Funded by UK Government

UK Civil Aviation Authority

STPA-based Safety Analyses of Hydrogen Refuelling and a Fuel Cell Electric Propulsion System

Contents

UK Civil Aviation Authority (CAA) Introduction

To successfully commence hydrogen electric aviation services, safe processes for hydrogen refuelling need to be produced, and a profound understanding of the risks and mitigations within the hydrogen fuel cell propulsion system must be obtained.

This is the rationale behind the work the Hydrogen Challenge is undertaking using the System Theoretic Process Analysis (STPA) technique. This report aims to update on the work undertaking towards this task thus far.

Hydrogen Challenge

Launched in November 2023 and supported by the Regulators' Pioneer Fund and now Department for Transport, the Hydrogen Challenge aims to:

- Identify safety risks and regulatory gaps linked to hydrogen in aviation
- Conduct targeted trials through our regulatory sandbox
- Collaborate with stakeholders

This work supports the broader Jet Zero Taskforce led by the UK Government.

We are addressing these issues through our challenge using a regulatory sandbox approach to make sure regulation is fit for purpose and reduce challenges associated with the potential introduction of hydrogen fuel.

Our Challenge will facilitate collaboration with industry and academia to improve understanding of hydrogen-related risks in aviation, identify gaps in policies, and propose new recommendations to develop net-zero policies.

This will allow for increased regulatory readiness, reduced risk of failure, and improved collaboration with the UK Civil Aviation Authority.

System Theoretic Process Analysis (STPA)

The UK CAA has recognised that it needs to augment its safety risk assessment and management tools to deal with ever-increasing complexity of aviation systems.

With hydrogen aircraft approaching technological and operational readiness, the UK aviation system has an opportunity to look at the future systemic risks and build an optimal system by design.

For this reason, the testing and validation of System Theoretic Process Analysis (STPA), an innovative hazard analysis tool, is being undertaken to validate the CAA-wide implementation of this technique.

STPA was devised by Professor Nancy Leveson of Massachusetts Institute of Technology, the need for which she sets out in her 2011 book, '*Engineering a Safer World'* (2011)[1]. The technique provides a *systematic* framework in which to analyse and control for system level hazards and risks, identifying and addressing risks that exist due to weaknesses in the interactions between actors in a system, and not just risks within its components. It was developed with the aviation sector in mind and has received the endorsement of other key regulatory bodies such as the United States' FAA[2].

Further detail regarding the theory of STPA is provided within a Technical Annex at the rear of this paper.

STPA and the Hydrogen Challenge

The Hydrogen Challenge provided many of the components required for an STPA to be undertaken in the British hydrogen aviation context. The Challenge contains safety professionals from a number of players in the industry, and aviation public servants. Many members of the group have technical backgrounds in hydrogen aviation

In the United Kingdom, WMG University of Warwick are recognised as a champion of the STPA technique, having produced numerous studies looking at connected and automated vehicles (Khastgir, 2021), and the UK response to COVID-19 (Chen, 2021). Through collaboration with WMG, we have been able to build upon the work completed looking into eVTOL operations and the key systemic hazards within two key hydrogen systems: refuelling and fuel cell electrical propulsion.

[1] https://direct.mit.edu/books/book-pdf/2280500/book_9780262298247.pdf
[2] Federal Aviation Administration, 2024, Evaluation of System-Theoretic Process Analysis (STPA) for Improving Aviation Safety DOT/FAA/TC-24/16

STPA Aims

The CAA's aims for this exercise were to:

1. Utilise STPA to undertake a hazard analysis for the Hydrogen refuelling and propulsion fuel cell.
2. Equip Hydrogen Challenge participants with knowledge of the key unresolved risks affecting their systems requirements, encompassing performance, design, airworthiness
3. Help the CAA form an evidence base understanding, ready to undertake a regulatory gap analysis of the current CS-23/25/E regulations

The Hydrogen Challenge elected to partner with WMG on this piece of work for which commenced in September 2025.

Given that this analysis looked at conventional operations as a means of identifying hydrogen systemic hazards, this paper is also an opportunity to look anew at the system-level risks associated with conventional refuelling processes.

Outcomes

The analysis has produced advice on aspects of the hydrogen aviation system requiring further consideration from a safety perspective, and suggestions on how to control for them. These are actionable by the:

- Regulator
- Operator
- OEM
- Infrastructure owner, e.g. aerodrome

From industry's perspective, these findings can assist in the development of Hydrogen Challenge stakeholders' Safety Management Systems, a key factor in addressing and meeting the Air Operations regulations in this country.

From the regulator's perspective, the report has undertaken a gap analysis whereby the WMG have presented safety factors brought to light by workshops and has

consulted with Subject Matter Experts to assess whether they constitute regulatory gaps.

As expected, this STPA review has elicited a significant number of potential issues for the regulator and industry to assess and consider.

Details on the nature of the findings and their prioritisation are provided within the main report.

The project has shown that STPA is capable of effectively analysing the advanced features of next generation aviation technologies and the complexity of proposed operational improvements. The findings elicited from this project demonstrate that STPA offers a thorough framework to identify limitations in existing regulations, policies, and procedures. The report validates the CAA's current approach to hydrogen aviation operations and reflects the current state of maturity of this emerging sector.

Further work/next steps

Using the results of this exercise

The CAA will now consider the findings of this exercise as part of our regulatory programme of works. Many of the determinations of the STPA have implications for the CAA's procedures, policies and regulations. Where regulatory changes are required, we will work with the CAA's Rulemaking team to begin the process of converting the study into aviation legislation. This process typically takes two years to complete but for new technologies this may take longer as technology emerges, evolves and changes as hydrogen is further understood and adapted for aviation applications.

Whilst this work has uncovered key safety considerations for the CAA as safety rulemaking material that may result in Requirements, Alternative Means of Compliance and/or Guidance Materials, the work has also produced a significant number of other lower priority considerations. These will be followed up collaboratively with industry, through the Hydrogen Challenge.

Further uses of STPA

The mapping of both the hydrogen aviation system and its integration with other users acts as a useful framework for emerging risks to be examined and controlled. In due course, these 'control structures' can be further developed to increase knowledge about a more diverse range of services and technologies. For instance, this study has only investigated the use of gaseous hydrogen, but what are the additional risks of using liquid or cryogenically compressed hydrogen?

The STPA can also be further developed to assess risks within parts of the system we have not yet explored. For instance, relationships with other system stakeholders including the wider supply chain.

From the perspective of industry, it is anticipated that the safety mitigations and causal factors generated will act as a basis for influencing further iterations of manufacturers' design processes, as well as helping them to mature their Safety Management Systems.

During the next phase of the Hydrogen Challenge, the CAA will continue to collaborate with all stakeholders of the hydrogen ecosystem to understand the systemic hazards involved, as they develop in readiness for passenger and commercial operations.

Executive Introduction

Problem Statement

Integrating an additional fuel into the current aviation ecosystem can pose new and emerging risks and hazards which require both identification and assessment.

Although regulatory bodies have been developing hydrogen-specific regulatory requirements, considering the complex interactions between different stakeholders' operation, the identified requirements cannot be claimed complete or fully assessed. Furthermore, due to the potentially large number of new or modified requirements that need to be implemented imminently, identifying and managing these new or modified requirements has brought more challenges. Current safety approaches fall short when analysing systems with emergent behaviour, especially multistakeholder systems with human-technology interactions.

Approach

To assess the risk posed by hydrogen operations, a systems thinking based safety analysis method, a Systems Theoretic Process Analysis (STPA), was chosen.

For successful results from an STPA, two types of contributing specialists are needed:

1) STPA experts.

2) Domain experts drawn from within the CAA as well as members of the wider reaching Hydrogen Challenge, encompassing industry and academia.

Summary of the findings

This initial STPA results identifies many Mitigations across the various stakeholders. Thus far the requirements exercise has generated many mitigations and scenarios in which Unsafe Control Actions (UCA) could manifest. Given the time constraints, our analysis of these UCA focused on those specific to the adoption of hydrogen as an aviation fuel, not aviation fuels in general. However, it is recognised that the STPA technique offers opportunities to uncover significant numbers of procedural and regulatory improvements to the refuelling processes for more conventional fuels.

The finalised mitigations represent targeted, high-impact opportunities for regulatory enhancement in various aspects of the ***Refuelling*** process such as:

- **Organisational performance**
- **Process review and improvement**

- **Assessment criteria**
- **Communication**
- **Training process**

  Automation and Simulation

Within the ***Fuel Cell Propulsion System***, the requirements are focused on:

- **Process review and improvement**
- **Assessment criteria**
- **Automation and Simulation**
- **Interoperation Dependency**

This project has shown that a STPA can effectively assess the sophisticated aspects of emerging aviation technologies and the associated intricacies of planned operational improvements. By revisiting current established regulations and practices a STPA could be of significant benefit in identifying areas for improving current procedures and safety practices.

Key recommended actions

The following actions are recommended as outcomes of this study, in order to respond to the UCAs, causal factors and safety mitigations this exercise has generated:

1. For both the fuel cell propulsion and refuelling systems, it needs to be determined whether both systems' Unsafe Control Actions and Causal Factors constitute regulatory 'gaps'. This exercise needs to be conducted in collaboration with Subject Matter Experts at the CAA.
2. CAA to incorporate these findings in the development of future hydrogen aviation regulations encompassing activities such as performance, design, airworthiness.
3. From the perspective of industry, it is anticipated that the safety mitigations and causal factors generated will influence further iterations of manufacturers' designs, as well as helping them to mature their Safety Management Systems. The CAA will continue to collaborate with all stakeholders of the hydrogen ecosystem to understand the systemic hazards, as they develop their products for passenger and commercial operations.

Project Overview

About STPA

System Theoretic Process Analysis (STPA) is a top-down approach based on the conceptual accident causality model called System Theoretic Accident Model and Processes (STAMP). It treats accidents as a Control Problem (CP) instead of a failure problem and it prevents accidents by enforcing constraints on the behaviour of the system. A STPA considers a diverse range of causal factors of the hazardous interactions, including flawed control algorithms due to flaws in their specifications, communication errors, and delays, conflicted controls, processing delays, misinterpretations of the received data or signals, etc. The conventional STPA approach involves four distinct steps.

Step 1: Define purpose of the analysis

STPA starts by identifying any losses which are unacceptable to the stakeholders and system-level hazards. The system boundary is also defined in this step. The system boundary defines the range of ownership and analysis – i.e., the components outside the system boundary are not accessible to the designer for any potential upgrades required, and the components within the boundary can be appropriately managed or redesigned if the analysis outcome suggests.

Step 2: Model the Control Structure

The subsequent step involves developing a system model referred to as a control structure. The control structure consists of hierarchical functional blocks illustrating the **functional** interactions between the system components by representing the system as a series of feedback control loops. Each control loop consists of a controller that provides control actions (CA) to control some processes and enforce constraints on the behaviour of the controlled process. The control algorithm represents the controller's decision- making process, it determines the control actions to provide. Controllers also have process models that represent the controller's internal beliefs (which may include beliefs about the process being controlled or other relevant aspects of the system or the environment), used to make decisions.

Step 3: Identify Unsafe Control Actions (UCA)

After identifying Control Actions (CA) in the control structure, each CA is further analysed to identify how the CA would manifest into an Unsafe Control Action (UCA). Depending on the context of providing a CA, it could lead to one or multiple system-level hazards, which in turn lead to the losses (identified in Step 1: (Define purpose of the analysis)). If a CA were always unsafe, then it would never be included in the system design. The CA is analysed in four categories to identify UCAs:

- **Not providing** the CA leads to a hazard.
- **Providing** the CA **incorrectly** or when not needed leads to a hazard.
- **Providing** the CA **too early** or **too late** or **in the wrong order** leads to a hazard.
- **Providing** the CA **too long** or **stopping providing the CA too soon** leads to a hazard.

Step 4: Identify Loss Scenarios

Once the UCAs are identified for all the control actions in the control structure, possible Loss Scenarios, which describe the Causal Factors (CFs) that can lead to the UCAs, are identified by analysing the specific control loops of the Control Actions. For a UCA to occur, the process model of the controller has a belief based on which it believes that the CA it is directing is safe when it is unsafe. The causes of such beliefs can be identified based on two types of Loss Scenarios – i.e., 'Type A' and 'Type B'. Type A Loss Scenarios mainly explain what triggers the CAs to be unsafe. Type B Loss Scenarios explain how correct CAs are not executed or are improperly executed, leading to UCAs. Once the Loss Scenarios and their corresponding Causal Factors are analysed, Mitigations are then defined for prevention or mitigation of these Causal Factors.

STPA for Hydrogen Methodology

The STPA project comprised of two parts:

- Hydrogen refuelling system
- Hydrogen fuel cell electric propulsion system

The objective was to analyse existing aviation regulations operations as a starting point and identify the variations when applied to the two hydrogen systems to be assessed.

This was followed by the identification of UCAs, highlighting those requiring consideration and mitigation strategies incorporating stakeholders' inputs during one-to-one workshops, and ultimately, the derivation and refinement of mitigations. By integrating experts' inputs at each phase and focusing on critical UCAs and Mitigations, the process ensured that requirements were effectively identified and addressed, supporting the safe deployment of hydrogen operations.

The problem statement and objectives of the project are listed below.

Problem Statement

Introduction of hydrogen operations will require input from multiple stakeholders (i.e., technology, policy, operations, infrastructure etc). Therefore, new and amended interactions may take place in the new operational environment, which will lead to emergent behaviours in the ecosystem. These emergent behaviours pose a risk both to the current ways of operating, and may introduce new risks as the ecosystem develops, particularly at scale. Applied research is therefore required to inform future policy and operational development to manage the safe introduction of hydrogen operations within a challenging environment.

Objectives and Planned Actions

Objective 1a: to map the control structures for the hydrogen refuelling to enable the exchanges of information between system components to be examined

Objective 1b: to map the control structures for the hydrogen fuel cell propulsion system to enable the exchanges of information between system components to be examined

Objective 2: To conduct analysis of unforeseen and unexpected interactions, which may compromise the stability and safety of the hydrogen ecosystem.

- **Action 2.1:** To conduct analyses of UCAs for the hydrogen refuelling and fuel cell propulsion systems.

Objective 3: To develop mitigations to prevent unsafe interactions between system components and equipment types, thereby mitigating emergent risks.

- **Action 3.1:** To identify scenarios leading to unsafe interactions between stakeholders.

Results Summary

Following the standard STPA process, in STPA Step-1, the System Boundary and five Losses were defined. The Losses covered both safety-critical (i.e., human loss and material loss) and business-critical losses (i.e., mission loss, consumer demands loss, and business goal loss). Throughout the project, the results created by the STPA experts were reviewed by domain experts through both in-person workshops and virtual meetings.

The domain experts came from a diverse range of backgrounds - this included the UK Aviation Regulator (CAA), Operators and Manufacturers.

In Step-2 Control Structures were created to capture the exchanges of information between hydrogen refuelling and fuel cell propulsion system components.

In Step-3, 102 UCAs were identified in total for hydrogen refuelling and 97 for the hydrogen fuel cell propulsion system.

Following Step-4, 35 Causal Factors (CFs) were identified for hydrogen refuelling and 47 for the hydrogen fuel cell propulsion system. 30 Mitigations were proposed to prevent or mitigate these hydrogen refuelling CFs and 110 for the hydrogen fuel cell propulsion system CFs.

Results of the STPA Analysis: Refuelling

Assumptions

This document is written with no assumptions of individual or combined limitations. This iteration of the STPA activity will collate and define the top-level limitations specific to the installation of a gaseous hydrogen propulsion system.

The limitations are listed, along with the associated parameters and the defined operating criteria. Where a limitation is affected by more than one component / equipment then the resulting top-level limitation is used with the rationale that this is the most conservative of the combination for this particular STPA study.

The STPA for the first phase of the analysis of hydrogen operations was based on the following assumptions and limitations:

For the hydrogen refuelling process:

- Aerodrome/airport only
- Certification Specification - 23 (CS-23) type aircraft only
- Refuelling vehicle (tanker) and refuelling nozzle interface only
- Aircraft pressure vessel not included at this stage of the analysis
- Fuel nozzle sized to permit the flow of 2 tonnes of Hydrogen in approx. 20 minutes after initialisation.

Assumptions about hydrogen features/characteristics:

- Gaseous hydrogen at this stage.
- Nominal 350 bar (G350).
- Not cryogenic, not liquid.
- No hydrogen leak detection systems considered at this time.
- No piping – although there will be piping within a full-scale system.

Assumptions about the Operating Environment:

- A service area located in an aerodrome/airport area, namely an apron. An outside, unroofed and unwalled naturally vented area.
- Hydrogen, if ignited on most occasions deflagrates and tends to burn upwards in a low intensity cloud.

STPA Step-1 Purpose of the Analysis

As part of STPA step 1, the losses that were unacceptable to stakeholders were identified. An initial list of losses was defined by the STPA analysts based on prior experience. These losses were then reviewed and ranked/prioritised by the stakeholders, based on their stake in the system, i.e. what they valued and what their goals were.

Table shows the list of ranked losses. Safety-critical losses (example – L1) were ranked high while non-safety critical or business-critical losses (example – L4, L5) were ranked low.

Loss-ID	Losses	Ranking
L-1	**Human Loss**: Loss of life or injury to 1st, 2nd or 3rd parties	1
L-2	**Material Loss:** Loss of or damage to the aircraft or the surrounding item/property/infrastructure/environment	2
L-3	**Mission Loss**: Loss of transportation mission	3
L-4	**Political Risk/Consumer Demands Loss**: Loss of customer satisfaction or public confidence in fuel cell-powered aircraft	4
L-5	**Ownership/Business Goal Loss:** Loss of the business goal of the Aircraft Operator	5

Table 1 List of Losses

Based on discussions with the stakeholders, the system boundary was also defined in this step. The system under analysis comprised of the Regulator, Operators and Manufacturers.

STPA Step-2 (Model the Control Structures (CS))

The diagram below is colour coded according to the differing levels of the Control Structure (see key within diagram).

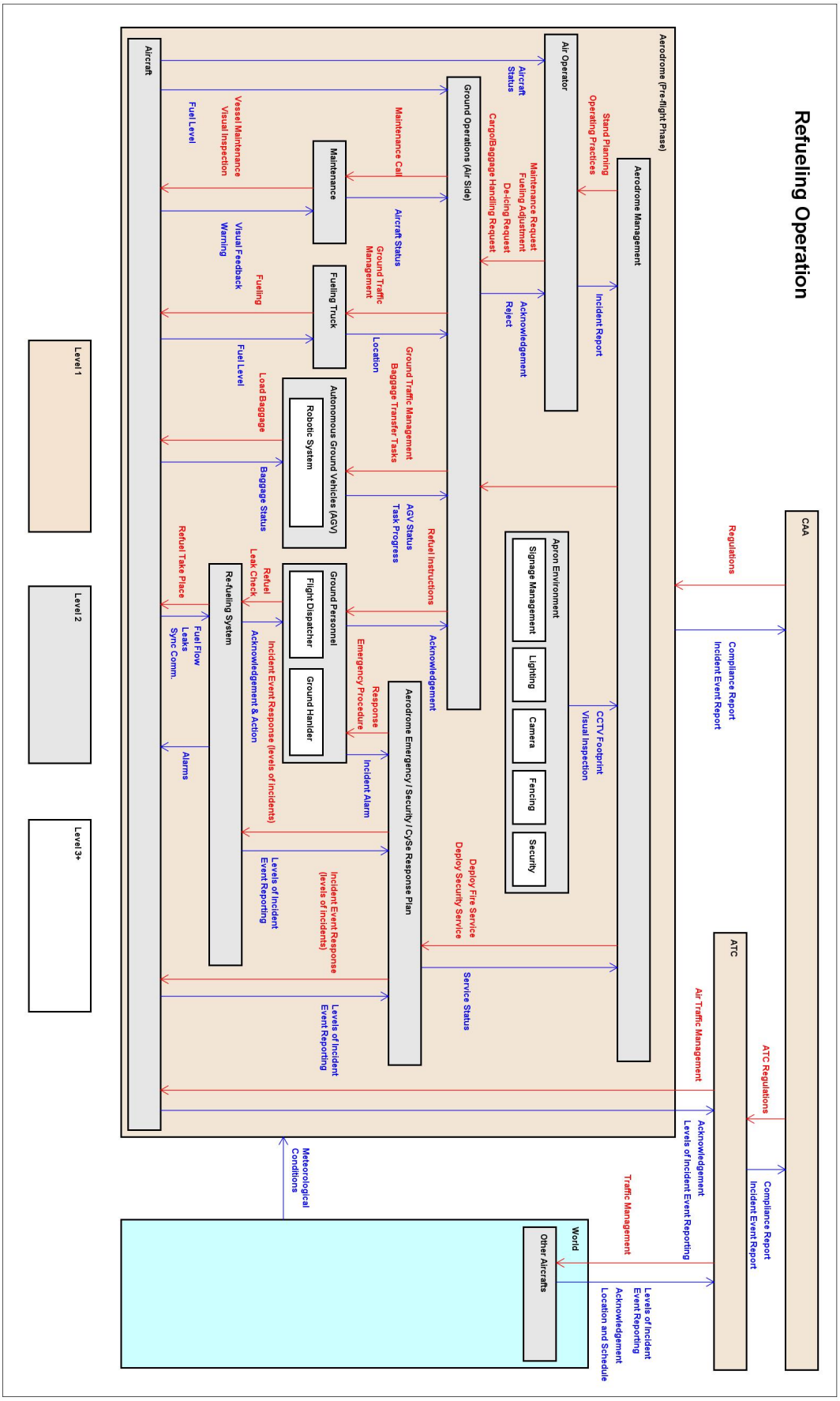

Figure 1 Control Structure for Refuelling

STPA Step-3 (Identify Unsafe Control Actions)

After the creation of the Control Structure (CS), Unsafe Control Actions (UCAs) were identified for each of the Control Actions (CA) in the Control Structure, as part of STPA Step-3.

There were 102 UCAs identified in total across the Control Structures. As the number of UCAs identified was high, it was necessary to prioritise the UCAs to streamline the activities for the next phase (identification of loss scenarios and mitigations) and focus on those specific to hydrogen refuelling (not refuelling in 'general').

Each UCA was assigned a unique ID (as indicated by the 'UCA-ID' column in Table 4) depending on the control structure/phase the corresponding UCAs were covered in.

UCA IDs are structured as follows: UCA X.Y.Z where:

- X denotes the number of the CA.
- Y represents the type of UCA, where:
  - Type 1: The CA is not provided
  - Type 2: The CA is provided incorrectly
  - Type 3: The CA is provided when not needed
  - Type 4: The CA is provided too early
  - Type 5: The CA is provided too late
  - Type 6: The CA is provided too long
  - Type 7: The CA is provided too short
- Z denotes the number of the UCA identified for the CA and same type.

For example, the **UCA-24.2.1** in Table 2 is the first UCA (i.e., Z = 1) of the CA number X = 24 (i.e. 'Aerodrome Emergency / Security / Cybersecurity Response Plan') from with type 2 UCA - i.e., Y = 2 (The CA is provided incorrectly).

In this project, the UCAs were directly linked to losses instead of hazards, deviating from the typical STPA process. This approach made it easier for SMEs who may not be STPA experts to comprehend the potential consequences of occurrence of UCAs.

The UCAs linked to each stakeholder were grouped, reviewed (through in person workshops and virtual meetings with the Regulator, Operators and Manufacturers) and then updated.

Refuelling

UCA-ID	UCA Description	Link to Losses
UCA24.2.1	Aerodrome Emergency / Security / Cybersecurity Response Plan provides an inadequate Emergency Procedure when the aerodrome has not established emergency procedures for H2 related incident (e.g., GH2 leak from high-pressure storage cylinder, flash fire near the storage tank etc).	**L-all**
UCA26.5.1	Aerodrome Emergency / Security / Cybersecurity Response Plan provides Incident Event Response (e.g., disconnect or disable the equipment) too late when the H2 refuelling is taking place, and there is a fire/leakage incident nearby in the aerodrome.	**L1,2**
UCA27.4.1	ATC provides the Air Traffic Management too early (which is also incorrect at that stage) when the aircraft has not reached the stage to implement the ATM.	**L-all**
UCA16.7.1	Fuelling Truck stops providing Fuelling too soon when the fuel level is not enough for the next flight.	**L3, L5**
UCA4.5.1	H2 system is repaired too late that is a reactive repair (might lead to fire risks).	**L2**
UCA1.2.2	Air Operator provides incorrect Refuel Request (incorrect quantity (volume, mass, weight), grade, which is not aligned with the Aircraft Requirement.	**L2, L3, L5**

Table 2 Some of the Refuelling UCAs identified as part of Step-3

STPA Step-4 (Identify Loss Scenarios)

In this step, all UCAs from the previous step (Step-3) were analysed to identify the potential Causal Factors that could lead to the occurrence of these UCAs. Later, Mitigations were proposed to prevent or mitigate these Causal Factors.

The Step-4 analysis resulted in the identification of Causal Factors. Mitigations were proposed to prevent or mitigate these Causal Factors.

As domain experts, the stakeholders (Regulator, Operators and Manufacturers) reviewed these potential Causal Factors and Mitigations.

Table 3 presents the statistics of the STPA Step-4 analysis results.

	Total No. of Causal Factors	Total No. Of Mitigations
Refuelling	35	30

Table 3 Statistics of STPA Step-4 Results

An extract of the Step-4 results showing the Mitigations proposed to address the various types of Causal Factors (organisational issues, communication errors, missing Feedback/information, inadequate Control Algorithms, delayed Feedback/information etc.) that could lead to UCAs associated with different stakeholders (Operator, Regulator, and Licensed Aerodrome), is presented in Table 4.

UCA Description	Causal Factors	Mitigations
Re-fuelling System providing refuel takes place incorrectly (e.g., malfunctioning, pressure regulator valve not open) which is not aligned with the Ground Personnel's intention.	Due to the incorrectly specified fuel nozzle. Due to incorrect Sync. Communications feedback (sensor, wiring or connection failure).	Clear colouring/labelling of different types of nozzles; Anti-fault design of nozzle types to ensure wrong nozzle types cannot be fitted in (Mechanical interlock) Electrical Interlock: the system shall detect the wrong fuel and provide warning automatically. Ensure that there is a physical, visual, pressure

UCA Description	Causal Factors	Mitigations
		gauge check available within the Re-fuelling System. Refuelling stops when the refuelling pressure is detected.
Aerodrome Emergency / Security / Cybersecurity Response Plan provides Responses too late (> tbd min) when the aerodrome has not established emergency procedures for H2 related incident that has already occurred.	Inadequate procedures (untested, unwritten)	Procedures must be properly documented and tested (identify gaps and improved) periodically. The procedures must then be shared and delivered to relevant personnel by Aerodrome Emergency / Security / Cybersecurity Response Plan Planning Group.
	Communication failure (cascaded airfield communication system, which can be automatic) from Aerodrome management - i.e., not told in the first place	Maintenance testing on the comm. Systems (annual basis). Contingency plans enforced.
	Miscommunication to/from ATC	Maintenance testing on the communications systems (annual basis). Contingency plans enforced.
	Delayed response due to major traffic congestion in the airport	Dedicated emergency response station nearby to be set up. PDA (Pre-Determined-Attendance) Maintenance testing on the comm. Systems (annual basis). Contingency plans

UCA Description	Causal Factors	Mitigations
		enforced.
	Communication delay between the Aerodrome management and the AE	Advanced notification so that additional/external resources can be called at the earliest possible time. Test the communication (functional testing) on a monthly basis.
	Lack of resources / overwhelmed Aerodrome Emergency / Security / Cybersecurity Response Plan (External for fire, ambulance delayed response) service due to previous response to other major incident.	Updated reports for traffic, accidents.
Re-fuelling System provides Refuel incorrectly (e.g., malfunctioning, pressure regulator valve not open) which is not aligned with the Ground Personnel's intention.	Due to the incorrectly specified fuel nozzle.	Clear colouring/labelling of different types of nozzles;
	Due to incorrect sync.	Anti-fault design of nozzle types to ensure wrong nozzle types cannot be fit in (Mechanical interlock)
	Communications feedback (sensor, wiring or connection failure).	Electrical Interlock: the system shall detect the wrong fuel and provide warning automatically. Ensure that there is a physical, visual, pressure gauge check available within the Re-fuelling System.

UCA Description	Causal Factors	Mitigations
		Refuelling stops when the refuelling pressure is detected.

Table 4 An extract from the Refuelling STPA Step-4 Results

Results of the STPA Analysis: Fuel cell propulsion system

Assumptions

This document is written with no assumptions of individual or combined limitations. This iteration of the STPA activity will collate and define the top-level limitations specific to the installation of a gaseous hydrogen propulsion system.

The limitations are listed, along with the associated parameters and the defined operating criteria. Where a limitation is affected by more than one component / equipment then the resulting top-level limitation is used with the rationale that this is the most conservative of the combination for this particular STPA study.

The STPA for the first phase of the analysis of hydrogen operations was based on the following assumptions and limitations:

Assumptions about hydrogen features/characteristics:

- Gaseous hydrogen at this stage.
- Nominal 350 bar (G350).
- Not cryogenic, not liquid.
- No hydrogen leak detection systems considered at this time.
- No piping – although there will be piping within a full-scale system.

Assumptions about the Operating Environment:

- A service area located in an aerodrome/airport area, namely an apron. An outside, unroofed and unwalled naturally vented area.
- Hydrogen, if ignited, on most occasions deflagrates and tends to burn upwards in a low intensity cloud.

Assumptions about hydrogen features/characteristics:

- Hydrogen type ambivalent at this time – assumed hydrogen is conditioned to suit fuel cell requirements at this stage.

Assumptions about the Operating Environment:

- Electric compressor to provide correct air volume for fuel cell reaction requirements at sea level only.
- Fuel cell based at sea level. Considerations for use at altitude to be addressed in further iterations. (variable air compressor ratio: altitude (air density).

STPA Step-1 (Define Purpose of the Analysis)

As part of STPA step 1, the losses that were unacceptable to stakeholders were identified. An initial list of losses was defined by the STPA analysts based on prior experience. These losses were then reviewed and ranked/prioritised by the stakeholders, based on their stake in the system, i.e. what they valued and what their goals were.

Table shows the list of ranked losses. Safety-critical losses (example – L1) were ranked high while non-safety critical or business-critical losses (example- L-4, L5) were ranked low.

Loss-ID	Losses	Ranking
L-1	**Human Loss**: Loss of life or injury to 1st, 2nd or 3rd parties	1
L-2	**Material Loss:** Loss of or damage to the aircraft or the surrounding item/property/infrastructure/environment	2
L-3	**Mission Loss**: Loss of transportation mission	3
L-4	**Political Risk/Consumer Demands Loss**: Loss of customer satisfaction or public confidence in fuel cell-powered aircraft	4
L-5	**Ownership/Business Goal Loss:** Loss of the business goal of the Aircraft Operator	5

Table 5 List of Losses

Based on discussions with the stakeholders, the system boundary was also defined in this step. The system under analysis comprised of the Regulator, Operators and Manufacturers.

STPA Step-2 (Model the Control Structures (CS))

The diagram below is colour coded according to the differing levels of the Control Structure (see key within diagram).

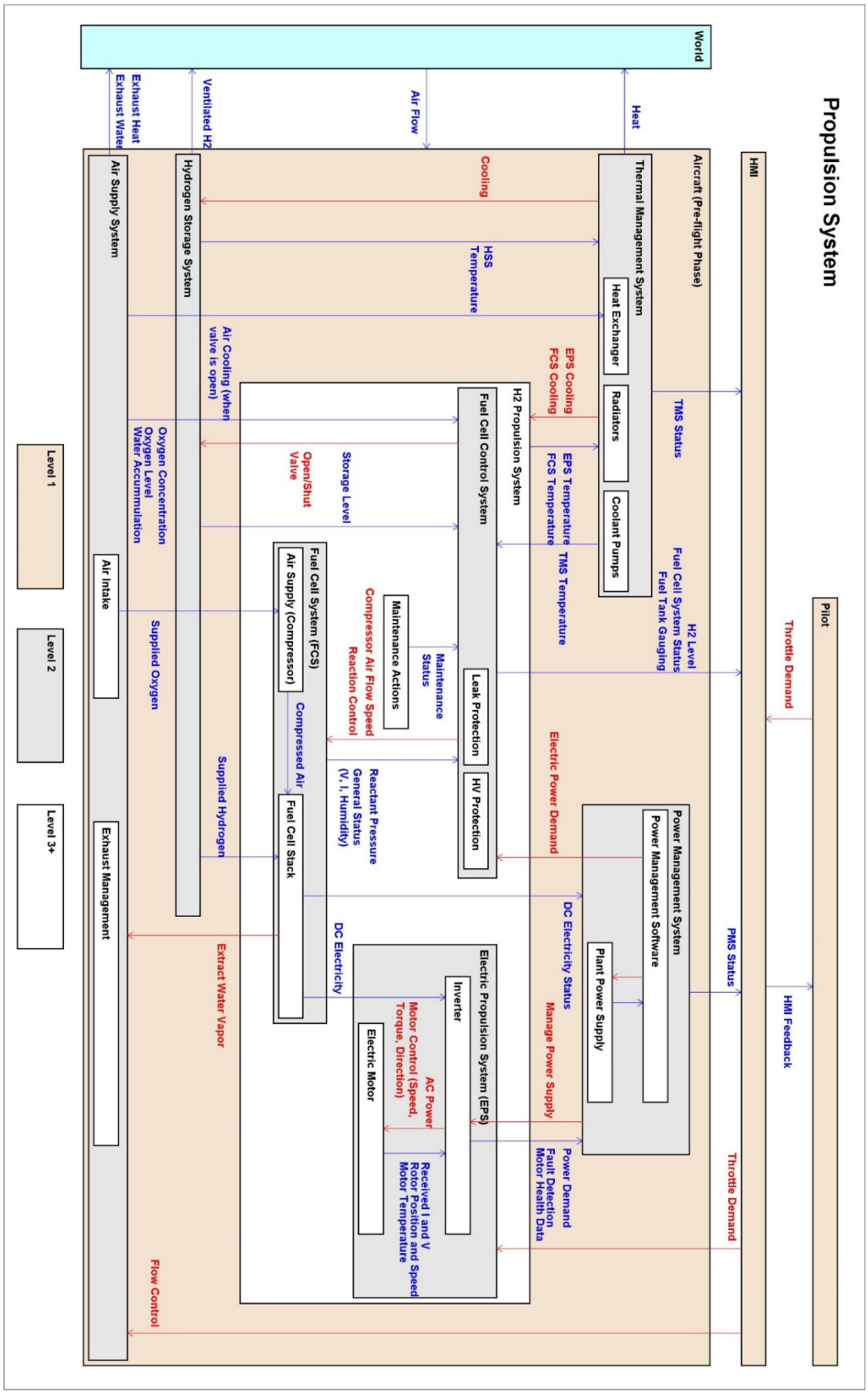

Figure 2 Control Structure for fuel cell propulsion system

STPA Step-3 (Identify Unsafe Control Actions)

After the creation of the Control Structure (CS), Unsafe Control Actions (UCAs) were identified for each of the Control Actions (CA) in the Control Structure, as part of STPA Step-3.

There were 97 UCAs identified in total across the Control Structure. As the number of UCAs identified was high, it was necessary to prioritise the UCAs to streamline the activities for the next phase (identification of loss scenarios and mitigations) and focus on those specific to hydrogen fuel cells (not fuel cells in 'general').

Each UCA was assigned a unique ID (as indicated by the 'UCA-ID' column in Table 4) depending on the control structure/phase the corresponding UCAs were covered in.

UCA IDs are structured as follows: UCA X.Y.Z where:

- X denotes the number of the CA.
- Y represents the type of UCA, where:
  - Type 1: The CA is not provided
  - Type 2: The CA is provided incorrectly
  - Type 3: The CA is provided when not needed
  - Type 4: The CA is provided too early
  - Type 5: The CA is provided too late
  - Type 6: The CA is provided too long
  - Type 7: The CA is provided too short
- Z denotes the number of the UCA identified for the CA and same type.

For example, the **UCA-12.1.1** in Table 6 is the first UCA (i.e., Z = 1) of the CA number X = 12 (i.e. 'Power Management Software') with type 2 - i.e., Y = 1 (the CA is not provided).

In this project, the UCAs were directly linked to losses instead of hazards, deviating from the typical STPA process. This approach made it easier for SMEs who may not be STPA experts to comprehend the potential consequences of occurrence of UCAs.

The UCAs linked to each stakeholder were grouped, reviewed (through in person workshops and virtual meetings with the Regulator, Operators and Manufacturers) and then updated.

Fuel cell propulsion system

UCA-ID	UCA Description	Link to Losses
UCA12.1.1	Power Management Software (PMS) does not provide Electric Power Demand when the reactant pressure is abnormal (leading to damage of the subsystem).	**L1, L2**
UCA11.5.3	Power Management Software manages power supply too late when the Pilot is engaging the powertrain system to avoid collision with other aircraft on the ground.	**L1, L2**
UCA9.2.2	Pilot provides Throttle Demand excessively when manoeuvring around the airport.	**L1, L2**
UCA12.5.1	Power Management Software provides Electric Power Demand too late when the push back/reversing command has been issued, thus blocking the passenger terminal gate.	**L3,4,5**
UCA3.2.1	Thermal Management System (TMS) provides incorrect Fuel Cell System (FCS) Thermal Management (excessive/insufficient) when FCS temperature is inadequate.	**L2, L3**
UCA4.1.1	TMS does not provide FCS Thermal Management when TMS fails and the FCS is outside the acceptable operational temperature limit (too hot or too cold - this also depends on where the aircraft is operating).	**L2, L3**

Table 6 Some of the Fuel Cell Propulsion System UCAs identified

STPA Step-4 (Identify Loss Scenarios)

In this step, all UCAs from the previous step (Step-3) were analysed to identify the potential CFs that could lead to the occurrence of these UCAs. Later, Mitigations were proposed to prevent or mitigate these CFs.

The Step-4 analysis resulted in the identification of Causal Factors. Mitigations were proposed to prevent or mitigate these Causal Factors.

As domain experts, the stakeholders (Regulator, Operators and Manufacturers) reviewed these potential Causal Factors and Mitigations.

Table 7 presents the statistics of the STPA Step-4 analysis results.

Phase	Total No. of Causal Factors	Total No. Of Mitigations
Fuel cell propulsion system	47	110

Table 7 Statistics of STPA Step-4 Results

An extract of the Step-4 results showing the Mitigations proposed to address the various types of Causal Factors (organisational issues, communication errors, missing Feedback/information, inadequate Control Algorithms, delayed Feedback/information etc.) that could lead to UCAs associated with different stakeholders (Operator, Regulator, and Licensed Aerodrome), is presented in Table 8.

UCA Description	Causal Factors	Mitigations
Thermal Management (TMS) System does not provide Fuel Cell System (FCS) Thermal Management when Thermal Management System fails and the FCS is outside the acceptable operational temperature limit (too hot or too cold - this also depends on where the aircraft is operating).	The TMS software has errors in the design and does not provide the CA. The TMS misinterprets the feedback FCS Temperature The TMS misinterprets the feedback Coolant Flow The TMS hardware fails and was unable to provide the CA.	The software Verification and Validation (V&V) shall be strictly aligned with the DO178 and DO326, and with redundancy systems available. The software error shall be visualized and notified to relevant stakeholders. Redundancy software/hardware (SW/HW) with different design architectures. There should be a mechanism to collect and summarize the data from multiple inputs to identify any faulty outputs. This should then notify relevant stakeholders. Redundancy (SW/HW) with different design architectures. There should be a mechanism to collect and summarize the data from multiple inputs to identify any faulty outputs. This should then notify relevant stakeholders. The HW V+V shall be strictly aligned with the DO-254, DO160, ARP4754b, and ARP4761 The HW error shall be visualized and notified to relevant stakeholders.
TMS provides FCS Thermal Management (heat up/cool down) too late after the FCS has exceeded the operating temperature limits.	FCS Low Temperature produces reduced power with potential shutdown when limits are reached. The FCS LT is slow to respond to the data with potential	R1: Redundancy (SW/HW) with different design architectures. R2: Asynchronous BUS protocols to resolve timing misalignment.

UCA Description	Causal Factors	Mitigations
	shutdown limits are reached.	R1: There should be a mechanism to collect and summarize the data from multiple inputs to identify any faulty outputs. This should then notify relevant stakeholders. R2: Multiple paths of BUS architecture for parallel data communication, with voting feature incorporated. R1: Redundancy (SW/HW) with different design architectures. R2: Asynchronous BUS protocols to resolve timing misalignment." R1: There should be a mechanism to collect and summarize the data from multiple inputs to identify any faulty outputs. This should then notify relevant stakeholders. R2: Multiple paths of BUS architecture for parallel data communication, with voting feature incorporated.
Pilot does not provide Throttle Demand when the permission has been granted, and the flight is scheduled to depart soon.	Pilot-HMI issue (mode confusion) Pilot misunderstood the communication. Pilot navigation error at the airport. Subsequent aircrafts are delayed.	Type training for pilots (rating and refresher courses). Enforce 'acknowledgement'. To use ground radar. Improve the road sign design.

Table 8 An extract from the Fuel Cell Propulsion System STPA Step-4 Results

Conclusion

The current aviation system requirements, encompassing performance, design, airworthiness, are based on a mature regulatory framework and ruleset.

Integrating a novel technology like Hydrogen into the existing system will create emergent behaviours. The existing system design and regulations may not be designed to safely react to such emergent behaviours, thus posing risk to hydrogen operations and their sharing of the aerodrome with existing users. With OEMs forecasting hydrogen operations in the near term (years), there is an urgent need for both identifying and assessing the risk posed by such emergent behaviours.

Traditional hazard analysis and risk management techniques, most of which were created decades ago for the less complex and linear systems of that time, cannot effectively handle the complex systems with multi-stakeholder interactions being developed today. More powerful and a systems thinking based approach to hazard analysis is needed. Systems-Theoretic Process Analysis is a relatively new type of hazard analysis technique based on a very different type of paradigm and assumptions about the causes of accidents.

In contrast to traditional safety analysis approaches which focus on component faults and failures driving by reliability assessments, STPA focusses on non-linear, indirect, and feedback relationships among events and actors.

In this project, safety analysis using STPA was conducted for hydrogen operations, identifying loss scenarios, causal factors, unsafe control actions and their corresponding mitigations to prevent or mitigate them. Many of the scenarios identified in this report include more than just component failures. Therefore, many of the Mitigations identified by the STPA analysis go beyond reliability and relate to the behaviour of system components (both human controllers and automation) and the information that those components receive and exchange. The initial STPA output yielded 30 mitigations to prevent or mitigate hydrogen refuelling Causal Factors and 110 for the hydrogen fuel cell propulsion system Causal Factors.

As the next step, the mitigations which have been identified as gaps from this analysis need to be developed into practical, implementable actions for each relevant stakeholder in the form of regulatory and policy updates, operational instructions, and practical guidance. For industry, it is anticipated that the safety mitigations and causal factors generated will act as a basis for influencing further iterations of manufacturers' design processes, as well as helping them to mature their Safety Management Systems.

Finally, this project has demonstrated that STPA is capable of effectively analysing the advanced features of the next generation aviation technologies and the complexity of the proposed operational improvements. The findings from this project demonstrate that STPA offers a thorough framework to identify shortcomings in existing regulations,

policies, and procedures. This approach helps to establish a robust safety management system that proactively addresses risks and evolves in response to the challenges posed by new technologies.

Technical Annex

System-Theoretic Process Analysis (STPA)

The standard STPA methodology developed by Professor Nancy Leveson of Massachusetts Institute of Technology, consists of four steps (Leveson N. G., 2018) as shown in Figure :

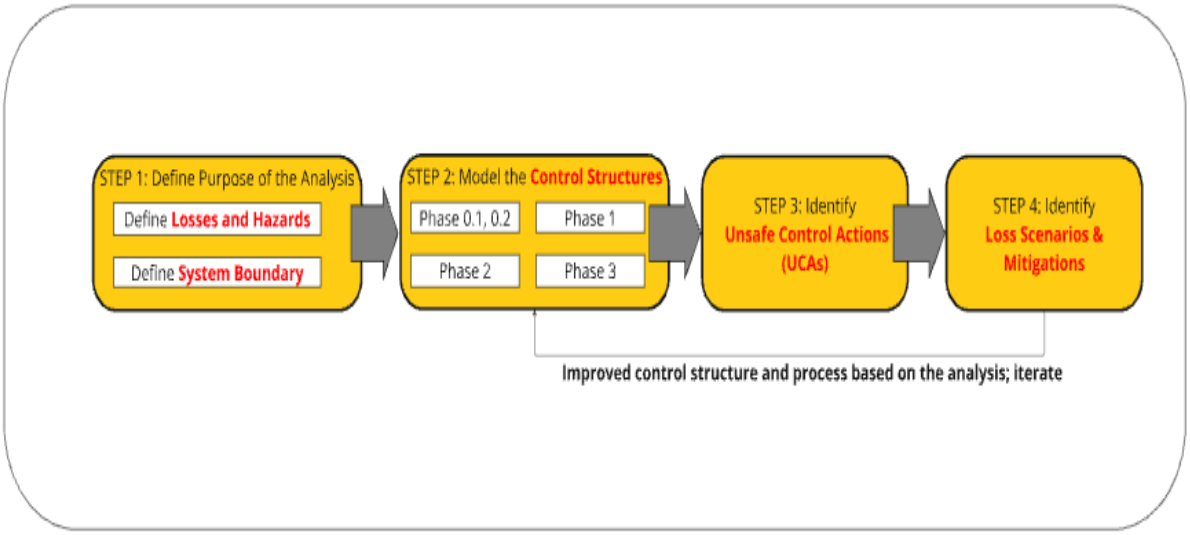

Figure 3 Overview of the STPA methodology

Step 1: Define Purpose of the Analysis

The initial step of the analysis involves identification of the objective of the analysis. Will STPA be limited to traditional safety objectives, such as preventing human fatalities, or will it also be used to address broader concerns like security, privacy, system performance, and other critical properties? Clearly defining the system to be analysed and establishing its boundaries is essential. This foundational step ensures clarity about what is included in the analysis and what lies outside its scope. This phase involves addressing several core questions to ensure a complete understanding of the analysis objectives. A crucial component of this stage is identifying potential losses and hazards, as these elements guide the focus and direction of the analysis.

This part involves carefully identifying any possible negative outcomes or adverse events that might arise due to hazards within the system. A *loss* involves something of value to the stakeholders such as human life or injury, pollution, loss of mission, reputation, or property which are unacceptable to stakeholders (Leveson N. G., 2018).

A basic approach to identifying losses might involve steps such as:

- Identification of stakeholders such as customers, users, operators, etc.

- Identification of stakes in the system such as their value, for example, human life, transportation, aircraft fleets, etc., and their goals, for example, providing medical treatments, maintaining aircraft fleets, providing transportation, etc.
- Finally, convert those values into loss. For example, loss of human life, aircraft, transportation, etc

Some examples of losses that users aim to prevent are:

- L-1: Loss of life or injury.
- L-2: Loss of or damage to system or vehicle.
- L-3: Loss of or damage to others in the environment.
- L-4: Loss of mission such as (transportation, defence, surveillance, etc.).
- L-5: Loss of client satisfaction.
- L-6: Environmental loss

The losses identified in STPA can be safety-critical (e.g. Loss of life or injury) or non-safety-critical or business losses (e.g. Loss of client satisfaction). Losses could also be from the environment level which could be out of the system designer's perspective. There should be documentation where explicitly excluded losses are mentioned and their exclusion justified. After the losses of concern in the analysis are identified, the subsequent step is to define the hazards related to these losses. A hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss. Typically, a hazard can result in multiple losses, and it's essential to link each hazard to its corresponding losses. This connection is usually indicated in brackets following the hazard description (Leveson N. G., 2018).

Listed below are some examples of hazards.

H-1: Aircraft violates minimum separation requirements in flight [L-1, L-2, L-4, L-5]

H-2: Airframe integrity of the aircraft is lost [L-1, L-2, L-4, L-5]

H-3: Aircraft leaves designated taxiway, runway, or apron on the ground [L-1, L-2, L-5]

Step 2: Model the control structure

The subsequent step involves developing a system model referred to as a control structure. In systems theory, components are organised in hierarchical levels: every level controls the level below. The behaviour in the lower level can be controlled or limited by components at higher levels. The control structure illustrates the functional interactions between the system components by representing the system as a series of feedback control loops.

In general, a hierarchical control structure contains at least five types of elements:

- Controllers
- Control Actions
- Feedback
- Other inputs to and outputs from components (neither control nor Feedback)
- Controlled Processes

Typically, a controller issues Control Actions (CA) to control a process, utilising feedback signals to monitor the Controlled Process, as shown in the generic control loop (Figure). The Control Algorithm represents the controller's decision- making process, it determines the CAs to provide. Controllers use Process Models to represent their internal understanding of the system or environment they are regulating—referred to as the Controlled Process. These models help guide decision-making. In the case of humans, this internal representation is typically called a mental model, and the decision-making mechanisms are often known as operating procedures or rules (Leveson N. G., 2018). Despite the different terminology, the fundamental idea remains the same.

Accidents often occur when there's a mismatch between the controller's Process Model and the actual state of the system or environment, highlighting the critical role of accurate system control. Issues can arise anywhere within the control loop, as shown in Figure 4. For instance, if a Process Model is inaccurate—such as when a controller believes a vehicle is in Park when it is actually in Reverse, or assumes an aircraft is descending when it's climbing—this can lead to unsafe Control Actions. Faulty sensors may also provide incorrect Feedback, resulting in dangerous outcomes. Furthermore, a system design might lack necessary Feedback mechanisms or deliver them too late, causing errors in the Process Model and leading to unsafe decisions or behaviour (Leveson N. G., 2018).

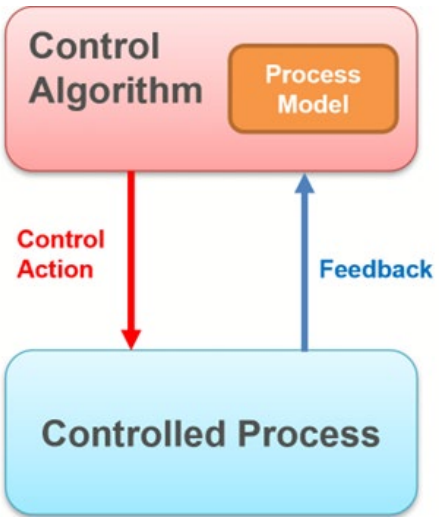

Figure 4 Generic Control Loop

Initially, the control structure is created at a high abstraction level (less detailed) and then, it is gradually refined through various iterations, adding more details about the system. A simple example of a control structure for aviation is shown in Figure 15. To manage system complexity, control structures often apply abstraction. For instance, in a commercial aircraft, there may be two or three pilots operating the flight. Rather than representing each pilot separately in the control model, they can be grouped as a single unit “flight crew” that collectively issues Control Actions and receives Feedback.

Similarly, instead of detailing every individual subsystem of the aircraft, the model can begin at a higher level of abstraction, distinguishing between aircraft automation systems and the physical components they manage. The vertical axis in a hierarchical control structure carries significance: it reflects the flow of control and authority. Higher-level controllers are positioned at the top, while lower-level entities appear at the bottom. Each element exercises control over those directly beneath it and, in turn, is governed by those directly above it in the hierarchy (Leveson N. G., 2018). For example, the Automated Controllers in Figure 5 can act as a Controller by sending control actions to the Physical Processes and monitor Feedback. At the same time, the Automated Controllers is also a Controlled Process that receives and executes Control Actions from the Flight Crew and sends Feedback to the crew.

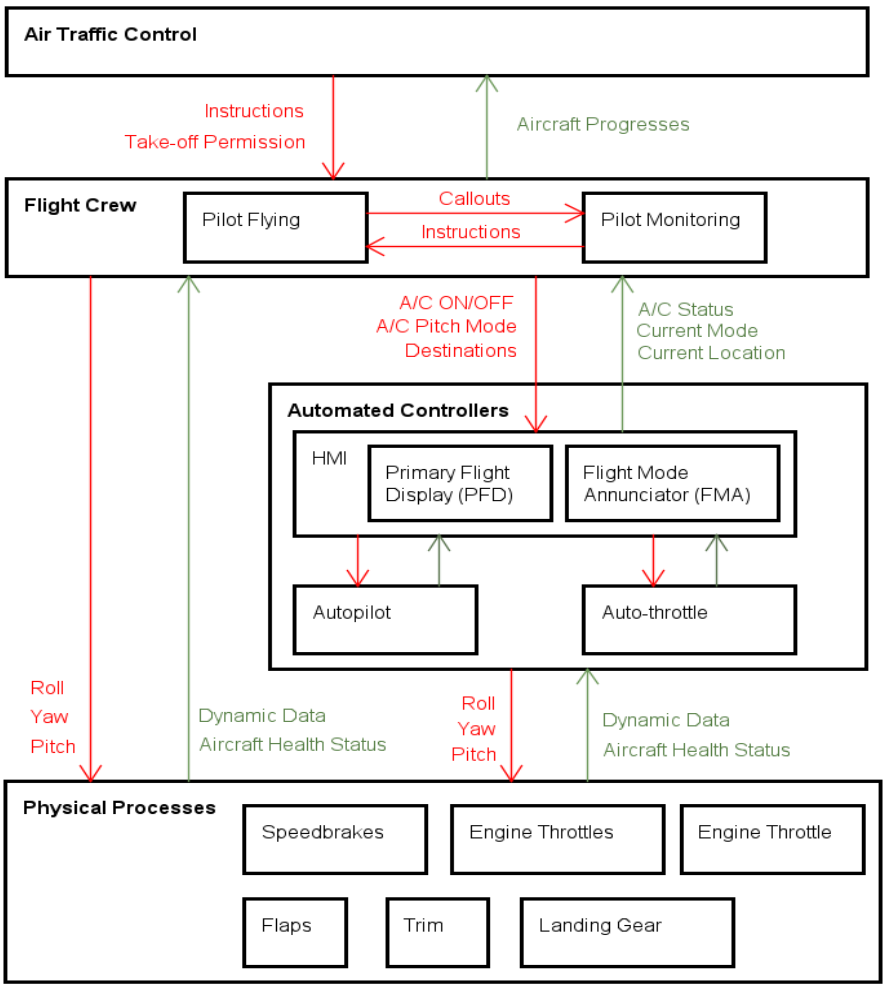

Figure 5 An example of a hierarchical control structure for Aviation

Sometimes, just drawing a simple control structure diagram can reveal flaws that were previously unnoticed. For instance, Control Actions (CA) might be issued by components lacking the essential feedback to choose safe CAs. Additionally, feedback could be offered to those unable to address it, and various controllers might give contradictory commands to the same component without the capability to identify or resolve such conflicts, among other scenarios (Leveson N. G., 2018).

Step 3: Identify Unsafe Control Actions (UCA)

After the control structure has been modelled, UCAs are identified for every CA in the control structure. Each CA is analysed to identify how the CA would manifest into a UCA. UCAs should specify the context in which the CA is unsafe. Context is essential when analysing Unsafe Control Actions (UCAs). If a Control Action (CA) were inherently unsafe in all situations, it likely would not have been incorporated into the system in the first place. Therefore, each UCA must clearly define the specific conditions under which the CA becomes unsafe. Identifying these contexts allows us to either eliminate such scenarios from the system design or develop mitigation strategies. A UCA can reference any context that contributes to its potential hazard, such as environmental conditions, the state of the Controlled Process, the Controller's

internal state, previous or repeated actions by the Controller, the behaviour or state of other Controllers, simultaneous or conflicting actions, or specific characteristics of the CA itself (e.g., a certain braking force being applied). Including words such as - “when,” “while” or “during” in the wording of UCAs, can be particularly useful for clearly defining the circumstances in which the CA becomes hazardous (Leveson N. G., 2018).

To identify a UCA, the CA is usually considered together with a particular context and worst-case environment. There are four ways a CA can be unsafe:

- Not providing the CA leads to a loss.
- Providing the CA incorrectly or when not needed leads to a loss.
- Providing a CA too early or too late or in the wrong order leads to a loss.
- Providing the CA too long or stopping the CA too soon leads to a loss (for continuous CAs, not discrete ones).

A UCA contains five parts, as shown in Figure .

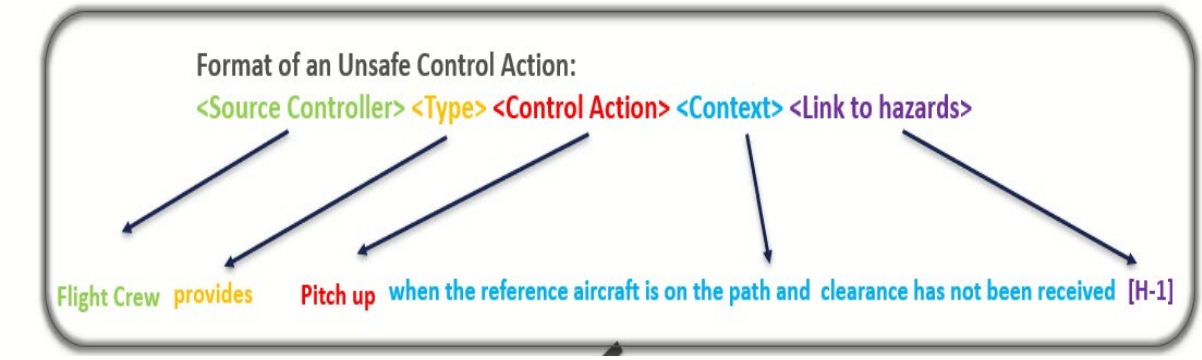

Figure 6 Structure of a UCA

The first part is the controller that can provide the CA. The second part is the type of unsafe CA (provided, not provided, too early or too late, stopped too soon or applied too long). It is worth noting that there may be multiple UCAs identified for the same type. The third part is the CA or command itself (from the control structure). The fourth part is the context discussed above, and the last part is the link to hazards (identified in Step-1). Some example UCAs linked to the CA – ‘Pitch-Up’ (issued by the Flight Crew) are shown in Table .

UCA Type	UCA Descriptions
Not Provide	UCA 1.1: Flight Crew does not provide Pitch up when it has received clearance [H-3]
Provide incorrectly or when not needed	UCA 1.2: Flight Crew provides Pitch up when the ref aircraft is on the path and clearance has not been received. [H-1,2]

UCA Type	UCA Descriptions
Provide too early or too late	UCA 1.3: Flight Crew provides Pitch up too early before clearance has been received[H-1,2]
Provide too long or too short	UCA 1.4: Flight Crew stops providing Pitch up too soon when the aircraft has not reached the designated altitude [H-1]

Table 9 A selection of UCAs for the CA- Pitch Up

Step 4: Identify Loss Scenarios

Once the UCAs are identified for all the CAs in the control structure, possible loss scenarios, which describe the Causal Factors (CFs) or causes that can lead to the UCAs, are identified by analysing the specific control loops of the CAs. Following this, Mitigations can be defined to prevent or mitigate these CFs.

A loss scenario describes the CFs that can lead to the UCAs and to losses. Two types of loss scenarios must be considered:

a) Why would unsafe or inadequate CAs occur?

b) If the CA was originally safe or adequate, why would it be improperly executed or not executed, leading to an UCA?

Until now, the analysis has focused on identifying potential Control Actions (CAs) and Feedback within the system, but it has not addressed how Feedback is obtained (e.g., through sensors) or how Control Actions are carried out (e.g., via actuators). To understand the specific causes of unsafe control and Feedback in real-world scenarios, it's beneficial to refine the control structure by explicitly incorporating sensors and actuators. This additional detail provides greater insight into how unsafe situations can arise and supports the development of more effective safety measures.

***a)* Why would unsafe or inadequate CAs occur?**

This type of loss scenario can be generated by starting with an Unsafe Control Action (UCA) and working backward to determine what could lead the Controller to issue (or fail to issue) that Control Action (CA). To identify type A loss scenarios, we must consider various factors, starting with the unsafe Controller behaviour that caused the UCA (Leveson N. G., 2018).

Scenarios that lead to UCAs are in general caused due to **1) unsafe Controller behaviour** and **2) inadequate Feedback or other inputs received**.

- **Unsafe Controller behaviour**

There are four general reasons why a Controller might provide (or not provide) a CA that is unsafe:

1. Failures involving the Controller (for physical Controllers)

2. Inadequate Control Algorithm (flawed algorithm, flawed implementation or degradation over time)
3. Unsafe control input (from another Controller)
4. Inadequate Process Model

Process model flaws happen when the Controller's understanding of the process doesn't align with what's actually happening. These flaws can arise if the Controller gets wrong feedback or information, if it receives correct feedback but misinterprets or disregards it, if the feedback is delayed or never received when needed, or if the necessary feedback simply doesn't exist (Leveson N. G., 2018).

The loss scenarios can be captured in a structured and efficient way by asking:

1. What was the Process Model's belief of the Controller?
2. What was the reason for this belief?
3. What was the cause (loss scenario) that triggered this reason?

Example:

UCA-1.4: The Pilot stops providing pitch up too soon when the aircraft has not reached the designated altitude [H-1]

Process Model (belief) of the Controller that could cause the UCA: The pilot believes that the aircraft has reached the designated altitude.

The reason for the Process Model Belief: The Pilot believes so because they received no Feedback confirming that the target altitude had been reached.

The CF that triggered this reason: The Feedback confirming whether the target altitude has been reached or not, is missing in the system design (*inadequate/missing Feedback*).

Loss Scenario 1 for UCA-2: The Pilot stops providing pitch up too soon when the aircraft has not reached the designated altitude because the pilot incorrectly believes that the aircraft has reached the designated altitude. This is due to the lack of a Feedback in the design providing confirmation to the Pilot on whether the designated altitude has been reached or not.

A Mitigation that can be proposed to address this loss scenario would be:

Mitigation to prevent the cause/CF: Feedback confirming that the target altitude has been reached, shall be included in the system design.

- **Causes of inadequate Feedback and information**

Scenarios involving insufficient feedback or information typically include:

1. Feedback or information not received
2. Inadequate Feedback is received

When a scenario reveals that Feedback or information (or the absence of it) could lead to an Unsafe Control Action (UCA), it's important to investigate the source of that information to understand what might contribute to the issue. Feedback typically originates from the Controlled Process, often through sensors, while other types of information may come from additional processes, other Controllers, or various components within the system or its environment. Identifying these sources helps uncover potential failure points and supports more effective risk mitigation.

b) Why would the CA (that was originally safe or adequate) be improperly executed or not executed, leading to an UCA?

Hazards may arise from Unsafe Control Actions (UCAs), but they can also occur even without a UCA if control actions are executed incorrectly or not executed at all. To identify such scenarios, it is important to examine **3) factors that affect the control path** as well as **4) factors that affect the Controlled Process** (Leveson N. G., 2018).

- **Factors involving the Control Path**

The control path illustrates how Control Actions (CAs) are transmitted from the Controller to the Controlled Process. It's important to analyse this path to identify how issues may prevent CAs from being delivered correctly—or at all. Such problems are often linked to communication delays or errors between the Controller and the Controlled Process, as well as failures or performance degradation in the Actuators responsible for executing those actions.

- **Factors related to the Controlled Process**

Although CAs might be transferred or implemented within the Controlled Process, their efficacy is not guaranteed, and they could potentially be superseded by other Controllers. Typically, scenarios involving the Controlled Process might encompass:

1. The CA being not executed (i.e., the CA is applied or received by the Controlled Process, but the Controlled Process does not respond) due to the received CA from other controllers.
2. The CA is improperly executed (i.e., the CA is applied or received by the Controlled Process, but the Controlled Process responds improperly) due to failure or degradations of the Controlled Process, and disturbances from other inputs.

Further guidance and examples of application of STPA can be found in (Leveson N. G., 2018).

Appendices

Appendix: Abbreviations

Abbreviation	Description
AAM	Advanced Air Mobility
ANAC	National Civil Aviation Agency of Brazil
ANSP	Air Navigation Service Provider
AOC	Air Operator Certificate
ATC	Air Traffic Control
CA	Control Action
CAA	Civil Aviation Authority
CAP	Civil Aviation Publication
CAST	Causal Analysis based on Systems Theory
CAT	Commercial Air Transport
CF	Causal Factor
CIF	Controller Impact Factor
CPL	Commercial Pilot Licence
DAL	Design Assurance Level
EASA	European Union Aviation Safety Agency
EC	Electronic Conspicuity
EJ	Expert Judgement
ETA	Event Tree Analysis
eVSLG	eVTOL Safety Leadership Group
eVTOL	electric vertical take-off and landing
FAA	Federal Aviation Administration
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
G350	Gaseous Hydrogen 350BAR

HAZOP	Hazard and operability study
ICAO	International Civil Aviation Organisation
LH2	Liquid Hydrogen (cryogenic)
MCS	Monte Carlo Simulation
NASA	National Aeronautics and Space Administration
NCC	Non-commercial operations with complex motor-powered aircraft
NCO	Non-Commercial Operations with other than complex motor-powered aircraft
NOTAM	Notice to Aviation
OEM	Original Equipment Manufacturer
PED	Portable electronic devices
PMS	Pre-mitigation Severity
RA(T)	Restricted Area (Temporary)
RF	Radio Frequency
RPM	Revolutions per minute
SAW	Simple Additive Weighting
SIF	Severity Impact Factor
SME	Subject Matter Expert
SoC	State of Charge
SPO	Specialised Operations
STAMP	System-Theoretic Accident Model and Processes
STPA	Systems- Theoretic Process Analysis
TAC	Temporary Aerodrome Creation
UCA	Unsafe Control Action
VMC	Visual Meteorological Conditions

List of Figures

List of Tables

References

Benhamlaoui, W. (2020). Comparative Study of STPA and Bowtie Methods: Case of Hazard Identification for Pipeline Transportation. Springer Nature.

Bensaci, C. (2020). STPA and Bowtie Risk Analysis Study for Centralized and Hierarchical Control Architectures Comparison. *Alexandria Engineering Journal*, 18.

(2023). *CAP 2576 - Understanding the downwash/outwash characteristics of eVTOL aircraft.* Civil Aviation Authority.

(2025). *CAP 3075 - Protecting the Future: Trials and Simulation of Downwash and Outwash for Helicopters and Powered Lift Aircraft.* Civil Aviation Authority.

Chatzimichailidou, M. M. (2018). A comparison of the Bow-Tie and STAMP approaches to reduce the risk of surgical instrument retention. *Risk Analysis*.

Chen, S. a. (2020). Identifying accident causes of driver-vehicle interactions using system theoretic process analysis (stpa). *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*.

Chen, S. a. (2023). A System-Based Safety Assurance Framework for Human-Vehicle Interactions. *SAE Technical Paper*.

Chen, S. K. (2021). Analyzing national responses to COVID-19 pandemic using STPA. *Safety Science*.

Chen, S., Khastgir, S., & Jennings, P. (n.d.). A System-Based Safety Assurance Framework for Human-Vehicle Interactions. *WCX SAE World Congress Experience.* SAE.

Defense, U. D. (10 Feb 2000). *MIL-STD-882D Standard Practice for System Safety.*

Harkleroad, E. a. (2013). *Review of systems-theoretic process analysis (STPA) method and results to support NextGen concept assessment and validation.* ATC-427 MIT.

Harkleroad, E., Vela, A., Kuchar, J., & Barnett, B. a.-B. (n.d.). *Risk-based modeling to support nextgen concept assessment and validation.* Lincoln Laboratory, Lexington, MA, Project Report ATC-405.

Heinrich, H. W. (1941). Industrial Accident Prevention. A Scientific Approach.

Ishikawa, K. a. (1990). *Introduction to quality control.* Springer.

James Elizebeth, M. a. (2023). *Comparison of FTA and Stpa approaches: a brake-by-wire case study.*

Khastgir, S. a. (2021). Systems approach to creating test scenarios for automated driving systems. *Reliability engineering & system safety*.

Leveson, N. (2004). A new accident model for engineering safer systems. *Safety science*.

Leveson, N. G. (2016). *Engineering a safer world: Systems thinking applied to safety.* MIT Press.

Leveson, N. G. (2018). *STPA Handbook.* MIT press.

Liu, T. a. (n.d.). Safety analysis of Civil aviation Flight and UAV Operation based on STAMP/STPA. *E3S Web of Conferences.*

McLeod, R. W. (2018). Bowtie Analysis as a prospective risk assessment technique in primary healthcare. *Policy and Practice in Health and Safety*.

Merrett, H. (2019). Comparison of STPA and Bow-tie Method Outcomes in the Development and Testing of an Automated Water Quality Management System. *MATEC Web of Conferences.*

Merrett, H. C. (2019). Comparison of STPA and bow-tie method outcomes in the development and testing of an automated water quality management system. MATEC Web of Conferences.

Merrett, H. C. (2019). Comparison of STPA and bow-tie method outcomes in the development and testing of an automated water quality management system. *MATEC Web of Conferences* (p. 18). MATEC Web of Conferences.

Natarajan, D. (2017). *ISO 9001 Quality management systems.* Springer.

Owens, B. D. (2008). Application of a safety-driven design methodology to an outer planet exploration mission. *IEEE aerospace conference*.

Qi, Y. a. (2025). Safety analysis in the era of large language models: a case study of STPA using ChatGPT. *Machine Learning with Applications*.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science*.

Reason, J. (2000). Human error: models and management. *Bmj*.

Rose, E. J. (2023). Monte Carlo sensitivity analysis for unmeasured confounding in dynamic treatment regimes. *Biometrical Journal*.

Silvis-Cividjian, N. a. (2020). Using a systems-theoretic approach to analyze safety in radiation therapy-first steps and lessons learned. *Safety science*.

smith2012mil. (2012). *MIL-STD-882E.* Department of Defence.

Stallings, W. (1976). *Gerald M. Weinberg. An introduction to general systems thinking. New York: Wiley, 1975, 279 pp.*

Stanton, N. A. (2019). Systems Theoretic Accident Model and Process (STAMP) applied to a Royal Navy Hawk jet missile simulation exercise. *Safety science*.

Sulaman, S. M. (2019). Comparison of the FMEA and STPA safety analysis methods-a case study. *Software quality journal*.

Sultana, S. a. (2019). Hazard analysis: Application of STPA to ship-to-ship transfer of LNG. *Journal of Loss Prevention in the Process Industries*.

Sun, L. a.-F. (2022). Comparison of the HAZOP, FMEA, FRAM, and STPA methods for the hazard analysis of automatic emergency brake systems. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering*.

Svedung, I. a. (2002). Graphic representation of accidentscenarios: mapping system structure and the causation of accidents. *Safety science*.

Thomas, J. P., & Van Houdt, J. G. (2024). *Evaluation of System-Theoretic Process Analysis (STPA) for Improving Aviation Safety -DOT/FAA/TC-24/16.* Center for Aviation Safety, Advanced Engineering Services.