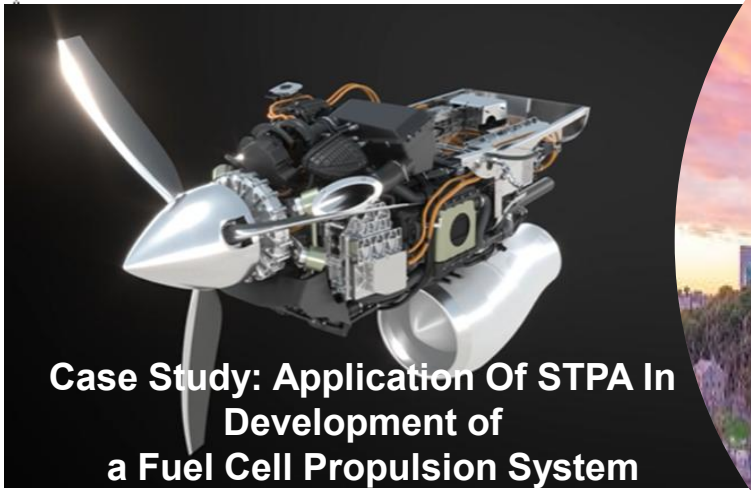
International Council on Systems Engineering

A better world through a systems approach



Case Study: Application Of STPA In Development of a Fuel Cell Propulsion System

Jean Machado, Edem Tsei, Shaarujan Prabakaran, Daniel Wilding

Cranfield Aerospace Solutions

Cranfield Technology Park, MK43 0AZ, UK

Case Study: Application Of STPA In Development of a Fuel Cell Propulsion System

Cranfield Aerospace Solutions Ltd

This presentation is a case study on the application of System Theoretic Process Analysis (STPA) to address inherent challenges that arise when developing systems.

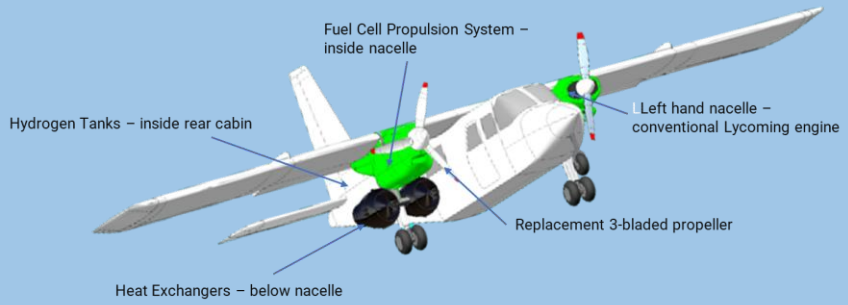
The aim is to demonstrate how STPA could help to define a comprehensive set of functional safety requirements that ensures the safe and efficient integration of complex systems by enabling early identification and implementation of mitigations against undesirable emergent behaviours.

Today's Agenda

- An Overview of Project Fresson
- Thrust Response Challenge
- Airworthiness and Safety requirements
- STPA process
- Results
- Conclusion
- Lessons learnt

Cranfield Aerospace Solutions Ltd

Case Study – Project Fresson



Project FRESSON 1a is a technology demonstrator programme that will fly an existing Britten-Norman BN-2B Islander aircraft modified to incorporate a Fuel-Cell Propulsion System (FCPS).

Cranfield Aerospace Solutions Ltd

Case Study – Project Fresson

The FCPS consists of the Hydrogen Fuel Cell System (HFCS), the Electric Propulsion Unit (EPU), and Pilot Communication and Interface System (PCIS).

The HFCS

- subsystem is a novel system for aerospace application

The EPU

- subsystem is an established system with novel features for aerospace application.

The PCIS

- subsystem is an established aerospace system.

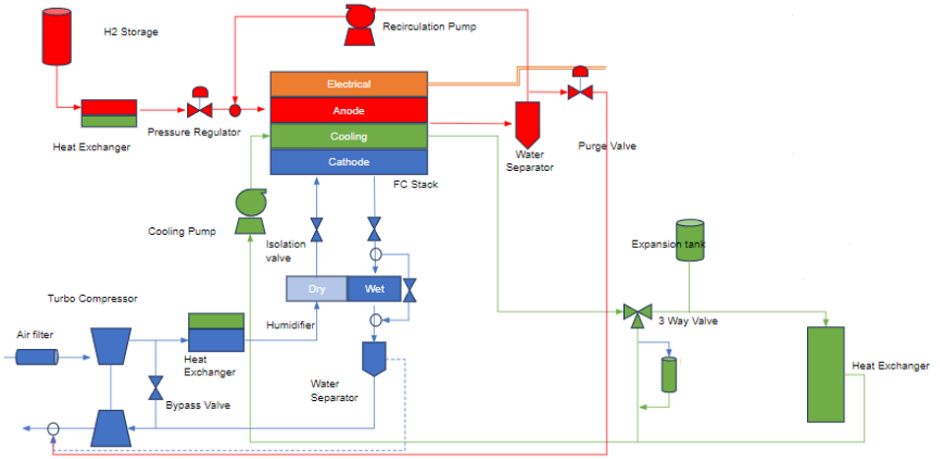
Cranfield Aerospace Solutions Ltd

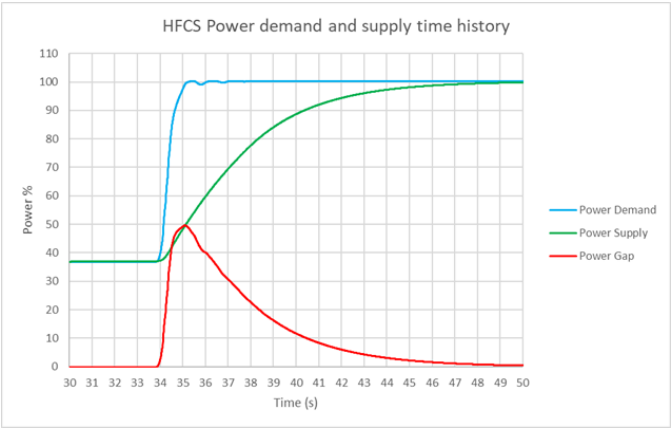
Thrust Response Challenges

Inherent Delay

Hydrogen fuel cells require time to ramp up their power output in response to a step input, such as a sudden demand for full power from the pilot in a go-around scenario.

This delay is inherent to the electrochemical processes within the fuel cell.





Airworthiness/Safety Requirements

Thrust Response

EASA CS-E 745 (a)(3) – Engine acceleration from 15% to 95% of the rated thrust shall be less or equal to 5 seconds.

Aircraft shall be capable to clear a 50 ft obstacle;

Decision to initiate Go-around must be done in TBD seconds.

Aircraft must be controllable during a single engine go-around.

Aircraft shall be capable to stop inside the runaway;

Aircraft must decelerate within TBD seconds.

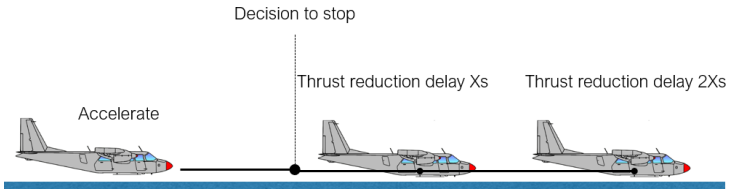
Aircraft must maintain directional control during a single engine rejected take-off.

Probability of Loss of FCPS shall be less than 1.00E-04 per flight hour.

Airworthiness/Safety Requirements

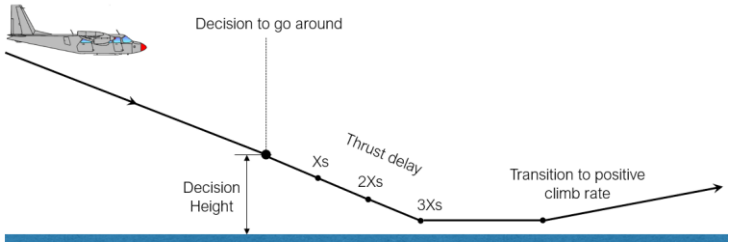
Critical Flight Phases

Rejected Take-off



Longitudinal Runway Excursion Speed	Failure Condition Severity Classification
> 60 kt	Catastrophic
> 30 – 60 kt	Hazardous
0 – 30 kt	Major
No runway excursion	Minor

Go-Around



EASA CS 23.67 (c) (4) requires the aircraft to maintain a climb gradient of 2.1% during a Go-around procedure, to effectively clear a 50 ft obstacle to 400 ft AGL, accelerate to 65 kts IAS and retract flaps.

Case Study – Late-Stage Requirements

Current Practices

Current practices limit safety analysis to establishing general reliability targets and high-level design recommendations, leaving critical functional safety requirements for later stages in development.

Early Identification

Without early identification of a holistic set of safety requirements, system architectures are often designed prematurely, leading to designs that may not safely or effectively achieve the system's goals.

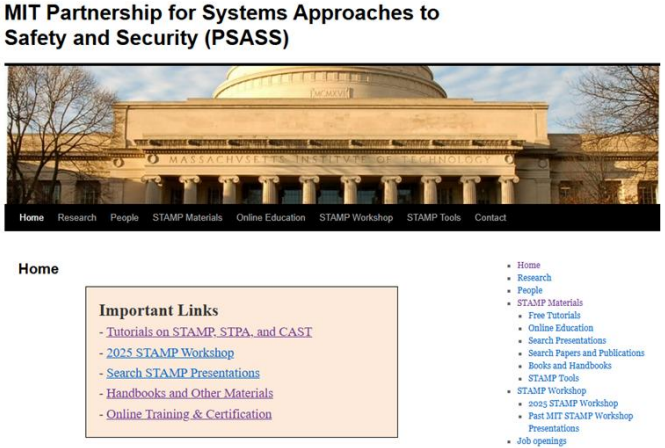
Generation of Safety Requirements

To mitigate these issues, there is a need to enhance development processes such that safety methodologies can be used earlier during the concept stage, enabling the generation of comprehensive safety requirements.

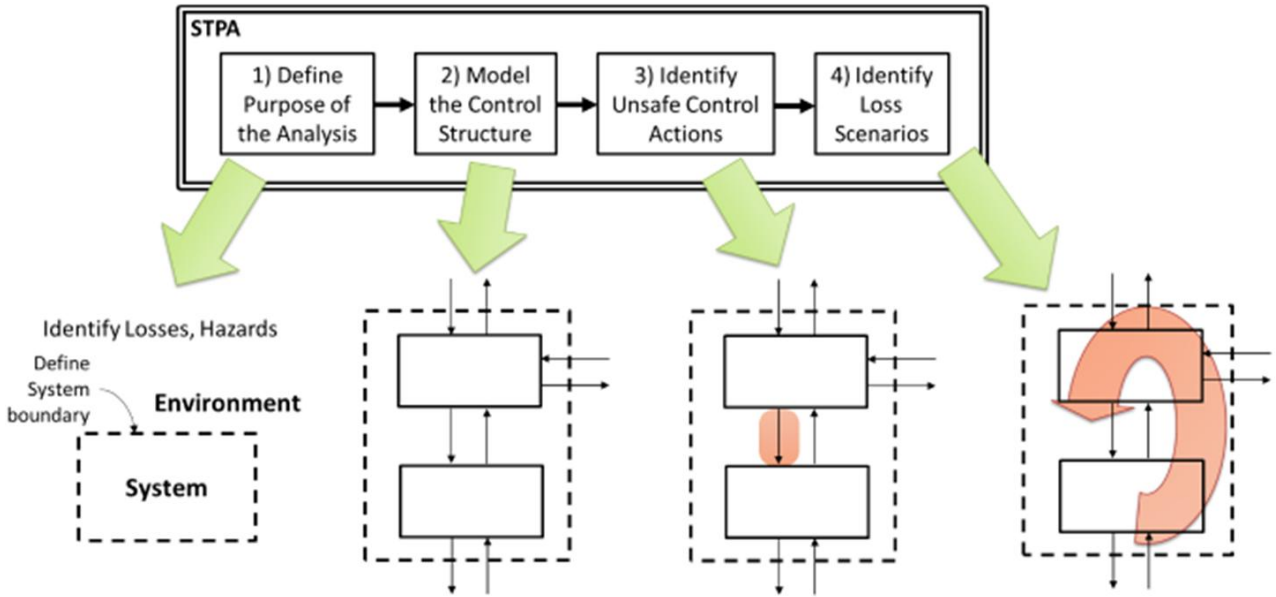
Cranfield Aerospace Solutions Ltd

Case Study – STPA Approach

STPA is a safety and hazard analysis methodology based on the Systems-Theoretic Accident Model and Processes (STAMP) framework by Dr Nancy Leveson. Primarily focus on control structures and interactions of a system, both within and with other systems.

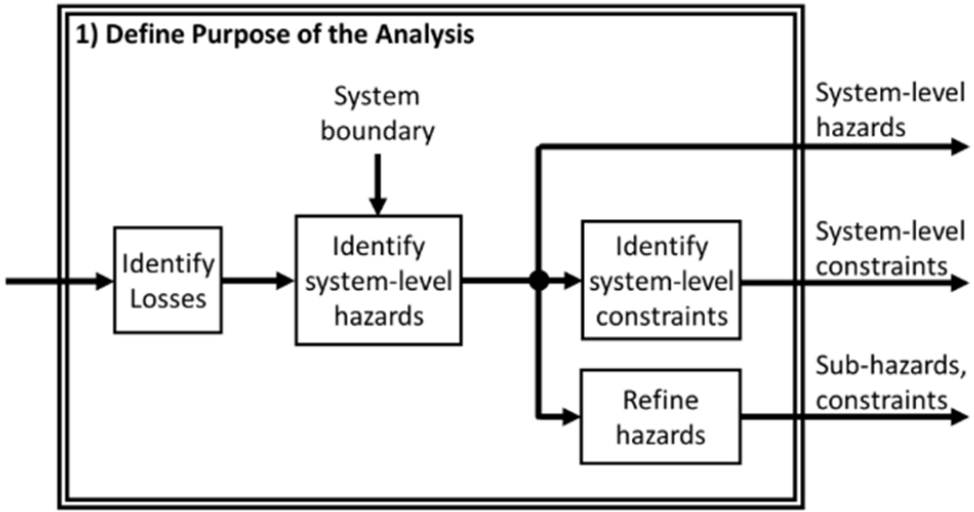


Case Study – STPA Process



Case Study – STPA Process

Step 1 – Define the purpose of the analysis



Cranfield Aerospace Solutions Ltd

Case Study – STPA Process

Step 1 – Define the purpose of the analysis

What kinds of losses will the analysis aim to prevent?
What is the system to be analyzed and what is the system boundary?

A1. Loss of life or injury to aircraft occupants.

A2. Loss or damage to aircraft.

Case Study – STPA Process

Step 1 – Define the purpose of the analysis – Refine Hazards

Accident/ Losses	Hazard ID	Hazard	Sub-Hazard ID	Sub- Hazard
A1, A2	H3	Aircraft comes too close to other objects on ground	H3-1	Deceleration is insufficient upon rejected take-off
			H3-2	Deceleration occurs after V1 point during rejected take-off
			H3-3	Acceleration continues to be applied during rejected take-off
			H3-4	Insufficient steering to keep the aircraft inside the runaway

Case Study – STPA Process

Step 1 – Define the purpose of the analysis – Constraints

Accident/ Losses	Hazard ID	Hazard	Safety Constraint ID	Safety Constraint
A1, A2	H1	Aircraft comes too close to terrain or obstacles during Go around	SC1	Decision to initiate Go-around must be done in TBD seconds.
A1, A2	H2	Aircraft loses controlled flight during a single engine go around	SC2	Aircraft must be controllable during a single engine go-around.
A1, A2	H3	Aircraft comes too close to other objects on ground	SC3	Aircraft must decelerate within TBD seconds.
A1, A2	H4	Aircraft deceleration manoeuvres aircraft toward other objects	SC4	Aircraft must maintain directional control during a single engine rejected take-off.

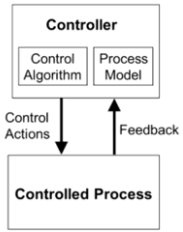
Case Study – STPA Process

Step 2 – Model the Control Structure

A control structure is a system model that is composed of feedback control loops.

In general, a controller makes decisions to achieve goals and provides control actions to control some process and to enforce constrains on the behavior of the controlled process.

The controller process is any process that is controlled, such as a physical process or another controller.



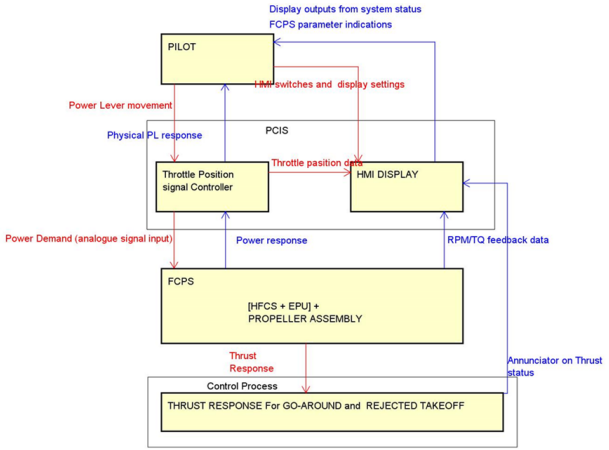
This study is limited to the following controllers:

1) Pilot

2) Throttle Position Signal Controller (TPSC);

3) Fuel Cell Propulsion System (FCPS);

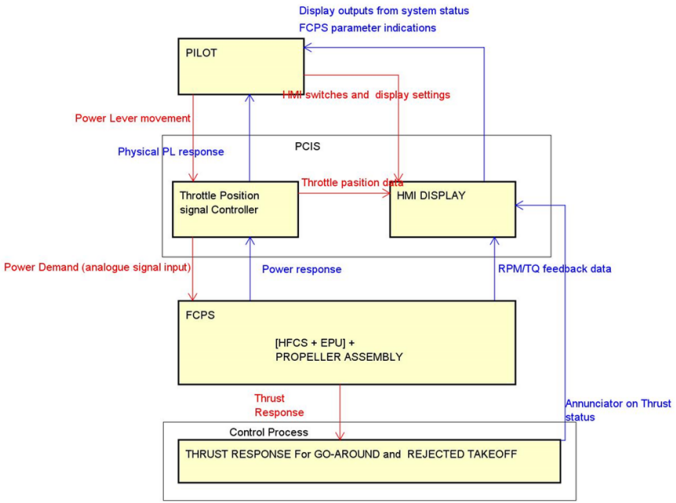
4) Human Machine Interface (HMI)



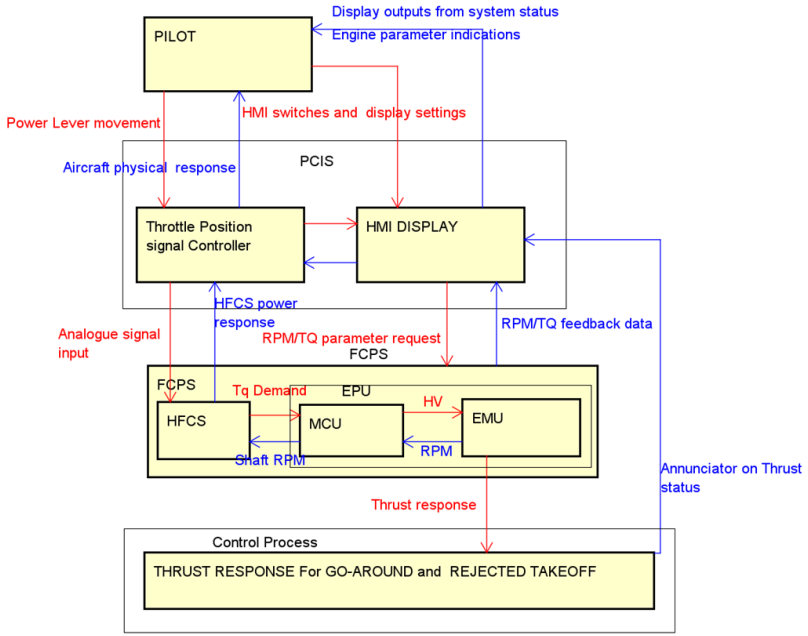
Case Study – STPA Process

Step 2 – Model the Control Structure

Conceptual Stage



Development Stage



Case Study – STPA Process

Step 3– Identify Unsafe Control Actions

An Unsafe Control Action (UCA) is a control action that, in a particular context and worst-case environment, will lead to a hazard.
There are 4 ways a control action can be unsafe:

i) Not providing the control action leads to a hazard;

ii) Providing the control action leads to a hazard;

iii) Providing a potentially safe control action but too early, too late, or in the wrong order;

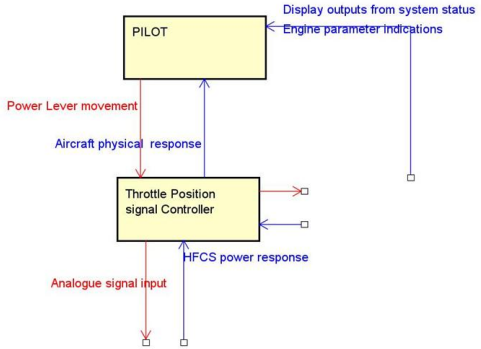
iv) The control action lasts too long or is stopped too soon

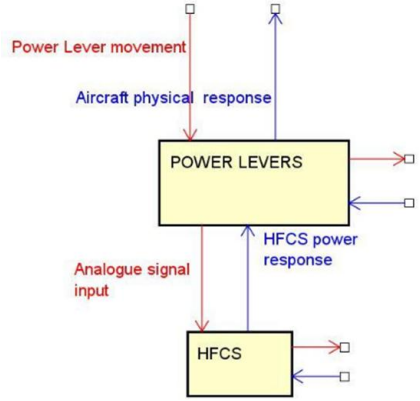
Case Study – STPA Process

Step 3– Identify Unsafe Control Actions

In this step the study identified the unsafe control actions (UCA) within the system.
These include situations where control actions are provided incorrectly, at the wrong time, or omitted entirely.
For instance, a delay in the propulsion system delivering full thrust during a go-around could lead to an unsafe control action.

This step forms the foundation for deriving safety constraints. This is because it presents a scenario where the system-to-system interaction alongside human factors work together to control the FCPS.





A loss in pilot situational awareness on aircraft Thrust perception, comprehension, decision and acting as explained by Endsley (1995), on any flight information presented on the HMI to the pilot will have consequences on thrust response in critical phases of flight.

Case Study – STPA Process

Step 3 – (a) Identify Unsafe Control Actions

CA	From	To	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
Power Lever movement	Pilot	TPSC Throttle position signal controller	(UCA2-N-1) Pilot does not provide power lever movement to Throttle position signal controller at RTO/Go-around [SC1]	(UCA2-P-1) Pilot provides bellow TBD power lever movement at RTO/Go-around [SC2] [SC3] [SC4]	(UCA2-T-1) Delayed pilot input to Throttle Position signal controller during Go-around/RTO leads to loss of A/C altitude/available runway. [SC1]	(UCA2-S-1) Pilot stops providing power lever movement to throttle position signal controller before Go-around speed and safe altitude is achieved.
Analogue signal input	TPSC	FCPS Fuel Cell Propulsion System	(UCA1-N-1) Throttle Position signal controller does not provide analogue signals to FCPS during RTO/ Go-around [SC3]	(UCA1-P-1) Un-commanded/Erratic analogue signal from Throttle Position signal controller to FCPS during RTO/ Go-around [SC3] [SC4]	(UCA1-T-1) Delayed analogue signal communication between Throttle Position signal controller and FCPS during RTO/GA [SC1], [SC2], [SC5], [SC7]	(UCA1-S-1) Throttle position signal controller stops providing analogue signal before FCPS attains TBD power for Go-around/ above signal required for RTO.

Case Study – STPA Process

Step 3 – (a) Posing High-level Controller Constraints

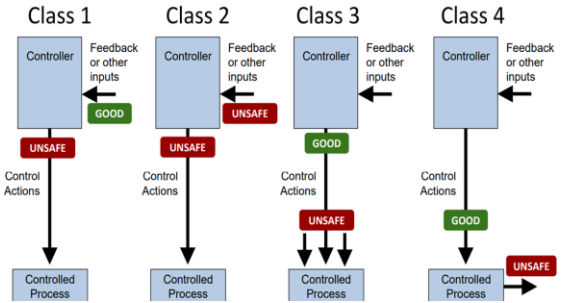
To prevent having Unsafe Control actions we pose high level controller constraints This guides the next step in identifying scenarios leading to this UCA.
Detailed system level safety constraints serve as a foundation for generating safety requirements.

Unsafe Control Actions	Controller Constraints
(UCA1-N-1) Throttle Position signal controller does not provide analogue signals to HFCS during RTO/ Go-around [SC3]	Throttle position signal controller must provide analogue signals to HFCS during RTO/Go-around
(UCA1-P-1) Un-commanded analogue signal from Throttle Position signal controller to HFCS [SC3] [SC4]	Throttle position signal controller must not provide uncommanded analogue signals to HFCS
(UCA1-T-1) Delayed analogue signal communication between Throttle Position signal controller and HFCS during RTO/Go-around [SC1], [SC2], [SC5], [SC7]	Signals from the throttle position signal controller must reach HFCS at RTO/Go-around within TBD seconds

Case Study – STPA Process

Step 4 – Identification of Loss Scenarios

A loss scenario describes the causal factors that can lead to unsafe control actions and to hazards.

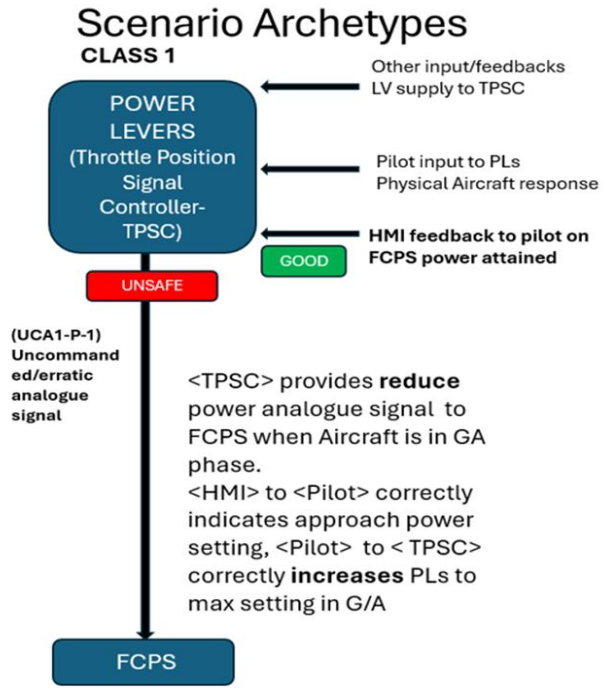


Archetype Scenario 1 at Go-Around	
A - Responsibilities	TPSC by design is responsible to report when it identifies an internal fault.
B - Control Algorithms or Decision-making	If there is no input during Go-Around, then the TPSC may select the high-power command.
C - Interpretation	TPSC incorrectly interpreted the physical position of the Power Levers.
D - Process Model	TPSC is updated incorrectly due to input that indicates that aircraft is not at Go-Around.
E - Controller States / Modes	If TPSC is in flight mode, it will continue to request the high-power command when there is no input.
F - Other Inputs	TPSC does not prevent low power command to FCPS when it has no electrical power.

Case Study – STPA Process

Step 4 – Identification of Loss Scenarios

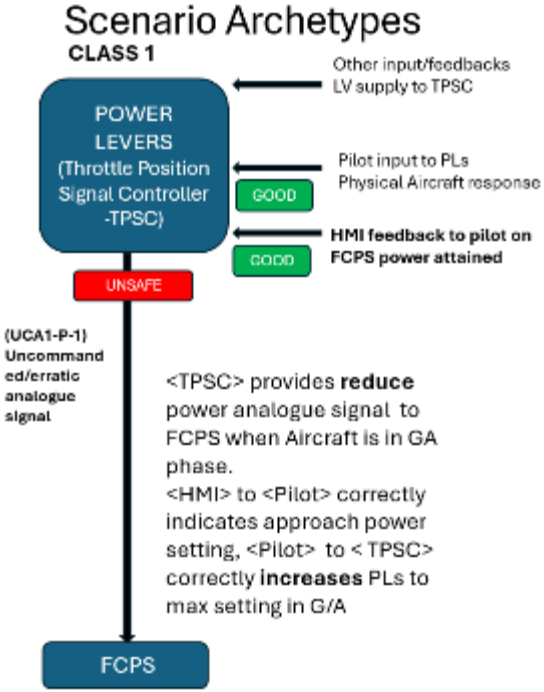
Archetype Scenario 1 at Go-Around	
A - Responsibilities	TPSC by design is responsible to report when it identifies an internal fault.
B - Control Algorithms or Decision-making	If there is no input during Go-Around, then the TPSC may select the high-power command.
C - Interpretation	TPSC incorrectly interpreted the physical position of the Power Levers.
D - Process Model	TPSC is updated incorrectly due to input that indicates that aircraft is not at Go-Around.
E - Controller States / Modes	If TPSC is in flight mode, it will continue to request the high-power command when there is no input.
F - Other Inputs	TPSC does not prevent low power command to FCPS when it has no electrical power.



Case Study – STPA Process

Step 4 – Identification of Loss Scenarios

Archetype Scenario 1 at Go-Around	
A - Responsibilities	The TPSC shall send a signal to the FCPS when it identifies an internal fault. The TPSC shall send a signal to the HMI when it identifies an internal fault to ensure that the pilot is aware of the issue.
B - Control Algorithms or Decision-making	The TPSC shall be capable to identify when aircraft is on flight.
C - Interpretation	If the FCPS power status conflicts with Throttle Position, the HMI shall inform the pilot.
D - Process Model	The TPSC shall have at least 2 different inputs to interpret if the aircraft is on flight.
E - Controller States / Modes	
F - Other Inputs	The TPSC shall be supplied with a stable low voltage power source, and this shall be available in emergency conditions.



Results

To evaluate the effectiveness of the STPA method, the traditional system safety approach identified airworthiness requirements of thrust response not > 5 seconds, aircraft ability to clear a 50 ft obstacle during Go-around

Regarding Rejected Take-off (RTO) flight phase, it is necessary to comply with the criteria established by the FTHWG (2017).

As mentioned before, in the traditional methods, the safety is based on the reliability of each system. Considering that the historical data of conventional propulsion systems, it is not expected that the fuel cell propulsion system will be capable to achieve a reliability lower than 1.00E-05. Therefore, based on the criteria summarised in Table 1, the thrust response shall be fast enough to keep the aircraft inside the runway.

Reviewing the scenario generation to prevent the TPSC sub system from providing erratic/un-commanded signals to the FCPS, it is possible to identify the following safety requirements thereby satisfying the Top-level safety constraint posed in step 4 .

Results

Proposed safety Requirements to satisfy Top-level safety constraints

SR1: The pilot input to PLs during a G/A shall be enough to ensure aircraft is capable to effectively clear a 50 ft obstacle.

SR2: The pilot input to PLs during an RTO shall be enough to ensure that the aircraft is capable of stopping inside the runway.

SR3: The TPSC shall send a signal to the FCPS and report any internal Fault to the HMI to ensure the pilot is situationally aware of the Thrust status in critical phases of flight.

SR4: The TPSC shall be supplied with stable LV source, and this shall be available in emergency conditions.

SR5: The TPSC shall not incorrectly interpret PL position, this shall be achieved by a comparison voting mechanism or having dual potentiometers channels for each power lever.

SR6: If the FCPS power status conflicts with PL positions, the HMI shall inform the Pilot of the conflict.

SR7: If TPSC experiences loss of LV it shall inform the HMI for pilot immediate actions in critical phases of flight.

Note: Pilot situational awareness of FCPS power status shall aid pilot Decision making to take timely corrective actions by shutting down the FCPS and rely on the conventional engine.

Conclusion

STPA is capable to generate more detailed requirements than the traditional approach, which is limited in the evaluation of certification requirements and system reliability to define the safety requirements.

It does not mean that the traditional safety approach does not have the potential to identify functional safety requirements, however it will only happen later in the development when there is more information about the systems and components, which means that it could lead to changes in the design. photo and add your own

Lessons from STPA application

- STPA effectively identifies hazards, unsafe control actions, and potential loss scenarios early on.
- Unlike traditional safety methods that rely on engineering judgment and focus on component failures,
- STPA emphasizes system interactions, control structures, and emergent behaviors.
- STPA allows for a thorough risk evaluation during the conceptual phase, prioritizing safety from the start.
- STPA offers accessibility and adaptability, making it usable for engineers at all levels.
- It helps identify unsafe control actions and defines control structures to explore alternative system architectures proactively.
- This flexibility aids in mitigating threats from emergent behaviors by converting safety constraints into system requirements.
- STPA identified intricate interactions involving the pilot, throttle position signal controller, Human-Machine Interface, and Fuel Cell Propulsion System, which may cause delayed or incorrect thrust responses in critical situations.
- This approach produced comprehensive safety requirements and uncovered potential gaps that traditional methods might miss..

Hello.

Jean Machado

Chief Systems & Safety Engineer

Cranfield Aerospace Solutions Ltd

Edem Tsei

System Safety & Human Factors Engineer

Cranfield Aerospace Solutions Ltd

Shaarujan Prabakaran

Systems Engineer

Cranfield Aerospace Solutions Ltd

Daniel Wilding

Senior Electrical Systems Design Engineer

Cranfield Aerospace Solutions Ltd

35th Annual INCOSE international symposium

hybrid event

Ottawa, Canada
July 26 - 31, 2025