Ergonomics

ISSN: 0014-0139 (Print) 1366-5847 (Online) Journal homepage: http://www.tandfonline.com/loi/terg20

Modelling Distributed Crewing in Commercial Aircraft with STAMP for a Rapid Decompression Hazard

Kirsten Revell, Craig Allison, Rodney Sears & Neville Stanton

To cite this article: Kirsten Revell, Craig Allison, Rodney Sears & Neville Stanton (2018): Modelling Distributed Crewing in Commercial Aircraft with STAMP for a Rapid Decompression Hazard, Ergonomics, DOI: 10.1080/00140139.2018.1514467

To link to this article: https://doi.org/10.1080/00140139.2018.1514467

Accepted author version posted online: 06 Sep 2018.

Modelling Distributed Crewing in Commercial Aircraft with STAMP for a Rapid Decompression Hazard.

Kirsten Revell*, Craig Allison, Rodney Sears & Neville Stanton
*Corresponding Author:

Contact details:
Dr. Kirsten Revell: K.M.Revell@soton.ac.uk, 02380 596795
Dr. Craig Allison: Craig.Allison@soton.ac.uk, 02380 593148
Prof. Neville Stanton: N.Stanton@soton.ac.uk , 02380 599065
Address:
Human Factors Engineering, Engineering Centre of Excellence, Boldrewood Campus, University of Southampton, Burgess Road, Southampton, SO16 7QF UK

Capt. Rodney Sears: wilts8874@hotmail.co.uk, 077 177 90555
Address:
Human Systems Integration Group, Faculty of Engineering, Environment and Computing, Coventry University Priory Street Coventry, CV1 5FB UK

Keywords: Aviation; STAMP-STPA; Distributed Crewing; Rapid Decompression; Accident Analysis;

Acknowledgements
This work was co-funded by Innovate UK.

ABSTRACT
Changes to crewing configurations in commercial airlines are likely as a means of reducing operating costs. To consider the safety implications for a distributed crewing configuration, System Theoretic Accident Model and Processes (STAMP) was applied to a rapid decompression hazard. High level control structures for current operations and distributed crewing are presented. The CONOPS generated by STAMP-STPA for distributed crewing, and design constraints associated with Unsafe Control Actions (UCAs) are offered to progress the route to certification for distributed crewing, and improve safety in current operations. Control loops between stakeholders were created using System-Theoretic Process Analysis (STPA). The factors leading to the Helios 255 incident demonstrated the redundancy that a ground station could offer without the risk of hypoxia, during a decompression incident. STPA analysis also highlighted initial UCAs that could occur within the hypothetical distributed crewing configuration, prompting consideration of design constraints and new CONOPS for ground station design.

Keywords
SPO, Distributed Crewing, STAMP, STPA, Safety, Rapid Decompression

Practitioner Summary

SPO in commercial aircraft is likely as a means to reduce costs. This paper makes a case for distributed crewing using STAMP-STPA. Comparing current operations with a distributed crewing configuration, the redundancy offered by a ground station is demonstrated. Design constraints and new CONOPs for distributed crewing, and current operations are proposed.

Introduction

Crew costs are a significant proportion of overall operating costs in commercial aircraft, accounting for up to 35% for small aircraft, and 19% for larger aircraft (Harris et al. 2015). A reduction in crew members can be seen as a continuing evolution in commercial aviation, that has already experienced a reduction from 3 crew members due to automation (Landry, 2012). Further changes to crewing configurations are likely, particularly when considering long term cost reductions (Malik & Gollnick, 2016) and a distributed crewing configuration could have the potential to reduce crew costs when high workload phases of flight such as take off and landing are staggered to enable the pilot on the ground to 'co-pilot' multiple aircraft (Harris et al. 2015). Due to the potential consequences associated with introducing risk to commercial airlines, cost alone is an insufficient driver for change; an equivalent or enhanced level of safety must be demonstrated before distributed crewing can become a reality, and a route to certification is necessary.

The term 'distributed crewing' is often referred to as Single Pilot Operations (SPO). Traditional Concepts of Operations (CONOPS) for commercial airline, comprise roles of 'pilot flying' (PF) and 'Pilot not flying' (PNF) (Harris, 2001). There are many different views of how an SPO configuration could operate (Schmid & Korn, 2017). Some replace the PNF role completely with automation (Deutsch & Pew, 2005), others, like Harris (2007) envision an aircraft designed specifically for SPO using enhanced automation in conjunction with a ground station crew. There is also debate over whether the ground station support is provided by a single crew member for the entire journey (e.g. Comerford et al., 2013), or swapping between different ground crew members with different duties or specialisms for different phases of flight (Bilimoria et al, 2014; Kooltz et al. 2015; Schmid & Korn, 2017). This paper will retain the term 'distributed crewing' to highlight that it is referring to a simplified view of SPO with a sole pilot in the cockpit (operating an aircraft with existing technology and current CONOPS), in conjunction with a second pilot on the ground (with replicated controls and functionality at the ground station). It assumes the ground station co-pilot supports the PF in the air in a PNF or 'Pilot Monitoring' (PM) mode where possible, for the entire journey, taking on the role of routine support for take-off and landing for multiple aircraft. This is similar to the concept of 'harbour pilots' (Bilimoria et al.,2014; Koltz et al 2015), with the additional responsibility for providing assistance and support during non-normal flying conditions to navigate hazards.

A key concern surrounding the concept of a single pilot in the cockpit, is the loss of intervention or redundancy by another crew member if one crew member behaves unexpectedly and is unable or unwilling to operate the aircraft safely. The catalyst for this concern stems partly from high profile incidents such as Germanwings Flight 9525. On 24 March 2015, after waiting for the Captain to leave the flight deck and preventing his return, a Germanwings A320 First Officer put his aircraft into a continuous descent from FL380 into terrain, killing all 150 occupants. Investigation concluded the motive was suicide (Bureau d'Enquêtes et d'Analyses, 2016). This incident occurred in duel crew flight, but the First Office (FO) was able to take advantage of safety measures intended to prevent aircraft hijacking following the 9-11 attack when terrorists seized control of 4 airborne aircraft over the USA. The safety measure required the installation of a flight crew compartment door designed to resist penetration by small arms and grenade and capable of being locked or unlocked only from within the cockpit. The aim of this measure was to prevent forcible intrusions by *unauthorised* persons. However, it negated the assumed 'redundancy' of duel crewing when an *authorised* crew member is suicidal or intent on jeopardizing the flight. Following this incident, the EASA Task Force reinstated the 'rule of two' demanding two crew must always be present in the cockpit (European Commission, 2015).

The reinstatement of the 'rule of two', as a means for providing redundancy for a single crew member in the cockpit who is eliciting unexpected crew behaviour, relies on the second crew

member present in the cockpit both being able, and willing to behave in accordance with protocol for a safe flight. This second crew member must also have the authority to override the inappropriate actions of the first crew member. Evidence of incidents of unexpected pilot behaviour where the presence of *two* authorised crew present in the cockpit have failed to prevented an accident, diminishes both the 'rule of two' safety measure, and the position against distributed crewing. In fact, since there are normally only 2 pilots on a flight, cabin crew are often required to be present on the flight deck as the second crew member.

The incident with Helios Airways international passenger flight from Larnaca to Athens provides such evidence. On 14 August 2005, the Boeing 737-300 (Flight B733) lost contact with ATC en-route. The aircraft departed controlled flight and impacted terrain almost three hours after take-off, destroying the aircraft and killing all 121 occupants. Incapacitation of the flight crew due to hypoxia following a decompression incident occurred prior to the crash. A number of different factors led to this accident including the aircraft being released to service with the cabin pressurisation set to manual, the crew failing to detect this setting, misinterpretation of the cabin high altitude warning as the Takeoff Configuration Warning (TCW) and failure to observe an alert that indicated that the cabin oxygen masks had automatically deployed when the cabin altitude had exceeded 14,000 feet. The Investigation found that before hypoxia began to affect the flight crew's performance, inadequate crew resource management (CRM) had occurred within a context of systemic organisational safety deficiencies. Part of this problem may have been due to crew dynamics, in the pairing of a Captain with a known record for authoritarian exercise of command with a First Officer whose training records referred to lack of discipline with checklists and difficulties following Standard Operating Procedures (SOP) (Hellenic Air Accident Investigation and Accident safety Board, 2006).

It is clear that safety measures such as the 'rule of two' was ineffective in preventing the incident with Helios Airways and as such may offer little argument against distributed crewing. Indeed, Harris et al. (2015) put forward that being able to control the aircraft from the ground may lead to enhanced, not reduced levels of safety. Whilst pilot homicide-suicide is rare and can stem from a variety of causes outside the direct control of airlines (Kenedi et al., 2016), 40–50 rapid and gradual decompression events occurring worldwide annually (Aviation Medical Society of Australia and New Zealand, 2000). The authors believe hazards, such as rapid decompression, that may result in incapacitation could highlight a key benefit for enhancing safety though a change to distributed crewing configurations.

According to Leveson (2011), safety is a system property, not a component property. As such, safety must be controlled at the system, not component level. Leveson proposes safety analysis should be conducted through the Systems Theoretic Accident Model and Process (STAMP) and associated predictive hazard assessment method the System-Theoretic Process Analysis (STPA). STAMP is an accident-modelling framework designed for complex socio-technical systems eminently suitable for the aviation domain (Leveson, 2004). It differs from traditional safety methods that can encourage linear 'chain-of-failure-events' notions of causality and seek causation from component / human failures (Leveson, 2011) such as Fault Tree Analysis (FTA) (Barlow, 1973), Failure Modes and Effects Analysis (FMEA) (Arnzen, 1964). These traditional methods are not designed to represent, and therefore fully take into consideration, the contribution of system factors, so limiting the comprehensiveness of the safety analysis possible. Both the introduction of the safety door following 9-11 and reinstatement of the 'rule of two' could be seen as reactive measures focussing primarily on the last step of a causal, linear chain of events following a specific high profile incident, rather than arising from consideration of each incident within a broader, system perspective.

Previous work by the authors demonstrated the utility of the STAMP-STPA method in identifying factors central to the Helios 522 accident when applied to a theoretical rapid decompression scenario in current operations (Allison et al. 2017), and for scoping the assumptions for exploring this hazard within a distributed crewing configuration (Revell et al., 2016). This paper progresses this work with a view to advancing the safety case for a distributed crewing configuration by demonstrating the utility of a systems approach to safety by mapping out the extent, influence and interdependence of Unsafe Control Actions (UCAs). STPA has been offered by Flemming & Leveson (2014) to be a means of aircraft certification, and propose that safety

should be designed into systems from their conception (Fleming & Leveson, 2015). Unlike linear event based analyses that require consideration of component failure, the STAMP framework is suited to concept design phases by considering a constraint based control of safety (Haruka et al, 2011). As such this method is highly appropriate for considering the safety case for a different crewing configuration. A comparison of the results of STAMP-STPA analysis for both current operations (whereby a pilot and co-pilot are collocated in the cockpit) and distributed crewing (whereby a single pilot is in the cockpit, and another is in the ground station) will be presented with the Helios 522 accident used to demonstrate the benefits of ground station crew in a rapid decompression scenario. The CONOPs and safety constraints generated through STAMP-STPA are presented to demonstrate this method as a means to of progressing the route towards safety certification for distributed crewing from a systems perspective.

Method

STAMP represents socio-technical processes as systemic performances in a state of dynamic equilibrium (Leveson, 2004). As such it is particularly suited to the aviation domain that is considered a system of systems (Carlock & Fenton, 2001; Harris & Stanton, 2010) comprised of numerous complex independent agents, distributed across a wide network (Allison et al. 2017). STAMP conceptualizes the constraints on multiple levels resulting in a hierarchical control structure. Identified stakeholders (social, technical or human) constrain the system, interacting non-linearly via control actions and feedback (Leveson, 2011). Within the STAMP framework, functional processes are the result of constraints reducing the degrees of freedom of the behaviour of a socio-technical system. The STAMP framework enables STPA to direct the mapping of factors that may contribute to specific hazards occurring in socially technical systems. This analysis uses a standardised error taxonomy to identify UCAs in order to generate 'safety constraints' to enforce safety at a system level.

STAMP-STPA has been applied to multiples domains such as space (Owens et al, 2008; Nakao et al. 2011; Ishimatsu et al, 2013; Leveson, 2009; Leveson, 2005), nuclear (Thomas et al.,2012), rail (Suo, 2012; Song et al. 2012), military (Pereira et al., 2006; Abrecht, 2016), automobiles (Placke et al, 2015), and medical domains (Pawlicki et al., 2016; Leveson et al., 2016; Leveson et al., 2012). In the aviation domain STAMP – STPA has been applied to improve safety in ATM (Fleming & Levseon; 2015), for Rotary aircraft (Abrecht et al, 2016), for NextGen avionics (Fleming et al, 2014) and Rapid decompression events (Revell et al., 2016; Allison et al., 2017).

To conduct STAMP – STPA analysis, a series of iterative steps that represent the system as a whole from a high level of abstraction to progressively more detailed levels of granularity, are undertaken. STAMP is a scenario based method that requires the analysis to be scoped by an identified hazard that can result in a defined accident. After a hazard has been identified, a high-level hierarchical control structure is constructed representing all stakeholders within the system under analysis and the control actions that link the independent stakeholders. Control actions (CAs) describe the interactions and feedback loops between stakeholders and complete the STAMP analysis. STPA starts by identifying unsafe control actions (UCAs) for each CA through application of a standardized taxonomy. This is achieved through the application of four guide sentences (i.e. 1. Action required but not provided; 2. Unsafe action provided; 3. Incorrect timing / order; 4. Stopped too soon / applied too long) to each CA to elicit the possible failings within the system to generate a complete failure analysis (Leveson 2004). Not all guide sentences are applicable to each CA, and multiple UCAs may be generated by single guide sentences. Each UCA identified prompts the need for a design constraint to ensure safety. This analysis was tabulated in MS Excel. Finally, the causes for the UCAs can be analysed in more detail through the construction of feedback loops for UCAs of interest. These diagrams allow the interaction of multiple UCAs to be examined. Feedback loops can be simple, involving two stakeholders only, or more complex with 3 or more stakeholders. Stakeholders are considered from the perspective of 'controllers' and 'controlled processes', with UCAs generated using the guide sentences. Once identified, these UCAs can be mapped to different sections of the loop to gain a better understanding of causal scenarios that could result in the prescribed hazards (Leveson, 2011). Figure 1 depicts the generic control loop showing typical positions of UCAs defined according to the criteria prescribed.

Figure 1 - Generic Control loop for STPA analysis

The System Engineering Foundation

Accidents & Hazard Identification

To specifically highlight the benefits and disadvantages of a distributed crewing configuration compared to current duel crew operations, the rapid decompression scenario was viewed from the perspective of the 'crews response' to the incident, rather than from an external or mechanical cause. The STAMP-STPA System Engineering Foundation requires the identification of accidents (in terms of undesired or unplanned losses or mishaps) and associated hazards (a set of conditions that combined with a worst-case set of environmental conditions, will lead to an accident) and the link between the two. In this case, the accident under consideration related to A1: The loss of pilot control through hypoxia and incapacitation (resulting in unexpected crew behaviour). The specific hazards identified relating to 'crews response' to the worst case environmental condition of a rapid decompression event, were identified as H1:Crew fail to ensure adequate oxygen supply, and H2:Aircraft fails to descend to a safe altitude of 10,000ft (where it is normally possible to breath adequately without supplemental oxygen). Both hazards (H1 & H2) link to A1, the key accident under consideration. In the broader STAMP STPA analysis, the authors recognize that the crews' response to a rapid decompression event, if inappropriate, can also threaten the life of the crew and passengers through either eventual neurological damage and death (through hypoxia). If hypoxia or incapacitation results in an aircraft collision, the crew and passengers could suffer losses such as injury or death, and airlines would suffer property and financial loss. In addition, loss of control of airspace by ATC could occur through crew failing to alert ATC of an incident through a Mayday call. The authors wish to emphasise that this paper draws its boundaries for analysis around unexpected crew behaviour and will focus primarily on the accidents and hazards linked to hypoxia as specified.

Assumptions

The process of constructing the high level STAMP control structure required a number of assumptions to be made relating to both current operations and a hypothetical distributed crewing configuration. These are summarised in table 1 (amended from Revell et al., 2016).

Table 1 – Assumptions generated for analysis (Revell et al. 2016)

Method of Analysis

This paper presents the application of the STAMP-STPA analysis to a generic hypothetical event, rather than a specific accident. As such, the analysis was generated following workshops with Subject Matter Experts (SMEs). Three workshops were undertaken using Subject Matter Experts (SMEs) in Human Factors, STAMP and Aviation. To reduce bias and improve the validity of the outputs, an aviation expertise was provided by 3 separate experienced pilots, each attending a single workshop. The sequence, purpose, outputs and attendees for each workshop are shown in Table 2.

Table 2 – Data collection & analysis process for a hypothetical rapid decompression scenario

Results and Discussion

This section displays the analysis outputs of STAMP-STPA for a hypothetical rapid decompression incident. These include high level control structures, selected STPA tables, and complex control loops relating to both current operations and the proposed distributed crewing configuration. The outputs are discussed to demonstrate how the STAMP analysis prompts consideration of new CONOPs and design constraints for enhanced safety for a distributed crewing configuration. It also shows how STPA deepens the analysis by systematically considering UCAs for CONOPs to generate design constraints both for distributed crewing and current operations. Finally, the Helios 522 accident is considered with reference to control loops

constructed for both current operations and distributed crewing to demonstrate a systems view to the incident and the benefit of redundancy with the addition of a ground station.

STAMP – High Level Control Structures

The high level control structures for current operations and distributed crewing are shown in figure 2. The rectangles represent primary stakeholders linked by arrows representing CAs (thin line style) and feedback loops (thick line style). Some actions are continuously performed during the scenario (e.g. constant monitoring and feedback to crew of aircraft warning systems) and some denote intermittent actions (e.g. air accident report from airline to regulator). For brevity, and to help visualize the additional CAs and Feedback loops to those identified for current operations after the addition of a ground station, the high level control structures have been combined with current operations depicted with a solid line, and a dashed line used to highlight distributed crewing additions.

Figure 2 – High level control structures for STAMP analysis showing both current operations and (solid line) and the hypothesized additions for a distributed crewing configuration

In figure 2, five key stakeholders relevant for 'crews response to rapid decompression' were identified for current duel crew operations comprising (from the top of the hierarchy) the regulator, airline, crew, aircraft and air traffic control (ATC) / air traffic management (ATM). With reference to figure 2, the control structure for current operations will first be described from the perspectives of crew interactions, CAs and Feedback loops (solid lines in figure 2). The changes resulting by the addition of a ground station in a distributed crewing configuration will then be discussed (dashed lines in figure 2).

Current Operations

Crew interaction

In figure 2, the crew stakeholder provides a high level description of activities (e.g. cross checking) occurring between the pilot flying (PF) who conducts the progress of flight, and the pilot monitoring (PM) who monitors progress. CAs and feedback are not provided as PF and PM are represented within the crew stakeholder box. These activities were depicted to prompt consideration of how these interactions would change during a distributed crewing configuration.

Control Actions

Working from the top of the hierarchy down, the control actions associated with each stakeholder for current operations are considered in turn. The regulator (top, figure 2) provides an aircraft operating certificate (AOC) to the airline, allowing them to operate and charge to transport passengers and freight on its aircraft fleet (arrow from regulator to airline, top left figure 2). The airline is then responsible for ensuring its crew is provided recurrent training with simulators for emergency and non-standard situations (arrow from airline to crew, figure 2). In the event of a rapid decompression event, the crew is responsible for completing the Quick Reference Handbook (QRH) drills to ensure both adequate oxygen levels for the crew and adequate pressure levels in the cabin. This includes donning oxygen masks, and descending to 10,000 feet where terrain permits (arrow from crew to aircraft, figure 2). CAs also exist between the crew and ATC/ATM (arrow from crew direct to ATC/ATM, far left of figure 2) with a Mayday call made by crew (including route and aircraft position changes resulting from the incident). The interrogation of the onboard transponder (identifying aircrafts position, altitude and call sign) represents a CA from ATC/ATM to the aircraft.

Feedback Loops

Working from the bottom of the hierarchy up, a feedback loop is shown from ATC/ATM to the crew to acknowledge the Mayday call sent, and offer assistance (arrow from ATC/ATM to Crew, figure 2). ATC/ ATM will also receive data fed back on board aircraft sensors should the scenario result in an accident, represented in the CA from Aircraft to ATC/ATM (left arrow from ATC/ATM, figure 2). The aircraft itself feeds back information to the crew through a variety of warning systems, including terrain warning systems that guide and manage the descent in high terrain (arrow from aircraft to crew, figure 2). On board flight data generated by the aircraft is also fed back to the operating airline (right arrow from aircraft to airline, figure 2) along with post incident flight data (used to judge crew performance and inform future crew training programs). The crew feeds back to the airline via flight

and safety reports to the operating airline after each flight (arrow from crew to airline, figure 2). The final feedback arrow reaching the top of the current operations hierarchy represents air incident reports sent from airline to regulator (arrow from airline to regulator, figure 2).

Distributed Crewing

In the distributed crewing configuration it is hypothesized that a single crew member remains in the aircraft, and a single crew member associated with the flight in questions resides in a hypothetical ground station (see dashed boxes in figure 2). The addition of a ground station enables extra control actions and feedback loops between stakeholders to those previously identified in the current operations control structure. This section will describe the additional CAs and feedback loops proposed as supplementary, rather than as replacements to those in current operations. For brevity the existing interactions will not be restated. The key areas of interest when considering a crews' response to rapid decompression, center around the crew, aircraft and ground station, however links between ground station and the airline and ATC/ATM stakeholders were hypothesized as relevant to the rapid decompression scenario under analysis (figure 2).

Crew Interaction

In the distributed crewing configuration, it is assumed that the single crew in the air will take prime responsibility for conducting the flight and the crew in the ground station for monitoring the progress of the flight. Underpinned by the assumption of a perfect communications link between crew and ground station, this analysis led to suggestion of new CONOPs. For example, crew (air) could verbalise checklists as actions were taken (dashed arrow from crew to ground station, figure 2). During the rapid decompression incident, in addition to calling a Mayday to ATC/ATM, it also proposed that the single crew (air) could request assistance from crew (ground), or conversely, crew (ground) could offer targeted assistance (dashed arrows from ground station to crew, figure 2). Underpinned by the assumption that an identical set of aircraft controls are present in the ground station, new CONOPS are offered whereby crew (ground) complete QRH drills within a safer environment but in conjunction with crew (air) to allow a faster response and recovery of the emergency. The crew (air) could also request the ground station interact directly with the aircraft instrumentation to assist in controlling the descent of the aircraft. Should hypoxia affect the crew (air), this may be picked up by the crew (ground) by issues identified when crew (air) verbalise checklists. Boy (2015) put forward that ground crew staff could adopt a role of monitoring for incapacitation (when considering technical solutions for health monitoring of pilots). This could prompt a new CONOP whereby the ground station takes full control of the aircraft if it becomes clear that the crew (air) is eliciting unexpected behaviour likely to place the aircraft and passengers at risk. The crew (ground) could then remotely ensure QRH checks are performed correctly and the descent to 10k feet is achieved. Schmid & Korn (2017) propose an SPO CONOP of this kind, where mandatory taking over control by the ground station occurs when critical criteria have been met such as high workload or incapacitation.

Control Actions

In addition to the CAs associated with crew interaction the ground station could assist the crew (air) by calling Mayday to ATC/ATM (dashed arrow from ground station to ATC/ATM, figure 2). The Airline stakeholder will have a responsibility to ground station crew to offer sufficient recurrent training for an effective remote respond to a rapid decompression hazard (dashed arrow from airline to ground station). This response may take the form of new CONOPS whereby the crew (ground) supply targeted information gained directly form ATC/ATM, or provide assistance by operating the flight controls as described above.

Feedback Loops

In addition to feedback loops associated with crew interaction, it was modeled that the ground station would have a responsibility to the airline to submit flight and safety reports to the airline to ensure training remains current and effective (dashed arrow from ground station to airline, figure 2). In the event that crew (air) become incapacitated, feedback from ATC/ATM to ground station would allow crew (ground) to check acknowledgment of a Mayday to ensure assistance was on the way. New CONOPS could be developed whereby ATC/ATM interact directly with crew (ground) to filter feedback from aircraft. Using the data link to show the results from QRH checks by crew (air) to crew (ground) would enable crew (ground) to verify verbal checklists by crew (air). This would be another way for the ground station to monitor and ensure crew were behaving as expected during a rapid decompression hazard. Feedback regarding the progress of descent could also be conveyed in this way enabling the crew (ground) to provide targeted assistance (dashed arrow from aircraft to ground station,

figure 2).

STPA Analysis – UCA tables and design constraints

The full STPA analysis revealed 11 CAs and 78 UCAs in current operations, and an additional 8 CAs and 54 UCAs when considering the hypothetical distributed crewing configuration. This section provides extracts of STPA tables in both current operations and distributed crewing configurations. Table 3 shows extracts of CAs from Crew (air) to Aircraft, ATC/ATM and Ground Station. Table 4 displays extracts of CAs from Ground Station to Aircraft and ATC/ATM. These provide evidence of the exhaustive and systematic process undertaken to generate design constraints to improve safety.

Table 3 - STPA table output showing UCAs and Design constraints arising from CAs from Crew to Aircraft, ATC/ATM and Ground Station.

Table 3 provides an extract of STPA analysis focusing on 3 CAs from Crew. 'Mayday call' to ATC and 'conduct QRH drills' to Aircraft are considered in both crewing configurations (with the additional UCAs and design constraints for distributed crewing highlighted in grey). The final CA 'Request Assistance' from Ground Station is present only in the distributed crewing condition (also shown in grey). From table 3 it is clear that the STPA analysis can also offer new design constraints for current operations, particularly where automation and alerts are suggested as these could more easily be implemented in a cockpit.

When considering UCAs for the Mayday call that could result in urgent help not being provided, novel automated or technical solutions, such as: 'relevant data sent automatically to ATC' if the Crew (Air) provide erroneous information to ATC, an Automated Mayday call to ATC when appropriate conditions are sensed, or an automated continuous Mayday call until acknowledge by ATC, if the crew stop the Mayday before acknowledged by ATC. In the distributed crewing configuration, the Ground station crew could act as redundancy in an environment not subject to the risk of hypoxia by taking the responsibility to call Mayday on behalf of Crew (air) if they fail to do so, or plan to do so too late. By monitoring communications between Crew (air) and ATC, the Ground station crew could query any misinformation based on comparison with data feeds to Ground Station direct from the Aircraft. Similarly through monitoring the Mayday call to ATC, the Ground Station crew could reinstate a Mayday call if stopped before acknowledgement.

Considering UCAs for 'Conduct QRH Drills' in response to a decompression incident, that could result in key steps missed that could lead to hypoxia (i.e. failing to put on Oxygen masks and failing to descend to 10k feet), design constraints considered include automated QRH checklists that prompt initiation of the QRH checks (if crew fail to conduct the drills), provide a sequence prompt (if QRH steps are missed or completed in the wrong order), and a progress or time prompt (if QRH steps are stopped before complete, or take too long). In a distributed crewing configuration, the ability of the Ground Station crew to monitor an automated QRH list as described (see figure 2), would enable them to offer assistance at conducting the QRH checks. It might also be a means for diagnosing disorientation by onset of hypoxia (in addition to assessment of Crew verbalizations) triggering a new CONOP to take control of the flight from the safe environment of the Ground station should the Aircraft and passengers be deemed to be at risk.

In the distributed crewing configuration, the CA for the Crew (air) to request assistance from Ground station could leave the single crew member with high workload when dealing with a rapid decompression incident, if they fail to request assistance, request assistance too late or refute the need for assistance. The transfer of data on aircraft state (including warnings) direct to the Ground Station (see figure 2) could require CONOPs such as the Ground station crew proactively offering assistance to Crew (air) in the form of monitoring, warning or taking over control if necessary.

Table 4 – STPA table output showing UCAs and Design constraints arising from CAs from Ground Station to Aircraft and ATC/ATM.

Table 4 provides an extract of STPA analysis focusing on 2 CAs from Ground Station in the distributed crewing configuration. 'Ground monitors Aircraft (switch positions with QRH Checks)' was a CA to provide redundancy to the Crew (air) in the 'co-pilot' role. With the suggestion that the ground station provides co-piloting support as well as acts as redundancy to the Crew (air), the STPA analysis must also consider UCAs could occur from the Ground station itself. A failure in the CA for ground station crew to effectively monitor QRH checks undertaken by Crew (air), could result in key steps, such as the donning of Oxygen masks and initiation of a

descent to 10K feet, being missed without correction. Design constraints relating to an automated QRH checklist fully synched with the Ground station was suggested, such that Ground station crew members could be prompted for monitoring in the same way that Crew (air) are prompted for action. This design constraint would also aid ground station crew if deemed necessary that they take over full responsibly for conducting the QRH drills from a request for assistance by the Crew (air) or a diagnosis that the Crew (air) were suffering from hypoxia.

The CA for Ground station crew to call Mayday to ATC/ATM in place of the Crew (air) would occur due to a request by Crew (air), or as redundancy due to an error or diagnosis of incapacitation of Crew (air). Failures in this CA could lead to ATC being unaware of the aircraft incident and potential diversion. Should the Ground station crew fail to call Mayday, provide erroneous information, or stop the Mayday call before acknowledgement, the same design constraints as for current operations would provide a safety constraint (e.g. automated Mayday call, relevant data sent directly to ATC, continuous Mayday until acknowledgment). Given that the Ground station crew would not be subject to the conditions causing hypoxia, UCAs relating to QRH drills or Mayday calls may be caused by high workload from co-piloting multiple flights, or lack of training. Operational design constraints are included in Table 4 suggesting the addition of a 'safety supervisor' in the Ground station to monitor non-normal incidents across a range of aircraft. This could be either to direct the relevant Crew (ground) to focus on the incident, to free up their workload by managing the incident, or relieve conflicting duties such as routine take-offs and descents for the other aircraft being managed. Ground station CONOPs and adequate emergency training would also need to be devised and provided for a robust distributed crewing configuration.

STPA Analysis – Control Loops

This section presents two control loops constructed to more deeply compare UCAs for current operations (figure 3) and the hypothetical distributed crewing configuration (figure 4) at a system level. The stakeholders represented in the control loops comprise Crew, Aircraft, ATC/ATM (for current operations), and the addition of Ground Station (for distributed crewing). The diagrams represent key CAs relating to QRH drills to ensure appropriate cabin pressure, including calling Mayday, the donning of oxygen masks and undertaking a descent to 10,000 feet (described for brevity as O_2 and descent QRH steps respectively). The direction of the thicker arrows in figures 3 and 4 indicate the 'controller' and the 'controlled process', whereas thin arrows represent feedback loops between these stakeholders. Following the systematic generation of UCAs by considering each CA in turn, the control loops presented in figures 3 and 4 bring the analyst back to a system view of a 'crews response to rapid decompression'. Here the impact of multiple UCAs are considered in unison to emphasise the over-simplification often found in linear error analysis that there exists a single 'start' and 'end' point for an accident. Some UCAs may occur within a single loop, others may cross multiple loops. To illustrate how the distributed crewing configuration could offer a considerable level of redundancy to a crews response to a decompression incident, the UCAs identified that correspond to those documented Air Accident Investigation and Accident safety Board report (2006), for the Helios 522 accident (*italicised*) will be considered for both configurations.

Figure 3 – Control loop comprising Crew, Aircraft and ATC/ATM for current operations

Figure 3 shows the control loop between Crew, Aircraft and ATC for current operations. Despite correct functioning of the equipment, the crew '*ignored the cabin pressure altitude warning'.* Their actions indicated that the warning had been misinterpreted as a take-off configuration warning suggesting they had an '*incorrect mental model of aircraft state'*. The warning was not cancelled resulting in '*cabin altitude warning continues too long'* creating an intrusion that may have affected decision making. The crew took no corrective action so '*failed to conduct QRH Checks*'. By missing the '*O2*' and '*descent*' steps that would have occurred during the QRH drill, the crew remained increasingly at risk of hypoxia effecting decision making and psychomotor performance. When the descent due to fuel exhaustion began, evidence of a Mayday message recorded on the cockpit voice recorder (CVR) was found, but the button to transmit to ATC was not pressed. The crew were '*too slow to call ATC*', and due to hypoxia '*were unable to call Mayday*' so ultimately '*failed to call ATC'.*

Figure 4 – Control loop comprising Crew (air), Ground Station, Aircraft and ATC/ATM for distributed crewing configuration.

Figure 4 shows the same control loop structure in a distributed crewing configuration, where the addition of a Ground Station enables redundancy in communications to ATC, feedback to Crew (Air) and monitoring of Aircraft state. The UCAs identified from the Helios 522 incident will be considered in turn. When the cabin pressure altitude warning sounded, Feedback of warnings from aircraft to ground station would have alerted the ground station crew to offer assistance to the Crew (air). This would only have been precluded (since the warning system in this case was functioning correctly), if the unlikely coincidence that the ground station crew also had an '*incorrect mental model of the aircraft*' and '*failed to notify the crew about the pressure warning'.* After notifying the Crew (air) of the air pressure warning, the Crew (air) or the Ground station crew (remotely) could then cancel the alert to prevent distraction to decision making from '*cabin altitude warning continues too long'*. The Ground station crew could then offer assistance with QRH checks to prevent '*failure to conduct QRH Checks'.* By monitoring the QRH checks the Ground station crew could ensure the '*O2*' and '*descent*' steps occurred. By monitoring communications from Crew (air) to ATC, the ground station crew could prevent the '*failed to call ATC*' UCA by making the call from the Ground station and checking for acknowledgement. If the Ground station crew diagnosed the Crew (air) were experiencing the effects of hypoxia, or were incapacitated, the Ground station crew could take control of the descent of the aircraft to 10k feet and divert to safety.

Whilst there are a number of UCAs attributable to the ground station crew, those relating to confusion or poor decision making are considerably less likely as the ground station will not be at risk of hypoxia. The authors consider the UCAs most likely to come into play in this particular example would be due to the attention of the ground station crew on routine assistance of other aircraft (take-off and landing). This may result in '*Ground offers assistance too late*', '*Ground responds to request for assistance too late' and 'Ground late calling Mayday'*. The design constraints suggested relating technological aids and operational organisation within the ground station (e.g. provision of a safety supervisor) would therefore need to be adopted for effective ground station support. It seems clear that depending on whether the rapid decompression hazard occurred during a passive monitoring, or active co-piloting period for the ground station crew, will determine if a 'harbour pilot' style role (Bilimoria et al., 2014; Koltz et al., 2015) may be able to provide effective support for a sole crew in the air. Bilimoria et al., (2014) describe passivation systems in the event of hijacking. Such a system applied to incapacitation, could provide redundancy to UCAs by ground control staff where a rapid decompression event occurred at the same time as scheduled support for take off and landing for alternate aircraft, minimising the cost for additional ground staff. Bilimoria et al. (2014) propose a 'hybrid' ground operator which serves multiple aircraft but will hand over to a dedicated ground station co-pilot in case a non-normal situation (such as rapid decompression) should occur (Schmid & Korn, 2017).

This paper has demonstrated through STAMP/STPA analysis how a distributed crewing configuration with a single pilot in the air and a single co-pilot in a ground station, has the potential to improve safety to duel crew in current operations, using a hypothetical rapid

decompression event. To further this work, the authors endorse STAMP-STPA, as well as other accident analysis methods or modelling techniques (see Stanton et al.2016), to be applied to ever evolving concepts of SPO and ground station design considering a variety of hazards. In particular, hazards that could result in unexpected pilot behaviour, or incapacitation as well as consideration of multiple controller hazards are necessary to ensure a robust route to certification for distributed crewing.
The example of Helios 255 was used to demonstrate the redundancy that a ground station could offer for enhanced safety compared to that for current operations, where pilots in the air may be at risk of incapacitation. The STPA analysis also proposed technological design constraints, such as automation and warnings, of benefit to current operations. Design constraints to ensure a hypothetical distributed crewing configuration with safety at its conception, suggested additional automation, and extra ground crew staff to support routine co-piloting staff, to monitor non-normal flight.

Conclusion

To progress the route to safety certification for a distributed crewing configuration, a STAMP-STPA analysis was applied to a hypothetical rapid decompression hazard to consider the risk of unexpected crew behaviour (e.g. due to hypoxia). High level control structures for current operations and a distributed crewing configuration were compared in terms of crew interactions, control actions and feedback loops. Design constraints were generated in response to UCAs to not only consider the safety steps required for the route to certification for distributed crewing, but also to improve the safety of current operations. These included automation, redundancy, new CONOPS, remote monitoring, remote control of aircraft, and alarms and warnings. The benefits of how the addition of a ground station could provide life-saving redundancy in a decompression incident, compared to current operations, was demonstrated by the factors relating to the Helios 255 incident at a system level using control loops examining Crew, Aircraft, ATC and Ground station. For the benefits of distributed crewing to be realised, the need to ensure appropriate design constraints relating to ground station support and CONOPs was emphasised.

References

Abrecht, B., Arterburn, D., Horney, D., Schneider, J., Abel, B. and Leveson, N., 2016, February. A New Approach to Hazard Analysis for Rotorcraft. In *American Helicopter Society Specialists Meeting on Development, Affordability, and Qualification* (pp. 9-10).

Abrecht, B.R., 2016. *Systems Theoretic Process Analysis Applied to an Offshore Supply Vessel Dynamic Positioning System* (Doctoral dissertation, Massachusetts Institute of Technology).

Air Accident Investigation & Aviation Safety Board (AAIASB) (2006) 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, 33km Northwest Of Athens International Airport

Allison, C.K., Revell, K.M., Sears, R. and Stanton, N.A., 2017. Systems Theoretic Accident Model and Process (STAMP) safety modelling applied to an aircraft rapid decompression event. *Safety Science*, *98*, pp.159-166.

American Institute of Aeronautics and Astronautics, Reston, VA, 2016, p. 3303.

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

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

Bilimoria, K. D., Johnson, W. W., and Schutte, P. C., Conceptual Framework for Single Pilot Operations," Proceedings of the International Conference on Human-Computer Interaction in Aerospace, HCI-Aero '14, ACM, New York, NY, 2014.

Boy, G. A., Requirements for Single Pilot Operations in Commercial Aviation: A First High-Level Cognitive Function Analysis," Complex Systems Design & Management, edited by F. Boulanger, D.

Korb, G. Morel, and J.C. Roussel, Springer International Publishing, Cham, Switzerland, 2015, pp. 227-234.

Bureau d'Enquêtes et d'Analyses (BEA) (2016) Final Report, Accident, 24.03.2015, Alpes-de-Haute-Provence, France, Germanwings, A320-211, D-AIPX

Fleming & Leveson, "Improving hazard analysis and certification of integrated modular avionics", *Journal of Aerospace Information Systems*, vol. 11, pp. 397-411, June 2014.

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

Comerford, D., Brandt, S. L., Lachter, J., Wu, S.C., Mogford, R., Battiste, V., and Johnson, W. W., NASA's Single-Pilot Operations Technical Interchange Meeting: Proceedings and Findings," 2013. Deutsch, S. and Pew, R. W., Single Pilot Commercial Aircraft Operation," 2005.

European Commision, (2015), Task Force on Measures Following the Accident of Germanwings Flight 9525 Final Report, http://ec.europa.eu/transport/modes/air/news/doc/2015-07-17-germanwings-report/germanwings-task-force-finalreport.pdf

Fleming, C.H. and Leveson, N., 2015, October. Integrating Systems Safety into Systems Engineering during Concept Development. In *INCOSE International Symposium* (Vol. 25, No. 1, pp. 989-1003).

Fleming, C.H. and Leveson, N.G., 2014. Improving hazard analysis and certification of integrated modular avionics. *Journal of Aerospace Information Systems*.

Harris, D., & Stanton, N. A. (2010). Aviation as a system of systems: Preface to the

Harris, D., A human-centred design agenda for the development of single crew operated commercial aircraft," Aircraft Engineering and Aerospace Technology, Vol. 79, No. 5, 2007, pp. 518-526.

Harris, D., Human Performance on the Flight Deck, Ashgate, Surrey, United Kingdom, 2011.

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 singlepilot operations for commercial aircraft. Ergonomics 58, 11, 1773-1791

Ishimatsu, T., Leveson, N.G., Thomas, J.P., Fleming, C.H., Katahira, M., Miyamoto, Y., Ujiie, R., Nakao, H. and Hoshino, N., 2014. Hazard analysis of complex spacecraft using systems-theoretic process analysis. *Journal of Spacecraft and Rockets*.

Kenedi, C., Friedman, S. H., Watson, D., & Preitner, C. (2016). Suicide and Murder-Suicide Involving Aircraft. *Aerospace Medicine and Human Performance*, *87*(4), 388–396.

Koltz, M. T., Roberts, Z. S., Sweet, J., Battiste, H., Cunningham, J., Battiste, V., Vu, K.-P. L., and Strybel, Landry, S. J., Human Factors and Ergonomics in Aviation," Handbook of Human Factors and Ergonomics, edited by G. Salvendy, John Wiley & Sons, Hoboken, NJ, 2012, pp. 1667{1688.

Leveson, N. (2011). Engineering a safer world: Systems thinking applied to safety. Mit Press.

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

Leveson, N., Couturier, M., Thomas, J., Dierks, M., Wierz, D., Psaty, B.M. and Finkelstein, S., 2012. Applying system engineering to pharmaceutical safety. *Journal of Healthcare Engineering*, *3*(3), pp.391-414.

Leveson, N., Samost, A., Dekker, S., Finkelstein, S. and Raman, J., 2016. A systems approach to 13nalysing and preventing hospital adverse events. *Journal of Patient Safety*.

Leveson, N.G., 2004. A systems-theoretic approach to safety in software-intensive systems. *IEEE Transactions on Dependable and Secure computing*, *1*(1), pp.66-86.

Leveson, Nancy G., "Software Challenges in Achieving Space Safety," *Journal of the British Interplanetary Society* (JBIS), Volume 62, 2009.

Malik, A. and Gollnick, V., Impact of Reduced Crew Operations on Airlines "Operational Challenges and Cost Benefits," 16th AIAA Aviation Technology, Integration, and Operations Conference, Vol. AIAA 2016-3303 of AIAA Aviation,

Nakao, H., Katahira, M., Miyamoto, Y. and Leveson, N., 2011, April. Safety guided design of crew return vehicle in concept design phase using STAMP/STPA. In *Proc. Of the 5th IAASS Conference* (pp. 497-501).

Nakao, H., Katahira, M., Miyamoto, Y. and Leveson, N., 2011, April. Safety guided design of crew return vehicle in concept design phase using STAMP/STPA. In *Proc. Of the 5th IAASS Conference* (pp. 497-501).

Owens, B.D., Herring, M.S., Dulac, N., Leveson, N.G., Ingham, M.D. and Weiss, K.A., 2008, March. Application of a safety-driven design methodology to an outer planet exploration mission. In *Aerospace Conference, 2008 IEEE* (pp. 1-24). IEEE.

Pawlicki, T., Samost, A., Brown, D.W., Manger, R.P., Kim, G.Y. and Leveson, N.G., 2016. Application of systems and control theory-based hazard analysis to radiation oncology. *Medical physics*, *43*(3), pp.1514-1530.

Pereira, S.J., Lee, G. and Howard, J., 2006. *A system-theoretic hazard analysis methodology for a non-advocate safety assessment of the ballistic missile defense system*. MISSILE DEFENSE AGENCY WASHINGTON DC.

Placke, S., Thomas, J. and Suo, D., 2015. *Integration of Multiple Active Safety Systems using STPA* (No. 2015-01-0277). SAE Technical Paper.

Revell, K., Allison, C., Stanton, N., and Sears, R., Modelling Distributed Crewing with STAMP," Proceedings of the International Conference on Human-Computer Interaction in Aerospace, HCI-Aero '16, ACM, New York, NY, 2016.

Schmid, D. and Korn, B., 2017. A Tripartite Concept of a Remote-Copilot Center for Commercial Single-Pilot Operations. In *AIAA Information Systems-AIAA Infotech@ Aerospace* (p.64).

Schutte, P. C., Complemation: An Alternative to Automation," Journal of Information Technology Impact, Vol. 1, No. 3, 1999, pp. 113{118.

Song, T., Zhong, D. and Zhong, H., 2012. A STAMP analysis on the China-Yongwen railway accident. *Computer safety, reliability, and security*, pp.376-387.

special issue of human factors in aviation. Ergonomics, 53 (2), 145 – 148.Stanton, N.A., Harris, D. and Starr, A. (2016) The future flight deck: Modelling dual, single and distributed crewing options. *Applied Ergonomics*, 53, 331-342.

Suo, D., 2012. A System Theoretic Analysis of the ‘‘7.23’’ Yong-Tai-Wen Railway Accident. <http://psas.scripts.mit.edu/home/get_pdf.php?name=System- Theoretic-Accident-Analysis-of-Railway-Accident.pdf> (accessed 27.10.17).

Koltz MT, Roberts ZS, Sweet J, Battiste H, Cunningham J, Battiste V, Vu KPL, Strybel TZ (2015) An investigation of the harbor pilot concept for single pilot operations. Procedia Manuf 3:2937–2944

Thomas, J., Lemos, F. and Leveson, N., 2012. Evaluating the safety of digital instrumentation and control systems in nuclear power plants. *NRC Technical Research Report2013*.

Table 1 – Assumptions generated for analysis (Revell et al. 2016)

Current CONOPS are assumed for defined hazards, CAs and UCAs identified through the analysis.	CONOPS are maintained, with the pilot flying being undertaken by Crew (air) and pilot monitoring role being undertaken by Crew (ground) located in the Ground station *(the analysis process was used to suggest new CONOPS needed in a distributed crewing configuration).*
Crew follow SOPs that have been taught and outlined within the available Quick Reference Handbook (QRH) and cross check monitoring and CRM is adequate.	A perfect data link exists between ground station and the aircraft, with no delay between actions or communications *(a significant technical challenge beyond the scope of this analysis).*
The operational state and capacity of the airline is sound, fully certified and airworthy. The Airline has a current Aircraft Operating Certificate (AOC), and ensures adequate crew training and post training examination.	Ground station crew has access to identical controls, instrument and aircraft feeds, as the crew (air) with the capability to take control of the aircraft remotely where necessary.
The flight path avoids mountainous terrain (i.e. Ground Proximity Warning System would allow the descent to 10,000 feet).	Communication and social issues not jeopardized with data link *(how this is achieved is beyond the scope of this analysis)*

Table 2 – Data collection & analysis process for hypothetical rapid decompression scenario

Workshop 1	• Identify appropriate scenario • Define associated hazards of interest	2 x Human Factors Analysts 1 x Pilot SME
Workshop 2	• Define assumptions for theoretical scenario • Construct 2 x high level control structures for STAMP (current and distributed crewing configurations) • Identification of UCAs and generation of Design Constraints • Construction of control loops (current and distributed crewing configurations)	3 x Human Factors Analysts 1 x STAMP expert 1 x Pilot SME
Workshop 3	• Independent validation of all outputs	2 x Human Factors Analysts 1 x Pilot SME

Table 3 - STPA table output showing UCAs and Design constraints arising from CAs from Crew to Aircraft, ATC/ATM and Ground Station.

Control Action from CREW (Air)	To	Safety consideration	Crewing Configuration	1. Action required but not provided	Design constraint	2. Unsafe action provided	Design constraint	3. Incorrect timing or order	Design constraint	4. Stopped too soon / Applied too long	Design constraint
MAYDAY Call	**ATC**	Urgent Help not provided. ATC unaware of aircraft incident and diversion or unable to provide guidance relating to desent and diversion.	Current Operations	CREW (Air) fail to call MAYDAY to ATC following decompression event so assistance is not provided and diversion is not offered (e.g. misdiagnose situation, lack of experience) **H2**	Automated MAYDAY call when critical conditions in aircraft sensed. Warning Alert to CREW when critical conditions sensed. Ensure Adequate training	CREW communicate Misleading / erroneous information regarding incident to ATC following decompression event. ATC unable to provide correct assistance (e.g. if incident misdiagnosed) **H2**	Ensure Adequate training Relevant data sent automatically to ATC	CREW (Air) call MAYDAY too late following decompression event so assistance arrives too late [e.g. if late diagnosing problem, poor CRM or inexperienced CREW) **H2**	Non-punative culture for unecessary MAYDAY calls Automated MAYDAY calls when appropriate conditions sensed	CREW (Air) stops MAYDAY call before it is acknowledged by ATC following decompression event so lack of certainty that assistance will be provided (e.g. if early onset of hypoxia impairs judgement, lack of experience, misdiagnosing problem has been solved) **H2**	Automated continuous Mayday until acknowledged by ATC Ensure sufficent staffing levels at ATC so call is responded to promptly
			Distributed Crewing	CREW (Air) fail to call MAYDAY to ATC following decompression event so assistance is not provided and diversion is not offered (e.g. misdiagnose situation, lack of experience) **H2**	CREW (Ground) act as redundency and call MAYDAY based on Aircraft data	CREW communicate Misleading / erroneous information regarding incident to ATC following decompression event. ATC unable to provide correct assistance (e.g. if incident misdiagnosed or CREW (Air) are inexperienced) **H2**	CREW (Ground) monitor COMMs to ATC and query information based on A/C data.	CREW (Air) call MAYDAY too late so assistance arrives too late following decompression event (e.g. if late diagnosing problem, poor CRM or inexperienced CREW) **H2**	CREW (Ground) act as redundency and call MAYDAY based on Aircraft data	CREW (Air) stops MAYDAY call before it is acknowledged by ATC following decompression event so lack of certainty that assistance will be provided (e.g. if early onset of hypoxia impairs judgement, lack of experience, misdiagnosing problem has been solved) **H2**	CREW (Ground) monitors COMMS between CREW (Air) & ATC and reinstate MAYDAY based on Aircraft data
Conduct QRH Drills	**AIRCRAFT**	Step missed (e.g. Oxygen / descent steps) so lack of oxygen or lack of descent. Risk of hypoxia from inadequate conditions for breathing	Current Operations	CREW (Air) Fail to conduct QRH Checks following decompression event so conditions for breathing are compromised (e.g. if situation is misdiagnosed) **H1/H2**	Electronic QRH checks with **initiation** prompt	CREW omit QRH steps (e.g. Oxygen masks, descend to 10K feet) following decompression event so conditions to prevent hypoxia are compromised (e.g. due to lack of experience, early onset hypoxia) **H1/H2**	Automatic Electronic QRH checks with **sequence** prompt	CREW undertakes QRH checks too slowly following decompression event so early effects of hypoxia are experienced (e.g. through lack of experience) **H1/H2**	Electronic QRH checks with **Time** prompt	CREW stops QRH checks too soon following decompression event so key steps are missed (e.g. through lack of experience of rapid decompression, or poor CRM) **H1/H2**	Electronic QRH checks with **Progress** prompt
								CREW performs QRH checks in wrong order following decompression event so 02 masks are not prioritized risking early onset hypoxia (e.g. through lack of experience) **H1**	Automatic Electronic QRH checks with **sequence** prompt	CREW (Air) have long delays between QRH actions following decompression event so early effects of hypoxia are felt (e.g. through uncertainty that the problem has been correctly diagnosed) **H1/H2**	Electronic QRH checks with **Time** prompt
			Distributed Crewing	CREW (Air) Fail to conduct QRH Checks following decompression event so conditions for breathing are compromised (e.g. if situation is misdiagnosed) **H1/H2**	Electronic QRH checks with **initiation** prompt monitored by CREW (Ground) CREW (Ground) takes control	CREW omit QRH steps (e.g. Oxygen masks, descend to 10K feet) following decompression event so conditions to prevent hypoxia are compromised (e.g. due to lack of experience, early onset hypoxia) **H1/H2**	Automatic Electronic QRH checks with **sequence** prompt monitored by CREW (Ground) CREW (Ground) takes control	CREW undertakes QRH checks too slowly following decompression event so early effects of hypoxia are experienced (e.g. through lack of experience) **H1/H2**	Electronic QRH checks with **Time** prompt monitored by CREW (Ground) CREW (Ground) takes control	CREW (Air) stops QRH checks too soon following decompression event so key steps are missed (e.g. through lack of experience of rapid decompression, or poor CRM) **H1/H2**	Electronic QRH checks with progress prompt monitored by ground control CREW (Ground) takes control
								CREW perform QRH checks in wrong order following decompression event so 02 masks are not prioritized risking early onset hypoxia (e.g. through lack of	Automatic Electronic QRH checks with **sequence** prompt monitored by CREW (Ground) CREW (Ground) takes control	CREW (Air) have long delays between QRH actions following decompression event so early effects of hypoxia are felt (e.g. through uncertaintly that	Electronic QRH checks with **Time** prompt monitored by ground control CREW (Ground) takes control
Requests Assistance	**GROUND STATION**	Single crew left to manage workload in isolation so risk that key actions to prevent hypoxia/incapacitance are not enacted effectively	Distributed Crewing	CREW (Air) Fail to request assistance from CREW (Ground) following decompression event so workload is increased (e.g. due to lack of experience / trust with CREW (Ground)) **H1/H2**	CREW (Ground) informed by warning and contacts CREW (Air)	CREW (Air) Refutes need for assistance and struggles with workload (e.g. misdiagnoses problem or amount of work to be undertaken) following decompression event **H1/H2**	CREW (Ground) informed by warning and engages in active monitoring / takes over if necessary	CREW (Air) Requests assistance too late following decompression event when early stages of hypoxia are present (e.g. lack of experience / late to diagnose problem) **H1/H2**	CREW (Ground) informed by warning and initiates offer of assistance to CREW (Air)	n/a	n/a

Table 4 – STPA table output showing UCAs and Design constraints arising from CAs from Ground Station to Aircraft and ATC/ATM.

Control Action from GROUND STATION	To	Safety consideration	1. Action required but not provided	Design constraint	2. Unsafe action provided	Design constraint	3. Incorrect timing or order	Design constraint	4. Stopped too soon / Applied too long	Design constraint
GROUND monitors Aircraft (switch positions QRH Checks)	**AIRCRAFT**	Step missed (e.g. Oxygen / descent steps) so lack of oxygen or lack of descent. Risk of hypoxia from inadequate conditions for breathing	GROUND fails to monitor QRH Checks following decompression event so key steps to avoid hypoxia / incapacitation are missed (e.g. if attention is diverted to other routine flight monitoring) **H1/H2**	Electronic QRH checks with **initiation Alert** synced between AIRCRAFT and GROUND	GROUND Fails to monitor O2 QRH step so lack of certainty that CREW (Air) are protected from hypoxia following decompression event (e.g. if attention diverted to other routine flight monitoring) **H1**	Electronic QRH checks with **sequence** synced between AIRCRAFT and GROUND	CREW (Air) QRH checks undertaken too slowly following decompression event so early effects of hypoxia are felt (e.g. through lack of experience) **H1/H2**	Electronic QRH checks with **time** prompt synced between AIRCRAFT and GROUND	CREW (Air) do not complete QRH checks following decompression event so key steps are missed (e.g. through lack of experience of rapid decompression, or poor CRM) **H1/H2**	Electronic QRH checks with **progress** prompt synced between AIRCRAFT and GROUND
					GROUND Fails to monitor descent QRH step so lack of certainty that CREW (Air) are protected from hypoxia following decompression event (e.g. if attention diverted to other routine flight monitoring) **H2**	Electronic QRH checks with **sequence** synced between AIRCRAFT and GROUND	QRH checks performed by CREW (Air) in wrong order following decompression event so Oxygen masks are not prioritized risking early onset hypoxia (e.g. through lack of experience) **H1**	Electronic QRH checks with **sequence** synced between AIRCRAFT and GROUND	CREW (Air) leave long delays between QRH actions following decompression event so early effects of hypoxia are felt by CREW (Air) (e.g. through uncertaintly that the problem has been correctly diagnosed) **H1/H2**	Electronic QRH checks with **time** prompt synced between AIRCRAFT and GROUND
GROUND calls MAYDAY to ATC	**ATC**	Urgent Help not provided. ATC unaware of aircraft incident and diversion or unable to provide guidance relating to desent and diversion.	GROUND fails to call MAYDAY to ATC following decompression event so assistance is not provided and diversion is not offered (e.g. if rapid decompression has not been identified by ground crew or they lack experience in this type of event) **H2**	Ensure Adequate GROUND STATION training Automated Mayday call from GROUND when critical conditions in aircraft sensed.	GROUND communicates misleading / erroneous information regarding incident following decompression event to ATC, who subsequently provide incorrect assistance (e.g. if incident misdiagnosed or ground crew are inexperienced) **H2**	Ensure Adequate GROUND training Relevant data sent automatically to ATC	GROUND is late calling MAYDAY following decompression event so assistance arrives too late (e.g. if attention diverted to other routine flight monitoring) **H2**	Additional safety supervisor on GROUND if GROUND co-pilot tied up with take-off/ descent for other aircraft	GROUND stops MAYDAY call following decompression event before it is acknowledged so lack of certainty that assistance will be provided (e.g. if attending to other routine flight monitoring or lacking experience) **H2**	Automated continuous Mayday until acknowledged by ATC Additional Safety supervisor on GROUND to monitor non-normal flights across range of aircraft

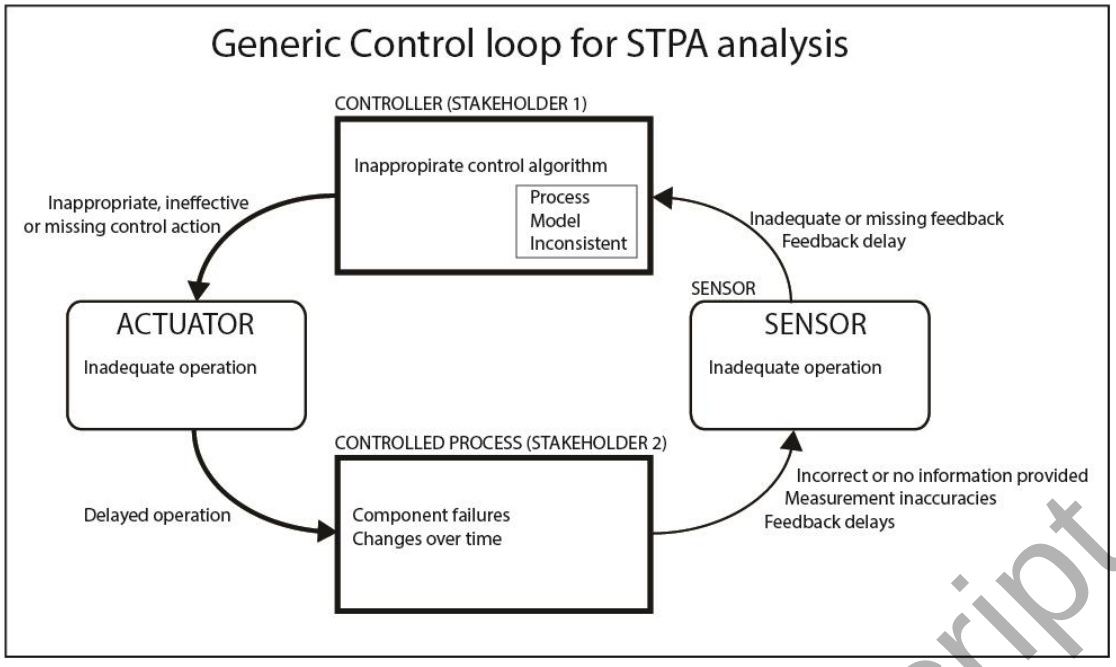

Figure 1 - Generic Control loop for STPA analysis

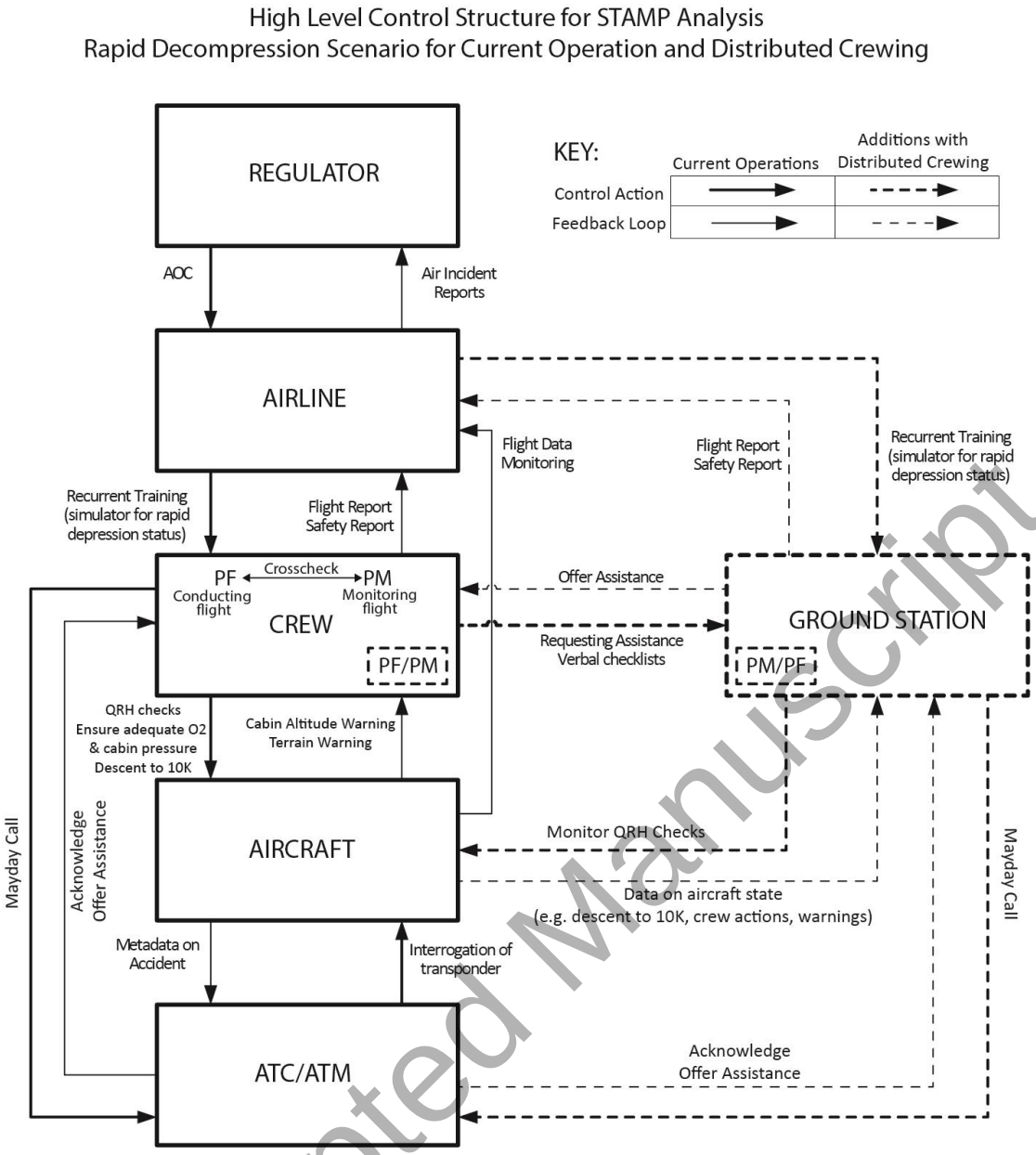

Figure 2 – High level control structures for STAMP analysis showing both current operations and (solid line) and the hypothesized additions for a distributed crewing configuration

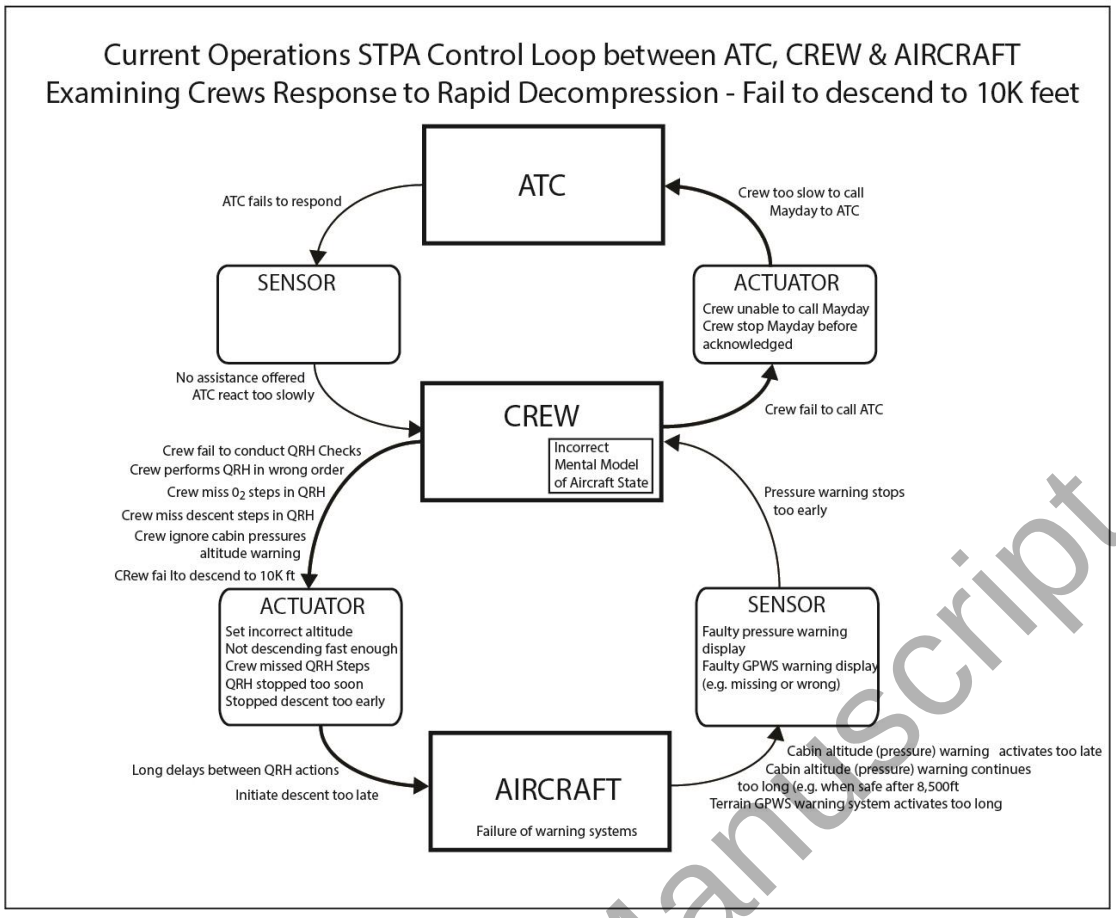

Figure 3 – Control loop comprising Crew, Aircraft and ATC/ATM for current operations

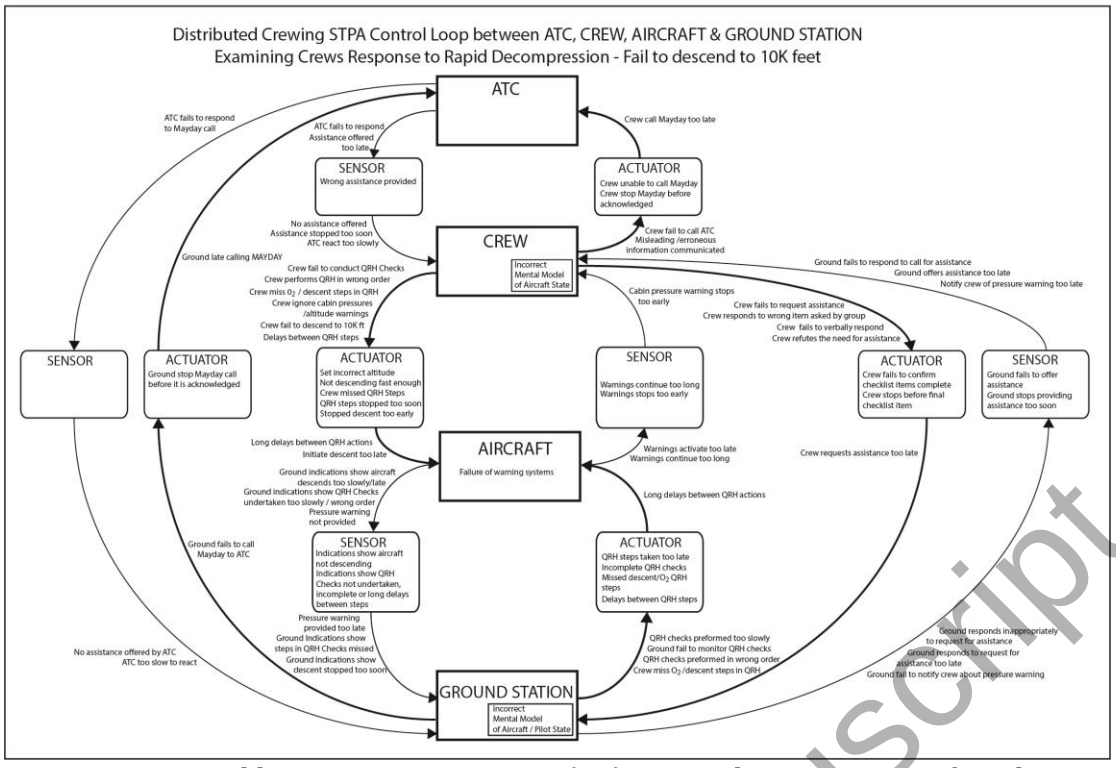

Figure 4 – Control loop comprising Crew (air), Ground Station, Aircraft and ATC/ATM for distributed crewing configuration.