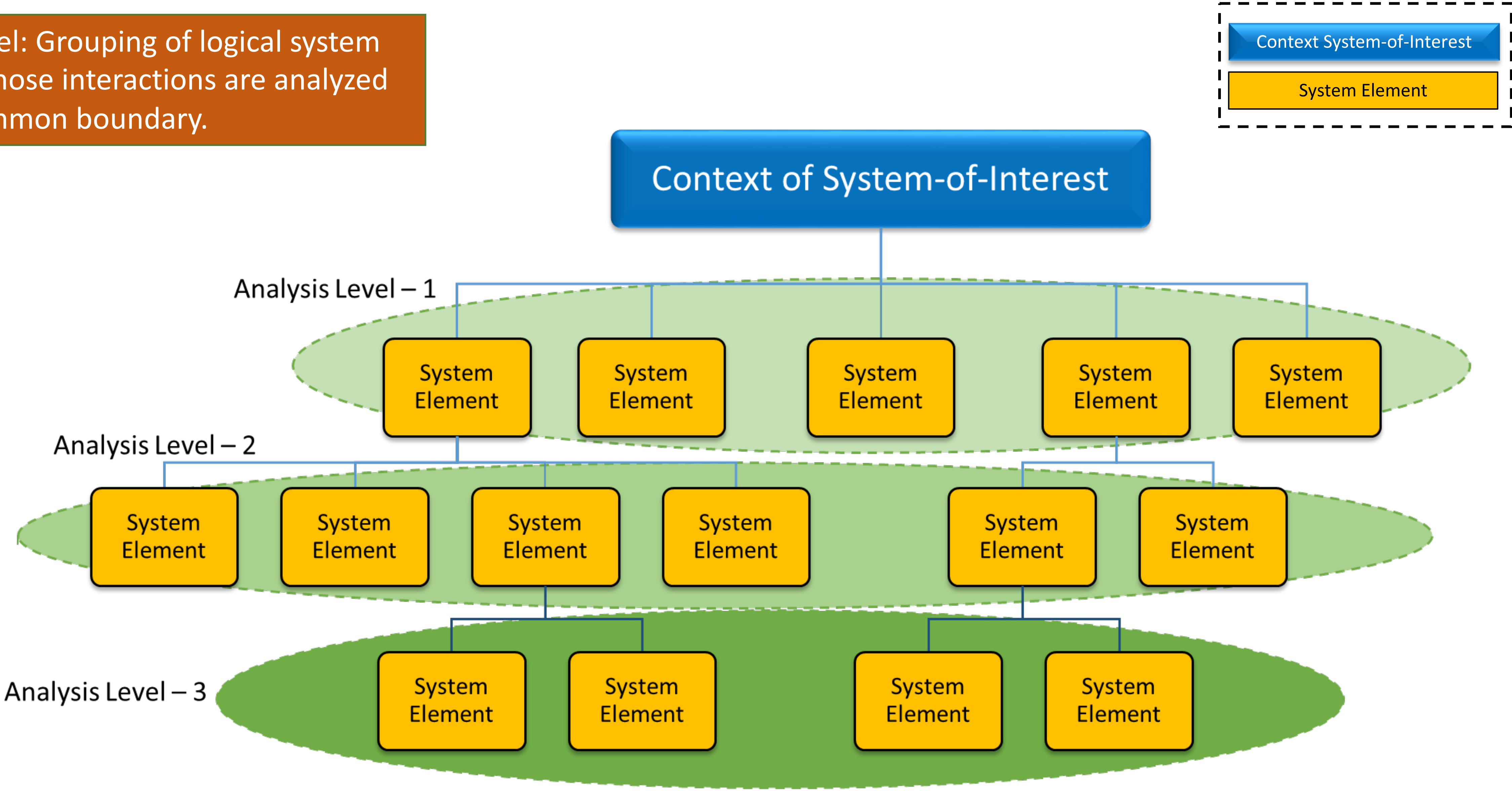
CF-1-4-1: The requestor accidently inputs an invalid pick-up location but does not realize the fallacy and proceeds to wait for the ride

CF-1-4-2**:** The ride schedule information is spoofed/hacked during transmission, and the Service Operations Management fails to identify that the signal is spoofed


Controller
Control Algorithm
Process Model of controlled process & environment / Input Validation
Other Controller(s) (with higher authority)
Control Input
Control Action
Sensor Input / Feedback
4. Inadequate Feedback and Other Inputs
System Element (Actuators)
System Element (Sensors)
Operation Execution
Execution of Controlled Process
Conflicting Control Action
Controlled Process

Multi-level Analysis using STPA

Analysis Level: Grouping of logical system elements whose interactions are analyzed within a common boundary.



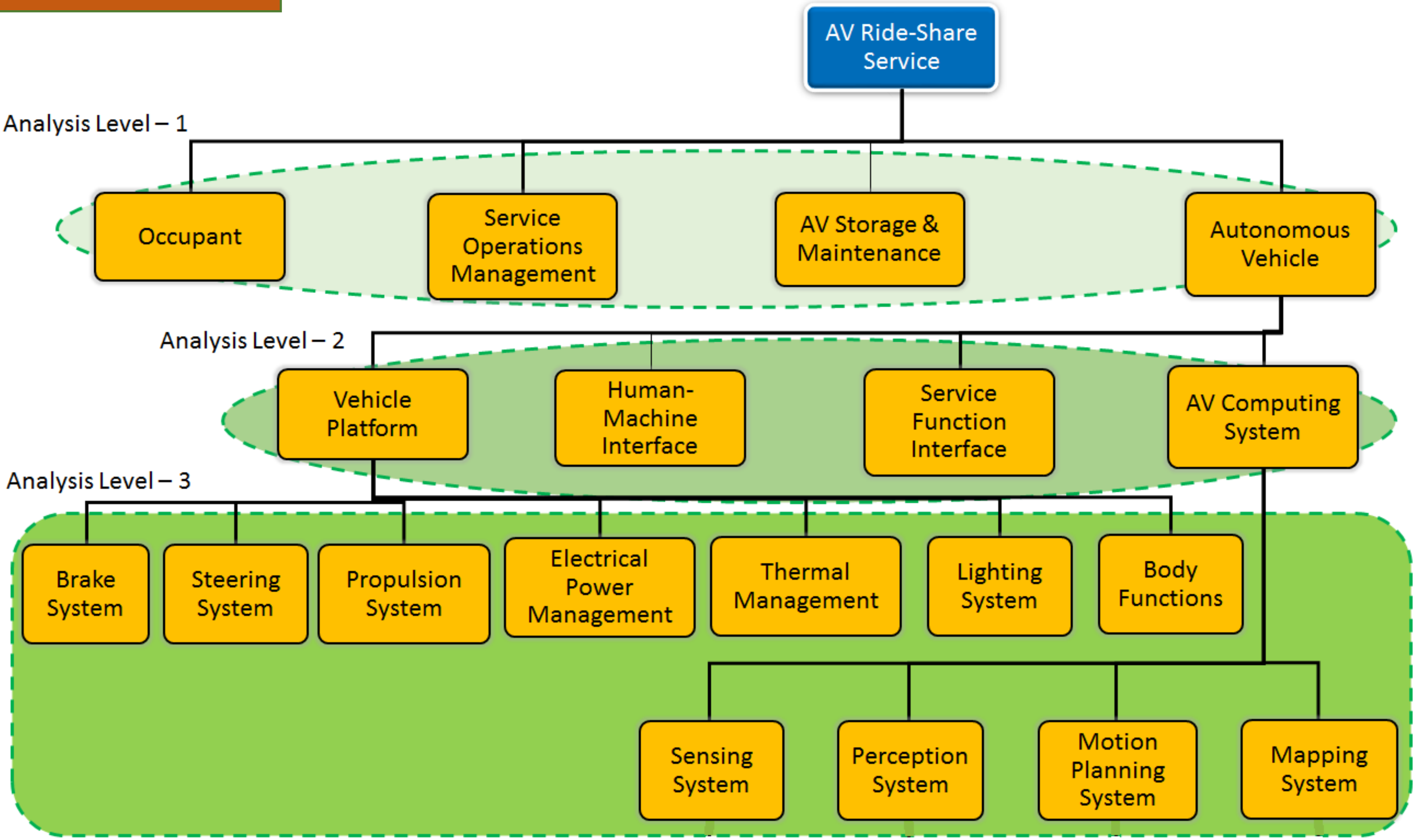
this figure is adapted from ISO/IEC/IEEE 15288:2015

Multi-level STPA – AV Ride-Sharing Service

Context System-of-Interest

System Element

Analysis Hierarchy Option – 1:

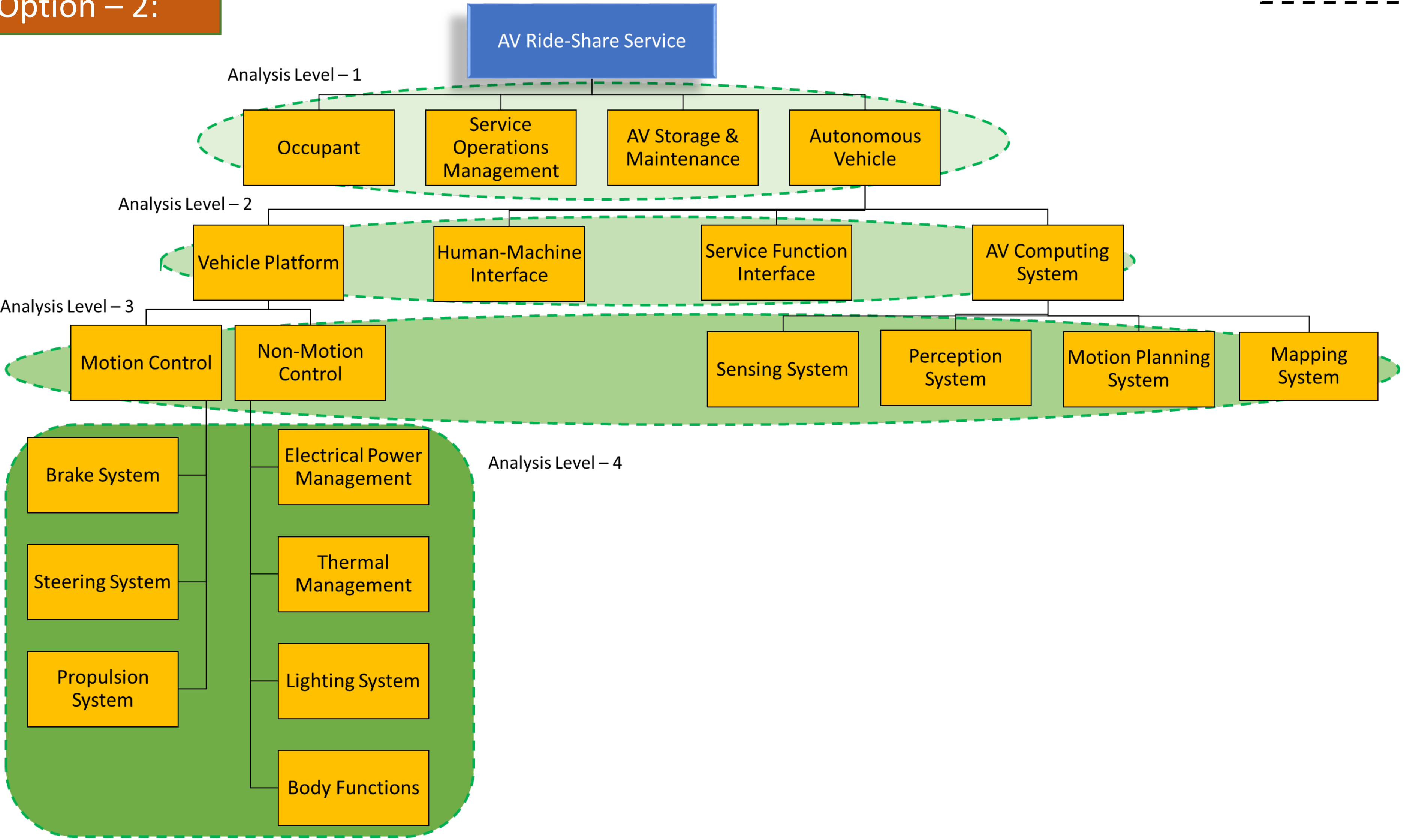


Multi-level STPA – AV Ride-Sharing Service

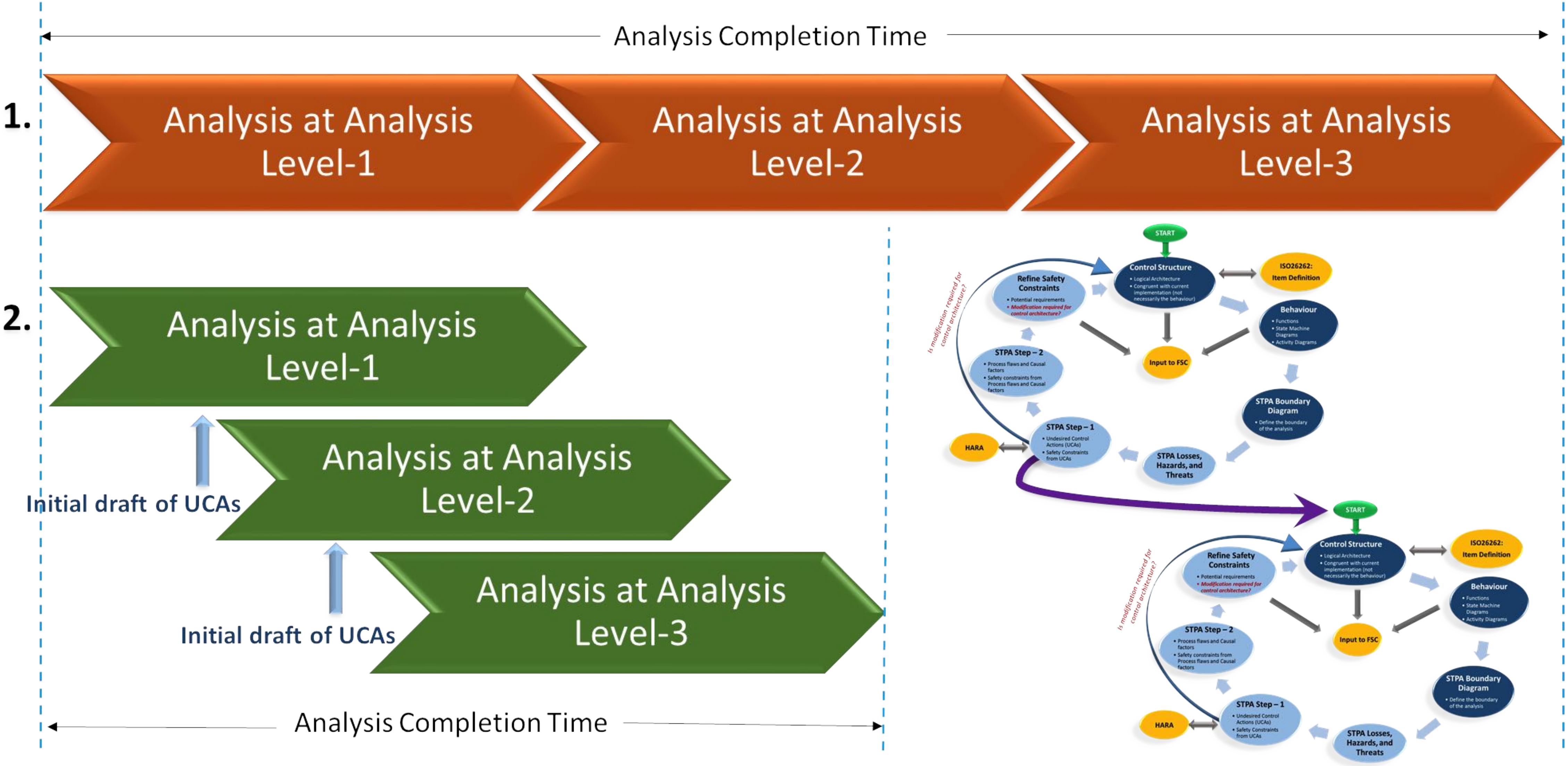
Context System-of-Interest

System Element

Analysis Hierarchy Option – 2:



Multi-level Hierarchy STPA Progression



Analysis Completion Time

1. Analysis at Analysis Level-1 → Analysis at Analysis Level-2 → Analysis at Analysis Level-3

2. Analysis at Analysis Level-1

Initial draft of UCAs

Analysis at Analysis Level-2

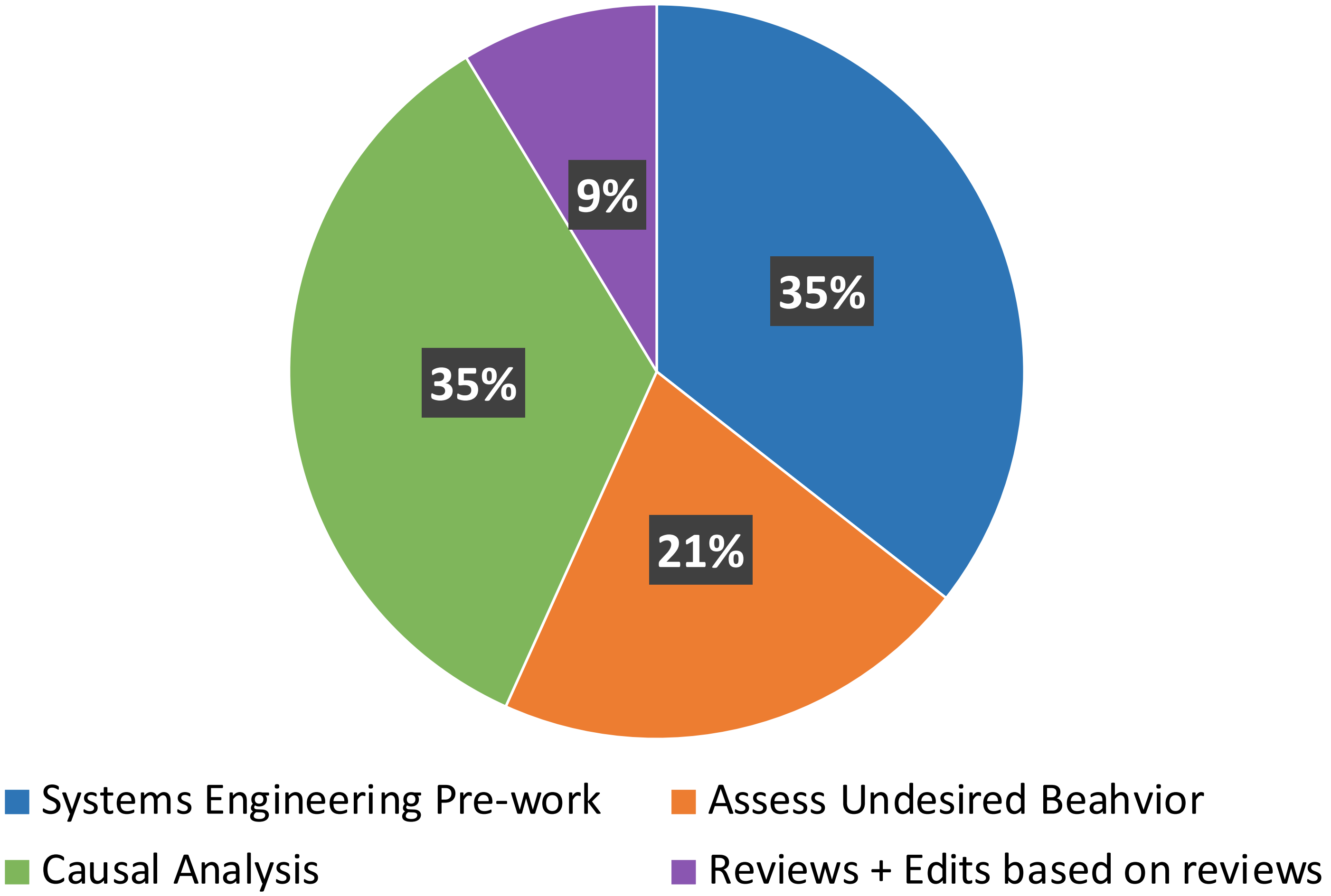
Initial draft of UCAs

Analysis at Analysis Level-3

Analysis Completion Time

START
Control Structure
• Logical Architecture
• Congruent with current implementation (not necessarily the behaviour)
ISO26262:
Item Definition
Behaviour
• Functions
• State Machine Diagrams
• Activity Diagrams
Input to FSC
STPA Boundary Diagram
• Define the boundary of the analysis
STPA Losses, Hazards, and Threats
STPA Step – 1
• Undesired Control Actions (UCAs)
• Safety Constraints from UCAs
HARA
STPA Step – 2
• Process flaws and Causal factors
• Safety constraints from Process flaws and Causal factors
Refine Safety Constraints
• Potential requirements
• Modification required for control architecture?
Is modification required for control architecture?
START
Control Structure
• Logical Architecture
• Congruent with current implementation (not necessarily the behaviour)
ISO26262:
Item Definition
Behaviour
• Functions
• State Machine Diagrams
• Activity Diagrams
Input to FSC
STPA Boundary Diagram
• Define the boundary of the analysis
STPA Losses, Hazards, and Threats
STPA Step – 1
• Undesired Control Actions (UCAs)
• Safety Constraints from UCAs
HARA
STPA Step – 2
• Process flaws and Causal factors
• Safety constraints from Process flaws and Causal factors
Refine Safety Constraints
• Potential requirements
• Modification required for control architecture?
Is modification required for control architecture?

Time Distribution for STPA Tasks based on AV Ride-Share Service STPA



Implementing STPA Successfully

- **Learning STPA**

Description	Effort	Effectiveness
Reading STPA Handbook	Medium	Medium
Reading existing books/reports/papers	High	Low
Participating in a STPA project	**Medium**	**High**
Attending a STPA training session	Low	Medium
STPA Webinar/Tutorial Videos	Low	Medium

- **Selecting the System of Interest**
  - Identify the level of detail needed/desired for the analysis
  - Identify the analysis goal(s) and areas of concern

- **Planning and Supporting STPA Project**
  - Clear R&Rs and objectives

Conclusion

- Systematic approach to apply STPA on complex systems
    - A degree of formalization helps implement STPA in fast-paced industry environment
- Ability to trace STPA causal factors to design requirements and subsequent analyses like DFMEAs, FTAs or PFMEAs

Potential Future Work:

- Enhance the methodology for complex systems by differentiating between structural aggregation and abstraction
- Explore integration of STPA in MBSE methodology
- Domain specific language to apply STPA directly within SysML environment

Contributors

- Boesch, Mathew
- Chea, Top
- D’Amato, Anthony
- Kassar, Sari
- Keshri, Ashish
- Mensah-Brown, Arnold
- Moore, Austin
- Munjal, Vijay
- Nuesch, Sandro
- Post, Kyle
- Qamar, Ahsan
- Yako, Sarra

29th Annual **INCOSE**
international symposium

Orlando, FL, USA
July 20 - 25, 2019

www.incose.org/symp2019

Thank you for your attention!

Abbreviations, Acronyms and Definitions

AV	Autonomous Vehicle	**OEM**	Original Equipment Manufacturer
CF	Causal Factor	**PF**	Process Flaw
FMEA	Failure Modes and Effects Analysis	**PFMEA**	Process Failure Mode Effects Analysis
FSC	Functional Safety Concept	**SOI**	System of Interest
FTA	Fault Tree Analysis	**STPA**	Systems Theoretic Process Analysis
HARA	Hazard Analysis and Risk Assessment	**TSC**	Technical Safety Concept
		UCA	Undesired Control Action

AV storage and maintenance	Resources necessary to keep the AV operational, including building(s)/location(s) where the AV is stored, serviced, maintained, etc.	**service operations management**	Offboard control center for the ride sharing service
occupant	any human(s) inside the autonomous vehicle	**service function interface**	Onboard system element that manages AV’s communication with off-board ride-share service management systems