# Active STPA: Integration of Hazard Analysis into a Safety Management System Framework

by

DIOGO SILVA CASTILHO

B.S. in Aeronautical Sciences, Brazilian Air Force Academy, 2000
M.S. in Aeronautical Engineering, Aeronautical Institute of Technology, 2014

Submitted to the Department of Aeronautics and Astronautics
in partial fulfillment of the requirements for the degree of

**DOCTOR OF PHILOSOPHY**
at the
**MASSACHUSETTS INSTITUTE OF TECHNOLOGY**

~~August 2019~~ [September 2019]



Signature of Author Signature redacted
Department of Aeronautics and Astronautics
August 11, 2019

Certified by Signature redacted
Nancy G. Leveson, Ph.D., Professor
Department of Aeronautics and Astronautics
Thesis Committee Chair

Certified by Signature redacted
Sheila E. Widnall, Ph.D., Professor
Department of Aeronautics and Astronautics
Thesis Committee Member

Certified by Signature redacted
Daniel R. Montes, Ph.D.
United States Air Force
Thesis Committee Member

Accepted by Signature redacted
Sertac Karaman, Ph.D., Associate Professor
Department of Aeronautics and Astronautics
Graduate Committee Chair

*[Page intentionally left blank]*

## Disclaimer

The views expressed in this document are those of the author and do not reflect the official position or policies of the Brazilian Air Force, Brazilian Defense Ministry, or the Brazilian Government.

*[Page intentionally left blank]*

# Active STPA: Integration of Hazard Analysis into a Safety Management System Framework

by

**Diogo Silva Castilho**

Submitted to the Department of Aeronautics and Astronautics on
August 6, 2019 in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Aeronautics and Astronautics

**Abstract**

This dissertation describes a new approach to integrate a hazard analysis into Safety Management Systems (SMS). This new engineering process guides safety managers and analysts in the identification of a migration toward states of higher risk. The solution is the use of an active version of STPA (Systems-Theoretic Process Analysis), a hazard analysis tool based on Systems-Theoretic Accident Model and Processes (STAMP). The Active STPA uses data collected during operations, such as Flight Data Monitoring events and voluntary reporting, to identify leading indicators of increasing risk. The events are compared with the STPA. The discrepancies lead to a reasoning about previous assumptions on human behavior and the environment in which the system operates. New defenses are identified and implemented. The output of the process is a set of new defenses for prevention and mitigation that will enforce the requirements and constraints generated by the STPA, allowing the generation of cumulative knowledge on system behavior over time. The feedback on SMS activities allows targeted safety improvement activities and provides qualitative information for hazard management integrating Active STPA into an SMS. Most of the indicators currently in use in the aviation industry are reactive because they measure only parameter exceedances. Active STPA allows a proactive identification of the potential cause of future accidents.

**Thesis Supervisor:** Nancy G. Leveson
**Title:** Professor of Aeronautics and Astronautics and Engineering Systems

***Keywords:*** *Hazard Analysis, STPA, Safety Management System, Leading Indicators*

*[Page intentionally left blank]*

# Acknowledgments

I want to thank everyone who participated and contributed to this achievement. First, thank you Prof. Nancy Leveson for accepting me as your student and advising me in so many lab meetings, classes, and late-night emails. Your guidance and the freedom that you gave to develop my own ideas was very important to me.

I also thank the Committee members Lt Col Dan Montes and Prof. Sheila Widnall, and the readers, Gus Larard, Shem Malmquist, Prof. John Carrol, Dr. John Thomas, and Prof. Oli De Weck for the valuable feedback on this research. Thank you, all MIT Professors and staff members for making these four years such a fascinating experience. My appreciation also goes to the airline safety managers Adam Johns, Peter Hudson, Elias Nikolaidis, Julian Oehling, Chrysa Tsimitri, and David Yatch for all the insight on how commercial aviation deals with safety.

I want to thank the Brazilian Air Force for giving me the opportunity to pursue a higher education. I hope I will be able to contribute to our projects, returning the investment of the Brazilian government provided by a CNPq scholarship.

This journey started in 2014 with a visit to the Systems Engineering Research Lab (SERL), which is now a group of the Engineering Systems Lab (ESL). In this visit, I had a first contact with what would become an essential part of my life. I was received by Dr. John Thomas, Dr. Cody Fleming, and Dr. Jonas Fulindi. The first impression given by their warm reception was a good glimpse of what was yet to come.

Right from the beginning of this doctorate, I had the chance to interact with outstanding lab mates, including Dajiang Suo, Megan France, David Horney, and Andrea Scarinci, who became a friend for life. Then, classes and projects brought amazing AeroAstro colleagues. I will keep the memories of our days playing volleyball in front of building 33 and so many other special moments during these years. The newcomers to the lab, Lawrence Wong, and Michael Schmid, were also vital as we had valuable discussions about research and life topics.

I want to thank our UROP Alex Lam for working on the research and all the ones who helped me revise my writing, especially April Larsen and Beata Shuster. The new friends I made were particularly important to me. The Muddy Fridays and the meetings of the Brazilian researchers' community helped to find them. In one of those meetings, I met my partner Rachel. Thank you for all your love and inspiration.

Finally, I am grateful for the example provided by my father, Newton, and my mother, Nanci. They gave me the tools to find my way in life. Something that I want to provide to my daughter. Victoria, the best version of me, thank you for giving me the strength to keep the pace, looking for higher skies.

*[Page intentionally left blank]*

# Table of Contents

Abstract ..... v
List of Figures ..... 11
List of Tables ..... 13
1. Introduction ..... 19
1.1 Problem Statement ..... 20
1.2 Research Background ..... 20
1.2.1 Research Purpose ..... 23
1.3 Methodology ..... 24
1.3.1 Research Steps ..... 25
1.3.2 Thesis Structure ..... 25
2. Literature Review ..... 27
2.1 Systems Safety Engineering ..... 27
2.2 Safety Management ..... 30
2.2.1 Safety Management Systems (SMS) ..... 31
2.2.2 Aviation standards for Safety Management Systems ..... 32
2.3 Bowtie ..... 36
2.4 STAMP ..... 37
2.5 Leading Indicators ..... 39
2.5.1 Assumption-based Leading Indicators ..... 40
3. Active STPA ..... 42
3.1 Case Study - Unstable Approaches ..... 47
3.1.1 Approach for landing ..... 47
3.1.2 Unstable Approaches for Landing ..... 48
3.2 STPA for Unstable Approaches ..... 51
3.2.1 STPA - Step 1 – Fundamentals ..... 51
3.2.2 STPA - Step 2 – Model the Control Structure ..... 54
3.2.3 STPA - Step 3 – Identify Unsafe Control Actions ..... 56
3.2.4 STPA - Step 4 – Identify Loss Scenarios ..... 57
3.2.5 Implementation of an STPA ..... 59
3.3 Partner data: An incident on a parallel approach ..... 60
3.4 Active STPA Phase 1: Inspect the STPA ..... 63

Case A - ATC ..... 69
Case B – B-737 ..... 72
Case C – A-340 ..... 75
3.5 Active STPA Phase 2: Reason about the Assumptions ..... 78
Case A - ATC ..... 81
Case B – B-737 ..... 82
Case C – A-340 ..... 83
3.6 Active STPA Phase 3: Solve and Update ..... 85
Case A - ATC ..... 89
Case B – B-737 ..... 90
Case C – A-340 ..... 91
4. Integrated Safety Management System ..... 94
4.1 I-SMS with Active STPA ..... 94
4.2 I-SMS for Commercial Aviation ..... 97
4.2.1 Hazard Alerting System ..... 99
4.2.2 Process 1 (P1) - Preparation of Active Hazard Analysis Input ..... 101
4.2.3 Process 2 (P2) - Active STPA ..... 109
4.2.4 Process 3 (P3) - Prevention and Mitigation ..... 111
4.4 Using I-SMS in the aviation industry ..... 114
4.4.1 Refining assumptions ..... 114
4.4.2 Leading Indicators ..... 119
4.4.3 ICAO SMS ..... 119
4.4.4 Aviation Safety Performance Indicators ..... 120
4.4.5 Comparison between Active STPA and ICAO SMS ..... 126
4.5 Consortium for I-SMS ..... 131
5. Conclusion ..... 132
5.1 Contributions ..... 133
5.2 Future work ..... 133
References ..... 135
Appendices ..... 138

# List of Figures

**Figure 1. Accident and fatal accident trend (2011-2015) (ICAO, 2016)** ..... 21
**Figure 2. The four components of the ICAO SMS (ICAO, 2018)** ..... 22
**Figure 3. Safety management and information flow (Leveson, 2011)** ..... 31
**Figure 4. Risk matrices (FAA, 2019)** ..... 32
**Figure 5. Risk acceptance criteria (FAA, 2019)** ..... 33
**Figure 6. Structure of the Bowtie model (CAA UK, 2019)** ..... 36
**Figure 7. STPA control loop with automated controller (Leveson, 2011)** ..... 38
**Figure 8. Phases of Active STPA** ..... 45
**Figure 9. Unstable approaches in Glideslope** ..... 48
**Figure 10. High-level functional control structure** ..... 55
**Figure 11. Structure of an UCA** ..... 57
**Figure 12. Generation of scenarios for the control action: pressing the GA button** ..... 58
**Figure 13. Elements of STPA and its implementation** ..... 60
**Figure 14. Parallel Approaches for landing (FAA, 2017)** ..... 60
**Figure 15. Reconstitution of the trajectory of both aircraft with FDM (Source: Partner)** .. 61
**Figure 16. Elements inspected in Phase 1** ..... 64
**Figure 17. Step 2: Control loop ATC - Crew extracted from the high-level control structure** ..... 70
**Figure 18. Representation of a Localizer overshot** ..... 72
**Figure 19. Step 2: Control loop Crew - Autopilot (AP) extracted from the detailed control structure** ..... 73
**Figure 20. Control loop Crew – Auto-Throttle extracted from the detailed control structure** ..... 76
**Figure 21. I-SMS General framework** ..... 94
**Figure 22. Customized I-SMS model for commercial aviation** ..... 98
**Figure 23. Safety information flow between development and operational organizations (Leveson 2012)** ..... 101
**Figure 24. Basic components of CAST (Leveson, 2019)** ..... 107
**Figure 25. Safety communication channels** ..... 112
**Figure 26. Unsafe Control Action identified in the STPA for the TO/GA event** ..... 115
**Figure 27. Throttle pedestal in Boeing 777** ..... 116
**Figure 28. Throttle pedestal in commuter aircraft** ..... 117
**Figure 29. Safety Performance Targets (SPTs) representation in comparison with Safety Objectives (FAA, 2019)** ..... 121
**Figure 30. Trend of an SPI on descent rate (Source AHK)** ..... 124
**Figure 31. Combination of trends (undisclosed partner airline, 2019)** ..... 125
**Figure 32. SMS information flow in SMM (ICAO, 2018)** ..... 126

**Figure 33. ICAO SMS framework** ..... 128
**Figure 34. Example of the link between leading and lagging indicators (SMM, 2018)** ..... 129
**Figure 35. Example showing the differences between the ICAO SMS and the I-SMS with Active STPA** ..... 130

# List of Tables

**Table 1. Summary of Phases and Tasks of the Active STPA** ..... 46
**Table 2. Description of the event after the investigation** ..... 62
**Table 3. Structure of Tasks of Active STPA Phase 1** ..... 65
**Table 4. Case A – ATC – Phase 1** ..... 71
**Table 5. Step 3: Listing control actions** ..... 72
**Table 6. Step 3: The UCAs for engaging LOC** ..... 73
**Table 7. Case B – Boeing 737 – Phase 1** ..... 75
**Table 8. Case C – Airbus A-340 – Phase 1** ..... 77
**Table 9. Structure of Tasks of Active STPA Phase 1** ..... 78
**Table 10. Case A – ATC – Phase 2** ..... 82
**Table 11. Case B – Boeing 737 – Phase 2** ..... 83
**Table 12. Case C – Airbus A-340 – Phase 2** ..... 84
**Table 13. Structure of Tasks of Active STPA Phase 1** ..... 85
**Table 14. Case A – ATC – Phase 3** ..... 89
**Table 15. Case B – Boeing 737 – Phase 3** ..... 90
**Table 16. Case C – Airbus A-340 – Phase 3** ..... 92
**Table 17. STPA Step 3 – Examples of UCAs** ..... 115
**Table 18. Standard STPA Step 4 – Scenario and Constraint** ..... 115
**Table 19. Assumption made in STPA** ..... 116
**Table 20. Revised analysis after Active STPA** ..... 118
**Table 21. Examples of SPIs, triggers, and SPTs from Partners** ..... 122
**Table 22. Examples of SPIs currently collected by a partner** ..... 123
**Table 23. Number of events per one-thousand flights** ..... 124

# Abbreviations and Acronyms

| | |
|---|---|
| AC | Aircraft |
| AC | Advisory Circular |
| ACARS | Aircraft Communications, Addressing and Reporting System |
| ADC | Air Data Computer |
| ADS-B | Automatic Dependent Surveillance-Broadcast |
| AFDS | Autopilot Flight Director System |
| AGL | Above Ground Level |
| AHAI | Active Hazard Analysis Input |
| AHK | Air Hong Kong |
| AHRS | Attitude and Heading Reference System |
| ALARP | As Low As Reasonably Practical |
| ALT | Altitude mode in autopilot |
| AP | Autopilot |
| APP | Approach |
| ARM | Autopilot mode engagement |
| ASAP | Aerospace Safety Advisory Panel |
| ASIAS | Aviation Safety Information Analysis and Sharing |
| ASR | Aviation Safety Report |
| ASRS | Aviation Safety Reporting System |
| A/T | Auto Thrust or Auto Throttle |
| ATC | Air Traffic Controller |
| ATIS | Automatic Terminal Information System |
| CAD | Hong Kong Civil Aviation Department |
| CAS | Calibrated Airspeed |
| CAST | Causal Analysis based on Systems Theory |
| CDO | Continuous Descent Operations |
| CDU | Control Display Unit |
| CFIT | Controlled Flight into Terrain |
| CFR | Code of Federal Regulations |
| CLB | Climb mode in autopilot |
| CRM | Crew Resource Management |
| CRP | Confidential Report Program |
| DEA | Data Envelopment Analysis |
| Deg | Degrees |
| DME | Distance Measuring Equipment |
| DOM | Duty Operations Manager |
| EASA | European Aviation Safety Agency |
| EFB | Electronic Flight Bags |
| ESL | Engineering Systems Laboratory |

| | |
|---|---|
| ETPS | Empire Test Pilot's School – United Kingdom |
| FAA | Federal Aviation Administration |
| FCOM | Flight Crew Operating Manuals |
| FCU | Flight Control Unit |
| FD | Flight Director |
| FDAP | Flight Data Analysis Program |
| FDM | Flight Data Monitoring |
| FLCH | Flight Level Change mode in autopilot |
| FMC | Flight Management Computer |
| FMEA | Failure Modes and Effects Analysis |
| FMECA | Failure Modes and Effects Criticality Analysis |
| FON | Flight Operations Notices |
| FOQA | Flight Operations Quality Assurance |
| FPA | Flight Path Angle |
| Ft | Feet |
| FT | Flight Testing |
| GA | Go Around |
| GAJSC | General Aviation Joint Steering Committee |
| GPS | Global Positioning System |
| GPWS | Ground Proximity Warning System |
| GS | Glide Slope |
| H | STPA Hazard |
| HAZOP | Hazard and Operability Analysis |
| HDG | Heading |
| HMI | Human Machine Interaction |
| IAF | Initial Approach Fix |
| IAS | Indicated Airspeed |
| ICAO | International Civil Aviation Organization |
| ICAO | International Civil Aviation Organization |
| ICBM | Intercontinental Ballistic Missile |
| IFR | Instrument Flight Rules |
| ILS | Instrument Landing System |
| IMC | Instrument Meteorological Conditions |
| IOC | Integrated Operations Control |
| IOSA | IATA Operational Safety Audit |
| IPEV | Flight Testing and Research Institute - Brazil |
| I-SMS | Integrated Safety Management System |
| Kt | Knots – nautical miles per hour |
| L | STPA Loss |
| LNAV | Lateral Navigation |
| LOC | Localizer |

| | |
|---|---|
| LOC-I | Loss Of Control in Flight |
| LOSA | Line Operations Safety Audit |
| MAC | mid-air collisions |
| MAPP | Missed Approach Procedure |
| MCP | Mode Control Panel |
| MCP | Mode Control Panel |
| MFD | MultiFunction Display |
| MFD | Multi-Function Display |
| MIT | Massachusetts Institute of Technology |
| MoC | Management of Change |
| MSAW | Minimum Safe Altitude Warning |
| MVA | Minimum Vectoring Altitude |
| NAS | National Airspace System |
| NDA | non-disclosure agreements |
| NOTAM | Notice to Airmen |
| NTZ | No Transgression Zone |
| NVS | National Voice System |
| ORD | Chicago O'Hare International Airport |
| PF | Pilot Flying |
| PFD | Primary Flight Display |
| PM | Pilot Monitoring |
| PRM | Precision Monitored Approach |
| RA | Resolution Advisory |
| RA | Radio Altimeter |
| RE | Runway Excursions |
| ROD | Rate of Descent |
| RWY | Runway |
| SA | Safety Analyst |
| SARP | Standards and Recommended Practices |
| SC | Safety Constraint |
| SFO | San Francisco International airport |
| SMM | Safety Management Manual |
| SMP | Safety Management Panel |
| SMS | Safety Management Systems |
| SO | Safety Objectives |
| SOP | Standard Operating Procedure |
| SPD | Speed hold mode in autopilot |
| SPI | Safety Performance Indicators |
| SPT | Safety Performance Targets |
| SR | Safety Requirement |
| SRM | Safety Risk Management |

| | |
|---|---|
| STAMP | Systems-Theoretic Accident Model and Processes |
| STPA | Systems-Theoretic Process Analysis |
| SWIM | System-Wide Information Management |
| TA | Transition Altitude |
| TCAS | Traffic Collision Avoidance System |
| TEM | Threat and Error Management |
| TO | Takeoff |
| TO/GA | Take Off / Go Around |
| TRK | Tracking |
| TWR | Control Tower |
| UAS | Undesired Aircraft States |
| UCA | Unsafe Control Action |
| USAFTPS | US Air Force Test Pilot School |
| Vapp | Approach Velocity |
| VDRP | Voluntary Disclosure Reporting Program |
| VHF | Very-High Frequency |
| VMC | Visual Meteorological Conditions |
| VNAV | Vertical Navigation |
| VRef | Reference Velocity |
| W/S | Windshear |

*[Page intentionally left blank]*

# 1. Introduction

Aviation manufacturing generates sophisticated equipment that requires many years of development and high investment in certification and production. Thus, for any aircraft, the lifetime is expected to be long. Modern heavy jets might experience more than four decades of operation. Throughout an aircraft's lifetime, all its equipment will be operated by different generations of pilots, flight attendants, and mechanics. This system comprised of hardware, software, and operators with operating culture will change over time. Therefore, the environment and mindset of crews and operators must adapt to modern standards and the ever-growing demand for safety. Technology will change, in the form of upgrades to components, increased functionalities, and different levels of automation. The challenge is to assure safety on operations when assumptions made at the beginning of the project are no longer valid.

The fact that commercial aviation has maintained satisfactory safety records leads us to feel safe because we are flying on well-established systems. However, the evolution of equipment in aviation requires the implementation of new procedures that affect the operations of the airspace. Many of these changes add new hazards that may not be properly controlled. For instance, NextGen is the implementation of satellite-based navigation, digital communications, and automated decision support tools. As part of NexGen, new systems like the Automatic Dependent Surveillance-Broadcast (ADS-B), DataComm, National Airspace System (NAS) Voice System (NVS), Terminal Flight Data Manager (TFDM), System-Wide Information Management (SWIM) were conceptualized, tested and entered into service in the past decade. The implementation of these systems is characterized by changes in training and operational practices that may lead to more incidents.

Moreover, the balance between efficiency and safety has always been a challenge for management, but it is needed to shape functioning safety management systems. Modern airlines are pushed to operate on the borderline of established safety constraints due to *on-time performance*. This mentality includes processing of passengers, baggage, and cargo. The schedules of modern companies are so optimized that there is low flexibility in crew resting time, logistics, and maintenance dynamics. The flight crew and ground personnel follow company specified operational procedures, which if changed, may affect the strategies created by the management responsible for the financial stability of the company. Therefore, human limitations, such as stressful conditions caused by delayed operations, require special consideration in modern aviation.

The study of the vulnerabilities of a system to act proactively in accident prevention is often organized in a hazard analysis. Careful hazard analyses are key to provide the knowledge necessary to reduce risks. The first hazard analysis of a new product begins during its development. In this phase, engineers are tasked to make assumptions about the operation of the product. Nevertheless, after years on the market, as the environment and the culture of users change, some of the original assumptions may become obsolete. For example, the Boeing 777 aircraft had its first group development meeting in 1990. Both the rollout and the first flight took

place in 1994, and it entered service in 1995. Back then, it would be impossible to imagine that airlines would be using electronic flight bags (EFB) or tablets[1]. It is easy to see this natural evolution in hindsight, but there were no smartphones before the B-777 entry into service. The lifetime of the first generation of the B-777 aircraft is expected to reach four decades, and the new generation (B-777X) shares parts of the same original hazard analysis. Therefore, to make the operations safer as the system evolves and matures, a process is required to actively update the hazard analysis using operational experience.

The operational performance must be constantly tested and verified by observations or measurements. This is not to predict the probability of future issues, but to identify changes in the current safety status of the system, and understand the causal factors of those changes. In aviation today, safety efforts focus on the measurement of safety performance to generate trends for visual identification of changing risk. However, the current practice using Flight Data Monitoring (FDM) to detect when flight parameters are different than normal is considered to be reactive. Dynamic systems require a process to actively run a hazard analysis throughout the operational lifetime of a system to promote operational safety.

## 1.1 Problem Statement

Risk is inherent in complex activities, particularly in aviation. Techniques currently in use for safety management based on risk assessment do not provide an effective method to identify when the risk of hazardous conditions is increasing. Therefore, a new approach to safety management is needed to analyze the available data and act proactively. Safety managers and analysts need a method to guide their decisions and actions to properly monitor the operational activity and to adjust procedures to make the system safer.

## 1.2 Research Background

After World War II, an aviation technical revolution resulted in the development of capable navigational equipment and more reliable aircraft systems that led to a significant reduction in the number of accidents. This reduction continued due to better safety regulation and the exploration of human factors. Modern approaches use data collection to generate safety trends and to develop reactive and proactive methodologies to monitor safety risks. All the effort to improve safety resulted in the continuation of a consistent reduction of the number of accidents, as described in the International Civil Aviation Organization (ICAO) Safety Report (Figure 1).

[11] EFBs and off-the-shelf tablets are accepted to be integrated into the dashboard to substitute all paper charts and aircraft manuals ( FAA InFO, 2011).

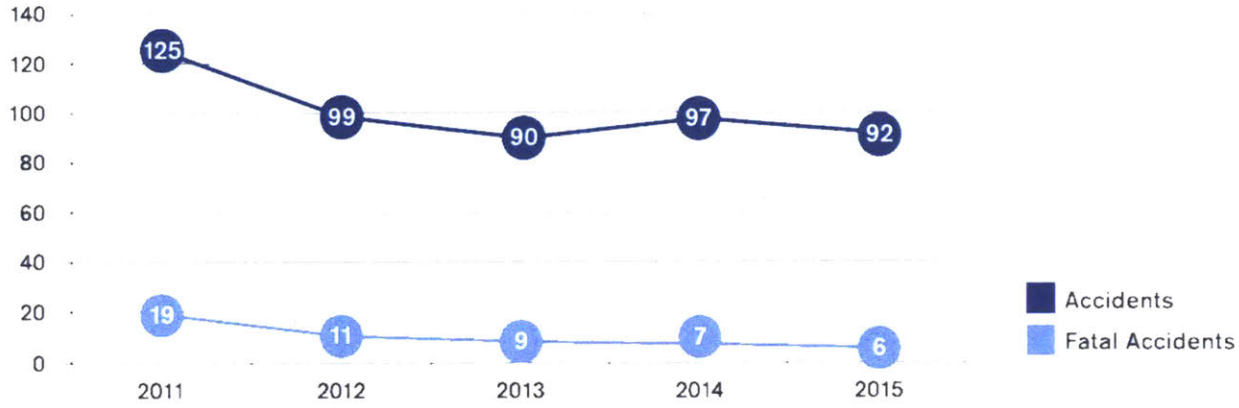



**Figure 1. Accident and fatal accident trend (2011-2015) (ICAO, 2016)**

Commercial aviation traffic around the world continues to increase consistently, both in number of passengers and in number of departures. According to FAA, in the United States of America, there are currently more than 14,000 air traffic controllers in 517 control towers, 155 radar facilities, and 21 air route traffic control centers. They control more than 43,000 flights a day, and during peak times, roughly 5,000 aircraft may be in the sky at any given time. They are required to work safely and pushed to do it efficiently.

In 2017, for the first time in aviation history, commercial aviation had one year without any fatal accident in passenger jets (IATA, 2018). Although this is an improvement, it does not mean there are fewer exposures to risk. In fact, several accidents have occurred in 2018 and 2019, including two major accidents involving new aircraft in similar conditions and due to the same causal factors. This does not mean that we are not learning from past accidents; on the contrary, most operators ensure pilots and crews gain the necessary knowledge, so they learn how to face similar situations. Instead, it means that there is more to learn, and new hazards are arising over time.

To reduce the number of accidents even more, eight aviation agencies[2] started the Safety Management International Collaboration Group (SM ICG) to continue the improvement of safety by treating it as a management problem. Safety Management Systems (SMS) is not a new term, but in aviation, it is a new requirement for air operations, maintenance, air traffic services, and airports. ICAO expanded these requirements to include flight training institutions and manufacturers involved in the design and production of aircraft. Annex 19, the document that formalized this initiative, is the first new ICAO Annex to come out in over thirty years. The Safety Management Panel (SMP) delivered the first phase of Annex 19 in early 2012. It was

[2] ICAO, National Civil Aviation Agency (ANAC) of Brazil, Civil Aviation Safety Authority (CASA) of Australia, European Aviation Safety Agency (EASA), Federal Office of Civil Aviation (FOCA) of Switzerland, United States Federal Aviation Administration (FAA) Aviation Safety Organization, Transport Canada Civil Aviation (TCCA), and Civil Aviation Authority of United Kingdom.

adopted by the ICAO Council on February 25, 2013, and became applicable in November 2013. Amendment 1 to Annex 19 came into effect on July 2016 and will be applicable in November 2019. Annex 19 organizes the SMS into four components as pictured in Figure 2.

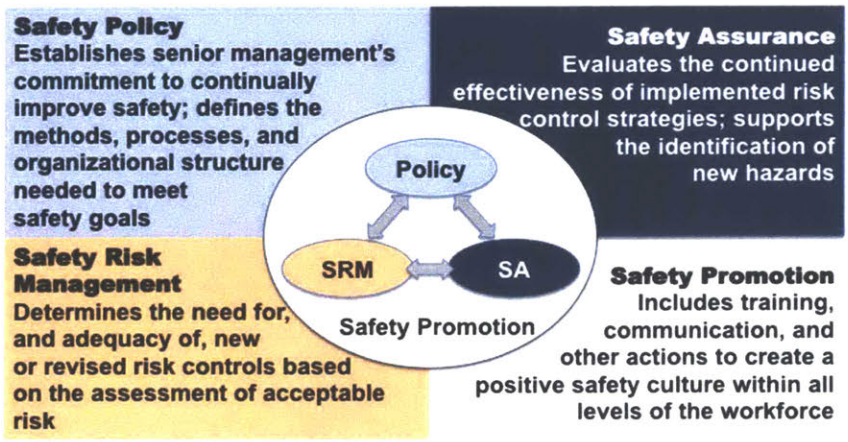



**Figure 2. The four components of the ICAO SMS (ICAO, 2018)**

The concept of Safety Management System (SMS) was introduced as a formal, top-down, organization-wide approach to manage safety risk to assure the effectiveness of safety risk controls. From this perspective, SMS aims to make aviation safer only by measuring and controlling risks, which leaves room for improvement in processes within SMS. The current SMS does consider software-controlled systems and higher levels of automation, but it fails to proactively identify the impacts of human factors and changes in the system environment, to reduce the exposure to hazards. It focuses on risk assessment (accident prediction) rather than hazard mitigation for accident prevention (FAA, 2016).

The new regulatory changes for SMS implementation have Performance-Based Oversight (PBO) requirements. Organizations need to demonstrate to regulators that they are meeting safety targets, presenting through safety performance indicators how acceptable levels of safety performance are achieved. After November 2019, ICAO will commence an audit program of all aviation organizations to verify their compliance with the Revision 1 of Annex 19. In the audit process, the airlines will be responsible for showing how they implemented an SMS program.

The FAA offers a manual to guide Safety Risk Management (SRM) and Safety Assurance (SA). The SRM and SA are fundamental processes of the SMS with high interaction among their phases. The manual suggests the use of techniques to manage risk based on the severity of the consequences of accidents and on subjective quantification of their probability. The use of those techniques expends management efforts on reducing to some pre-defined acceptable criteria the probability of accidents or the severity of its consequences.

However, the use of probabilities is not the best choice to analyze new systems because there is not enough data to support its assumptions, and the frequency of past events cannot predict future ones. Technology follows along the same line; for example, software behavior is also not stochastic and therefore cannot be evaluated using probabilities. Besides, software (such as electronic flight bags) is continually being updated, and new versions introduced.

In this context, systems theory provides an improved solution for risk management by treating safety as a control problem. It includes a human factors approach, which considers the operator's behavior to be the result of social, psychological, and even environmental conditions. The mapping of actions applied to a controlled process, and the analysis of the feedback that the operator is receiving, provide a qualitative understanding of the real issues behind the unsafe behavior.

### 1.2.1 Research Purpose

This research evaluates an engineering process to identify when risk is increasing during operations by verifying the validity of assumptions incorporated in the hazard analysis, and the effectiveness of operating procedures. This is accomplished by linking concepts of system safety engineering and management actions to show how to apply systems-based concepts to collect operational data and update a hazard analysis. It does that implementing a hazard analysis into a Safety Management System as it identifies indicators of increasing risk to eliminate or control hazards during operations

Therefore, the purpose of this research is to develop and demonstrate an engineering process to identify leading indicators of increasing risk to enforce the imposed constraints over time. The Integrated Safety Management System (I-SMS) is introduced as a safety management framework to guide safety analysts to act on the prevention of accidents. The I-SMS incorporates the treatment of collected data to foster the effectiveness of the system defenses. This new model has a general framework that safety managers can adjust to each specific system. Based on the analysis of data collected in commercial aviation, we hypothesize that the use of the I-SMS will enhance the safety status of aeronautical organizations by providing a qualitative evaluation of system migration towards a state of higher risk.

The I-SMS applies to any complex system, not restricted to the domain of the aeronautical examples provided. The theoretical foundation of the new methods is the Systems-Theoretic Accident Model and Processes (STAMP). STAMP is a modern causation model based on Systems Theory that has proven to be successful in aviation and other industries. The STAMP tool for hazard analysis is called Systems-Theoretically Process Analysis (STPA). The main I-SMS process developed in this research is the Active STPA, a process that treats the data collected during operations to identify the causal factors of unsafe occurrences to reduce the exposure to hazards. The Active STPA integrated with SMS aims to improve the completeness

of any application of STAMP techniques, and to help the generation of new requirements and the refinement of the existing ones.

## 1.3 Methodology

There is always a natural gap between the state of the art and the state of the practice. To understand the state of practice and the challenges that organizations face coping with the new SMS standards, contact with partner airlines was established. During this first stage of research, each partner provided documentation for analysis. In the Summer of 2018, a visit to Air Hong Kong and Cathay Pacific, both in Hong Kong, explored the activities of safety teams in terms of dealing with pilot voluntary reports, internal investigation of occurrences, treatment of Flight Data Monitoring, and preparation for audits with local aviation authorities. Air Hong Kong provided the audit report and SPI trends, while Cathay Pacific sent their safety manuals and arranged a training session in a Boeing 747 simulator. Southwest Airlines was also visited in Dallas and LATAM in São Paulo. The safety managers explained practical examples of the application of their methods to manage safety, including the identification of new hazards and their tools for risk assessment. In general, airlines are using the tools recommended by their corresponding aviation agencies to facilitate the process of compliance during audits.

In order to test the new active process, a complete and original STPA was created by the author, another graduate student of the Engineering Systems Laboratory (ESL), and two MIT undergraduate students. This STPA focused on approach for landing in commercial airliners to reduce the scope of the analysis. The STPA received expert feedback from commercial pilots for refinement. This feedback was complemented by information provided by safety managers of the following commercial aviation partners: Air Hong Kong, Cathay Pacific Airways, Lufthansa, LATAM Airlines, Southwest Airlines, FedEx, Swiss International Airlines, and Emirates.

The data collected from partner operations were protected by non-disclosure agreements (NDA). NDAs that allow the use of observed flight data are especially critical in aviation and require formal acceptance by the pilot's union. Over 1,600 voluntary and mandatory reports were received and organized. After filtering for phases of flight, the number of reports related to unstable approaches for landing was reduced to 155. Each collected event was de-identified, merged, and organized in a single spreadsheet only with the date of their occurrences and a description of the incidents. Additionally, one of the partners sent a complete investigation of a complex event involving parallel approaches, and the data from this event was used for a case study.

The result of this study is the introduction a new method to integrate a modern hazard analysis into an SMS framework, generating indicators that are not currently observed by any of the partner airlines, and that provide relevant safety information for management decision-making. Although the data was collected from a few airlines, the study is shown to have a strong external validity as most airlines comply with the same standards. There are unique aspects

related to cultural differences in terms of attitudes and skills, but the variability of the contexts and human behavior remains the same everywhere.

### 1.3.1 Research Steps

To develop the new framework, the research activities were organized in the following steps:

- Develop an original STPA in aviation
- Identify current safety management practices interviewing safety managers[3] of partner aviation organizations
- Develop a process to identify assumption-based leading indicators for SMS
- Run an Active STPA case study with data collected from a partner[4]
- Develop a new SMS framework
- Run multiple cases to identify new leading indicators

### 1.3.2 Thesis Structure

This dissertation is divided into five chapters. In chapter 2, a review of the applicable literature is presented, starting with an investigation on traditional models and the origins of Systems Safety to discuss the need for modern techniques. Then, there is a discussion of recent solutions for safety management, including the aviation standards for SMS. Finally, an explanation of STAMP, its tools, and its recent studies is provided with a review of the fundamental concepts over which the new models are constructed.

In chapter 3, the Active STPA is introduced. It is divided into three phases, each containing tasks to guide safety analysts on the identification of missing elements of the original analysis. This structure comprises a reasoning about the assumptions made during the implementation of the STPA, and tasks for the elaboration of new defenses to avoid any repetition of unsafe events. Chapter 3 also presents a case study in which the phases and tasks of the Active STPA are exemplified. This case derived from real operational events communicated by one of our partners. An original STPA is used to analyze the case on unstable approaches for landing in commercial aviation. The reasoning about the assumptions is extended to create a discussion of the applicability of the Active STPA in other events.

---

[3] The safety managers who explained current practices were informed that their comments would remain anonymous and their identities or disclosed information could never be tied to them or their organizations. Therefore, there responses are considered to be truthful.

[4] The partner organizations of this study were airlines, one Air Force squadron, and one flight testing institute. The identification of the source of the information presented in this research is not provided to respect non-disclosure agreements signed with each of those partners.

In Chapter 4, the general framework of the I-SMS is presented, followed by a sample structure developed for the case study of Chapter 3. The framework is divided into processes that explain the particularities of the sources of information to the Active STPA. It then describes how the output of the Active STPA should be implemented on the current operating systems. Special consideration is made on the benefits of using the I-SMS in organizations that perform flight testing. The discussion extends to the comparison between assumption-based leading indicators generated by the Active STPA, and the Safety Performance Indicators used today for the aviation SMS.

Finally, Chapter 5 summarizes the conclusions made in this research, listing limitations, contributions, and recommending future studies to explore the new processes.

# 2. Literature Review

The integration of a systems-based hazard analysis into a Safety Management System (SMS) requires multidisciplinary research. This study applies concepts from Systems Safety to address operational concerns through management activities. Thus, it is opportune to review the theory in the following subjects: Systems Safety Engineering, Safety Management, and Safety with STAMP. Additionally, publications on safety leading indicators are reviewed and considerations on the methodology applied to this study are made.

## 2.1 Systems Safety Engineering

A system is an aggregation of elements, referring to parts and people, and processes. Thus, "Systems Engineering is the design of the whole as distinguished from the design of the parts" (Booton and Ramo, 1984). When a system becomes too complicated for a person to understand, there becomes a need for a different approach. Two of the first applications of Systems Engineering were the intercontinental ballistic missile (ICBM) program in the 1950s, followed by the NASA Apollo program in the 1960s. The evolution of the field continued, and the modern complex systems in activity cannot be studied solely with solutions developed in the past, created for simpler and purely mechanical systems. Traditional techniques break down large systems into smaller subsystems to understand it. However, in systems with complex and indirect interactions, socially dynamic environments, and extensive use of software, these parts are not independent, i.e., they would behave differently if isolated from the rest (Rasmussen, 1997).

Traditional accident causality models explain accidents in terms of chains-of-failure-events and have been described using metaphors for easy understanding, such as the Domino model developed by Herbert Heinrich in 1931 and the James Reason's Swiss Cheese model (Reason, 1990). In linear models, accidents are assumed to result from a chain of directly related events, each one necessary and sufficient for the occurrence of the next. In these models, the causes of accidents derive from structural failures, human errors, or energy problems. Using these approaches, failures of the components are considered random, and the appropriate action to make a system safer is to increase the reliability of its components, to design with redundancy, or to add barriers. Therefore, the safety of each system is based on the calculated reliability for each component, and the general approach to reduce risk is to improve each system component' reliability to minimize the chances of an occurrence that would initiate or propagate the chain of events (ICAO, 2018).

Analysis techniques and probabilistic models based on linear causality model, such as Fault Tree Analysis, Event Tree Analysis, Failure Modes and Effects Analysis (FMEA), Failure Modes and Effects Criticality Analysis (FMECA) and Hazard and Operability Analysis (HAZOP), are still widely used (Altabbakh, 2013). These models are still taught in flight safety courses and used by aviation carriers. They explain the basic concepts of flight safety but fail to

analyze the operation of complex systems currently in use (Montes, 2016). The standard causality models do not consider how financial or competitive pressures affect people's behavior. Changes in these behaviors may lead to attitudes that make the system as a whole move to a state of higher risk (Leveson, 2011).

Systems Theory, on the other hand, productively explains the relationship between components as a complex structure, rather than consisting only of simple and direct connections. Each hierarchical level controls the relationship among the lower-level components, imposing constraints on their degrees-of-freedom, and controlling their behavior (Checkland, 1981). A system is an abstraction, which is made up of a set of components that act together as a whole to achieve some common goal, objective, or end. Systems are embedded in their environment, which is defined as a set of components, and their properties, that are not part of the system but whose behavior can affect the state of the system. Systems are shaped by law and industry standards, but they are also affected by business relations and markets. For example, as it relates to aviation, unsafe conditions go far beyond equipment failures. Aircraft crews experience fatigue, act based on limited information, and use techniques learned from an instructor during training. Therefore, the safety level of operational tasks such as takeoff, approach, and landing, would be wrongfully represented only by quantitative metrics. Safety is better represented as a control problem of a hierarchically organized complex system.

One of the emergent properties of a complex system is safety. Leveson (1996) defines safety as freedom from harm, not meaning that a safe operation is risk-free. Similarly, ICAO 9859 states that the objective of safety efforts is to reduce the risk of harm. The application of concepts of systems theory to safety initiated an entire new field.

*"Systems safety covers the total spectrum of risk management. It goes beyond the hardware and associated procedures of systems safety engineering. It involves: attitudes and motivation of designers and production people, employee/management rapport, the relation of industrial associations among themselves and with government, human factors in supervision and quality control, documentation on the interfaces of industrial and public safety with design and operations, the interest and attitude of top management, the effects of the legal system on accident investigations and exchange of information, the certification of critical workers, political considerations, resources, public sentiment and many other non-technical but vital influences on the attainment of an acceptable level of risk control. These non-technical aspects of system safety cannot be ignored"* (Lederer, 1985).

There are many key figures who contributed to theories of system safety. C.O. Miller, for example, introduced system theory concepts to safety in the 1950s and started applying to aviation in the 1960s. He also claimed to be the first to use the term "System Safety." Some of the ideas and tools developed for systems safety became industry standards. For example, an important reference on systems safety for military applications is the MIL-STD-882E (2012), in which system safety is defined as "the application of engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational

effectiveness and suitability, time, and cost throughout all phases of the system life-cycle." Therefore, based on standards like the MIL-STD-882E, modern organizations started to implement procedures for risk management.

Currently, most aeronautical organizations decide on how to prioritize the implementation of safety controls, and to judge if action is worth taking, based on risk assessments. This risk management is the evaluation of both on-going and new initiatives in a systematic attempt to address areas with the potential to pose a risk to safety during operations. Head and Horn (1991) define risk management as "the process of making and implementing decisions that will minimize the adverse effects of accidental and business losses." This traditional approach seeks to evaluate and reduce the likelihood of an event or minimize its consequences. In the long term, any of those actions should maximize the benefits regarding time and cost. However, people have different thresholds when assuming risks. Everyone has a particular idea of acceptable risk. Judgment on likelihood with one expert assessment is inaccurate as two different people could make significantly different estimations based on their knowledge on a particular subject (Wiegmann, 2005). Therefore, such prediction of future events usually has weak foundations when the system is complex, as are many of the software-controlled ones.

As some degree of risk is a fundamental reality, risk management becomes a process of tradeoffs. For example, the term ALARP (As Low as Reasonably Practical), used by a few agencies and airlines, means that the risk is low enough that attempting to make it lower, or the cost of mitigating it, would actually be costlier than any cost likely to come from the risk itself (ICAO, 2019). The problem is indirect costs of operating under hazardous conditions, such as the impact on reputation, are difficult to calculate, and often go far beyond the direct costs. In addition, it is impossible to assess the risk because "reasonably practical" is undefined and highly subjective, and depends on who is paying for the risk reduction activities versus who is assuming the risk.

To build safety into systems, it is necessary to understand the limitations of its components to design appropriate protections. Fitts (1954) compared humans and machines, pointing that humans have natural advantages like adaptability and disadvantages like inconsistency. Therefore, human error alone is not a justification for any unsafe event (Dekker, 2006) because the system must be designed for the variability of human behavior. In a robust safety-critical system, single component failure or a common human error should not result in catastrophic consequences. Also, safety relates to all physical and abstract parts of a system, including not only people, materials, and equipment, but also procedures, software, and tools. Thus, safety requires a holistic approach because the environment, including social and cultural particulars, has contributing factors that cannot be ignored anymore.

## 2.2 Safety Management

The balance between efficiency and safety has always been a challenge for management. This delicate balance is needed to prevent losses and shape functioning Safety Management Systems (SMS). Safety Management is a function of an organization that combines principles and processes to prevent accidents and adverse consequences that may come from it. "Safety management practices not only improve working conditions but also positively influence employees' attitudes and behaviors with regard to safety, thereby reducing accidents in workplace" (Vinodkumar and Bhasi, 2010). Every organization that deals with safety-critical events need a safety management system. These events might be related to production processes, services, or even the use of products by customers. Large and complex companies, such as aircraft manufacturers, need to deal with events from all of the above activities and safety becomes a part of a company with many professionals entirely dedicated to run the SMS. They need to react to incidents and to act proactively to avoid future ones. This process is a continuous set of tasks that requires diligence and is enhanced by experience.

Leveson explains (Figure 3) that management leadership creates a safety culture, which drives the behavior of people. Managers are required to establish a safety policy and create a control structure with responsibilities, accountability, authority, safe controls, and feedback channels. Safety management shall communicate safety requirements and constraints to the organizations running the operations. These organizations, must report operational issues to allow continual improvement.

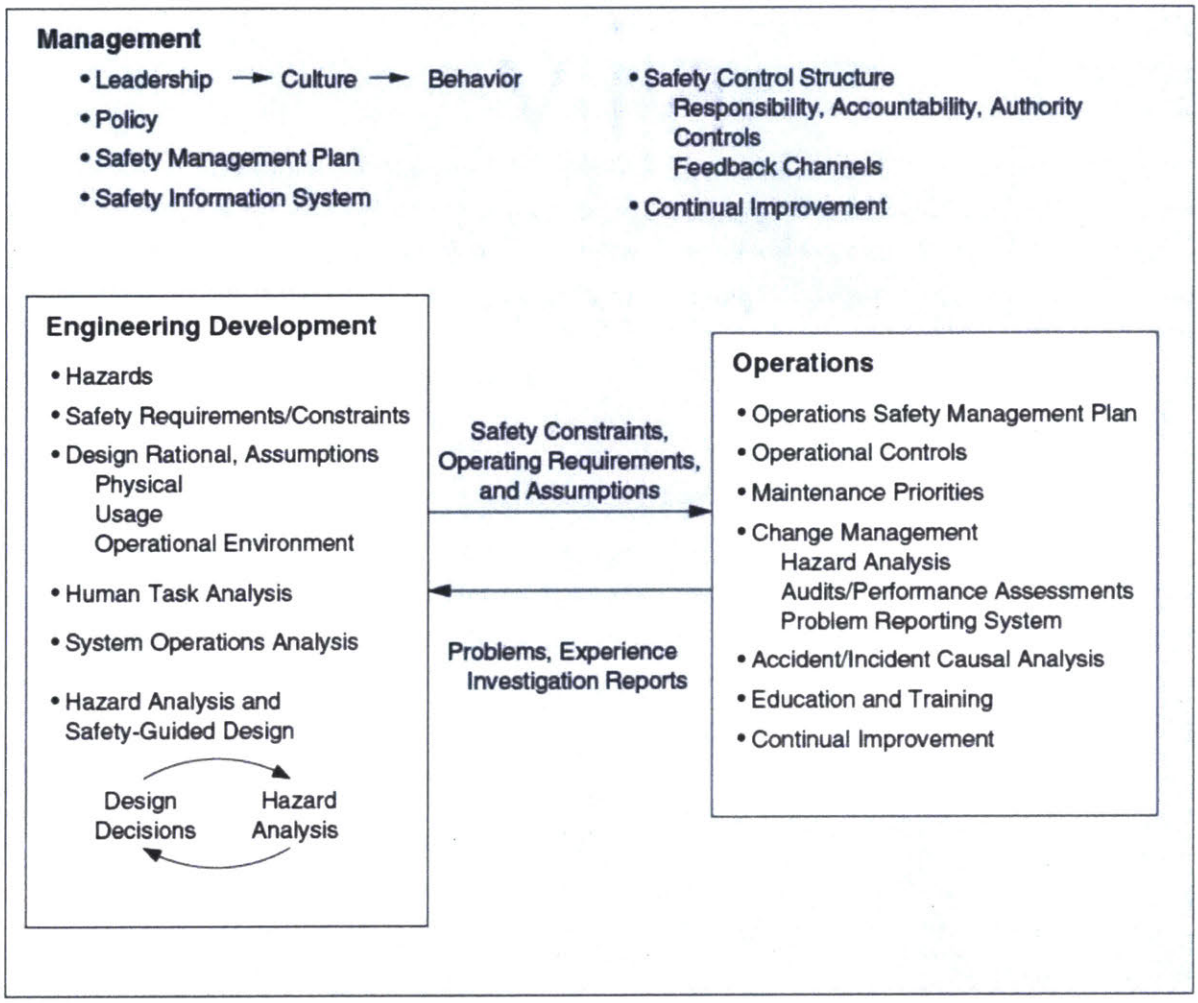



**Figure 3. Safety management and information flow (Leveson, 2011)**

### 2.2.1 Safety Management Systems (SMS)

Every company that has complex and safety-critical operations has safety objectives. The implementation of a structured Safety Management System (SMS) helps to achieve these objectives. The structure is different for every company and defined by the type of service provided, and the sociotechnical and regulatory environment that it operates in. An SMS should include the definition of a safety control structure to map expectations and responsibilities to eliminate or reduce losses. The assignment of who is responsible for what in the control structure determine the distribution of the accountability for incidents and accidents. In this context, the analysis of incidents should include identifying why the safety control structure was unsuccessful in preventing it.

A control structure is not restricted to mapping hierarchical relationships; it also shows the required coordination between the components of a complex system. This coordination is especially important when more than one person is responsible for the same process. When both

controllers believe that the other is monitoring the process, there will be a moment when no one is actually doing it (Leveson, 2013). The delegation of responsibilities and the communication channel for coordination must be clear to avoid losses caused by simple misunderstandings.

Li and Gundenmund (2018), compared different theoretical modeling of SMS, in a vast literature review. They analyzed the impact of SMS models based on cause-effect relationships and the insertion of safety barriers in an event sequence to connect the chain of failure events model to the management model. Recently, there are studies being conducted measuring the SMS effectiveness of those approaches using different techniques, such as the treatment of operational data with the model Data Envelopment Analysis (DEA) (Stolzer et al., 2018).

### 2.2.2 Aviation standards for Safety Management Systems

The concept of an SMS exists in many industries, and it is defined in aviation standards as a systematic approach to identify and control risk (Federal Aviation Administration, 2015). The concept of risk is defined by the MIL-STD-882E, ICAO, and FAA publications as a combination of the probability of an outcome and the severity of its consequences usually organized in risk matrices (Figure 4).

| Risk probability | Risk severity | | | | |
|---|---|---|---|---|---|
| | Catastrophic A | Hazardous B | Major C | Minor D | Negligible E |
| Frequent 5 | 5A | 5B | 5C | 5D | 5E |
| Occasional 4 | 4A | 4B | 4C | 4D | 4E |
| Remote 3 | 3A | 3B | 3C | 3D | 3E |
| Improbable 2 | 2A | 2B | 2C | 2D | 2E |
| Extremely improbable 1 | 1A | 1B | 1C | 1D | 1E |

**Figure 4. Risk matrices (FAA, 2019)**

The coding in the risk matrix may vary, but all solutions are used to feed acceptance criteria, like the one shown in Figure 5. Risk is clearly understood in hindsight after an accident but can be proactively identified through formal safety management programs or experts' intuition.

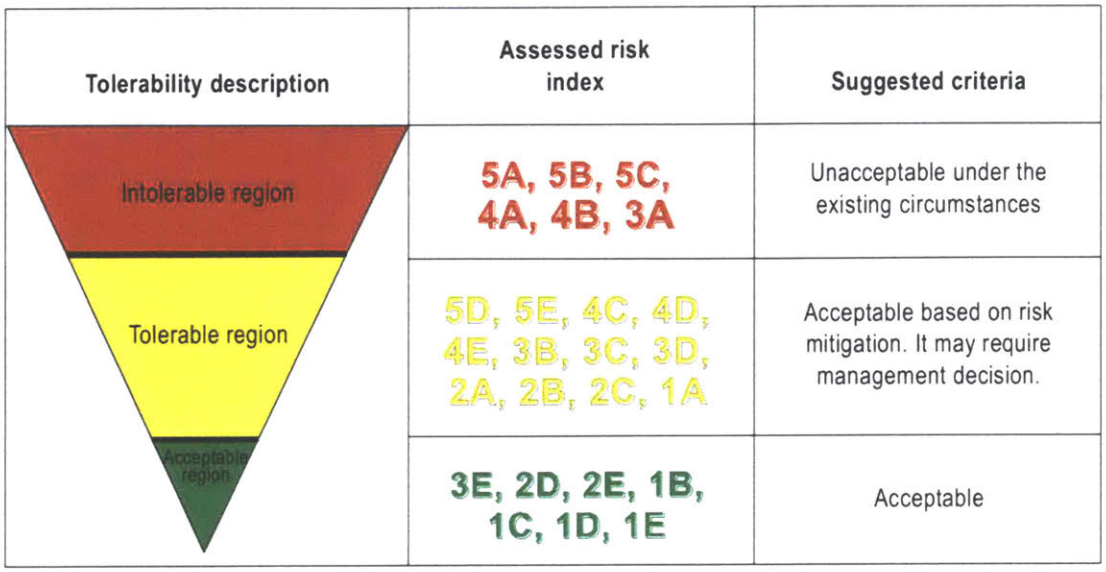



**Figure 5. Risk acceptance criteria (FAA, 2019)**

The International Civil Aviation Organization (ICAO) defines SMS as a systematic approach to manage safety. In aviation, SMS has a structured way to ensure compliance with regulatory standards (FAA, 2015). Its main objective is the operation with minimization of occurrences (incidents and accidents), or more directly, the minimization of damage to aircraft and injury to people. To achieve this objective, aviation agencies use official documents to specify how to develop and implement an SMS, pointing to the necessity to make continual improvement in the level of safety in operations.

In the United States, Title 14 of the Code of Federal Regulations (14 CFR) Part 5 suggests, with regards to statutory requirements, a basic set of processes integral to an effective Safety Management System (SMS). The advisory circular (AC) 120-92B is a document that presents methods for implementation of 14 CFR part 5 SMS requirements. It defines SMS as an organization-wide comprehensive and preventive approach to managing safety (FAA, 2015). The methods suggested in AC 120-92B are not the only means of compliance; it also recognizes that SMS needs to have formal methods for identifying hazards and risk mitigation. The SMS is intended to be developed by the organization using existing operations and business decision processes to assure the improvement of the overall safety performance, and create a positive safety culture[5]. Likewise, the AC-120-92B describes SMS requirements for Aviation Service Providers suggesting in its Appendix 2 a standard form to list hazards, their potential consequences, severity, and likelihood.

[5] Culture is defined by Edgard Shein (Borovec et al., 2011) as a pattern of shared basic assumptions learned by a group as it solved its problems of external adaptation and internal integration.

The severity is always considered as the worst foreseeable scenario while probability is an estimation of future likelihood of failures or errors based on the observed frequency of past events to predict the future based on experience (e.g., frequency of past events) and common sense (or engineering judgment). On systems with low innovation rate, the expected probability of future events is not so different than the recorded frequency of past events. But as aviation is an innovative industry and deals with rare events that affect safety, the estimation on the frequency of occurrences may be completely wrong. Thus, assigning probabilities for unsafe events is not a reliable metric.

In any probabilistic model, such as Bayesian inference, the assumption of independence made in every estimation hardly hold in fielded operations. Since accidents are rare and the causal factors are different in most modern accidents, ignoring conditions because they have a low probability would not avoid most of the recent accidents. Events classified as *improbable* with a *minor severity* are automatically considered by current classification as *acceptable* as it is, meaning that no further mitigation is required, even when the defense[6] would be easily implemented. Therefore, any complex scenario with a combination of *acceptable* elements constitutes a potential accident that will never be avoided using risk matrices.

The concept of an acceptable level of safety (ALoS), used by ICAO and aviation agencies, including FAA, in SMS standards, is measured by Safety Performance Indicators (SPI) and Safety Performance Targets (SPT). In organizations using this approach, SPIs are linked to the major components of the Safety Management Systems (SMS) and become the measure of the level of safety for each internal department. SPTs (goals or objectives) are determined by considering what safety performance levels are desirable and realistic. These solutions are in place because the company top management wants measurable safety targets that are acceptable to regulators and other stakeholders, as well as consistent with SMS. Title 14 CFR, paragraph 5.71 on Safety performance monitoring and measurement, states that the operator must develop and maintain processes to acquire operational data to monitor the safety performance of the organization. These processes and systems must include the following:

1. *Monitoring of operational processes.*
2. *Monitoring of the operational environment to detect changes.*
3. *Auditing of operational processes and systems.*
4. *Evaluations of the SMS and operational processes and systems.*
5. *Investigations of incidents and accidents.*

---

[6] The term *defense* in ICAO SMS standards is defined as *specific mitigating actions, preventive controls or recovery measures put in place to prevent the realization of a hazard or its escalation into an undesirable consequence.*

6. *Investigations of reports regarding potential non-compliance with regulatory standards or other safety risk controls established by the certificate holder through the safety risk management process.*
7. *A confidential employee reporting system in which employees can report hazards, issues, concerns, occurrences, incidents, as well as propose solutions and safety improvements.*

The airline is also to use the data collected with the sources above, to maintain a process to analyze the data. For Safety performance assessment, the operator must:

1. *Ensure compliance with the safety risk controls established by the certificate holder.*
2. *Evaluate the performance of the SMS.*
3. *Evaluate the effectiveness of the safety risk controls and identify ineffective controls.*
4. *Identify changes in the operational environment that may introduce new hazards.*
5. *Identify new hazards.*

Paragraph 5.75 of the FAA 14 CFR refers to continuous improvement and requires the certificate holder to "establish and implement processes to correct safety performance deficiencies" identified in a safety performance assessment. However, this current approach focus on informing the SA about what occurred in the past without explaining important causal factors that affect safety and may result in accidents, such as:

- Pilot's awareness of hazards
- Effectiveness of CRM call-outs
- Complacency with rules
- Willingness to report
- Practicality of procedures
- Reliability of equipment
- Safety of the airspace and airports

In theory, the measurement of safety performance in SMS is supposed to provide a preventive approach to safety in all operations. However, the lack of a structured hazard analysis prohibits pro-active actions, and in practice, most of the actions of safety managers are reactive, often when it is too late. "Hazard analysis is the heart of system safety approach" (Roland and Moriarty, 2009). Careful hazard analyses are key to provide the knowledge necessary to reduce risks. However, in dynamic systems, operational safety depends on a process to actively run a hazard analysis throughout its operational lifetime.

The limitation to an active hazard analysis is that, currently, there are a restricted number of safety inspectors to perform a complete safety oversight on operations. Even with the number of accidents, per hours of flight, lower than ever, as described in Chapter 1, air transportation growth may outpace the safety management capability. The solution is the development of more

effective tools for safety management. SMS methods may map actions applied to a controlled process, and operator feedback analysis, to provide a qualitative understanding of the real issues behind unsafe behavior. Therefore, it becomes necessary to review models introduced to manage safety. An example of a model currently in use by some agencies and airlines is called Bowtie.

## 2.3 Bowtie

This model originated from fault and event tree methodologies but evolved to become a visual tool to depict risk and identify safety barriers currently in place, or those lacking in the system. Bowtie was created in the late 1960s and gained more interest when the oil and gas industry started to use it in the 1990s, and has extended to other industries since then. It is a chain of events model designed for Performance-Based Regulations (PBR)[7].

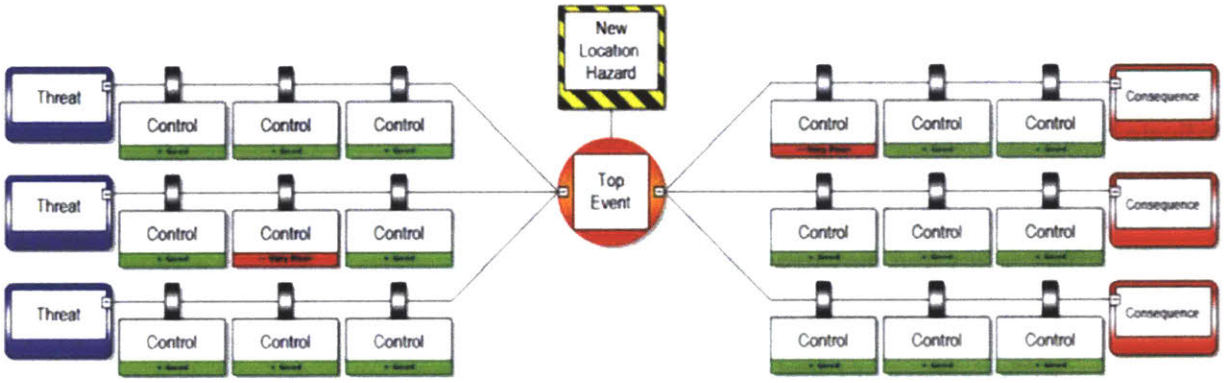



**Figure 6. Structure of the Bowtie model (CAA UK, 2019)**

Figure 6 depicts the structure of the Bowtie model. According with the CAA UK, on the left side, Preventative Measures are used to eliminate the threat or prevent the threat from causing the Top Event recovery; while on the right side, Control Measures are used to reduce the likelihood of the Top Event or mitigate the severity of its consequence. The model recognizes controls as barriers, similar to Reason's Swiss Cheese model but adds failure mechanisms called "Escalation Factors," i.e., explanations for the ineffectiveness of controls.

Bowtie also lists hazards as potential sources of harm. In Bowtie, hazards are objects or activities with the potential of causing injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function. Hazards are organized at a higher level of abstraction and detailed for particular concerns. It uses the term "Top Event" to define an unsafe state that is not yet an accident, i.e., events with the potential to become disasters if not controlled in time, such as a loss of control during a flight. This definition of the term Top Event in bowtie relates closely to the meaning of a Hazard in safety engineering.

[7] Performance-Based Regulation (PBR) is an incentive regulation to strengthen performance incentives, such as the aviation safety performance indicators.

Threats are characterized as possible causes for the potential release of a hazard by producing a Top Event. They are listed on the left side of the model. Between the threat and the Top Event there is a linear sequence of controls. On the right side, a list of consequences is depicted. Between the Top Event and each consequence, there are a series of independent recovery controls. The idea of organizing the controls sequentially is that if one fails, the next comes into play.

Each control has a list of Escalation Factors. It is important, in the Bowtie model, that these factors are detailed, although this can cause the list to be very long, which may impede it from fitting into any reasonable visual diagram. Finally, each escalation factor receives specific new controls, adding more complexity to the analysis.

This approach is supposed to be used as a reactive classification of safety events and a proactive risk assessment tool for aviation SMS. However, Bowtie has an analytic restriction as controls are organized linearly, causing its analysis to be intrinsically simply an event chain. Parallel controls may be implemented to capture systems-level problems. However, in some situations, controls are not independent as assumed, as they may overlap and conflict.

## 2.4 STAMP

Systems-Theoretic Accident Model and Process (STAMP) is a new model of causality, which is based on Systems Theory and Control Theory. It includes both technical and social aspects, explaining the interaction between components and behavioral events. STAMP applies to very complex systems because it works top-down from a high level of abstraction rather than bottom-up. Systems are seen as a hierarchy of organizational levels in a dynamic control environment (Leveson, 2011). STAMP is useful because it includes software, humans, organizations, and safety culture as causal factors in accidents and other types of losses without having to treat them differently or separately (Leveson, 2004).

Systems-Theoretic Process Analysis (STPA) is a hazard analysis technique based on STAMP. STPA covers not only the accidents caused by component failures but also those caused by a faulty interaction between components of a system, that are each functioning properly, as a consequence of system design flaws. It recognizes safety and security as emergent properties of a complex system caused by the interaction of its components. The main characteristic of security is the malicious intentions behind control actions. But the term safety can be treated as more comprehensive, encompassing both well-intended operators and the ones attacking the system.

STPA is a rigorous top-down systems' engineering technique that has the ability to identify potential design flaws. It begins by identifying the possible losses and their associated hazards. Losses are consequences of an undesired, unacceptable, and unplanned event as a result of a hazard. Hazards must be prevented because they could lead to a loss in a worst-case

scenario. When the focus is analyzing security, a hazard is also known as a vulnerability. Both of these terms are defined as a system state that leads to an accident or loss.

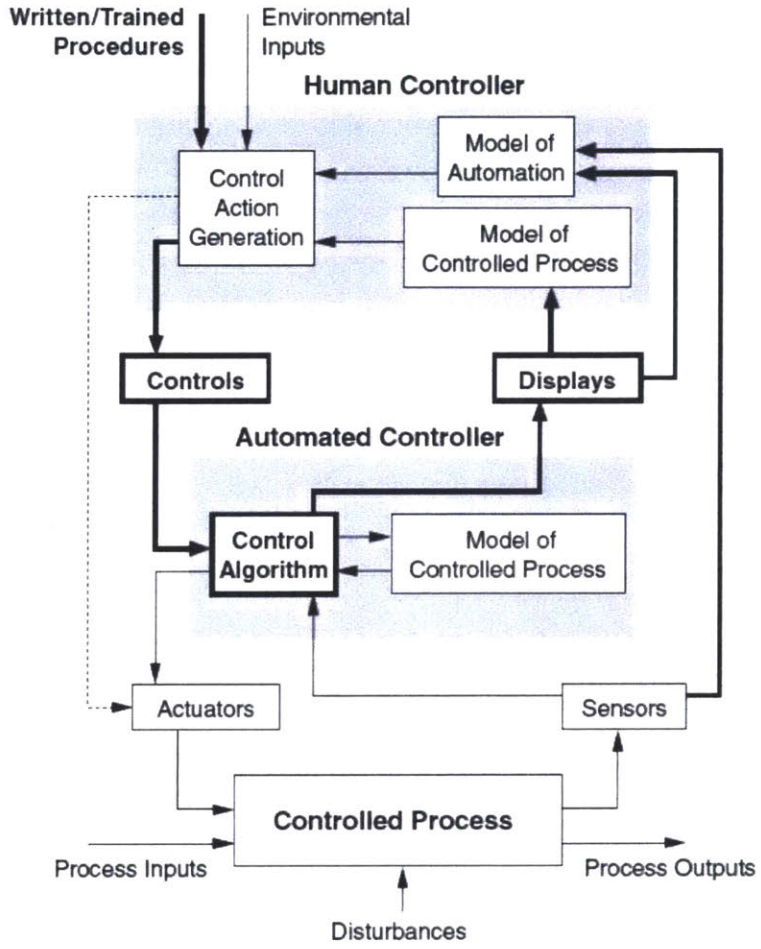



**Figure 7. STPA control loop with automated controller (Leveson, 2011)**

STPA uses a model of the systems' safety control structure, as presented in Figure 7, for the identification of potential unsafe control actions. Each unsafe control action is explored to generate scenarios that can lead to them. Finally, the analyst generates system and component safety requirements and constraints, as well as design changes that can eliminate or mitigate the causal scenarios. STPA also includes human factors in the analysis, exploring even psychological issues that contribute to causal scenarios (Leveson, 2014). Chapter 3 of this dissertation gives an example of a complete STPA on approaches for landing, using partner data.

Another widely used technique based on STAMP is CAST, which stands for Causal Analysis based on Systems Theory (Leveson, 2019). It is a tool for accident analysis that, compared with STPA, has a retrospective nature. Its purpose is to identify the causal factors of an accident that has already occurred.

The STPA has been augmented for security (Young, 2014), human factors and flight testing (Montes, 2015 and France, 2017), coordination among multiple controllers (Johnson, 2017), continuous closed-loop systems (Castilho et al., 2018), and many other aspects. STPA is the ideal hazard analysis technique for this research because it is systems-based and top-down. The update of a hazard analysis is more straight forward using STPA because it begins at a higher level of abstraction and goes deeper into details as the analysis progresses.

## 2.5 Leading Indicators

The use of hazard analysis is paramount to map the weaknesses of a system, but human and equipment behavior may deviate from the original design to a state of higher risk (Rasmussen, 1997). One of the reasons for this deviation from the baseline performance is that managers often make optimistic assumptions on operator training, motivation, and competency. Deviation occurs when practices replace official procedures and risky behavior becomes normal. It is driven by complacency and characterized by a false sense of safety. Understanding deviation, its causes, and its intensity become important when designing actions to correct the deviation and maintain a higher level of safety. However, even an analysis with a rigorous scientific approach may be unsuitable for operations without continuous improvement. Therefore, a comprehensive method is needed to enforce vigilance and guide the analysis of the collected data.

Indicators may be divided into two types: leading and lagging. Lagging indicators are output measurements after the fact. They are more common in the industry because they are easily identified. Modern systems use computers to monitor the data read by multiple sensors. The value of those readings has a band that represents a normal operation. Indicators that use parameter values that exceed that band are considered as lagging indicators. Therefore, they are useful to run statistics and to prepare trend charts.

However, the proactive treatment of data requires the observation of parameters that may become a contributing factor in future unsafe events. Therefore, leading indicators are the ones that signal when intervention in the system becomes necessary before any incident. Leading indicators are predominantly used in occupational safety (Gallagher et al., 2016), focusing on the identification of both quantitative and qualitative approaches. There are several purely quantitative approaches trying to measure the result of SMS practices on risk exposure (Oien et al., 2011), but the focus is on measuring risk without providing the information necessary to eliminate it. One of the challenges of using leading indicators is the isolation of their contribution to prevention.

After a loss, it may be easy to identify in hindsight the signs that an accident was about to occur within the system. In real operations, however, the identification of those signs before the accident can be highly challenging. Airlines are collecting a large amount of data, hoping that useful information will eventually be generated. One of the aviation partners of this research is recording terabytes of flight data per week, extracting only basic trends from it, and storing these

data on hard drives for future analysis. According to this partner, safety managers hope that one day, a new method or set of new tools will be able to read the big data, identify patterns, and tell them how to improve safety and efficiency.

### 2.5.1 Assumption-based Leading Indicators

Leveson (2015) proposed the idea of the assumption-based leading indicator as an approach for risk management in engineering, defining it as "*a warning sign that can be used in monitoring a safety-critical process to detect when a safety-related assumption is broken or dangerously weak and when action is required to prevent an accident. Alternatively, a leading indicator is a warning signal that the validity or vulnerability of an assumption is changing*".

The goal of an assumption-based leading indicator program is to monitor the assumptions upon which the safety of the system was assured, both to find assumptions that originally were incorrect and those that have become incorrect over time. The assumptions considered are mechanical, social, organizational, and managerial (Leveson, 2015). Assumption-based leading indicators are identified when an assumption is violated, and corrective action is necessary. The challenge is to develop a method able to capture the unintentional degradation of safeguards and controls, that lead to the migration of the whole system to a state of higher risks.

In this idea, useful leading indicators of increasing risk can be identified based on the assumptions underlying the safety design process for the specific organization, product, or operations. This approach recommends the following assumptions be checked:

- The models used during initial decision making and design are correct.
- The system is constructed, operated, and maintained in the manner assumed by the designers.
- The models and assumptions are not violated by changes in the system, such as workarounds or unauthorized changes in procedures, or by changes in the environment.

Safety analysts also make assumptions on how the system will operate in the future. These assumptions depend on the experience with previous products and engineering judgment. They can also be verified by adding requirements to product testability. The assumptions made during the elaboration and implementation of an STPA may come from:

- High-level system goals generated during concept development
- System-level requirements generated from system goals
- Assumptions about the external environment in which the system will operate
- System behavioral requirements imposed by safety-related environmental requirements and constraints (including constraints on the use of the system)

- STPA-generated hazards, the hierarchical control structure, unsafe control actions, and causal scenarios
- Design features devised to manage the causal scenarios
- Operational requirements created to manage causal scenarios
- Limitations in the design of safety-related controls, including operational controls

To guide the identification of assumptions-based leading indicators of increasing risk, Chapter 3 introduces the Active STPA.

# 3. Active STPA

This Chapter starts with a general description of the Active STPA. Before getting into detail, a case study is presented, including the description of an original STPA on unstable approaches for landing. Then, the Phases and Tasks of the Active STPA are introduced and applied to the case study.

Upon visiting our partner aeronautical organizations, we observed current safety management as typically reactive, with no structured methods to anticipate future problems. Based on the formal documentation provided, when management is concerned about a specific issue, they run a hazard analysis, which tends to have a limited scope. The outcome may lead to changes in procedures and extra monitoring activities, but as soon as the changes are implemented, the analysis is only revisited if an incident or accident occurs. This reactive system does not prevent accidents effectively. It is also an inefficient use of analysts' working time.

This study defines a new process to keep a live update of an existing Systems Theoretic Process Analysis (STPA). This process, called Active STPA, uses operational data to check for assumption-based leading indicators. In Active STPA, an STPA performed during system development or in fielded systems becomes a structure that will constantly be evolving as it is revisited during the lifetime of the system. The output of this active hazard analysis helps the organization adapt to its dynamic reality.

In an ideal system, STPA should start in the Concept of Operation (ConOps) stage to write system-level requirements. An exhaustive hazard analysis leads to a product that is more robust when fielded for two reasons. First, systems are safer when developers build safety from the beginning. Second, it is easier and less expensive to fix problems in the early stages of system design and development. The enhancement of the hazard analysis requires shaping test events to explore particular scenarios. Testing these scenarios in a controlled environment is safer than waiting for the scenario to occur during operations.

Ideally, the developer should deliver the hazard analysis to the operator as part of the product. However, this is hard to implement because any losses in operations could be followed by lawsuits using the hazard analysis to question design decisions. Yet, if the operator never receives a hazard analysis from the manufacturer, it is still possible to perform an STPA while the system is operating. Such analyses could give a picture of the current deficiencies of system operations and deliver the STPA constraints[8].

For instance, consider that an organization performed a complete STPA for the operation of new equipment. Also, assume that it has followed STPA's four basic steps, i.e., defining the purpose of the analysis, modeling the safety functional control structure, identifying the Unsafe Control Actions (UCA), and identifying loss scenarios. The STPA would have already identified behavioral and social peculiarities for training and operational contexts. However, the fact that

[8] According to Leveson (2011), constraints represent "acceptable ways the system or organization can achieve the mission goals."

the analysis was finished, and the defenses[9] applied, does not necessarily make the system free from surprises. In general terms, the potential flaws would be:

- Analysts made inaccurate assumptions about the operation
- The analysis was incomplete
- The mapped defenses were not completely applied
- The requirements or the constraints were not followed or intentionally violated
- Changes that occurred during operations invalidated the assumptions embedded into the STPA

Thus, the safe operation of a system using STPA requires:

- An accurate and up to date safety control structure
- A reasonably complete set of UCAs and scenarios
- The assurance that defenses are applied
- Conformance with identified safety requirements and constraints
- An active process to identify when assumptions made in the original analysis are no longer valid or are systematically violated

Safety-critical organizations need to explore operational experience to develop effective preventive activities. Safety should not only count on the experience of a few professionals, as they would have only been exposed to a part of the possible hazards, instead, it must be a process that observes the operation and collects data to learn from its vulnerabilities. If an accident happens on a system that has already performed STPA, there is a chance that the analysis already covered the problem, but the procedures based on lower-level constraints were not practical. The Active STPA was developed to identify leading indicators of increasing risk using feedback from operations throughout the system's lifetime, continually updating the STPA.

To apply the Active STPA, the organization needs to:

1. Create an original STPA or use an existing one
2. Implement the controls recommended by the STPA
3. Collect operational data
4. Run the Active STPA

[9] In Active STPA, defenses are safety risk mitigations, or more specifically, actions that control the implementation of changes to operating procedures, equipment, or infrastructure.

The STPA may have a reduced scope or cover the entire operation of the organization, depending on its complexity and the available resources. The STPA includes a traceability system that connects all STPA elements, from Losses to Constraints. This system facilitates the identification of missing elements when running an Active STPA case.

Once the STPA is finished and implemented, the SA uses data collected from different sources, such as the description of an operational incident. Incidents in aviation are occurrences associated with the operation of an aircraft which affects or could affect the operational safety (ICAO, 2018). Incidents differ from accidents[10] as they are events that do not result in a serious loss but have the potential to if occurred in a certain context. Incidents should be looked at as a sign of weak safety defenses due to dysfunctional interactions between systems components.

The Active STPA starts by analyzing an input message, such as a voluntary report, to determine whether the hazard analysis is incomplete or procedures in practice are ineffective. When a hazard analysis is incomplete, a SA (Safety Analyst)[11] conducts a systematic process to evaluate the problem and update the hazard analysis. Conversely, when the analysis is complete, but constraints were violated, the SA investigates why the rules were not followed to adapt the procedures or to enforce the current ones. In both cases, management needs a method to identify which actions are necessary to avoid future repetition of the event.

The description of the incident becomes a message to the SA called AHAI (Active Hazard Analysis Input). The AHAI uses a specific format to describe events. It starts with the context, followed by a description of all control actions of each controller, even from different hierarchical levels. The description of the incident must explain in chronological order all the actions (or absence of action) of each de-identified controller in full sentences. For example, the AHAI describing an incident involving the ATC (Air Traffic Controller) and two aircraft could be:

- *The ATC cleared aircraft A to land on runway 18 when aircraft B was taking off. Aircraft B aborted takeoff at 90kt due to bird strike on engine 2. Aircraft B reported aborting to ATC at 8:30:55. Aircraft A decided to go around at 8:30:58 after touch down and before the application of brakes or reverse thrust. Aircraft A passed 80ft above Aircraft B between taxiway C and D.*

As a reasonable description of the facts is mandatory, the SA must investigate incidents using multiple sources and add the findings to the AHAI. If the investigation finds conflicts

[10] Accident is defined by the Convention on International Civil Aviation Annex 13 as an occurrence in which "a person is fatally or seriously injured, the aircraft sustains significant damage or structural failure, or the aircraft goes missing or becomes completely inaccessible" (ICAO, 2016).

[11] Safety Analysts (SA) are domain experts. In aviation, some of them are active pilots in their companies, others are safety specialists working full time in the safety division of the organization.

among different sources, all versions must be registered as this may be a sign of confusion, fear of blame, or cognitive/memory limitations.

The Active STPA is a process divided in the following three Phases named to represent what the SA is expected to achieve:

- Phase 1: Inspect the STPA
- Phase 2: Reason about the Assumptions
- Phase 3: Solve and Update

From one AHAI, one or more Cases[12] may be generated. To avoid confusions caused by events with multiple controllers, the SA runs independent Cases, one for each identified controller in a higher-level functional control structure. If two similar controllers (same hierarchical level) committed different Unsafe Control Actions (UCAs), there will be two Cases running in parallel. Figure 8 shows how an AHAI, describing an incident, becomes the input used to generate Cases into the Active STPA. In each Case, the SA runs all three Phases to understand what the underlying problem is and to find a solution to fix it.

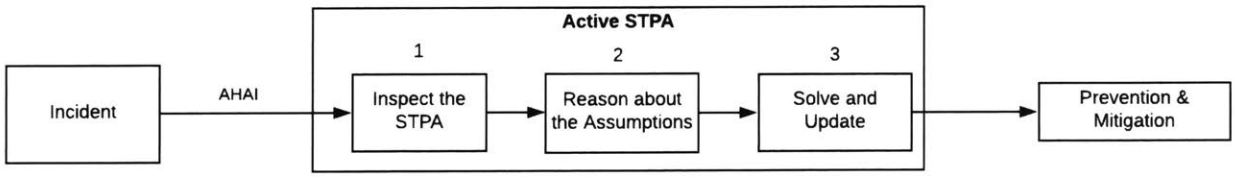



**Figure 8. Phases of Active STPA**

Each of the three Phases is divided into tasks, as presented in Table 1. Tasks are actions that the SA is required to perform in each Case.

[12] In this dissertation, the terms Case, Phase, and Task have their first letter capitalized when referring to Active STPA elements.

**Table 1. Summary of Phases and Tasks of the Active STPA**

| **Phase 1 - Inspect the STPA** |
|---|
| 1.1 – Search for applicable rules and procedures |
| 1.2 – Verify requirements and constraints |
| 1.3 – Verify causal scenarios |
| 1.4 – Verify control actions and UCAs |
| 1.5 – Verify control relations in safety control structure |
| 1.6 – Verify System-level requirements and constraints |
| 1.7 – Verify Hazards and Losses |

| **Phase 2 - Reason about the Assumptions** |
|---|
| 2.1 – Identify violated assumptions |
| 2.2 – Analyze trends |
| 2.3 – Investigate causal and contributing factors |
| 2.4 – Determine the reason for broken assumptions |
| 2.5 – Identify if contingency protections worked |

| **Phase 3 - Solve and Update** |
|---|
| 3.1 – List possible defenses |
| 3.2 – Analyze tradeoffs |
| 3.3 – Determine the optimum solution |
| 3.4 – Implement new defenses and protections |
| 3.5 – Update the STPA |

The explanation of what the SA is supposed to perform in each of the Tasks requires examples. Therefore, a case study on unstable approaches is presented in the following section.

## 3.1 Case Study - Unstable Approaches

*"The duty of an air carrier is to provide service at the highest level of safety in the public interest". (Title 49 USC 44702)*

This section begins with an overview of the actions that take place in the cockpit during an approach for landing and a description of what makes approaches unstable. Then, a STPA pertaining to approaches for landing developed for this study is presented. Information collected from our partners explains how airlines observe and treat data to help mitigate unstable approaches. Finally, the Tasks of the Active STPA are explained using an incident to run three Active STPA Cases.

According to the Safety Performance Monitoring Survey developed by the Flight Safety Foundation (2019), 76% of the global aviation industry sets targets for their performance metrics, and 83% of these targets are on unstable approaches. Among the methods for data analysis, the *causal factor analysis* corresponds to 68% of the methods and voluntary reports correspond to 94% of the cases as a source of data while Flight Data Monitoring is the source in 61% of the events. Thus, it is opportune to discuss unstable approaches by the light of the Active STPA using data from pilot reports and flight data monitoring.

### 3.1.1 Approach for landing

There are numerous ways in which an aircraft can navigate for landing. Up until the 1940s, all approaches were visual, but technology has allowed an evolution of airborne systems that granted precise landings in Instrument Meteorological Conditions (IMC). Most aircraft are equipped with technology, such as antennas that sense the signal from radio beacons installed on the ground, including special antennas close to the runway threshold and from satellites. Today, most commercial airliners use the ILS (Instrument Landing System), even in Visual Meteorological Conditions (VMC), on approaches for landing. The ILS has separate antennas for horizontal and vertical guidance. Horizontal guidance is provided by an array of antennas known as a localizer (LOC). The signal of this antenna is interpreted by the navigation system of the aircraft, while the Primary Flight Display (PFD) shows the deviation from the alignment with the center of the runway. Similarly, the vertical guidance comes from another set of antennas called Glide Slope (GS). When the indication of the GS to the pilot is centered, the trajectory of the aircraft is a slope of approximately three degrees to a touchdown point located roughly one thousand feet beyond the runway threshold.

Satellite-based navigation systems (e.g., GPS) are part of an embedded navigation system. The system is combined with the inertial system and signals from ground beacons to

enhance the accuracy of the aircraft position, improving the resilience against external electromagnetic interference. It is necessary to note that these interferences may cause a disagreement between the ILS and satellite-based systems. For simplification in this case study, all approaches are considered to be stand-alone ILS.

### 3.1.2 Unstable Approaches for Landing

Historically, the largest number of accidents occurred in the landing phase of the flight. This has led to the creation of more criteria, including standard operating procedures that only permit touchdown when the final approach is stabilized in path and speed. Every approach for landing requires a reduction in speed, which is accomplished by reducing the throttle and increasing the drag with spoilers or by lowering flaps, slats, and the landing gear. Besides increasing the drag, the flaps and slats also provide more lift, reducing the angle of attack at lower speeds. The engines are accelerated again to maintain the approach speed as the aircraft intercepts both LOC and GS at a distance from the runway that allows the stabilization of the trajectory. Each of these parameters has a range defined by the Flight Operations as a good balance between safety and efficiency. The approach is considered unstable when the acceptable range of one or more parameters is not met.

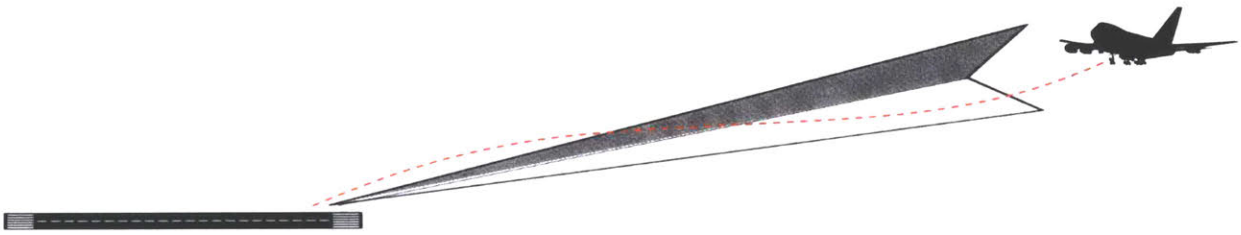


**Figure 9. Unstable approaches in Glideslope**

For the ILS, the limits for LOC and GS have a different interpretation. The lateral deviation (LOC) from the runway alignment is symmetric on both sides of the runway alignment and corrected with turns to converge to the center. However, the vertical (GS) deviations are combined with the speed of the aircraft to tell the aircraft's state of energy. For example, if the aircraft flies centered on GS and 40kt above the approach velocity (Vapp), the negative vertical speed (VS) is too high. The pilot could raise the nose of the aircraft to reduce the speed and fix two parameters for stable approaches (Vapp and VS), but the GS would get out of limits, like pictured in Figure 9.

Every time the approach parameters become unstable below a certain altitude (usually 1000ft), the pilots are required to execute a missed approach procedure (MAPP). This action is also known as Go Around (GA). Being a time-critical situation, pilots are responsible for deciding whether or not to GA. When a crew decides to GA, they increase the throttles to

accelerate, pitch to a climbing attitude, and retract the landing gear and flaps. In modern aircraft, they are also required to press the GA button on the throttle levers or pedestal. This action communicates the crew's intention to the system software, changing the modes of the autopilot and the auto-throttle.

Some instructors in flight schools teach that a landing is a Go Around (GA) that wasn't needed. The idea behind this concept is that pilots should be ready to go around in every approach. But the decision to go around is not a simple one. Missed approaches are expensive, especially with heavier aircraft or on busy airports. When the Pilot Monitoring (PM) communicates the GA decision, ATC sends vectors to a holding pattern while trying to fit this new approach into the line of other aircraft arriving at the same airport and at the same time.

In normal conditions, a MAPP itself is not unsafe, but it may result in relevant losses. According to the Australian Civil Aviation Safety Authority, the mean extra flight time for a GA is 10 to 15 min. However, the total cost of a missed approach is not calculated with a simple multiplication of time and fuel consumption. The extra flight time impacts the delays of other flights and initiates a cascade of secondary costs, such as extra working time for the crew and a reduction in the predictability of the traffic flow. The latter adds stress to the ATC to merge the aircraft in MAPP with the rest of the traffic.

Furthermore, fuel calculations are made for a single missed approach profile followed by flying to the alternative destination, and 45 minutes holding[13] in maximum endurance regime. A combination of multiple GAs and holding time means that flying to an alternative airport can lead to a low fuel emergency and higher stress in the cockpit. Passengers may also become distressed as missed approaches are disruptive, not expected, and may take a while before the crew is able to communicate the reason for the missed approach. All of these secondary factors impact on the decision making inside the cockpit.

There are many possible causes for missed approaches. First, missed approaches are mandatory and justified when the runway is not clear. It could be another aircraft on a late run for takeoff or slowly leaving the runway after landing. The cause could also be a vehicle, animals or debris contaminating the surface. In small airports, when the only active runway becomes unavailable because of a simple tire burst, all aircraft aligned in the final approach must GA. ATC guides them to *holding patterns* at different fixes and altitudes. If the waiting time is long, aircraft with less endurance time must fly to and land at alternative airports, significantly increasing operational losses. In addition, during the descent, ATC commands changes in speed as they are responsible for spacing the aircraft to avoid wake turbulence. Each aircraft approaches with a different reference speed. If an aircraft with a higher Vapp becomes too close to the slower traffic ahead, on the final approach, ATC will command a MAPP to the faster aircraft.

[13] Holding patterns are racetrack navigation patterns based on a holding fix used to keep an aircraft flying under Instrument Flight Rules (IFR) waiting for a proper time to initiate the approach for landing.

Weather also plays a major role in decisions about missed approaches. Some modern aircraft have computers that interpret the trends in energy to identify when the aircraft is flying through windshear. Pilots receive a visual alert accompanied by an aural warning. In modern aircraft, the flight director reverts automatically to a special windshear GA profile. In older aircraft, the pilot is expected to press the GA buttons on the thrust levers and to accelerate all engines. Thus, unless the crew has clear signs of a false alarm, when the aircraft recognizes a windshear, the decision is clear, a missed approach must be preventively performed. Furthermore, strong crosswinds and gusts, not identified as windshear, are also dangerous. Strong winds with regular flow swirl closer to buildings and ground obstacles. In approaches with strong winds, the aircraft may be stabilized during the approach until a couple of hundred feet above the runway, but a sudden and abrupt change in roll or pitch has the potential to cause a hard landing, a runway excursion, or even a crash, such as a tail or engine strike.

Finally, according to our collected data, the major cause of a GA is an inappropriate amount of energy. More specifically, the excess of energy is one of the most frequent causes for missed approaches. It may be caused by miscalculations, ATC requests to keep a higher speed, or a restriction in altitude during descent. It is usually described as a lack of anticipation of the crew in a complex scenario.

Unstable approaches are one of the main topics in recent initiatives to improve safety. In a voluntary partnership with most European agencies, the European Aviation Safety Agency (EASA) developed the European Authorities coordination group on Flight Data Monitoring (EAFDM). This group aims to foster the implementation of FDM programs to increase the safety effectiveness of those agencies. The EAFDM offers a set of standardized FDM-based indicators for four types of occurrences: runway excursions (RE), controlled flight into terrain (CFIT), loss of control in flight (LOC-I), and mid-air collisions (MAC). The purpose is to offer guidance for monitoring operational risks. One of the standardized FDM-based indicators is named "unstable shortly before landing." The trigger logic is a decreasing radio-height, below a predefined value, while:

- Aircraft not in landing configuration (landing gear, flaps, and slats);
- More than a fixed value of angular Localizer deviation;
- Airspeed too high or too low relative to approach reference speed;
- Vertical speed higher than the predefined value;
- Pitch attitude below zero;
- The absolute value of Roll attitude above predefined value; or
- The setting of thrust control or power control is manually changed.

There is a recommendation for all predefined threshold values and an indication of the severity of the deviance. There are additional indicators for low GA, for GA below a minimum decision altitude, and rejected landing, when GA occurs after touching the runway. The respect

for those triggers during operations is another source of concern. A safety manager of KLM, Ewout Hiltermann, said that data proved that between 3% and 4% of approaches are unstable, which represents more than one thousand unstable approaches every day. However, pilots abort the landing and execute go-arounds only in 3% of unstable approaches. To solve this problem, prevention activities need to act on possible reasons for the need to go-around, which requires an understanding of the systemic factors that lead pilots to avoid missed approaches when they are necessary. To explore systemic factors, the next item describes an original STPA on unstable approaches for landing.

## 3.2 STPA for Unstable Approaches

The goal of STPA is to prevent losses that are unacceptable to stakeholders by identifying how the controlled process can get into a hazardous state. The following STPA was performed by three MIT students using the STPA Handbook (Leveson and Thomas, 2018). Pilots (experts) from the partner aviation organizations participated in refining the analysis. In aviation, the term "organization" applies to companies offering transportation services, aircraft manufacturers, the third-party companies, the aviation agencies, the ATC, and the airports that the company operates. Safety is a common goal for all of these stakeholders.

### 3.2.1 STPA - Step 1 – Fundamentals

The analysis started by defining the possible losses that could result from an accident during the approach for landing phase of a regular flight:

L1: Human: life, injury, motion sickness, fear, stress.

L2: Environmental: oil and fuel pollution, debris in nature.

L3: Material or Financial:

- Insurance company: premium for the accident and third-party property damage
- Airline: extra fuel and crew working hours on missed approaches, damage to the aircraft, cleaning debris, providing hangar to the investigation, and lawsuits. Additionally, the operational impact of grounding an aircraft model, i.e., situations in which the whole fleet is forbidden to fly after an accident, until the definition of the cause of the accident.
- Airline investors: reduction on the value in the stock market
- Manufacturer: cost of investigation and changes to manuals and checklists

- Third-party companies: a variety of possible losses depending on their product or service.
- Countries: Military search and rescue missions, aviation agencies accident investigations.
- ATC: losing a controller for a few weeks after accidents
- Airports: Equipment loss, runway damage, runway or apron interdiction.
- Passengers: personal belongings and multiple secondary consequences of not finishing the planned trip.
- Cargo clients: loss of packages.

L4: Company reputation:

- The manufacturer: media questioning the design philosophy and pointing to deficiencies.
- Airline: people questioning the company crew selection, quality of training, or seriousness on imposing the rules

L5: Operational performance: delays and consequences on planning

In Loss 1, the high-severity personal losses, like human life and injury, are complemented by lower-level personal losses. For most passengers, flights are ordinary, and fear is not an issue in normal conditions. For others, flying causes a physiological reaction characterized by hyperarousal. These people become significantly stressed during takeoffs, turns, and landings. For them, the lack of information during missed approaches causes an acute stress response that may be significantly traumatic.

For Loss 3, a list of stakeholders was made to identify their particular losses. This is important when the ones who decide on risks are not the ones who have more to lose. Detailed listings are important to understand how the losses are associated with the ones taking responsibility for safety matters.

Next, a list of system-level Hazards was generated. Each of the following hazards represents a state or condition of the controlled process:

H1: Aircraft violates criteria for stable approaches [All Losses]

H1.1: Lateral instability: Aircraft lands misaligned or outside the lateral runway limits [L1, L3]

H1.2: Longitudinal instability: Hard landing [L1, L3, L5]

H1.3: Energy excess: runway excursion [All Losses]

H1.4: Lack of energy: stall or touchdown before runway threshold [L1, L2, L3, L5]

H1.5: Loss of control [All Losses]

H2: Controlled Flight into Terrain (CFIT) [All Losses]

H3: Aircraft violates minimum separation from airspace or other aircraft [All Losses]

H4: Missed approach procedures [L1, L3, L4, L5]

H4.1: Another attempt to land is made with less fuel reserve [L3, L5]

H4.2: The ATC keeps the aircraft on a waiting pattern [L3, L5]

All hazards are related to one or more losses. In these steps, the traceability system starts to map how the STPA elements relate to each other. There is not a standard codification for traceability, but it is useful to follow the same pattern throughout the analysis and keep an organized index to facilitate the Active STPA Tasks. For this analysis, the Hazards 1 and 4 were refined because of their close relation with unstable approaches. From the list of hazards, it is now possible to derive a list of System-level Constraints (SC) and System-level Requirements (SR), as follows:

- SC-1: Aircraft must maintain criteria for stable approaches [H-1]
- SR-1: Flight Data Monitoring equipment must detect when flight parameters exceed the limits that characterize unstable approaches defined by the Flight Operations
    - SC-1.1: Aircraft must be within lateral navigation limits [H-1.1]
    - SR-1.1: If lateral navigation is off-limits, the PM must detect and inform [H-1.1]
    - SC-1.2: Aircraft must be within vertical navigation limits [H-1.2]
    - SR-1.2: If the aircraft is longitudinally unstable before landing, the PF must GA [H-1.2]
    - SC-1.3: Aircraft must reduce any excess of energy (high speed or high on GS) before landing [H-1.3]
    - SR-1.3: If the shaker is activated, the PF must GA [H-1.3]
    - SC-1.4: Aircraft must keep a minimum amount of energy (Vapp and PAPI[14]) [H-1.4]

[14] PAPI, or Precision Approach Path Indicator, is a set of lights located close to the runway threshold that provides a visual vertical guidance for pilots. When the aircraft is centered on glide slope path, the pilot sees two red and two white lights.

    - SR-1.4: If the aircraft is more than 500ft above recommended altitude at the middle marker or more than 300ft above at final marker, the PF must GA [H-1.4]
    - SC-1.5: Flight must be controlled [H-1.5]
    - SR-1.5: Pilots need to be trained to recover the control of their aircraft, including CRM procedures [H-1.5]
- SC-2: Aircraft must fly at or above Minimum Sector Altitude (MSA) [H-2]
- SR-2: If aircraft flies below MSA, there must be a warning and the crew must react climbing with full power to correct deviation [H-2]
- SC-3: Aircraft must keep minimum separation from airspace or other aircraft [H-3]
- SR-3: Minimum separation from airspace or other aircraft must be detected by ATC and the navigation system (airspace) or TCAS (other aircraft). When alerted, the crew must act to increase separation above minimum standards [H-3]
- SC-4: Aircraft must land with fuel level above minimum [H-4]
- SR-4: The crew must manage fuel consumption and inform ATC when their instructions may cause a low fuel level before landing [H-4]

### 3.2.2 STPA - Step 2 – Model the Control Structure

The second step of the STPA starts by defining the System's boundary: this analysis is restricted to the approach for landing of commercial aircraft. The analyzed controllers were the crew, automation (main computers and autopilots), ATC, and the crew of other aircraft. The functional control structure in Figure 10 maps the interfaces of the system. The top-down nature of the analysis is represented by a series of control loops with controllers sending commands to and receiving feedback from their controlled processes.

Every commercial airliner crew consists of at least one captain. The other pilot may be another Captain or a First Officer. As the control structure maps functional relationships, in this analysis the crew is always composed of a Pilot Flying (PF) and a Pilot Monitoring (PM). Pilots usually take turns in both positions. For example, when the first officer is the pilot flying, the captain acts as a PM, being responsible for all external communications and checklist items, such as adjusting the pressurization system. During the approach for landing, the PF asks the PM to set flaps or lower the landing gear. The PM executes the action, verifies if it was successful, and provides the feedback to the PF (e.g. "gear down and locked").

This study focused on two control loops: the ATC (Air Traffic Control) controlling multiple aircraft, and a crew controlling the aircraft subsystems. ATC has a higher hierarchical

level than crews from different aircraft. The radar display allows ATC to have a better visualization of the whole situation. ATC also knows the planned trajectory of all aircraft in their terminal. On the other hand, pilots see things that ATC is unable to see, such as a flock of birds, a flying object without a transponder, such as a balloon or a drone, or debris on the runway. Thus, the crew acknowledges and follows the directives from the ATC controller, but pilots are always the final authority on their aircraft navigation path. Appendix A shows a detailed control structure that depicts all processes controlled by a crew.

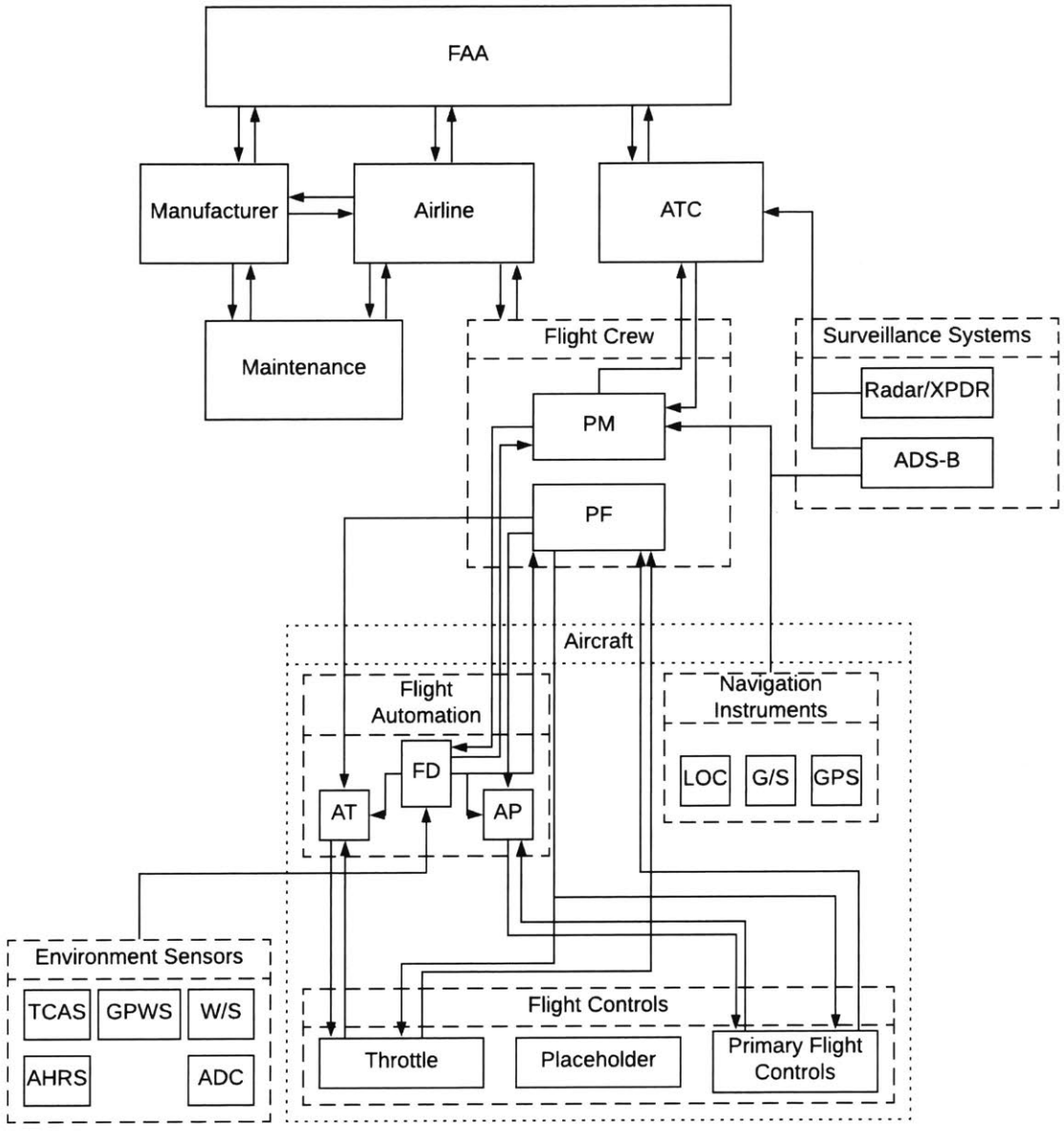



**Figure 10. High-level functional control structure**

Every modern avionics system has computers to calculate parameters for guidance. These computers have different names depending on the avionics manufacturer. In this study, the Flight Director (FD) is the computer in which pilots push buttons and turn knobs to select a target altitude, vertical speed, speed, or heading. The computer used to load a sequence of navigation profiles is the Flight Management Computer (FMC). The FMC is the interface with which the crew selects the procedures for departure, climb, arrival, and landing. The crew gets the authorization from ATC, finds and selects these codes in the FMC database, and checks if the route represented in the displays correspond to their planning visualized in navigation charts.

Once configured for landing, the FMC sends continuous information to the Primary Flight Displays (PFD) showing with a symbol the ideal attitude to fly the calculated profile. In this analysis, the V-bar is the reference used for this symbol. To follow the selected navigation profile, the PF or the autopilot must match the symbol of the current attitude with the V-bar calculated by the computers. Any offset from the V-bar will cause a deviation in the navigation profile. The autopilot is programmed with gains to smoothly capture the V-bar and intercept the desired profile with minimal deviations. When the autopilot is disengaged, the PF dedicates substantial attention to follow the V-bar. This activity represents a high workload for new pilots and becomes normal with flight experience.

Those two possibilities, autopilot engaged or disengaged, demand two different interpretations of the functional control structures. Primarily, when the autopilot is engaged, the relation is more straightforward because the Crew Resource Management (CRM) determines that the PF adjust the FD, which sends information to the autopilot. The control loop closes with the feedback from displays, with less interference of the PM. In the second case, the autopilot is disengaged and the PF is flying manually. The CRM determines that the PF sends voice commands to the PM. The PM adjusts the FD, and the PF follows the FD V-bar. The functional relation in the control structure should not be represented by a linear sequence of components because it has complex interactions. For example, a miscommunication may lead the PM to enter a different parameter in the FD, and the PF will follow the symbols without noticing that the path is different than what was requested.

In this STPA, the design of the detailed control structure took the responsibilities of all controllers (ATC, PF, PM, and the autopilot) into account. The necessary feedback is also organized and evaluated to assure that the system is providing all necessary information for proper situation awareness of the crew. This is also required for emergency situations, when the crew needs to identify any malfunction to intervene properly.

### 3.2.3 STPA - Step 3 – Identify Unsafe Control Actions

The next step is finding Unsafe Control Actions (UCA). UCAs are actions that, in a specific context, leads the system to a Hazard. Timing is important in STPA, and approaches for

landing are a sequence of actions on many different subsystems. UCAs are organized into four types:

1. Not provided causes hazards
2. Provided leads to hazard
3. Provided too early, too soon or out of order
4. Continuous actions provided for too long or stopped too soon

Every UCA is composed of five parts (Leveson and Thomas, 2018), as observed in the following UCA from the analysis (Figure 11).

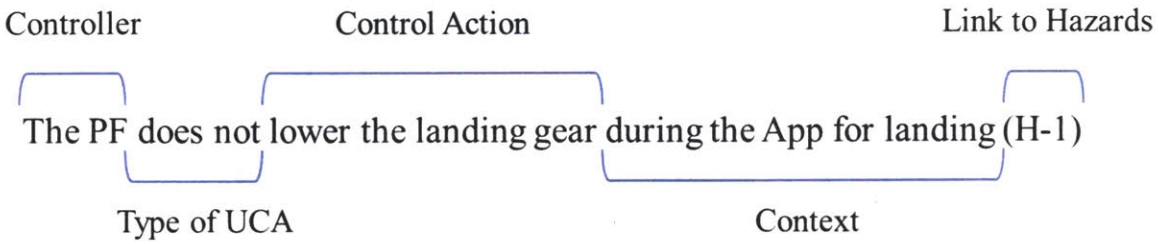



**Figure 11. Structure of a UCA**

The Appendix B and D show the UCAs of ATC and the crew as controllers, respectively. It is important to make clear that, if an event involves UCAs from two different aircraft, the same analysis is used as a reference as both controllers have the same responsibilities and are in the same hierarchical position in the control structure. The system is designed with safeguards, and the probability of a component failure or human error at the most critical time may be very small. However, even when the context of the UCA is rare or represents a small fraction of the operational time, UCAs must be exhaustively listed to represent all worst-case scenarios, because rare events are often the causal factors of recent accidents in aviation.

### 3.2.4 STPA - Step 4 – Identify Loss Scenarios

For each of the UCAs found in step 3, the SA generates scenarios using group meetings or the participation of experts to identify the causal factors and the rationale that could lead to each specific UCA. When thinking about scenarios, we considered possible component failures, lack of information on feedback, absence of feedback, incomplete requirements, lack of requirements, and design errors. In this study, it was assumed that the design of equipment and airspace could not be changed; instead, the operational practices need to adapt. Appendix C and E present in tables the scenarios developed for both ATC and crew STPA.

If the SA keeps the scenarios at a higher level to find more general constraints, then the constraints will not be specific enough to derive reasonable rules and procedures. On the other hand, if the SA goes for detailed causal factors, the number of scenarios increases, which requires more time to finish the analysis. To illustrate the generation of scenarios, consider the control action "pressing the GA (Go Around) button" in the context "when the approach for landing is unstable." Figure 12 shows the components involved with this control action.

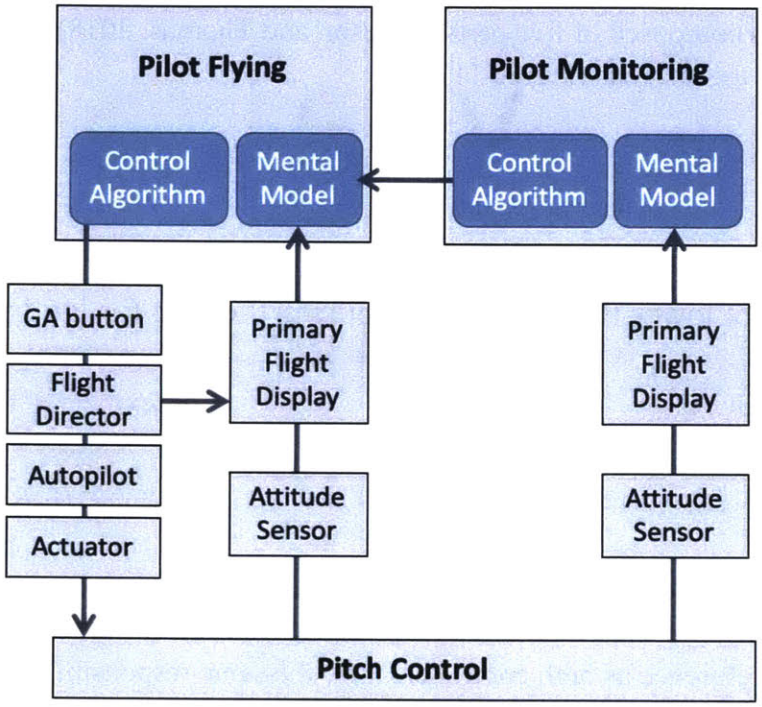



**Figure 12. Generation of scenarios for the control action: pressing the GA button**

The STPA found nine scenarios from five different sources with a single UCA, as follows:

1. Controller (pilot flying)

    1.1 Pilot Flying decided not to press the GA button because he or she believes that it is possible to land safely

    1.2 Pilot pressed the wrong button because the cockpit suffered a sudden negative "g" under severe turbulence

2. Execution (GA button and systems in series)

    2.1 Button malfunction

2.2 Pilot did not press strong enough, but believed that the system was activated (this button is rarely pressed)

3. Controlled Process (pitch control)

3.1 Crosswind and turbulence deteriorate response in pitch, eventually causing a delay in the response in terms of flight path

3.2 Software programmed to inhibit GA when there is weight on wheels

4. Feedback (sensors and displays)

4.1 Personal Flight Display processor shows a long delay because it has to re-calculate the vertical profile on a complex IFR procedure

4.2 System not showing the symbology for the GA mode on the screen due to a software problem

5. Coordination (Interference by ATC or the PM)

5.1 PM thinks the approach is stable because he/she is not checking all relevant parameters

STAMP is effective to study cockpits because the scenarios explain situations of confusion or lack of coordination among crew members, such as a pilot who believes that the other is monitoring a parameter when it is not true, or a communication flaw due to high workload during an IFR procedure. For instance, one of the experts who revised part of the STPA is a pilot. He revealed common mistakes that were added to the analysis, such as the mistaken selection in the autopilot between Flight Path Angle and Vertical Speed, or wrong altimeter setting by ten units. This kind of information is important to write scenarios that properly reflect why UCAs would occur.

The outcome of step 4 is a list of lower-level requirements and constraints derived from those scenarios. These constraints were then used to write preventive and mitigating defenses that may result in changes to the documentation of the company, such as policies, procedures, and training manuals.

### 3.2.5 Implementation of an STPA

The STPA delivers a list of requirements and constraints. To implement the STPA, the SA is required to develop controls to guarantee that the constraints will be respected. Figure 13 summarizes all the elements considered during the STPA and the subsequent implementation of defenses in accordance with requirements and constraints.

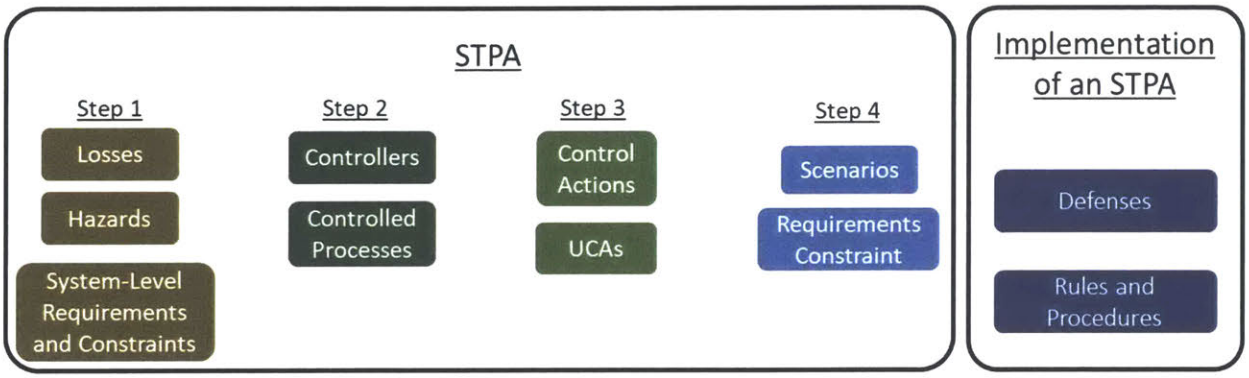



**Figure 13. Elements of STPA and its implementation**

### 3.3 Partner data: An incident on a parallel approach

When the STPA was finished, real data from the partner airlines was used to run the Active STPA. One of the events collected for analysis is an example of how more than one Case may derive from events with more than one controller. This Event was divided into three different cases and adapted in this section to explore the possible outcomes of an Active STPA.

An Airbus A-340 operated by one of our partners was on approach for landing at an International airport. This airport has parallel runways and has specific procedures for parallel approaches. In this procedure, two aircraft align side by side with two parallel runways, as pictured in Figure 14. There are minimum distances regulated for this type of operation, and the forbidden airspace between the two approaches is called the No Transgression Zone (NTZ).

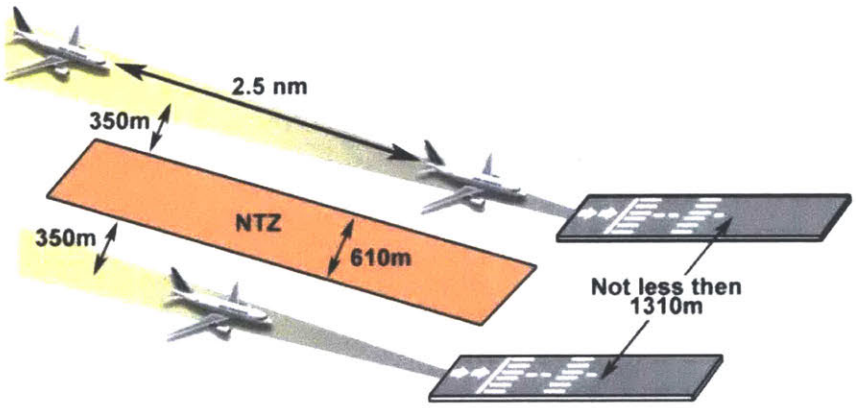



**Figure 14. Parallel Approaches for landing (FAA, 2017)**

Parallel approaches are relatively new in aviation. The FAA started using simultaneous approaches to parallel runways in 1962 at the Chicago O'Hare International Airport (ORD). In

1974, the minimum distance between runways implemented in the Atlanta International Airport was 4300ft. To reduce the minimum distance to 3000ft and include many other airports, the procedure Precision Monitored Approach (PRM) was created using a high-update-rate radar (Massimini, 2006). The requirements for PRM include having two independent radios to listen to the regular tower channel on one radio and to a PRM controller on another frequency. The aircraft transmits only on the tower frequency but receives both radios.

An Airbus A-340 had already intercepted the LOC of runway 28R[15] when a Boeing 737 of another airline overshot the interception of the LOC of runway 28L. Both aircraft were equipped with transponders and TCAS (Traffic Collision Avoidance System). When the B-737 entered the NTZ higher than the A-340, the alarm on the TCAS of the A-340 was triggered, and resulted in an RA (Resolution Advisory), commanding the PF (Pilot Flying) to pitch down to increase the descent rate. Neither pilot in the A-340 could get visual contact with the B-737 because it was relatively behind and above. The PF followed the TCAS RA and increased the descent ratio.

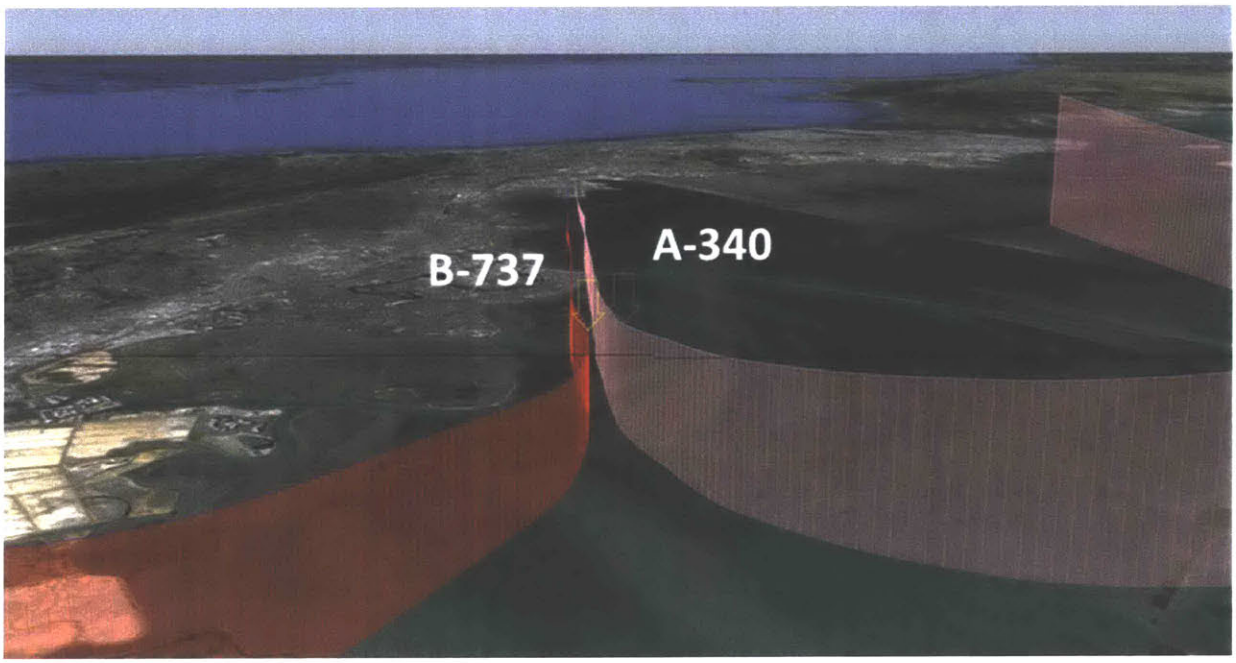



**Figure 15. Reconstitution of the trajectory of both aircraft with FDM (Source: Partner)**

At this point, the crew of the A-340 was facing a dilemma: the company rules state that any unstable approach requires the crew to execute the missed approach procedure. However, TCAS was still showing the B-737 behind them and higher. With the feeling that it would be

[15] When an airport has two parallel runways, the number of the runway receives a letter L (left) or R (right). When there are three runways, the one in the center receives a letter C.

more hazardous to GA than to land after an unstable approach, the captain decided to land. Figure 15 shows a visual representation of the trajectory of both aircraft generated for the investigation, while Table 2 shows the description of the event by the pilot, the Flight Data Monitoring (FDM) analyst, and the judgment of the Flight Operations.

**Table 2. Description of the event after the investigation**

| ***Title*** | ***TA ON APPROACH - SFO*** |
|---|---|
| ***Pilot Description*** | *Intruder aircraft TA at 1200' TCAS showing relative position 10 o'clock 200' above. No VIS contact. At 1000' RA to descend received. F/O carried out maneuver CPT told ATC "RA". Traffic became visual for us at approximately 700'. Until then TCAS was showing on top of us. I made the decision not to go around as this would have jeopardized our safety since we had no idea of the exact proximity of the traffic. Once we had him in sight we stabilized at 600'. As we were visual to the ground and could not at first see the traffic and once we saw him he was to close for a go around. I decided the safest course of action was to continue to land.* |
| ***Flight Data Analysis*** | *At 1310 ft TCAS RA 1500 FPM descent was activated for 16 seconds and the aircraft descent to 928 ft. the aircraft levelled off at about 740 ft at 3.3 DME and climbed to 790 ft at 2.8 DME.*<br>*A/P was immediately off when the RA was activated.* |
| ***Flight Ops Risk Analysis*** | *This was a well handled event given the conflict of SOP and safety constraints that the crew found themselves experiencing. The Captain was interviewed and it was evident that his actions were correct given the information he was processing at the time of the event. Although stabilized approach criteria were not met, safety was maintained through the see and avoid philosophy. Animation was created and reviewed. 1 high rate of descent FDAP was triggered as a response to the RA descend command at 1300'. Aircraft was stabile on flight path by 750'.* |

At the time this event took place, Flight Operations was in charge of reviewing the event, and determining if the actions taken were within company standard operating procedures. When they consider that the decision of the pilot was correct, they communicate the event to other

pilots, and the event is filed. On the other hand, if the pilot actions are in hindsight considered to be an error, the Flight Operations alert the other pilots to avoid the repetition of the event. The airline operating the B-737 probably made a similar event analysis, investigating the actions of the pilot that overshoot the LOC and ingressed into the NTZ. The position assumed by the Flight Operations becomes a reference on what is the acceptable behavior in future similar events.

The description above was used to generate the Active Hazard Analysis Input (AHAI) with the context and the actions of all the controllers involved:

*AHAI: During simultaneous parallel approach (A-340 to 28R and B-737 to 28L), the B-737 overshot the localizer, entering the NTZ, 200ft above and 1000ft behind the A-340. The Tower did not correct the 737.*

As this Event has three controllers, it was divided into three Cases: The ATC (Case A), the B-737 crew (Case B), and the A-340 crew (Case C). The objective of each Case is to answer:

- Case A: Why the ATC did not follow the rules for parallel approaches?
- Case B: Why the B-737 overshot the localizer and entered the NTZ?
- Case C: Why the decision of the A-340 captain, considered correct by the Flight Operations, is not part of the current procedures?

There are more subtleties to this event, as in many other aviation incidents, but as the focus is to demonstrate the application of the Active STPA, for the sake of simplicity of the analysis, details on procedures and training practices are not presented. The following sections of this chapter describe each Phase of the Active STPA and their associated Tasks followed by examples using the three Cases described above.

## 3.4 Active STPA Phase 1: Inspect the STPA

In organizations that elaborated an STPA and implemented its recommendations, incidents are a sign that something may be incorrect or missing. This incorrect or missing element may be a rule, a procedure, or parts of the STPA used to generate them. Phase 1 of the Active STPA investigates what went wrong, finding the elements that were designed to protect the system against the incident. The SA receives the AHAI describing an incident and starts Cases visiting the existing documentation that is associated with the incident, including training manuals and formal procedures written to prevent this unsafe occurrence. If the event is hazardous, but it does not break any written rule, it means that the hazard analysis is either incomplete, operations have changed after the elaboration of the hazard analysis, or the recommended defenses are inadequate or have yet to be fully implemented.

In general, the reasons for an incomplete analysis may be:

- Limited time to run the analysis

- Limited information about the system
- Analysts who are underqualified on the technical or operational practices
- Analyses made only to pass audits or certification processes
- High-complexity of the analyzed system
- Lack of considerations of interactions with other systems

Cognitive difficulties in dealing with complex systems are natural. The problem is simpler when isolated, and the temptation to quickly come up with a sound solution may blind the SA from hidden interactions and faults in the hazard analysis. The lack of a scenario, UCA, or even a controlled process requires figuring out why the STPA is incomplete, before trying to fix the system with another ineffective solution.

A well-organized traceability system allows faster identification of the UCAs and the scenarios made for each of them. This coding system links the whole analysis, from the Losses to the rules and procedures. Figure 16 shows the sequence of results of an STPA process, which are elaborated from left to right. The SA highlights all the pertinent elements and visits every step of the STPA in the opposite direction, from right to left, until finding all missing parts. Different approaches were tried for the identification of missing elements in Phase 1, including the use of a regular order (left to right) and starting from the UCA. The reverse methodology, i.e., starting from the rules and procedures, was found to be faster than the regular order because the SA reviews only the pertinent items, and more logical than starting from the UCA because it avoids confusions for new analysts who did not participate in the elaboration of the STPA.

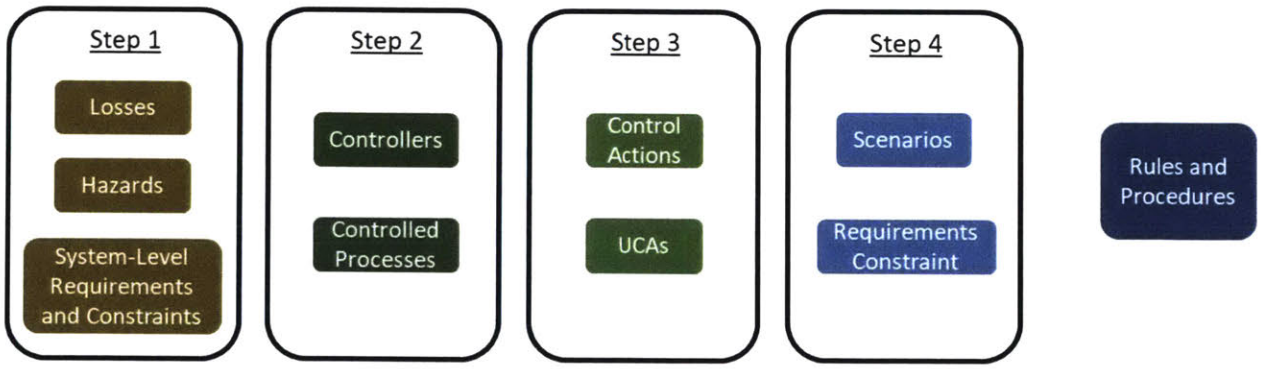



**Figure 16. Elements inspected in Phase 1**

The Tasks of Phase 1 presented in Table 3 are detailed and exemplified in the following sections.

**Table 3. Structure of Tasks of Active STPA Phase 1**

| **Phase 1 - Inspect the STPA** |
|---|
| 1.1 – Search for applicable rules and procedures |
| 1.2 – Verify requirements and constraints |
| 1.3 – Verify causal scenarios |
| 1.4 – Verify control actions and UCAs |
| 1.5 – Verify control relations in safety control structure |
| 1.6 – Verify System-level requirements and constraints |
| 1.7 – Verify Hazards and Losses |

One might think that, in Phase 1, the SA does not need to complete all the Tasks because finding a step that covers the event would mean that everything to the left is complete. Similarly, from the first missing part to the right there would be a cascade of incompleteness, and something missing from the beginning, such as a hazard that was not mentioned, could create a non-functional system leaving room for errors to occur. This line of thought makes sense because while constructing the original STPA, the UCAs come from the control actions, the scenarios come from the UCAs, and so forth. However, the STPA is not like a tree with independent branches. For instance, a single item in a procedure might be able to address many constraints. It is also possible that the SA finds a reasonable procedure that is prior to the STPA implementation, and there are no documented scenarios that properly describe the event. Similarly, it is possible that another scenario with different reasoning in terms of mental, or process models, already generated a constraint that prevents multiple causal scenarios. The missing scenario must be added to the analysis to allow a better understanding of the system, even when existing constraints are appropriate.

### *Task 1.1 – Search for applicable rules and procedures*

Management communicates with the operators using technical documents, such as manuals and checklists. If the STPA is properly applied, then these documents take into account the responsibilities of the controllers. Four major possibilities cover all cases:

- Violation of an adequate procedure
- The STPA is complete, but the procedure is inadequate
- The STPA is incomplete
- A change has occurred that invalidates what was done previously

If the SA finds a procedure that is supposed to prevent the incident described in an AHAI, it is necessary to think about why it was not effective. An investigation becomes necessary to determine if rules should be adapted or if defense mechanism must be enforced. The defense may not be effective, or it may have simply not been applied, even when the STPA has a requirement or constraint to prevent the detected event. There are several reasons for not applying a defense, such as:

- The defense is too expensive to implement
- There was no time to implement all defenses
- The recommended defense is not feasible
- The defense conflicts with existing procedures
- The results of the analysis were not communicated to the proper recipients

In the first two examples, the Case becomes an argument for increasing the prioritization level of a defense. If the defense is not feasible or it conflicts with others, the Case is actually an opportunity to refine the documentation, adding better procedures. If all results of the analysis were not directly translated into procedural changes because the defense was not received by the responsible party in charge of changing the process, then the Case becomes a sign of a flawed Safety Communication System. The hierarchy between the safety and flight operations managers may be an obstacle in promoting new defenses, which could be surmounted by better communication channels between the two. Thus, the connection between both safety and operations teams must be incentivized so that the SA can learn from operational particularities to suggest more appropriate procedures.

Unfortunately, in some industries, many safety defenses are not incorporated into technical documentation because some risks are considered to be low, and the implementation of changes can be expensive and time-consuming. There is an operational reality in which risk estimation for management decisions are based on cost/benefit analysis. However, this management aspect is out of the scope of this research.

### *Task 1.2 – Verify requirements and constraints*

The goal of using an STPA is to identify the safety constraints and how they could be violated. However, years after running an STPA, the system may drift to a condition that safety constraints are no longer enforced, and additional constraints or enforcement mechanisms are required. Also, the process model of the controller may no longer be valid for the controlled process, delays may have been added or changed, or assumptions about the system may no longer be effective (Leveson, 2013).

In this Task, the SA uses the traceability system to identify, from the procedures, a set of lower-level constraints. Then, the SA verifies if there was already a constraint designed to avoid the incident described by the AHAI. If the constraint exists, the SA moves onto the next Task.

However, the absence of a constraint leads the SA to investigate why the STPA was incomplete. When the analyst is adding detail to the lower level in STPA, it is common to find scenarios that require multiple constraints to be prevented. One possible mistake that would explain the lack of a constraint is that the analyst stopped considering new constraints after writing a few for a specific scenario.

### *Task 1.3 – Verify causal scenarios*

The generation of scenarios in step 4 of the STPA deciphers how and why the Unsafe Control Actions (UCA) would happen. In this Task, the SA compares the AHAI with the scenarios found by the traceability system. If there are no existing scenarios explaining the process model flaws that resulted in the incident described by the AHAI, the SA is required to investigate why before moving to the next Task.

During the elaboration of an STPA, there is a natural tradeoff in the generation of scenarios. If the SA keeps the scenarios at a higher level of abstraction to find more general constraints, it is easier to achieve completeness, but the constraints will not be specific enough to derive effective rules and procedures. On the other hand, if the SA goes for detailed causal factors, the number of scenarios increases, but there are more chances of missing a causal scenario.

Therefore, the complexity of modern systems makes it challenging for inexperienced analysts to achieve absolute completeness during the generation of scenarios in STPA. This explains why the lack of a causal scenario has shown to be the problem in most analyzed Cases because the variability in causal factors makes it harder to derive assumptions on which behavior or mistakes should be considered as common. The SA may have missed a scenario in the original STPA because the possible causal factors were not completely mapped or considered never to occur.

With Active STPA, on every new Case with a missing scenario, the process populates the analysis in Phase 3 with new detailed scenarios. This approach allows the observation of unforeseen behaviors and the generation of more realistic scenarios. It also allows writing scenarios about contexts that were initially identified but considered sufficiently unlikely.

### *Task 1.4 – Verify control actions and UCAs*

Scenarios come from UCAs, and each UCA is a type of control action. The SA now verifies if the control action described in the AHAI corresponds to any of the documented UCAs. In the STPA Step 3, the elaboration of contexts may be extensive, but careful consideration of all possibilities can cover the entire spectrum of possibilities. Even though, if the analysis has an inadequate UCA, or it is missing one, the SA should verify the validity of assumptions made on how the system works, checking if the responsibilities of each controller and their relation with all of the controlled processes still apply.

In very complex systems, such as aircraft cockpits, there are numerous physical buttons and touchscreens with multiple pages and modes. The list of possible actions grows quite large when all possibilities are taken into account. One might say that only general actions like "climb" should be considered. In this line of thought, all possible ways of commanding the aircraft to climb are considered as one single control action. This approach helps to find system-level constraints, but constraints derived from the analysis of lower-level components are necessary to write proper rules and procedures.

Another possible mistake is not considering a specific control action when performing a partial analysis. For instance, a SA might think that adjusting the seat height should not be part of the STPA on approaches for landing. However, we must always consider that human operators will eventually act and decide differently than the assumed behavior. The pilot could set the seat height for a resting position during cruise and remember to adjust it for landing only during the final approach. In this case, only a more detailed analysis would consider if the position of the switch that commands the seat height is in a position that prevents inadvertent actuation while flying in turbulence.

#### *Task 1.5 – Verify control relations in safety control structure*

In Systems Theory Accident Model and Process (STAMP), risk is defined in terms of the effectiveness of the controls used to enforce safe system behavior, i.e., the design and operation of the safety control structure (Leveson, 2011), measured by the lack of effectiveness of the defenses that protect the system from hazards. One does not need to be an engineer to understand the language of the functional control structures. Every system has a higher-level control structure including the hierarchical relations among all controllers. For complex activities, lower-level controllers require a more detailed control structure showing all the subsystems and equipment. The task of the SA is to look to both control structures to identify all pertinent control loops, even when they are in different hierarchical levels. Each controller has several controlled processes, and the SA needs to focus on the responsibilities of each controller to identify the correct elements of the system.

For example, if the description says that the crew maintained a higher than normal speed during the final approach for landing, the SA needs to investigate the observed event to understand whether the causal scenario relates to a pilot's lack of attention or a response to an ATC request that the crew received. The investigator may ask the crew about the higher-than-normal speed to understand why they violated the criteria for stable approaches. This investigation is important to define which control relation, in the safety control structure, has the UCA. The occurrence may indicate a general unsafe behavior in response to a changing environment, such as an increase of stress caused by higher than normal traffic at a specific airport. The analyst must use the control structure to verify if the incident relates to more than one UCA in different control loops.

Usually, the reason for the unsafe behavior at a lower level is influenced by control actions from higher levels in the control structure, or by a lack of coordination among peers on the same level. For those cases, the SA explores interactions in multiple hierarchical levels in the original STPA. Although the hierarchical organization of the controllers may be a very straightforward process, in innovative systems, it may be challenging to consider all their responsibilities in the original analysis, when there is no previous experience in that kind of operation.

In the STPA Step 2, the processes of designing control loops and listing control actions are quite clear and straightforward. The missing parts are usually related to the changes in the system structure that occurred after performing the original STPA. Thus, the lack of a controller or a controlled process may indicate that the system has profoundly changed, and it must be mapped again to have a more comprehensive control structure. It will require a new analysis with a deeper understanding of the interconnections among system components. The SA must look for changes in the responsibility of controllers and collateral effects of those changes. Consequently, the SA needs to revisit the fundamentals of the analysis and re-address responsibilities.

### *Task 1.6 – Verify system-level requirements and constraints*

High-level requirements or constraints derive directly from Hazards. They may be incomplete after significant changes in the system, such as the introduction of new equipment, or in the environment, such as a construction site that affect the operation. The completeness in high-level constraints is important because their violation may directly lead to a loss. System-level requirements and constraints may be inadequate or fail to cover the whole spectrum of the lower-level ones.

### *Task 1.7 – Verify Losses and Hazards*

Finally, the search for missing elements in the STPA brings the analyst back to what was elaborated at the beginning of the STPA to search for missing Losses, Hazards, and system-level requirements and constraints. An example of a missing Loss is the 'damage to the company reputation', while a missing Hazard could be the 'collision with a drone on final approach for landing'. A missing Loss or Hazard is supposed to be extremely rare in Active STPA.
The Tasks of Phase 1 are exemplified by the following three Cases.

## Case A - ATC

Phase 1 of Case A is initiated by searching for a procedure. If an aircraft enters the No Transgression Zone (NTZ) between the runway alignments, the PRM controller is supposed to command a breakout maneuver instruction to the other aircraft. An example of the breakout command is "*Traffic Alert, [call sign], turn left immediately heading 140, climb and maintain 4000*". The PF who receives a breakout command is required to fly it manually. This means that

the crew disconnects the autopilot, initiates the turn, accelerates the engines, retracts the landing gear, and reduces the flaps to climb position.

This Case is concerned with the control loop of Figure 17, in which the ATC is the controller, in communication with the PM to control the actions of the PF. There were two independent STPA step 3 and 4 for the ATC and the Flight Crew as controllers. The ATC STPA for approaches found 43 UCAs, 131 scenarios, and 129 constraints, shown in Appendices B and C.

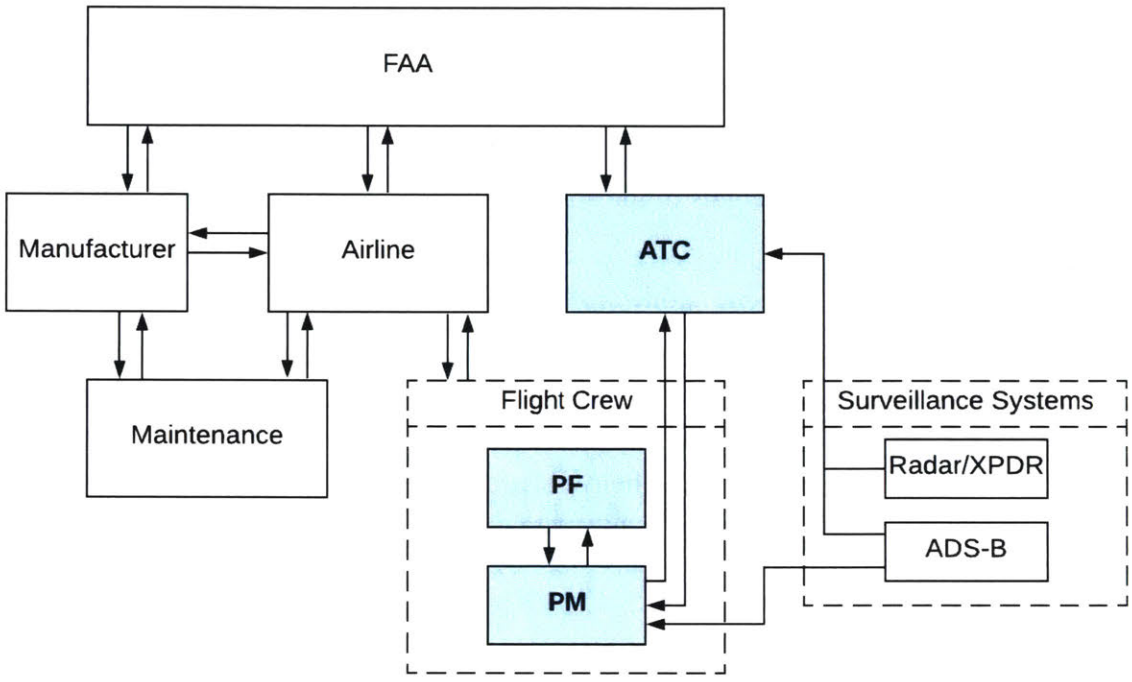



**Figure 17. Step 2: Control loop ATC - Crew extracted from the high-level control structure**

The ATC is a peculiar type of controller because, today[16], most control actions to the crew are still voice commands. The high-level control structure has the ATC sending commands to the crew. The PM is responsible for all solicitations and acknowledgments in external communications, but the PF is the final destination if ATC orders. Table 4 summarizes the findings of Phase 1.

[16] The NextGen and similar programs are testing the use of datalink messages for ATC directives. The new system will require significant changes in the hazard analysis and new protections for cyber security.

**Table 4. Case A – ATC – Phase 1**

| Case A - ATC | | | |
|---|---|---|---|
| **Phase 1 – Inspect the STPA** | | | |
| **Task** | **Description** | **Analysis** | |
| **1.1** | Search for applicable rules and procedures | 1 - The PRM controller is supposed to alert every time an aircraft enters the NTZ (No Transgression Zone)<br>2 – Aircraft observed to overshoot the localizer interception turn, or to continue on a track which will penetrate the NTZ, will be instructed to return to the correct final approach course immediately. | |
| **1.2** | Verify requirements and constraints | ATC must be familiar with AC dynamics for course correction (constraint 3.4) | |
| **1.3** | Verify causal scenarios | ATC has a flawed mental model on how much time it takes for the other AC to perceive and react with course correction (Scenario 3.4) | |
| **1.4** | Verify control actions and UCAs | Switch / Selector | Voice command |
| | | Control Action | GA |
| | Identify UCAs | ATC does not vector AC away from NTZ when AC is imminently entering NTZ (UCA 3) | |
| **1.5** | Verify control relations in safety control structure | Controller | ATC tower controller |
| | | Controlled Process | Crew B-737 |
| **1.6** | Verify system-level requirements and constraints | SC-1.1: Aircraft must be within lateral navigation limits [H-1.1] | |
| **1.7** | Verify Hazards and Losses | H3: Aircraft violates minimum separation from airspace or other aircraft [All losses] | |

## Case B – B-737

Case B relates to the B-737 that overshot the localizer (Figure 18) and entered the NTZ. It starts by finding the current procedure relating to overshooting the localizer. During descents, pilots are required to study the approach charts and brief the rest of the crew about the approach for landing. The briefing must contain the relevant restrictions from the charts, the automation settings sequence, and the missed approach profile. When the autopilot is engaged, the PF is responsible for setting up the modes of the flight director. When it is disengaged, PRM rules determine that the PF must ask the PM to execute the settings. In this Case, it was determined the autopilot was engaged, and the PF pressed LOC too late while following PRM rules.

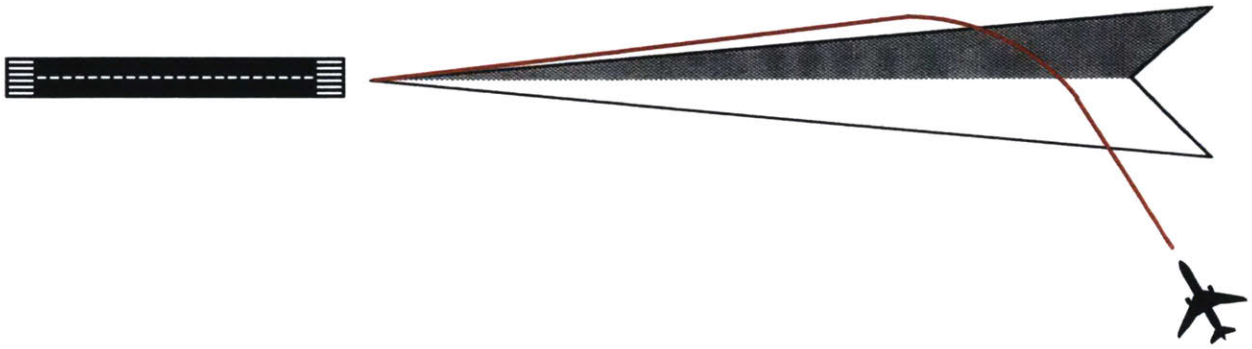


**Figure 18. Representation of a Localizer overshot**

The STPA for the crew was developed taking into consideration all control actions that a crew may perform during an approach for landing. Table 5 shows one example of the control relations found in the analysis.

**Table 5. Step 3: Listing control actions**

| Controller | Process | Switch / Selector | Control Actions |
|---|---|---|---|
| PF | Autopilot | LOC | Engage LOC Mode |

From the STPA detailed control structure, the SA identifies the applicable control loop (Figure 19).

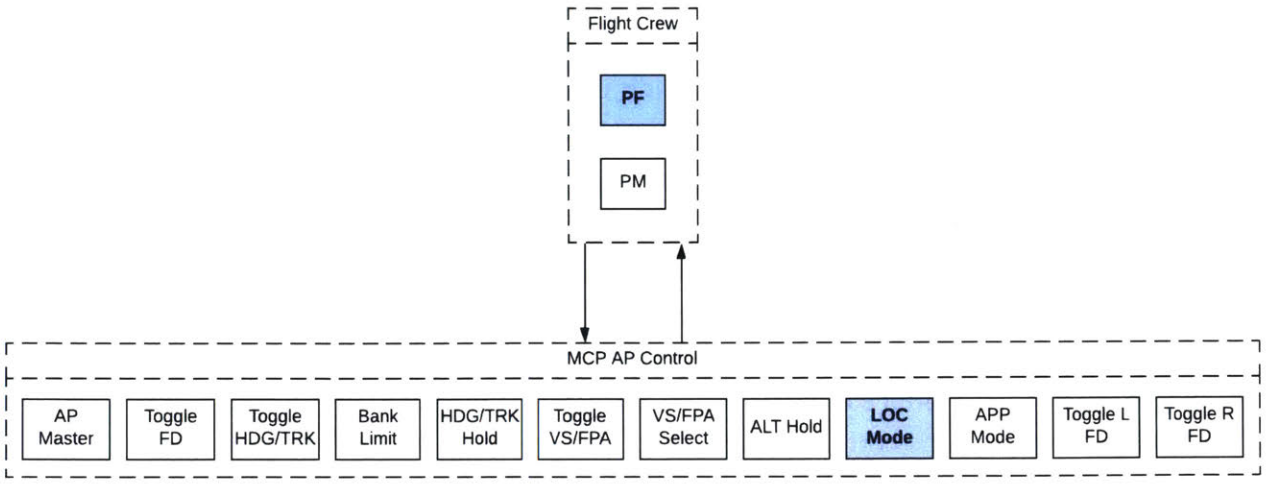



**Figure 19. Step 2: Control loop Crew - Autopilot (AP) extracted from the detailed control structure**

In this research, the original STPA analysis of crew control actions found 77 UCAs in the crew analysis (Appendix D). Table 6 shows an example of three UCAs generated from the control action "Engage LOC."

**Table 6. Step 3: The UCAs for engaging LOC**

| Type | # | Unsafe Control Actions |
|---|---|---|
| **Provided causes Hazard** | 23 | Engage LOC when AC is under vectors flying outbound (H3, H4) |
| **Not Provided causes Hazard** | 24 | Not engaged when aircraft (AC) passes ideal turning point (H1.1, H3) |
| **Applied for too long or too short** | - | N/A |
| **Wrong timing or order** | 25 | Engaged too late when there is high intercept angle, and AP is unable to capture without overshoot (H1.1, H3) |

There are many reasons why a crew would delay the LOC selection, both intentional and unintentional. Intentional delays must be investigated using decision-making models that consider mental models generated during training. It is important for the crew to fly the planned track, but other reasons such as a flock of birds in the flight path require a judgment call. The crew knows that it is possible to turn later and still make the LOC by executing the delayed turn at a higher bank angle. There are also a number of reasons for unintentional delays. Many of

which are related to human factors, including lack of attention or memory issues. The lack of attention could be caused by low or excessive workload (Yerkes and Dodson, 1908). The SA is responsible for investigating these boundary conditions, and eventually consulting a human factors specialist.

Controllers develop a model of the controlled process in their minds. One example of flaws in process models is: after commanding the PM to prepare the autopilot for approach, the PF assumes that the aircraft have the correct modes engaged. To be successful, first, the PM needs to understand the command. The CRM has requirements for acknowledgment call outs, but operationally, stress caused by communications with ATC and the high workload of multiple tasks eliminates many required callouts. Second, the PM needs to press the correct buttons and the software must engage the correct vertical and horizontal modes. This latency requires the PF to wait a few seconds after the command to check in his PFD if the desired modes have engaged.

Table 7 shows a summary of Phase 1 results.

**Table 7. Case B – Boeing 737 – Phase 1**

| Case B – Boeing 737 | | | |
|---|---|---|---|
| **Phase 1 – Inspect the STPA** | | | |
| **Task** | **Description** | **Analysis** | |
| **1.1** | Search for applicable rules and procedures | PRM procedure was not followed<br>The PF is responsible for pressing LOC when the autopilot is engaged.<br>Briefing during descent must finish before the initial approach fix (IAF) | |
| **1.2** | Verify requirements and constraints | LOC must be selected with enough anticipation to avoid overshoot of Localizer by more than 1 dot | |
| **1.3** | Verify causal scenarios | PM splits attention between ATC communication and reading IFR procedures and forgets to press LOC before ideal turning point | |
| **1.4** | Verify control actions | Switch / Selector | LOC |
| | | Control Action | Engage LOC |
| | Identify UCAs | Engaged too late when there is high intercept angle and autopilot is unable to capture without overshoot (H1.1, H3) | |
| **1.5** | Verify control relations in safety control structure | Controller | PF |
| | | Controlled Process | Autopilot |
| **1.6** | Verify system-level requirements and constraints | SC-1.1: Aircraft must be within lateral navigation limits<br>SR-1.1: if lateral navigation is off-limits, the PM must detect and inform [H-1.1] | |
| **1.7** | Verify Hazards and Losses | H1.1: Lateral instability [L1, L3]<br>H3: Aircraft violates minimum separation from airspace or other aircraft [All losses] | |

## Case C – A-340

Case C discusses the actions of the crew of the A-340. This crew was stable in the final approach, received an RA (Resolution Advisory) from the TCAS, followed the RA increasing the descent ratio, and decided to land after an unstable approach because they judged that a GA would be more dangerous. This crew did not cause the conflict, but their decision went against

the rules of the company. Figure 20 shows a lower-level control structure with the pertinent controllers and controlled process. The company did the right thing, acknowledging that their procedures were incomplete and that the crew made the right decision; not condemning the actions of the crew to reinforce inadequate procedures.

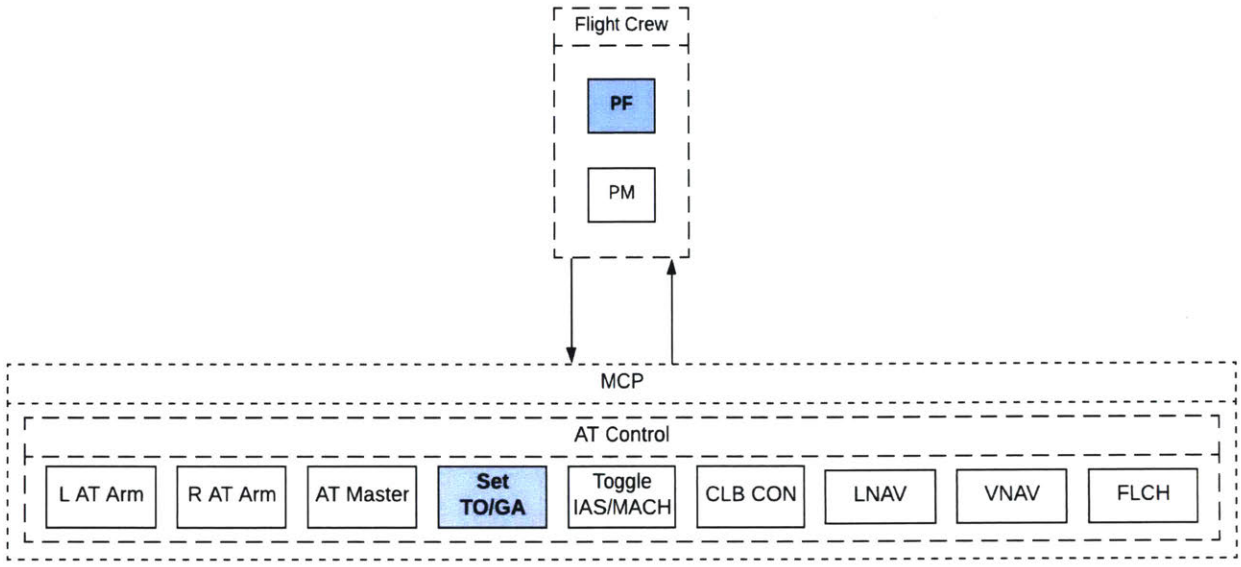



**Figure 20. Control loop Crew – Auto-Throttle extracted from the detailed control structure**

The Traffic Collision Avoidance System (TCAS) provides important situational awareness to crews and accurate guidance to avoid collisions when the ATC does not ensure minimum separation between two aircraft. One problem with adding redundancy to collision avoidance is the possibility of conflicting information or directives from two different systems.

For example, in 2002, a mid-air-collision happened over Uberlingen, Germany. One of the causal factors was a conflict between the ATC instructions and the TCAS Resolution Advisory (RA)[17]. One pilot decided to follow the ATC instructions and the two aircraft collided. For the PRM, the FAA standard explains that, during a breakout maneuver, if the crew receives a TCAS RA in conflict with instructions from the PRM controller, the crew must follow the TCAS RA. This is exactly what the crew initially did in this Case, but the problem was that the crew had to level off at 700 ft AGL (Above Ground Level) because there is a height floor for the TCAS RA. At this point, the RA is deactivated, meaning that the crew is still able to see the other aircraft, but the equipment is no longer recommending a path to avoid the collision.

Table 8 is a summary of what was found inspecting the STPA.

[17] Resolution Advisory (RA) is a mode of TCAS that has an aural annunciation and an instruction on displays to avoid a mid-air collision. For example, the aural message may be "descent, descent" and the instruction will recommend a vertical speed of 1500 ft/min or more.

**Table 8. Case C – Airbus A-340 – Phase 1**

| Case C – A-340 | | | |
|---|---|---|---|
| **Phase 1 – Inspect the STPA** | | | |
| **Task** | **Description** | **Analysis** | |
| **1.1** | Search for applicable rules and procedures | 1 – Pilots are required to GA every time the aircraft meets the criteria for unstable approaches<br>2 – TCAS RA must be followed with a higher priority than ATC commands | |
| **1.2** | Verify requirements and constraints | The crew must GA when the approach is characterized as unstable | |
| **1.3** | Verify causal scenarios | After fluctuations of parameters, crew feel comfortable to continue with landing, avoiding the consequences of a missed approach, including extra work reporting to operations and the negative impact on their reputation | |
| **1.4** | Verify control actions and UCAs | Switch / Selector | TO/GA button |
| | | Control Action | Press TO/GA |
| | Identify UCAs | Not pressing TO/GA when the approach is unstable | |
| **1.5** | Verify control relations in safety control structure | Controller | PF |
| | | Controlled Process | Throttle pedestal |
| **1.6** | Verify system-level requirements and constraints | SC-1.2: Aircraft must be longitudinally stable [H-1.2]<br>SR-1.2: if the aircraft is longitudinal unstable before landing, the PF must GA [H-1.2] | |
| **1.7** | Verify Hazards and Losses | H1: Aircraft violates criteria for stable approaches<br>H1.2: Longitudinal instability [L1, L3, L5]<br>H3: Aircraft violates minimum separation from airspace or other aircraft [All losses] | |

## 3.5 Active STPA Phase 2: Reason about the Assumptions

The SA investigated in Phase 1 all the elements of the STPA and why the incident occurred, including inadequate defenses that did not avoid the incident. In Phase 2, the SA reasons about the violated assumptions, to understand what is wrong, before fixing procedures or the analysis. To run Phase 2, the SA uses the Tasks represented in Table 9 and explained in the following sections.

**Table 9. Structure of Tasks of Active STPA Phase 1**

| **Phase 2 - Reason about the Assumptions** |
|---|
| 2.1 – Identify violated assumptions |
| 2.2 – Analyze trends |
| 2.3 – Investigate causal and contributing factors |
| 2.4 – Determine the reason for broken assumptions |
| 2.5 – Verify if contingency protections worked |

### *Task 2.1 – Identify violated assumptions*

Assumptions are naturally made in all steps of an STPA and the implementation of its recommendations. They are based on the SA knowledge about the environment particularities, how the system works, and how people behave. For instance, there might be an assumption on who receives feedback in the control structure, an assumption on human factors in UCAs, or an assumption on the operational environment in scenarios. Assumptions are also made when the SA considers that a procedure is an effective solution to prevent a hazard. There is a natural tendency to assume all controls are implemented, not degraded, and used as envisioned by the designers.

When written procedures or rules are violated, it is important to determine why the operators wanted or felt the need, to disregard the procedures or rules. Concluding that the operators were at fault because they did not follow the written rules does not solve the problem in the long-term. Human error is a symptom, not the root cause. In this Task, the SA must understand the underlying reasons for the violation of each assumption. One change in the operational environment has the potential to affect one or multiple assumptions.

If an assumption is violated for the first time, it is a leading indicator of changes to the system. However, if in future incidents, assumptions are repeatedly challenged, the SA must be able to recognize that the solutions implemented in previous Cases were not effective, and use that information in Phase 3.

### *Task 2.2 – Analyze trends*

One single event might not be enough to determine that an assumption is absolutely flawed. However, a single incident is a fact that prompts the SA to investigate deeper into the operational data, searching for trends that represent changes in the system, in the operators' behavior, or in the environment. For example, the SA may have assumed in the original STPA that limiting the approach speed in one specific airport to 180kt prevents bird strikes, as slower speeds give more time to birds to break out of the flight path of an incoming aircraft. One bird strike incident may prompt the SA to check if the number of birds is increasing in that region. However, the incident may be an isolate unfortunate event and there is no real need to change the approach speed.

If the organization already have a monitoring activity produces, there is data stored that may be used to identify if this incident was a unique event or a trend. In this Task, the SA searches for previous situations of unsafe behavior that were not identified as incidents, but tell if the assumption has been violated systematically, and provide information on how a change from the desired behavior is occurring.

### *Task 2.3 – Investigate causal and contributing factors*

All complex systems are designed with limited knowledge about the environment in which they will operate. It is hard for analysts to derive an accurate set of assumption on human, technical, and organizational potential contributing factors to accidents, such as human behavior under stress or fatigue. Moreover, modern systems running complex software have rare and very specific conditions in which automation confuses operators.

Every scenario has a single or a set of causal factors that result in the UCA. These factors may be organized using multiple taxonomies available in the literature to address concerns on mental states or organizational processes. The taxonomy must be adequate to the type of operation and cover distraction, memory limitations, human behavior under high workload, and other Human Factors. Finally, the analyst uses the observation of unsafe behavior, to identify the consequences of a repetition in other contexts, and to act preemptively to avoid repeating the same causal factor in future similar events.

### *Task 2.4 – Determine the reason for broken assumptions*

The results of Tasks 2.2 and 2.3 allows the SA determine if the assumption was flawed or if it still holds and the incident was an isolated event. If the SA recognizes that the assumption that was violated is incorrect, then it is necessary to learn from mistakes, figuring why the assumption was flawed before looking for solutions. Maybe, the assumptions made sense in one condition because it was true when considered independently, while it is false in rare conditions. Also, prior assumptions may have been accurate when the initial analysis was carried out, but

changes made it obsolete. The recognition of past mistakes helps to understand the capabilities and deficiencies of the Safety Management System (SMS).

The statement of the reasons for broken assumptions must be documented. The summary tables used in the case studies are an example of a template that facilitates the access to information in future Cases. More sophisticated software solutions would allow faster access to the complete history of past reasoning. The process models must be reevaluated, including previous considerations on mental models, to provide the understanding that is necessary to write a robust new rule or procedure. This process might require the participation of a group of experts because misleading assumptions may corrupt other parts of the analysis. The information from the previous Tasks are sufficient to start the discussion, but further investigation might be necessary. The SA must use the control structure to consider if other parts of the STPA could have been affected.

The acknowledgment of a previous mistake by an organization is still a taboo. In many industries, situations in which rules are not followed still have a single outcome: blaming the operator who had the responsibility to follow that rule. Organizations blame operators to avoid assuming responsibilities. This practice relies on the belief that punishment changes the behavior of other controllers. In some systems, this approach may produce the desired results for some time, but the fear of committing repeated mistakes exponentially decays with time and may not be entirely passed to a new generation of controllers. Thus, this strategy may not reduce the chances of repetition of similar events.

On the other hand, Active STPA may be used to condemn unacceptable behavior and to enforce the current procedures with Safety Promotion activities. However, reckless behavior or illegal actions may become a state of practice when safety policies are not covering all circumstances under which disciplinary actions would apply. In this case, the Active STPA becomes a formal method to identify gaps in safety policies and re-state what is acceptable. More than that, it also becomes a source of information on how people challenge the rules when their training is inefficient or when controllers are guided by bad intentions. Deliberate violations and the intervention of adversaries might be rare in some industries and relatively common in others. Therefore, the SA is required to learn from those violations to set better defenses and prevent similar violation of the rules.

### *Task 2.5 – Verify if contingency protections worked*

A system's robustness should not rely only on constraints. The Active STPA has an underlying hypothesis that all the assumptions made when designing the system may be violated. Therefore, hazards with higher severity require a *Contingency Protections*. These protections, such as redundancies, are defenses set during development to avoid accidents, or reduce damage, when assumptions fail. In this Task, The SA must verify if the system already has those protections in place, if they were effective, or if new defenses must be created. If this defense

was not effective in preventing losses, the SA learns about its weakness to create new protections based on new assumptions.

## Case A - ATC

After inspecting the completeness of the STPA in relation to the event, it becomes clear in hindsight that the Assumption made considering only the reaction time of the ATC controller was violated. This assumption is flawed because it does not consider situations in which the controller believes that the intruder AC knows that their position has deviated from course, and had already begun the correction. As a consequence, the constraint in 1.2 is unable to prevent the incident. This constraint does not help the SA write reasonable procedures. Prevention would require more detailed constraints and rules that are clearer to follow.

The fundamentals were complete, but at least one constraint was inaccurate or missing. So, why is the STPA incomplete, starting with the context of the UCA? It turns out that the action "breakout" command, that is exclusive of parallel approaches, was not thoroughly considered due to a misunderstanding about how parallel approaches differ from regular ones. The analyst associated the missed approach procedure with a regular GA in this scenario. The lack of this context to a specific action caused a cascade effect on the STPA. Every time elements of the STPA are missing, it is a sign of a flawed assumption. It is natural for an analyst to miss STPA elements when a specific context is not considered. This kind of mistake is common when developing an analysis with limited time, a restricted number of analysts, or lack of experts.

One particularity of dealing with ATC as a controller is that assumptions about the controller mental models involve other assumptions about the crew's situational awareness[18]. In Phase 2, the SA needs to visit ATC trends of pilot's behavior, such as a history of NTZ incursions, regular reaction time for pilots and controllers after an NTZ incursion, or the number of previous breakout commands. This will help evaluate what the required attitude of ATC controllers should be. The contributing factors to those trends allow the SA to write a proper assumption and a new protection, as summarized in Table 10.

[18] *Situation awareness is an important component of pilot/system performance in all types of aircraft. It is the role of the human factors engineer to develop aircraft cockpits which will enhance situation awareness. Research in the area of situation awareness is vitally needed if system designers are to meet the challenge of providing cockpits which enhance SA.* (Endsley, 1988)

**Table 10. Case A – ATC – Phase 2**

| Case A - ATC | | |
|---|---|---|
| **Phase 2 - Reason about the Assumptions** | | |
| **Task** | **Description** | **Analysis** |
| **2.1** | Identify violated assumptions | When a crew realizes that they are flying inside an NTZ, they will converge to their localizers.<br>Distance from NTZ boundary to RWY centerline and AC speed provide ATC sufficient time to take action<br>Distance from NTZ boundary to RWY centerline and AC speed provide ATC sufficient time to take action |
| **2.2** | Analyze trends | There are no trends on how often ATC controllers delay on calling an NTZ intruder AC |
| **2.3** | Investigate causal and contributing factors | The ATC controller avoids criticizing pilots for small mistakes if they perceive that the intruder AC already started a turn to correct its path |
| **2.4** | Determine the reason for broken assumptions | The definition of "convergence" is not accurate. If an aircraft converges to intercept the runway alignment only in the threshold, it will be flying for too much time in the NTZ, and the TCAS RA of both aircraft will remain activated |
| **2.5** | Verify if contingency protections worked | The protection is given by the fact that all aircraft must have a working TCAS and pilots are supposed to follow RAs. In this Case, the protection worked because the pilot of the A-340 increased the rate of descent, avoiding an accident |

## Case B – B-737

An assumption was identified about the ideal amount of workload during approaches for landing. Unintentional delays in procedures lead the SA to look into human factors to explain human error. After checking whether the protection for this assumption worked, the SA searches for trends and related leading indicators in the FDM data or in voluntary reports. This extra data helps in the identification of causal factors. This reasoning will finally lead to a better understanding of why the assumption was flawed. Only the acknowledgment of what is wrong

allows the judgment that is necessary to write a robust new assumption and an efficient protection feature. The results of Phase 2 are summarized in Table 11.

**Table 11. Case B – Boeing 737 – Phase 2**

| Case B – Boeing 737 | | |
|---|---|---|
| **Phase 2 - Reason about the Assumptions** | | |
| **Task** | **Description** | **Analysis** |
| **2.1** | Identify violated assumptions | 1 - If the procedure is briefed before IAF, workload level is not a reason to forget selecting LOC<br>2 – The PM always checks if the PF engaged LOC before the ideal turning point |
| **2.2** | Analyze trends | Change: There is a new responsibility for the PM: check visually for separation with the other AC in parallel App. |
| **2.3** | Investigate causal and contributing factors | Memory error caused by distraction or high workload.<br>PM was visually searching for the other aircraft during a parallel approach<br>TCAS RA of both aircraft remained activated due to low convergence to re-intercept the runway alignment |
| **2.4** | Determine the reason for broken assumptions | The assumption that the PM had time enough to engage the LOC when under vectors was correct for regular approaches, but not necessarily for parallel approaches |
| **2.5** | Verify if contingency protections worked | The protection is the supervision and intervention of the ATC controller. In this Case, ATC GA order to B737 was late.<br>The other Aircraft is supposed to execute an evasive maneuver based on TCAS RA. This protection worked. |

## Case C – A-340

The procedures in place did not cover the scenario in this event. The lack of a causal scenario is expected to be the problem in most Cases because the variability in causal factors depend on a vast number of assumptions. A scenario that is similar in terms of flight path is not valid for this event because it is based on different pitch attitudes. The fact that the decision in the event was made because the alternative (GA) was more dangerous places it in a different

context, resulting in the need for a new UCA and new scenarios. This is part of the reasoning developed in Table 12.

**Table 12. Case C – Airbus A-340 – Phase 2**

| Case C – A-340 | | |
|---|---|---|
| **Phase 2 - Reason about the Assumptions** | | |
| **Task** | **Description** | **Analysis** |
| **2.1** | Identify violated assumptions | 1 When another aircraft enters in the NTZ, the ATC will command their breakout turn.<br>2 The ATC acts in less than 10s when another aircraft enters the NTZ<br>3 When there is no visual contact, it is dangerous to GA<br>The approach of major airports is usually controlled by selected and more experienced controllers. These controllers are expected to have a good ability to deal with complex scenarios, showing more initiative and correcting mistakes more effectively. |
| **2.2** | Analyze trends | The history of NTZ incursions is getting lower overtime because pilots are getting experienced with the new procedure |
| **2.3** | Investigate causal and contributing factors | The A-340 pilot is experienced in parallel approaches but never faced a similar event |
| **2.4** | Determine the reason for broken assumptions | During PRM, if our aircraft is flying the localizer and another aircraft enters the NTZ, there will be a resolution from TCAS that could be to climb or descend, and the ATC will command a breakout turn<br>PRM standards define that the breakout turn is commanded to the aircraft that is correct, not to the one that entered the NTZ |
| **2.5** | Verify if contingency protections worked | The protection is the TCAS RA and it worked in this event |

## 3.6 Active STPA Phase 3: Solve and Update

In Phase 2, the SA understood what was wrong and documented new assumptions that must now be translated into actions. It is also important to complete what was missing and fix what was inaccurate in the STPA. The first four Tasks of Phase 3 usually require a meeting with experts and the participation of the Flight Ops team. This meeting starts by presenting the result of previous Phases to initiate a discussion about possible solutions. Phase 3 is organized in the Tasks detailed in Table 13 and in the following sections.

**Table 13. Structure of Tasks of Active STPA Phase 1**

| **Phase 3 - Solve and Update** |
|---|
| 3.1 – List possible defenses |
| 3.2 – Analyze tradeoffs |
| 3.3 – Determine the optimum solution |
| 3.4 – Implement new defenses and protections |
| 3.5 – Update the STPA |

### *Task 3.1 – List possible defenses*

After understanding what went wrong, and formulating new assumptions, it is time to decide on how to adapt the system to make it safer. In simple systems, there may only be one reasonable solution to address the problem, but in complex systems, there may be many plausible solutions to operational problems. The SA or a group meeting creates a set of possible solutions to attain the desired change. The list should be exhaustive but avoid solutions that are clearly ineffective or unfeasible.

There must be a multi-factorial spread among the set of solutions, showing ones with smaller impacts on current procedures and solutions that require more investment of resources. This variability allows management to exert judgment on how to apply limited resources. It is not just a question of cost/benefit but a reality for organizations that are limited in qualified personnel and have numerous new defenses to apply.

### *Task 3.2 – Analyze tradeoffs*

The analysis becomes a management problem, requiring the use of management tools. There are several ways to run a tradeoff analysis, and the group should use the methods that are already incorporated by the organization. In general, the discussion begins with a comparison of the advantages and disadvantages of each possible solution. The discussion continues

considering how each solution would be accepted and what would be the technical and social collateral effects. Every organization has a preferred tool for ranking solutions, such as the use of decision matrixes and scorecards. The discussion may require a revision of the generation of new assumptions from the end of Phase 2.

The safety manager must serve as a moderator and someone needs to document the key arguments to later incorporate their reasoning into the STPA. Tradeoff studies require an exploration of more detailed STPA scenarios (Horney, 2017) to complement the results of other management tools. The group must avoid simple and broad solutions. Solutions requiring deeper changes must initiate a study to incorporate their impact in the analysis. Candidate solutions with less compatibility with other existing rules demand a collateral analysis.

### *Task 3.3 – Determine the optimum solution*

After organizing all the necessary information, the group finally deliberates and then decides on one or multiple solutions among the ones listed in 3.1. This solution has a new set of requirements and constraints and the changes that are required in rules, procedures, and manuals for operators.

The SA needs to find a balance between prevention and mitigation. The term 'prevention' means avoiding any consequence while 'mitigation' focuses on minimizing consequences. When the resources for safety are unlimited and there is no conflict among constraints, all defenses can be implemented to 'prevent' the identified unsafe scenarios. The system would be safer with some degree of efficiency loss. For systems in which a balance between efficiency and safety is necessary, risk is reduced with sound 'mitigating' defenses. The strategy for both types of defenses involves a range of possible actions, including:

- Revision of the system design with changes to the functional control structure
- Modification of operational procedures
- Re-arrangements of staffing
- Training of personnel to specific scenarios
- Development of emergency and contingency plans
- Ceasing operation

For impactful decisions or when there is an internal conflict of interests, higher-level management of the organization must have access to the tradeoff analysis and participate in the decision process. With the solution chosen, it is then time to implement them.

### *Task 3.4 – Implement new defenses and protections*

The optimum solution has a set of new defenses, and eventual requests for testing and evaluation. The defenses are already de-conflicted with other rules and procedures. All updates of the hazard analysis will result in changes in the company's documentation. Higher-level

documents, such as the policy for security, receive a great benefit from the STPA. In the Active STPA, more updates are expected in lower-level documents, like procedures and manuals. Every change must have a declaration of who is responsible for the implementation of defenses and a deadline for making these changes.

One might simply execute the changes and broadcast them to all operators. However, considering that with Active STPA there will be a regular flow of changes, constantly sending notes to operators does not transform mental models effectively. This management approach becomes a transfer of responsibilities possibly resulting in blaming operators for lack of adaptation. What needs to be done instead is a coordinated use of different communication channels to deliver the new procedures to the operators in a timely manner.

Most safety-critical organizations have standard procedures to guide the actions of their users. Procedures are taught during training and enforced throughout the operation. They are culturally integrated to avoid blame. In other words, if the procedure was followed and an accident happened, the blame is partially transferred to the organization. When action against a procedure is necessary and the operator shows good judgment, he or she is rewarded, and the procedure is updated. To understand when hazards could lead to that kind of situation, managers need to understand the safety knowledge required for operation. This is only possible by exploring the human factors related to each activity.

The desired safe behavior requires building mental models to facilitate proper actions when specific conditions are detected and recognized. It also requires responding to instances of those conditions that alert proximity to a hazard. That becomes necessary as humans are affected both by an excess of information, which causes high workload and stress, and lack of information, which leads to low situation awareness and distractions. Most systems have hazards related to both extremes, but prevention is possible using methods to measure the workload in primary and secondary tasks (activities).

The process to implement new procedures explores communication opportunities that depend on how operations are organized. In general terms, four categories are proposed as a reference:

- **Training:** The first opportunity to teach and to present limitations and rules has the benefit of a mind clearer of biases and preconceptions. The study of manuals must have a reasonable set of information regarding safety. That will be used to form the mental models and to serve as a consultation source during operations.

- **Planning:** The time dedicated to planning a set of actions (e.g., a mission in military activities) is an opportune time to communicate safety concerns to operators. The addition of safety information during the planning activity reduces surprises and the variability of improvisations.

- **Setup:** When the task is complex and requires a fast and accurate response, the operator prepares himself or herself by recalling the mental models and remembering the required reactions for off-nominal situations. In many systems, checklists are safeguards against memory limitations. In modern systems, software solutions provide ways to feed up-to-date information, like a display of items that automatically clears what was done and highlights what is left to do.

- **Operation:** In dynamic phases of operations, there is no time to search for the manual or to read documents. The solution for the communication of safety information is the use of aural, haptic, and visual cues. They must be simple, recognizable, and unequivocal.

This safety communication method respects the way people incorporate tacit and explicit knowledge, and they are in accordance with the standards for Safety Promotion in the SMS framework. Even though, to monitor the effectiveness of the elected changes, new defenses must be monitored. The monitoring of the effectiveness of the changes in procedures and policies is an important feedback to determine if the managers are actually learning.

The changes that are necessary to implement new defenses must include new protections to substitute the contingency protections that failed, or could have failed in the incident. New protections need to be independent of the causal factors that would affect the flawed assumption because a single factor would endanger the system by violating the assumption and its protection. At the same time, the robustness of the new protections depends on the reevaluation of the severity of their failures. If the Active STPA already identified a relevant number of broken assumptions, the system must have more effective contingency protections.

### *Task 3.5 – Update the STPA*

The new set of assumptions must be incorporated into the STPA and, consequently, all the identified missing elements should be added. The elements that already exist and were not correct due to a flawed assumption are now fixed. This task results in changes to the list of safety requirements and constraints. This list is not just important to the current operation, but it is also used as a reference for modifications and design of future equipment. This update follows the standard orientation explained in the book Engineering a Safer World (Leveson, 2011) and the STPA Handbook (Leveson and Thomas, 2018). The SA should start fixing from the first missing step because it facilitates the maintenance of logical connection among steps. For instance, if a scenario is the first missing part, then a new one is generated, leading to new requirements or constraints and new procedures.

Finally, the SA must keep in mind that correcting the parts that are missing do not guarantee that all missing parts were found. Also, it does not mean the new set of defenses for the new constraint will be adequate. Analysts with the best intentions may overlook latent failures that lie dormant for a long time. Active STPA is a learning process that allows trials and

errors. It is also a way of better understanding the system's vulnerabilities and assists in the refinement of rules or procedures for operations.

## Case A - ATC

As with any problem in complex operations, there are multiple solutions. Further tradeoff analysis and decision making choosing the optimum solution requires consulting an ATC expert. Even though, there is no available information of an implementation of the SPIs found in this analysis. If implemented, it would have the potential to show if parallel approaches are becoming safer because pilots and controllers are becoming more familiar with them, or on the other hand, whether an increase in traffic is making it more a more hazardous procedure. In the final Phase of this Case, Table 14 summarizes solutions found, implementation of new procedures, and a subsequent updated STPA with changes to the system.

**Table 14. Case A – ATC – Phase 3**

| Case A – ATC | | |
|---|---|---|
| **Phase 3 - Solve and Update** | | |
| **Task** | **Description** | **Analysis** |
| **3.1** | List possible defenses | Solutions:<br>1. Reinforce controllers' responsibility to alert both crews when NTZ intrusion occurs during parallel approaches<br>2. Identify and discipline controllers every time a trigger is exceeded |
| **3.2** | Analyze tradeoffs | As a first action, controllers should be reminded about their responsibilities. If the trend continues, the identification of controllers followed by disciplinary actions will occur |
| **3.3** | Determine optimum solution | Reinforce controllers' responsibility to alert both crews when NTZ intrusion occurs during parallel approaches |

| Task | Description | Analysis |
|---|---|---|
| **3.4** | Implement new defenses and protections | CRM new procedure: Crews who entered in NTZ must communicate that they are correcting their path<br>To re-interception of the LOC when the deviation is greater than two dots, the crew must use a heading that is at least twenty degrees different than the course of the LOC<br>- The current protection must continue<br>- Activate visual alarm for controllers when an aircraft is in NTZ to prompt their action |
| **3.5** | Update the STPA | STPA was complete. Procedures are adequate and will be reinforced |

## Case B – B-737

The discussion of the impact of the candidate solutions is organized on a tradeoff analysis listing their pros and cons. The optimum solution establishes new defenses, SPIs, and triggers as exemplified in the summary Table 15. Finally, in this Case, the STPA was complete and correct.

**Table 15. Case B – Boeing 737 – Phase 3**

| Case B – Boeing 737 | | |
|---|---|---|
| **Phase 3 - Solve and Update** | | |
| **Task** | **Description** | **Analysis** |
| **3.1** | List possible defenses | Solutions:<br>1. Transfer responsibility to select LOC to PF<br>2. Eliminate the requirement that PM acquire and maintain visual contact with other AC<br>3. Determine that PM should start visual search only after setup of AP and call out to PF |
| **3.2** | Analyze tradeoffs | (1) PF has other responsibilities and high workload<br>(2) This responsibility is a Contingency Protection for another assumption |

| Task | Description | Analysis |
|---|---|---|
| **3.3** | Determine optimum solution | Determine that PM should start visual search only after setup of AP and call out to PF (Solution 3) |
| **3.4** | Implement new defenses and protections | Communicate new CRM procedure to all pilots:<br>CP: PM should start visual search only after setup of autopilot and call out to PF on parallel Approaches<br>The ATC must focus on the separation between two aircraft when the second one is converging |
| **3.5** | Update the STPA | No changes – low-level constraint is still valid |

## Case C – A-340

This investigation has pointed to another flaw in current standards for parallel approaches. Although most TCAS in operation provide a RA associated with a vertical directive, such as *increase the rate of descent*, the ATC controller procedure is a breakout turn command. This mismatch may lead to undesirable outcomes. The crew might react to the RA pitching down, inducing a high rate of descent, when the PRM controller commands the breakout turn to a specific heading. The orders are not conflicting, and, if the PF follows both, the aircraft will be turning with a high rate of descent, which may require a recovery maneuver not currently trained in simulators. This argument becomes part of the tradeoff analysis of Phase 3, summarized in Table 16.

The investigation of this event also led to the exploration of other causal factors. The FAA recommends keeping the audio of the PRM frequency off in the beginning of the approach, turning it on only after changing the primary radio to the tower frequency. If the crew fails to execute this extra PRM procedure, a breakout command could be ignored. Thus, the crew is required to have the PRM frequency selected and at a proper volume. One possible solution to accomplish with this requirement could be to adjust the secondary radio to the PRM monitor frequency in advance. However, listening to a channel with constant communication too early may interfere with other communications.

**Table 16. Case C – Airbus A-340 – Phase 3**

| Case C – A-340 | | |
|---|---|---|
| **Phase 3 - Solve and Update** | | |
| **Task** | **Description** | **Analysis** |
| **3.1** | List possible defenses | 1 – Notify the tower controller when a TCAS RA is received, to avoid the breakout turn<br>2 – Initiate the breakout turn before receiving PRM controller instructions<br>3 – When receiving an RA due to an aircraft that is behind, accelerate the engines, retract the landing gear, keep the GS until reaching 180kt, and initiate a climb<br>4 – Initiate a GA immediately after receiving an RA<br>5 – Add a scenario for simulator training |
| **3.2** | Analyze tradeoffs | - There are no standards for pilot communication to the tower during PRM<br>- After overshooting the localizer, the other aircraft may turn outward and converge quickly to the localizer. The PRM controller may judge that there is no need for breakout<br>- GA with a resolution to descend is hazardous when the other aircraft is higher and behind |
| **3.3** | Determine optimum solution | - When receiving an RA due to an aircraft that is behind, accelerate the engines, retract the landing gear, keep the GS until reaching 180kt, and initiate climb (3)<br>- Add a scenario for simulator training (5) |
| **3.4** | Implement new defenses and protections | - A new procedure for similar situations must be communicated in two days by Flight Ops<br>- Safety must coordinate with ATC the new procedure in one week<br>Pilot judgment in situations with conflicting orders is paramount |

| Task | Description | Analysis |
|---|---|---|
| **3.5** | Update the STPA | Add scenario: Upon receiving a TCAS RA to descend because there is an AC behind and higher, crew executes a regular GA procedure because they remember that they are supposed to GA, but they do not remember that they need to accelerate until 180 kt before climbing.<br><br>Add constraint: pilots need to accelerate to a minimum of 170kt before climbing when the intruder of an RA is behind during approach |

In this Chapter, three Cases covered the three possible findings of an Active STPA: a situation in which the procedures are appropriate but not followed by operators, an analysis that was complete when performed and became outdated due to changes, and an analysis that was incomplete from the beginning. In Case A, the ATC controller, the procedure does not have to change, but enforced to avoid the attention of the controller being shared with other activities. In Case B, the procedure was initially correct, but the introduction of parallel approaches made the original procedure obsolete, requiring an adaptation in the procedures. Finally, in Case C, the scenario that the Airbus crew faced was never imagined, or considered not to occur, requiring the SM to add new elements to the STPA.

The Active STPA becomes an exercise in critical thinking, as the analyst evaluates an issue to re-think a judgment previously made. It requires the understanding of functional relationships and the application of standards to determine the real problems. Logical reasoning behind each scenario may aid in predicting potential hazards. The result is transformative knowledge of how the system works in multiple contexts. The hazard analysis is used to monitor the validity of the assumptions to be adaptive for dynamic systems.

# 4. Integrated Safety Management System

The Active STPA described and exemplified in Chapter 3 is one of the processes of a framework called Integrated Safety Management System (I-SMS). In this chapter, the I-SMS is introduced, exemplified with an aviation case, and compared with aviation SMS practices. Therefore, an explanation of the ICAO's Safety Management System (SMS) is necessary. Finally, the concept of a shared hazard analysis is proposed.

## 4.1 I-SMS with Active STPA

Pro-active management requires effective communication and monitoring activities. The proposed solution is the use of a structure with a hazard analysis at its core in order to inform higher-level management of necessary facts and information. The Integrated Safety Management System (I-SMS) proposed in this research is a management model that is designed to enhance monitoring and communication tasks in organizations where safety is critical. The objective is to offer a common language or protocol to communicate the observations made during operations. These are then used to verify the validity of the assumptions made in the hazard analysis and to identify leading indicators. This will also help in the identification of increasing risks and how to respond to a changing system. The general framework of the I-SMS is presented in Figure 21.

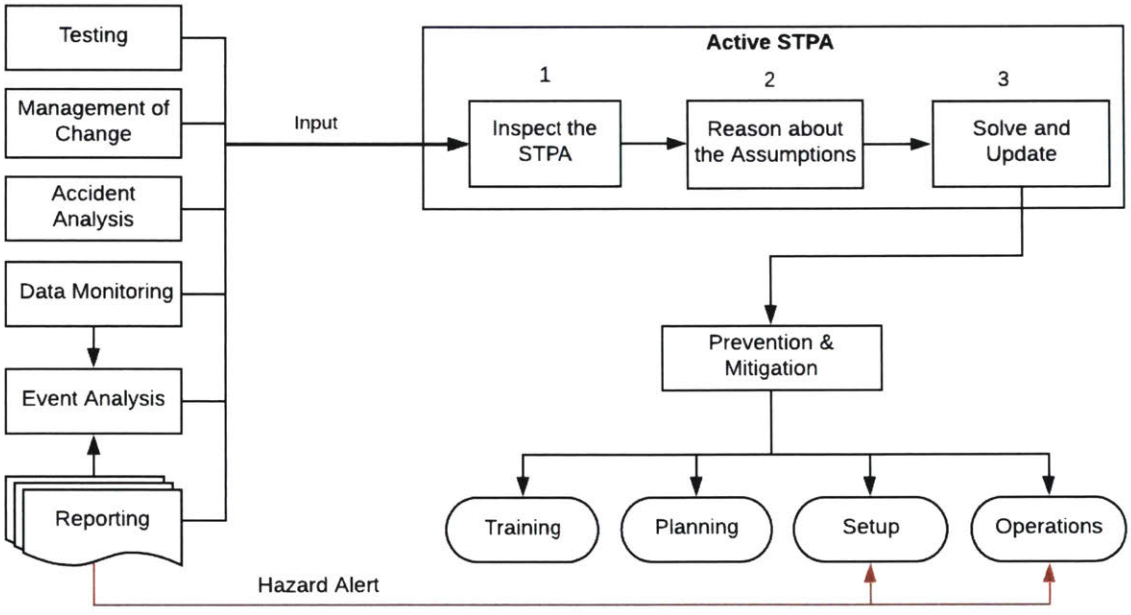



**Figure 21. I-SMS General framework**

The left side of the diagram shows the many sources responsible for the input of information into the Active STPA. The verification and validation tests become opportunities to

add details to the analysis that developers did not consider when the product was just a concept or an abstract idea. When the system is already operating, changes lead to the initiation of a process that requires revisiting the hazard analysis to avoid unexpected events. Moreover, in addition to learning from accidents, the I-SMS also learns from voluntary reports of incidents. The stakeholders' participation regarding hazardous conditions works both to enhance the system, and to foster a safe attitude, keeping the organization aligned with its culture. A proper safety culture ensures the focus is not on blaming or punishing, but ensuring everyone is comfortable with reporting issues, even pointing out when a procedure is forgotten.

Proactive SMS requires effective channels to communicate safety information. This goal is obtained only if all stakeholders use the same language. In an ideal system, a coding system using letters and numbers to identify STPA elements make them traceable until the end of the product's life. The first safety concerns should come from the elaboration of the Concept of Operations (ConOps), followed by all other concerns, which should continue to be organized and filed during development. Throughout a system's lifetime, there will be many opportunities to make the hazard analysis more robust. The following items are a reference of sources of the general framework:

- **Testing and Certification:** The preliminary hazard analysis evolves with engineering simulations, and is complemented during the testing phase. Testing is the first opportunity to detect wrong or incomplete assumptions as the new environment is evolving. It is possible to measure symptoms of undesired behavior in a test environment, before certification and the beginning of regular operations, when it is easier and less expensive to change the project. If accidents happen in a testing environment, the losses are minimal compared to those during operations.

- **Active Data Monitoring:** Most modern complex systems rely on software solutions to monitor performance. The collection of data is straightforward, but the analysis is not trivial. Without knowing what to look for, an immense amount of data may be organized by a metric that is not appropriate to detect safety or security issues. Data must be collected, organized, stored, and secured. But there is no point in doing so if the data is not used to enhance the process. The purpose and rules for monitoring must be clear. Operators are prone to accept the observation of their performance in specific events, but many are not comfortable with constant surveillance.

- **Inspections:** Inspections are systematic ways to observe if the system is running as planned. To assure comprehensive inspections, the frequency must be high enough to be considered routine, but not so high as to interfere with performance. Audits are another form of safety inspection performed by an internal company division or third-party experts.

- **Management of Change:** Most complex systems have a long life, which increases the chances of changes in the product (modernization or association with other products), the user (cultural changes) or the environment in which they are used. Management of Change is a process to plan and execute a change that has an impact on operations; one example would be the inclusion of a new electronic warfare pod on a fighter jet. Leading indicators are useful to measure how an organization handles planned and unplanned changes. Feedback from the Active STPA can be used to adjust policies of Management of Change and to adjust procedures when operational changes are detected.

- **Investigations:** Accidents and incidents are opportunities to enhance operations as they are usually caused by a combination of social and technical factors. Investigations are also recommended when there was no loss, but an unexpected hazardous condition was perceived and communicated. Investigations often show evidence of unusual factors, including behavior, happening before any damage or injury, i.e., when something could be done to avoid a loss. These signs are referred to as safety leading indicators (Leveson, 2015), and must be identified and translated into the hazard analysis.

- **Voluntary Reports:** In modern safety systems, when a product is delivered to the operating company, there is abundant feedback from users. Users may describe incidents in structured messages, using a format is recommended for better organization and efficient updating of the hazard analysis.

The output of the Active STPA is a solution that updates and enhances rules and procedures already in place, suggests testing activities, or even modifications to the design of system components. The new defenses update the system's information flow, bringing it to a safer state. However, effective management demands an understanding of the operator's needs and difficulties. The application of new defenses needs to consider how and when critical information should be delivered to operators and appropriately assimilated.

A manager must guarantee that the information generated by the active STPA will arrive at the desired destination, communicated to, and understood by everyone necessary. Those tasks demand an observant manager to ensure that all previous safety communications are effective. Without monitoring the information flow, an accident could occur due to a causal factor that was already identified and treated, but the defenses used to prevent it were not implemented or correctly followed.

If management properly promotes the actions required to run the I-SMS in the organization, attitudes, including the acceptance of higher risk for higher productivity, will be discouraged. If the operators believe managers are actively discussing each new event and doing more than just complying with regulations (culture of compliance), they will become actively

engaged in trying to identify and solve problems. Moreover, putting safety at the forefront, through frequent discussions on hazard awareness and prevention during daily operations, will help promote a positive safety culture and reduce risk.

The proper implementation of the model to a specific system requires tailoring the general framework. That means that each box, in Figure 21, on the left side as well as the bottom of the general framework may receive a more specific label. Once this structure is developed, it is then divided into three processes:

P1: Preparation of AHAI and Hazard Alert

P2: Active STPA

P3: Prevention & Mitigation

Each of these processes is explained in the following sections to guide the organization of effective actions on management activities.

## 4.2 I-SMS for Commercial Aviation

Aviation is still the safest means of transportation worldwide, and it is also growing at a faster pace than other forms of transportation. However, having good safety records should not restrict the implementation of modern approaches to hazard analysis. The aerospace industry has been a leader in integrating sophisticated approaches for safety. Aviation is a known testbed for methods extensively applied to similar systems in other fields of study.

The application of I-SMS to any specific type of industry or commercial service requires customization of the framework to adapt to its particular environment. For instance, commercial aviation has many standards and acronyms that stand for the name of the protocols developed for each activity. Figure 22 shows the I-SMS model adapted to airline operations.

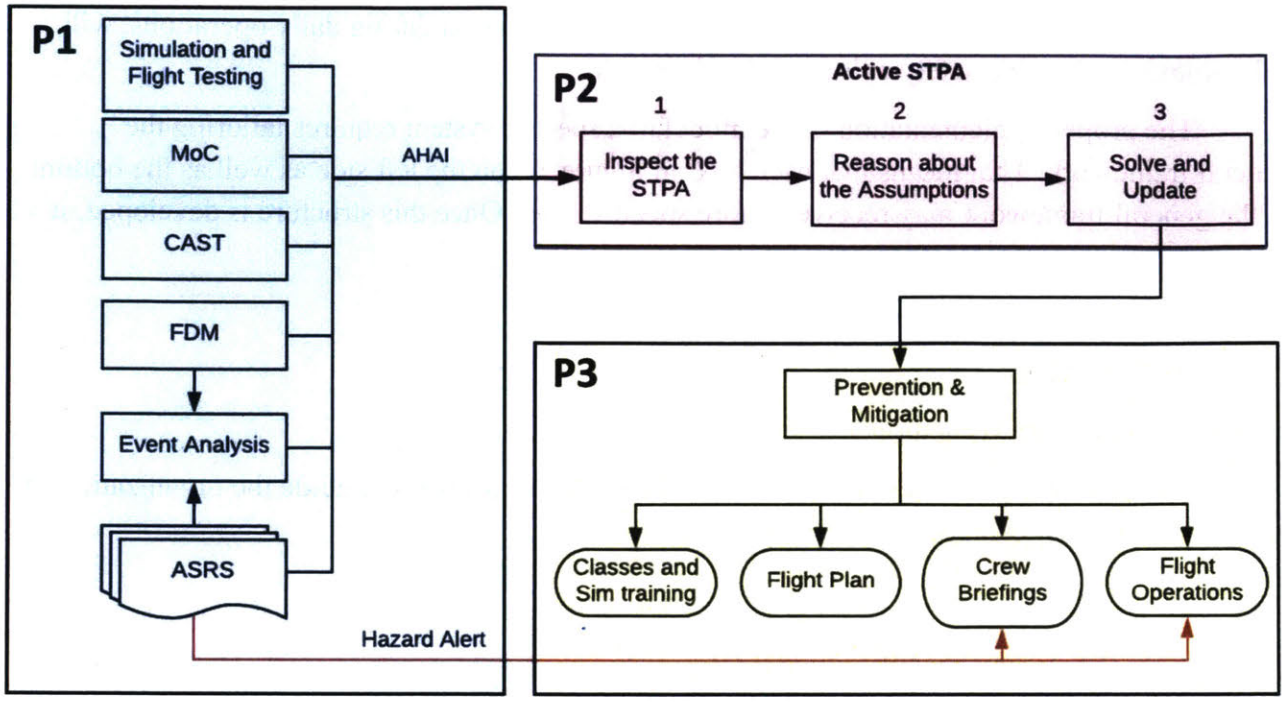



**Figure 22. Customized I-SMS model for commercial aviation**

When adapting the inputs for aeronautical examples on the left side of Figure 22, the following changes are necessary:

- Testing becomes simulation, flight testing, and certification processes.
- The Management of Change is now a formal document abbreviated as MoC, and it has more specific guidelines than the general approach.
- Accident Investigations could assume different forms depending on the country investigating, as investigations are the responsibility of federal agencies. In this study, the reference tool for accident investigation is CAST, a tool of STAMP that is described in more detail in this Chapter.

- Current Active Data Monitoring has a similar format but has adopted different names. For instance, many American companies use Flight Operations Quality Assurance (FOQA), this method is used for Flight Data Monitoring (FDM) which is also a part of the Flight Data Analysis Program (FDAP).
- Voluntary Reports may take many different forms in aviation. One example is the Aviation Safety Report (ASR).

The required safety knowledge of a commercial airliner crew is quite extensive and specific. It is represented on the bottom of the Figure 22. Part of the critical safety information is better assimilated during training; such as the appropriate timing to retract a landing gear after

takeoff. Other critical information, like the obstacles on a departure procedure, needs to be fresh as it may depend on a dynamic environment. The pilot is required to merge mental models of safety information generated in:

- Regular classes, practice in simulators, and flight instruction.
- Information provided before going to the airplane, such as the Notice to Airman (NOTAM) and meteorological briefings.
- Takeoff and approach briefings[19].
- In-flight data, such as airspeed limitations on instrument approach plates, which are provided during the flight on paper, pages of electronic flight bags, or displays cues.

The combined safety information from multiple channels must cover all the required information that is necessary to operate safely in normal and emergency situations.

### 4.2.1 Hazard Alerting System

In the I-SMS framework, voluntary reports from the event may receive two designations: Active Hazard Analysis Input (AHAI) and Hazard Alert. The AHAI described in the previous sections of this chapter is the regular path that all reports must take. For time-sensitive situations, when there is no time to run the three Phases of the Active STPA, the person reporting needs this bypass channel to reach the ones who will face the hazard shortly. These time-critical observations, such as a drone crossing the runway on final approach, potentially dangerous environmental phenomena, or even criminal actions, require instant communication. These additional messages that communicate events when hazards only last a short duration are called Hazard Alerts. The Hazard Alerts are messages with the same content as an AHAI. The main difference is their destination. They may be transmitted using software solutions for mobile connectivity to select other operators and alert them instantly.

One critical problem managing safety relates to the time it takes from the identification of the problem until the implementation of the solution. The SA receives numerous inputs from multiple sources, and it takes time to read their content and run all three phases of the Active STPA for each of them. The processing may not be immediate, as it may require the presence of experts. When the solution is decided, there is another delay in the execution of the changes and the communication of them to everyone who needs to know them. If the change requires training, there is still a final delay to provide training on the new practices and to extinguish the negative learning effect from the previous procedure.

[19] Briefings are meetings that the crew, and eventually other people working in the operation, get together to: communicate how the flight or part of it will develop, define what are the actions needed, and prepare for emergency situations.

Moreover, systems have vulnerabilities that are explained as latent conditions, such as poor process design, improper procedures, human attitudes (including complacency), inadequate supervision or controls, or undetected maintenance errors. Within a system, latent conditions can lie dormant and undetected for years. When those conditions appear, there might be no time for a proper analysis, and the system must react quickly to time-critical events.

Suppose that a pilot sees a drone and communicates its position to the control tower. The airport administration is then responsible for finding the drone operator, and ensuring its operation is ceased. Meanwhile, ATC continues to inform pilots arriving in the Terminal Area about the hazard. If the hazard persists, the Automatic Terminal Information System (ATIS) is updated with a message that will automatically alert all arriving crews.

Hazard Alerts allow operators to communicate a hazardous condition directly to everyone who needs it. Ideally, pilots should receive a feed with information that is pertinent to that specific flight. The feed becomes part of the safety briefing for the flight. A smartphone app is one proposed tool that would allow communications involving weather, airport conditions, and navigational information to pilots, as well as safety features that are specific to the operators of each model of aircraft. This is possible using built-in algorithms, and a set of filters applied by whoever is reporting, to spread information more efficiently. To avoid an overflow of non-relevant content, users would be educated on the types of reporting that are found acceptable while using this information channel.

According to a partner airline, the current protocol for pilots who observe time-critical hazards is to contact the Integrated Operations Control (IOC). The IOC can call other crew members if they have not pushed-back[20] yet or send an ACARS message if they are taxiing or flying. If the issue requires a decision from higher-level management, the pilot calls or sends an email directly to the Duty Operations Manager (DOM), a 24-hour service that always connects the crew with selected management personnel. The DOM decides about the appropriate solution and contacts the affected crew or the IOC to send the ACARS.

The use of such collaborative tools is complementary to traditional techniques and has the IOC and DOM as managers of the platform. Participants can share their ideas or build on other's ideas for a deeper understanding of the problem. This online system might have incentives for participants to make the debate on safety issues more convenient and productive. Such incentives may be the concession of safety awards as part of safety promotion activities. There are similar solutions in use, but they are informal and not integrated with the SMS.

The Aviation Safety Information Analysis and Sharing (ASIAS) program is widely accepted and works closely with the Commercial Aviation Safety Team and the General Aviation Joint Steering Committee (GAJSC) to monitor known risk, evaluate the effectiveness of deployed mitigations, and detect emerging risk. The Hazard Alert messages may use similar

[20] Push-back is a procedure in which the aircraft is pushed backwards from the terminal building and positioned in the apron to start the taxi.

channels to communicate across organizations. When operators realize the reporting system is effective because the messages they receive are relevant and increase their awareness, they become encouraged to observe the system more carefully to proactively report, reinforcing the loop.

### 4.2.2 Process 1 (P1) - Preparation of Active Hazard Analysis Input

The new sources of information identified in tailored I-SMS for commercial aviation are discussed in the following sections, combined with the peculiarities of already established sources of information in the industry, and how they could provide adequate input for the Active STPA.

#### *4.2.2.1 Flight Testing and Certification*

The use of models and methods to design tools for new aircraft development are essentially different than tools for operations. However, development engineers need to understand operational difficulties, while system operators need to understand engineering limitations. Thus, the development and the operational hazard analyses should converge to a single language and platform to allow faster and more efficient communication of safety problems. This channel should allow the communication of the information listed in Figure 23, the requests from operations to test scenarios, and the AHAI for the Active STPA.

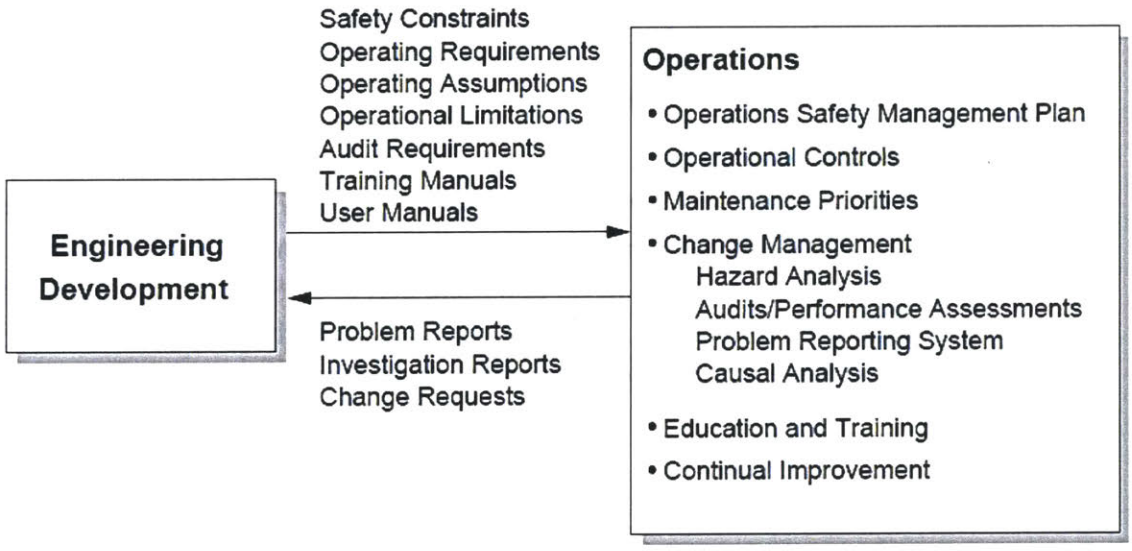



**Figure 23. Safety information flow between development and operational organizations (Leveson 2012)**

Many aircraft manufacturers invest in developing simulators to study Human-Machine Interaction (HMI) and to test fly-by-wire handling qualities. The HMI tests go from finding an appropriate position and format for controls to pinpointing confusing solutions of new automation panels and displays. Simulations are the first opportunity to test software-related UCAs, but activity in a controlled environment, such as flight testing (FT), provides the ability to successfully test STPA scenarios.

Complete evaluations of new aircraft, during inflight testing, are divided into three major areas, namely, performance, handling qualities, and airborne systems. For the evaluation of handling qualities, the aim is to extract values that represent the reaction of the aircraft to control inputs. In-flight evaluations are used to explore the ability to register the test pilot's qualitative opinion about the aircraft controllability. Flight testing can be planned to investigate complex environments, exploring rare or extreme conditions. Therefore, the following FT campaign phases are seen as opportunities for the exploration of new scenarios:

- **Cockpit evaluation:** This test is a detailed assessment, usually performed in a training environment. It is used to examine the ground activity, the night lighting, and solutions for HMI. The test pilot executes all normal and emergency procedures from the checklist, trying to identify design solutions that may be the source of mistaken actions or misinterpretations.

- **Handling Qualities:** Operational tasks are designed to evaluate the handling qualities of the new aircraft in flight. The test pilot provides qualitative observations and a score in the Cooper-Harper[21] scale. An example could be a directional control task while taxiing that results in a low score due to lack of ability to easily keep the centerline or a weapon tracking task that has poor performance due to dynamic lateral stability. In practical terms, low Cooper Harper scores mean there is an unsafe scenario that needs to be explored.

- **Airborne Systems tests:** Testing events, such as electromagnetic tests[22], are part of the certification process and provide opportunities to identify new scenarios. Some events tested in flight add environmental issues like vibration, sun glare, and load factor. These are factors that may be an important part of an STPA scenario, and may aid in the explanation of more specific mental models (e.g., the pilot lost visual contact with the leader aircraft because of reflections of sun glare inside the cockpit).

[21] The Cooper-Harper scale is the most common scale used in qualitative assessment of handling qualities. It has a score from 1 to 10 to evaluate whether the aircraft is unacceptable because it is not controllable, if it requires an improvement because a high workload is necessary to perform the task, or if it is satisfactory without improvement.
[22] Electromagnetic test is a systemic sequence of procedures that aims to verify if there is interference among all the clustered equipment in and around the cockpit.

The outcome of an FT campaign is an FT report. One of the accepted structures for reporting in Western FT organizations is the "7-part paragraph"[23]. This structure is the standard at the Empire Test Pilot's School (ETPS) and Flight Testing and Research Institute (IPEV). Each test evaluation is organized as follows:

1. Test and test conditions
2. Present the data
3. Analyze & discuss the data
4. Role relate
5. Conclude
6. Recommend
7. Specification compliance

The first field specifies the conditions in which the system was tested. Those conditions are planned by the test pilot and the FT engineer. The Active STPA could assist in this planning to choose what conditions would better explore the scenarios. When reporting, test pilots evaluate in the field 'Role Relate' how unsafe scenarios would affect operations. This is the channel that test pilots have to communicate their concerns. It is also the first opportunity for preventive thinking after experiencing a real flight with the new equipment.

Today, operational pilots do not have access to flight testing reports. The proposed solution involves the direct access for the SA running the Active STPA to what test pilots wrote in the "role relate" fields. They would then translate their reports into AHAI messages. This translation may require the participation of experts from the manufacturer and the operator. A limitation to this solution is that some tests are not a recurrent task, as qualitative testing events are usually executed only once, but this procedure would be key to integrate flight testing findings into an operational hazard analysis.

As major development programs get delayed and over budget, there is a natural management pressure to reduce testing activities to a minimum, instead of focusing on improving them. This also happens because thorough testing usually finds design flaws. Nonetheless, defenses can be elaborated upon with the Active STPA by exploring scenarios in flight testing events. These scenarios may prove the value of hazard analysis in the design phase when compared with the cost of fixing problems after fielding.

One might suggest the use of simulators to explore scenarios to spending less resources than with an FT campaign. Simulators are effective training tools to build mental models for

[23] The US Air Force Test Pilot School (USAFTPS) uses a similar version named "6-Part paragraph". The manual that specifies how to write FT reports in USAFTPS (Montes et al., 2019) explains that the aim of the FT report "should be to convey the important mission-relatable message" to support the conclusions.

normal and emergency situations. However, research in neuroergonomics (Biferno, 1985; Kramer et al., 1987) showed that there is a significant difference in electroencephalogram readings between pilots doing a flight pattern in simulators and in real flights. The stress and physiological reactions caused by noise, vibrations, and body accelerations in real flights affects cognitive and workload limitations. Findings in simulations do not represent completely the real operation, and they can mislead the assumptions on human behavior.

#### *4.2.2.2 Management of Change*

The operation of systems with many interactions among components is more hazardous during changes because the system was designed to work as a symbiotic environment. Changes to one component may have an unpredicted impact on the behavior of other components, and the scenarios generated by all possible combinations of these behaviors is too big to be re-analyzed.

Management of Change (MoC) in aviation is a formal process used for the systematic identification of hazards. MoC applies to all changes concerning safety, including the introduction of new equipment or procedures. The procedure for parallel approaches investigated in Chapter 3 is an example of a new procedure that requires a MoC. The same applies to other new procedures, such as Continuous Descent Operations (CDO) or parallel takeoffs. MoC requires a system description, a hazard identification and analysis, and a process for evaluating different ways to implement the changes. The Active STPA can be used to analyze how changes on a system affect the previous operational safety status. The structure of the Active STPA helps guide discussions among engineers, pilots, and safety experts to define how changes should be implemented. The reasoning and solutions found with Active STPA become the MoC report.

#### *4.2.2.3 Flight Data Monitoring*

Flight data recording started decades ago for accident investigation and training purposes. Airlines realized that the evolution of recording equipment could provide essential information and data became central to the aviation industry. Commercial aviation is a competitive and global market, where small changes make a significant difference when multiplied by the number of flights. The ability to manage data properly is critical, and that makes the air transportation industry a good testbed for techniques that deal with big data.

One must understand that there are many different sources of data recording in a cockpit. All information displayed to the pilots is recorded directly from the aircraft data bus[24]. The information that is not displayed, such as sensor readings, is also recorded. A major restriction to the complete understanding of incidents is that, without an official accident, the voice and video recording[25] must be deleted to guarantee that pilots are de-identified. Upon the investigation of

[24] Data bus is a physical and electrical interface that connects electronic equipment in modern aircraft
[25] The technology to do it is available but voice and video are not recorded to provide privacy to the crew.

an event, these Flight Data Monitoring (FDM) practices result in the need to detail at least one pilot's recollection of the events, which is subjective in nature.

The reference method for data collection regulated by the FAA AC 120-82 is FOQA (Flight Operational Quality Assurance). In this voluntary safety program, companies share de-identified aggregate information with FAA, that monitors national trends in aircraft operations. The objective is to apply resources to reduce or eliminate operational risks (FAA, 2004).

FOQA is used in two ways:

1. Generate statistics for internal use and to send to FAA to monitor national trends. Aggregation is the process that groups and mathematically combines individual data elements based on some criterion
2. Investigation of events triggered by parameter exceedance.

There are scientific approaches in which a multivariate cluster analysis is applied to distinguish navigation profiles that are different than the nominal ones (Das et al., 2012). However, the appropriate use of FOQA is not the identification of outliers for punishing crews for behaving differently than how a computer would do on a fully automated flight. The outliers are opportunities to investigate latent conditions to focus on understanding the causal factors and adjusting the system to the next similar mistake. Case B explained in Chapter 3 shows how a FOQA parameter exceedance, combined with a pilot report, initiated the reasoning on assumptions that resulted in new leading indicators.

#### *4.2.2.4 Operations Safety Inspections*

There are internal and external inspections on regular flights. An example of internal inspection is a scheduled flight inspection to verify if the operation is abiding by company guidelines. When an activity demands a closer look, the SA will go on an observation flight, which is a regularly scheduled flight, to observe and collect data about a specific issue. Airlines use on-flight inspections or observation flights to verify what cannot be seen using FDAP. The observer is seated[26] in the cockpit and does not interfere with the crew's routine.

Meanwhile, governmental agencies can conduct audits as major external inspections. Audits are compliance protocols performed by aviation agencies to gain a higher-level perspective. The auditor brings a list of points that are needed to verify if the company has a baseline SMS. There should be no surprises if the organization is aware, in advance, of all items on the list. One of the most used standards for audits in aviation is the IATA Operational Safety Audit (IOSA). It is internationally recognized and accepted by airlines and agencies as an evaluation system designed to assess the operational management and control systems.

[26] The long-haul aircraft have permanent seats for extra crew members and regional aircraft have a jump seat close to the door that gives access to the cockpit.

Safety Managers also plan smaller inspections, such as spot checks, walk-throughs, checklist inspections, and site surveys. Major companies often contract third-party consultants to conduct and deliver a Line Operations Safety Audit (LOSA) report. LOSA uses the Threat and Error Management (TEM) framework, referenced in the ICAO Annexes. In TEM, *threat* is defined as events that increase operational complexity, such as runway changes, deteriorating weather, or non-working NAVAIDs. The more complex, challenging, and distracting the environment, the greater is the crew's workload to manage that environment. The goal is to map undesired aircraft states (UAS), using threats to keep the operational complexity manageable.

The LOSA Report is used for risk assessment to prioritize organizational interventions. LOSA is collaborative in nature, and its archive contains data from more than sixty airlines. Companies pay for a LOSA report to have a diagnostic snapshot of their safety performance in comparison with benchmark competitors. The LOSA inspectors take a series of flights monitoring all crew actions. The outcome is a document that reports numerous observations, such as 'if the airport chart was visible for both pilots during taxi'. One of the challenges of LOSA is that the crew usually behaves at the upper end of the performance range when they are being evaluated. Thus, it fails to capture a relaxed behavior. One downfall in these inspections is that single events are unable to capture seasonal trends such as operation in icy conditions.

The relationship between LOSA and the I-SMS works both ways. First, LOSA reports are a good resource for input into the Active STPA. These reports add observations that should have been reported, but pilots were not able to identify the problem, or they were afraid of the consequences of reporting. Second, LOSA inspectors may receive leading indicators from the Active STPA when new defenses have not been effective to change the behavior on recurrent problems.

#### *4.2.2.5 CAST*

*"Many accident investigations do not go far enough. They identify the technical cause of the accident, and then connect it to a variant of "operator error." But this is seldom the entire issue. When the determinations of the causal chain are limited to the technical flaw and individual failure, typically the actions taken to prevent a similar event in the future are also limited: fix the technical problem and replace or retrain the individual responsible. Putting these corrections in place leads to another mistake – the belief that the problem is solved." (Columbia Accident Investigation Board, 2003)*

Some aircraft accidents transform aviation. Accidents are always investigated by local federal authorities. For example, in the USA, they are investigated by the NTSB, in Hong Kong by the Air Accident Investigation Authority (AIAA), and in Brazil by the Cenipa.

For the investigation of accidents, the use of recorded data allows a more conclusive explanation of the causes of an accident than testimonies and examination of aircraft wreckage. As a consequence, investigation boards spent less time identifying what has happened and more

time identifying why the accident happened. The STAMP based tool for accident analysis is Causal Analysis Based on Systems Theory (CAST), which was proved to have advantages over other systems-based techniques because it requires less training and additional resources, such as dedicated software (Mogles et al., 2018). Also, CAST can be used as a stand-alone accident analysis approach by safety experts, and it finds causal factors missed by almost all other investigation tools.

There are many benefits of using STPA and CAST together in the same system, as both are based on STAMP. When an accident happens, the analyst can easily extract from the Active STPA part of the information described in Figure 24, including hazards, the control structure, and the safety requirements and constraints.

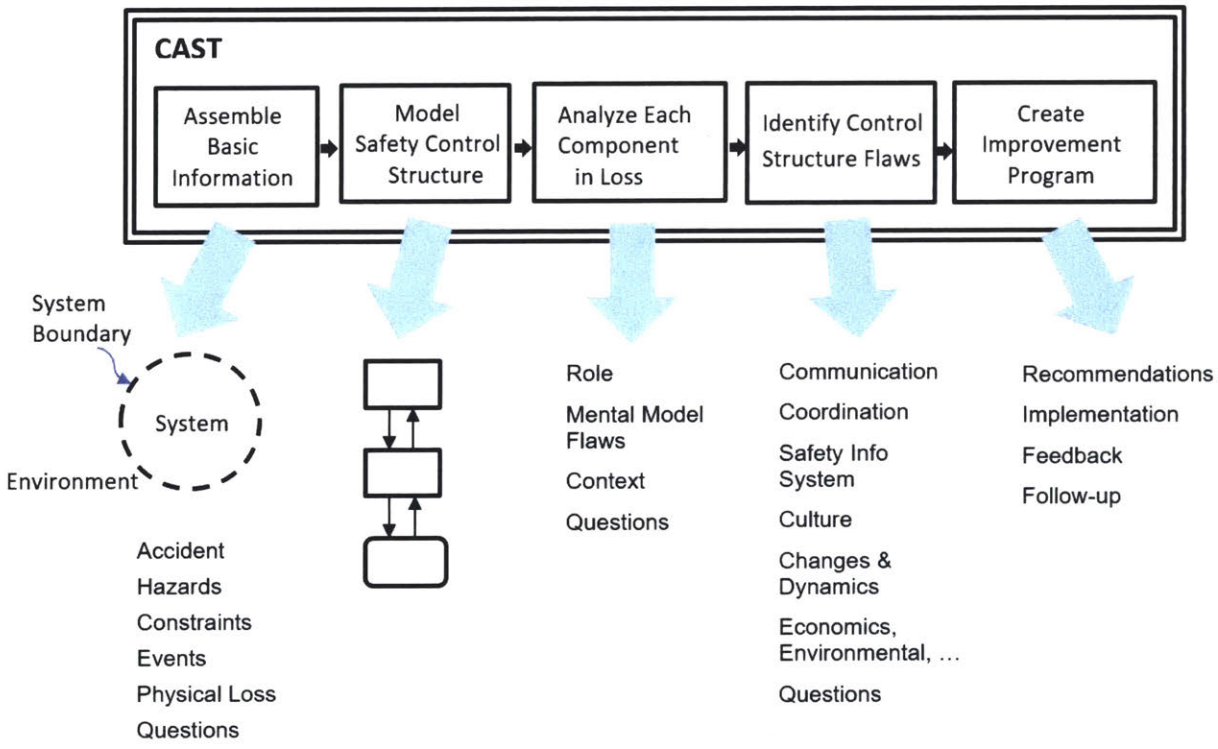



**Figure 24. Basic components of CAST (Leveson, 2019)**

Then, when the CAST is finished, the new information is used to update the Active STPA. CAST results, such as the identification of mental model flaws, new contexts, and aspects of communication and coordination are directly used to update the STPA. Additionally, the analysis of responsibilities and process model flaws in CAST may aid in the identifications of new assumptions-based leading indicators.

#### *4.2.2.6 Voluntary Occurrence Reporting*

An essential trigger for action is the voluntary report of hazardous situations written by the crew, maintenance, or ground operation personnel. Voluntary reports can be filled out by any professional in aviation. Every condition observed that could affect safety or security can be reported using specific templates. The Federal Aviation Administration (FAA) uses the Voluntary Disclosure Reporting Program (VDRP), but NASA developed the Aerospace Safety Advisory Panel (ASAP) and the Aviation Safety Reporting System (ASRS). In Brazil, CENIPA's standard form is called a Prevention Report.

Regardless of the institution, there is a protocol for Mandatory Occurrence Report (MOR) for severe occurrences. For all other situations, reporting is voluntary and can be anonymous. Usually, these reports are emailed to the safety officer or deposited in a physical box installed in hangars. The safety officer reads the reports and decides who should formally respond to it, and then disseminates it through the proper channels. This process may take days for any action to take place.

A supplement to regular reporting is the Confidential Report Program (CRP). These reports are identified, but the SA de-identifies the report before any internal communication. The main objective of CRP is to give all employees of the company an opportunity to freely express their concerns. Management must ensure employees feel encouraged to disclose safety issues using the voluntary reporting system. The system needs to be seen as non-punitive, assuming there are no clear signs of gross negligence, deliberate or willful disregard of regulations, or illegal acts. The idea behind it is to provide a dynamic communication of safety-related information among peers who share similar hierarchical positions on the system.

The wide use of FDAP changed reporting rates because pilots believe that every anomaly will be identified. If a pilot thinks someone will watch an event, he or she will use the report to explain their reasoning. Non-punitive reporting is paramount because safety information depends on the willing participation of the workforce. Thus, reporting rates are a good diagnostic of safety culture.

Safety is a shared responsibility where employees are part of the solution. It is paramount that workers from every hierarchical level feel heard and believe that their concerns are taken seriously. Top management is constantly faced with tight schedules and cost limitations. However, for critical safety operations, the top management needs to reinforce that safety has a higher priority, and act accordingly when safety needs conflict with a cost/benefit analysis. These decisions should be properly communicated to employees, so there is a clear understanding of what is expected of them.

Finally, safety data from different sources may seem to be unrelated, but when treated and analyzed to become safety information, their connection becomes clear to support data-driven decisions.

### 4.2.3 Process 2 (P2) - Active STPA

The P-2 is the Active STPA, as described and exemplified in Chapter 3. It is organized in Phases and Tasks. In Phase 2, violated assumptions are identified as leading indicators of increasing risk. This structured method avoids heuristic biases as it invites the safety managers to think about why previous assumptions were wrong. In this section, these problems are analyzed in more detail, showing how the Active STPA may help to identify useful leading indicators of increasing risk.

After running a hazard analysis, accidents may happen because:

- Poor design of the system
- Incomplete implementation of hazard analysis
- Incorrect assumptions made on the effectiveness of rules and procedures
- Changes to the operational environment invalidating previous assumptions

When a new system is fielded, the hypothesis on system and operators' behavior, and on the environment, are tested at once. The stakeholders need to know if the system operates as imagined. This is possible by checking if the controls are implemented and used as designed. Each Case of Active STPA may get to the conclusion that an existing assumption was broken. If an assumption was broken, it is a sign of a lack of expertise by the safety analysts or a piece of evidence that something is changing and the system needs to adapt.

In the first case, the analyst may have made a flawed assumption in human factors or on the construction of mental models. These assumptions may be related to the effectiveness of training or the variability of operator behavior. Additionally, the system may be much more complex than initially framed, or the environment was not well understood. In the second case, the broken assumption shows that there is a social change affecting the behavior of operators or the environment is more dynamically changing. In general, it signs to the degradation of the SMS safety culture, safety control structure, or safety communication channels. The source of invalidated assumptions may be explored to verify if they originated from ineffective controls in the original development process, from changes in the assumptions about how the system needs to operate as business needs change over time, from changes in human behavior as they optimize their work processes, or from changes in the environment (e.g., changes in ATC approach procedures or the design of the airports).

There is relevant information that can be generated with the organization of the results of running multiple Cases with Active STPA. One example of information is the determination of the quality of the rules and procedures in place. New assumptions usually lead to an update on the defenses implemented to respect the constraints. Every update is an evolution of the system, meaning that more updates to procedures are a sign of less maturity of the procedures or more dynamic changes in operations. If the changes are not restricted to defenses and affect the original set of control actions or the control structure, the changes are a sign of system

degradation, which requires a broader adaptation. Inconsistencies between the model of the process used by the controller and the actual process state lead the controller to provide inadequate control, resulting in accidents. Performance metrics and leading indicators of potentially unsafe changes in the safety control structure are a form of feedback that can provide a means for measuring the risk in the current state of the process and the safety control structure. They provide important signals about the potential for an accident (Leveson, EAGER Proposal, 2018).

Some Cases are cognitively harder than others for understanding the causal factors and on the decision for appropriate defenses. The main reasons for the repetition of violations to reasonable assumption are:

- The communication channels are not effective for all operators
- The enforcement of the constraints is not adequate
- The judgment on whether the procedure is reasonable is incorrect
- There are no resources to implement the solutions
- The identified solutions were not yet implemented

If the analysis of the new Case finds that the causal factor is a repetition of a previous Active STPA Case, the SA must verify whether the solution of the previous one was implemented or not. If it was implemented, the defense was ineffective to avoid a new event. The reasons may include new procedures that are infeasible in some circumstances or a lack of adherence to a reasonable new procedure. On the other hand, if the new defense was never implemented, the SA must verify what was the restriction. If it was lack of time, the Case becomes an argument to request more people working in the safety team. If it was lack of resources, the SA runs a cost/benefit analysis to promote the implementation of the new defense. In both cases, the repetition of events with the same causal factors points to a lack of management commitment to safety, as the main barriers to implement new defenses are the lack of available resources, schedule pressure, and insufficient personnel. The cause for the lack of commitment may be a flawed perception of the relative importance of each defense or the impact of competitive or financial pressures affecting high-level management decisions.

Another aspect of safety management that may be evaluated is the strength of the safety culture of the organization. When a company develops a safety culture, everyone shares the knowledge of the hazards and the risks that the activity implies. Safety culture becomes a product of behavioral and psychological aspects, such as values, attitudes, and competencies that determine the commitment to aviation safety health. One example of a sign that rules are getting challenged because there is a lack of harmony between the operation and the organization values, are deliberate violations of reasonable written procedures without any specific justification. The violations may be a sign of complacency, which triggers the enforcement of the constraints with more intense Safety Promotion activities. It may also be a sign of malicious actions, when there

is an intentional attack on system defenses. This diagnostic requires the orientation of the operators, the construction of new defenses to reduce the vulnerabilities of the system, or even the application of disciplinary actions.

When an unintended violation of a reasonable procedure is identified, the SA must investigate if training is insufficient or if the operator is not valuing safety. In some cases, doubts on responsibilities result in mistakes in which the operator believed his or her actions were correct. If the investigation does not provide a clear answer, the SA should act on both problems, improving training to respond to the scenario and reinforcing the current defenses.

Additionally, the last task on Phase 2 in Active STPA is the design of contingency protections for the situations in which the assumptions fail. In every event in which an assumption is violated, it is possible to evaluate if the protections worked. The system's vulnerability to accidents depends on the robustness of contingency protections. Thus, failed protections are events that require thorough reasoning and an effective fix. For instance, the data from the airlines included a description of CRM breakdown, when tough discussions between crew members interfered on call outs and affected decision making. This fact reminds that not everyone has high maturity and skills, which makes it more difficult for the analyst to design proper protection. Breakdown situations are hard to prevent because it is difficult to build scenarios for them, but their consequences can be relevant. The best approach to crew heated discussions is to implement a defense that obligates them to postpone any personal issues they might have to solve until after landing, especially when there is a significant hierarchical difference between them.

Finally, in a comprehensive and detailed analysis, the database may grow, and the individual leading indicators will have some overlap. The SA must reason on how to reduce the total number of indicators to be able to continue managing them all.

### 4.2.4 Process 3 (P3) - Prevention and Mitigation

The I-SMS model (Figure 25) shows arrows coming from Phase 3 to the Prevention and Mitigation process. This process was organized separately because it has interactions with other SMS practices, including communication channels already in use.

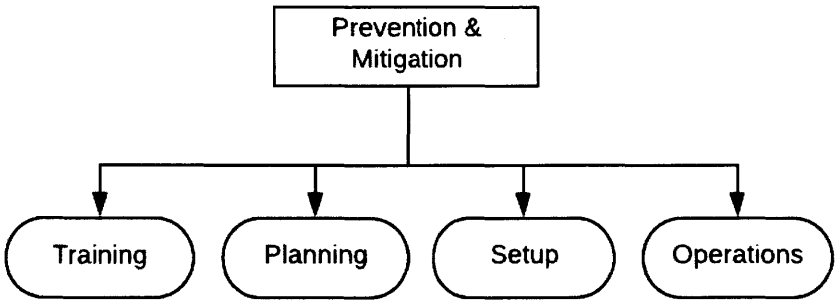



**Figure 25. Safety communication channels**

The proposed reinforcement of safety information shown in the I-SMS aviation framework is needed because aviation initial training may be not enough. In training, simulators are widely used to construct mental models and to indicate when judgment is required. When the training is completed, the responsibility is then assumed to be transferred to the pilots. However, this method is flawed because providing all knowledge necessary for safe operation in a single training period is not effective for crews to behave as desired. If an accident occurs, it is wrong to attribute blame to a pilot because he or she had one training session on that specific subject. Nonetheless, this management approach is common because reputation is critical in aviation organizations. Ideally, the transfer of safety information must consider operator memory limitations to implement reminders using all four opportunities described in the I-SMS framework.

In aviation, there are two main types of training. In the initial training, students receive fundamental information. The flight courses manuals explain all the reasoning behind the rules. Then, an initial series of simulator training complete the construction of mental models. Later, during operations, pilots return to periodic simulator training sessions. This training is necessary for two reasons: pilots must recall emergency procedures memorized in basic training (most of which they never had to use), and the protocols for safe operation are enforced to undo bad habits and to detect mental model flaws.

After training, the next opportunity to communicate safety issues is to use established channels and protocols. At Air Hong Kong for instance, before the flight, pilots are expected to open an app, click on a link called Flight Operations Notices (FON), previously called Notice to Crew, read its contents, and acknowledge that they received the information. These messages are used as an augmentation to training.

Another channel to send information is the Notice to Airmen (NOTAM). There are two types of NOTAMs; the general one emitted by the aviation authority and the company-specific NOTAM. The general NOTAM is organized by airports and airspaces, with open access. For long flights, a complete set of NOTAM has several pages of coded information. Thus, the

company filters the data according to the navigation plan and sends the crew only the essential information about the airspace, the origin, destination, and alternate airports. Companies take advantage of the NOTAM channel to inform their crews about safety issues that are important for specific flights, such as special weather forecast or unusual flight operations taking place in the area.

Both types of NOTAMs are delivered to the crew in a documentation folder prior to each flight. Missing content and careless reading of NOTAMs may be catastrophic. In 2014, during the battle of Shakhtarsk in Ukraine, a coded NOTAM added coordinates of a new restricted airspace. Most companies changed their flight plans and explained the hazard to the pilots flying over the war region, but a Boeing 777 from Malaysia Airlines kept the original navigation plan and was shot down by artillery.

Similar communication is necessary after volcanic eruptions. When volcanic ash is carried by the wind, it often affects a significantly large section of airspace. This information may be necessary to communicate during the flight. For those cases, there is a system called Aircraft Communications, Addressing and Reporting System (ACARS) that uses datalink to send messages via Very High Frequency (VHF). Every modern airliner has the proper equipment to receive coded ACARS messages, along with the ability to print them onboard. This method is used when management needs to address the crew of a single flight, e.g., about a change affecting the crew of the following flights. The crew is trained to acknowledge every message after reading.

Another system already in use is a continuous broadcast of recorded aeronautical information called Automatic Terminal Information Service (ATIS). All pilots are expected to listen to an airport ATIS before requesting to start the engines and before the starting point of approach procedures. It is a coded message with a sequence of important information, such as the runway in use, weather information, and exceptional limitations. The last part of the message is reserved for safety information.

The multiple sources of available safety information help to prepare pilots to make quick decisions or to communicate their planning in formal briefings. The flight briefing is usually a meeting with the whole crew to explain peculiarities of the flight. The takeoff and the approach briefings are used to discuss procedures for each airport. This includes flight restrictions, such as altitude constraints, as well as procedures for critical emergencies, like engine flameout during takeoff.

Finally, the last chance to communicate safety issues is embedded in aircraft design. When a critical moment is coming, and the risk is increasing, the operator must have a complete situation awareness. Final approaches for landing are an example of a dynamic sequence of events in which design solutions, such as visual cues, aural warnings, and haptic feedback, are combined with voice CRM callouts, and written procedures. The usefulness of Active STPA is extended to elaborate trends. In one specific phase of the flight, if the Active STPA registers a

significant amount of reports showing a clear a trend on the lack of situation awareness, the solution might be a design change to include new alerts and warning cues for pilots.

## 4.4 Using I-SMS in the aviation industry

The data analyzed in this research helped to elaborate the Active STPA structure and to evaluate its results. The partners provided flight monitoring data, pilot reports, observation flight reports, as well as investigation reports on unstable approaches for landing. To avoid the correlation of companies with incidents, all data was condensed in one single database and analyzed altogether. Partners sent over 1,600 reports, both voluntary and mandatory, protected by non-disclosure agreements (NDA). Filtering this data to our scope on unstable approaches for landing, the number of reports was reduced to 155. Among the analyzed events, Cases in which FDM data was also available, including the three Cases presented in Chapter 3, were given more emphasis. The analysis of those Cases found missing scenarios in our original STPA, and inadequate procedures that we have designed to enforce the constraints.

### 4.4.1 Refining assumptions

One of the Cases analyzed was an event in which the PF pressed the Auto-Throttle engage/disengage switch of a Boeing 777 when he intended to press the TO/GA button to initiate a missed approach procedure. The pilot flying perceived that the aircraft did not respond with the expected increase in pitch and heard the aural message of Auto-Throttle disconnection. The pilot immediately realized what was the mistake and executed the missed approach maneuver manually pitching up and accelerating the engines to maximum power. In this event, there was no loss, but this scenario could have led to a situation in which:

- The pilot does not pitch up when it is necessary to Go Around, as the crew believes the autopilot is engaged and will do it.
- The pilot pitches up and the aircraft stalls because the pilot did not accelerate the engine, because the PF assumed the Auto-Throttle was engaged, as it was a few seconds prior.

The TO/GA switches, one for each engine, are located in the throttle pedestal in most aircraft. In modern aircraft, when a TO/GA switch is pressed, the computer calculates the desired attitude for a missed approach procedure, and the autopilot follows the navigation guidance.

Phase 1 of the Active STPA found the following crew control action from the STPA:

- Controller: Crew
- Controlled Process: Autopilot
- Control Action: Press Takeoff/Go Around (TO/GA) switch

This control action already had the list of UCAs organized in Table 17.

**Table 17. STPA Step 3 – Examples of UCAs**

| Unsafe Control Actions | | | |
|---|---|---|---|
| **Provided leads to Hazard** | **Not Provided causes Hazard** | **Provided too early, too soon or out of order** | **Provided for too long or stopped too soon** |
| Pressing TO/GA switch after touchdown, when it is inhibited. (H-5) | Not pressing TO/GA when the approach is unstable (H-1, H-5) | Pressing TO/GA after raising the nose, when the speed is too low [H-3] | N/A |

The UCA that relates to the incident is the following (Figure 26):

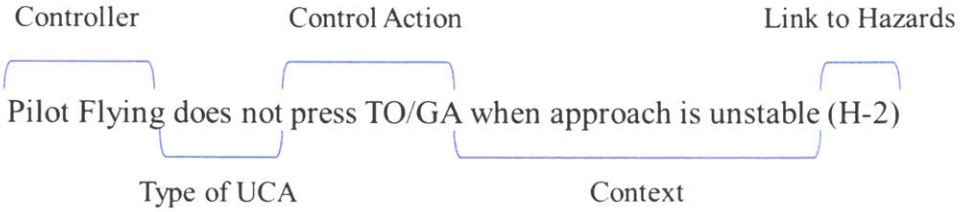



**Figure 26. Unsafe Control Action identified in the STPA for the TO/GA event**

For each of the UCAs found in step 3, there were scenarios in the analysis on unstable approaches that included component failures, process model flaws, lack of information on feedback, absence of feedback, incomplete requirements, lack of requirements, and design errors. The outcome of step 4 was a list of lower-level requirements and constraints derived from those scenarios. Table 18 shows an example of the scenario and constraint that relates to the event.

**Table 18. Standard STPA Step 4 – Scenario and Constraint**

| Scenario | Constraint |
|---|---|
| PF (Pilot Flying) decides to Go Around and, by mistake, presses the Auto Throttle (A/T) disengagement button instead of the TO/GA switches because pilots are fatigued | The crew must press TO/GA when the approach is unstable |

This constraint was used to write a rule and Table 19 identifies an assumption made when the rule was created. This assumption was not previously documented. However, Active STPA identifies its violation as a leading indicator of increasing risk.

**Table 19. Assumption made in STPA**

| Defenses | Assumption |
|---|---|
| Pilots must perform five missed approach procedures during simulator training every year<br><br>Provide resting time to the crew according to dedicated regulation | This mistake is unlikely to happen because the format of A/T disconnect button is very different from the TO/GA switches and they are far from each other |

The reasoning on causal factors in Phase 2 prompted an investigation to determine if the assumption was correct. This event took place in a Boeing 777, in which the TO/GA and the A/T switches are positioned as pictured in Figure 27.

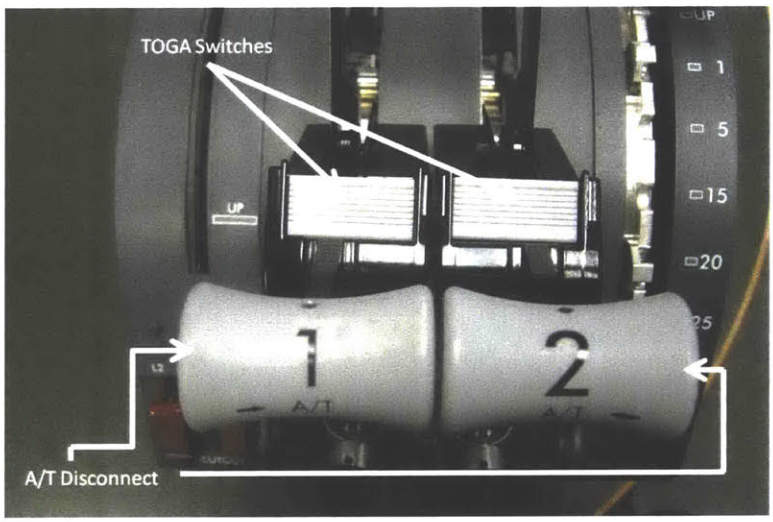



**Figure 27. Throttle pedestal in Boeing 777**

The majority of pilots that transition to the Boeing 777 come from older wide-body models, such as the Boeing 767, or smaller aircraft, such as the Boeing 737. In the Boeing 767, the TO/GA switches are spring-loaded and have a very different logic, in which releasing the throttle levers automatically initiates the TO/GA. In Airbus aircraft, the switches are in a position that is similar to the Boeing 767, but the logic is the opposite (press to engage), which would not explain the confusion. Also, in Airbus, the A/T disconnect switch is in the same position as the Boeing 777. The Boeing 737 switches have a different format but are also located in the same position as the Boeing 777. However, in several commuter aircraft, the TO/GA switch is located as pictured in Figure 28.

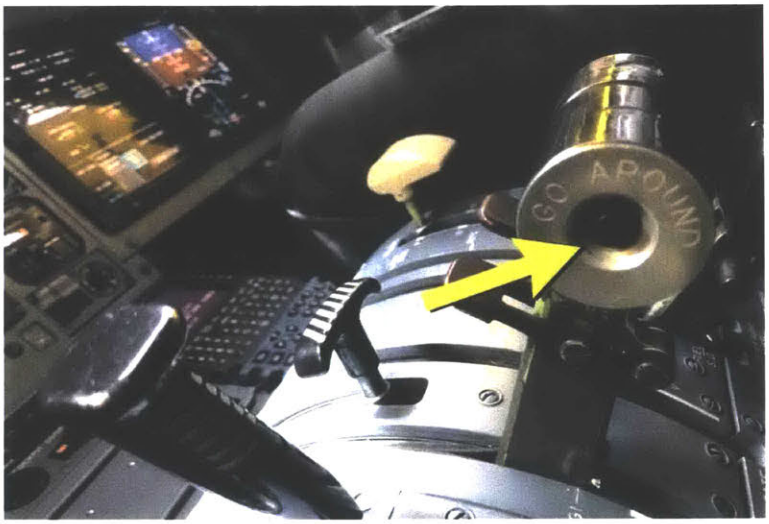



**Figure 28. Throttle pedestal in commuter aircraft**

The differences in the position of the controls in the Airbus, Boeing 737 or 767 could justify *not pressing the GA button when required* as a common human error, but would not explain why a pilot would press the Auto Throttle disengage button by mistake. However, in commuter aircraft, the simpler design of the throttle levers has the TO/GA buttons in the same position as the A/T buttons of the Boeing 777. It is logical to install the GA buttons in that position because it is ergonomic, and most commuter aircraft do not have an Auto-Throttle system.

Commuter aircraft are usually the first aircraft pilots fly early in their careers. Each aircraft is thoroughly studied by pilots when they are constructing mental models during flight training. This phase in a pilot's education also introduces highly complex simulator training. During simulator training, the crew performs normal and abnormal procedures many times per session. The instructors are tasked with creating scenarios for the students, including unexpected failures and unusual situations, which force them to stay alert and develop initiative.

Comparatively, when pilots start to fly commuter aircraft, the lack of flight experience mixed with complex airport environments leads to more frequent missed approaches. Meanwhile, an experienced Boeing 777 pilot may rarely perform a missed approach. This leads us to reason that human error, captured in this incident, should be considered a normal mistake made as a result of negative learning, i.e., pilots without experience in commuter aircraft adapt faster to the new system than the pilots who received training in commuter aircraft. With this information, the safety manager can advise instructors to enforce the construction of the correct mental models for missed approach procedures.

In this Case, Phase 1 found:

- An inadequate STPA element: the rationale described in the scenario using fatigue as a causal factor was incomplete
- An assumption on the unlikeliness of the mistake was wrong

Note that what changed in the scenario (Table 20) was the explanation for the behavior because the context of the UCA still the same. Also, the constraint was correct and did not need to be updated. In Phase 2, The SA identifies the violated assumptions as a leading indicator of increasing risk, and consequently, designs new defenses to enforce the same constraint. The STPA scenario is updated in Phase 3, creating a new responsibility for flight instructors.

**Table 20. Revised analysis after Active STPA**

| Assumption | Defenses |
|---|---|
| Pressing A/T buttons instead of TO/GA switches is a common mistake in pilots with high time in commuter aircraft for pilots transitioning to the B777. This mistake can be mitigated with training and close monitoring during normal operations. | Include eight missed approaches during simulator training per year, and exploring sudden needs for missed approaches<br><br>Add a Note on manual alerting to this transitional mistake<br><br>Alert flight instructors to verify if pilots are showing signs of confusion upon pressing TO/GA switches |

| Scenario | Constraint |
|---|---|
| PF (Pilot Flying) decides to Go Around and, by mistake, presses the A/T disengagement button instead of the TO/GA switch **because this button in B777 is at the same position as the TO/GA button in the PF previous operational aircraft** | The crew must press TO/GA when the approach is unstable |

The original STPA performed on a fielded system had already pointed to deficiencies of system operations and delivered the constraints under which defenses were written. However, the situation identified by the incident was not previously considered and the scenario was updated as a Case of the Active STPA to better reflect the real problem.

### 4.4.2 Leading Indicators

To address the need to move from a reactive to proactive safety culture, this research proposes the use of assumption-based leading indicators, generated with Active STPA as a tool to achieve the Safety Objectives of aeronautical organizations. This process provides a structured reasoning to use the violation of previous assumptions as leading indicators of increasing risk. If new incidents violate assumptions repeatedly, the SA must investigate why the solution was not useful or effective. The causes of the inability to fix the problem in the first opportunity may be a consequence of the natural complexity of the system or a sign of the need for more experts working in the safety team. The identification of flaws in the SMS provided by these proactive indicators allows, in the long-term, an enhancement towards more robust procedures for operations, feedback on enforcement mechanisms for system defenses, and information to assist top-management decision making.

The Active STPA represents an improvement to current methods as it provides guidance to analyze systems phenomena using a hazard analysis at the operational level. This technique may become an integral part of the risk management practice, as it provides information for decision-makers on how to address risk, complementing and eventually substituting current practices that monitor parameter exceedances for risk assessment, used by aviation as Safety Performance Indicators, which is explained in the following sections.

### 4.4.3 ICAO SMS

The International Civil Aviation Organization (ICAO) is a United Nations specialized agency that, in 1944, was established by States to manage the administration and governance of the Chicago Convention on international civil aviation. Today, ICAO coordinates the work of industry groups and 193 Member States to reach consensus in Standards and Recommended Practices (SARPs) and policies. ICAO's goal is to promote and ensure that local civil aviation operations conform to those regulations to facilitate the operation of aviation's global network (ICAO, 2019).

Safety Management System (SMS) in aviation is defined as a systematic approach to manage safety, including the necessary organizational structures, accountability, responsibilities, policies, and procedures (FAA, 2019). As described in Chapter 1, the ICAO SMS is a recent initiative to improve safety, and all aviation organizations will have to comply with SMS standards by November 2019.

These standards are the Annex 19 (obligatory) and the Safety Management Manual (SMM). Published in 2013, SMM is a recommendation on how to conform with the Annex 19 requirements. Each country produced similar SMS standards associated with their version of requirements. The FAA's Aviation Safety Organization published in 2015 the 14 Code of Federal Regulations (CFR). 14 CFR Part 5 specifies the applicability and implementation of the new SMS framework for aircraft operators certificated under Part 121 (commercial air carriers).

Similar to the ICAO SMM, the reference document used for the implementation of SMS in FAA is the AC-120-92B Safety Management Systems for Aviation Service Providers.

The implementation of an SMS in an organization requires management commitment, compliance with all previous methods, and a commitment to maintain and continuously improve the overall effectiveness of the SMS. Service providers are expected to show compliance by delivering a series of documents, starting with a system description and an organized list of processes, activities, and interfaces, both internal among divisions of the company, and external entities and authorities.

Appendix 2 of Annex 19 (2013) lists responsibilities for the airlines, determining that "the service provider shall develop and maintain a process to identify hazards associated with its aviation products or services.". It explains that "hazard identification shall be based on a combination of reactive and proactive methods," and requires that "the service provider shall develop and maintain a process that ensures analysis, assessment, and control of the safety risks associated with identified hazards" under the item "safety risk assessment and mitigation."

### 4.4.4 Aviation Safety Performance Indicators

Every industry treats indicators differently. This section explores modern aviation standards for safety performance indicators. Appendix 2 of the ICAO Annex 19 treats the framework for an SMS. The following definitions are presented in Chapter 1 of the same Annex.

- ***Safety performance:*** *A State or a service provider's safety achievement as defined by its safety performance targets and safety performance indicators.*

- ***Safety performance indicator (SPI)****: A data-based parameter used for monitoring and assessing safety performance.*

- ***Safety performance target (SPT)****: The State or service provider's planned or intended target for a safety performance indicator over a given period that aligns with the safety objectives.*

The ICAO solution for Safety Assurance (Component 3 of SMS) is monitoring and measuring safety performance with indicators, as determined by the following paragraphs from ICAO Annex 19:

- *The service provider shall develop and maintain the means to verify the safety performance of the organization and to validate the effectiveness of safety risk controls. (item 3.1.1)*

- *The service provider's safety performance shall be verified in reference to the safety performance indicators and safety performance targets of the SMS in support of the organization's safety objectives. (item 3.1.2)*

In SMS, Safety Objectives are high-level statements of desired performance outcomes or safety achievements that the organization aims to meet within a specified period of time. Thus, SPTs are characterized as small steps to reach the Safety Objectives (Figure 29). In fact, SPTs formalize what the organization considers to be a reasonable Acceptable Level of Safety Performance (ALoSP) for that period. Targets have a particular impact on Safety Culture as short-period performance challenges, eventually followed by a reward system, are especially attractive to employees. Although achieving an SPT is not an indication that safety management has improved. A poor choice of targets or unmapped changes in the system could mask a poor safety practice if the SPT results are not accompanied by an analysis that takes into account the overall view. For instance, if the SPT is defined as *less than five unstable approaches per month due to the horizontal path*, the pilot would stress about meeting the target, stealing attention from other checks. For example, trying to be precise on the interception of the localizer, the pilot could forget a checklist item or a CRM callout. The performance could be seen as improved because the SPTs on unstable approaches were met. The numbers would say that the system is operating safer because there are no SPTs on birds strikes, as it is considered to be an unfortunate event, and not as a consequence of crews looking less to the outside.

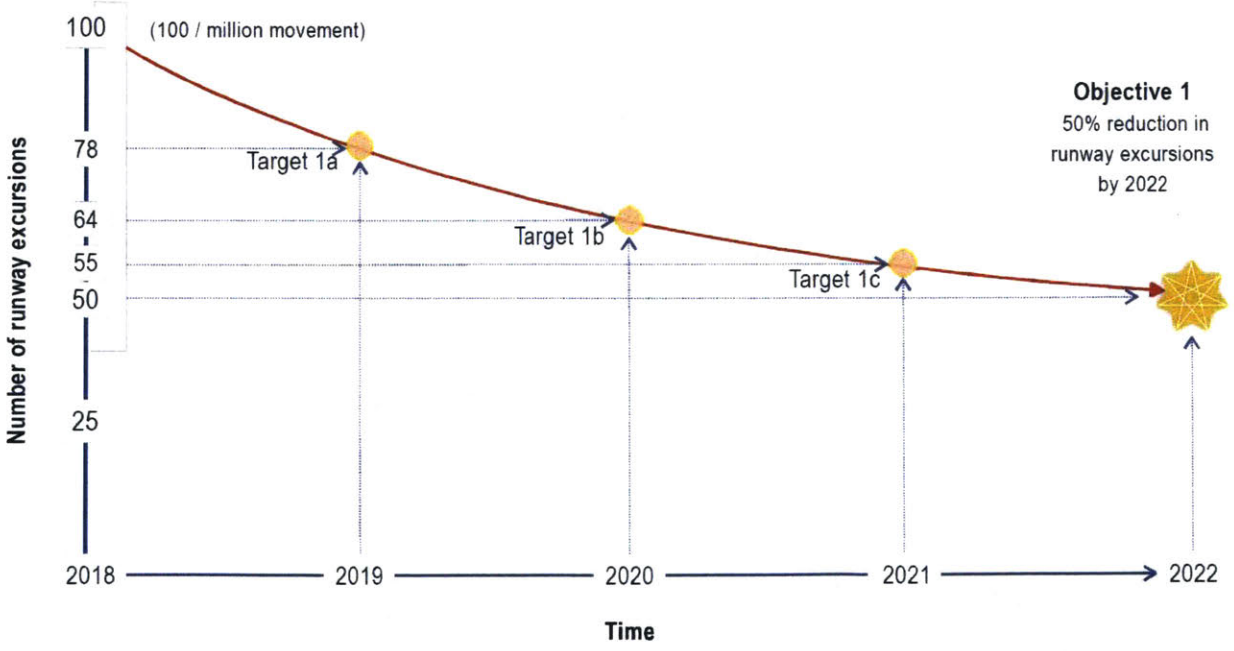



**Figure 29. Safety Performance Targets (SPTs) representation in comparison with Safety Objectives (FAA, 2019)**

To achieve the SPTs, the SMS Manual (Doc 9859) provides guidance on how to set these SPIs as a solution to evaluate trends with SMS. All partners of this study use this terminology to define criteria to measure trends in safety. According to their manuals, to be useful, an SPI needs to be reliable, representative of all relevant aspects, resistant to bias and manipulation, and cost-effective. Common examples of SPI adopted by aviation organizations and currently in practice are presented in Table 21. Most current SPIs check for parameter exceedances of the available flight data monitoring. Every new quantitative SPI has a trigger and a target (SPT) with levels of tolerance and acceptability. The SA needs to adjust these thresholds to avoid an excessive number of false alarms while efficiently monitoring for significant changes.

**Table 21. Examples of SPIs, triggers, and SPTs from Partners**

| **SPI (number per year)** | **Acceptable (SPT)** | **Tolerable (alert level)** | **Not acceptable** |
|---|---|---|---|
| Unstable Approaches | <120 | 120-180 | >180 |
| Voluntary Reports | <100 | 100-130 | >130 |
| Airworthiness Directives Irregularities | <8 | 8-12 | >12 |

Note that the way the limits on the right are set, it motivates the system to report less or to point to fewer irregularities. If Safety Promotion initiatives are more active, for instance, and operators become in general more aware of risks and potential hazards, they will report more, and the SPI trend will wrongfully be evaluated as a sign that risk has increased.

The following Table 22 shows the current parameters of an unstable approach used by one of the partners of this study[27]. This company provided a complete list of their monitored SPIs and triggers.

[27] The access to flight data with partner airlines was granted by signing a non-disclosure agreement with the company and the Union of the pilots. For this reason, all safety data in this research with a possible negative implication is de-identified.

**Table 22. Examples of SPIs currently collected by a partner**

| SPI | Trigger |
|---|---|
| Approach speed high - between 500 ft and 50 ft | CAS ≥ Vref + 30 kts for at least 2 sec |
| Approach speed low - between 2500 ft and 1000 ft | CAS ≤ Vapp Target - 5 kts for at least 2 sec |
| Excessive bank angle - between 100 ft and 500 ft | Bank angle ≥ 30 deg |
| High rate of descent - below 400 ft | ROD ≥ 1000 ft/min for at least 1 sec |
| Go-around | Go-around initiated below 200 ft AGL |
| Go-around after a touchdown | Touchdown and Go-around |
| Glideslope | Warning triggered for at least 1 sec |
| Late landing gear | Gears down and locked below 1000 ft AAL |
| TCAS RA | Warning triggered for at least 3 sec |
| Deviation below glideslope | 1-dot below glideslope for at least 2 sec between 1000 ft AGL and 150 ft AGL |
| Deviation above glideslope | 1-dot above glideslope for at least 2 sec between 1,000 ft AGL and 150 ft AGL |
| Deviation left of localizer | 1 dot left of localizer for at least 2 sec between 1,000 ft AGL and 150 ft AGL |

This company is currently monitoring 128 SPIs, and 67 of them are related to approaches for landing. All monitored SPIs are FDM parameter exceedances, meaning that the company uses dedicated software showing all the events in which one of the listed parameters exceeded their pre-defined limits. Table 23 shows data from the same partner with a normalized number of exceedances organized by phase of flight. The last line is a combination of the approach, landing, and missed approaches. These phases of flight consistently have more parameter exceedances then takeoff, climb, cruise, or decent, combined.

**Table 23. Number of events per one-thousand flights**

| Total Events in each phase of Flights (Rate/1000) | | | |
|---|---|---|---|
| **Phase of flight** | **Current Period** | **Previous Period** | **One Year Before** |
| **TakeOff to 5000'** | 4.99 | 7.87 | 9.24 |
| **Climb** | 0.00 | 0.00 | 0.00 |
| **Cruise** | 3.75 | 5.25 | 12.70 |
| **Descent to 5000'** | 0.00 | 0.00 | 0.00 |
| **App/Land/Mapp** | 28.71 | 32.81 | 35.80 |

From the analysis of quantitative SPIs, trends are elaborated using graphic exceedances per a certain period of time. The current practice of the companies in terms of SPIs for approaches is to produce normalized graphics showing trends (Figure 30) of each parameter over time to provide a visualization of safety performance to the top management of the company.

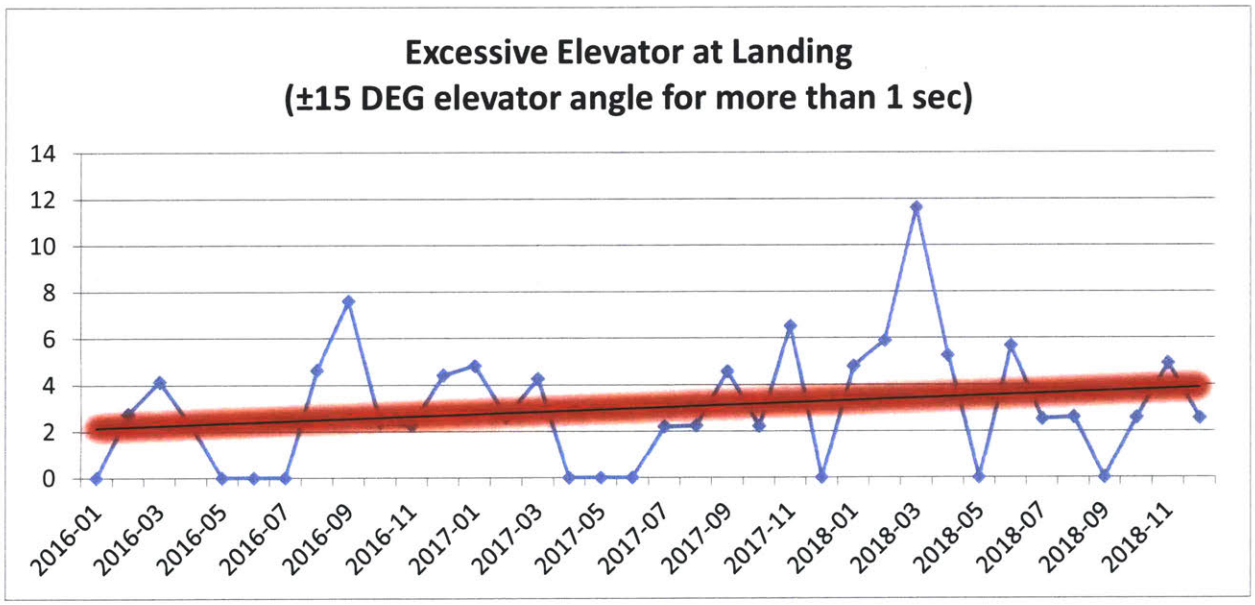



**Figure 30. Trend of an SPI on descent rate (Source AHK)**

In relatively small airlines, the number of exceedances is low. Linear regression on trends does not tell reliably if the operation is getting safer or more hazardous. One solution in place to compare the results with the desired SPTs is using a combination of several quantitative SPIs to get a sense of the total risk of the operation, as pictured in Figure 31.

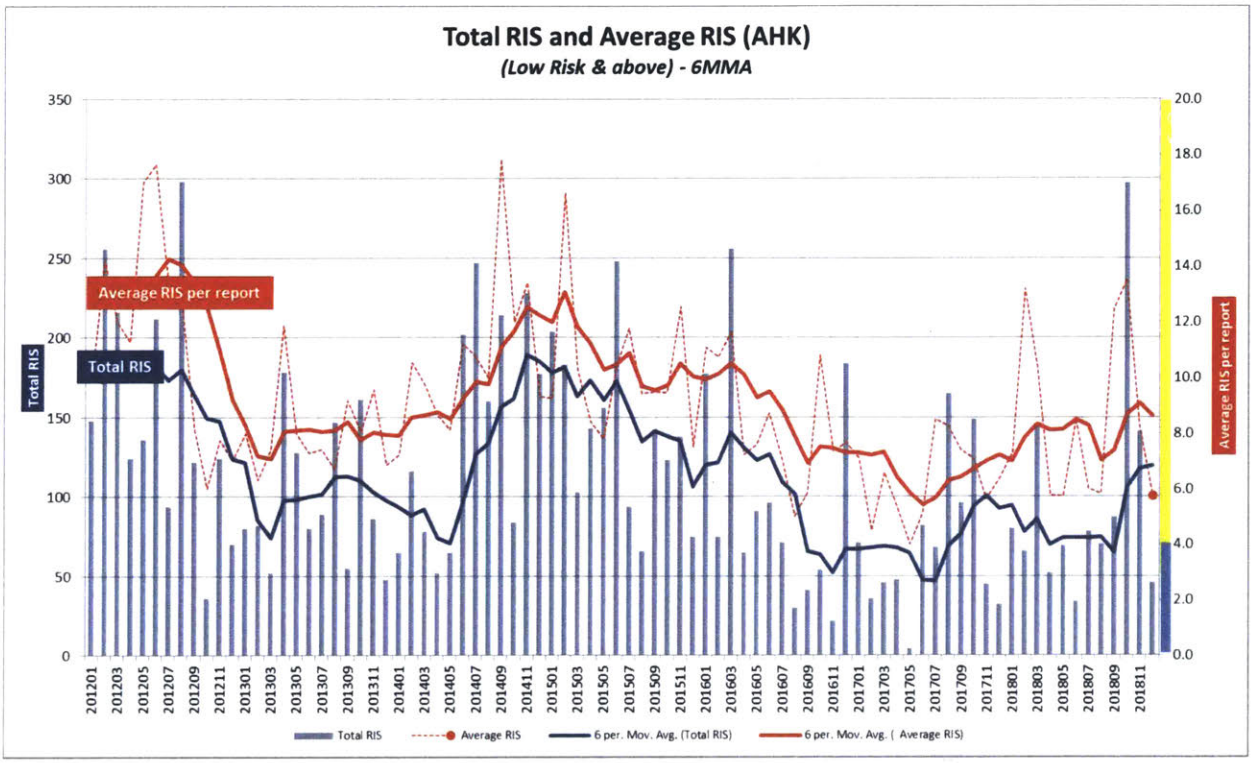



**Figure 31. Combination of trends (undisclosed partner airline, 2019)**

Although for management purposes, the graphic representation may make sense because it shows the total number of exceedances, the summation of different SPIs masks the reasons behind the exceedances. This visual result hides the interactions between different parameters. For instance, if ATC at a specific location has a new procedure to accommodate more landings per hour, a higher number of speed exceedances might be expected. It is unclear though if this will lead to a higher number of localizer overshoots[28]. If top-management is more concerned with learning precisely how the company is doing compared with competitors in general metrics, it may be a satisfactory information. However, to act on causal factors to improve safety, the use of leading SPIs becomes necessary.

Qualitative indicators, i.e. the ones that inform how a behavior is different than assumed, can be combined to give a better explanation of the observed symptoms. For example, consider that an SPI signaled someone's lack of attention to an important activity. Isolated, this SPI could be interpreted as a high workload on shared-attention activities. However, combined with other SPIs, it could lead to the identification of a symptom of stress or depression.

[28] Localizer overshoots occurs when the aircraft starts to turn too late and crosses the runway alignment. The LOC indicator measures the angular deviation from the runway alignment in standard dots.

### 4.4.5 Comparison between Active STPA and ICAO SMS

Data collection and the use of indicators are key to informed decision-making. ICAO defines data collection as Safety Data Collection and Processing Systems (SDCPS). The SPIs are combined with safety triggers as tools to verify if the organization is making progress towards their safety objectives and Safety Performance Targets. Figure 32 shows the flow of safety data presented in the SMM from the SDCPS to Safety Promotion.

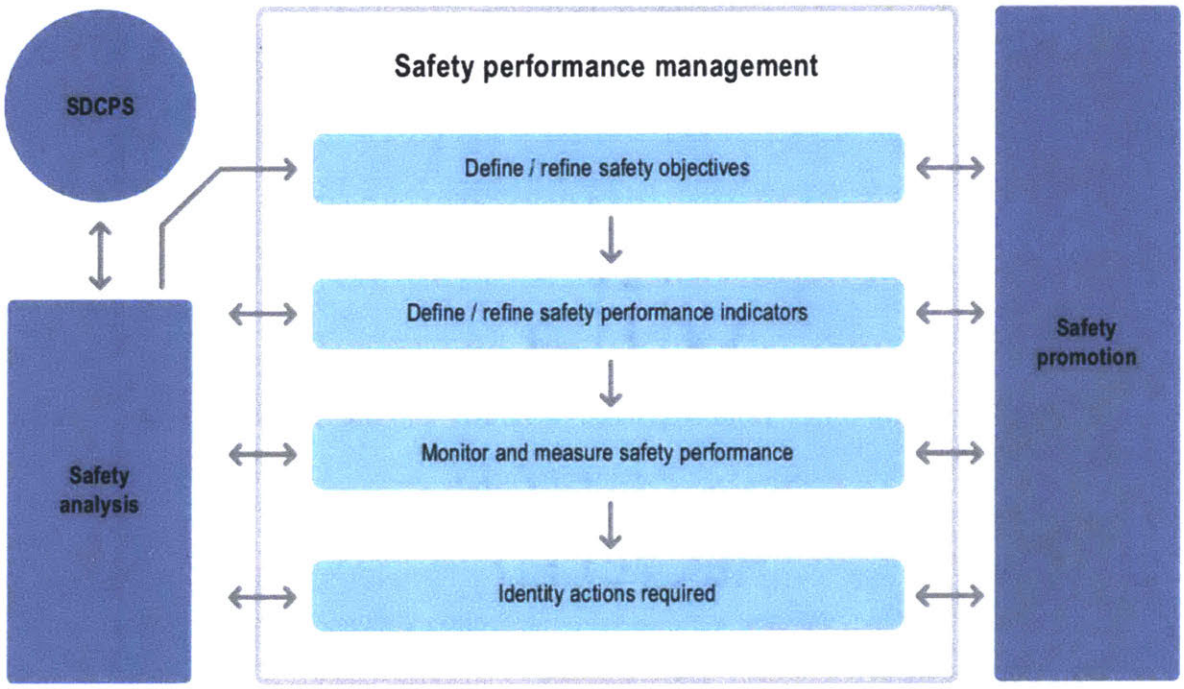



**Figure 32. SMS information flow in SMM (ICAO, 2018)**

The SMS stresses communication to all personnel about the expected behaviors concerning procedures. The organization is also required to explain their discipline actions in response to unacceptable individual behaviors. From the STPA, it is also possible to explain the expected behavior using the operator's responsibilities from the analysis. The SA may communicate those responsibilities to explain the expected behavior and derive the unacceptable behaviors straight from the UCAs.

The definition of system boundaries and the organization of a higher-level functional control structure are requirements of the ICAO SMS to provide a clear organization of internal and external interfaces. Similarly, the safety control structure generated by the STPA explains how the controls are implemented and the desired feedback. It also shows, in the control structure, what kind of controls the higher-level controllers use. These responsibilities become the starting point for the creation of a process similar to the activities required by the aviation

SMS. The comparison between the current organizational structure, and what would be an ideal one, shows the gap in which management needs to apply resources.

The next stage in SMS is to run a hazard identification. The SMM defines hazards as "a dormant potential for harm that may assume different forms as a natural condition or a technical status." The manual divides the hazard identification methodologies in reactive and proactive. Reactive methods include the investigation of past safety occurrences while the proactive ones involve collecting data to act on future performance. These are typically events with a lower consequence, to assess the performance of the system in terms of frequency of occurrence. The problem is there is no guidance on how to make proactive identification of hazards. The broad list of possible causal factors, such as human-machine interface factors, makes it difficult to list hazards without a process.

As SMS becomes the standard for safety, regulators try to harmonize their efforts in collaboration on topics of common interest. This sharing of lessons learned is essential to the progression of the SMS. In one of the SMS initiatives, ICAO and civil aviation authorities worldwide formed a Safety Management International Collaboration Group (SM ICG) to promote a "common understanding of safety management principles and requirements, facilitating their application across the international aviation community" (EASA, 2010a). The SM ICG Standardization workgroup developed the hazard taxonomy (SM ICG Hazard Taxonomy WG). This taxonomy is part of a process that includes the merger of data collected from all operators (EASA, 2010b). The following high-level categories represent the areas in which a hazard may occur:

- Environmental
- Technical
  - Aerodrome
  - Air Navigation
  - Operations
  - Maintenance
  - Design and Manufacture
- Economic
- Organizational
- Human – Limitation of the human which in the system has the potential for causing harm
  - Medical condition
  - Handicap
  - Psychology of person

If the agency running an audit to examine the SMS requires the use of this taxonomy, the SA of an organization using the Active STPA may easily organize the events using the identification of causal factors in Active STPA from the Phase 2. Otherwise, if the audits are not rigid in terms of methods to perform hazards identification, the classification of hazards may come directly from the step 1 of the STPA, where losses and hazards are listed, refined, and

related. The safety information running in Active STPA, however, may work for the ICAO hazard identification methodology.

SMS requires a safety risk assessment. Figure 33 shows a framework of how the ICAO SMS uses operational information for risk assessment. STPA does not provide any quantification of risks, but the use of the Active STPA allows the observation of the most common mistakes and failures. Qualitative arguments explaining the cause of incidents are stronger for decision-making than statistics, which only describe the frequency of occurrences in the past.

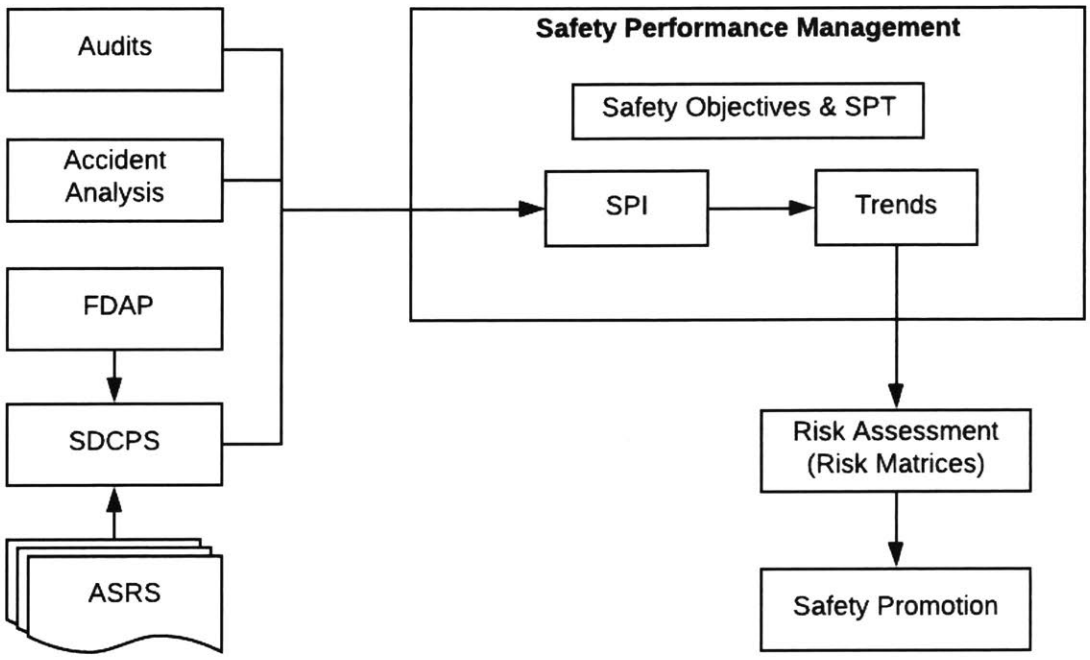



**Figure 33. ICAO SMS framework**

The SMS also requires an Interface Safety Impact Assessment (item 1.3.3.2 of SMM) to measure increases in safety risks induced by problems in the interface of systems' components. States and Service Providers are responsible for managing and monitoring hazards related to those interfaces. Step 3 of the STPA takes a closer look at every control loop, resulting in a list of control actions and the generation of Unsafe Control Actions (UCAs) for different contexts. The combined set of UCAs documented for every hierarchical relation between controllers, eventually added with a coordination analysis among same-level controllers (Johnson, 2017), provides similar information.

Moreover, SMS requires to show a process for Monitoring and Management of Interfaces. Phase 1 of the Active STPA does this by monitoring and inspecting all new inputs. In

this process, all control actions and UCAs are verified, and the reasoning about the assumptions in Phase 2 will determine if the analysis is adequate or if the constraints must be enforced. By running the Active STPA, both monitoring and management of interfaces are already performed.

The SMM explains that a periodic Maturity Assessment (item 1.3.4.3) should verify if the SMS is effective and functioning properly. The outcome of SPI within the ICAO SMS help identify if Safety Objectives and Safety Performance Targets (SPTs) are met. It also determines if operations are occurring within the intended Acceptable Level of Safety Performance (ALoSP) in the organization. Meanwhile, in Active STPA, the fact that the assumptions previously violated are not violated anymore is an indication of improvements in system maturity. However, if new leading indicators refer to the same problem, it becomes an indication of system degradation in safety because the solutions are not being effective.

In terms of indicators, there is a significant difference between the processes proposed to identify leading indicators in ICAO documents and with Active STPA. Figure 34 shows an example of the generation of what ICAO considers as a leading indicator: the percentage of pilots with training.

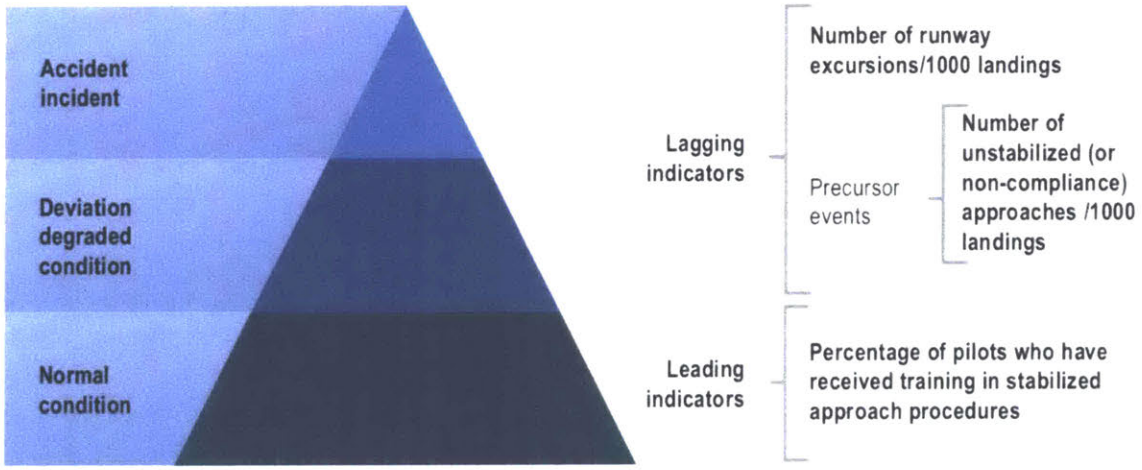



**Figure 34. Example of the link between leading and lagging indicators (SMM, 2018)**

It is true that an increase in the percentage of trained pilots reduces the number of unstable approaches. However, this leading indicator is only one of many other causal factors of unstable approaches and its correlation with the number of unstable approaches (lagging indicator) is not necessarily positive. This is proved by the fact that, even when 100% of pilots are trained, there will be unstable approaches.

Interviews with safety managers of partner airlines found that current SPIs are not accurate in explaining the causal and contributing factors of recent incidents and accidents. Safety Managers need a structured process to guide the conception of a set of SPIs that covers all

major causal factors. The Active STPA is designed to enhance and complement the processes that the organization already has. It does not demand a drastic change in practices, but a combination of processes into an Integrated SMS (I-SMS).

The diagram presented in Figure 35 shows examples of both the use of ICAO SMS and Active STPA to the Case B explored in Chapter 3. This case relates to the Boeing 737 that turned late to intercept the localizer because the attention of one of the pilots was shared between internal checks and a new responsibility: perform visual checks for the other aircraft during a parallel approach for landing. On the left side, there is a Reactive SPI to count the number of unstable approaches. The trends produced by the ICAO SMS inform about the system's safety performance but does not explain to the SA what defenses are needed to improve safety. According to their example, the safety manager would increase training in the current procedures to reduce human error. However, on the right side of the same figure, there is an example of results of an Active STPA to the same incident. The information obtained by the Active STPA helps the SA to act on the source of the actual problem concerning unstable approaches. The SA uses the process to identify the causal factor and generate a more effective solution.

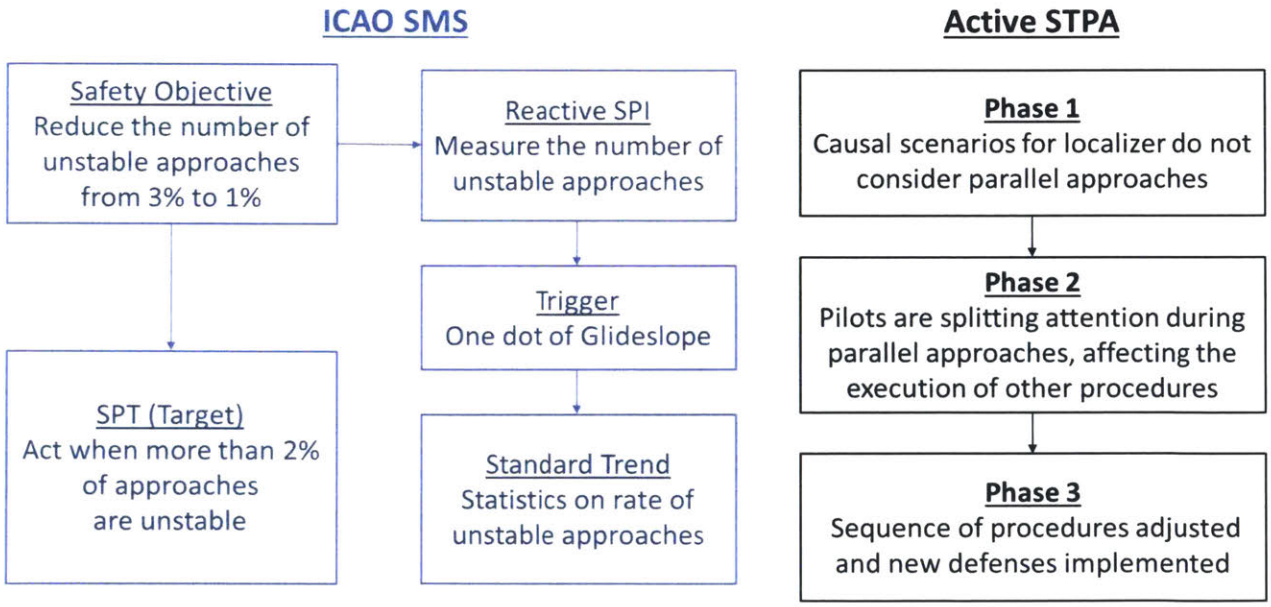



**Figure 35. Example showing the differences between the ICAO SMS and the I-SMS with Active STPA**

ICAO differentiates safety from security stating that the latter is concerned with malicious, intentional acts to disrupt the performance of a system while safety focuses on the negative impact caused by unintended consequences of a combination of factors. Apart from all

the considerations made on safety in this study, STPA was proved to also work for security (Young and Leveson, 2013), another emergent property of a complex system.

## 4.5 Consortium for I-SMS

The elaboration of an STPA on a limited scope requires a few working hours of the SM, and the participation of an expert to assist in the completion of scenarios. For a complex system, an STPA requires a whole team and may take days, or maybe even weeks to be finished. The implementation of both the STPA and the Active STPA, demands a substantial effort from an organization, which may be infeasible for smaller airlines. The Active STPA is best performed and produces better results if the lessons learned when a live STPA is shared with other organizations that operate a similar system.

To develop a common Active STPA for many organizations, it must start with a group formed by organizations with mutual trust, and get expanded as a consortium of several organizations, before becoming part of a federal program. In all of these levels, the de-identification practices already implemented for FOQA/FDM need to be extended to de-identify the incidents. Idealistically, for each aircraft model, all airlines, the manufacturer, and ICAO (including all the agencies) should share a global Active STPA. It all begins with airlines organizing themselves to run concurrent analyses for each flight phase, such as ground operations, takeoff, climb, cruise, descent, approach, and landing. One of the SA should be designated as a custodian of safety data to de-identify the events and protect the integrity of the data. The analyses are then combined, and all partners have access to a complete STPA, an organized set of assumptions, and more robust procedures.

Finally, there is a current effort to incorporate STPA into standards, as an accepted method for safety assessment. If the STPA becomes recognized by agencies, the implementation of the Active STPA will require significantly less company resources.

# 5. Conclusion

The purpose of this research was to: *develop and demonstrate an engineering processes to identify leading indicators of increasing risk during operations to enforce the imposed constraints over time.*

The technique called Active STPA was developed to integrate a hazard analysis into a Safety Management System (SMS). The new model was demonstrated in an aviation case study, using data collected from our aviation partners, to design new defenses for safer operations. The proposed approach may enhance the safety status of an organization using engineering processes that identify when risks are increasing during operations. This identification is made possible by identifying the violations of previous assumptions as leading indicators of higher risk.

The Active STPA is divided into phases and tasks. The first phase searches for ineffective procedures and inspects an STPA to identify incorrect or missing parts of the hazard analysis. The second phase is composed of tasks to guide safety analysts on reasoning about the assumptions that were violated in operational incidents. The third phase helps guide the decision-making process as it relates to the identification of the optimum solutions for system defenses, their implementation, and the update of the STPA.

Active STPA has a formal theoretical basis on STAMP and seeks to extend the capabilities of STPA by providing a process to enforce constraints over time. The Active STPA is about identifying when risk is increasing to act preemptively identifying hazards through analysis and processes within the organization. It is also capable of generating an improved set of requirements by fixing or refining the existing ones.

An original STPA on unstable approaches was presented and served as a basis for the Active STPA. Information from an incident was used to run three Active STPA cases. In each of those cases, broken assumptions were identified as leading indicators of increasing risk. The result of those cases was a set of changes to current training practices and operational procedures recommended to promote a safer operation. Another result was the evolution of the hazard analysis and the enforcement of the defenses that the system already had.

This project had the participation of major airlines in Asia, Brazil, Europe, and the United States. The data on incidents collected with partners was used to test the Active STPA and to develop case studies. During the analysis, new assumptions guided the adaptation of the STPA and new and more effective procedures.

The processes introduced in this study were compared with the current aviation standards for SMS, to show how it differs. The Active STPA has proved to be able to identify assumption-based leading indicators of risk, that are capable of preventing accidents proactively using operational data.

Finally, the Integrated Safety Management System (I-SMS) framework was introduced as a systems-based framework for safety management to foster the effectiveness of system defenses over time. This structure has processes that use operational data as an input to the Active STPA. The result is a set of new preventing and mitigating actions that update rules and procedures, enforcing the defenses that the system has, or building new ones. The I-SMS general framework has no analogous method in current literature, and it can be modeled by safety managers to adjust to any organization running safety-critical systems.

## 5.1 Contributions

The broader impact of this research is:

- Qualitative evaluation of system migration towards a state of higher risk
- Feedback on enforcement mechanisms for constraints
- Information for top-management to assist in long-term planning and decision making

The contributions of this research start with the advantages of the integration of a modern hazard analysis technique at the operational level, allowing organizations, such as airlines, to identify causal factors of operational incidents. The novelty of this approach is the identification of violated assumptions, allowing a better understanding of the environment, and the system itself.

An additional benefit of using Active STPA is the ability to populate an STPA and procedures using the observation of unforeseen behaviors. The continual use of the Active STPA may lead to an increased maturity of the system. Although the I-SMS may require more effort from the safety team than current practices, there are relevant advantages in investing the required resources because, as operators observe positive changes to the system, they develop trust in the process to elaborate new defenses, which fosters better safety communication and safety culture.

## 5.2 Future work

This research was limited by the amount of data received and the inability to implement the recommended changes to the current operation of our partners. To measure the impact of the implementation of those changes, future research should verify the following aspects of long-term use of the I-SMS:

- Evaluation of the use of I-SMS on a testbed of aviation operations
- The creation of analytical tools to allow user-friendly implementation and continual use

- Exploratory studies to investigate the feasibility of the approach and design of the I-SMS and the tools used to support it
- Comparative analysis with other proposed approaches

Additionally, the framework of the I-SMS shows only one-way arrows connecting the sources (Process 1) with the Active STPA (Process 2). However, future research may show that an output from the STPA could facilitate the execution of Testing and Management of Change. The new scenarios added when updating the STPA in the end of Phase 3 could be used to create testing events. Also, the organization may adapt the format of Management of Change reports to include the reasoning of the Active STPA. Also, the information of the Active STPA could be used to facilitate a new CAST analysis of an accident.

Finally, the Active STPA may be extended to emergent properties other than safety. For example, while security is not the focus of this research, the identification of leading indicators of increasing cybersecurity risk could be treated similarly. Thus, the concepts introduced in this research may be extended to identify system vulnerabilities.

# References


Altabbakh, H.M., 2013. Risk analysis: comparative study of various techniques. Missouri University of Science and Technology.

Biferno, M.A., 1985. Mental workload measurement: Event-related potentials and ratings of workload and fatigue. Long Beach, CA, United States.

Booton, R.C., Ramo, S., 1984. The Development of Systems Engineering. IEEE Trans. Aerosp. Electron. Syst. AES-20, 306–310. https://doi.org/10.1109/TAES.1984.4502055

Borovec, K., Balgač, I., Karlović, R., 2011. Estimation of satisfaction with internal communication in the Ministry of the Interior of the Republic of Croatia. 18th BledCom Int. Public Relations Res. Symp. 216. https://doi.org/10.1080/09595230802089917

Castilho, D.S., Urbina, L.M.S., Andrade, D. De, 2018. STPA for continuous controls: A flight testing study of aircraft crosswind takeoffs. Safety Science. 108, 129–139. https://doi.org/10.1016/j.ssci.2018.04.013

Checkland, P., 1981. Systems Thinking, Systems Practice, Systems Thinking Systems Practice. https://doi.org/10.1016/0143-6228(82)90039-X

Columbia Accident Investigation Board, 2003. Report of Columbia Accident Investigation Board, Volume I I, 1–248. https://doi.org/10.1177/0020852309104177

Dan Montes, 2015. Intelligent-Controller Extensions to STPA.

Das, S., Li, L., Srivastava, A., Hansman, R.J., 2012. Comparison of Algorithms for Anomaly Detection in Flight Recorder Data of Airline Operations. 12th AIAA Aviat. Technol. Integr. Oper. Conf. 14th AIAA/ISSMO Multidiscip. Anal. Optim. Conf. 9–11. https://doi.org/10.2514/6.2012-5593

Dekker, S., 2006. The Field Guide to Understanding Human Error, Ergonomics. https://doi.org/10.1080/00140130701680544

EASA, 2010a. Safety Management International Collaboration Group.

EASA, 2010b. Development of a Common Taxonomy for Hazards.

FAA, 2016. FAA Order 8000.369B - Safety Management System.

FAA, FAA InFO, 2011. The Apple iPad and Other Suitable Tablet Computing Devices as Electronic Flight Bags (EFB).

Federal Aviation Administration, 2015. Advisory Circular 120-92B (Safety management systems for aviation service providers) 1–4.

Fitts, P.M., 1954. The information capacity of the human motor system in controlling the amplitude of movement. J. Exp. Psychol. https://doi.org/10.1037/h0055392

Foundation, F.S., 2019. Safety Performance Monitoring [WWW Document]. URL https://flightsafety.org/gsip/safety-performance-monitoring/

France, M.E., 2017. Engineering for Humans : A New Extension to STPA. Massachusetts Institute of Technology.

Gallagher, C., Dip, B.A., Becon, E., Underhill, E., Mcom, B., 2016. Policy and Practice in Health and Safety Occupational safety and health management systems in Australia : barriers to success O 3996. https://doi.org/10.1080/14774003.2003.11667637

Goetsch, S., 1996. Safeware: System Safety and Computers , by Nancy Leveson . Med. Phys. 23, 1821–1821. https://doi.org/10.1118/1.597766

Head, Horn, 1991. Essentials of risk management: volume 1. Insurance Institute of America.

Horney, D.C., 2017. Systems-Theoretic Process Analysis and Safety-Guided Design of Military Systems.

IATA, 2018. IATA Releases 2017 Airline Safety Performance, Iata.Org.

ICAO, 2018. Doc 9859, Safety Management Manual (SMM).

ICAO, 2016. Annex 13 to the Convention on International Civil Aviation - Aircraft Accident and Incident Investigation.

Johnson, K.E., 2017. Systems-Theoretic Safety Analyses Extended for Coordination. Massachusetts Institute of Technology.

Kramer, A.F., Sirevaag, E.J., Braune, R., 1987. A psychophysiological assessment of operator workload during simulated flight missions. Hum. Factors 29, 145–160. https://doi.org/10.1177/001872088702900203

Lederer, J., 1985. HUMAN FACTORS IN OPERATIONAL COMMUNICATIONS. Prof. Saf.

Leveson, N., 2019. CAST Handbook.

Leveson, N., 2015. A systems approach to risk management through leading safety indicators. Reliab. Eng. Syst. Saf. 136, 17–34. https://doi.org/10.1016/j.ress.2014.10.008

Leveson, N.G., 2015. A systems approach to risk management through leading safety indicators. Reliab. Eng. Syst. Saf. 136, 17–34. https://doi.org/10.1016/j.ress.2014.10.008

Leveson, N.G., 2014. Using STAMP to develop leading indicators. Lect. Notes Informatics (LNI), Proc. - Ser. Gesellschaft fur Inform. P-232.

Leveson, N.G., 2013. The Need for New Paradigms in Safety Engineering.

Leveson, N.G., 2011. Engineering a Safer World: Systems Thinking Applied to Safety, Vasa. https://doi.org/10.1017/CBO9781107415324.004

Leveson, N.G., 2004. A systems-theoretic approach to safety in software-intensive systems. IEEE Trans. Dependable Secur. Comput. 1, 66–86. https://doi.org/10.1109/TDSC.2004.1

Leveson, N.G., Thomas, J.P., 2018. STPA Handbook 188. https://doi.org/10.2143/JECS.64.3.2961411

Li, Y., Guldenmund, F.W., 2018. Safety management systems_ A broad overview of the

literature. Saf. Sci. 103, 94–123. https://doi.org/10.1016/j.ssci.2017.11.016

Massimini, S.V., 2006. Simultaneous Independent and Dependent Parallel Instrument Approaches.

MIL-STD-882E, 2012. Mil-Std-882D Standard Practice for System Safety. Mctechsystems.Com.

Mogles, N., Padget, J., Bosse, T., 2018. Systemic approaches to incident analysis in aviation: Comparison of STAMP, agent-based modelling and institutions. Saf. Sci. 108, 59–71. https://doi.org/10.1016/j.ssci.2018.04.009

Montes, D.R., 2016. Using STPA to Inform Developmental Product Testing. Massachusetts Institute of Technology.

Montes, D.R., Hill, T.D., Cookson, J., Cannon, G., 2019. The Evolution of the USAF Test Pilot School Education - Paradigm toward a Systems-Engineering Foundation. https://doi.org/10.2514/6.2018-2919

Oien, K., Utne, I.B., Tinmannsvik, R.K., Massaiu, S., 2011. Building Safety indicators: Part 2 - Application, practices and results. Saf. Sci. 49, 162–171. https://doi.org/10.1016/j.ssci.2010.05.015

Rasmussen, J., 1997. Risk management in a dynamic society: A modelling problem. Saf. Sci. https://doi.org/10.1016/S0925-7535(97)00052-0

Reason, J., 1990. The contribution of latent human failures to the breakdown of complex systems. Philos. Trans. R. Soc. Lond. B. Biol. Sci. 327, 475–484. https://doi.org/10.1098/rstb.1990.0090

Roland, H.E., Moriarty, B., 2009. System Safety Engineering and Management, System Safety Engineering and Management. https://doi.org/10.1002/9780470172438

Stolzer, A.J., Friend, M.A., Truong, D., Tuccio, W.A., Aguiar, M., 2018. Measuring and evaluating safety management system e ff ectiveness using Data Envelopment Analysis. Saf. Sci. 104, 55–69. https://doi.org/10.1016/j.ssci.2017.12.037

Vinodkumar, M.N., Bhasi, M., 2010. Safety management practices and safety behaviour: Assessing the mediating role of safety knowledge and motivation. Accid. Anal. Prev. 42, 2082–2093. https://doi.org/10.1016/j.aap.2010.06.021

Wiegmann, D., 2005. Developing a Methodology for Eliciting Subjective Probability Estimates During Expert Evaluations of Safety Interventions: Application for Bayesian Belief Networks. Aviat. Hum. Factors Div. Inst. Aviat. 92, 0–19.

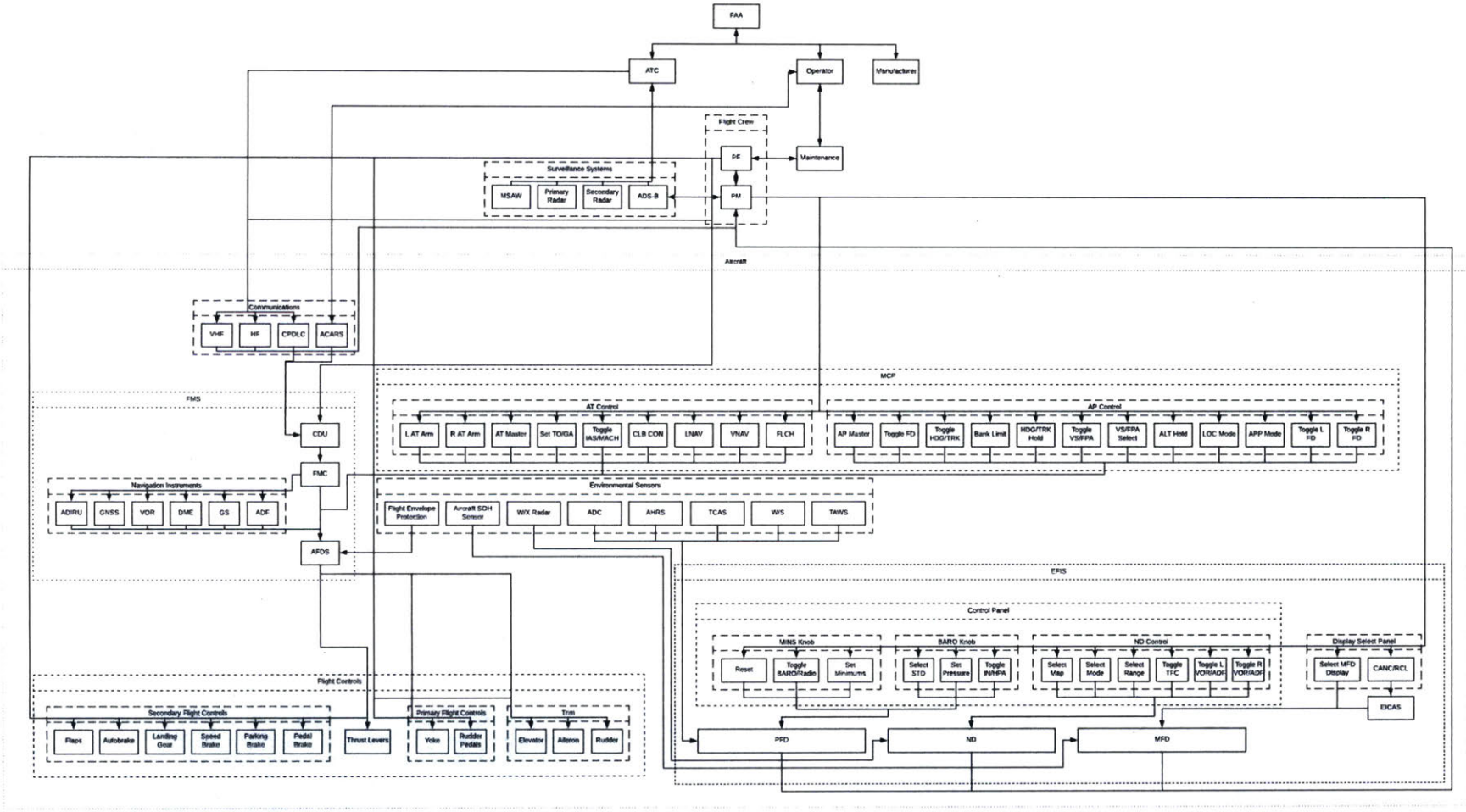
Young, W., 2014. Applying System-Theoretic Process Analysis for Security ( STPA-SEC ) to Support Mission Assurance and Security.

Young, W., Leveson, N., 2013. Systems Thinking for Safety and Security 1–8. https://doi.org/10.1145/2523649.2530277

# Appendices

# Appendix A

## Detailed Safety Control Structure – Step 2



## Appendix B
## ATC STPA Step 3

| STPA Step 3 - Unsafe Control Actions (UCA) | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Control Actions | Provided causes Hazard | | | Not Provided causes Hazard | | | Applied for too long or too short | | | Wrong timing or order | | |
| | UCA | H* | Description | UCA | H* | Description | UCA | H* | Description | UCA | H* | Description |
| Heading | 1 | H3 | ATC vector AC towards NTZ when AC is in close proximity of NTZ | 2 | H3 | ATC does not vector AC for a breakout when AC is threatened by a neighboring AC intruding into NTZ | | | | 3 | H3 | ATC does not vector AC away from NTZ when AC is imminently entering NTZ |
| | | | | | | | | | | 4 | H2 | ATC does not vector AC when AC is imminently breaching obstacle clearance |
| | | | | | | | | | | 5 | H3 | ATC does not vector AC when AC is imminently breaching separation |
| Climb | 6 | H3 | ATC instructs AC to climb when there is traffic above | 7 | H2 | ATC does not instruct AC to climb when AC is below minimum altitude for the sector | | | | | | |

| Control Actions | Provided causes Hazard | | | Not Provided causes Hazard | | | Applied for too long or too short | | | Wrong timing or order | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | UCA | H* | Description | UCA | H* | Description | UCA | H* | Description | UCA | H* | Description |
| Descend | 8 | H3 | ATC instructs AC to descend when there is traffic below | | | | | | | 9 | H1.3 | ATC clears AC to descend too late when AC is imminently high in relation to specified glidepath |
| | 10 | H2 | ATC instructs AC to descend when AC is at the minimum altitude for the sector | | | | | | | | | |
| Maintain altitude | 11 | H2 | ATC instructs AC to maintain altitude when AC is imminently breaching obstacle clearance (e.g. in a rising terrain) | | | | | | | 12 | H2 | ATC instructs AC to maintain altitude too late when AC is imminently descending below minimum altitude for the sector |
| | 13 | H1.3 | ATC instructs AC to maintain altitude when AC is late to establish a stable approach | | | | | | | | | |

| Control Actions | Provided causes Hazard | | | Not Provided causes Hazard | | | Applied for too long or too short | | | Wrong timing or order | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | UCA | H* | Description | UCA | H* | Description | UCA | H* | Description | UCA | H* | Description |
| Change radio frequency | 14 | H1, H2, H3 | ATC instructs AC to change radio frequency when provided frequency is not used by the controller in the next phase (e.g. not in range, or has no controller) | | | | | | | 15 | H1, H2, H3 | ATC instructs AC to change radio frequency too late when radar identification has been handed off to the controller in the next phase |
| | 16 | H1, H2, H3 | ATC instructs AC to change radio frequency when coordination has not been made with the controller in the next phase | | | | | | | | | |
| Cleared Approach | 17 | H3 | ATC clears AC for APP when the APP protected area is not clear | | | | | | | | | |
| | 18 | H3 | ATC clears APP procedure that conflicts with procedures followed by other AC | | | | | | | | | |

| Control Actions | Provided causes Hazard | | | Not Provided causes Hazard | | | Applied for too long or too short | | | Wrong timing or order | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | UCA | H* | Description | UCA | H* | Description | UCA | H* | Description | UCA | H* | Description |
| Cleared Approach | 19 | | ATC clears APP when AC does not have latest ATIS and relevant info is not provided by ATC | | | | | | | | | |
| Intercept ILS | 20 | H3 | ATC instructs AC To intercept the ILS when AC is at risk of overshooting the turn due to high speed | | | | | | | 21 | H3 | ATC instruct AC to intercept ILS too late when AC is imminently entering NTZ |
| | 22 | H1, H2 | ATC clears AC to intercept the ILS when AC is not in a position to do so (too high on the GS or LOC intercept angle too large) | | | | | | | | | |
| Adjust speed | 23 | H1. 3 | ATC instructs AC to maintain speed higher than Vapp when in final APP | 24 | H3 | ATC does not instruct speed changes when AC imminently breaches separation | | | | | | |

| Control Actions | Provided causes Hazard | | | Not Provided causes Hazard | | | Applied for too long or too short | | | Wrong timing or order | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | UCA | H* | Description | UCA | H* | Description | UCA | H* | Description | UCA | H* | Description |
| Side step to parallel runway | 25 | H3 | ATC instructs side step when parallel approach is in progress | | | | | | | 26 | H1 | ATC instructs AC to side step when AC is in final APP |
| Cleared to land | 27 | H3 | ATC clears AC to land when RWY is occupied | 28 | | ATC does not clear AC to land when AC has low fuel | | | | | | |
| Go Around/ missed approach | 29 | H4 | ATC instructs AC To GA when aircraft is not at risk | 30 | H3 | ATC does not instruct AC to GA when RWY is occupied | | | | 31 | H2, H3 | ATC instructs AC to GA too late when AC has already started decelerating |
| | 32 | H3 | ATC instructs AC to GA when there is traffic above | 33 | H1, H2, H3 | ATC does not instruct AC to GA when radar contact is lost | | | | | | |
| | | | | 34 | H1 | ATC does not instruct AC to GA when AC is too high/low for safe approach | | | | | | |
| | | | | 35 | H1 | ATC does not instruct AC to GA when AC is too far left/right for safe approach | | | | | | |

| Control Actions | Provided causes Hazard | | | Not Provided causes Hazard | | | Applied for too long or too short | | | Wrong timing or order | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | UCA | H* | Description | UCA | H* | Description | UCA | H* | Description | UCA | H* | Description |
| Hold Short | | | | 36 | H3 | ATC does not instruct AC to hold short when crossing RWY in use | | | | 37 | H3 | ATC instructs AC to hold short too late when AC has passed hold short line |
| Cleared to takeoff | 38 | H3 | ATC instructs AC To TO when RWY is occupied | | | | | | | | | |
| Line up and wait | 39 | H3 | ATC instructs AC to LUAW when another AC is on short final for the same RWY | | | | | | | | | |
| Hold | 40 | | ATC instructs AC to hold when fuel is low | 41 | H1 | ATC does not instruct AC to hold when APP is imminently impacted by weather | 42 | | ATC instructs AC to hold for too long when fuel becomes low | | | |
| Comand Breakout turn | | | | 43 | H1, H3 | ATC does not command breakout turn when AC ingress NTZ | | | | | | |

**Appendix C**
**ATC STPA Step 4**

| STPA Step 4 | | | |
|---|---|---|---|
| **UCA #** | **UCA** | **Scenarios** | **Constraint** |
| 1 | ATC vector AC towards NTZ when AC is in close proximity of NTZ | Only one ATC monitoring parallel approach of two AC, the ATC commands missed approach procedure to the wrong AC<br><br>ATC gets mistaken between left and right when the navigation profile to intercept the LOC is from the top to the bottom of the screen | Missed approach procedure must not involve a turn towards NTZ<br><br>ATC must be familiar with missed approach procedure<br><br>ATC must not mis-identify AC requiring missed approach procedure |
| 2 | ATC does not vector AC for a breakout when AC is threatened by a neighboring AC intruding into NTZ | NTZ mis-represented on the radar display<br><br>Intruder AC location mis-represented on the radar display<br><br>Two ATC monitor parallel approach RWY's, the ATC responsible for the RWY has a short-time confusion of which RWY he/she is monitoring<br><br>Another aircraft is communicating on the frequency | NTZ must be represented correctly on the radar display<br><br>AC location must be presented correctly on the radar display<br><br>Where two ATC monitor parallel approach RWYs, responsibility of the RWY being monitored must be clearly delineated<br><br>ATC must be able to override any aircraft transmission on a frequency |

| | | | |
|---|---|---|---|
| 3 | ATC does not vector AC away from NTZ when AC is imminently entering NTZ | NTZ miss-represented on the radar display<br><br>AC location and course info miss-represented on the radar display<br><br>ATC misjudges whether the AC has time for course correction<br><br>Another aircraft is communicating on the frequency | NTZ must be represented correctly on the radar display<br><br>AC location and course info must be presented correctly on the radar display<br><br>Where two ATC monitor parallel approach RWYs, responsibility of the RWY being monitored must be clearly delineated<br><br>ATC must be familiar with AC dynamics for course correction<br><br>ATC must be able to override any aircraft transmission on a frequency |

| | | | |
|---|---|---|---|
| 4 | ATC does not vector AC when AC is imminently breaching obstacle clearance | AC location and course info miss-represented on the radar display<br><br>MSAW does not provide a warning to ATC when it should<br><br>ATC believes the MSAW is engaged when it is not<br><br>ATC has a flawed information of minimum safe altitudes in the sector<br><br>ATC believes that the AC is able to do more effective course correction than it actually can<br><br>Another aircraft is communicating on the frequency | AC location and course info must be presented correctly on the radar display<br><br>MSAW shall provide warning based on configured parameters and meet reliability requirement<br><br>ATC must know the status of MSAW functionality<br><br>ATC must know the applicable minimum safe altitudes<br><br>ATC must be familiar with AC dynamics for course correction<br><br>ATC must be able to override any aircraft transmission on a frequency |
| 5 | ATC does not vector AC when AC is imminently breaching separation | AC location and course info miss-represented on the radar display<br><br>ATC misjudges the required separation distance when zooming the screen<br><br>Another aircraft is communicating on the frequency | AC location and course info must be presented correctly on the radar display<br><br>ATC must know the applicable separation distance in sector<br><br>ATC must be familiar with AC dynamics for course correction<br><br>ATC must be able to override any aircraft transmission on a frequency |

| | | | |
|---|---|---|---|
| 6 | ATC instructs AC to climb when there is traffic above | AC location info miss-represented on the radar display<br><br>ATC provides the climb instruction to another AC not requiring climb maneuver | AC location must be presented correctly on the radar display<br><br>ATC must not miss-identify AC requiring climb maneuver |
| 7 | ATC does not instruct AC to climb when AC is below minimum altitude for the sector | AC location and course info miss-represented on the radar display<br><br>MSAW does not provide a warning to ATC when it should<br><br>Another aircraft is communicating on the frequency | AC location and course info must be presented correctly on the radar display<br><br>MSAW shall provide warning based on configured parameters and meet reliability requirement<br><br>ATC must know the status of MSAW functionality<br><br>ATC must know the applicable minimum safe altitudes<br><br>ATC must be familiar with AC dynamics for course correction<br><br>ATC must be able to override any aircraft transmission on a frequency |

| | | | |
|---|---|---|---|
| 8 | ATC instructs AC to descend when there is traffic below | AC location info miss-represented on the radar display<br><br>ATC believes that the descend instruction does not conflict with VFR traffic<br><br>ATC provides the descent instruction to another AC not requiring descend maneuver | AC location must be presented correctly on the radar display<br><br>ATC must be familiar with VFR traffic pattern and sector boundary<br><br>ATC must not miss-identify AC requiring descend maneuver |
| 9 | ATC clears AC to descend too late when AC is imminently high in relation to specified glidepath | AC location info miss-represented on the radar display<br><br>ATC has representation of the of the glidepath that is incorrect<br><br>ATC delays descent instruction due to high workload<br><br>ATC provides the descent instruction to another AC not requiring descend maneuver | AC location must be presented correctly on the radar display<br><br>ATC must be familiar with glidepath<br><br>Absent of safety-of-flight condition, priority shall be given to providing descent instruction for AC in final APP<br><br>Workload of sector must not exceed ATC capacity<br><br>ATC must not miss-identify AC requiring descend maneuver |
| 10 | ATC instructs AC to descend when AC is at the minimum altitude for the sector | AC location and course info miss-represented on the radar display<br><br>ATC does not know the minimum safe altitudes in the sector | AC location and course info must be presented correctly on the radar display<br><br>ATC must know the applicable minimum safe altitudes |

| | | | |
|---|---|---|---|
| 11 | ATC instructs AC to maintain altitude when AC is imminently breaching obstacle clearance (e.g. in a rising terrain) | AC location and course info miss-represented on the radar display<br><br>ATC believes that the minimum safe altitudes in the sector are lower | AC location and course info must be presented correctly on the radar display<br><br>ATC must know the applicable minimum safe altitudes<br><br>ATC must be familiar with AC dynamics for course correction |
| 12 | ATC instructs AC to maintain altitude too late when AC is imminently descending below minimum altitude for the sector | AC location and course info miss-represented on the radar display<br><br>ATC does not know the turning radius of the AC | AC location and course info must be presented correctly on the radar display<br><br>ATC must know the applicable minimum safe altitudes<br><br>ATC must be familiar with AC dynamics for course correction |
| 13 | ATC instructs AC to maintain altitude when AC is late to establish a stable approach | AC location info miss-represented on the radar display<br><br>ATC does not know where is the position of glideslope interception<br><br>ATC believes that traffic exists to impede safe descent of AC | AC location must be presented correctly on the radar display<br><br>ATC must be familiar with glidepath<br><br>ATC must maintain situational awareness of all aircraft in sector |

| | | | |
|---|---|---|---|
| 14 | ATC instructs AC to change radio frequency when provided frequency is not used by the controller in the next phase (e.g. not in range, or has no controller) | ATC does not know which frequency must be set in the next phase<br><br>Modification of frequency setting is not coordinated between ATC sectors<br><br>Inability to contact the controller in the next phase is not subsequently reported by AC to ATC | ATC must be familiar with frequency setting of the controller in the next phase<br><br>Modification of frequency setting must be coordinated between ATC sectors<br><br>Inability to contact the controller in the next phase must be reported by AC to the last contacted ATC |
| 15 | ATC instructs AC to change radio frequency too late when radar identification has been handed off to the controller in the next phase | ATC believes that the AC has been instructed to change radio frequency<br><br>ATC delays frequency change instruction due to high workload | ATC must maintain correct status of all AC in area of control of sector<br><br>Workload of sector must not exceed ATC capacity |
| 16 | ATC instructs AC to change radio frequency when coordination has not been made with the controller in the next phase | ATC believes that the coordination has already been made with the controller in the next phase | ATC must maintain correct status of all AC in area of control of sector |
| 17 | ATC clears AC for APP when the APP protected area is not clear | AC location info miss-represented on the radar display<br><br>ATC believes that the APP protected area is different because he or she learned about the with incorrect information | AC location must be presented correctly on the radar display<br><br>ATC must know the applicable APP protected area |

| | | | |
|---|---|---|---|
| 18 | ATC clears APP procedure that conflicts with procedures followed by other AC | AC location and course info miss-represented on the radar display<br><br>ATC believes that APP procedure does not conflict with procedure followed by another AC | AC location and course info must be presented correctly on the radar display<br><br>ATC must be familiar with acceptable APP procedure pairing for parallel approach |
| 19 | ATC clears APP when AC does not have latest ATIS and relevant info is not provided by ATC | ATIS alphabet code is not provided by AC to ATC<br><br>ATC did not receive the latest ATIS alphabet code and change information<br><br>ATC thinks that the AC has the latest ATIS<br><br>ATC believes that all relevant info is provided to AC without the latest ATIS | AC must provide ATIS alphabet code to ATC when applicable<br><br>Latest ATIS alphabet code and change information must be provided to ATC<br><br>ATC must maintain correct status of all AC in area of control of sector |
| 20 | ATC instructs AC To intercept the ILS when AC is at risk of overshooting the turn due to high speed | AC location and course info miss-represented on the radar display<br><br>ATC believes that AC have time for course correction | AC location and course info must be presented correctly on the radar display<br><br>ATC must be familiar with AC dynamics for course maneuver |

| | | | |
|---|---|---|---|
| 21 | ATC instruct AC to intercept ILS too late when AC is imminently entering NTZ | NTZ miss-represented on the radar display<br><br>AC location miss-represented on the radar display<br><br>Another aircraft is communicating on the frequency | NTZ must be represented correctly on the radar display<br><br>AC location must be presented correctly on the radar display<br><br>ATC must be able to override any aircraft transmission on a frequency |
| 22 | ATC clears AC to intercept the ILS when AC is not in a position to do so (too high on the GS or LOC intercept angle too large) | NTZ miss-represented on the radar display<br><br>AC location miss-represented on the radar display<br><br>ATC gets confused between two AV<br><br>ATC does not know the ideal interception point of the GS at that altitude | NTZ must be represented correctly on the radar display<br><br>AC location must be presented correctly on the radar display<br><br>ATC must be familiar with glidepath, LOC intercept requirement |
| 23 | ATC instructs AC to maintain speed higher than Vapp when in final APP | AC location miss-represented on the radar display<br><br>AC speed restriction miss-represented on the radar display<br><br>ATC does not know the ideal Vapp of an AC<br><br>Speed assignment to AC is provided with the wrong termination fix or without one | AC location must be presented correctly on the radar display<br><br>AC speed restriction must be presented correctly on the radar display<br><br>ATC must be familiar with AC dynamics for course maneuver<br><br>Speed assignment to AC must be provided with an accurate termination fix when provided near final APP |

| | | | |
|---|---|---|---|
| 24 | ATC does not instruct speed changes when AC imminently breaches separation | AC location and course info miss-represented on the radar display<br><br>ATC thinks that the required separation distance is different than actual value<br><br>ATC does not understand the influence of speed in turning radius<br><br>ATC misjudges whether the AC to have limited speed change ability (given current configuration)<br><br>Another aircraft is communicating on the frequency | AC location and course info must be presented correctly on the radar display<br><br>ATC must know the applicable separation distance in sector<br><br>ATC must be familiar with AC dynamics for course correction<br><br>ATC must be able to override any aircraft transmission on a frequency |
| 25 | ATC instructs side step when parallel approach is in progress | ATC thinks that side step instruction for parallel approach is permitted<br><br>AC location and course info miss-represented on the radar display<br><br>When two ATC monitor parallel approach RWY's, the ATC instructing the side step thinks that the parallel approach path is not occupied | ATC must be familiar with the permitted and prohibited maneuvers in a parallel approach<br><br>AC location and course info must be presented correctly on the radar display<br><br>ATC must be familiar with acceptable APP procedure pairing for parallel approach |

| | | | |
|---|---|---|---|
| 26 | ATC instructs AC to side step when AC is in final APP | ATC believes that side step instruction for parallel approach is permitted<br><br>AC location and course info miss-represented on the radar display<br><br>Where two ATC monitor parallel approach RWY's, the ATC instructing the side step thinks that the parallel approach free | ATC must be familiar with the permitted and prohibited maneuvers in a parallel approach<br><br>AC location and course info must be presented correctly on the radar display<br><br>ATC must be familiar with acceptable APP procedure pairing for parallel approach |
| 27 | ATC clears AC to land when RWY is occupied | AC location and course info miss-represented on the radar display -- both in air and on ground, if applicable<br><br>ATC believes that the AC in the ground have time for RWY clearance | AC location and course info must be presented correctly on the radar display<br><br>ATC must be familiar with AC dynamics for ground maneuvers and approach |
| 28 | ATC does not clear AC to land when AC has low fuel | ATC is not notified of low fuel condition<br><br>Weather and RWY equipment precludes ATC from clearing AC for safe landing | ATC must be notified of low fuel condition<br><br>AC must be diverted to alternate airport with sufficient lead time when weather and RWY equipment does not allow for safe landing |

| | | | |
|---|---|---|---|
| 29 | ATC instructs AC To GA when aircraft is not at risk | AC location and course info miss-represented on the radar display -- both in air and on ground, if applicable<br><br>ATC believes the RWY is occupied when it is not<br><br>ATC thinks that the AC landing exhibit dynamic anomaly when it is not | AC location and course info must be presented correctly on the radar display<br><br>ATC must maintain correct status of all AC in area of control of sector |
| 30 | ATC does not instruct AC to GA when RWY is occupied | AC location and course info miss-represented on the radar display -- both in air and on ground, if applicable<br><br>ATC thinks that RWY is unoccupied when it is not<br><br>RWY occupancy is not reported by third party aircraft witnessing the condition | AC location and course info must be presented correctly on the radar display<br><br>ATC must maintain correct status of all AC in area of control of sector<br><br>RWY occupancy must be reported by third party aircraft witnessing the condition |
| 31 | ATC instructs AC to GA too late when AC has already started decelerating | AC location and course info miss-represented on the radar display -- both in air and on ground, if applicable<br><br>ATC believes that the AC is at risk of runway overrun or collision when it is not | AC location and course info must be presented correctly on the radar display<br><br>ATC must maintain correct status of all AC in area of control of sector |

| | | | |
|---|---|---|---|
| 32 | ATC instructs AC to GA when there is traffic above | AC location info miss-represented on the radar display | AC location must be presented correctly on the radar display |
| 33 | ATC does not instruct AC to GA when radar contact is lost | AC location and course info miss-represented on the radar display<br><br>Loss of radar contact is not annunciated on the radar display<br><br>ATC believes that the landing AC is on radar contact when it is not | AC location and course info must be presented correctly on the radar display<br><br>ATC must maintain correct status of all AC in area of control of sector |
| 34 | ATC does not instruct AC to GA when AC is too high/low for safe approach | AC location and course info miss-represented on the radar display<br><br>ATC thinks that the landing AC is on a stable APP when it is not because radar representation is inacurate | AC location and course info must be presented correctly on the radar display<br><br>ATC must maintain correct status of all AC in area of control of sector |
| 35 | ATC does not instruct AC to GA when AC is too far left/right for safe approach | AC location and course info miss-represented on the radar display | AC location and course info must be presented correctly on the radar display<br><br>ATC must maintain correct status of all AC in area of control of sector |

| | | | |
|---|---|---|---|
| 36 | ATC does not instruct AC to hold short when crossing RWY is in use | AC location and course info miss-represented on the radar display<br><br>Where multiple controllers are managing traffic at the airport, the controllers do not understand the limit in individual responsibilities because there is a cultural lack of communications<br><br>Where multiple controllers are managing traffic at the airport, a ground controller believes that a RWY is not in use<br><br>ATC thinks that the AC on ground has time for RWY clearance, but AC is taxiing slower than normal | AC location and course info must be presented correctly on the radar display<br><br>Where more than one ATC manage traffic at the airport, responsibilities must be clearly delineated<br><br>ATC must maintain correct status of all AC in area of control of sector<br><br>ATC must be familiar with AC dynamics for ground maneuvers and approach |
| 37 | ATC instructs AC to hold short too late when AC has passed hold short line | AC location and course info miss-represented on the radar display<br><br>Hold point marking is unclear from the tower<br><br>ATC thinks the AC was instructed to hold short of the line<br><br>Another aircraft is communicating on the frequency | AC location and course info must be presented correctly on the radar display<br><br>Holding point must be clearly visible from the tower<br><br>ATC must maintain correct status of all AC in area of control of sector, including the instruction given<br><br>ATC must be able to override any aircraft transmission on a frequency |

| | | | |
|---|---|---|---|
| 38 | ATC instructs AC To TO when RWY is occupied | AC location and course info miss-represented on the radar display<br><br>ATC believes that occupying AC have time to vacate the RWY prior to the AC taking off reaching the location | AC location and course info must be presented correctly on the radar display<br><br>ATC must maintain correct status of all AC in area of control of sector<br><br>ATC must be familiar with AC dynamics for ground maneuvers and approach |
| 39 | ATC instructs AC to LUAW when another AC is on short final for the same RWY | AC location and course info miss-represented on the radar display<br><br>ATC believes that the AC taking off will initiate TO run immediately | AC location and course info must be presented correctly on the radar display<br><br>ATC must maintain correct status of all AC in area of control of sector<br><br>ATC must be familiar with AC dynamics for ground maneuvers and approach |
| 40 | ATC instructs AC to hold when fuel is low | ATC is not notified of low fuel condition<br><br>Weather and RWY equipment precludes ATC from clearing AC for safe landing | ATC must be notified of low fuel condition<br><br>AC must be diverted to alternate airport with sufficient lead time when weather and RWY equipment does not allow for safe landing |

| | | | |
|---|---|---|---|
| 41 | ATC does not instruct AC to hold when APP is imminently impacted by weather | Weather location and course info miss-represented on the radar display<br><br>AC location and course info miss-represented on the radar display<br><br>ATC thinks that the AC have time enough to land prior to the weather reaching the location<br><br>ATC forget about the procedure holding point | Weather location and course info must be presented correctly on the radar display<br><br>AC location and course info must be presented correctly on the radar display<br><br>ATC must be familiar with dynamics for AC on approach and weather<br><br>ATC must maintain correct status of all AC in area of control of sector<br><br>ATC must be familiar with the hold points in the APP |
| 42 | ATC instructs AC to hold for too long when fuel becomes low | ATC is not notified of low fuel condition<br><br>Weather and RWY equipment precludes ATC from clearing AC for safe landing | ATC must be notified of low fuel condition<br><br>AC must be diverted to alternate airport with sufficient lead time when weather and RWY equipment does not allow for safe landing |
| 43 | ATC does not command breakout turn when AC ingress NTZ | ATC is working on multiple tasks and believes that entered in the NTZ already turning will safely intercept the LOC by the other side | Controllers must command Breakout turn every time a AC enters the NTZ |

## Appendix D
### Crew STPA Step 3

| Process | Switch / Selector | Control Actions | STPA Step 3 - Unsafe Control Actions (UCA) | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Provided causes Hazard | | | Not Provided causes Hazard | | | Applied for too long or too short | | | Wrong timing or order | | |
| | | | UCA | H | Description | UCA | H | Description | UCA | H | Description | UCA | H | Description |
| Vertical path on Autopilot | VNAV | On | 1 | 3 | Crew engages Profile Mode (VNAV) before descent path is properly programmed (configured) | | | Crew does not engage VNAV when chart limitations become impossible to achieve | | | | 2 | 4 | Crew engages Profile Mode (VNAV path) that violates ATC clearances or published altitude restrictions |
| | | | 3 | 3 | Crew arms Profile Mode (VNAV) below 400 ft AGL and expects Profile Mode (VNAV) to engage | | | | | | | | | |
| | | | 4 | 2 | Crew engages Profile Mode Speed (VNAV SPD) in descent | | | | | | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | when target speed is set too low, no stall protection provided in this mode. | | | | | | | | | |
| | | Off | | | | | | | | | VNAV disengages when the AC is descending, before intercepting the glide slope | | | |
| | **FLCH** | On | 5 | 4 | Crew engages FLCH when excess amount of energy | | | Crew does not press FLCH when chart requires descent and ALT is selected | | | | 6 | 3 | Crew engages FLCH before FCU (MCP) is at correct altitude |
| | | Off | | | | | | | | | | | | |
| | **VS/FPA** | On | 7 | 1 | Crew engages VS/FPA with excess thrust | | | Crew dos not press VS/FPA when FLCH VS is not enough to obey constraints | | | | 8 | 3 | Crew engages VS/FPA before FCU (MCP) is set to correct |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | target altitude |
| | | | 9 | 2 | Crew engages VS/FPA with insufficient thrust during VS/FPA descent | | | | | | | | | |
| | | Value | | | Crew does not select correct VS/FPA value | | | | | | | | | |
| | | Toggle VS/FPA | 10 | 3 | Crew selects VS when intending to select FPA | 11 | 2 | Crew dos not use VS/FPA when FLCH VS is not enough to meet constraints | | | | | | |
| | **APP/Land** | On | 12 | 4 | Selecting APP prior to ATC clearance | | | | | | | 13 | 3 | Late activation of Approach/ Land mode before ideal point to intercept glideslope or localizer |
| | | Off | 14 | 3 | APP/Land mode is unintentionally disengaged after pushing | | | | | | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | selector again above 1,500 RA | | | | | | | | | |
| **Lateral path on Autopilot** | **LNAV** | On | 15 | 3 | Crew selects NAV below 50 ft AGL and expects it to engage | | | | | | | 16 | 3 | Engaging NAV while not on intercept track |
| | | Off | | | | | | | | | | | | |
| | **HDG HOLD** | On | 19 | | Crew selects heading select when intending to select heading hold | | | | | | | 20 | 3 | Crew selects heading hold when intending to select heading select |
| | | Off | | | | | | | | | | | | |
| | | Toggle Heading | 21 | 3 | Crew selects track hold when intending to select heading hold. | | | | | | | | | |
| | | Toggle Track | 22 | 3 | When under vectors | | | | | | | | | |
| | **LOC** | On | 23 | 3<br>4 | Engage LOC when AC is under vectors flying outbound | 24 | 1.<br>1<br>3 | LOC not engaged when aircraft (AC) passes ideal turning point | | | | 25 | 1<br>.<br>1<br>3 | Engaged too late when there is high intercept angle, and AP is unable to |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | capture without overshoot |
| | | Off | | | | | | | | | | | | |
| | **Bank Limit** | Set Manual | 26 | 3 | Too low bank angle may cause intercept path overshoot | | | | | | | | | |
| | | Set Auto | | | | | | | | | | | | |
| **Throttle** | **Thrust Levers** | Select TO/GA | 27 | 5 | Pressing TO/GA button after touchdown (it is inhibited) | 27 | 15 | Not pressing TO/GA when approach is unstable | 28 | 3 | Pressing TO/GA after raising the nose, when the speed is too low | | | |
| | | | 29 | 1 | Pressing TO/GA after raising the nose | | | | | | | | | |
| | | Set Climb Power | 30 | 1 | Pressing TO/GA when a GA is not intended | 31 | 2 | Not selecting climb power in a climb when AC has low energy | 32 | 2 | Selecting cruise power prior to TO/GA | | | |
| | | Set Idle | 33 | 2 | Not pressing TO/GA when approach is unstable | 34 | 3 | Overriding auto-throttle may cause excess thrust available on touchdown | | | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Deploy Reverse | | | | 35 | 3 | Crew does not select reverse thrust when required, for example, on a slippery runway. | 36 | 3 | Possible debris ingestion when thrust reversers are deployed at low airspeed | | | |
| | | Stow Reverse | | | | | | PF does not stow reverse below 60kt | | | | | | |
| | **A/T Arm** | Arm | | | | 37 | 3 | Crew does not arm A/T during final approach | | | | | | |
| | | Off | | | | 38 | 3 | Crew does not select auto-throttle off when after ideal point to reduce to idle | | | | | | |
| | **A/T Master** | On | | | | | | | | | | | | |
| | | Off | | | | | | | | | | | | |
| | **CLB CON** | On | 39 | 1 | PF does not stow reverse below 60kt | 40 | 2 | Crew does not select CLB CON when required. | | | | | | |
| | | Off | | | | | | | | | | | | |
| | **IAS/Mach Toggle** | Set IAS | 41 | 1 | Crew does not select auto- | | | | | | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | throttle off when after ideal point to reduce to idle | | | | | | | | | |
| | | Set Mach | 43 | 2 | Crew selects CLB CON when not required. | | | | | | | | | |
| Flight Director | **Left Seat F/D** | On | | | | | | | | | | | | |
| | | Off | | | | | | | | | | | | |
| | **Right Seat F/D** | On | 46 | 3 | Crew selects one F/D on and one off, causing A/T to maintain HOLD mode | | | | | | | | | |
| | | Off | 47 | 3 | Crew selects F/D off during GA | 48 | 3 | Crew disconnects autopilot but leaves one or both flight directors on, leaving last selected autopilot modes engaged. | | | | | | |
| **Flaps** | **Up** | Select | 49 | 3 | Crew sets Flaps up when speed is low during a GA<br><br>Crew selects | 50 | 1 | Crew does not select flaps up after GA | | | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | flaps up inadvertently | | | | | | | | | |
| | **T/O** | Select | 51 | 1 | Crew selects flaps up with negative rate when GA | 52 | 3 | Not incrementally adding flaps on approach when speed is low | | | | | | |
| | **Landing** | Select | | | | | | | | | | | | |
| | | Select | 53 | 1 | Crew selects flaps to landing with speed above limits | 54 | 3 | Crew does not select flaps down before landing | | | Crew selects flaps down prior to reaching maximum flap speed. | | | |
| | | | | | | | | | | | | | | |
| **Spoilers** | **Spoiler Control Lever** | Retract | 55 | 1 | Crew retracts the spoiler when the speed is still high | 56 | 1 | Crew does not retract spoilers when speed drops | 57 | 2 | Leaving spoilers deployed when speed is low | | | |
| | | Arm | | | | 58 | 3 | Crew does not set to arm before landing on short runway | | | | | | |
| | | Deploy | 59 | 2 | Unintentional airborne stowing | 60 | 1 | Crew does not deploy spoilers when AC has too | 61 | 3 | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | much energy for the profile | | | | | | |
| **Landing Gear** | **Gear Select Lever** | Up | 62 | 1 | Crew selects gear up before positive rate of climb observed. | 63 | 1 | Crew does not select gear up after positive rate during GA | | | | | | |
| | | Down | 64 | 1 | Crew selects gear down before reaching maximum gear speed | 65 | 1 | Crew does not lower the landing gear below 1000ft | | | | 66 | 4 | Crew lowers the landing gear too soon, when the AC is expected to fly maintaining altitude |
| **Pitch** | **Yoke** | Increase Pitch | 67 | 1 | Crew overrides stall protection system by providing excessive force on the yoke | | | | | | | | | |
| | | Decrease Pitch | 68 | 1 | Crew reduces g below 0 when pitching down in altitude transitions | | | | | | | | | |
| **Roll** | | Increase Bank | 69 | 1 | Crew increases the bank angle above limits | | | | | | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Decrease Bank | | | | | | | | | | | | |
| **Yaw** | **Rudder Pedals** | Increase Yaw | 70 | 3 | Crew uses excessive yaw command on the pedals | | | | | | | | | |
| | | Decrease Yaw | | | | | | | | | | | | |
| **Trim** | **Trim Wheel** | Trim Nose Up | | | | | | | | | | | | |
| | | Trim Nose Down | 71 | 3 | Automation trims down at low altitudes | | | | | | | | | |
| **Brakes** | **Toe Brakes** | Set | 72 | 3 | Crew breaks too strong to vacate the runway on a specific taxiway | 73 | 3 | Crew does not provide adequate braking force when autobrake is disengaged | 74 | 3 | Crew lands with brake pressure on | | | |
| | **Minimums Knob** | Set Minimums | | | | 75 | 3 | Crew does not select minimums when a there are mountains close to the flight path (CFIT) | | | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Altimeter** | Set Local Pressure | | | | 76 | 3 | Crew failing to select local pressure after passing transition altitude may cause inaccurate altimeter readouts | | | | | | |

**Appendix E**
**Crew STPA Step 4**

| UCA # | UCA | Scenarios | Constraint |
|---|---|---|---|
| Example | Engaged too late when there is high intercept angle and AP is unable to capture without overshoot | PM shares attention with phraseology and reading IFR procedures and forgets to press LOC before the ideal turning point | LOC must be selected with anticipation enough to avoid overshoot of Localizer by more than 1 dot |
| 1 | Crew engages Profile Mode (VNAV) before descent path is properly programmed (configured) | One of the pilots believe the descent is already setup | Pilots need to check navigation profile before engaging VNAV modes |
| 2 | Crew engages Profile Mode (VNAV path) that violates ATC clearances or published altitude restrictions | Crew loaded wrong IFR procedure due to miscommunication with ATC<br><br>Crew loaded the procedure that they know is the most common for that runway | Crew must engage the correct App plate informed by ATC |
| 3 | Crew arms Profile Mode (VNAV) below 400 ft AGL and expects Profile Mode (VNAV) to engage | Crew reverts to a different vertical mode to avoid cloud or birds and wants to resume to VNAV | Below 1000ft, once reverted to different vertical mode, VNAV shall not be re-engaged |

| | | | |
|---|---|---|---|
| 4 | Crew engages Profile Mode Speed (VNAV SPD) in descent when target speed is set too low, no stall protection provided in this mode. | Crew selects this mode this mode to reduce the speed faster during descent | Crew have to adjust target speed before engaging VNAV SPD |
| 5 | Crew engages FLCH when excess amount of energy | crew believes that FLCH descent ratio is limited by Terminal speed | Crew must adjust VS to avoid exceeding speed limits |
| | Crew does not press FLCH when chart requires descent and lower ALT is selected | Crew prepares to descent, but get distracted and misses the ideal point to press FLCH | Crew must engage FLCH with anticipation enough to keep the AC within charts limitations |
| 6 | Crew engages FLCH before FCU (MCP) is at correct altitude | Crew wants to change altitude ASAP | Target altitude must be selected before FLCH |
| 7 | Crew engages VS/FPA with excess thrust | Crew selects descent and forgets to reduce throttle | Throttle must me reduced during descent to avoid over speed |
| 8 | Crew engages VS/FPA before FCU (MCP) is set to correct target altitude | Same as 6 | |
| 9 | Crew engages VS/FPA with insufficient thrust during VS/FPA descent | Crew reduces VS when the speed is high. They leave the throttle in idle because it is necessary to decelerate, but forget to set thrust when target speed is achieved | Throttle must be adjusted to target speed during VS/FPA descent |

| | | | |
|---|---|---|---|
| | Crew does not select correct VS/FPA value | During turbulence, the selection and reading of VS is more difficult | Any change in VS/FPA must be verified by both pilots |
| 10 | Crew selects VS when intending to select FPA | Both selections are on the same dial and there is a range where numbers could be the same, differing only by a dot | Crew must select correct mode |
| 11 | Crew dos not use VS/FPA when FLCH VS is not enough to meet constraints | Crew does not know FLCH is not going to meet constraints because ND is in PLAN mode rather than MAP mode so no green arc is displayed for the distance to MCP altitude | |
| 12 | Selecting APP prior to ATC clearance | Crew wants to prepare the aircraft to intercept ILS as early as possible, but engaging APP early may cause deviation from intended course due to localizer secondary lobes | Crew shall not select APP before ATC clearance |
| 13 | Late activation of Approach/Land mode before ideal point to intercept glideslope or localizer | Crew has low situational awareness of ideal turning point due to intensive ATC communication with other AC | APP/Land mode must be engaged before ideal turning point to intercept localizer |
| 14 | APP/Land mode is unintentionally disengaged after pushing selector again above 1,500 RA | Crew faces situations of high turbulence | Crew must check AP mode after severe turbulence |
| 15 | Crew selects NAV below 50 ft AGL and expects it to engage. | | |
| 16 | Engaging NAV while not on intercept track | Crew believes the AC will curve to intercept NAV track and it never happens | AC must be convergent to NAV track before engaging NAV |

| | | | |
|---|---|---|---|
| 19 | Crew selects heading select when intending to select heading hold | because pilot does not perceive the differences in symbology | Pilots must be sure that the heading hold is selected when required |
| 20 | Crew selects heading hold when intending to select heading select | same as previous | same as previous |
| 21 | Crew selects track hold when intending to select heading hold. | because crew is leaving a holding pattern and forgets in the previous mode | same as previous |
| 22 | Crew toggle to track mode when under Vectors | Crew believes system is in HDG | Crew must verify AC response after the end of turns to check if stopped turning at the correct heading |
| 23 | Engage LOC when AC is under vectors flying outbound | Crew wants to anticipate the selections before base leg or turn | Crew must select Loc only when inbound (difference from heading and LOC course below 90 degrees) |
| 24 | LOC not engaged when aircraft (AC) passes ideal turning point | the PF is flying with AP disengaged and believes that the PM already selected LOC | The PF must verify the selected modes when assuming the controls |
| 25 | LOC engaged too late when there is high intercept angle and AP is unable to capture without overshoot | PM splits attention between ATC communication and reading IFR procedures and forgets to press LOC before ideal turning point | LOC must be selected with anticipation enough to avoid overshoot of Localizer by more than 1 dot |
| 26 | Too low bank angle may cause intercept path overshoot | Same as previous | PM must verify selected bank angle during the turn using this mode |

| | | | |
|---|---|---|---|
| 27 | Pressing TO/GA button after touchdown (it is inhibited) | Pilots are trained to press TO/GA in every missed approach. If the decision happens after touchdown, crew presses TO/GA expecting the engine to accelerate and FD to revert to TO/GA mode<br><br>Pilot Flying decided not to press the GA button<br><br>Pilot pressed the wrong button<br><br>Button malfunction<br><br>Pilot did not press strong enough<br><br>Crosswind and turbulence deteriorate response in pitch<br><br>Software programmed to inhibit GA when there is weight on wheels<br><br>Personal Flight Display processor with a long delay<br><br>System not showing the symbology for the GA mode on the screen<br><br>PM says the approach is stable because he/she is not checking all parameters | Crew should not press TO/GA after touchdown |

| | | | |
|---|---|---|---|
| 28 | Not pressing TO/GA when approach is unstable | After fluctuations of parameters, crew feel comfortable to continue with landing, avoiding the consequences of a missed approach, including extra work reporting to operations and the negative impact on their reputation<br><br>Upon receiving a TCAS RA to descend because there is an AC behind and higher, crew executes a regular GA procedure because they remember that they are supposed to GA, but they do not remember that they need to accelerate until 180 kt before climbing. | Crew must GA when approach is characterized as unstable<br><br>pilots need to accelerate to a minimum of 170kt before climbing when the intruder of an RA is behind during approach |
| 29 | Pressing TO/GA after raising the nose | Crew initiate pitch movement and delays to press TO/GA and accelerating the engines, letting speed to drop below Vapp | TO/GA and engine acceleration must happen before significate pitch movement |
| 30 | Pressing TO/GA when a GA is not intended | PF unintentionally presses GA when squeezing the throttle levers in situations with severe turbulence. The approach shall be continued, but FD cues will be incorrect. | TO/GA should not be pressed inadvertently |
| 31 | Not selecting climb power in a climb when AC has low energy | Crew leaves the throttle at intermediary position because pilots believe that the auto-throttle is engaged | The visual cue of auto-throttle engagement must be checked by the crew every time that a change in engine setting is performed |
| 32 | Selecting cruise power prior to TO/GA | Pilots believe that the use of TO power in an early GA is too disruptive | Pilots must follow the procedures using TO power in every GA |

| | | | |
|---|---|---|---|
| 33 | Not pressing TO/GA when approach is unstable | PF (Pilot Flying) decides to Go Around and, by mistake, presses the A/T disengagement button instead of the TO/GA switch. This button in B777 is at the same position as the GA button in the PF previous operational aircraft | The crew must press TO/GA when the approach is unstable |
| 34 | Pressing TO/GA after raising the nose, when the speed is too low | The crew presses the A/T by mistake | Crew needs to be trained to observe the mode changing during the GA pitch up |
| 35 | Overriding auto-throttle may cause excess thrust available on touchdown | Pilots unintentionally presses climb under severe turbulence | Pilots must react fast to unintentional commands or execute a conservative GA to avoid the excess of energy |
| 36 | Crew does not select reverse thrust when required, for example, on a slippery runway. | Crew decides do GA because the misaligned touchdown may result in losing directional control, hitting illumination poles | Any GA below 50ft must be manual, without expecting the PFD to show a target attitude |
| 37 | Possible debris ingestion when thrust reversers are deployed at low airspeed | Crew believe it is not necessary | Reverse thrust must be selected in all wet landings or landings in short runways |
| 38 | Deploy reverse during flare before touchdown | Crew believes that debris ingestion is not a problem because the runway seams clean | Pilots must close the reverse below 20kt |
| 39 | PF does not stow reverse below 60kt | Crew believe that the mechanical protection would avoid the deployment | Pilot should not apply reverse before touchdown even when there is a mechanical lock |

| | | | |
|---|---|---|---|
| 40 | Crew does not arm A/T during final approach | Crew believes that upset recovery should be conducted with A/T OFF rather than A/T ARM and A/T disconnected with switches on thrust levers | Pilots must follow the procedure trained in the simulator for upset recovery |
| 41 | Crew does not select auto-throttle off after ideal point to reduce to idle | Pilot in transition from modern aircraft believes that idle will occur automatically | All pilots operating this aircraft must select idle after crossing the runway threshold |
| 42 | Crew selects CLB CON when not required | Pilot selects CLB inadvertently after glide capture | Pilots should not rest their hands in the throttle pedestal when the A/T is engaged |
| 43 | Crew does not select CLB CON when required. | Crew believes FLCH is the pitch mode in use | Crew must monitor speed decreases in every transition that involves pitching up |
| 46 | Crew selects one F/D on and one off, causing A/T to maintain HOLD mode | One of the pilots believes the other already did it | All CRM call outs must be communicated out loud |
| 47 | Crew selects F/D off during GA | crew wants to return to a higher level of automation | Crew must flight manually after a GA until selecting a new navigation profile |
| 48 | Crew disconnects autopilot but leaves one or both flight directors on, leaving last selected autopilot modes engaged | Crew take over in a critical flight condition to perform a recover maneuver | After disengaging the AP, the PM shall verify the accordance between F/D |
| 49 | Crew sets Flaps up when speed is low during a GA | Crew performs a memorized procedure, not giving time for the AC to accelerate or inverting the order of the procedures | Crew must wait for the A/C to accelerate to Vapp+30KIAS before setting flaps to up |

| | | | |
|---|---|---|---|
| 50 | Crew does not select flaps up after GA | Crew starts communicating with ATC and forgets to set flaps to up, causing the AC to continue descending | After coordinating with ATC, crew shall re-start the checklist from the beginning |
| 51 | Crew selects flaps up with negative rate when GA | Crew performs a memorized procedure, not giving time for the AC to accelerate or inverting the order of the procedures | Crew shall wait for a positive climb rate before setting retracting flaps |
| 52 | Not incrementally adding flaps on approach when speed is low | crew forgets to increment flaps position due to high workload in the cockpit | Crew needs to monitor the angle of attack to evaluate the timing to increaser the flaps setting |
| 53 | Crew selects flaps to landing with speed above limits | Crew has excess of energy and spoilers can't be used and any pitch up becomes a FOQA event | Pilot shall anticipate speed reduction to avoid situations with excess of speed |
| 54 | Crew does not select flaps down before landing | Crew forgets to set flaps to landing due to the high workload of a final approach, causing a long landing with potential runway overrun | There must be a CRM call out to verify if the landing configuration is complete at 500ft AGL |
| 55 | Crew retracts the spoiler when the speed is still high | Crews try to keep a higher speed to be faster and more efficient during approach | The spoilers shall be used to loose energy in accordance with Flight Ops orientation |
| 56 | Crew does not retract spoilers when speed drops | Crew forget to retract the spoiler (there is no checklist item to retract spoilers) and the aircraft present a buffeting and signs of stall | Pilots shall be trained to always check if the spoiler is retracted before lowering the landing gear |
| 57 | Leaving spoilers deployed when speed is low | Crew forget to retract the spoiler (there is no checklist item to retract spoilers) and the aircraft present a buffeting and signs of stall | Pilots shall be trained to always check if the spoiler is retracted before lowering the landing gear |

| | | | |
|---|---|---|---|
| 58 | Crew does not set to arm before landing on short runway | Crew does not trust the equipment to deploy the spoilers only after WoW | Crew must set the spoiler in Arm before landing on any short runway |
| 59 | Unintentional airborne stowing | Crew accidentally hits the switch while egressing the seat to use the bathroom | The cockpit must have a protection cover to the critical flight controls |
| 60 | Crew does not deploy spoilers when AC has too much energy for the profile | Crew tries to perform a faster and more efficient approach by keeping a higher than normal speed | The Flight Ops shall determine key speed limits to avoid the excess of energy during final approach |
| 62 | Crew selects gear up before positive rate of climb observed. | Crew perceives that the AC is close to the ground and retracts the landing gear to reduce drag and accelerate faster | The crew must keep the landing gear down until reaching at least 50ft ABL with a positive rate of climb |
| 63 | Crew does not select gear up after positive rate during GA | Crew performs a memorized procedure and forgets to retract the landing gear | Crew must retract the landing gear as soon as the vertical speed becomes positive during GA |
| 64 | Crew selects gear down before reaching maximum gear speed | Crew does not read the speed limit of the landing gear, or considers the wrong speed, when using the landing gear to increase drag | The speed limit of the landing gear must be memorized and respected |
| 65 | Crew does not lower the landing gear below 1000ft | Crew tries to lower the landing gear as late as possible to be more efficient and misses the 1000ft limit | Pilots must plan to have the landing gear down and locked before crossing 1000ft AGL |
| 66 | Crew lowers the landing gear too soon, when the AC is expected to fly maintaining altitude | Crew uses the extra drag of the landing gear to reduce speed, but the ATC commands a holding pattern to the AC | The reduction of speed above 3000ft ABL must be made using spoilers |

| | | | |
|---|---|---|---|
| 67 | Crew overrides stall protection system by providing excessive force on the yoke. | Crew pull up at low speeds to avoid collision with drone, balloon, or flock of birds | Crew must respect the speed shaker and the stick pusher to maintain the AC under control |
| 68 | Crew reduces g below 0 when pitching down in altitude transitions | PF wants to pitch down promptly after ATC authorization to descend to avoid becoming above GS | Transitions involving pitch down must be careful, mainly during turbulence |
| 69 | Crew increases the bank angle above limits | Crew loses situation awareness or PF gets spatial disorientation flying IFR with turbulence | Both pilots must focus on the PFT during turns in IFR with turbulence |
| 70 | Crew uses excessive yaw command on the pedals | Crew misuses the pedals while correcting for crosswinds while landing | Pilots need to fly coordinated, keeping pedals within a limited range during the final approach for landing |
| 71 | Automation trims down at low altitudes | Failures in the AC automation system cause a pitch down movement at lower altitudes | Pilots must be trained to use the pitch trim cut-off in simulator trainings |
| 72 | Crew over-controls yaw when correcting heavy crosswinds | Crew brakes too hard to vacate the runway on a specific twy | Crews should not modulate braking to vacate a runway on a specific spot, compromising the whole operation due to a tire blowout |
| 73 | Crew does not provide adequate braking force when autobrake is disengaged. | Crew trusts the autobrake system and takes too much time to react when it fails | Both pilots must be ready to take over when the auto brake system fails |
| 74 | Crew lands with brake pressure on | Crew keeps pressure to the top of the pedals without realizing | Pilots must change the position of their feet upon landing to be sure that the top of the pedals does not have pressure |

| | | | |
|---|---|---|---|
| 75 | Crew does not select minimums when a there are mountains close to the flight path (CFIT) | Charts of IFR procedures of airports surrounded by mountains have more altitude limitations than in other places | Pilots must be trained in the sim to face the most complicated situations in the most complicated environment |
| 76 | Crew failing to select local pressure after passing transition altitude may cause inaccurate altimeter readouts | Crew forgets to change the altimeter setting at the Transition Altitude | Crews must adjust the altimeter before crossing the Transition Altitude |