Systems Theoretic Accident Model and Process (STAMP) Safety Modelling Applied to an Aircraft Rapid Decompression Event

Craig K. Allison1, Kirsten M. Revell1, Rod Sears2 & Neville A. Stanton1

*1. Transportation Research Group, University of Southampton, UK*

*2. Faculty Of Engineering And Computing, Coventry University, UK*

Address for Correspondence

Dr. Craig Allison

Transportation Research Group

Faculty of Engineering and Environment

University of Southampton

Boldrewood Innovation Campus

Southampton SO16 7QF

Email Craig.Allison@soton.ac.uk

Tel: +44 (0)23 8059 3148

ABSTRACT

Understanding a crew’s response to a rapid decompression, and factors which can influence the decisions crew members make, can facilitate a safe resolution of a potentially life threatening hazard. Anticipating the Human Factors issues is an appropriate way to assess potential risk factors before such an event happens. The Systems Theoretic Accident Model and Process (STAMP) and its predictive risk assessment method, System-Theoretic Process Analysis (STPA), is a systemic approach to safety analysis. This approach is ideal when considering complex systems, such as aviation. The scenario of an aircraft experiencing a decompression event was analysed using STAMP-STPA across a series of workshops during which key safety elements were identified and reflected upon. It was found that the use of the STAMP-STPA methodology successfully identified factors central to the Helios 522 accident. Based on the outputs of this research, it is suggested that, due to its inherent utility, the STAMP-STPA method can be used to elicit a variety of safety critical insights, and does so in a way that considers individuals, organisations and technology at the same level of granularity, in a way that does not attribute blame to any single agent.

KEY WORDS

STAMP, Systemic Safety, Aviation, Systems Thinking

INTRODUCTION

 British Airways flight 5390, June 1990, was a standard passenger flight between Birmingham Airport, United Kingdom and Malaga Airport, Spain. The flight received notoriety however, when approximately 13 minutes into the flight, a window in the aircraft cockpit failed, resulting in the captain of the flight, Tim Lancaster, being largely pulled out of the aircraft. Co-pilot, Alastair Atchison, was forced to make an emergency landing at Southampton Airport United Kingdom, with a flight attendant desperately holding on to the unconscious captain, who was buffeted against the outside of the aircraft suffering from frostbite and hypoxia. The co-pilot was able to successfully land the aircraft, with no loss of life, with all crew recovering from their injuries, including Captain Lancaster, who returned to work just a few short months after the event. Flight 5390 experienced a rapid decompression event, one that was fortunately not fatal due to the work of both the co-pilot and the support offered by the aviation system. Although an enquiry identified the cause of the incident was an incorrect fitting of bolts within the cockpit window (Air Accidents Investigation Branch, 1992), it can be argued that other factors also contributed to the incident, both its start and resolution, including the crew’s training, guidance from Air Traffic Control as well as other agents, such as aircraft components. This paper explores the system of systems that exists within aviation to limit the impact of decompression incidents and exposes this system to a Systems Theoretic Accident Model and Process (STAMP) safety analysis (Leveson, 2004).

Aviation can be considered a system of systems (Carlock, & Fenton, 2001; Harris & Stanton, 2010). It comprises numerous complex independent agents, distributed across a wide network, each of whom acts in concert to ensure the safe operation of, potentially multiple, aircraft. Each of the agents within this distributed network however operates with their own goals and objectives. Any one agent working in isolation, however, cannot achieve the global objective of the wider system, which is dependent on multiple agents successfully collaborating (Boardman & Sauser, 2006). Due to the disparate and complex nature of interactions within systems of systems, understanding the safety considerations that exist within these networks is a great challenge (Stanton & Harvey, 2016).

Systemic approaches to understanding safety have been proposed to adequately understand safety issues that can arise within systems of systems. The systemic approach to safety, despite an initially slow adoption (Leplat, 1984), has grown in both prominence and importance to become the prevailing approach in accident analysis (Salmon, Williamson, Lenné, Mitsopoulos-Rubens, & Rudin-Brown, 2010). The systemic approach has been advocated by a variety of researchers including Rasmussen (1997), Hollnagel (2004) and Leveson (2004), each of whom identified independent theoretical limitations with cause-effect safety models. Of central concern is the tendency of cause-effect chain models to focus on the allocation of blame, seeking a singular root cause of an accident and often halting the investigation when an appropriate source of blame is identified (Leveson, 2004). By accounting for the greater complexity present within modern systems, and considering the role of the human actor within the system (Lindberg, Hansson & Rollenhagen, 2010), systemic safety approaches, it has been argued, operate as a more informative and holistic approach to safety recommendations (Underwood & Waterson, 2013).

Despite criticisms of the systemic safety models that have been developed (Salmon, Cornelissen & Trotter, 2012; Stanton, Rafferty & Blane, 2012), the number of such models have grown to include Functional Resonance Analysis Method (FRAM) (Hollnagel, 2012), AcciMaps (Rasmussen, 1997) and EAST broken-links approach (Stanton & Harvey, 2016). The most widely cited within academic literature (Underwood & Waterson, 2012) however is Systems Theoretic Accident Model and Process (STAMP) approach (Leveson, 2004). Previous STAMP analysis has been used to identify hazards related to the pollution of a local drinking water supply (Leveson, Daouk, Dulac, & Marais, 2003), an oilrig explosion (Altabbakh, AlKazimi, Murray, & Grantham, 2014) and aircraft security (Laracy & Leveson, 2007).

STAMP is an accident-modelling framework that conceptualises socio-technical processes as systemic performances in a state of dynamic equilibrium, enabled by multi-layered feedback loops of information and control between different stakeholders. Leveson, (2004), proposed that STAMP offers three distinct advantages over traditional safety methods; 1) enabling the safety researcher to consider the role of systemic feedback, and actions taken in response to feedback; 2) encapsulating organisational constraints, technological constraints and personological constraints at the same level of granularity within the same analysis, and; 3) improving the safety of the overall system rather than seeking a “root cause” of an accident. In this vein, similarities can be drawn between the STAMP approach and Rasmussen’s (1997) notion of hierarchies of control, present within the AcciMaps framework, upon which it is based.

 According to STAMP, functional processes are the result of constraints reducing the degrees of freedom of the behaviour of the socio-technical system. STAMP conceptualizes constraints on multiple levels resulting in an often hierarchical control structure (Stanton et al., 2013). Constraints are imposed by various stakeholders with non-linear interactions between them acting as feedback. Hence, STAMP is particularly suited to assessing the safety of complex socio-technical systems characterised by a high level of interactive coupling, whereby multiple stakeholders, both human and non-human, simultaneously constrain operational processes (Leveson, 2004), such as present within systems of systems (Salmon et al., 2012; Stanton et al., 2012; Harvey & Stanton, 2014). Due to its complexity as a socio-technical system of system, aviation is an ideal candidate for use of a STAMP analysis (Johnson & Holloway, 2003).

All high altitude flights operate within pressurised environment of an aircraft cabin. This is needed to ensure an adequate supply of breathable oxygen for crew and passenger life support. Should the pressurisation within the cabin fail, either as a result of a failure of the pressurisation system itself, or as a result of a structural failure within the aircraft, (for example the loss of a window), the aircraft will undergo a decompression event. The rate of the decompression is affected by numerous factors, including the pressurisation differential between the pressurised space and the external environment and the extent of the damage to the pressurisation system or aircraft structure. Although a significant and potentially life-threatening hazard, a rapid decompression event is generally not immediately fatal to passengers and crew. Should a rapid decompression occur, it is essential that the aircraft descend rapidly, but safely, to an altitude of approximately 10,000 feet to ensure an adequate supply of breathable oxygen for all on board. The aircraft crew are then required to seek an appropriate location to divert, should their original destination be no longer reachable.

During a rapid decompression event, an aircraft cockpit can become a highly chaotic environment, often filling with vapour, noise and lose detritus. The skills of an aircrew to respond to a rapid decompression scenario can often mean the difference between an air incident, and the survival of the aircraft and those on board, and an air accident, resulting in the loss of the aircraft as well as the lives of those on board. To support the aircrew in dealing with this rare, but dangerous event, a control structure, comprising numerous agencies has been developed. The case of a rapid decompression is therefore an ideal scenario for a STAMP analysis.

The initial aim of this paper is to understand the rapid decompression scenario and identify the stakeholders who can influence a crew’s response to a rapid decompression. This paper seeks to highlight potential areas within the identified interactions that could result in unsafe actions being undertaken.

 This will be achieved via the use of a STAMP-STPA analysis of an exemplar hypothetical rapid decompression event. The analysis seeks to construct a high-level control structure for the scenario, applying the System-Theoretic Process Analysis (STPA) error taxonomy to evoke emergent Unsafe Control Actions (UCAs) and populate an example control loop with the generated UCAs. This is to demonstrate both the usefulness and the utility of the STAMP-STPA framework.

METHOD

System-Theoretic Process Analysis (STPA) is the predictive risk assessment method within the STAMP framework. It enables the mapping of factors that can contribute to specific hazards occurring in socio-technical systems. Following the identification of the potential hazard(s), STPA is conducted in three iterative steps, all of which represent the system as a whole, starting from an initially high level of abstraction and progressing towards increasing level of granularity. The first step of the STPA analysis involves the construction of a high-level hierarchical control structure. The control structure presents all stakeholders within the system under analysis and the control actions that link the independent stakeholders. Control actions constitute the main source of feedback and interaction between the multiple stakeholders. During the second step of the STPA analysis, unsafe control actions (UCAs) are identified through applying a standardised error taxonomy to each of the control actions identified in the first step. Within STPA, the error taxonomy is driven by the use of four guide sentences:

1) Action required but not provided;

2) Unsafe action provided;

3) Incorrect timing / order;

4) Stopped too soon / applied too long.

These guide sentences are set as part of the STPA methodology (Leveson, 2004) and are designed to elicit all the possible failings within the system in order to create the complete failure taxonomy. It is important to note that not all guide sentences are applicable in all cases and equally each guide sentence may generate more than one UCA. Finally, the causes for the UCAs can be analysed in more detail through constructing feedback loops for identified UCAs. This enables the researchers to examine how multiple UCAs can interact.

As this study presents the application of a safety metric to a hypothetical event, the main analysis was generated following workshops with Subject Matter Experts (SMEs). Three workshops were undertaken using SMEs in Human Factors, STAMP and Aviation. Aviation expertise was provided by three independent, experienced, pilots (one per workshop) to reduce bias and improve the validity of the produced outputs. The first workshop sought to identify an appropriate scenario for the STAMP analysis and gain an understanding of associated hazards. The second workshop was undertaken to construct the high-level control structure for current operations (Presented within the results section). The second workshop also began to generate the unsafe control actions that could potentially emerge, following the use of the standardised STPA error taxonomy. Following the second SME workshop, the research team continued to generate potential UCAs that could emerge using the control structure generated. The outputs were then validated by an independent aviation SME during the final workshop. The third workshop also produced an exemplar control loop using the identified UCAs.

The analysis presented is based on current concepts of operations (CONOPS) for aircraft in a major commercial airline. In the future, with the development and integration of newer technology and changes in working practices, not only CONOPS, but also the design of, and the availability of, aircraft systems and controls are likely to change. As a result, activities chosen within the present study may change and or disappear from operational practice.

In addition, assumptions have been made regarding the operational state and capacity of the airline, whereby it is assumed that the Airline has a current Aircraft Operating Certificate (AOC), and ensures adequate crew training and post training examination. Furthermore, it is assumed that the crew within the current scenario will follow standard operating procedures that are taught within regular recurrent training courses and outlined within the Aircraft’s Quick Reference Handbook (QRH). It is also assumed that cross-check monitoring and Crew Resource Management (CRM) is adequate. In addition, it is an assumption that the aircraft operated within the scenario is certified and airworthy, although this does not prevent systems from failing during the flight. It should be noted that the analysis presented does not consider the role of any cabin crew or passengers within the scenario, but rather focuses on the role of the pilot and co-pilot, supported by Air Traffic Control (ATC) and Air Traffic Management (ATM). It is acknowledged that, within commercial flight operations, cabin crew do have a role to play in the safety of passengers, as they did in BA5390 (Air Accidents Investigation Branch, 1992), however within the confines of the current analysis, this role is not deemed as central as that of the flight crew in the aircraft operation.

To simplify the analysis, it is assumed that within the current scenario the flight path is not over mountainous terrain; therefore the Ground Proximity Warning System (GPWS) would not preclude a descent to 10,000 feet. Future research considerations should however be given to flight over mountainous regions, including the Alps and Himalaya whereby the terrain frequently rises to above 15,000 feet. Should a flight over mountainous terrain be considered, the required descent to 10,000 feet could potentially have disastrous results, resulting in the loss of the aircraft due to collision with the terrain. To avoid this, pilots would be required to plot a route to the minimum safe altitude (MSA) and continue to descend as and when the terrain allows. This is a considerably more complex task, with numerous additional steps and considerations, which fall outside the remit of the current investigation.

Within STAMP analysis, a hazard is defined as *‘A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss)’* (Thomas et al., 2013). Based on the STAMP framework, a hazard is something which can be controlled, but that could also lead to a potential accident.

As noted previously, STAMP – STPA is a scenario-based method in the sense that the analysis starts with identifying the hazard(s). Hazard(s) represent system states and define the boundaries of the analysis. Moreover, the results (e.g. control actions, causes of UCAs) depend on the level of granularity chosen by the analyst. In the present study, the units and granularity of the analysis were informed by the results of the initial SME workshop. Results from the initial pilot study revealed that complex systems such as aviation performance could be studied from multiple perspectives, also referred to as frames of observation (Hutchins, 2010). Choosing a suitable perspective is essential for valid and representative results.

 The initial step in the STAMP-STPA analysis involves the definition of hazards that could lead to an accident. In the current case study, the potential accident was defined as the crew’s response to a rapid decompression event and potential hazards were defined as follows:

* Aircraft fails to descend to 10,000 feet (a safe altitude, whereby sufficient oxygen is present in the atmosphere to sustain life);
* Crew fail to ensure adequate oxygen supply.

 Should the crew fail to ensure an adequate oxygen supply, for example by failing to deploy oxygen masks, and failing to initiate a descent, the crew will become hypoxic, leading to incapacitation, eventual neurological damage and potentially even death. Rapid decompression events are therefore threatening to both the overall structural stability of an aircraft and the life of all on board. The analysis focuses on the control structure and control actions that support an adequate response to the hazards associated with rapid decompression in order to avoid these potentially fatal consequences.

RESULTS AND DISCUSSION

 The control structure of the system that enables crew reaction to rapid decompression for the current operations is depicted in Figure 1. This control structure development was based on the analysts’ knowledge of the case study of rapid decompression, gained from the SME workshops. The control structure represents the highest level of abstraction within the overall system under investigation. The STAMP-STPA method is designed to start at the highest level of abstraction and then focus into lower levels as necessary. The control structure within the current analysis takes a generally hierarchical form. In the current case study, seven primary stakeholders were identified, Regulator, Airline, Crew, Aircraft, ATC/ ATM, Other Aircraft and Airframe Manufacturer. These stakeholders are linked by control actions, as shown by the labelled arrows in Figure 1. Some actions are continuously performed during the current scenario whilst others denote intermittent actions, for example an action performed after an event has occurred. An example of constant feedback during the scenario is aircraft warning systems that operate between the aircraft and the crew, whilst an air incident report between the airline and the regulator occurs intermittently following the event.

 

OTHER AIRCRAFT

Figure 1 - Control structure for current operations, crew response to rapid decompression

Working from the top of the hierarchy, the Regulator provides an AOC to the airline, allowing the airline to operate and charge for the transportation of passengers and freight on its fleet of aircraft. Although this appears as a singular point within the current analysis, to hold an AOC an airline must demonstrate significant capacity and competency, including the possession of significant infrastructure, training regimes and personnel to support their operations. The airline in turn has a responsibility to the crew of its aircraft to provide recurrent training within simulators for emergency and non-standard situations, such as the rapid decompression scenario. In the event of a rapid decompression, the crew have a responsibility to the aircraft to complete standardised QRH drills, including the donning of oxygen masks and initiating a descent to 10,000 feet (or the minimum safe altitude appropriate for the surrounding terrain). During such an emergency, the crew also has a responsibility to call a mayday, informing ATC/ ATM of the situation of the aircraft and the changes in the route and position of the aircraft caused by the need to descend. In response, ATC/ ATM has a responsibility to acknowledge the crew’s mayday call and offer assistance to help the crew manage the situation. ATC/ ATM will also receive data regarding the incident/emergency from on board aircraft sensors. Positional data on the aircraft is provided by ATC/ ATM interrogation of the on-board transponder, identifying the aircraft’s position, including altitude, and the aircraft’s call sign. This information is used by ATC/ ATM to inform other aircraft within the vicinity of the stricken aircraft of the emergency and highly unusual situation. This is in order to minimise the likelihood of mid-air collisions with aircraft whose flight path may take them below or directly into the path of the stricken aircraft. The airframe manufacturer has a responsibility to ensure that the aircraft itself in turn provides the crew with a variety of warning systems, supplying valuable information regarding the operational state of the aircraft and valuable information in allowing the crew best to manage the situation. On board flight data generated by the aircraft can also provide the operating airline with post incident flight data, which could potentially be used to judge crew performance and inform future crew training programmes. The crew equally has a responsibility to provide flight reports and safety reports to the operating airline following a flight. Finally, following an aviation emergency, the airline itself feeds back information to the regulator via air incident reports.

The control structure presented can be seen operating when considering the incident of Singapore Airlines A388, an Airbus A380-800, which on a routine flight from London Heathrow to Singapore experienced a rapid decompression over northern Afghanistan in 2014 (Air Accident Investigation Bureau of Singapore, 2015). During the flight, the aircraft lost cabin pressurisation as a result of a failure of a door seal. Following procedures, crew of the aircraft contacted ATC and initiated a descent to 10,000ft, as well as deploying oxygen masks to ensure the safety of passengers. Although initially gaining no response from ATC due to limited communication range, the MAYDAY call was relayed via a secondary aircraft. Upon contact with ATC, assistance was offered to the crew of aircraft, and ATC advised a suitable diversion airport as it became apparent the crew selected airport was not suitable. Following the incident, Singapore Airlines and Airbus used data from the incident to support procedural recommendations for the flight crew during future rapid decompression incidents.

Based on the control structure presented within Figure 1, each of the control actions were considered in turn to compile a failure taxonomy using the standardised STPA method discussed previously. In total, 78 UCAs were identified which could act as a potential source of failure within the system. To consider the UCAs in greater detail, an exemplar control loop was generated for the interaction between crew and aircraft. To create a control loop, a pair of stakeholders was assigned status as ‘controller’ or ‘controlled process’. UCAs were considered and based upon their characteristics, mapped to different sections of a generic loop structure, as proposed by Leveson (2011). This stage of the analysis enables the exploration of how and why UCAs occur, so that mitigation strategies can be targeted to appropriate points within the control loops.

The mapping of UCAs can be done for every identified UCA; in this case this process would involve the generation of 78 control loops, which is not feasible within the confines of the current paper, (due to space constraints). Instead, standard practice suggests that only the control loops of real interest to a particular component are analysed at this level of detail (Stanton et al., 2013). Due to these limitations, a compromise whereby the control actions are mapped between a pair of stakeholders was adopted.

Control Loop between Crew and Aircraft

 Four control actions (CAs) were identified between ‘Crew’ (as ‘controller’) and ‘Aircraft’ (as ‘controlled process’) comprising of:

1) Ensure adequate pressure in cabin;

2) Ensure adequate O2 levels for crew;

3) Descend to 10,000 feet, and;

4) Conduct QRH Drills (Figure 1).

A failure in any of these CAs during rapid decompression could ultimately lead to hypoxia due to lack of oxygen, with potentially fatal consequences. These four CAs were used to generate a total of 21 UCAs, presented in Table 1. The Generated UCAs were subsequently mapped to a control loop, generating Figure 2, using the guidance presented in Leveson (2011). In the top left corner of Figure 2, inappropriate, ineffective or missing UCAs controlled by the crew, could occur in a number of ways, such as: failure to maintain cabin safe altitude; failure to descend to 10,000 feet or failure to don O2 masks (amongst others). In this control loop, 10 inadequate operations by the crew were also identified and placed within the ‘Actuator’ box in Figure 2, for example stopping the decent too early, performing QRH checks in the wrong order, or crew remove masks too early. Delayed operations are placed in the bottom left section of Figure 2 and UCAs identified for the crews’ response to rapid decompression were delays in donning their O2 masks, closing the pressure valve, initiating the descent, or merely conducting QRH checks too slowly (Figure 2).

The bottom centre of the control loop considers component failure or changes over time relating to the controlled process (Figure 2). Considering the control loop in Figure 2, this involves issues caused by the Aircraft, rather than the Crew, which never-the-less influence the crew through a feedback loop. Whilst this analysis makes the assumption that the Aircraft is ‘airworthy’ in that the AOC requirements from the Regulator have been adopted by the Airline (Figure 1), the SME consulted as part of the analysis verified that this did not preclude technical issues or component failures from occurring during flight. For this scenario, relevant UCAs identified that related to component failure comprised failure of the pressure, altimeter and GPWS warning systems (Figure 2). In the bottom right corner of Figure 2, UCAs relating to feedback delays, inaccurate or missing information and measurement inaccuracies are positioned (Figure 2). UCAs mapping to this part of the control loop relate to the GPWS and pressure warning systems activating too late to enable the crew to take appropriate action, or continuing for too long and so distracting the crew when they are trying to take action during the scenario. On the right of the control loop, the ‘Sensor’ box includes UCAs relating to ‘inadequate operation’, rather than failure (Figure 2). Failures of the displays (rather than components themselves) relating to the pressure and GPWS warning systems populate this box in Figure 2. Completing the feedback loop back to the Crew, inadequate, missing, or delayed feedback, are represented in the top right part of the control loop diagram. UCAs mapping to this criteria comprised ‘Pressure warnings stopping too early’ (e.g. before a distracted crew were aware of the problem), and ‘GPWS warning activates too late’ (e.g. before crew have time to take effective action). UCAs feeding back into the Crew due to component, display and warning issues can all contribute to the development of an incorrect mental model of the aircraft state, at the top of the control loop (Figure 2). This in turn could promote further UCAs whereby Crew ignore warnings or data relating to the emergency.



Figure 2 - Control Loop comprising 'Crew' and 'Aircraft'



Table 1 - UCAs and corresponding Safety Constraints generated for Control Loop comprising 'Crew' and 'Aircraft' for crew response to rapid decompression.

In addition to presenting the aforementioned UCAs, Table 1 provides a sample of novel safety constraints for UCAs resulting from the Crew interacting with the Aircraft (left hand side of Figure 2). The addition of new safety constraints allows the analysts to progress the STPA methodology and begins to develop potential mitigation strategies for the identified UCAs (Leveson, 2014). The types of safety constraints that were proposed within this work include the provision of warnings, indicators or alerts, (e.g. ensuring the crew have sufficiently salient pressurisation warnings). This was a major factor in the Hellios Flight 552 accident (Hellenic Air Accident Investigation and Accident safety Board, 2006). In addition, the methodology led to the identification of essential training required to reduce the severity of and potentially mitigate emergent errors, (e.g. ensuring the crew rapidly dons oxygen masks, and adequately descends the aircraft). Other safety constraints generated relate to prompts (e.g. Descent rate prompt) or automation (e.g. providing automatic descent). Technical design solutions for the cockpit were also considered to provide novel safety constraints, such as Automatic QRH checks, with sequence, time or progress prompts. All of which could be potentially used to reduce pilot workload during the decompression event. Of central concern and building on an advantage of the STAMP-STPA methods is that each of these safety constraints were developed in a way that does not attribute blame, using a non-causation focussed approach.

It is important to reiterate that the high-level control structure presented in Figure 1 is constructed based on the assumptions presented within the methods. Different assumptions may generate a different control structure, with different stakeholders, control actions and subsequent emergent unsafe control actions. A key aspect of STAMP is to emphasise, through the use of control structures and control loops, is that the identification of a ‘start’ and ‘end’ point for an UCA is an oversimplification. Some UCAs may link as one reads around a control loop. Others may start or end at different parts of the loops. Each UCA can, never the less, cause significant issues during the hazard under investigation, as such safety Constraints should be put in place to address each potential UCA. This may be particularly useful for an incident where the crew does not correctly address the failure due to the assumption of an incorrect mental model or lack salient emergency warnings. In fact the model successfully addressed the first major requirement in any pressurisation event, as shown in Table 1, the first action listed requires verification of the cabin altitude. Unfortunately, although not a rapid de-pressurisation, this primary concern was overlooked by the crew on Helios Flight 522 (Hellenic Air Accident Investigation and Accident safety Board, 2006), who mistook a pressurisation warning for an undercarriage warning, with fatal consequences. Future research hopes to explore whether similar safety constraints emerge when consider other hazard scenarios, for example an engine failure or a failure of cockpit display systems.

Leveson et al. (2003) points out that the use of a systemic accident model like STAMP may not be satisfying to those focussed on attributing blame, as it does not lead to the identification of single causal factor or variable. It does, however, offer a different perspective to chain of events models such as Fault Tree Analysis (FTA) (Barlow, 1973) and Failure Modes and Effects Analysis (FMEA) (Arnzen, 1964), by providing information about the changes needed at a system level to prevent, or minimise the impact of, accidents in the future. As each of the stakeholders identified in the high-level control structure are all considered at the same level of granularity, human based, machine/technology based, and organisation based constraints receive a level playing field.

Future works aims to explore the decompression event further, constructing additional control loops for other regions of the control structure and considering the role of dangerous terrain in greater detail. Furthermore it would be useful to consider other hazardous scenarios in order to examine whether the identified safety constraints within the current scenario would be beneficial during other hazardous events. This analysis can be further extended to consider the potential safety implication of moving forward to new proposals for flight operations (Harris, Stanton & Starr, 2015; Stanton, Harris, & Starr, 2016).

Conclusions

This research set out to explore the potential safety issues that can emerge when considering crew’s response to a rapid decompression scenario. This paper applied STAMP-STPA as a method to both elicit and address potential safety issues generated when considering a hypothetical aviation incident. Although technical solutions for addressing decompression scenarios are available, and increasingly added during production of newer business jets, the decompression scenario remains a useful gateway event when exploring systemic safety.

In addition to generating a large number of CAs and UCAs, initial safety constraints have been provided for each UCA, ranging from additional redundancy within the system, the development of future potential CONOPS, the provision of additional alarms and warnings, to remote monitoring and automation. These safety constraints are useful for considering ways in which to address the generated UCAs, including both required technology and potential developments within crew training procedures. Overall, the STAMP-STPA approach should be viewed as an additional tool to improving systemic safety. STAMP-STPA can be used to identify potential safety constraints that can inform and justify the development of new technology and software that could improve the overall safety of future flight operations.

Acknowledgements

This work was completed as part of the Future Flight Deck programme and was co-funded by Innovate UK.

The Authors would like to offer thanks to Dr. Andrew Astill (Future Flight Deck Programme Manager) for advice and feedback during preparation of this manuscript, and Joy Richardson for assistance in the production of the figures presented.

GLOSSARY OF TERMS

AOC Aircraft Operating Certificate

ATC Air Traffic Control

ATM Air Traffic Management

CA Control Action

CONOPS Concepts of Operations

CRM Crew Resource Management

FMEA Failure Modes and Effects Analysis

FRAM Functional Resonance Analysis Method

 FTA Fault Tree Analysis

GPWS Ground Proximity Warning System

QRH Quick Reference Handbook

SME Subject Matter Expert

STAMP Systems Theoretic Accident Model and Process

STPA System-Theoretic Process Analysis

UCA Unsafe Control Action

MSA Minimum Safe Altitude

References

Air Accident Investigation & Aviation Safety Board (AAIASB) Accident Investigation Report 11/ 2006 Accident of the a/c 5B-DBY of Helios Airways, Flight HCY522 on August 14, 2005, in the area of Grammatiko, Attikis, 33 km Northwest Of Athens International Airport

Air Accident Investigation Bureau of Singapore Interim ReportAirbus A380, Registration 9V-SKE Diversion To Baku, Azerbaijan, AIB/AAI/CAS.101 September 2015

Air Accidents Investigation Branch (1992). Report on the accident to BAC One-Eleven, G-BJRT over Didcot, Oxfordshire on 10 June 1990.(Aircraft Accident Report 1/92). Retrieved from <https://assets.publishing.service.gov.uk/media/5422faa7e5274a131400078d/1-1992_G-BJRT_2_.pdf>

Altabbakh, H., AlKazimi, M. A., Murray, S., & Grantham, K. (2014). STAMP–Holistic system safety approach or just another risk model? *Journal of Loss Prevention in the Process Industries*, *32*, 109-119.

Arnzen, H. E. (1964). Failure Mode and Effect Analysis. *A powerful engineering tool for component and system optimization*.

ATSB Research And Analysis Report B2006/0142 Final Depressurisation Accidents and Incidents Involving Australian Civil Aircraft 1 January 1975 to 31 March 2006

Barlow, R. E. (1973). *Fault Tree Analysis*. John Wiley & Sons, Inc.

Boardman, J., & Sauser, B. (2006, April). System of Systems-the meaning of. In *2006 IEEE/SMC International Conference on System of Systems Engineering* (pp. 6-pp). IEEE.

Carlock, P. G., & Fenton, R. E. (2001). System of Systems (SoS) enterprise systems engineering for information‐intensive organizations. *Systems Engineering*, *4*(4), 242-261.

Harris, D., & Stanton, N. A. (2010). Aviation as a system of systems: Preface to the special issue of human factors in aviation. *Ergonomics, 53 (2),* 145 – 148.

Harris, D., Stanton, N. A., & Starr, A. (2015). Spot the difference: Operational event sequence diagrams as a formal method for work allocation in the development of single-pilot operations for commercial aircraft. *Ergonomics*, *58* (11), 1773-1791.

Harvey, C., & Stanton, N. A. (2014). Safety in System-of-Systems: Ten Key Challenges. *Safety Science*, *70*, 358-366.

Hollnagel, E. (2004). Barriers and accident prevention. Aldershot, UK: Ashgate

Hollnagel, E. (2012). *FRAM, the functional resonance analysis method: modeling complex socio-technical systems*. Ashgate Publishing, Ltd.

Hutchins, E. (2010). Cognitive ecology. *Topics in Cognitive Science*, *2*(4), 705-715.

Johnson, C. W., & Holloway, C. M. (2003). The ESA/NASA SOHO mission interruption: Using the STAMP accident analysis technique for a software related ‘mishap’. *Software: Practice and Experience*, *33*(12), 1177- 1198.

Laracy, J. R., & Leveson, N. G. (2007, May). Apply STAMP to critical infrastructure protection. In *2007 IEEE Conference on Technologies for Homeland Security* (pp. 215-220). IEEE.

Leplat, J. (1984). Occupational accident research and systems approach. *Journal of Occupational Accidents*, *6*(1), 77-89.

Leveson, N. (2004). A new accident model for engineering safer systems. *Safety science*, *42*(4), 237-270.

Leveson, N. (2011). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press.

Leveson, N. G., Daouk, M., Dulac, N., & Marais, K. (2003). Applying STAMP in accident analysis. *Second Workshop on the Investigation and Reporting of Accidents,* Williamsburg, September 2003.

Lindberg, A. K., Hansson, S. O., & Rollenhagen, C. (2010). Learning from accidents–what more do we need to know? *Safety Science*, *48*(6), 714-721.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science*, *27*(2), 183-213.

Salmon, P. M., Cornelissen, M., & Trotter, M. J. (2012). Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP. *Safety Science*, *50*(4), 1158-1170.

Salmon, P., Williamson, A., Lenné, M., Mitsopoulos-Rubens, E., & Rudin-Brown, C. M. (2010). Systems-based accident analysis in the led outdoor activity domain: application and evaluation of a risk management framework. *Ergonomics*, *53*(8), 927-939.

Stanton, N. A., & Harvey C. (2016) Beyond human error taxonomies in assessment of risk in sociotechnical systems: a new paradigm with the EAST ‘broken-links’ approach. *Ergonomics, (In Press).*

Stanton, N. A., Harris, D., & Starr, A. (2016). The future flight deck: Modeling dual, single and distributed crewing options. *Applied ergonomics*, *53*, 331-342.

Stanton, N. A., Rafferty, L. A., & Blane, A. (2012). Human Factors Analysis of Accidents in System of Systems. *Journal of Battlefield Technology*, *15*(2), 23- 30.

Stanton, N., Salmon, P. M., Rafferty, L. A. Walker, G. H. Baber, C., & Jenkins, D. P. (2013). *Human factors methods: a practical guide for engineering and design*. Ashgate Publishing, Ltd.

Thomas, J., Antoine, B., Fleming, C., Spencer, M., Hommes, Q., Ishimatsu, T., Helferich, J. (2013) *STAMP experienced users tutorial*., MIT. Retrived from http://psas.scripts.mit.edu/home/get\_pdf.php?name=1-3-Advanced-Experienced-STPA-Guided-Exercise.pdf

Underwood, P., & Waterson, P. (2012). A critical review of the STAMP, FRAM and Accimap systemic accident analysis models. *Advances in Human Aspects of Road and Rail Transportation. CRC Press, Boca Raton*, 385-394.

Underwood, P., & Waterson, P. (2013). Systemic accident analysis: examining the gap between research and practice. *Accident Analysis & Prevention*, *55*, 154-164.