STPA and SFHA combined: Airbus A320 High-lift System Case Study

Kiyofolo Benjamin Ouattara

Department of Air Transport / Faculty of

Transportation Sciences Czech Technical University in Prague

MIT STAMP workshop

Introduction

Increasing system complexity challenges traditional safety methods. STPA addresses non-failure hazards but is not part of certification. How can STPA fit into ARP4761A?

To address this question, we compare STPA and SFHA results, analyze the differences, and discuss integration challenges.



Our goal is to apply this approach to a complex system, evaluate the outcomes, and examine the challenges of implementation.

CTU
CZECH TECHNICAL UNIVERSITY IN PRAGUE

Airbus A320 Family ATA 27 High-lift System

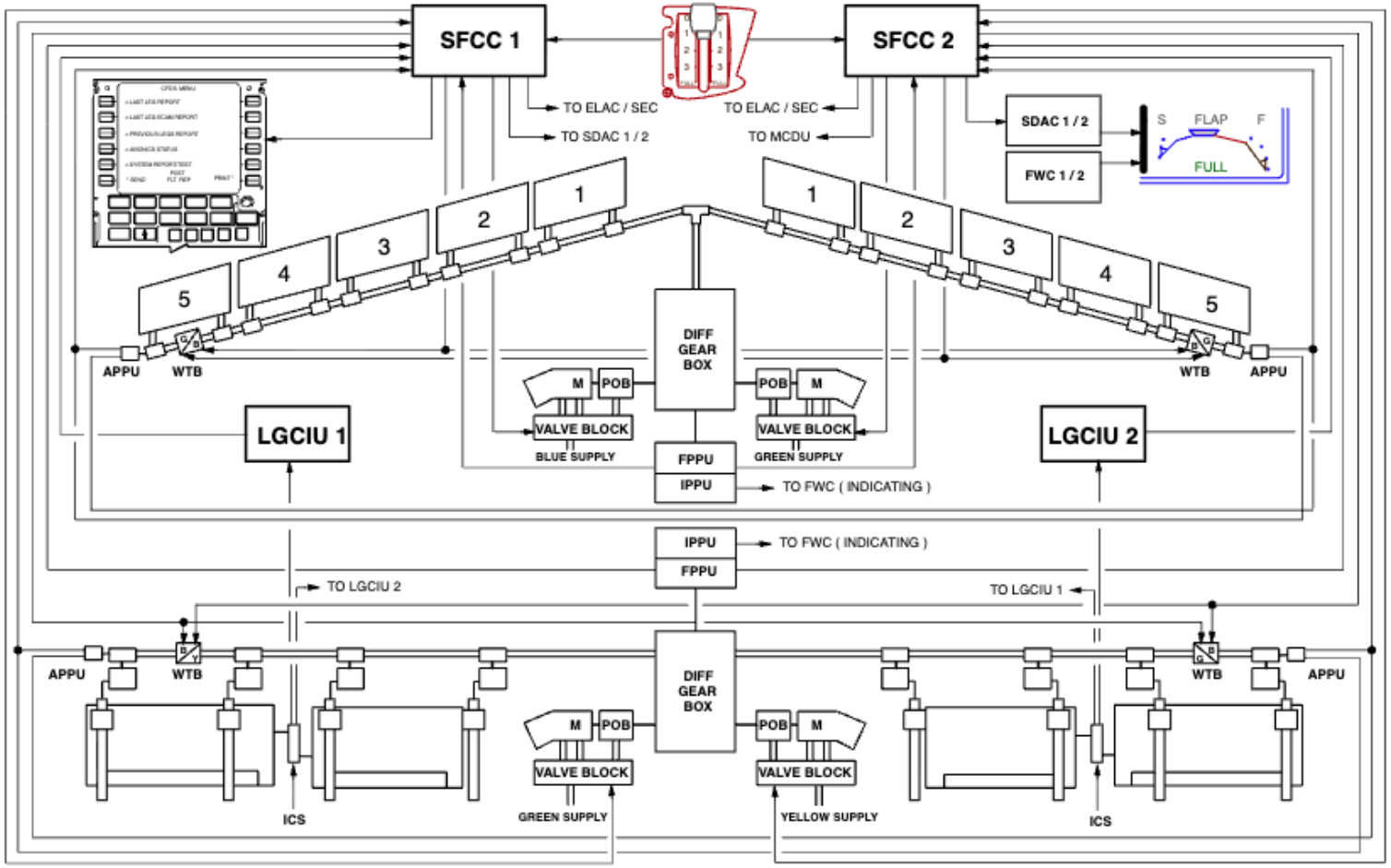
Airbus A320 Family ATA 27 High-lift System

Key Component

- Pilot Interface: Flap Lever
- Control Computers: SFCC
- Power & Hydraulic Control: PCU
- Actuation & Transmission: Gearbox, Transmission Shafts
- Braking & Load Protection: POB, WTR
- Position Feedback & Monitoring: PPU, Flap and Slat Sensors
- Indication & Crew Alerting: ECAM Interface
- Leading and Trailing-Edge Devices: Slats and Flaps

System Function

•increases wing lift at low speeds
•Reduces stall speed
•Enables safe takeoff and landing
•Improves low-speed control



Flaps and Slats system schematic. (Airbus, 2005)



SFHA analysis of Airbus A320 Family High-lift System

SFHA analysis of High-lift System

System Function	Failure ID	Scenarios	Safety Effects	Crew detection	Crew action	Classification
To provide system information	F1 : Total loss of S/F position information	Loss of Flap/ Slat actual position indication during all flight phases	The crew loses position Indication during all flight phases	Loss of flaps actual position displayed on ECAM	Crew may perform troubleshooting to identify the actual flaps position.	MIN
To move Flaps and Slats	F2: Total loss of Flap/Slats movement	Total loss of Flap/Slats drive during all flight phases	The A/C cannot move flaps/slats	F/CTL Flaps locked alert on ECAM	N/A	MAJ

More than 100 Failure conditions



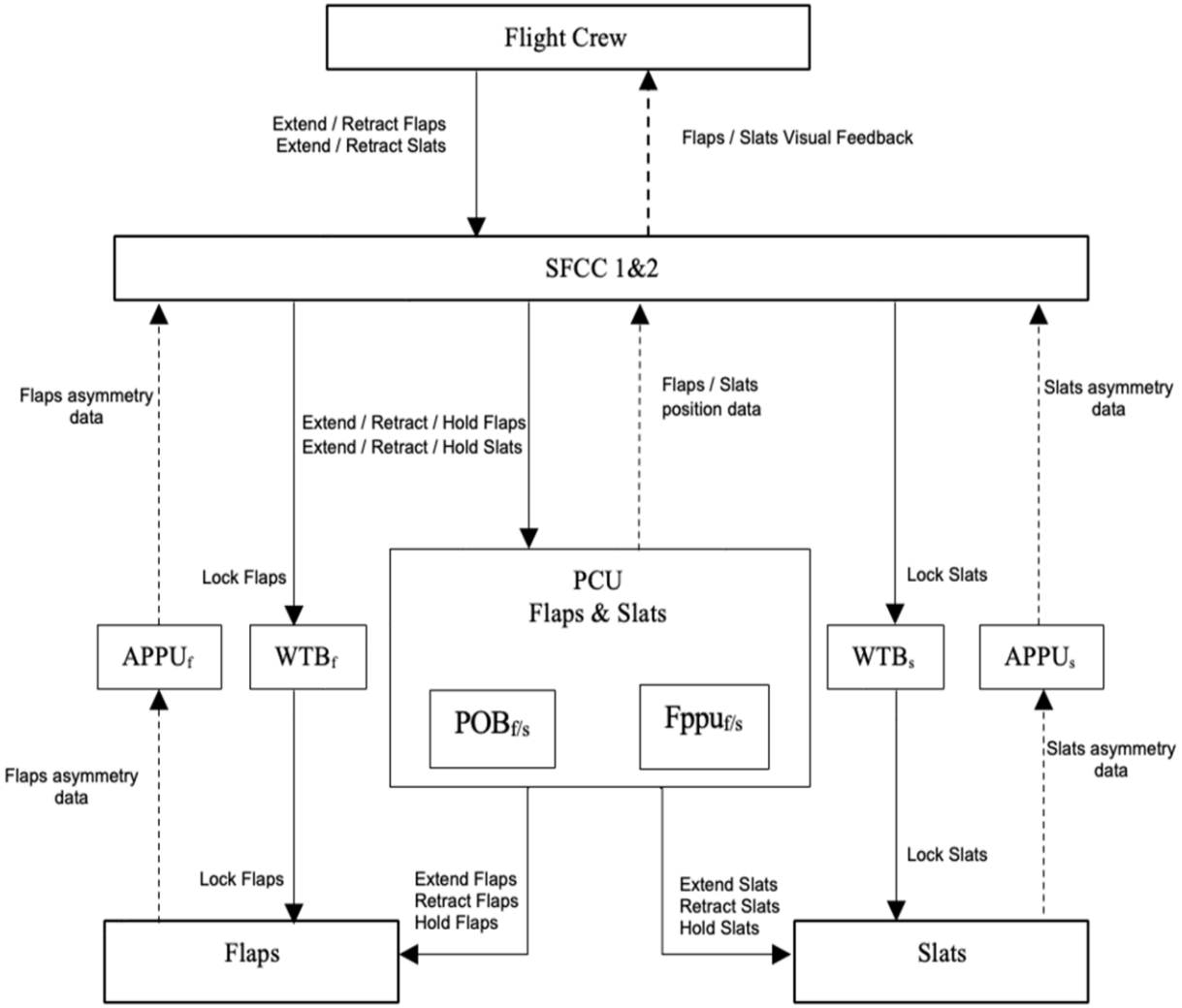
STPA analysis of Airbus A320 Family ATA 27 High-lift System

STPA analysis of High-lift system

1. Defining the purpose of analysis

Losses	Hazards	**System-level Constraint**
L-1: Loss of life or injury to people (Crew, Passenger)	H-1: The system exceeds safe operating envelope during any flight phases. (L-1, L-2, L-3)	SC-1: The system must operate within the defined safe envelope during all flight phases.(H-1, H-2)
L-2: Loss of or damage to A/C	H-1.1: Asymmetric deployment of Slats and Flaps during all flight phases. (L-1, L-2, L-3)	SC-2: The system must ensure symmetric deployment of Slats and Flaps under all operating conditions and flight phases. (H-1, H-2)
L-3: Loss of mission	H-2: Inadvertent operation of system(Slats, Flaps, Rotary actuators, Bevel gearboxes, Tee gearboxes, Gear racks, Tracks, etc) (L-1, L-2, L-3)	SC-3: The system must not operate inadvertently during ground operation and all flight phases.(H-1, H-2)

2. Modelling the control structure



STPA analysis of High-lift system

3. Identification of UCAs

Control action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order
Retract Slats and Flaps	UCA-19: SFCC does not provide the Retract Slats and Flaps action when the Flight crew commands during take - off or landing even when Slats and Flaps are extended, the A/C is within the flight envelope, and the High Lift System is operating normally. (H-1, H-2)	UCA-17: SFCC provides the Retract Slats and Flaps action when the Flight crew does not command during take - off, climb, approach, landing or cruise even when Slats and Flaps are already retracted or extended, the A/C is within or outside the flight envelope and the High Lift System is operating abnormally. (H-1, H-2)	UCA-20:SFCC provides the Retract Slats and Flaps action too late when the Flight crew commands during take - off, climb, approach, landing or cruise even when Slats and Flaps are already extended or retracted, the A/C is within or outside the flight envelope and the High Lift System is operating. (H-1, H-2)
Retract Slats and Flaps	UCA-48: Flight Crew does not provide the Retract Slats and Flaps action during take - off, landing even while Slats and Flaps extended when the A/C is within the flight envelope with normal High Lift System operation. (H-1, H-2)	UCA-47: Flight Crew provides the Retract Slats and Flaps action during take - off, climb, approach, landing or cruise even while Slats and Flaps are transitioning from extended to retracted positions or from retracted to extended positions, or in extended or retracted positions when the A/C is within or outside the flight envelope with abnormal or normal High Lift System operation. (H-1, H-2)	UCA-45. Flight Crew provides the Retract Slats and Flaps action too late during take - off, climb, approach, landing even while Slats and Flaps in extended positions when the A/C is within outside the flight envelope with normal or abnormal High Lift System operation. (H-1, H-2)

57 high level UCAs

STPA analysis of High-lift system

4. Identification of loss scenarios

Unsafe control action	Unsafe controller behaviour	Unsafe feedback path	Unsafe control path	Unsafe controlled process behavior
UCA-20:SFCC provides the Retract Slats and Flaps action too late when the Flight crew commands during take - off, climb, approach, landing or cruise even when Slats and Flaps are already extended or retracted, the A/C is within or outside the flight envelope and the High Lift System is operating. (H-1, H-2)	LS-42: The SFCC provides the slats and flaps retraction command too late. It is true that the SFCC received control input indicating on time that the flight crew commanded slats and flaps retraction	LS-111: The control input received by SFCC does not indicate on time that the Flight crew commanded Slats and Flaps retraction. It is true that the Flight crew commanded Slats and Flaps retraction.	LS-43: The SFCC provides the slats and flaps retraction command on time when the flight crew commands slats and flaps retraction. It is true that the slats and flaps retraction command is received by the PCU too late.	LS-44: The slats and flaps retraction command is received by the PCU on time when the flight crew commands slats and flaps retraction. It is true that the PCU does not respond adequately (e.g. response is too late).
[UCA-45] Flight Crew provides the Retract Slats and Flaps action too late during take - off, climb, approach, landing even while Slats and Flaps in extended positions when the A/C is within outside the flight envelope with normal or abnormal High Lift System operation	LS-14: Flight Crew provides the slats and flaps retraction command too late. It is true that the flight crew received timely feedback (or other indications) that slats and flaps retraction was required.	LS-114: Feedback received by Flight Crew does not indicate on time Slats and Flaps are extended during take - off, climb, approach or landing. It is true that Slats and Flaps are extended during take - off, climb, approach or landing.	LS-12: Flight Crew provides the slats and flaps retraction command on time. It is true that the slats and flaps retraction command is received by the SFCC too late.	LS-115: The slats and flaps retraction command is received by the SFCC on time. It is true that the SFCC does not respond adequately (e.g. response is too late).

188 Loss Scenarios

Comparison of the STPA output and SFHA output

1. STPA output = SFHA ouput

System Function	SFHA Failure Condition	STPA Loss Scenario
To provide data to the flight crew	Loss of Slat operation combined with misleading slat information and loss of warning Loss of Flap operation combined with misleading flap information and loss of warning • Total loss of S/F position information on EWD) • Loss of alert	[LS-111] The control input received by SFCC does not indicate on time that the Flight crew commanded Slats and Flaps retraction. It is true that the Flight crew commanded Slats and Flaps retraction.

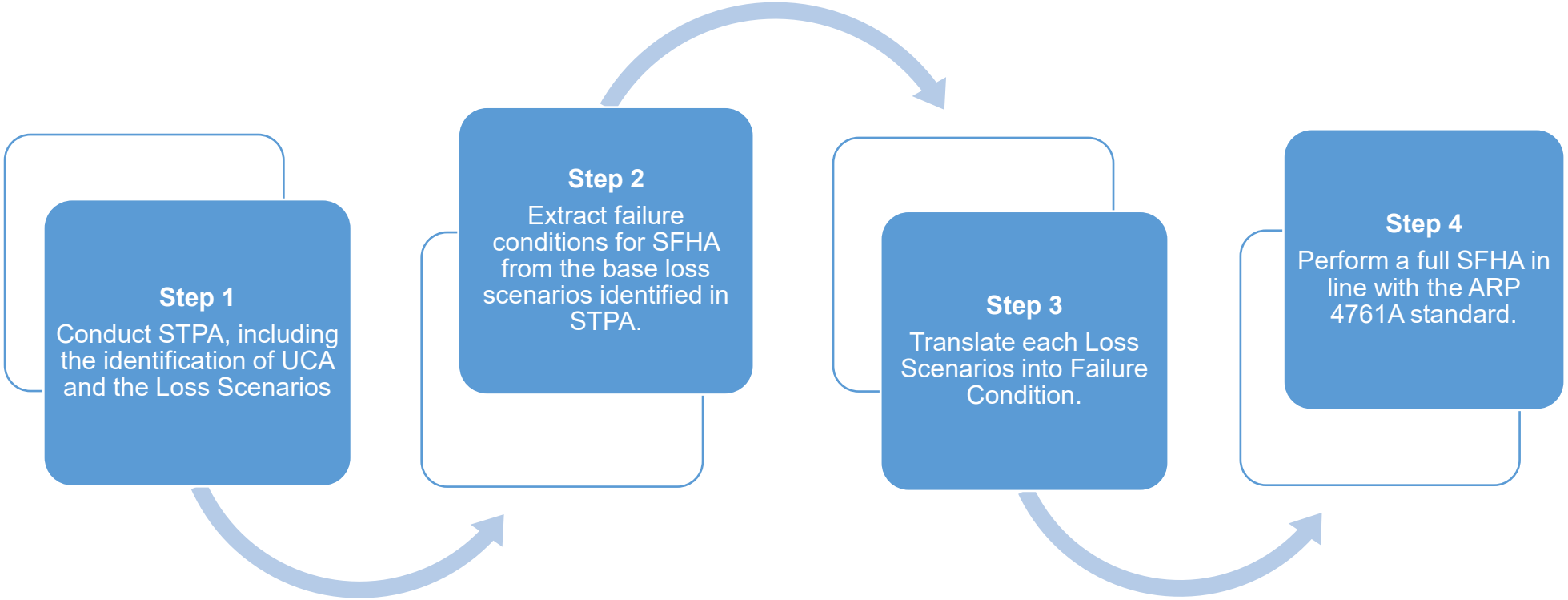
188 LS identified - 110 LS correspond FC

2. STPA output ≠ SFHA ouput

System Function	SFHA Failure Condition	STPA Loss Scenario
To provide HLS configuration	Not covered by SFHA	[LS-114] Feedback received by Flight Crew does not indicate on time Slats and Flaps are extended during take - off, climb, approach or landing. It is true that Slats and Flaps are extended during take - off, climb, approach or landing.

78 Loss Scenarios DO NOT correspond to FC

Results: combination of STPA and SFHA



Example of Translating LS into FC

STPA Loss Scenarios

SFHA Failure Condition

STPA Unsafe Control Action

[UCA-19]SFCC does not provide the Retract Slats and Flaps action when the Flight crew commands during take - off or landing even when Slats and Flaps are extended, the A/C is within the flight envelope and the High Lift System is operating normally. [H1, H2]

LS-70: SFCC does not provide the Retract Slats and Flaps action. It is true that it received command from the flight crew to provide it.

LS-108: SFCC didn't receive the retract Slats and Flaps command from the flight crew during take – off or landing even when Slats and Flaps are extended. The A/C is within the flight envelope, and the High Lift System is operating normally. It is true that the flight crew provide the command.

LS-109: SFCC does provide the Retract Slats and Flaps action, but Retract Slats and Flaps action is not received by each PCU.

LS-38: The Retract Slats and Flaps action is received by each PCU, but the PCUs does not respond adequately.

- Total Loss of SFCC
- Partial loss of SFCC
- Erroneous functioning of SFCC

- Total Loss of PCU
- Partial loss of PCU
- Erroneous functioning of PCU

LS output into FC

Discussion

01 Collaboration with design teams is essential for understanding system limitations during STPA development.

02 Defining hazardous contexts relevant to control actions remains a significant challenge.

03 Terminology differences (e.g., “inadequate feedback” vs. “misleading information”) complicate integration.

Conclusion

Capture systemic hazards, human interactions, and control logic issues.

Demonstrated feasibility of combining STPA and SFHA under ARP4761, using the A320 High-Lift System.

Completed safety assessment while staying ARP4761-compliant.

Future work: apply the approach to more complex systems.