MONITORING SAFETY DURING AIRLINE OPERATIONS:

A SYSTEMS APPROACH

by

Andrea Scarinci

M.E. Aeronautical Engineering, Politecnico di Torino, 2013
M.E. Aeronautical Engineering, ISAE-SUPAERO Toulouse, 2013
B.S. Aeronautical Engineering, Politecnico di Torino, 2011

SUBMITTED TO THE DEPARTMENT OF AERONUATICS AND ASTRONAUTICS IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
June 2017

Signature of Author: ____
Department of Aeronautics and Astronautics
May 12, 2017

Certified by: ____
Nancy Leveson
Professor of Aeronautics and Astronautics and Engineering Systems
Thesis Supervisor

Accepted by: ____
Youssef M. Marzouk
Associate Professor of Aeronautics and Astronautics
Chair, Graduate Program Committee

[Page intentionally left blank]

ABSTRACT

Flight Operation Quality Assurance (FOQA) programs are today customary among major airlines. Technological progress has made it possible to monitor more than 1000 parameters per flight. Given the limited amount of resources an airline can allocate to analyze this amount of data, a need has emerged for more effective approaches to extract useful information out of FOQA programs.

A new approach to flight data monitoring and analyzing is presented in this thesis, with the intent to help air carriers identify unsafe system behavior during operations. This new approach builds on two main concepts: hazard analysis based on system theory (STPA - System Theoretic Process Analysis) and hazard management through assumptions identification and leading indicators.

STPA is a new hazard analysis technique that allows taking into account not only hardware failures, but also human behavior, requirement flaws, organizational aspects and non-linear component interactions. Once hazard scenarios are identified, mitigation actions are put in place to deal with these hazards, and the assumptions that lie behind these mitigation measures are made explicit. The objective is to define key parameters that allow monitoring the validity of the assumptions through the use of FOQA data. These parameters are called leading indicators.

The use of the flight data monitoring approach presented in this thesis is particularly beneficial when it comes to monitoring human behavior since humans are the part of the system on which the greatest number of assumptions is made (respect of procedures, knowledge of automation, situational awareness etc.). Moreover, by linking assumptions identification to FOQA data it is possible to continuously monitor whether the mitigation measures put in place are really effective or not. In other words the loop between the design phase of a system and its operations is closed.

Thesis Supervisor: Nancy Leveson
Thesis Author: Andrea Scarinci
Title: Professor of Aeronautics and Astronautics

ACKNOLEDGEMENTS

Now that this part of my "MIT journey" is ending, I feel the need to thank the people that have contributed to making these two years such an amazing experience. Without their support, advice, sympathy, warmth, friendship, love and kindness I would have never been able to reach this goal.

First of all, my sincere gratitude goes to my advisor, Professor Nancy Leveson, whom I had the fortune to meet and work with, without whose guidance and teachings this adventure wouldn't have been possible. Thank you, Nancy, for encouraging me to keep pursuing my interests and giving me the opportunity to make my dreams come true. You got me fascinated by research and convinced me I belonged in this place a lot more than I initially thought.

I would also like to thank those who have made my life easier and pleasant in the department. I am particularly grateful to Dr. John Thomas for his precise and practical advice, which has always been very useful and has surely helped me to avoid many mistakes.

Thank you Meghan for your friendship. It has certainly been reassuring to know I had someone I could share so many interests and thoughts with.

Thank you David. You have been an incredible friend throughout these two years. Not only because you put up with my laziness at the gym, but also because of your sympathy and genuine kindness.

Thank you Diogo, my favorite pilot, irreplaceable Portuguese teacher and "elder brother", for giving a helping hand whenever I needed it.

A special thanks goes to Carlos Lahoz for his suggestions on how to develop some of my research ideas and for contributing to making my last summer's stay in Brazil a really exceptional experience.

Thank you Alex for your friendship, for sharing with me your passion about airlines and for all the interesting discussions about America.

Many thanks go to all the professionals I encountered during my various excursions into industry in these two years: Ricardo, Felipe, Amanda and Danilo, who made my experience at Embraer such a rewarding one; Capt. Gus Larard, for all the interesting insights he shared with me into the world of piloting today; Capt. Alessandro Giusti, for sending me that very first email that literally got my research started; Capt. Stewart Harro and all the FedEx people I worked with, hoping that our cooperation will grow stronger.

My stay here wouldn’t have been so special without Mildred and Francesca. Thank you very much for being such good friends. You have been very patient with me and with my long midnight chats. You have made my life more cheerful and provided very precious support, which has helped me to grow as a person.

Finally, a big thanks goes to my family. Mamma, papà, Silvia, if it hadn’t been for your perseverance and love I would have probably never made it so far from those foggy Italian hills where I was born and that I still often think about.

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF ACRONYMS

A/C	Aircraft
A/P	Auto-Pilot
A/T	Auto-Thrust
ATC	Air Traffic Control
CATS	Crew Activity Tracking System
EASA	European Aviation Safety Agency
F/D	Flight Director
FAA	Federal Aviation Administration
FADEC	Full Authority Digital Engine Control
FAF	Final Approach and Fix point
FCOM	Flight Crew Operating Manual
FCTM	Flight Crew Training Manual
FDAP	Flight Data Analysis Program
FDM	Flight Data Monitoring
FLCH	Flight Level Change
FMC	Flight Management Computer
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
FOQA	Flight Operation Quality Assurance
G/S	Glide Slope
GPU	Ground Power Unit
HAZOP	Hazard and Operability analysis
ICAO	International Civil Aviation Organization
LI	Leading Indicator
MCP	Multipurpose Control Panel
NASA	National Aeronautics And Space Administration
ND	Navigation Display
NOTAM	Notice to Airmen
NTSB	National Transportation Safety Board
PAPI	Precision Approach Path Indicator
PF	Pilot Flying
PM	Pilot Monitoring
SID	Standard Instrument Departure
STAMP	System Theoretic Accident Model Process
STPA	System Theoretic Process Analysis
TOGA	Take-Off Go-Around (thrust)
V/S	Vertical Speed

1

INTRODUCTION

1.1 Motivation

Today, data collection and monitoring during operations is considered a key element of any safety management plan [DOT, 37] [FAA, 13]. Improvements in recording and storage devices have drastically increased the number of parameters that can be observed. The main objective is to learn from experience: detect early signs of major problems and correct them before accidents occur.

ICAO (Annex 6, Part 1, Chapter 3) requires every operator of an airplane of a maximum certificated take-off mass in excess of 27,000 kg to establish and maintain a flight data analysis program as part of its safety management system. The Federal Aviation Administration (FAA), through its Advisory Circular 120-82 [12], has provided guidelines on how to implement such monitoring system by defining what is known as the Flight Operational Quality Assurance (FOQA) program.

The EASA as well, in its Commission Regulation (EU) No 965/2012 [11], requires each operator to: “establish and maintain a flight data monitoring (FDM) system, which shall be integrated in its safety management system, for airplanes with a maximum certificated take-off mass of more than 27,000 kg” and that “the flight data monitoring system shall be non-punitive and contain adequate safeguards to protect the source(s) of the data.” Consequently, a coordination group has been established to provide guidelines and good practices on how to implement a FDM (flight data monitoring system). FDM and FOQA are sometimes also referred as FDAP (flight data analysis program).

Given this need, enormous progress has been achieved in terms of data collection. QAR (Quick Access Recorders) together with FDRs (Flight Data Recorders) have increased the number of available parameters to collect. While only 280 parameters are available in an Airbus A330, up to more than 1000 can be monitored in latest generation aircraft like the Airbus A380 and the Boeing 787 [Campbell, 6].

A significant number of tools have also been developed to store and visualize these data. NASA has been developing since 1993 an Aviation Performance Measuring System (APMS) to foster FOQA programs. These first efforts included graphic viewers, automatic report generation, animations etc. However, it soon became clear that collecting and storing data is not the only (and certainly not the major) problem in the attempt to identify those accident precursors that constitute the ultimate aim of the entire FOQA program. The NASA space shuttle project was collecting 600 metrics per month right before the Columbia accident [23]. Unfortunately, none of those helped the engineers in understanding what was about to happen.

Similar issues are experienced by airliners today. Chidester [35], from the NASA research space center, states: “While the available technologies for managing and processing data have improved dramatically, FOQA programs have moved only minimally beyond the analysis of exceedance”. Exceedance analysis is the primary technique adopted to perform FOQA data analysis. It consists in identifying hazardous “events” that need to be monitored during operations and building a set of parameters that model these events. When the parameters exceed a certain threshold, the hazardous event has occurred i.e. the system has entered an unsafe state. Exceedance events are the equivalent of what are known in the safety filed as leading indicators (or accident precursors). Since the number of data collected everyday has increased, it has become more difficult for FOQA analysts to define useful events and also to interpret them correctly.

In fact, most of the contextualization of the evidence coming from collected data has to be done “manually”. Experts need to look at the data signaled by the software and check through other contextual data (for that specific flight or day) to determine whether a significant safety risk is really present or not. This activity is obviously highly time consuming and because the resources airlines can allocate to FOQA analysis are limited, the result is that a lot of the collected data is simply ignored. A large international airline reported downloading 45GB of data per week of which only “a small fraction is used”.

Statistical and data-driven methods have also been applied to the FOQA analysis problem. These techniques can be useful in detecting anomalies by first establishing the profile of a “nominal” flight or a set of “nominal” flights, and then mathematically identifying outliers (i.e. flights whose profile is significantly different from that of the nominal ones). These methods do not require a problem to be known in advance before being detected (as opposed to exceedance analysis), but still show some limitations. The problems found are not clearly contextualized and extensive expert analysis is required after detection to understand causality patterns.

The research presented in this dissertation focuses on the improvement of exceedance analysis. As explained in detail in the following chapter, the biggest shortcoming of this approach is the lack of a powerful hazard analysis technique to support it. Hazard analysis is needed in order to understand “what” has to be looked for in the data and “why”. The “events” normally used when applying exceedance analysis are too basic. Particularly, they do not target some of the most relevant issues faced in piloting today: human-automation interaction. More meaningful and contextualized parameters or combination of parameters need to be identified to target specific issues such as mode confusion, policy compliance etc.

The research problem addressed in this thesis can therefore be framed as follows:

Exceedance Analysis for FOQA data requires preventive identification of hazards and associated parameters to monitor their occurrence. Given the rapid increase in the amount of data recorded by on-board computers, it has become more and more difficult to achieve the desired insight both in terms of quantity of issues detected and quality. Current FOQA data analysis approaches lack a model to which the identified issues can be referred in order to achieve better contextualization and causality identification. How can all of these aspects be improved?

1.2 Research Approach

The research presented in this thesis proposes a new approach to FOQA data analysis. Particularly, traditional exceedance analysis is improved. The new methodology helps identify the so called “events” that need to be detected during flight operations and is articulated around two main concepts:

- The use of STPA, a new hazard analysis technique: STPA (System Theoretic Process Analysis) is a hazard analysis technique derived from a new accident causality model based on systems theory. It allows predicting unsafe system behavior not only due to individual component failures, but also dysfunctional non-linear interactions between components, flawed human-system interactions as well as organizational aspects (currently overlooked by exceedance analysis);

- Assumption-based identification of leading indicators: instead of building FOQA events directly from the hazard scenarios, leading indicators are derived from the assumptions that lie behind any mitigation measures put in place to deal with the identified hazards (assumption-based engineering).

The hypothesis made in this thesis is the following:

Hypothesis: *Generating the hazard analysis through STPA (i.e. by referring to a precise controller/controlled process model of the system) together with the concepts of assumption -based engineering allows establishing a process for the identification of leading indicators ("events") for FOQA data analysis.*

In the remaining of this thesis, this new approach is also referred to as STAMP-based approach or systems approach to FOQA data analysis.

1.3 Thesis Outline

The thesis is articulated as follows:

- **Chapter 2 - Background:** state of the art relative to the FOQA data analysis techniques; literature review on leading indicators; limitations of current accident causality models; introduction to STAMP as a new accident causality model and derived hazard analysis technique (STPA), introduction to assumption-based leading indicators;
- **Chapter 3 – A Systems Approach to FOQA data analysis:** description of the characteristics of the proposed new STAMP-based data monitoring methodology;
- **Chapter 4 – Examples and applications**;
- **Chapter 5 – Conclusions**.

2

BACKGROUND

2.1 FOQA DATA ANALYSIS TECHNIQUES: STATE OF THE ART

The FAA Advisory Circular 120-82 [12] deals with many aspects linked to the FOQA program: its implementation, the actors involved, the technology selection, data collection and transmission modalities etc. When it comes to the *Data Analysis* part, two main analysis techniques are identified: exceeding analysis and statistical analysis.

2.1.1 FAA circular on FOQA data analysis

Exceedance analysis: The airline is supposed to identify a list of parameters to be monitored that should never exceed a certain threshold during operations. These parameters are usually derived from the company operating standards and relate to aspects such as speed limits during a given phase of the flight, pitch angle values, flaps position etc. The intent is to identify the occurrence of specific events such as late landing configuration, pitch high during landing, low power on approach etc.

A list of “events” to be monitored is provided in the FAA circular [12]. These events can sometimes include the combination of more than two parameters. As an example, the event “late landing configuration” is triggered based on the values of three parameters: height above touchdown, landing gear position and flap position. According to regulations, only 88 flight parameters per 25 flight hours need to be recorded [FAA, 14] and airlines can then build specific events based on these parameters.

Thanks to the enormous progress made in recording devices, however, airlines tend to monitor a lot more parameters with the specific aim of defining a more and more precise flight envelope pilots will have to fly within. The strategy pursued is that of standardizing flight operations in order to increase their safety level. In other words, fewer decisions left to pilots' discretion, reduces the possibility of making mistakes. The circular also recommends that after one of these events is detected, further investigation is conducted to understand the dynamics of the occurrence (e.g., by interviewing the crew).

Statistical analysis: statistics can be used for two main purposes: 1) establish standard/nominal flight profiles to compare the performance of single flights; 2) detect specific trends in flight operations that may signal safety concerns. A typical example is the modelling of the approach phase to detect unstable approaches at specific airports. Once the model is established, statistics are used to point out whether there are currently significant deviations from the standard path. In this sense, statistical techniques can also be used to point out deficiencies in training programs and/or policies and provide an opportunity to review them.

2.1.2 Other Analysis Techniques

While the concept of exceedance analysis is quite clearly defined by the authorities, a lot of margin is left on how to actually implement the statistical approach. Also, both the FAA and EASA state that the analysis techniques presented in their documents constitute a way, but not *the only* way to implement a valid FOQA program. A certain amount of literature has therefore emerged trying to identify innovative techniques that aim at developing more insightful approaches to FOQA data analysis. Most of these techniques tend to differentiate themselves from the exceedance analysis approach and are based on the concept of "anomaly" identification.

Li et al. [26] have proposed an approach in which multivariate cluster analysis is applied to distinguish "anomalous" flights from nominal ones. This approach goes beyond the need to identify single parameters and relative thresholds to monitor. While with exceedance analysis a problem needs to be known before looking at the data to countercheck its occurrence, the authors claim here that the relevant parameters to look at will automatically emerge from the cluster analysis. Flights that are outliers will be analyzed by experts and the parameters that brought the flight out of the clusters will be identified as a consequence. Of course, a flight will still need to be modelled through a vector of parameters whose choice will imply assumptions about which parameters are relevant to the analysis.

Another interesting approach is the one offered by Budalakoti [3]: the idea is to identify anomalous situations by monitoring the sequence of values assumed during the flight by some discrete parameters that correspond to the position of specific switches in the cockpit. One of the most interesting findings was that cases of mode confusion were identified by detecting repeated and anomalous cycling between autopilot modes (different autopilot buttons).

Das et al. [8] have applied a data mining technique to identify accident precursors: Multiple Kernel Anomaly Detection. Again, a flight is modelled through a set of discrete parameters (pilot inputs) that influence the overall aircraft state (represented through a fixed number of continuous parameters). The types of anomalies identified included a go-around, the extension of landing gears before flaps, gusty winds, a landing with flaps not fully extended and an “abnormal” approach. Most of the issues described in the paper, though, were classified by the domain expert as not necessarily safety related (e.g. go-around is abnormal, but not unsafe). This means the algorithm can actually detect anomalies (within the scope of the model generated through the selected parameters), but expert interpretation is still necessary to understand whether a safety issue is present or not. Data mining acts here as a filter, but contextualization is still needed.

In another work, Gorinevsky et.al. [16] use multiple variable regression to fit FOQA data. Deviations are then identified by comparing the same data to the model built with the regression. The anomalies found relate to abnormal values of angles of attack, accelerations, aircraft gross weight, elevator oscillations, elevator and aileron bias, etc. No specific information, however, is provided on the actual significance of these discrepancies from a safety point of view. This means that while they certainly represent a numerical anomaly, further actions are required to understand their exact nature. In some cases, the anomalies have been reported to disappear after some flights without any record of maintenance actions performed by the airline. These kinds of occurrences point out that spurious anomaly detection (due to computational reasons, for example) can also affect this kind of methodology.

A radically different approach was proposed early in the days of the FOQA program by Callantine [5]. The analysis is focused on pilots’ interaction with the cockpit instrumentation and on possible errors they can commit. The intent is to help interpret FOQA data in order to disambiguate pilot errors from other causes and detect error-inducing contexts. The methodology, called Crew Activity Tracking System (CATS), was in fact born in the context of supporting training programs because it allows a “real time” analysis of pilots’ actions. The process starts by first building a model of the specific operation or scenario that the airline wants to analyze (e.g. approach, descent). State space variables associated with this scenario are identified (e.g. altitude, speed, autopilot modes etc.) together with relative constraints. These could come from operational limitations, airline policies or from ATC instructions.

The second step in the process is to build a model of all possible actions the pilot could take to perform a specific function within the scenario identified. In CATS the model takes the form of an AND/OR tree that articulates the function into low level pilot actions (e.g. pulling speed brakes, engage an autopilot mode). Given the state variables, constraints and the mapping of all possible pilot's actions, FOQA data is then analyzed through an algorithm that detects any discrepancies from what has been established as the nominal scenario(s).

Once an anomaly is detected, the analyst will be immediately capable of referencing the context in which it occurred (the constraints and options available will be clearly displayed). In this sense, CATS differs radically from statistical and data-mining approaches, while it aligns more with the exceedance analysis philosophy. The context is clearly identified prior to actually looking at recorded data, which allows for easier interpretation of the occurrence. Obviously, the accuracy and level of detail of the modelling will greatly influence the results as well as the computational load.

A comparison has been done by Das et al. [7] between data-driven methods (cluster analysis and multiple kernel) and traditional exceedance analysis methods. The overall conclusion is that there is no single method that encompasses all of the results the other methods produce based on the same set of data. In other words, there is never complete overlap. Exceedance analysis requires previous hazard analysis in order to identify possible risks/problems that need to be monitored. This implies a better contextualization of data and therefore an easier interpretation of the events detected. However, the authors claim, only known problems are looked at, i.e. if the analysts are not aware of a specific issue they will not define an associated exceedance event and thus the problem will be overlooked.

Data-driven techniques are presented as more suitable to find “new issues” because mathematical treatment of the data will automatically select the anomalous flights. The authors also point out that this approach has the advantage of better distinguishing between rare occurrences and real problems that affect more than a limited number of flights. A drawback of this aspect, though, is that if a problem is recurrent enough for the algorithm to detect it as “normal”, it will not appear among the anomalies.

2.1.3 Conclusions and research gap

All of the techniques presented so far try to address two main issues of flight data monitoring: quantity of collected data and interpretation of this data within the appropriate context. The key problem is therefore to understand which parameters need to be collected and how they have to be interpreted in order to obtain useful information to prevent accidents.

Although a comparison of benefits and disadvantages of currently available techniques has already been presented by Das et al. [7], the list is now recapitulated and integrated with the objective of precisely defining the problem being addressed through the STAMP-based approach presented in this thesis (Table 1). Exceedance analysis appears to present more significant/meaningful results in terms of issues discovered because experts can directly refer them to familiar contexts. However, given that the main purpose of the FOQA program is to identify accident precursors, i.e. accidents/incidents before they occur, the biggest open question for this methodology remains how to identify hazardous behavior and increasing risk in a more structured way, rather than simply relying on accumulated knowledge.

Data-driven methods, on the other hand, although more straightforward in their implementation, lack contextualization once anomalies have been detected by the algorithm. Experts need to carefully review the results to evaluate whether a real issue is present or not.

Exceedance Analysis	Data-driven methods
Strengths	
Allows detecting very specific issues and complex events	Do not need preliminary safety assessment to identify possible risks/issues
Findings are well contextualized/easier to interpret	Not only known problems are identified
Allows monitoring both continuous and discrete data	Compare flights among them
Not computationally heavy	Can detect anomalous trends in variation of continuous and discrete parameters within a single flight
Weaknesses	
Needs preliminary safety assessment to identify possible risk/issues	Lack of contextualization;
Safety assessment can be time/resource consuming;	Findings are limited by the parameters considered in the model (must be few to avoid excessive computational burden);
Only known problems are identified;	Deep expert analysis required to understand significance of anomalies reported by the algorithm;
Does not allow comparing a flight with all other flights, but only flights with modeled events.	Recurrent errors might go undetected

Table 1 - Exceedance analysis vs Data-driven methods comparison

Additionally, when specific trends are identified as affecting multiple flights, or an anomalous trend has been spotted within the duration of a single flight, almost no clues are offered to identify the cause of the singularity. The macroscopic view offered by these methods though is certainly beneficial to detect specific issues.

The approach proposed in this paper stands more on the exceedance analysis side because the ultimate objective is to identify specific events (mostly identifiable through parameters with associated thresholds) to monitor though FOQA data. No statistical or data-mining techniques are applied. The new element of the methodology proposed is related to how these events are actually identified, a process that normally represents the most difficult part (and thus limitation) of exceedance analysis.

2.2 LEADING INDICATORS: THEORETICAL BACKGROUND AND INDUSTRY USE

This section discusses the concept of leading indicator (LI), a concept that has been widely used in many industries (Chemical, Mining, Oil and Gas, Shipping etc.) [1, 20, 31, 36] and that has been the object of an extensive discussion in the academic world [10, 15, 17, 18, 19, 21, 22, 23, 29, 30, 32, 33]. LIs are important for the purpose of this thesis as they constitute the basis of exceedance analysis for FOQA data.

The best way to deal with a hazard is, of course, trying to eliminate it, but this is not always possible. It is therefore necessary to adopt other hazard management strategies, which means either mitigating the hazard consequences or reducing its frequency as much as possible [Øien, 29]. A number of mitigation measures can be put in place to address both aspects, however the question is left of whether they are actually effective. One way to keep the safety level of a system under control is to use Leading Indicators (LI).

This section is divided in two sub-sections. In the first one, a review of current scientific research around LIs is provided, while the second sub-section contains an industry perspective.

2.2.1 Review of current scientific literature

Øien [29] discusses the theoretical foundations of LIs. The main concept presented, which also justifies the whole effort of identifying LIs, is that many times after an accident occurs, investigations show a number of “warning” signs that could have been identified in advance about the incoming mishap. If properly managed, they would have helped in avoiding the accident. Looking for LIs therefore means looking for these “early warning signs” or “accident precursors”.

The national academy of Engineering identifies LIs as precursors i.e. “conditions, events or sequences that precede and lead up to accidents” [33]. This definition includes some core concepts behind the idea of a LI: 1) LIs are not the outcome of an accident, but something that precedes it and represents a “potential” threat; 2) LIs can be events or sequences of events or simply a specific state the system may end up in before the accident. Both elements can fit in a variety of causality models, including the classical Swiss cheese model (Reason 1990) or Domino model (Henrich 1932). LIs can therefore be considered as the “ingredients” of an accident, although, most of the time, they result in a near miss or incident rather than actual harm.

Corcoran [33] describes accidents as situations in which, together with the “precursors,” some “exacerbating” factors occur to produce the real loss. In other words, LIs do not reach the threshold necessary to create an accident, but identify a situation very close to it. As a matter of fact, most of the times an accident takes place, it is possible, with the benefit of hindsight, to identify similar situations that had occurred in the past, but those had not been considered as “warning signs” significant enough to act upon. This is the case of the Concorde: according to Corcoran [33], nearly a half-dozen events had occurred during take-off with foreign objects on the runway or tire-burst. Similarly, many other Boeing 777s had entered into the same auto-thrust mode that led to the crash-landing of Asiana flight 214 [NTSB, 27].

Aside from the effort of establishing a definition of a leading indicator (which still is the object of debate within the safety community [Øien, 29]), researchers have also focused on strategies to identify LIs.

Leveson [23] distinguishes between LIs that mainly relate to the technical aspects of a system and those that mainly relate to organizational aspects.

On the technical side, one approach is to try to identify indicators starting from actual accident/incident reporting systems [Øien, 29]. However, some limitations exist with respect to this strategy, the main one being that only known problems are taken into consideration. In addition, it would be desirable not to wait until an accident takes place before acting upon its causes. James Bagian [33] says: “There are numerous sources of information about hazards and risks. The challenge becomes determining how to prioritize reports and what to do with the information. […]. In determining action to be taken, it is essential to look at the root causes and contributing factors that led to an undesirable condition or event. There is seldom a single cause. A thorough analysis of underlying causes can provide insight into the problem and a basis for taking steps to correct or prevent the problem”. For this reason, as Øien [29] pointed out, there has been a shift from this simple re-active approach, towards a more pro-active approach. In other words, organizations have tried to predict possible hazardous scenarios and establish appropriate indicators to monitor the progress of the system towards an unsafe state.

Leveson [23] identifies two main trends in the efforts made to predict hazard scenarios: use of probabilistic risk assessment and use of hazard analysis techniques. The use of probabilistic risk assessment has been investigated by Pate-Cornel [32] in a work about establishing the right threshold in setting LIs. A warning signal that almost never triggers does not provide reliable information on the status of the system. On the opposite side, a system that triggers too often can even become unsafe as operators may stop paying attention to it and just judge it as an unreliable source of information. The probabilistic-based approach, although mathematically sound, is not practical for those cases in which probabilistic estimates cannot be made (e.g. human behavior, design error etc.) [Leveson, 24]. The National Academy of Engineering as well warns against the high number of assumptions that lie behind this kind of analysis [33], particularly the assumption of two or more events being stochastically independent.

Aside from probability theory, a lot of use has been made of hazard analysis techniques in the attempt to capture the complex causality relations that lie behind any accident. A paper by Hale et al. [18] describes the efforts made within the safety community to model accidents, an essential step in establishing useful LIs: “The central issue for study and development has been how to model the complex relations between causal or influence factors and the events leading to accidents and how to represent the risk control measures able to prevent their development. Accidents are multilayered phenomena, with causal factors found at the technical and human level of functioning, which are conditioned by decisions at organizational, regulatory and societal levels. Many models of accidents as processes are available in the literature […] All are faced with the problem of how to conceptualize the core of the process by which the accidents occur and how to link that to the organizational and societal/regulatory tasks and actions which prevent that process from occurring”.

As a matter of fact, as Leveson also pointed out [23], all these hazard analysis techniques rely on traditional accident causality models, which do not offer the broad and systemic view of safety that is very much required in contemporary complex socio-technical systems. Leveson’s work [24] provides a path to follow, in this sense, towards a more comprehensive view of safety and accident causation. This is the view adopted in this thesis.

What is discussed so far only concerns the efforts made in identifying technical safety indicators, but, as mentioned earlier, a large literature body also exists on how to establish organizational LIs ([Kongvik, 22], [Flinn, 15]). The techniques applied in this case include quantitative risk assessment (e.g. Fault Tree, Bayesian Networks, Task Analysis). According to Leveson [23] all of these approaches lack a precise model “that specifies the causes, content, and consequences of safety culture”, where safety culture is defined by Shein [34] as the ensemble of corporate values shared by the employees and management.

Hudson [19] points out that one of the main issues in LIs programs is the difficulty of proving a “direct” causality link between what is being measured and the accident. This difficulty has two main consequences. First of all, organizations tend to focus more on what are commonly known as lagging indicators i.e. measures of frequency of occurrence of accidents and incidents [Øien, 29]. This is because their significance cannot be challenged as easily as that of a leading indicator, but, as explained by Øien [29], they are not necessarily those “pre-warning” signs that are useful in determining whether the system is migrating towards an unsafe state or not.

The second effect of establishing a poor leading indicator program is the loss of the capability of shaping the behavior of managers and workers. For the managers, when “poor” LIs are used to measure their performance, a temptation may exist to “distort” their meaning to avoid any responsibility for a bad state of things. On the workers side, issues may arise whenever the perception that the LI is not really measuring anything “useful” becomes predominant. Hudson [19] suggested that the use of control theory can solve these issues. When safety is framed as a control problem [Leveson, 24], it becomes easier to make sure that the right causal pathways are monitored and LIs can be adjusted according to the dynamic evolution of the system.

Leveson in [23] proposes an innovative view of LIs by linking them to the assumptions made during the design of every engineering system. This approach constitutes an important aspect of the solution proposed in this thesis on the improvement of FOQA data analysis. It is described in Chapter 5.

As a final remark, it is important to remember that at present there is not a large literature on rigorous validation of the effectiveness of LIs (at least in the engineering field). Some attempts have been made in the financial sector [Kaminsky, 21], [Diebold, 10], while Grabowski [17] conducted an empirical analysis of LIs of safety for an international energy transportation company concluding “individual and vessel-level LIs can provide important input to an organization's continuous safety measuring and monitoring systems”. While scientific validation of LIs is out of the scope of this thesis, it may be the objective of some future work starting from the innovative approach proposed in the following chapters.

2.2.2 An industry perspective

In this sub-section, a few examples of applications of LIs in industry are reported. The purpose of this short survey, is to show how there is still not a wide consensus on how a LIs program should be implemented. While this may depend on the fact that each field has its own needs, it appears clear that no method to identify LIs has proved itself to be good enough to become universally used.

Many organizations that have dealt with LIs have used traditional hazard analysis techniques to identify possible unsafe scenarios and associated LIs. The American Bureau of Shipping (ABS) [1] suggests a statistical approach to determine positive or negative correlation between pairs of LIs (“safety metrics”) and lagging indicators (“safety performance” parameters). The kind of metrics considered by the ABS, however, are generally “high-level” and do not enter in the operational details of the system.

Examples of safety metrics are: number of safety meetings, percentage of employees receiving communication training, percentage of crew receiving feedback on safety audits etc. These parameters are compared to lagging indicators such as the number of accidents/incidents. When a negative correlation emerges between the number of safety meetings, for example, and the number of accidents, then it is considered that a decreasing number of safety meetings will probably result in an increase of accidents. The ABS also uses this kind of statistical analysis to determine differences in safety performance between shipboard and shoreside activities. Correlation, however, does not necessarily prove causality, which means this kind of methodology could lead to erroneous conclusions.

Another approach is suggested by the International Council on Mining and Metals [20], which classifies the LIs coming out of their analysis as *quantitative LIs*. Fault tree analysis, failure mode and effects analysis, root cause analysis, procedure analysis and other tools such as control and run charts are suggested as means to validate causal pathways and also weight the contribution of each LI to the final outcome (Pareto analysis). A special note is made on statistical methodologies by the Mining and Metals Council [20]: they can be useful, but they can "induce a false sense of confidence if they are not measuring the appropriate things".

Many institutions, such as the ABS, the council of Mining and Metals and the UK Health and Safety Executive, stress the fact that LIs are also needed to "measure" socio-technical aspects of a company's organization that impact safety [1], [20], [36]. The state of the safety culture within the company is "measured" through surveys distributed to employees and management.

The role of management is emphasized by the same institutions as a key element in achieving good performance (other institutions support this idea as well [1], [20], [36]). According to the Organization for Economic Co-operation and Development (OECD) [31]: "The most important factor for achieving a safe workplace is the belief by all personnel and others involved in the operation that safety is critical". Information sharing is also identified as a key element in identifying accident precursors: often, reports about near-misses, incidents or other minor occurrences are not widely shared among all the departments of the company, making it more difficult to identify adequate LIs.

2.3 CHALLENGING TRADITIONAL ACCIDENT CAUSALITY MODELS

The greatest challenge that emerges from what is discussed in the previous sections appears to be that of predicting and tracking possible safety issues during operations. Although data-driven methods partially bypass this issue by letting mathematical algorithms detect anomalous trends in the collected data, some sort of post-detection analysis is still required to really understand the causality patterns that lay behind any incident or accident. What is needed, therefore, is a robust hazard analysis technique that allows looking at the data with more insight than has been done so far. In this section, traditional accident causality models are described as well as the assumptions underlying them. A critical view of these assumptions is also provided to better justify the choice of the hazard-analysis technique made in this thesis to address the FOQA data analysis problem.

2.3.1 Traditional accident causality models

The two most widely known accident models are Henrich's Domino Model (1931) and Reason's Swiss Cheese model. Both models assume accidents are caused by a series of concatenated events. Henrich proposes a chain of events that looks like the one shown in (Figure 1).

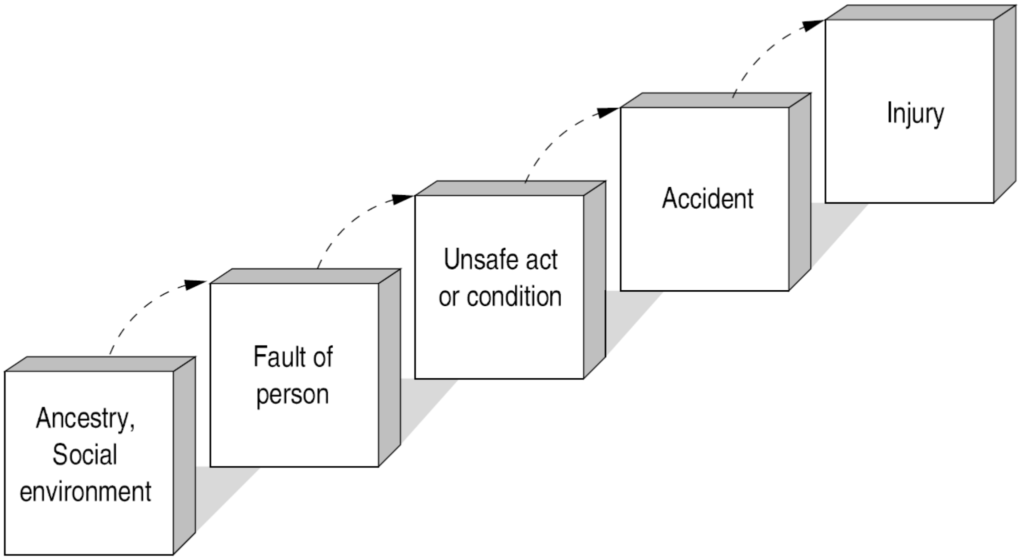


Figure 1 – Henrich's Domino Model of Accidents Causation [Leveson, 24]

The basic idea is that every accident is triggered by a staring event that induces a second event and then a third one and so on until the loss or injury occurs. Although the series of events can be long and include not only technical, but also societal and managerial aspects, it still is assumed that the sequencing is linear and that there is a single “root” cause behind every accident (i.e. the triggering event).

If an accident is preceded by a chain of failure events, then the clear solution to preventing accidents is either to prevent the events themselves or to put barriers between events so that the failures do not propagate to create subsequent failure events.

Reason’s model is a more limited form of Henrich’s model. Reason emphasizes barriers between the events. According to Reason, each of these barriers has some weaknesses or “holes in the cheese slice”. These failures remain “latent” during normal operations until specific circumstances occur so that all of the “holes” align and the accident takes place.

2.3.2 Challenging traditional models

Most of the accident causality models and hazard analysis methodologies widely spread in industry were conceived at least 50 years ago when the nature of the technical and socio-technical systems was very different from today [Leveson, 24]. Leveson, in her *Engineering a Safer World* book [24] has questioned some of the assumptions that underlie these models.

When systems were mainly electro-mechanical, most of the safety problems were related to the reliability of the single components. For this reason, reliability has long been used as a synonym for safety, although the two concepts are radically different. A system that is reliable is not necessarily safe, and a system that is safe may be highly unreliable. In the first case a system may work exactly as designed, but the interactions between its components may cause an unwanted and unsafe outcome.

Leveson [24] calls this type of accident "component interaction accidents". Many examples of component interaction accidents exist. The recent Asiana flight 214 crash in San Francisco took place because of an unintentional auto-thrust mode switch made by the pilot that led the aircraft to an unsafe state, although the autopilot worked exactly as designed (more details on this accident later).

What has been said so far is translatable to the human components of a system too: the fact that a pilot will always follow a procedure is a sign of high reliability, but this may be unsafe if no exception is made when a specific context requires it, i.e. when following the procedure becomes more important than actually analyzing the scenario. The first conclusion made by Leveson is therefore that reliability is neither necessary nor sufficient for safety.

Another important assumption that is questioned by Leveson is the linearity of the traditional accident causality models. Leveson says:

"the causal relationship between the events in the event chain models (between dominoes or Swiss cheese slices) are required to be direct and linear, representing the notion that the preceding event must have occurred and the linking conditions must have been present for the subsequent event to occur: if event A had not occurred then the following event B would not have occurred. As such, event chain models encourage limited notions of linear causality, and it is difficult or impossible to incorporate nonlinear relationships".

New hazard analysis tools should aim at going beyond this concept by acknowledging that, with the rising complexity of socio-technical systems and coupling among their components, accidents are often the result of non-linear interactions between the various elements involved (both human and non-human). The biggest problem with looking at accidents as chain of events is that there is a risk of poorly understanding all of the causal factors that lead to the loss.

Referring to the Swiss cheese model, for example, the assumption is that adding another barrier between the safe state of the system and the hazardous state will be enough to prevent future accidents. This approach, however, discounts the “systemic factors” that contributed to the accident that may affect all the cheese slices. The chain of events may look slightly different, but it presents the same problem.

An example could be that of a pilot committing an unsafe action by not respecting a specific procedure issued by the airline or the aircraft manufacturer. It would be very easy to solely blame the pilot for not acting as established in the documentation, but the right question to ask is, would another pilot have done the same thing? Or better, could this mistake be the result of a deficiency in training? Unclear wording in the documentation? Too high workload conditions? If none of these possibilities are carefully analyzed, it is very probable that the same mistake will be committed by another pilot in the future. Leveson [24] therefore concludes that: “Accidents are complex processes involving the entire sociotechnical system. Traditional event-chain models cannot describe this process adequately”.

In the next section, the theoretical foundations of the new accident causality model (STAMP) proposed by Leveson [24], and used in this thesis, are described. It is shown how it can overcome all of the issues of the previous traditional approaches discussed so far, with particular emphasis on how those systemic factors that are so important in determining the safety level of a system are accounted for.

2.4 SYSTEM THEORY APPLIED TO SAFETY: STAMP

The main objective of STAMP is to look at a system in a way that complex interactions leading to accidents can be captured as causes of accidents. As a matter of fact it is from these kinds of interactions and not simple component failures that most accidents originate today.

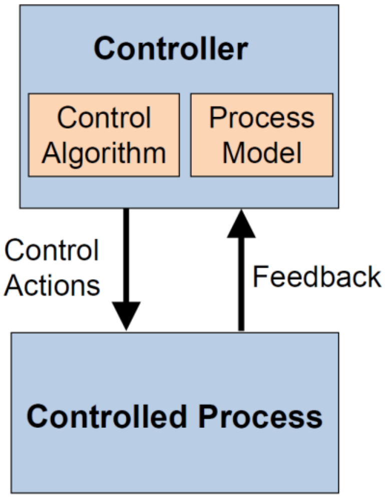


Figure 2 – Control Structure

The theoretical foundations of STAMP lie in systems theory. According to systems theory, emergent properties, such as safety, must be controlled. A controller is responsible for maintaining a given controlled process within the boundaries of what is considered an acceptable and/or desired behavior. The ways in which the controller can influence the status of the controlled process are called “control actions”, while updates about the actual current state of the process are provided through feedback mechanisms (Figure 2). Examples of controllers and controlled processes can be a pilot controlling the position of the flight-control surfaces of the aircraft or the auto-park function of a computer installed on a car and the steering, acceleration and brake controls it can command. Control actions would then be the pilot acting on the yoke or the computer sending digital commands to the car’s appropriate actuators.

The ways in which a controller makes decisions about what is the correct control action to take and when are described through the concepts of control algorithm and process model, which both characterize a controller. A control algorithm is any kind of process (e.g. rules, procedures etc.) based on which a controller selects the correct actions to take. In humans, the decision making strategies can vary from individual to individual and according to context.

Control algorithms use process models to support the decision making process. In other words, the controller needs to have a model (a mental model in the case of a human controller) of what is the current state of the system and also of how it will behave after a specific control action is provided. The process model of a controller is another key concept in understanding the STAMP approach to safety. Leveson [23] says: "the process model includes assumptions about how the controlled process operates and about the current state of the controlled process. Accidents in complex systems, particularly those related to software or human controllers, often result from inconsistencies between the model of the process used by the controller and the actual process state. The inconsistency contributes to the controller providing inadequate control". Leveson [24] describes the features a process model must have (whether it is part of a human or an automated controller) in order to be effective. The relationships among the various system variables (control laws), the current state of the system (described through a number of variables and their associated values) and the ways the process can change state.

Feedback mechanisms play an important role in updating process models. Feedback can be sensors (e.g. temperature sensors, position sensors) or reporting mechanisms in the case of the organizational components of systems. This last type of feedback is very important in determining the safety level of a system. If the management levels of a company are unaware of the exact state of the process they are responsible for (e.g. conditions of a power plant, level of knowledge of pilots in an airline), then adequate resources will not be provided to correct the situation. Hazards also arise when feedback is in place, but it provides wrong or distorted information about the process.

In STAMP there are four ways in which a controller can produce a hazard [Leveson, 24]:

- A provided control action leads to a hazard;

- The lack of a control action leads to a hazard;
- A potentially safe control action is provided too early, too late, or in the wrong sequence;
- A continuous control action is provided for a too long or too short duration.

The reasons why one of the unsafe control actions described occurred, could be traced to problems or defects in the elements of the control structure illustrated above (Figure 2). The control algorithm may be inadequate, the process model incomplete or not updated due to an issue in the feedback channel. Control actions may also simply go unexecuted due to component failure or not executed appropriately because of flaws in the execution chain. More detailed examples of how these concepts can be interpreted in a real engineering design can be found in a book by Leveson [24].

As a conclusion, it can be stated that by describing systems behavior in these terms, STAMP frames safety as a control problem. The controller, through its control actions, imposes safety constraints on the system. When these constraints are violated or simply not adequate, accidents occur. This description allows taking into account a lot more aspects that affect system safety in comparison to traditional chain of events models. As controllers and control actions can be humans, computers, organizations etc., this accident causality model is not limited to hardware component failure, but can easily capture all the non-linear dynamics of interactions among system elements. Given the use of the control-loop model, STAMP also allows “anticipating the risk-related consequences of change and adaptation [of the system] over time” [Leveson, 23]. Organizational aspects are included by making use of the hierarchical control structure concept, which is also derived from systems theory. A hierarchical control structure is made of multiple feedback control loops: an example is provided in Figure 3. The system represented was the one in place during the accident that occurred to American Airlines flight 965 from Miami (United States) to Cali (Colombia) on the 20th of December 1995. While approaching the destination airport at night, the aircraft collided with a mountain chain that surrounded the valley. Numerous causes contributed to the fatality. Some of them are summarized here below:

- While descending towards Cali, the flight crew selected the wrong waypoint in the Flight Management Computer (FMC, navigation computer), which put the aircraft on the wrong course;
- The identifier of the correct waypoint used on the paper chart provided by the manufacturer of the FMC (Jeppesen) did not correspond to the identifier used in the computer (i.e. the pilots selected a waypoint based on the information provided on the chart believing it was correct, while it was not);
- Identifier duplicates existed and pilots were not alerted of the related danger by neither American Airlines or Jeppesen;
- The Cali airport could not provide radar service that night due to a sabotage act by the FARC carried out in 1992;
- The international and national civil aviation authorities (ICAO, FAA, AEROCIVIL) did not provide clear guidelines on how the charts and FMC should be designed to ensure consistency.

The control structure helps identify and analyze the organizational elements and responsibilities that had an influence on the accident and that are often overlooked when assessing the safety of a system.

It is exactly because of this flexibility of STAMP when it comes to describing systems that this approach was chosen in this thesis to help FOQA analysis to use more complete models of the systems being analyzed.

The following section describes how a new hazard analysis technique can be derived from this model of accident causality.

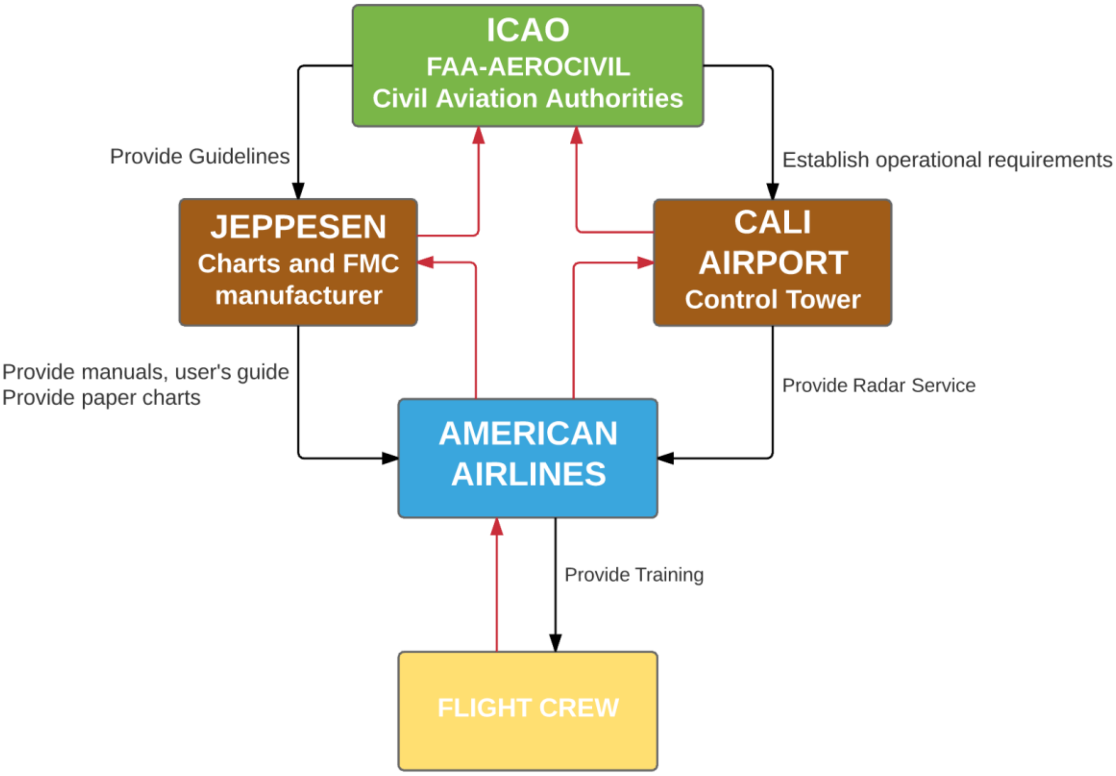


Figure 3 – Organizational control structure for American Airlines Flight 965.

2.5 SYSTEM THEORETIC PROCESS ANALYSIS

Based on the traditional accident causality models, a number of hazard analysis tools have been created in order to assess safety in a system and predict possible issues before entry into service. Among them, the most widely used are: Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), Event Tree Analysis, Failure Mode Effects and Criticality Analysis (FMECA) and HAZOP. These tools heavily rely on probabilistic risk assessment concepts that are not suitable to assess systems that make large use of software and include human operators [Leveson, 24].

STPA is different in that more causal factors can be potentially included in the generation of accident scenarios and particular attention is given to the identification of those emergent properties of a system that often result in hazards.

STPA involves:

- Identification of accidents and hazards for the system being analyzed;
- Modeling of the system by a control structure;
- Identification of possible unsafe control actions;
- Generation of causal scenarios.

Hazards and Accident Identification

The technique starts by identifying the accidents that must be avoided while operating the system. An accident is defined by Leveson [24] as **“**an undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.”

Given the accidents, the analyst then identifies the hazards i.e. “a system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss)”. Hazards are not accidents, but conditions that bring the system potentially close to accidents. The overall effort during the STPA analysis will be to make sure that enough safety constraints are in place so that the system operation does not lead to hazards. To provide a simple example, a hazard could be the temperature of a nuclear reactor rising above a certain value. Before the reactor meltdown (accident) occurs, additional conditions will be needed, nevertheless all possible controls should be put in place so that the temperature is kept under control and never rises above the established threshold.

Modeling the system as a control structure

A control structure contains controllers and controlled processes and a description of the way they interact in terms of control actions and feedback. A control structure can contain several levels of control loops and information about how they are interrelated. An example is shown in Figure 4. The flight crew controls a number of cockpit interfaces such as the yoke and rudder pedal to manually adjust the aircraft attitude (pitch, roll and yaw). The command sent by the pilots goes directly to the physical aircraft (flight control surfaces). Automation is instead activated and handled through the Flight Control Unit - FCU (or Multipurpose Control Panel - MCP) as well as the Multi-Function Control and Display Unit – MCDU (or Control Display Unit – CDU). These inputs go to the Flight Control Computer (FCC), which transforms them into appropriate signals to command the actuators of the flight control surfaces. The secondary flight controls (such as flaps, slats, spoilers), although commanded manually, are also handled through the FCC. Finally, the engines are controlled through the throttle, whose signals are almost always routed through the engine control computer (FADEC) except in few old-generation aircraft.

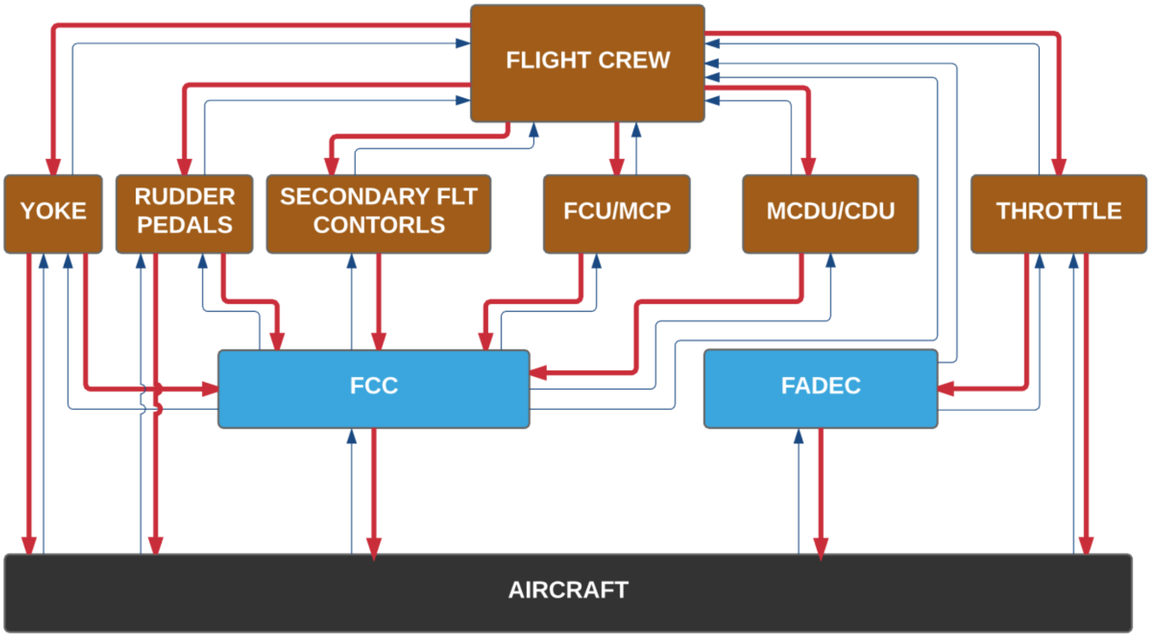


Figure 4 – Control structure of a generic Auto Flight System in a modern civil aircraft

Identification of possible unsafe control actions

Once the control structure is ready and all control actions identified, they should be analyzed to identify when they could generate possible hazards. As already stated, according to STAMP, hazards can be created when [Leveson, 24]:

- a control action required for safety is not provided or not followed;
- an unsafe control action is provided that leads to a hazard;
- a potentially safe control action is provided too late, too early, or out of sequence;
- a safe control action is stopped too soon (for a continuous or nondiscrete control action) or applied too long.

To provide a concrete example, if the control action is:

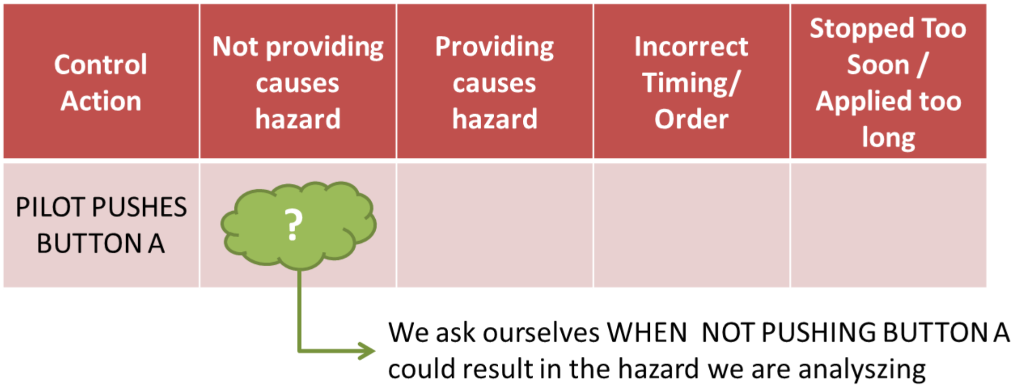
C.A. = Pilot pushes button A

Then, the questions to answer to are:

1. In which contexts would pressing button A result in an unsafe outcome?
2. In which contexts would not pressing button A result in a unsafe outcome?
3. In which contexts would pressing the button too late or too early or in the wrong sequence with respect to another action result in an unsafe outcome?
4. In which contexts would pressing button A for too long or too short result in an unsafe outcome?

The results of this process can be recorded in a table. This table contains the context under which the modeled control actions can be unsafe (Figure 5). Each of the unsafe control actions can be transformed into a safety constraint on the controller that could produce it.

As an example, if the U.C.A. is “The pilot pressed button A during landing”, then, the safety constraint for the pilot would be “The pilot must not push button A during landing”. This information can be included in manuals, training or any other appropriate means used to make sure pilots fly the aircraft appropriately. If instead of a human the controller were a computer, this would translate into software safety requirements.



Control Action	Not providing causes hazard	Providing causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
PILOT PUSHES BUTTON A	?			

We ask ourselves WHEN NOT PUSHING BUTTON A could result in the hazard we are analyszing

Figure 5 – STEP 1: unsafe control actions

Generation of causal scenarios

The information identified as a result of this step does not explain “why” a certain unsafe action might occur, it simply describes what the unsafe control actions are. While it is important to identify unsafe conditions, in order to make the system safe it is important to understand why the unsafe control actions might be generated, i.e. the scenarios that can lead to the unsafe control actions. Starting from the example of the pilot pushing button A during landing, the question to be asked is why would he or she do it? Some possible causal factors could be that the pilot is confused about the implications of pressing button A (training issues or lack of detailed content in manuals) and presses it believing the action is safe (wrong mental model). The aircraft may be providing incorrect feedback with respect to the actual position of the button (e.g. button A is a pushbutton and the only way to know whether the button has been pressed or not is whether a green light behind the button illuminates. If this light is broken, it becomes impossible for the pilot to understand the status of the button). A short-circuit may also be the cause of the button being activated even without pilot action. The causal scenarios (an example is shown in Figure 6 contain information about why the UCA could happen. These scenarios should be built looking at the control structure as a whole in order to capture as many of those unexpected non-linear interactions between system elements as possible. .

The STPA analysis generates a number of accident scenarios that need to be addressed through specific design features or mitigation actions.

Scenario: The Flight Crew does not know that there is insufficient time to safely land the helicopter given the power remaining and the amount of power being used by the mission equipment unless the amount of mission equipment is reduced. This flawed process model could result because:

a) The amount of battery power remaining is not presented to the Flight Crew.
b) The amount of power time that is remaining given battery power remaining and mission equipment on is not presented to the Flight Crew.
c) The Flight Crew is unaware of a battery low charge condition due to a failure of the battery low charge caution display.

Figure 6 – STEP 2: causal scenarios [Abrecht, 2]

2.6 ASSUMPTIONS BASED ENGINEERING AND LEADING INDICATORS

This section discusses the transition from the results of the application of STPA i.e. accident/incident scenarios, to the identification of appropriate leading indicators to monitor air operations. The basis for the following discussion come from a work by James Dewar [9] on *Assumptions-based planning* (ABP) and a paper published by Leveson [23], which draws on the ideas of ABP to create leading indicators for safety.

The first sub-section discusses what an assumption is. The second illustrates how it is possible to transition from hazard scenarios to appropriate leading indicators.

2.6.1 What are assumptions?

One of the key concepts in engineering design is that of assumptions. Every time a product or a system is conceived, there are a number of simplifications and suppositions that need to be made about how the system will work and its operating environment. Leveson [23] describes six types of assumptions related to safety:

1) Assumptions about the system hazards and the causes of the hazards. Because systems evolve as a result of the context in which they operate (technological, sociological or economical), new hazards may arise as well as related assumptions on their causality;
2) Assumptions about the effectiveness of the controls. Consider structural resistance to loads: the rudder of an airplane can be designed to resist to aerodynamic forces up to a certain magnitude. The designer is forced to make assumptions on what are the maximum aerodynamic loads this part of the aircraft will be exposed to. In some cases these assumptions may be proven wrong (American Airlines Flight 587 [NTSB, 28]). Another example could be the effectiveness of training. Training is a "control" measure with respect to operators' knowledge on how to operate a system. It is often assumed that what is taught in training will be retained by the individuals participating in it, while it is everyone's experience that this does not correspond to reality;
3) Assumptions about how the system will be operated and the environment (context) in which it will operate. Assumptions about human behavior are contained in this category;
4) Assumptions about the development environment and processes. Sometimes product defects are not due to bad design, but arise from problems during the production phase. Engineers often do not take into adequate consideration the

limitations of the manufacturing process and this results in a number of assumptions being made and then violated;

5) Assumptions about the organizational and societal safety control structure during operations. Many accidents (e.g. Überlingen [4]) demonstrate that the organizational and societal parts of a system do not always behave "as designed".
6) Assumptions about vulnerability or severity in risk assessment. Risk can change over time.

One reason why assumptions are often not monitored and therefore their violation not detected is that assumptions are usually not described in system specifications or other technical documentation. Leveson [25] proposed a specification format called "Intent Specifications" in which assumptions are explicitly stated whenever it is appropriate for a given requirement. Examples from the intent specification for TCAS[1] II include:

1.18: TCAS shall provide collision avoidance protection for any two aircraft closing horizontally at any rate up to 1200 knots and vertically up to 10,000 feet per minute.

Assumption: This requirement is derived from the assumption that commercial aircraft can operate up to 600 knots and 5000 feet per minute during vertical climb or controlled descent and therefore two planes can close horizontally up to 1200 knots and vertically up to 10,000 fpm.

1.19.1: TCAS shall operate in enroute and terminal areas with traffic densities up to 0.3 aircraft per square nautical miles (i.e., 24 aircraft within 5 nmi).

Assumption: Traffic density may increase to this level by 1990, and this will be the maximum density over the next 20 years.

Making an assumption means making an estimate about a certain aspect of the future and such estimates can be accurate or not. Assumption breaking starts be-

[1] TCAS (Traffic Alert and Collision Avoidance System) is a collision avoidance system for aircraft.

coming a problem when it is not monitored or detected and operations continue without any corrective action being taken.

2.6.2 From hazard identification to leading indicators

One of the key parts of this thesis is the criteria suggested to connect the results of a hazard analysis performed with STPA to the definition of FOQA events (i.e. leading indicators). The idea is the following [Leveson, 23]: the safety analyst performs an assessment of a specific aspect of the airline operations (e.g. a new procedure, a specific approach maneuver at an airport, the use of specific autopilot mode etc.). The result of this assessment, in STPA terminology, will be a list of possible accident scenarios i.e. identified vulnerabilities of the system. To comply with the basic principles of any safety management system, the airline will have to show reasonable mitigation measures have been put in place to abate these risks.

The nature of these mitigation measures can vary greatly, although in the specific case of air operations (piloting), they often relate to the establishment of specific procedures and/or specific pilot training content. In any case, regardless of the type of mitigation measures taken, there will still be a number of assumptions made beyond the decision of accepting that action as an adequate response to the threat identified. The idea proposed by Leveson [23] is that the identification of appropriate leading indicators should start exactly from these assumptions. As explained in the previous sub-section, the violation of assumptions is often the reason why accidents occur and therefore leading indicators should be built in order to monitor these assumptions.

The violation of an assumption constitutes a near miss as it indicates some of the safety measures put in place are not being effective. The airline will evaluate, once the violation has been detected, how to best correct the situation: change the nature of the mitigation action, invest more resources on it, etc.

To provide an example, consider the simple case of the design of the cockpit window. Among many other factors, the glass is designed to be resistant to the impact of birds during the approach phase or climb. Obviously, an assumption has to be made on what the maximum speed of the aircraft will be under a given altitude and another assumption on the altitude above which it will be unlikely to find birds flying. Figure 7 illustrates this concept.

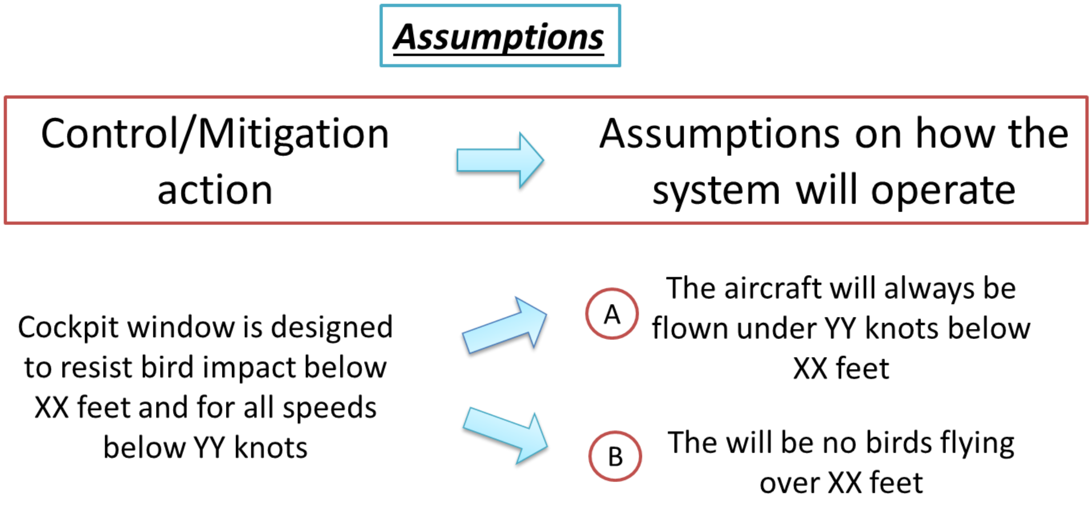

Assumptions
Control/Mitigation action
Assumptions on how the system will operate
Cockpit window is designed to resist bird impact below XX feet and for all speeds below YY knots
A
The aircraft will always be flown under YY knots below XX feet
B
The will be no birds flying over XX feet

Figure 7 – Mitigation Measures and Assumptions

Given the two assumptions it becomes straightforward to identify the leading indicators that should be defined in order to monitor them. In the first case (assumption A) a FOQA event could be easily built: raise a flag every time the aircraft flies above YY knots below XX feet. For assumption B, FOQA data cannot be used, but other alternatives exist such as pilot reports. The frequency of this event will be low enough that it is unlikely that reporting will translate into excessive workload for the crew. It is also an event that will likely attract the crew's attention anyway.

As a conclusion, an assumption-based definition of leading indicators is established by Leveson [23]:

"Leading indicator: 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 that 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”.

Based on this definition, a good leading indicators program should then be [Leveson, 23]:

- Complete: all critical assumptions leading to an accident are identified. Leveson acknowledges that, of course, full completeness is almost an unreachable objective, but all efforts shall be made to get as close to it as possible. This may translate into a very large set of leading indicators being identified and thus a process for determining what should be checked, how, and when becomes an important part of leading indicators program (this thesis attempts to provide an answer to this specific problem by suggesting a specific documentation format. See following chapters);
- Consistent: contradictions in the assumptions underlying the leading indicators need to be identified and analyzed as they are probably symptoms of a flawed design;
- Effective: the link to the associated assumptions, uncertainties, and vulnerabilities must be clear and as objective as possible;
- Traceable: each leading indicator must be clearly associated to the mitigation action put in place to address the assumptions being monitored;
- Minimal: extraneous assumptions, checks, or actions that are not necessary have to be avoided;
- Continually improving: the set of leading indicators has to be continually reviewed over time in response to feedback about its effectiveness;
- Unbiased: the process for the identification of leading indicators should avoid standard biases in risk assessment and management.

3

A SYSTEMS APPROACH TO FOQA DATA ANALYSIS

This chapter shows how a new systems approach to FOQA data analysis can be built in order to answer the research problem highlighted in chapter 1: how to define more meaningful events (leading indicators) to monitor safety during airline operations and facilitate their post-detection interpretation. Particular emphasis is put on how human-automation interaction issues can be easily captured through this approach, covering an area that is usually overlooked by traditional exceedance analysis (as well as by the statistical/data-driven approaches).

3.1 General principles

As explained in chapter 2 section 1, exceedance analysis for FOQA data presents the following issues:

1. A limited number of hazards/events are tracked (mainly based on accumulated knowledge and expertise brainstorming);

2. The kind of issues tracked tend to overlook human-automation interaction problems;
3. The lack of a model and of a clear causal analysis makes it difficult to interpret the detected events.

In order to address these three main points, the use of STPA as a hazard analysis tool is proposed in this thesis. The benefits of this new technique applied to FOQA data analysis are described in the numbered list below (numbers in this list reference the shortcoming identified just above):

1. STPA, by providing a more structured process to conduct hazard analysis, allows predicting more hazardous scenarios with comparison to what could normally be identified by simply limiting the scope of the analysis to problems that are already known and/or the results of unstructured brainstorming conducted by experts of the domain. What is learned from accidents, incidents or near-misses still needs to be included in the database of "FOQA events", but the process of expert brainstorming could be significantly enhanced with the support of this tool. Moreover, by using STPA it is also possible to set up leading indicators to monitor newly introduced modifications to the current air operations system. As an example, an airline could decide to modify the approach procedures at a certain airport: by applying STPA it would be possible to predict what could be the pitfalls that pilots may face while following this new procedure, establish appropriate mitigation actions and monitor their effectiveness. In other words, the airline would not have to wait until an accident or incident happens before taking corrective actions;
2. As explained in the previous chapter STPA allows capturing a lot more causal factors for a given hazardous scenario than traditional hazard analysis techniques. Because it is possible, through the controller/controlled-process model, to study human-machine interactions, automation-related issues could be easily addressed. Mode confusion, selection of inappropriate auto-

pilot modes during certain flight phases are areas that can be covered by the systems approach introduced through STPA. Given the capability of this hazard analysis technique to also look at the influence of organizational factors on air operations, specific FOQA events could be defined to evaluate the effect of training on pilots (e.g., are go-arounds executed at the time and in the fashion indicated by company procedures? Are pilots systematically mishandling certain off-nominal scenarios being taught during simulation sessions? And so on.).

3. Because STPA requires the definition of a control structure i.e. a precise model of the system being analyzed and the definition of causal scenarios closely linked to the various elements that compose this model, it should be easier for the analysts to contextualize the findings. Not only it is clear “what” hazardous scenario is being monitored, but also what are the possible causes that could generate it. The burden of post-detection analysis should therefore be, at least partially, reduced.

As already explained in chapter 1, however, the methodology proposed in this thesis does not end with the identification of leading indicators simply associated with the results of the hazard analysis. Airlines are required to establish appropriate mitigation measures for each potential threat identified. The traditional way of evaluating the effectiveness of these measures heavily relies on probabilistic considerations. Basically, the mitigation actions are deemed adequate when a sufficiently low probability can be associated with their failure. As discussed, this is not always a practical path to follow. As an alternative approach, it is proposed to use assumption-based hazard management (or planning), which considers instead that any control action is subject to failure if the assumptions that lie behind it are proven to be wrong (chapter 2). The issue of determining the likelihood of a failure in the safety constraint enforcement process is therefore by-passed: instead of deciding a priori whether a certain scenario is likely to happen or not, the assumptions that lie behind a given system design are identified in order to be closely monitored during operations.

Leading indicators are therefore established exactly on the basis of these assumptions. Recalling the definition by Leveson [23], a leading indicator is:

"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 that 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 process of identifying leading indicators to monitor the validity of the assumptions is straightforward when they can be directly related to a precise model of the system (like the one STPA provides). This approach (the conjoint use of STPA and leading indicators) is particularly suitable in evaluating human behavior-related assumptions. In the Asiana flight 214 accident, an inappropriate auto-throttle mode was involuntarily entered by the pilots during approach. Because the system allowed this unsafe action, the assumption made by the designers was that no crew would ever commit that mistake. Monitoring that specific mode selection may have alerted that the assumption was wrong and a dangerous use of the autopilot was current practice at Asiana (at least). The parameter, linked to a precise context, immediately puts the analyst in the right direction (more details on this case are presented in chapter 4).

The STAMP-based approach proposed in this study is therefore composed of two main parts:

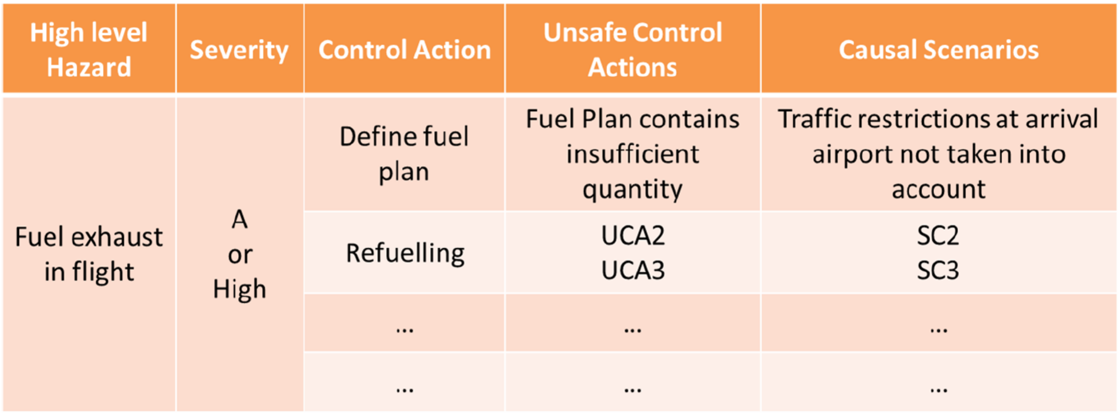
- HAZARD IDENTIFICATION through STPA: given a specific hazard (for example, aircraft over-speed run), a number of causal scenarios are identified;
- HAZARD MANAGEMENT through ASSUMPTIONS IDENTIFICATION AND LEADING INDICATORS: for each hazard scenario identified in the previous step, a mitiga-

tion action is identified. Associated with this mitigation measure, the relative underlying assumptions are made explicit and a suitable leading indicator is chosen for monitoring purposes.

3.2 Documentation

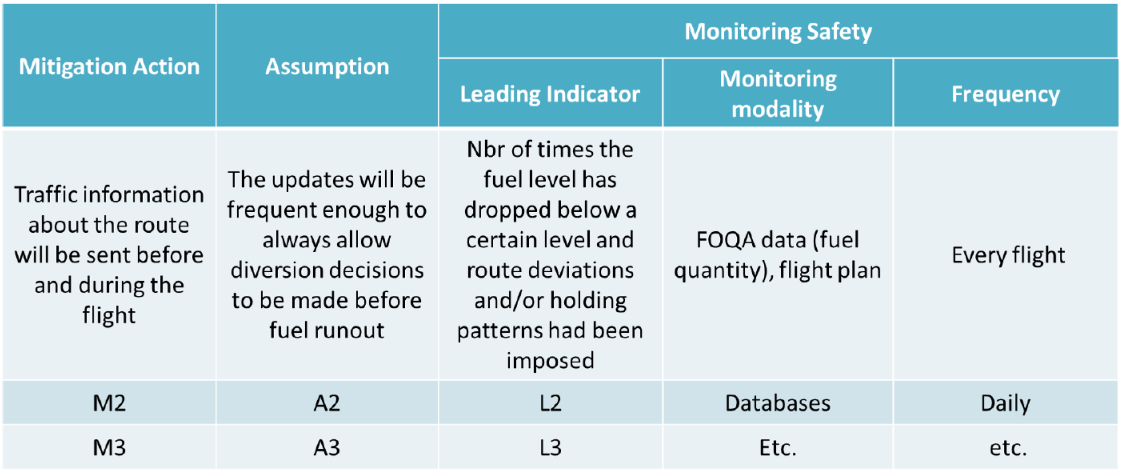
It is suggested to keep track of the whole analysis process through one single document that is organized along the lines of what are generally known as hazard-logs. The HAZARD IDENTIFICATION part of the analysis is reported as in Figure 8. The first column contains the name of the hazard to be controlled. The second column defines the severity of the hazard. This is particularly important in a real-life context in which the hazards to control are many and priorities necessarily need to be established. The third column deals with the control actions related to the hazard. The last column defines causal scenarios for the unsafe control actions i.e. why and how the unsafe control actions might occur. The goal of this first part of the document is to document in a compact format the hazard analysis process the airline has put in place.

The second part of the table (Figure 9) focuses instead on HAZARD MANAGEMENT. The first column identifies the mitigation actions the airline has put in place to avoid the causal scenarios linked to the hazard. For each of these mitigation measures, the underlying assumption is identified in the second column. Because there are no mitigation actions that are failure proof, but only some that are more likely to fail than others, this likelihood is here “tested" by monitoring the assumption validity. The third column identifies the parameter(s) or leading indicators through which this monitoring activity will be conducted. For each indicator, the modality and frequency of the data will be indicated in the adjacent columns. For FOQA data, the frequency will be every flight (or at least every flight under this program). However, other modalities may exist to monitor flight operations according to the nature of the leading indicator: surveys, performance audits, pilot reports etc. In these cases, the frequency needs to be lower for obvious reasons: cost and time.



High level Hazard	Severity	Control Action	Unsafe Control Actions	Causal Scenarios
Fuel exhaust in flight	A or High	Define fuel plan	Fuel Plan contains insufficient quantity	Traffic restrictions at arrival airport not taken into account
		Refuelling	UCA2 UCA3	SC2 SC3
		…	…	…
		…	…	…

Figure 8 – STAMP-based FOQA data analysis: Hazard Identification part



Mitigation Action	Assumption	Monitoring Safety		
		Leading Indicator	Monitoring modality	Frequency
Traffic information about the route will be sent before and during the flight	The updates will be frequent enough to always allow diversion decisions to be made before fuel runout	Nbr of times the fuel level has dropped below a certain level and route deviations and/or holding patterns had been imposed	FOQA data (fuel quantity), flight plan	Every flight
M2	A2	L2	Databases	Daily
M3	A3	L3	Etc.	etc.

Figure 9 – STAMP-based FOQA data analysis: Hazard Management part

3.3 The logistics of the STAMP-based FOQA data analysis technique

Before looking at examples and applications of the methodology proposed, this section is dedicated to discuss how a STAMP-based leading indicators program can be implemented in an industrial context i.e. the resources and process that performing this hazard management requires. The estimates presented are an estimate based on the author’s past experience with STPA and the recent ongoing applications of this new methodology.

The process of applying the new STAMP-based FOQA data program consists in the following phases:

PHASE 1 - Topic definition. The system of interest needs to be identified. There is no minimum/maximum system “size" requirement. This means as many control actions as desired can be monitored. Clearly, applying this methodology to every system and every control action part of that system can easily become unmanageable and not necessarily useful. This tool is meant to be applied to areas that require specific attention and for which other hazard analysis techniques are deficient. The length and number of subjects involved in this phase largely depend on the airline needs and policies;

PHASE 2 - Hazard analysis. The hazard analysis on the topic of choice is performed through STPA. This analysis should be carried out by the people in charge of the safety management of the airline, although, for the causal scenarios identification, it is of fundamental importance to involve the actors directly involved in the operation of the systems. The goal is to obtain valuable and realistic insight about why certain unsafe control actions may occur (rather than a simple intellectual exercise). To perform a complete STPA analysis of a function of a complex system like the auto-thrust, two or three engineers may be required together with the cooperation of a number of experienced pilots. Working full time this may take from two to four days.

PHASE 3 - Assumption and leading indicators identification. The identification of the assumptions is quite straightforward once the mitigation actions have been identified and can be performed by the engineers who led the first part of the analysis. The choice of the leading indicators is however more complex because it requires the knowledge of what is actually recordable through the FOQA program and the significance of the parameters also needs to be studied carefully. Overall, this may require an additional two to three days of full-time work and the cooperation of an expert on FOQA recordings. In case no FOQA data is available, audits, surveys or other instruments may be put in place, which may require additional time for resource identification.

PHASE 4 - Program launch and unrolling. Once the monitoring plan has been identified, a certain amount of time needs to elapse before looking at the results. The number of flights to be monitored depends on the size of the fleet of the airline adopting this methodology as well as the type of event being tracked. If the object of the monitoring is, for example, the activation of a specific autopilot mode during every landing, it will not be necessary to collect as much data as it would be when issues related to a maneuvers such as go-around are tracked (a pilot normally performs a go-around once or twice a year). When using FOQA data, it is easier to obtain significant results in a relatively short time, while longer monitoring periods are necessary when collecting data through audits, surveys or other less "automated" modalities. FOQA data is also normally stored, which means great insight, at least for certain issues, can be obtained by analyzing historic data.

PHASE 5 - Data Analysis. Once enough data has been collected, it is straightforward to verify whether the assumptions have been respected or not. Engineering judgment can be used to establish the critical number of times after which the occurrences represent a safety concern.

In summary, for a system like the auto-pilot, in order to define a hazard management plan for a specific function, a team of 2 or 3 people will be occupied for two weeks full-time. Along with these, cooperation will be required from the actual operators of the system being analyzed (pilots, ground personnel etc.).

4

EXAMPLES AND APPLICATIONS

In this chapter the reader is provided with some examples of how the new STAMP-based FOQA data analysis technique can be used to monitor a number of different issues concerning airline operations. The first four examples represent typical situations in which FOQA data can be directly used to track the identified hazards. The fifth example shows an application of the methodology to ground operations. Although the thesis addresses the FOQA data analysis problem primarily, an application is also presented where the same concept can be used in a slightly different context than air operations. As a matter of fact, it is part of the systems approach to safety underlying STAMP to not just look at a single element of a system (i.e. air operations – pilots), but at their interactions (e.g. ATC, ground operations etc.).

Before discussing the examples, a brief description of the autopilot (A/P) and auto-thrust (A/T) systems that equip all modern civil aircraft is provided. This should facilitate understanding the applications presented in this chapter.

The A/P and A/T are both activated through a button on a panel generally situated in the pilots' direct line of sight. This panel is called MCP (Multipurpose Control Panel) in Boeing aircraft and FCU (Flight Control Unit) on Airbus aircraft.

The A/P allows the pilot to set automatic management of the lateral and vertical path of the aircraft as established in the FMC (flight management computer) and/or through the selection of some specific modes. Among these, the ones used in the hazard log examples are the following:

- G/S – glide slope: maintainance of a specific descent path (constant glide angle);
- FLCH – flight level change: transition from current flight level to the one indicated on the MCP (Boeing);
- V/S – vertical speed: selection of a specific descent rate (feet per minute);

The aircraft can also be manually flown, but following the visual cues provided on the primary flight display by what is known as the Flight Director (F/D). Activation/deactivation of the F/D is achieved by setting a switch on or off on the MCP/FCU. In the Boeing design, one switch is provided for the display of the Pilot Flying (PF) and one for the Pilot Monitoring (PM).

As for the A/T modes:

- SPEED mode: the thrust (together with aircraft attitude) are managed so that a specific target speed is maintained constant;
- HOLD mode: the thrust is manually managed by the pilots;

The A/T commands specify thrust levels, corresponding to certain throttle positions (minimum or IDLE, maximum or TOGA – take-off/go-around, CLIMB level).

Refer to the acronym list at the beginning of this thesis for the definition of the acronyms used in this chapter.

4.1 EXAMPLE 1: Asiana flight 214 Crash at San Francisco International Airport

This example refers to the Asiana 214 accident that took place at San Francisco International airport on the 6th of July 2013. An extensive investigation was conducted by the NTSB on the causes of this accident and a number of vulnerabilities in the Boeing A/P system as well as in the airline policy were identified. FOQA data can be used as an instrument to monitor whether the countermeasures taken to deal with these vulnerabilities are effective or not.

-CONTEXT DESCRIPTION-

Runway 28L at San Francisco (SFO) airport was operating under visual conditions, however the G/S signal (raw-data) (normally used by pilots to conduct an approach) was not available due to a malfunction. At 15.4NM from the runway threshold, the PF intercepted the localizer. For the whole duration of the descent, the aircraft constantly remained above the glide path.

At 5NM, the A/C still was 400ft above the desired path. Therefore, the PF decided to increase the descent rate by switching to FLCH mode on the MCP. However, because the pre-selected MCP altitude was 3000ft (visual go-around altitude), the A/C started climbing. The PF reacted by disconnecting the A/P and setting the throttles to IDLE. Unfortunately, he did not notice and/or was unaware of the fact that putting the throttles to IDLE when the A/T is in SPEED mode causes a transition to HOLD mode, a mode that does not provide speed control nor stall protection.

At 2.9NM, the PM stated the A/C was still “high” and therefore the descent rate was increased to 1500ft/min. At 1000ft, the A/C was 243ft above the glide path and the PAPI[2] showed four white lights. As a consequence, the descent rate was further increased up to 1800ft/min. At 500ft above the ground, the aircraft reached correct speed and glide angle, but was descending at 1,200ft/min (while the correct V/S would be around 700ft/min). Moreover the speed was not being controlled, which means it dropped below 132kt. At 200ft, the speed was 122kt and the PAPI showed 4 red lights. The PF reacted by increasing the pitch, which results in an additional speed decrease. By 100ft the speed was 114kt. The PM realized a go-around had to be initiated and pushed both throttles to TOGA. Unfortunately, at this point, the energy of the aircraft was too low to recover from the excessive rate of descent and the aircraft impacted the seawall short of the runway. The fuselage spun 330 degrees, and the tail broke apart.

The analysis conducted by the NTSB [27] pointed out a large number of contributing factors to the accident (from fatigue to poor cockpit coordination, PF inexperience etc.). Only the few points that are relevant to the application are here reported:

1. Unhandled/Unexpected transition of the A/T from SPEED to HOLD mode (primary cause of the aircraft loosing energy in an irreversible way):
    a. The Boeing 777 FCTM states that "The use of FLCH is not recommended after the FAF point (final approach fix). However, no reason is given why such mode should be avoided, so the pilot has no incentive not to use it;
    b. The Asiana Automatic Flight System training module emphasized that a "flight envelope protection" (i.e. stall prevention) was always active even with the A/T not engaged. This led the pilots to feel relatively safe with respect to the risk of incurring a low speed configuration. The module also did not indicate that the A/T would not activate when in HOLD mode;

[2] Precision Approach Path Indicator: a set of four lights is located next to the runway. The aircraft is on the correct glide-path when two lights are white and two are red. When red lights are predominant (3/4 or 4/4) the aircraft is below the path; when the white ones are predominant then the aircraft is above the glide-path.

c. The Boeing 777 FCOM was only updated with the information concerning the absence of speed protection in HOLD mode in 2012;

d. The information was transmitted aurally by ground school instructors and presented as an "anomaly" in the B777 A/T functioning. However, it wasn't very clear in many pilots' minds that bringing the throttles to IDLE while in SPEED and FLCH mode would result in the activation of the HOLD mode;

2. F/D cycling: by analyzing FOQA data, it emerged that both the PM and the PF had cycled the F/D from ON to OFF to ON before landing and when the A/T was already in HOLD mode. The F/D cycling was common practice at Asiana, however it was never clearly specified in Boeing manuals or by Asiana instructors what the difference would be between turning both F/Ds off at the same time or not. Had the Asiana 214 pilots had their F/D off at the same time, the A/T mode would have switched back to SPEED, avoiding the tragedy;

-APPLYING THE SYSTEMS APPROACH-

All of the three points presented above are symptoms of systemic issues with responsibilities that span from Asiana to Boeing, ATC and Regulators. Assumptions were made on the unlikelihood of pilots selecting the FLCH mode during the descent. The danger of HOLD mode activation from THR mode was also underestimated (absence of speed protections). The STAMP-based methodology for FOQA data analysis could be used to establish and monitor whether the mitigation actions are being effective or not. The ultimate goal is to check whether similar situations to that of Asiana 214 are still occurring.

The first step of the analysis requires the definition of the high-level hazard that needs to be avoided. In this case, the hazard can be defined as: uncontrolled flight into terrain. The associated severity of the hazard can be chosen according to company criteria, but it can be hypothesized that, on a scale from High to Low, a High level can be chosen in this case. The second step in a STPA analysis is to draw the control structure associated with the system under study and identify all related control actions. A simple version of what could be the control structure for this case is shown in Figure 10 below (yellow lines represent control actions and blue lines feedback from the controlled entity).

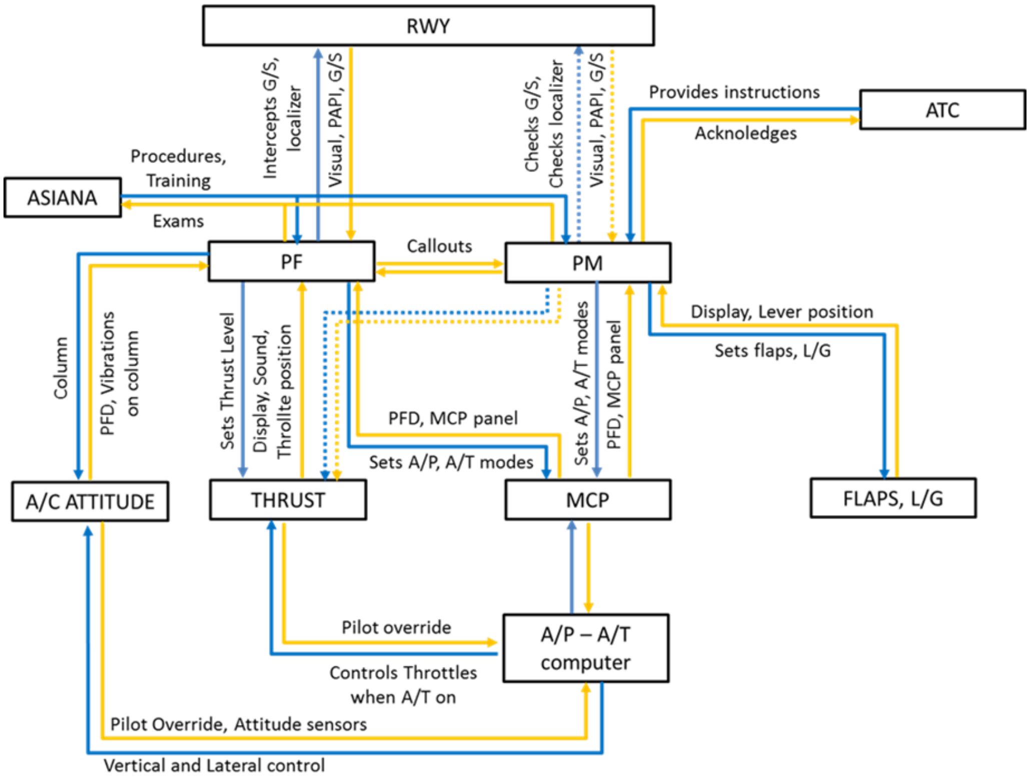
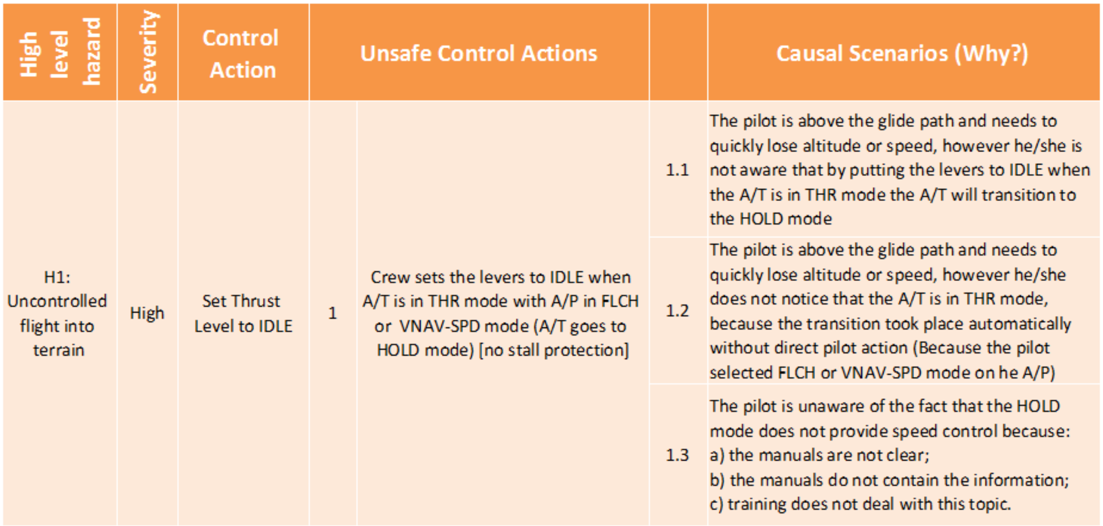


Figure 10 – Control Structure Asiana 214

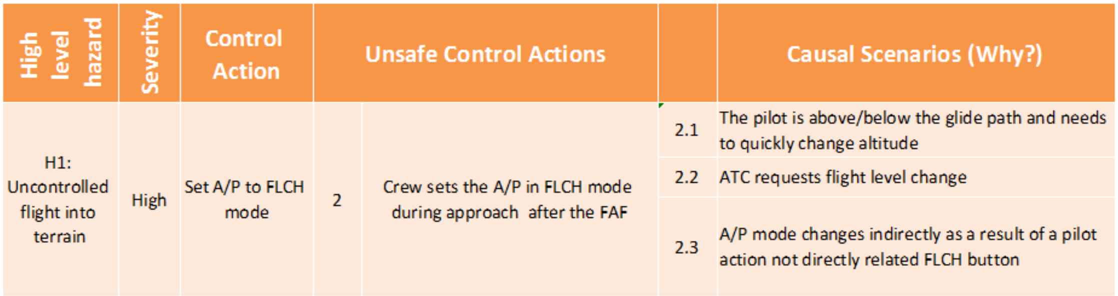
This control structure is rather complex. The control action “Set Thrust Level” from PF/PM to the Thrust Levers is the one of interest for this example. Obviously, although the expression “Thrust Level” has been used for brevity purposes, in order to perform a meaningful hazard analysis, it is necessary to specify which level is being selected by the pilots. In this example, the “Set Thrust Level to IDLE” control action is considered to perform the STPA hazard analysis. The results are reported in Figure 11.

As can be seen, both unsafe control actions and their causal scenarios are reported in the tabular form described in section 3.2. The scenarios reported in the table represent what happened during the Asiana accident (particularly scenarios 1.2 and 1.3). Another interesting control action to analyze is "Set A/P – A/T modes". Here again the FLCH mode setting control action is considered only (Figure 12). Another candidate for monitoring through FOQA data is the F/D cycling issue (Figure 13).



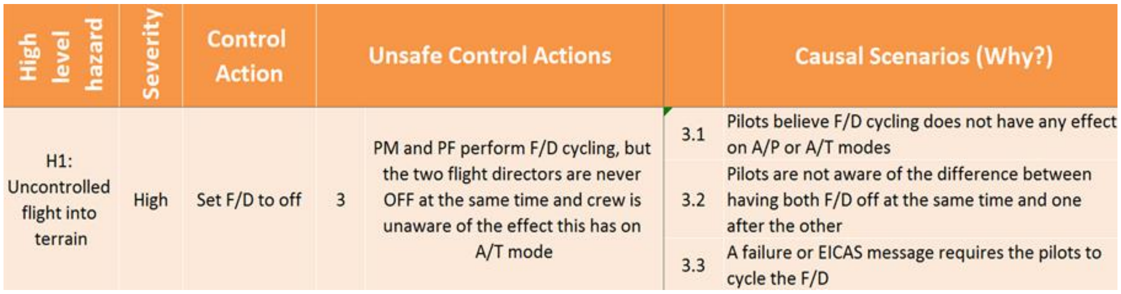
High level hazard	Severity	Control Action	Unsafe Control Actions			Causal Scenarios (Why?)
H1: Uncontrolled flight into terrain	High	Set Thrust Level to IDLE	1	Crew sets the levers to IDLE when A/T is in THR mode with A/P in FLCH or VNAV-SPD mode (A/T goes to HOLD mode) [no stall protection]	1.1	The pilot is above the glide path and needs to quickly lose altitude or speed, however he/she is not aware that by putting the levers to IDLE when the A/T is in THR mode the A/T will transition to the HOLD mode
					1.2	The pilot is above the glide path and needs to quickly lose altitude or speed, however he/she does not notice that the A/T is in THR mode, because the transition took place automatically without direct pilot action (Because the pilot selected FLCH or VNAV-SPD mode on he A/P)
					1.3	The pilot is unaware of the fact that the HOLD mode does not provide speed control because: a) the manuals are not clear; b) the manuals do not contain the information; c) training does not deal with this topic.

Figure 11 – Hazard Identification (Thrust to IDLE)



High level hazard	Severity	Control Action	Unsafe Control Actions			Causal Scenarios (Why?)
H1: Uncontrolled flight into terrain	High	Set A/P to FLCH mode	2	Crew sets the A/P in FLCH mode during approach after the FAF	2.1	The pilot is above/below the glide path and needs to quickly change altitude
					2.2	ATC requests flight level change
					2.3	A/P mode changes indirectly as a result of a pilot action not directly related FLCH button

Figure 12 – Hazard Identification (A/P mode)



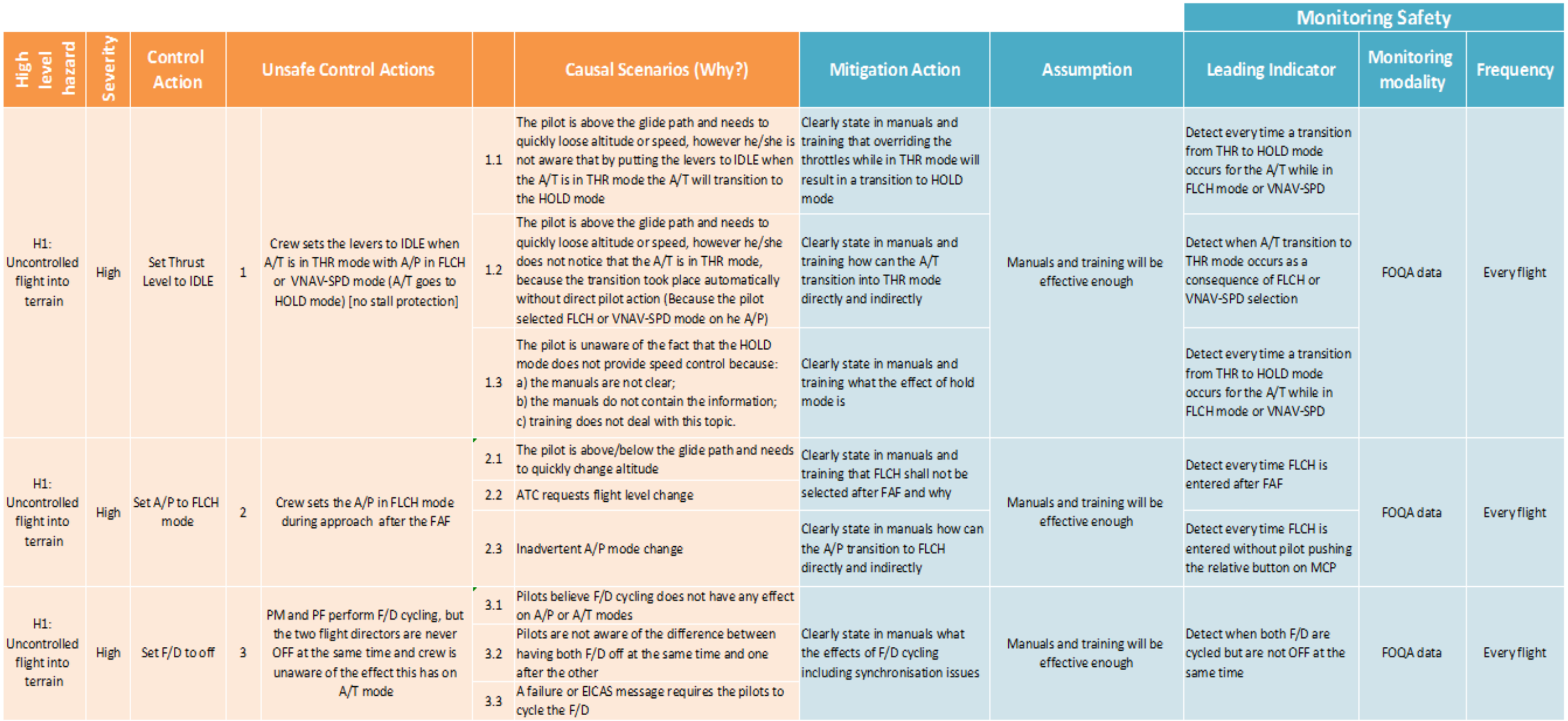
High level hazard	Severity	Control Action	Unsafe Control Actions			Causal Scenarios (Why?)
H1: Uncontrolled flight into terrain	High	Set F/D to off	3	PM and PF perform F/D cycling, but the two flight directors are never OFF at the same time and crew is unaware of the effect this has on A/T mode	3.1	Pilots believe F/D cycling does not have any effect on A/P or A/T modes
					3.2	Pilots are not aware of the difference between having both F/D off at the same time and one after the other
					3.3	A failure or EICAS message requires the pilots to cycle the F/D

Figure 13 – Hazard Identification (F/D)

At this point, the safety monitoring part of the analysis needs to be conducted. The first column of this part requires defining mitigation actions for each of the hazard scenarios identified i.e. how the airline has planned to deal with the hazard. The second column requires writing down why the subject conducting the analysis, in this case the airline, believes the chosen measure is adequate.

Figure 14 shows the results of this process. All of the mitigation actions refer to training and manuals as the airline (at least in the short term) has no means to intervene on the physical design of the aircraft and therefore “eliminate the hazard”.

The big assumption behind the establishment of any procedure, checklist or manual, as well as any training program, is that the information will be retained by the crew. FOQA data provides a means to easily check whether this assumption is true or not: autopilot modes are recorded through FOQA and a series of events can be coded in order to verify if the undesired mode is entered during the approach phase or not. The leading indicators established in this case, together with monitoring modality and frequency are also shown in Figure 14.



									Monitoring Safety		
High level hazard	Severity	Control Action	Unsafe Control Actions			Causal Scenarios (Why?)	Mitigation Action	Assumption	Leading Indicator	Monitoring modality	Frequency
H1: Uncontrolled flight into terrain	High	Set Thrust Level to IDLE	1	Crew sets the levers to IDLE when A/T is in THR mode with A/P in FLCH or VNAV-SPD mode (A/T goes to HOLD mode) [no stall protection]	1.1	The pilot is above the glide path and needs to quickly loose altitude or speed, however he/she is not aware that by putting the levers to IDLE when the A/T is in THR mode the A/T will transition to the HOLD mode	Clearly state in manuals and training that overriding the throttles while in THR mode will result in a transition to HOLD mode	Manuals and training will be effective enough	Detect every time a transition from THR to HOLD mode occurs for the A/T while in FLCH mode or VNAV-SPD	FOQA data	Every flight
					1.2	The pilot is above the glide path and needs to quickly loose altitude or speed, however he/she does not notice that the A/T is in THR mode, because the transition took place automatically without direct pilot action (Because the pilot selected FLCH or VNAV-SPD mode on he A/P)	Clearly state in manuals and training how can the A/T transition into THR mode directly and indirectly		Detect when A/T transition to THR mode occurs as a consequence of FLCH or VNAV-SPD selection		
					1.3	The pilot is unaware of the fact that the HOLD mode does not provide speed control because: a) the manuals are not clear; b) the manuals do not contain the information; c) training does not deal with this topic.	Clearly state in manuals and training what the effect of hold mode is		Detect every time a transition from THR to HOLD mode occurs for the A/T while in FLCH mode or VNAV-SPD		
H1: Uncontrolled flight into terrain	High	Set A/P to FLCH mode	2	Crew sets the A/P in FLCH mode during approach after the FAF	2.1	The pilot is above/below the glide path and needs to quickly change altitude	Clearly state in manuals and training that FLCH shall not be selected after FAF and why	Manuals and training will be effective enough	Detect every time FLCH is entered after FAF	FOQA data	Every flight
					2.2	ATC requests flight level change					
					2.3	Inadvertent A/P mode change	Clearly state in manuals how can the A/P transition to FLCH directly and indirectly		Detect every time FLCH is entered without pilot pushing the relative button on MCP		
H1: Uncontrolled flight into terrain	High	Set F/D to off	3	PM and PF perform F/D cycling, but the two flight directors are never OFF at the same time and crew is unaware of the effect this has on A/T mode	3.1	Pilots believe F/D cycling does not have any effect on A/P or A/T modes	Clearly state in manuals what the effects of F/D cycling including synchronisation issues	Manuals and training will be effective enough	Detect when both F/D are cycled but are not OFF at the same time	FOQA data	Every flight
					3.2	Pilots are not aware of the difference between having both F/D off at the same time and one after the other					
					3.3	A failure or EICAS message requires the pilots to cycle the F/D					

Figure 14 – STAMP-based FOQA data analysis - Asiana flight 214

After the accident, many airlines (including Asiana) reported that they looked at past FOQA data and discovered many of their flights had been in similar situations to that of the accident. This indicates that, if backed up by a thorough hazard analysis, FOQA data can become an excellent instrument in monitoring safety and preventing incidents/accidents.

4.2 EXAMPLE 2: FMS Malfunction

This case is inspired by a real incident that occurred at a large international airline this year.

-CONTEXT DESCRIPTION-

Airline ABC noticed that at a specific airport KYYY there is an inconsistency in the information conveyed though the ND (Navigation Display) and the F/D (Flight Director) for the SID (Standard Instrument Departure) of RWY24. Just after take-off, the flight plan contains a "conditional waypoint" of "2000A", however with this kind of waypoint the software of the ND has difficulties in tracing the exact flight path the aircraft should follow (the result of a software bug) and displays a tentative course. The tentative course is incorrect and leads the aircraft out of the SID, flying over an active military base and populated areas with noise level restrictions.

The F/D, however, gives different instructions compared to what is shown on the ND. In particular, it makes the aircraft initiate a left-turn well before the 2000A waypoint, keeping it on the SID. A company NOTAM was issued for pilots to follow the flight director and disregard the track displayed on the navigation display for this airport and this runway. The assumption made by the Airline ABC was that the pilots would retain the information contained in the NOTAM and that they would follow F/D instructions even when performing a manual take-off. A couple of months after the NOTAM was issued, Airline ABC was contacted by the ATC of airport KYYY complaining about the fact that most of the ABC flights out of the airport were not respecting the SID track, largely deviating and flying over prohibited areas.

- APPLYING THE SYSTEMS APPROACH-

The fact that the ATC of the airport contacted the airline reporting several violations is a symptom of a systemic issue that needs to be understood and addressed. In this example, it is shown how Airline ABC could use the STAMP-based methodology illustrated in this thesis as an instrument to carry out this analysis.

In this case, the aspects of the flight that need to be monitored are manually flown departures and the company rules associated with them. The analyst must perform a complete hazard analysis using STPA, although a short version of this analysis is presented given the demonstrative purpose of this document.

As before, the first step to take is the definition of the high-level hazard that has to be avoided. In this case the hazard can be defined as: unacceptable deviations from the horizontal flight path. The associated severity of the hazard is chosen to be high because flight track deviations could lead to collisions with other traffic or terrain. A simple version of the control structure for this case is shown in Figure 15. Red lines represent control actions and blue lines represent feedback from the controlled entity.

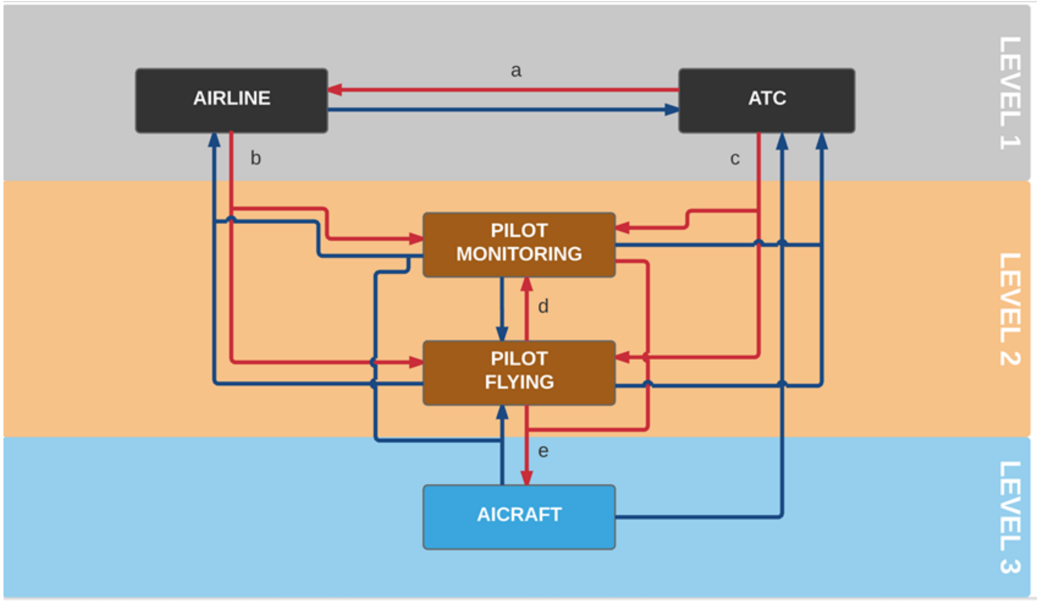
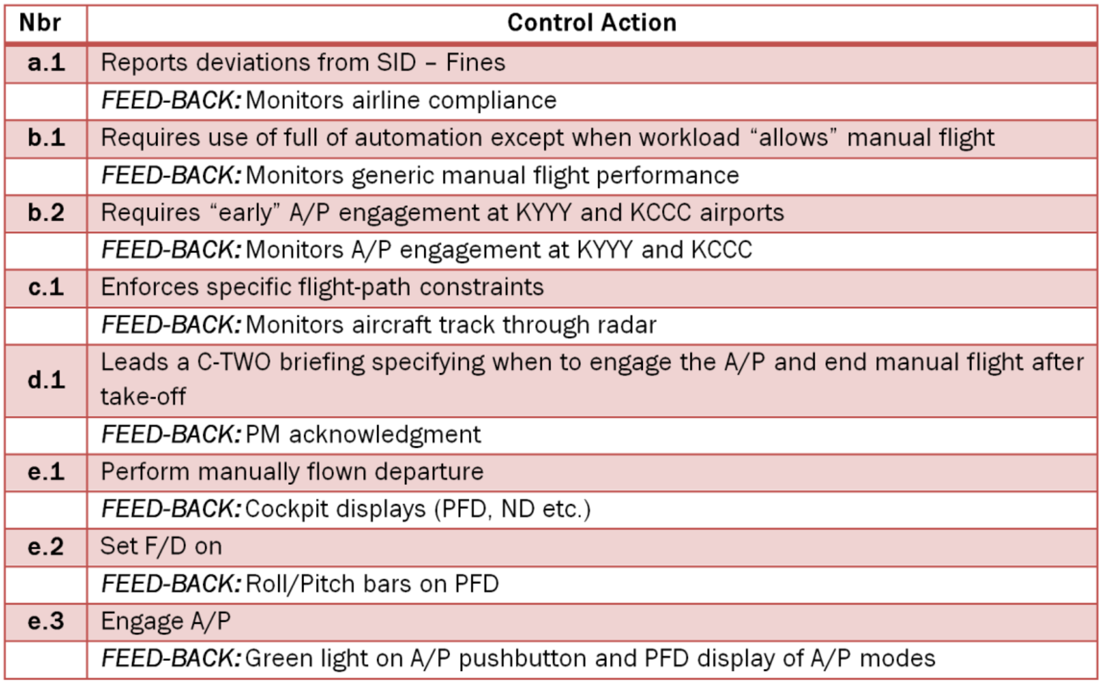


Figure 15 – Control Structure FMS malfunction

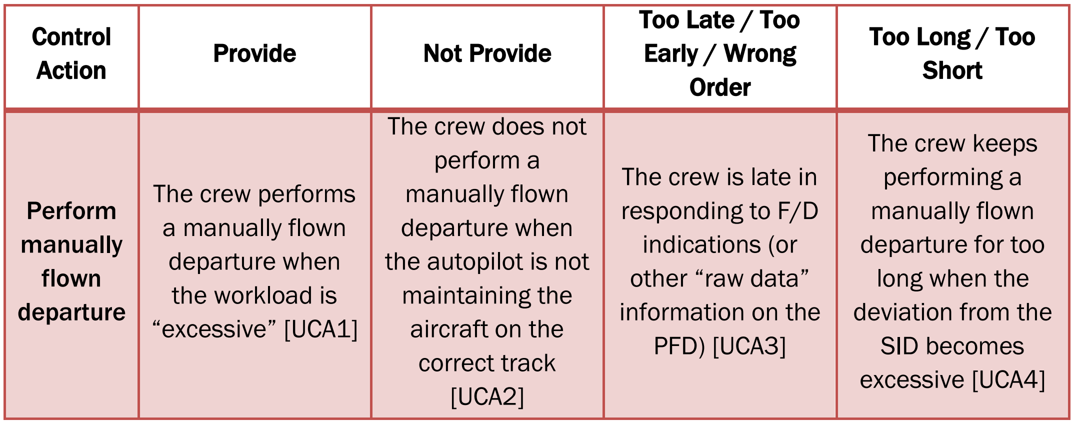
The detail of each control action can be found in Figure 16.



Nbr	Control Action
a.1	Reports deviations from SID – Fines
	FEED-BACK: Monitors airline compliance
b.1	Requires use of full of automation except when workload “allows” manual flight
	FEED-BACK: Monitors generic manual flight performance
b.2	Requires “early” A/P engagement at KYYY and KCCC airports
	FEED-BACK: Monitors A/P engagement at KYYY and KCCC
c.1	Enforces specific flight-path constraints
	FEED-BACK: Monitors aircraft track through radar
d.1	Leads a C-TWO briefing specifying when to engage the A/P and end manual flight after take-off
	FEED-BACK: PM acknowledgment
e.1	Perform manually flown departure
	FEED-BACK: Cockpit displays (PFD, ND etc.)
e.2	Set F/D on
	FEED-BACK: Roll/Pitch bars on PFD
e.3	Engage A/P
	FEED-BACK: Green light on A/P pushbutton and PFD display of A/P modes

Figure 16 – Control Actions FMS malfunction

Control action e.1 is analyzed to find out in which contexts a manually flown departure can be dangerous (Figure 17).



Control Action	Provide	Not Provide	Too Late / Too Early / Wrong Order	Too Long / Too Short
Perform manually flown departure	The crew performs a manually flown departure when the workload is "excessive" [UCA1]	The crew does not perform a manually flown departure when the autopilot is not maintaining the aircraft on the correct track [UCA2]	The crew is late in responding to F/D indications (or other "raw data" information on the PFD) [UCA3]	The crew keeps performing a manually flown departure for too long when the deviation from the SID becomes excessive [UCA4]

Figure 17 – UCA for Manually Flown Departure

UCA1 refers to an unsafe action of the crew with respect to the instructions provided by the airline i.e. not to fly a departure manually when the workload requires full use of automation (control action b.1). UCA2 includes the case in which the automation may not work appropriately and may direct the aircraft onto the wrong course. Finally, UCA3 and UCA4 consider the case of manually flown departures that start correctly, but then significantly deviate from the established SID. UCA1 and UCA3 both represent an aspect of what happened in the sample case. However, the goal of an STPA analysis is to tackle the problem highlighted by the incident from many different angles (systemic approach to safety). For this reason, the control structure and the control actions do not just take into consideration the pilots and the aircraft, but the airline policy and ATC as well. This part of the analysis would therefore be more articulated than what is shown if it were to be performed fully.

Again, for demonstrative purposes, the focus is placed on UCA3 only and its causal factors. Looking for causal factors means, in this case, looking for reasons why the pilot would keep performing a manually flown approach even though the aircraft is deviating from the SID. Some reasons could be:

1) The pilot is not following the correct SID (chart not updated, wrong chart used etc.);
2) ATC intervenes with other instructions;

3) Unexpected weather;

4) Unexpected traffic;

5) The ND is displaying an incorrect track and the pilot is following that track;

6) The F/D is off;

7) The F/D is on and providing incorrect instructions.

Causal factor 5) represents what happed at Airline ABC taking off from KYYY, however this list of possible causes is certainly incomplete and is best compiled when a number of field experts participate in the process. Performing more complete and extensive hazard analysis allows detecting situations similar to the one in the incident and addressing them at the same time. Establishing a STAMP-based leading indicator program should allow better monitoring in this sense.

At this point the first part of the STAMP-based FOQA data analysis would be complete and look as shown in Figure 18:

High level hazard	Severity	Control Action	Unsafe Control Actions			Causal Scenarios (Why?)
H1: Unacceptable deviations from the horizontal flight path	High	Perform a manually flown departure	1	The PF keeps performing a manually flown departure for too long when the deviation from the SID becomes excessive	1.1	The pilot is not following the correct SID (chart not updated, wrong chart used etc.), because: a) the airport has not provided them; b) the airline has not updated them; c) the pilot has not picked the correct chart;
					1.2	ATC intervenes with other instructions;
					1.3	Unexpected whether the ATC was not aware of;
					1.4	Unexpected Traffic;
					1.5	The ND is displaying an incorrect track and the pilot is following that track;
					1.6	The F/D is off;
					1.7	The F/D is not working appropriately driving the aircraft out of track

Figure 18 – Hazard Identification (Manually Flown Departure)

After the hazard analysis, the safety monitoring part of the methodology needs to be carried out. The results of this step are shown above are reported in Figure 19.

High level hazard	Severity	Control Action	Unsafe Control Actions			Causal Scenarios (Why?)	Mitigation Action	Assumption
H1: Unacceptable deviations from the horizontal flight path	High	Perform a manually flown departure	1	The PF keeps performing a manually flown departure for too long when the deviation from the SID becomes excessive	1.1	The pilot is not following the correct SID (chart not updated, wrong chart used etc.), because: a) the airport has not provided them; b) the airline has not updated them; c) the pilot has not picked the correct chart;	Airline process to ensure: a) correct/updated information is available form airports; b) charts are updated quickly enough; c) the pilot will use correct documentation;	Quality assurance methods will be effective (ex. The airline has the capacity of updating a chart before the next flight takes off from the specific airport the chart refers to);
					1.2	ATC intervenes with other instructions;	Clearly define what the crew is expected to do when receiving conflicting instructions from ATC;	Crew will never face a situation where airline policy seems unclear and/or inadequate (ex. Specific countries, particular ATC policies at certain airports etc.);
					1.3	Unexpected whether the ATC was not aware of;	Clearly define what the crew is expected to do when encountering unexpected bad weather conditions;	Crew will never face a situation where airline policy seems unclear and/or inadequate (ex. The trade-off provided by airline policy is inadequate);
					1.4	Unexpected Traffic;	Airline policy: avoiding traffic is the priority;	There will never be a situation where avoiding traffic would be worse than respecting the SID;
					1.5	The ND is displaying an incorrect track and the pilot is following that track;	Airline NOTAMs to warn the pilots of situations where the ND is displaying incorrect information (ex. KYYY and KXXX); Require early engagement of A/P at KYYY and KXXX airport;	Pilots will acknowledge the NOTAM; Pilots will have an adequate judgement of what "early" engagement of automation means;
					1.6	The F/D is off;	Airline policy: require pilots to always perform F/D-on take-offs;	Pilots will acknowledge the policy;
					1.7	The F/D is not working appropriately driving the aircraft out of track;	Encourage reporting of anomalies from pilots; Airline NOTAMs to warn pilots of anomalies.	Pilots will acknowledge the NOTAM; Pilots will report anomalies.

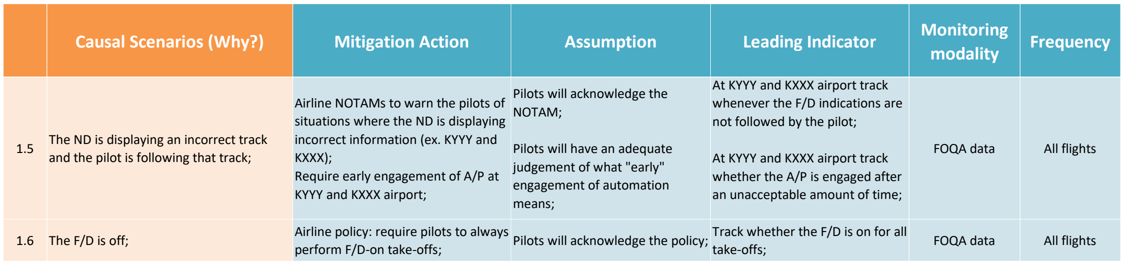
Figure 19 – STAMP-based FOQA data analysis - FMS Malfunction

Some of the mitigation measures listed may look generic but this is because the details depend on individual airline policies and internal organization. Once again, these examples are for demonstration purposes only, but with the cooperation of field experts the information contained in the analysis can be more detailed and relevant.

Two mitigation measures will be analyzed in particular: those associated with causal factors 1.5 and 1.6. As a matter of fact, these were the measures taken by the airline with respect to the incident being used as a sample case. Because the pilots already had a NOTAM for airport KYYY warning them about ND and F/D discrepancies, the assumption previously made that this would be enough to avoid excessive SID deviation was obviously not valid. The airline reacted by rewriting the NOTAM (making it clearer) and by enforcing the "early" use of automation at airports KYYY and KCCC (an airport with a similar issue). The assumptions behind these measures are that pilots will read and understand the NOTAM and that they will engage the automation "early" enough to avoid unacceptable SID deviations.

The other mitigation measure considered is the requirement enforced by the airline of never performing an F/D-off take-off. During the incident discussed, the pilots did have the F/D on and dismissed its indications. However, considering manually flown departures, it is important to monitor whether one of the rules implemented by the airline is actually working or not (tackling the problem from different angles—systemic approach). The assumption is that pilots will respect the no-F/D-off take-off rule, but, of course, this could not happen for a variety of reasons that may not be immediately clear at the time the rule was established. Expert judgment can estimate whether the action taken should be considered acceptable, at least momentarily. Nevertheless, instead of stopping the safety effort here, the STAMP-based FOQA data methodology requires the identification of ways to monitor whether the assumptions made are true i.e. whether the mitigation measures are effective.

The instrument to be used for this safety monitoring part is FOQA data. Once again, the analysis is limited to the mitigation actions 1.5 and 1.6. What are all possible events that could indicate the mitigation measure is not effective? The answers to this question are shown in Figure 20.



	Causal Scenarios (Why?)	Mitigation Action	Assumption	Leading Indicator	Monitoring modality	Frequency
1.5	The ND is displaying an incorrect track and the pilot is following that track;	Airline NOTAMs to warn the pilots of situations where the ND is displaying incorrect information (ex. KYYY and KXXX); Require early engagement of A/P at KYYY and KXXX airport;	Pilots will acknowledge the NOTAM; Pilots will have an adequate judgement of what "early" engagement of automation means;	At KYYY and KXXX airport track whenever the F/D indications are not followed by the pilot; At KYYY and KXXX airport track whether the A/P is engaged after an unacceptable amount of time;	FOQA data	All flights
1.6	The F/D is off;	Airline policy: require pilots to always perform F/D-on take-offs;	Pilots will acknowledge the policy;	Track whether the F/D is on for all take-offs;	FOQA data	All flights

Figure 20 – Hazard Management (ND and F/D)

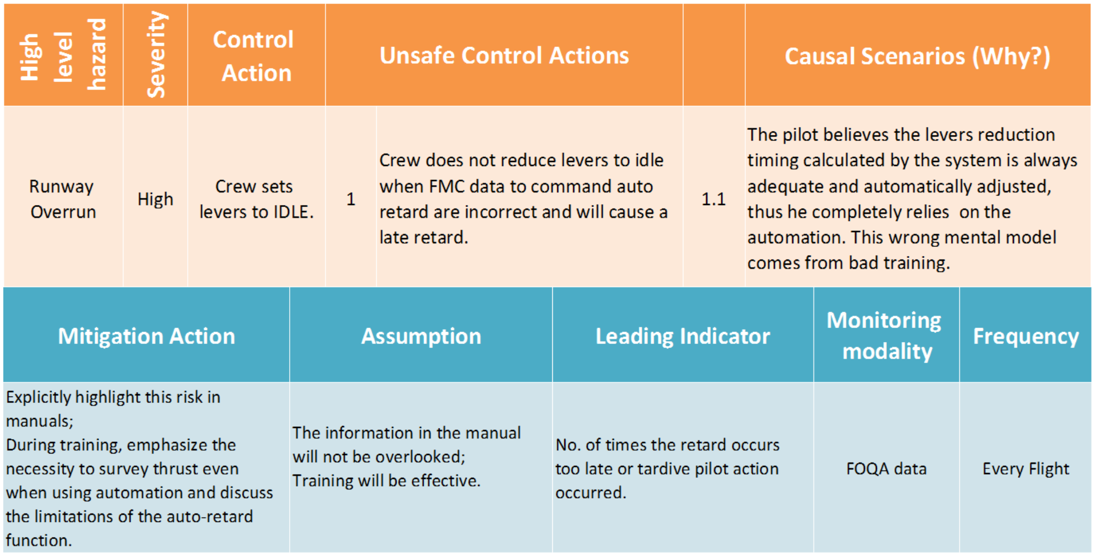
FOQA data can be used to monitor compliance with airline NOTAMs, A/P "early" engagement rule and F/D-ON take-off policy. Once leading indicators are identified through software that automatically looks for them in FOQA data, the airline simply needs to wait and see how frequently these anomalies occur. Some degree of post-detection analysis will be needed to decide whether new mitigation measures need to be put in place or not. If so, the analysis can be updated with the new counter-measure, the assumption lying behind it, and the appropriate leading indicators to monitor its effectiveness.

For the following examples the description of the full STPA process is omitted. The problem targeted is described together with the corresponding solution offered by the STAMP-based FOQA data analysis methodology.

4.3 EXAMPLE 3: Late Auto-Retard

On the Boeing 777, when the autopilot is in use, a function exists to ensure the automatic retard of the throttles a few seconds before touch down. In some cases however, due to specific weather conditions or not perfectly updated data in the

FMC, the auto-flare may occur late. The risk in this case is pilots' over-reliance on automation, which may cause them to wait for too long before taking any corrective action. The Hazard here is RUNWAY OVERRUN with the same severity as the previous example. The control action is the setting of the throttles to IDLE, which is unsafe when not done with an incorrectly calibrated auto-flare (the auto-flare could be incorrectly calibrated for multiple reasons: from a bug in the software to incorrect data entered at the beginning of the flight). Adequate mitigation actions could be updating manual content or training: emphasizing the limitations of the auto-retard function and the necessity to always survey the thrust setting on final approach even when using automation. The assumption here is that the manuals will not be overlooked and the training will be effective enough. A good leading indicator to monitor this aspect is the number of times the auto-retard occurs too late or requires pilot intervention. Figure 21 shows the complete analysis for this example.



High level hazard	Severity	Control Action	Unsafe Control Actions			Causal Scenarios (Why?)
Runway Overrun	High	Crew sets levers to IDLE.	1	Crew does not reduce levers to idle when FMC data to command auto retard are incorrect and will cause a late retard.	1.1	The pilot believes the levers reduction timing calculated by the system is always adequate and automatically adjusted, thus he completely relies on the automation. This wrong mental model comes from bad training.

Mitigation Action	Assumption	Leading Indicator	Monitoring modality	Frequency
Explicitly highlight this risk in manuals; During training, emphasize the necessity to survey thrust even when using automation and discuss the limitations of the auto-retard function.	The information in the manual will not be overlooked; Training will be effective.	No. of times the retard occurs too late or tardive pilot action occurred.	FOQA data	Every Flight

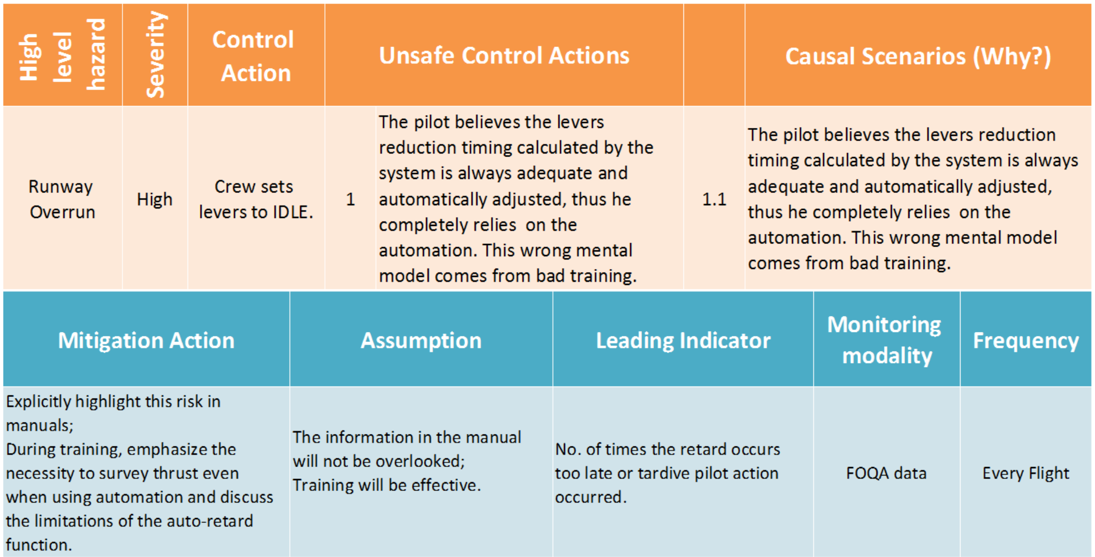
Figure 21 – STAMP-based FOQA data analysis - Late Auto-Retard

4.4 EXAMPLE 4: Auto-thrust on Touchdown

A fundamental difference between Boeing and Airbus auto-throttle systems is the absence in the latter of the feedback mechanism that makes the throttles move according to the thrust target commanded by the FADEC (a computer that controls the engines). In all the AIRBUS aircraft designed after the A320, the auto-throttle operates with the levers in a fixed position called CLB (climb). Along with the benefits associated with this configuration, there are some disadvantages, namely the discrepancy between the throttle position and the actual thrust delivered by the engine. The scenario targeted here is the case of a pilot forgetting to bring both throttle levers to idle before touch-down in order to disengage the auto-thrust. During the descent, the thrust is automatically managed. Therefore, the crew is not necessarily focused on the actual position of the throttles. Once on the ground, however, the auto-thrust does not disconnect. Instead, it keeps increasing the thrust to meet the speed target previously set until the pilot intervenes to switch to manual control.

This increase in thrust just after touch down can be dangerous especially in bad weather conditions and when the runway is short. Although the cases of a pilot forgetting to bring the throttles to idle before touch down is rare, it can happen and has been a contributing factor in a number of accidents (TAM fight 3054 and Philippines Airlines flight 137). The hazard in this case is RUNWAY OVERRUN. The control action is setting the throttle levers to CLB position, which becomes unsafe when this is done for too long, i.e. until touch-down.

One way to prevent this from happening could be to impose a procedure or a company policy to always call-out “throttles to idle" before touch down. In order to monitor whether the assumption that this call-out will not be dismissed is valid or not, FOQA data could be analyzed for every fight to find out how often it happens that pilots “forget" the throttle at CLB until touch-down. This may often not result in a catastrophic outcome, but is a clear symptom that the safety margins are being eroded. Figure 22 shows the complete analysis for this example.



High level hazard	Severity	Control Action	Unsafe Control Actions			Causal Scenarios (Why?)
Runway Overrun	High	Crew sets levers to IDLE.	1	The pilot believes the levers reduction timing calculated by the system is always adequate and automatically adjusted, thus he completely relies on the automation. This wrong mental model comes from bad training.	1.1	The pilot believes the levers reduction timing calculated by the system is always adequate and automatically adjusted, thus he completely relies on the automation. This wrong mental model comes from bad training.

Mitigation Action	Assumption	Leading Indicator	Monitoring modality	Frequency
Explicitly highlight this risk in manuals; During training, emphasize the necessity to survey thrust even when using automation and discuss the limitations of the auto-retard function.	The information in the manual will not be overlooked; Training will be effective.	No. of times the retard occurs too late or tardive pilot action occurred.	FOQA data	Every Flight

Figure 22 – STAMP-based FOQA data analysis - Auto-Thrust at Touchdown

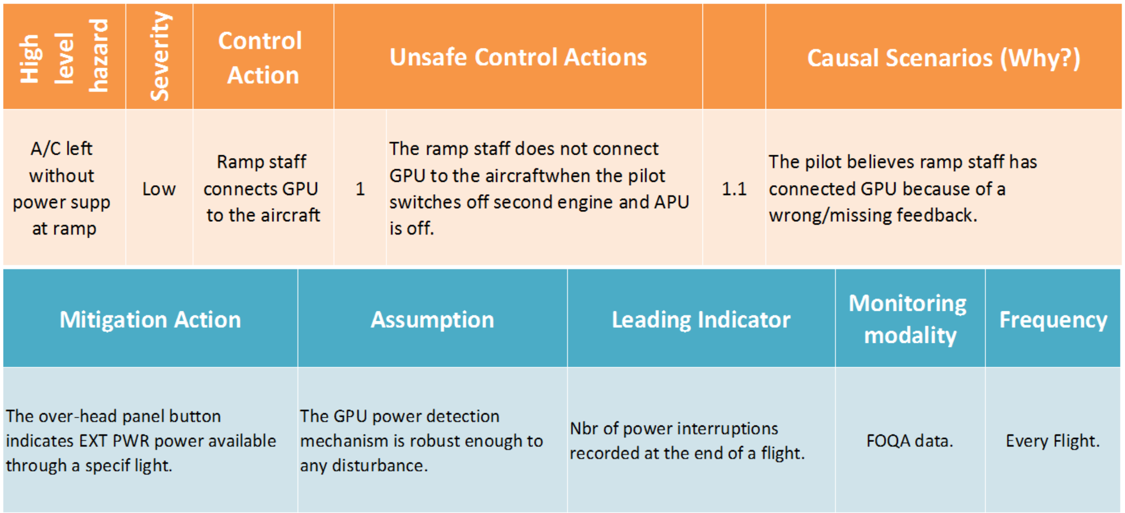
4.5 EXAMPLE 5: GPU Connection

The final example is a case where the methodology introduced in this thesis can be applied to a problem not strictly related to flight operations although still trackable with FOQA data. The scenario is the following: once the aircraft reaches the ramp area at the end of a flight, the pilots may want to decide to ask for Ground Power Unit (GPU) connection. Usually, the pilots are able to see whether ground power is available or not by a feedback-light on the EXTERNAL POWER push-button in the overhead panel. However, there are some instances when this light illuminates even though external power is not actually available (wrong plug, overused or loose plug etc.). When this occurs, the pilot switches off all other power sources believing the GPU is already connected and the aircraft is left without power supply.

This hazard is a minor one, in the sense that it is unlikely to result in injuries or damage to the equipment. However, it is an annoying occurrence during busy airport operations and can be harmful to the aircraft avionics.

The control action in this case is the connection of the GPU. When this is not done properly, the system may enter a hazardous state. The mitigation action is the feedback light itself with the assumption that it will always work or at least fail at an acceptable rate (assumptions do not necessarily need to be about the infallibility of the mitigation action).

The appropriate leading indicator here is how many times a power interruption is recorded in FOQA data, with the frequency of checking being every flight. Of course power interruptions may occur for other reasons than the mishandling of the shift between power sources. However, the specific phase of flight when this occurs and the frequency of occurrence already restrict the number of possible causes: if the power interruption was due to a malfunction in the system, it would be very unlikely for this to take place very frequently and always at the end of the flight. As already mentioned, even with the methodology here proposed, a certain degree of post-detection analysis will be required. The established FOQA events and the underlying STPA model, however, should facilitate the process. The corresponding results of the application of the STAMP-based approach are shown in Figure 23.



High level hazard	Severity	Control Action	Unsafe Control Actions			Causal Scenarios (Why?)
A/C left without power supp at ramp	Low	Ramp staff connects GPU to the aircraft	1	The ramp staff does not connect GPU to the aircraftwhen the pilot switches off second engine and APU is off.	1.1	The pilot believes ramp staff has connected GPU because of a wrong/missing feedback.

Mitigation Action	Assumption	Leading Indicator	Monitoring modality	Frequency
The over-head panel button indicates EXT PWR power available through a specif light.	The GPU power detection mechanism is robust enough to any disturbance.	Nbr of power interruptions recorded at the end of a flight.	FOQA data.	Every Flight.

Figure 23 – STAMP-based FOQA data analysis - GPU connection

5

CONCLUSIONS

5.1 Summary

In the first part of this thesis, the current challenges faced in the field of FOQA data analysis were presented. The quantity of data collected has increased dramatically and it has become increasingly difficult to analyze in a meaningful way. The traditional event-based approach (exceedance analysis – as per FAA circular AC 120-82) only detects a limited number of issues and is becoming insufficient to cover the complexity of airline operations today.

Statistical and data-driven methods have been defined to address this problem as they do not require problems to be known beforehand (i.e., before looking at the collected data). However, the phenomena mathematically highlighted by these methods are at times difficult to interpret as they lack contextualization. Also, data-driven methods can easily become computationally expensive if complex aspects of piloting need to be tracked (e.g., human-automation interaction).

The thesis concentrates on how exceedance analysis can be improved. The characteristics of a good leading indicator program have also been presented.

The unique features of the STAMP approach as an accident causation model were presented as well as the derived hazard analysis technique (STPA). This technique represents an enhanced tool to identify possible hazard scenarios to look for in FOQA data. The systemic approach in STAMP and the flexibility of STPA in taking into account not only hardware aspects, but also software design, human operations and other socio-technical factors, will allow the analysist to anticipate a greater number of issues with respect to traditional safety assessment techniques. Moreover, these issues will be more contextualized (the control structure serving as a model of the system). A section was then dedicated to describing how leading indicators can be derived from the hazard scenarios identified through STPA, using assumption-based engineering concepts.

The third chapter of the thesis illustrated how STPA together with the concepts of assumption-based engineering allows establishing a new methodology for the identification of leading indicators ("events") for FOQA data analysis (as per the hypothesis identified in chapter 1).

5.2 "Emergent Properties" of the STAMP-based approach to FOQA data analysis

To conclude the discussion, some more high-level considerations on the properties of this new methodology are described such as its role in the normal engineering process of systems development.

The STAMP framework, but also the assumption-based methodology used to identify leading indicators, are particularly suitable to monitor human behavior during system operations. The main reason behind this belief is that operators are the element of the system on which the greatest number of assumptions is made. It has already been discussed how much information is conveyed through training and manuals, procedures or checklists and how pilots are expected to remember all of these and dynamically adapt them to the various scenarios they face while flying. Also, the traditional probabilistic approach is not particularly suitable when it comes to human decision making. Establishing the probability that an operator will or will not perform a certain action is an almost impossible task especially in a complex environment like that of a cockpit. Context highly influences people's choices and an action that may seem unnatural and counterintuitive when analyzed as a whole, may become sensible when specific conditions arise. This new approach to FOQA data analysis accounts for human behavior without the need to adopt a stochastic approach.

The second property of the STAMP-based approach is the role it plays if examined within the context of a regular engineering process. In the development phase of a system, the STPA process involves the definition of accidents and hazards, from which safety constraints can be established. The safety constraints are the result of the iterative application of the hazard analysis technique, which highlights possible hazard scenarios or weaknesses of the design. When expert judgement determines that the safety constraints imposed (alias mitigation measures) are likely to succeed, then the assumptions behind the decisions are made explicit. At this point, the system development or study phase has ended and operations start.

The STAMP-based approach to FOQA data analysis "covers" operations by requiring appropriate leading indicators to be established in order to monitor the validity of the assumptions made. In case these assumptions are found to be invalid, the hazard analysis previously performed will have to be reviewed, new mitigation measures put in place, new assumptions highlighted together with corresponding updates to leading indicators. With this new approach to FOQA data monitoring, the loop between the design phase of a system and its operations is closed. All the safety efforts made “in the office” will not be simply archived with a document providing justifications about why the remaining risk is “low”, but will be counterchecked with a set of leading indicators, establishing an iterative approach (Figure 24).

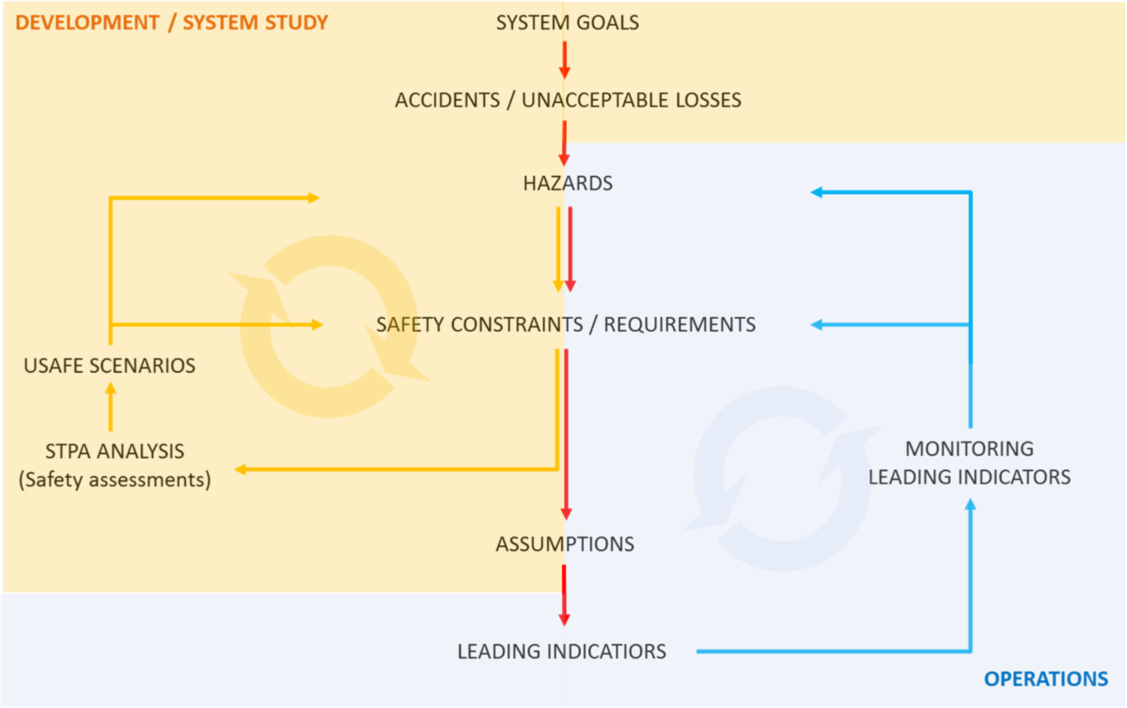


Figure 24 – STAMP-based FOQA data analysis:
between development and operations

REFERENCES

[1] American Bureau of Shipping, *Safety Culture and Leading Indicators of Safety*, January 2012, Houston

[2] Blake Abrecht, Dave Arterburn, David Horney, Brandon Abel, Jon Schneider, Nancy Leveson. *A New Approach to Hazard Analysis for Rotorcraft*, Proceedings of the 2016 American Helicopter Society Technical Meeting, Huntsville, AL, February 2016.

[3] Budalakoti et al., *Anomaly detection and diagnosis algorithms for discrete symbol sequences with applications to airline safety*, IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 39.1 (2009).

[4] Bundesstelle fur Flugunfalluntersuchung, *Investigation Report, German Federal Bureau of Aircraft Accidents Investigation*, 2004.

[5] Callantine, Todd, *The crew activity tracking system: Leveraging flight data for aiding, training and analysis*, Digital Avionics Systems, 2001. DASC. 20th Conference. Vol. 1. IEEE (2001).

[6] Campbell, Neil, *The Evolution of Flight Data Analysis*, Australian Society of Air Safety Investigators regional conference (2007).

[7] Das et al., *Comparison of algorithms for anomaly detection in flight recorder data of airline operations,* AIAA Aviation Technology, Integration, and Operations Conference (2012).

[8] Das et al., *Multiple kernel learning for heterogeneous anomaly detection: algorithm and aviation safety case study*, Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM (2010).

[9] Dewar James. *Assumption-Based Planning*, Cambridge University Press, 2002.

[10] Diebold et al., *Scoring the leading indicators*, Journal of business, 369-391, 1989.

[11] European commission, *Commission Regulation (EU) No 965/2012*, Official Journal of the European Union L296/1 (2012).

[12] Federal Aviation Administration, *AC 120-82 - Flight Operational Quality Assurance*, Retrieved from www.faa.gov (2004).

[13] Federal Aviation Administration, Destination 2025, pg. 3 Retrieved from www.faa.gov=about=plans reports=media=Destination2025:pdf (2011).

[14] Federal Aviation Administration, *Section 121.344*, CFR, Title 14 Chapter I › Subchapter G › Part 121 (2010).

[15] Flinn et al., Measuring safety climate: identifying the common features, Safety Science 34, 177-192, 2000.

[16] Gorinevsky et al., *Aircraft anomaly detection using performance models trained on fleet data*, Intelligent Data Understanding (CIDU), 2012 Conference on. IEEE, (2012).

[17] Grabowski et al, *Accident precursors and safety nets: leading indicators of tanker operations safety*. Maritime Policy & Management 34.5, 405-425, 2007.

[18] Hale et al., *Modeling accidents for prioritizing prevention*, Reliability Engineering and System Safety 92, 1701–1715, 2007.

[19] Hudson, *Process indicators: Managing safety by the numbers*, Safety Science 47, 483–485, 2009.

[20] International Council on Mining and Metals, *Overview* of *Leading Indicators for Occupational Health and Safety in Mining*, ICMM, 2012.

[21] Kaminsky et al., *Leading indicators of currency crises*. Staff Papers 45, 1-48, Springer, 1998.

[22] Kongvik, *Organizational safety indicators: Some conceptual considerations and a supplementary qualitative approach*, Safety Science 48, 1402-1411, 2010.

[23] Leveson Nancy, *A Systems Approach to Risk Management Through Leading Safety Indicators,* MIT, 2015.

[24] Leveson Nancy, *Engineering a Safer World,* MIT, 2011.

[25] Leveson, N.G. and Reese, Jon D, *TCAS Intent Specification*, http://sunnyday.mit.edu/papers/tcas-intent.pdf

[26] Li, Lishuai, et al., *Anomaly detection in onboard-recorded flight data using cluster analysis,* Digital Avionics Systems Conference (DASC), IEEE/AIAA 30th. IEEE, 2011.

[27] National Transportation Safety Board, *Descent Below Visual Glidepath and Impact With Seawall, Asiana Airlines Flight 214, Boeing 777-200ER, HL7742, San Francisco, California July 6, 2013*, Washington https://www.ntsb.gov/investigations/Accident Reports/Reports/AAR1401.pdf, 2014.

[28] National Transportation Safety Board, *In-Flight Separation of Vertical Stabilizer American Airlines Flight 587, Airbus Industrie A300-605R, N14053, 2001*, Washington, https://www.ntsb.gov/investigations/AccidentReports/Pages/AAR0404.aspx, 2004.

[29] Øien et. al, *Building Safety indicators: Part 1 – Theoretical foundation*, Safety Science 49, 148-161, 2011.

[30] Øien et. al, *Building Safety indicators: Part 2 — Application, practices, and results*, Safety Science 49, 162-171, 2011.

[31] Organization for Economic Co-operation and Development (OECD). 2003. *OECD Guidance on Safety Performance Indicators*. Paris: OECD

[32] Pate-Cornell, *Warning systems in risk management*, Risk Analysis, 223-234, Wiley Online Library, 1986.

[33] Phimister JR, Bier VM, Kunreuther HC, editors. *Accident precursor analysis and management: reducing technological risk through diligence*, Washington, DC: The National Academies Press; 2004

[34] Shein, *Organizational Culture and Leadership*, Jossey-Bass, 2004.

[35] Chidester, *Understanding Normal and Atypical Operations Through Analysis of Flight Data,* Proceedings of the 12th International Symposium on Aviation Psychology, Dayton, OH, pp. 239–242 (2003).

[36] UK Health and Safety Executive, *Step-by-Step Guide to Developing Process Safety Performance Indicators*, UK Health and Safety Executive, HSG254, 2006.

[37] US Department of Transportation NextGen Joint planning and development office, *Next Generation Air transportation System Integrated Plan*, pp. 12 (2004).