

Hazard analysis of aircraft inspection by drone assistant system using STPA

A strong partner in building a trustable future.

PROTECT

Hanaa KHAIL

Systems Safety engineer

MIT STAMP workshop

25/09/2025



CTU
CZECH TECHNICAL
UNIVERSITY
IN PRAGUE

FACULTY OF TRANSPORTATION SCIENCES
DEPARTMENT OF AIR TRANSPORT

AIRBUS

The Team



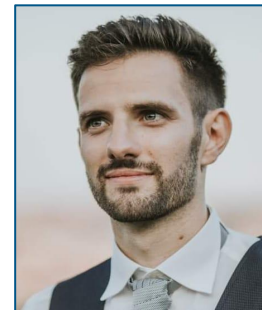
Hanaa KHAIL

System safety engineer
Airbus Protect



Julien VIDALIE

MBSA safety engineer
Airbus Protect



Max CHOPART

Ph.D. Candidate
Department of Air Transport / Faculty of
Transportation Sciences
Czech Technical University in Prague

Introduction

Introduction



We're challenging the traditional idea that accidents are only caused by failure. We ask "what if that's not the case?"

To answer this, we use STPA, a method that identifies hazards by considering both failure and non-failure scenarios.



Our objective is to apply this methodology to a complex system, analyze the results, and discuss the challenges of its implementation.

AIDA system

AIDA system

- **AIDA:** Drone system
- **Origin:** Developed as part of the project MOISE at IRT Saint Exupery
- **Main mission:** Assist the pilot in pre-flight aircraft inspection
- **System composition:** A quadcopter drone, a control desk, and a remote control.



AIDA



AIDA: Aircraft Inspection by Drone Assistant

AIDA system

AIDA capabilities

Inspect the aircraft
Detect the anomalies
Produce the mission report
Locate ice accretion areas on the aircraft
Monitor AIDA state
Mitigate AIDA failures

AIDA benefits

Access to high parts of the aircraft
Reduce operation time
Provide reliable results
Need basic piloting skills



[AIDA System Architecture](#)

STPA analysis of AIDA system

: STPA analysis of AIDA system >>

1. Defining the purpose of analysis

Losses	Hazards	System level safety constraints
L-1: loss of mission	H-1: AIDA provides erroneous or incomplete inspection results (L-1, L-3)	AIDA must provide reliable inspection results (H-1)
L-2: loss or damage of drone	H-2: AIDA violated the minimum separation between the drone and the aircraft (L-1, L-2, L-3, L-5, L-6)	the drone must maintain a safe distance from aircraft and airport passengers (H-2, H-3)
L-3: loss of operational performance	H-3: AIDA violated the minimum separation between the drone and human being (L-1, L-2, L-3, L-5, L-4)	AIDA must ensure the communication with the stakeholders and the environment (H-4)
L-4: loss or injury of people	H-4: the drone flies in unauthorized areas (L-1, L-2, L-3, L-4, L-5, L-6)	AIDA inspection duration shall not exceed the time limit (H-5)
L-5: loss of compliance with regulations	H-5: delays in AIDA mission execution (L-1, L-3)	the drone must maintain its stability and controllability even under the worst conditions (H-6)
L-6: unacceptable damage to the aircraft	H-6: uncontrolled drone behavior (L-1, L-2, L-3, L-4, L-5, L-6)	

Comprehensive overview of AIDA system’s losses, hazards, and safety constraints

: STPA analysis of AIDA system >>

1. Defining the purpose of analysis

01

- Identifying stakeholders

Drone operator, flight crew, maintenance team, airport, airlines, ATM, UTM/U-space, manufacturer

03

- Extracting hazards

Examples: AIDA provides erroneous inspection results, drone violates minimum separation distance, drone flies in unauthorized areas..

02

- Defining losses

Examples: loss of mission, loss or damage of the drone, unacceptable damage to the aircraft, loss or injury of people...

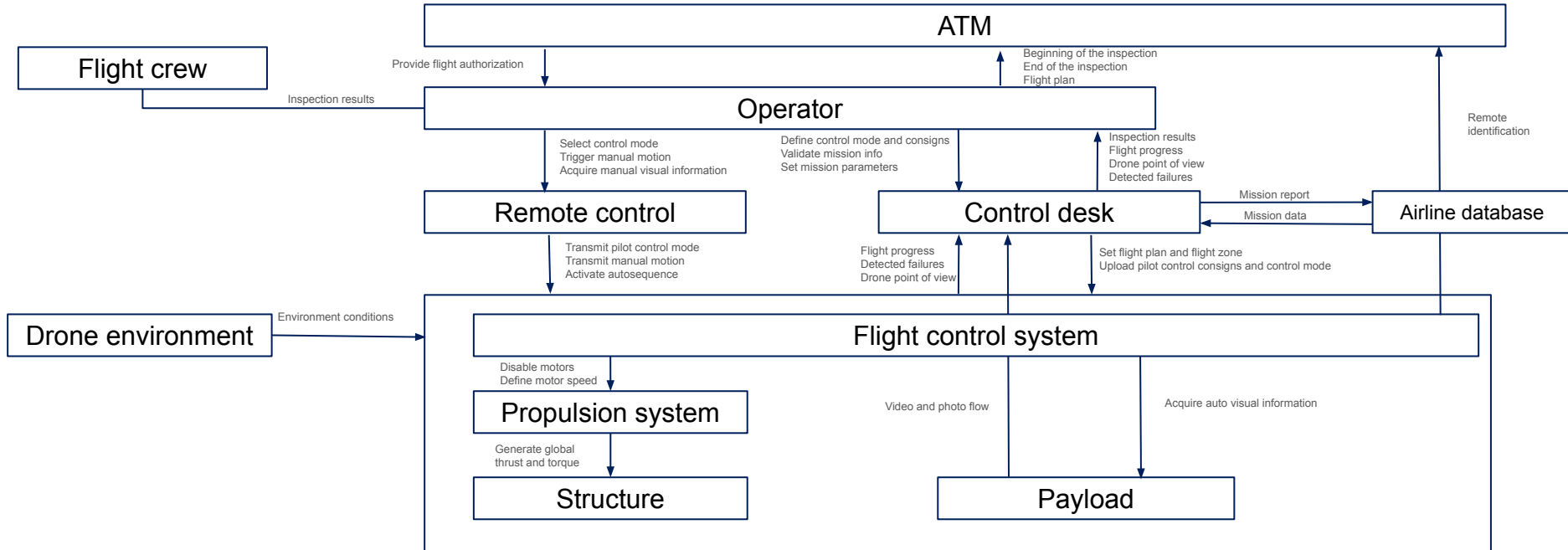
04

- Defining safety constraints

Examples: AIDA must provide reliable inspection results, the drone must maintain a safe distance from aircraft and airport passengers..

: STPA analysis of AIDA system >>

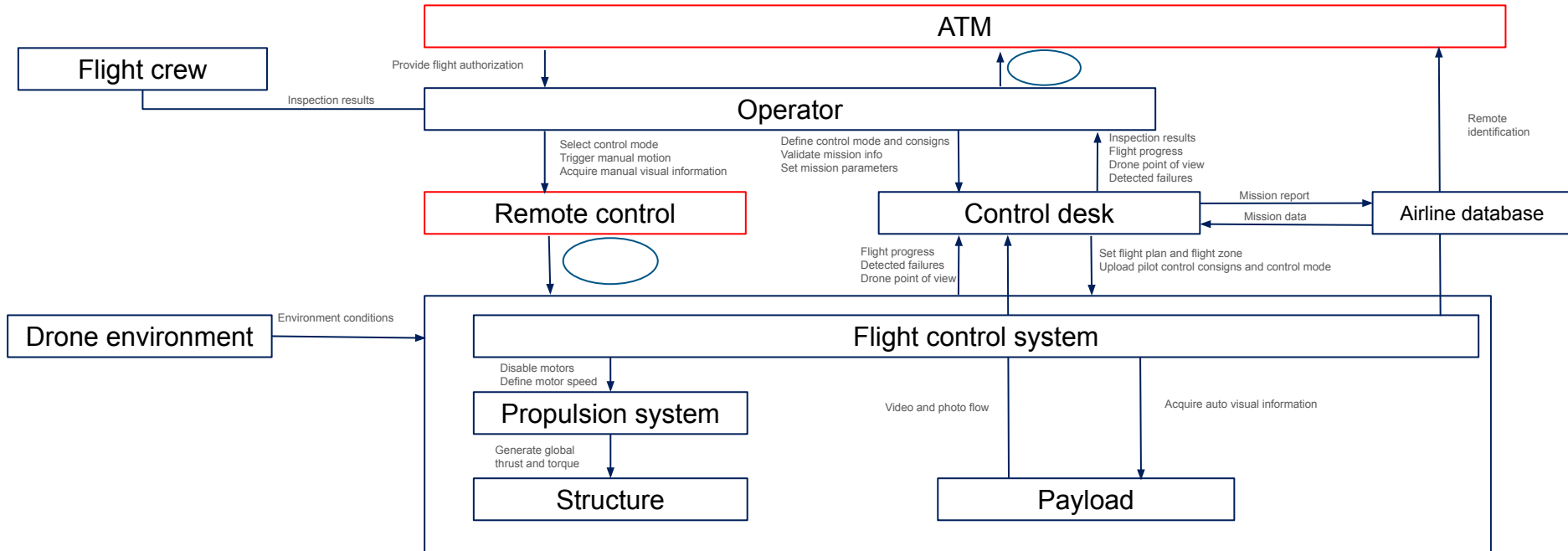
2. Modeling the control structure



The control structure of AIDA system

: STPA analysis of AIDA system >>

2. Modeling the control structure



The control structure of AIDA system

: STPA analysis of AIDA system >>

2. Modeling the control structure

01

• Analyzing AIDA architecture to identify controllers, controlled process and control actions



Entity	Logical functions	Physical functions	Control actions
Remote control	<ul style="list-style-type: none"> - Acquire manual motion commands - Acquire pilot control mode - Acquire auto-sequence commands - Display drone point of view - Display detected failures 	<ul style="list-style-type: none"> - Acquire pitch order - Acquire roll order - Acquire yaw order - Acquire vertical speed order - Acquire manual override order - Acquire manual payload control 	<ul style="list-style-type: none"> - Transmit manual motion - Activate auto sequence command - Transmit pilot control mode

02

• Deriving feedback from controllers' responsibilities and process models



Entity	Responsibilities	Process model	Feedback
ATM	<ul style="list-style-type: none"> - Provide flight authorization 	<ul style="list-style-type: none"> - The operator started the inspection - The operator ended the inspection - The drone is in the authorized areas 	<ul style="list-style-type: none"> - The beginning of inspection - The end of inspection - Drone remote identification - Flight plan

: STPA analysis of AIDA system >>

3. Identification of UCAs

Control action	Not providing causes hazard	Providing causes hazard	Too early, too late, out order	Stopped too soon, applied too long
Give the authorization to fly	UCA1: ATM doesn't provide the authorization to fly even if all the conditions are met and the flight zone is safe (H-6)	UCA2: the authorization is provided while an aircraft is taxiing in the flight zone (H-3, H-2)	UCA3: the ATM provides too late the authorization to fly after the transmission of a safe flight zone (H-1, H-5)	UCA4: the authorization stopped before the end of the inspection (H-1, H-2, H-3)



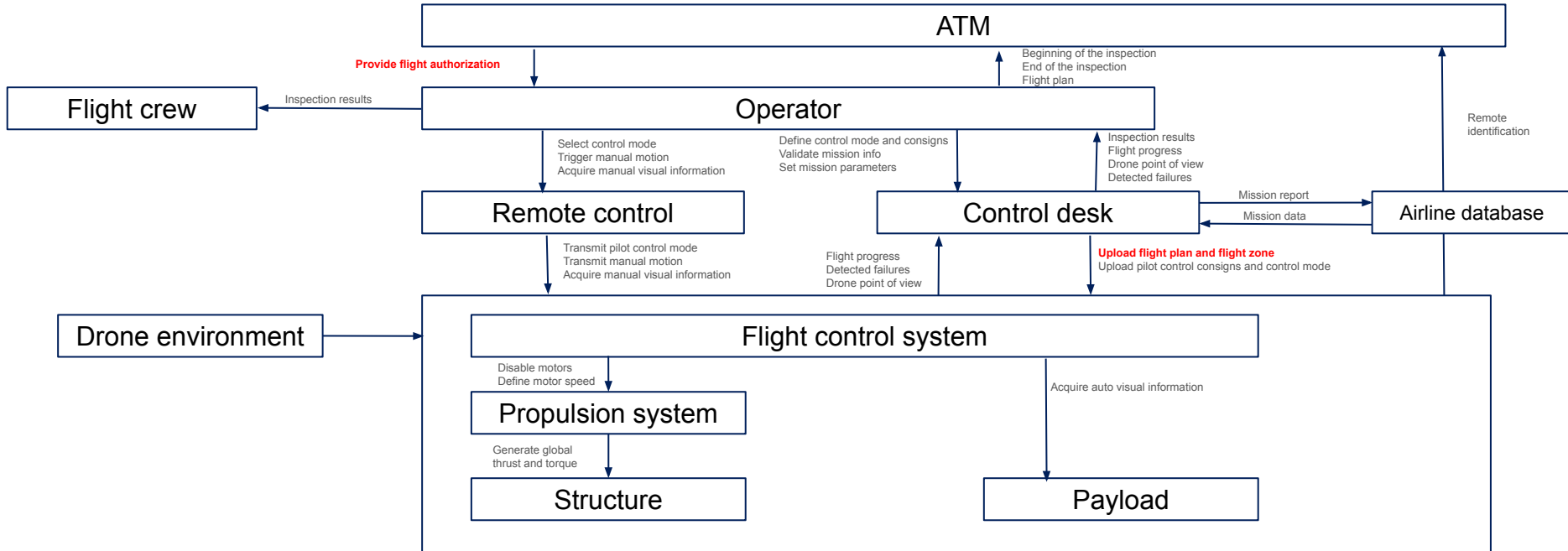
Provides pitch and roll consign	UCA83: the flight control system doesn't provide the pitch and roll consign when the drone needs to maintain a specific orientation. (H-1, H-2, H-3, H-4, H-5, H-6)	UCA84: the flight control system provides erroneous pitch and roll consign. (H-1, H-2, H-3, H-4, H-5, H-6)	UCA85: the flight control system provides too late the pitch and roll consign after an unpredictable obstacle appears. (H-1, H-2, H-3, H-4, H-5, H-6)	
---------------------------------	---	--	---	--

85 UCAs

UCAs of AIDA system

: STPA analysis of AIDA system >>

3. Identification of UCAs



: STPA analysis of AIDA system >>

3. Identification of UCAs

Control action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Provide flight authorization	UCA1: ATM doesn't provide authorization to fly even if all the conditions are met and the flight zone is safe (H-5)	UCA2: ATM provides authorization while an aircraft is taxiing in the flight zone (H-2, H-3, H-4)	UCA3: ATM provides authorization to fly too late after the transmission of a safe flight zone (H-1, H-5)	UCA4: the authorization stops before the end of the inspection (H-1, H-2, H-3)
Upload flight plan and flight zone	UCA28: the control desk fails to upload the flight plan and flight zone when the drone is in AP mode (H-2, H-3, H-4, H-5, H-6)	UCA29: the control desk uploads erroneous flight plan and flight zone (H-1, H-2, H-3, H-4, H-6)		

: STPA analysis of AIDA system >>

4. Identification of loss scenarios

UCA	Unsafe controller behavior	Unsafe feedback path	Unsafe control path	Unsafe controlled process behavior
UCA1	LS1: ATM doesn't provide the authorization to fly command when all the conditions are met and the flight zone is safe. ATM received feedback that indicates all the conditions are met and the flight zone is safe.	LS2: feedback received by the ATM does not adequately indicate that the flight zone is safe and the conditions are suitable for flying. The conditions are suitable for flying and the flight zone is safe.	LS3: ATM does provide the authorization to fly when the flight zone is safe and the conditions are suitable for flying. The authorization to fly is not received by the operator when the flight zone is safe and the conditions are suitable for flying.	LS4: the authorization to fly command is received by the operator when the flight zone is safe and the conditions are suitable for flying. But the operator does not start the inspection.



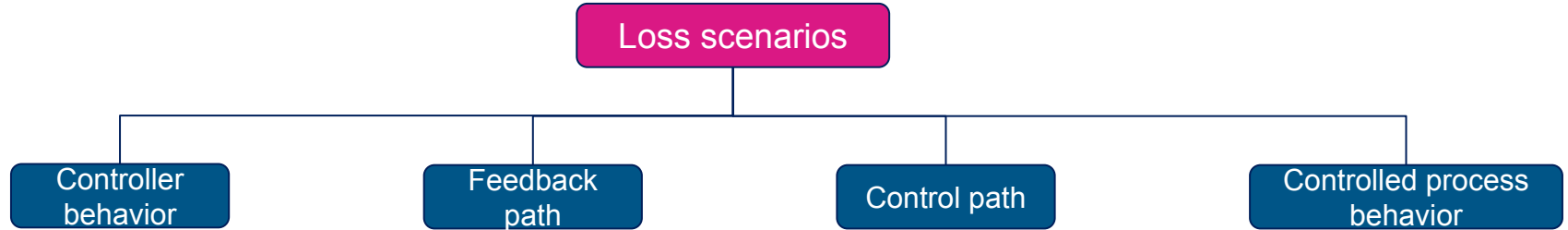
UCA85	LS324: the function control attitude and altitude MON provides pitch and roll consign too late after an unpredictable obstacle appears. The function control attitude and altitude MON received feedback that indicates the detection of an unpredictable obstacle on time.	LS325: feedback received by the function control attitude and altitude does not indicate the detection of an unpredictable obstacle too late. It is true that an unpredictable obstacle appears.	LS326: the function control attitude and altitude MON does not provide in time the pitch and roll consign when an unpredictable obstacle appears. The pitch and roll consign is received by the function compute navigation data MON too late when an unpredictable obstacle appears.	LS327: the pitch and roll consign is not received by the function compute navigation data MON too late when an unpredictable obstacle appears. The function compute navigation data provides too late navigation.
-------	---	--	---	---

327 loss scenarios

Loss scenarios of AIDA system

: STPA analysis of AIDA system >>

4. Identification of loss scenarios



<p>LS116: the control desk provides flight plan and flight zone when they are erroneous. The control desk received feedback that indicates that the flight plan and flight zone are erroneous.</p>	<p>LS117: feedback received by the control desk does not adequately indicate that the flight plan and flight zone are erroneous. The flight plan and flight zone are erroneous.</p>	<p>LS118: the control desk doesn't provide the flight plan and flight zone when they are erroneous. The drone receives the flight plan and flight zone when they are erroneous.</p>	<p>LS119: the flight plan and the flight zone are not received by the drone when they are erroneous. The drone follows an erroneous flight plan and flight zone.</p>
--	---	---	--

Example: UCA29

: STPA analysis of AIDA system >>

4. Identification of loss scenarios

Refined scenarios:

LS116: the control desk provides flight plan and flight zone when they are erroneous. The control desk received feedback that indicates that the flight plan and flight zone are erroneous.



The control desk ignores the operator validation

With Failure

Without failure

LS119: the flight plan and the flight zone are not received by the drone when they are erroneous. The drone follows an erroneous flight plan and flight zone.



The drone applies an outdated flight plan and flight zone

With Failure

Without failure

Conclusion

: STPA analysis findings on AIDA system >>



Reveals that human factor is a key contributor to loss scenarios



Reveals design flaws :

Control Desk: Missing interlock requiring validation

Drone: Lacks software for updating stored data after the inspection



Provides clear documentation for complex systems

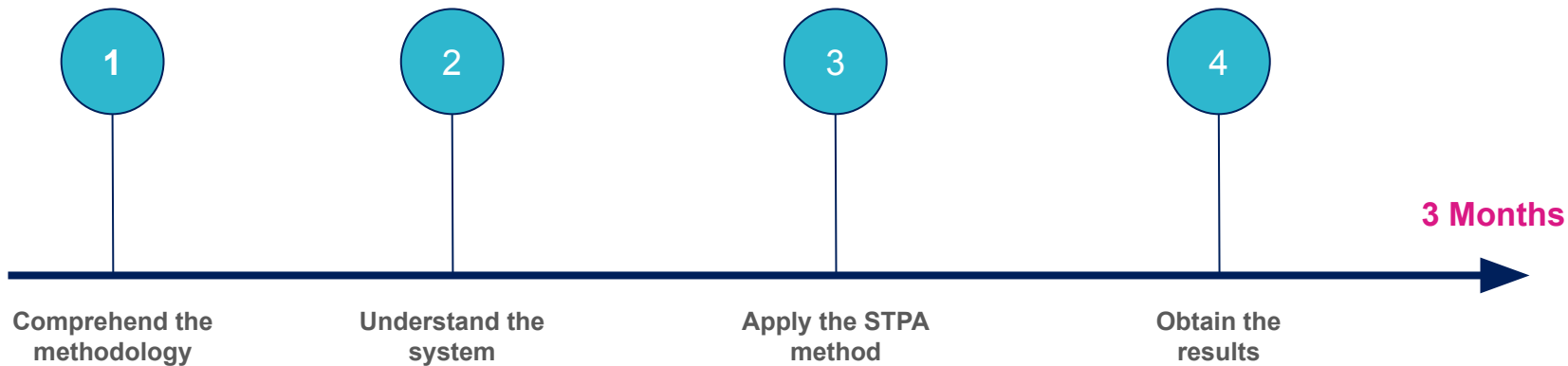


Presents a more detailed analysis as shown in the results: 85 UCAs, 327 loss scenarios



Highlights interactions with external environments

:Work approach >>



: STPA challenges >>

01

- The initial integration and adoption of the STPA method within industries may require a longer time frame compared to traditional methodologies.

02

- Difficulty in defining relevant hazardous contexts for control actions




03

- Conducting an STPA study necessitates collaboration with design teams to fully understand system limitations

04

- Identifying potential factors and context of UCAs presents difficulty, especially for design, human, and external interactions

: Next ... Steps >>

-  Correlate STPA results with the FHA analysis to evaluate the apport of STPA
-  Apply the integration approach of STPA with MBSA
-  Validate the integration approach through an extensive study case

“

thank you

”