Human-Intelligent Systems Integration (2019) 1:27–42
https://doi.org/10.1007/s42454-019-00001-y

RESEARCH ARTICLE

A future airliner's reduced-crew: modelling pilot incapacitation and homicide-suicide with systems theory

Daniela Schmid[1] · Neville A. Stanton[2]

Received: 6 September 2018 / Accepted: 11 March 2019 / Published online: 16 April 2019

Abstract
One main hurdle towards commercial airliners' Reduced-Crew Operations (RCO) is how to encounter pilot incapacitation. The aim of this modelling study is to evaluate the potential effects of a single-pilot's incapacitation on a future design approach to RCO. Most solutions propose a ground support of the pilot by a remote operator whom control should be handed over in case of an emergency. Both incapacitation and homicide-suicide have been discussed in the literature but neither of these events have been modelled nor evaluated empirically. We introduce a future operational design concept for RCO which includes a remote-copilot as ground support and automation tools monitoring pilot's health and entries into aircraft systems. The hazard analysis technique System-Theoretic Process Analysis (STPA) was used to model and analyse scenarios of incapacitation/homicide-suicide. A hierarchical control structure showed how RCO can be embedded into commercial aviation. The STPA of pilot incapacitation and two scenarios of pilot homicide-suicide showed how unsafe control actions leading to an incident or accident after incapacitation/homicide-suicide could be prevented. The possible detection and take-over of control by the ground support in the case of incapacitation raised the question for detailed procedures on how to react to its detection. Either an autoland by the remote-copilot or by an affiliated system is possible. An additional breakup of data-link may only be solved by an automatic landing system on-board.

Keywords System-Theoretic Accident Model and Processes (STAMP) · Single-pilot operations · Systems theory · Accident modelling · Aviation

1 Introduction

Commercial Reduced-Crew Operations (RCO) synonymously referred to as Single-Pilot Operations (SPO) have been debated as an alternative to Multi-Crew Operations (MCO) in research for approximately two decades (Deutsch and Pew 2005; Johnson et al. 2012). The two-crew flight deck represents the modern standard for commercial MCO in industry and practice. By way of contrast, SPO have only one pilot on the flight deck. At the moment, they are exclusively employed for different aircraft models in general and business aviation as for example in Embraer's (2015) Phenom 300. If we consider SPO for commercial operations, the term RCO is more comprehensive for SPO by including long-haul and ultra-long-haul flights with a relief pilot on-board. The relief pilot is only assigned to pilot duties in distinct portions of a flight determined by the operator to enable another crew member taking a rest (International Civil Aviation Organization [ICAO] 2012b).

From the 1950s until the 1980s, the flight crew was continuously de-crewed from five to two members on the flight deck (Boy 2016). For example, the Flight Engineer (FE) had ensured that all aircraft systems were working properly. The introduction of electronic flight management and automated monitoring of aircraft systems and engines had made his profession obsolete in the 1980s. Similarly, communication and navigation officers were replaced by developments in radio and wayfinding technologies. The next step would be to further reduce the crew to one pilot on-board. Some of the functions could be assumed by either on-board automation or

✉ Daniela Schmid
daniela.schmid@dlr.de

[1] German Aerospace Centre (DLR), Institute of Flight Guidance, Lilienthalplatz 7, 38108 Braunschweig, Germany

[2] Human Factors Engineering, Transportation Research Group, Boldrewood Innovation Campus, University of Southampton, Burgess Road, Southampton SO16 7QF, UK

ground-based systems (Harris 2007; Stanton et al. 2016). This next step in de-crewing towards a single-piloted commercial aircraft sounds promising when we consider the anticipated benefits. Commercial RCO/SPO could potentially save operating costs that offer an economic benefit to the operating airline in the long term. Three different calculation models supported the claim for this potential (Graham et al. 2014; Malik and Gollnick 2016; Norman 2007). The costs required developing a single-pilot aircraft, its operations and procedures, and the technical infrastructure have not been considered in any formal model yet. A retrofit of current aircraft models to RCO seems not to be economically viable because most of the cockpit avionics would require redesign and replacement (Driscoll et al. 2017b). Ground infrastructure is required to compensate for the loss of redundancy by the copilot in case of emergencies on-board. The deployment and operation of a ground override system linked to the aircraft systems would have to be developed and integrated into new aircraft designs. Hence, a re-conceptualisation of aircraft systems including the flight deck and the role of single-pilot are required before RCO can be taken into practice (Harris 2007).

Five main issues have been identified for RCO: automation, operational, pilot incapacitation, communication/social, and certification (Johnson et al. 2012). For example, a concept of RCO has to offer a safe solution for handling possible in-flight incapacitation of the single-pilot to guarantee flight safety (Lachter et al. 2017). Different concepts of RCO have already been introduced (Bilimoria et al. 2014), modelled on a conceptual level (Stanton et al. 2016) and investigated empirically in simulations (Lachter et al. 2017). They all establish different types of remote ground support to provide assistance during high-workload situations and emergencies. Nevertheless, the issue of pilot incapacitation per se has only been addressed in very few studies on RCO (Revell et al. 2018; Stanton et al. 2016; Stanton et al. 2019). Hence, the present paper's aim is to model pilot incapacitation and its potential effects. Pilot incapacitation can have detrimental effects on SPO which is why it has to be considered in connection with operational and automation issues for commercial RCO.

In-flight incapacitation is "any reduction in medical fitness to a degree or of a nature that is likely to jeopardise flight safety" (ICAO 2012a, p. I-3-1). In addition, it is defined operationally as "any physiological or psychological state or situation that adversely affects performance" (ICAO 2012a, p. I-3-1). For the purposes of this paper, incapacitation was further classified operationally into "obvious" and "subtle" subtypes, which refers to their appearance during flight operations. An obvious incapacitation is immediately apparent to the other pilot as for example unconsciousness of his colleague. A subtle incapacitation is more difficult to detect because although the pilot may look healthy, he is not. For example, in one incident, a pilot had complained about abdominal pain, intermittently ignored the radio communications and then the copilot's questions (Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile [BEA], 2011). When his speech had become incoherent, the copilot took over control, declared an emergency and landed the aircraft safely. In this example, the pilot had suffered from hypoglycaemia which was hard to detect in its early stages.

In general, such cases of in-flight incapacitation are rare. For example, the annual incapacitation rate for commercial pilots was 0.25% in the UK in 2004 (Evans and Radcliffe 2012). This calculation was based on incidents reported to the UK Civil Aviation Authority. A more precise and complete incident rate for a medical in-flight incapacitation in commercial aviation is difficult to estimate due to a lack of prospective international long-term studies (Hinkelbein et al. 2008). The routine periodic medical examination for commercial pilots for medical certificate class 1 is administered to assess physiological and psychological health. It aims to keep the risk for a medical incapacitation at low levels by only issuing healthy pilots with a certificate (Evans et al. 2016). This precondition will not change in RCO. In MCO, the "two communication" rule was introduced to detect especially subtle incapacitations before they affect flight operations (ICAO 2012a). It refers to each pilot being sensitive to such behaviour as when a crew member does not respond appropriately in verbal communications and deviates from standard operating procedures. Once detected, ICAO's (2012a, p. I-3-6) Standards and Recommended Practices (SARPs) recommend three steps on how to handle an in-flight incapacitation: (a) maintain control of the aircraft, (b) take care of the incapacitated crew member and (c) reorganise the cockpit and bring the aircraft to a safe landing. Step (b) was formalised as an abnormal and emergency procedure called "crew incapacitation" which is trained regularly in the simulator (Airbus 2011). They are applicable to most kinds of in-flight incapacitation whereas pilot homicide-suicide is an exception and needs further refinement.

Pilot homicide-suicide represents a special subtype of a subtle incapacitation resulting primarily from an adverse mental health state. The pilot as a perpetrator crashes the aircraft intentionally with the motive to commit a homicide-suicide. It is mostly lethal for passengers and crew (Kenedi et al. 2016). The causation is multifactorial comprising (but not limited to) mental health, occupational, family and legal issues. Hence, every case of pilot homicide-suicide must be separated from incapacitation and considered on a case-by-case basis. There are only 17 known cases of pilot homicide-suicide with large aircraft, with and without passengers, in the history of aviation (Aviation Safety Network 2015; Kenedi et al. 2016). The prevention and handling of a pilot homicide-suicide differ from those of usual incapacitation. A comprehensive mental health assessment is currently considered as part of the certification

process for the initial medical certificate class 1 in most European countries (European Aviation Safety Agency [EASA], 2016a). It should help to detect the likelihood of a homicidal-suicidal pilot. Furthermore, the EASA SIB 2016-09 of the minimum cockpit occupancy has introduced the requirement to have at least two authorised persons on the flight deck during flight, based on a safety and security risk assessment of the operator (EASA 2016b). Hereby, the rule aims to prevent a homicide-suicide by having another person present whose main task is to open the security door when the flight crew member returns to the cockpit. Environmental conditions and corresponding procedures need to be specified by the individual airline.

In commercial RCO, pilot incapacitation and homicide-suicide need to be handled differently to MCO. Safe operation of the aircraft in case of an incapacitated single-pilot is challenging due to the issue of initial detection of the incident as well as recovery from it (Bilimoria et al. 2014; Harris 2007). Reliable detection of an adverse health state of the single-pilot is required in the first instance. If the single-pilot on-board does not self-report a decrease in fitness, then advanced automation tools are required to detect it (Harris 2007). The development of a pilot health monitoring system needs to address the detection of conspicuous physiological health states based on behavioural and physiological signals. Among these are high-workload states or physical stress leading to a degraded capability and suspect physiological conditions (Johnson et al. 2012). They can be summarised as some behavioural indications for a cognitive degradation which require reliable measurement equipment. Only non-intrusive sensors would be suitable for commercial flight operations because they must not interfere with safe flight operations (Matessa et al. 2017). Hence, it is desired that these (preferably) remote sensors are as comfortable as possible. At the moment, several approaches to monitor the health of pilots in aviation have been proposed, but they are currently still under development (Çakır et al. 2016; Maiolo et al. 2017; Oliveira et al. 2012). Further processing of health data has not been integrated into systems explicitly recommended for commercial RCO. Hence, all approaches to measure pilot health for RCO are of low technical maturity at present. By way of contrast, technical solutions for monitoring aircraft systems security and landing an aircraft autonomously do currently exist for MCO and can be assumed mature enough for commercial RCO. They are introduced subsequently.

Aircraft systems monitoring is required to detect attempted pilot homicide-suicide, which represents a unique type of unauthorised operation of aircraft systems. Table 1 exemplifies systems which have already been developed for MCO to deal with such activities. They detect the entries into the aircraft systems, evaluate their hazardousness for flight safety and propose solutions, to either warn the crew or land the aircraft. Some methods can inhibit all system entries on airside to protect the aircraft and ensure a safe landing at an adjacent airport (Gaultier and Security of Aircraft in the Future European Environment [SAFEE] Consortium 2008; Schmitt et al. 2010). These advanced new automation systems may be equally applicable to handle a detected attempt for pilot homicide-suicide in RCO. In all reduced-crew Concept of Operations (ConOps), the recovery from a loss of control on airside is solved by transferring control to a ground operator, who lands the aircraft safely at an adjacent airport (Bilimoria et al. 2014; Lachter et al. 2017; Matessa et al. 2017; Stanton et al. 2016). This remote-pilot is supposed to either land the aircraft or oversee on-board automation landing the aircraft with Air Traffic Control (ATC)–supported (exceptional) emergency handling (Lachter et al. 2017). For example, Table 1 includes a Flight Reconfiguration Function (FRF) which autonomously re-plans the flight to return them safely to the most suitable airfield and lands it safely (Gaultier and SAFEE Consortium 2008; Laviv and Speijker 2007). Automation tools, like the FRF, have the potential to be combined with RCO (Benitez et al. 2018).

The present modelling paper investigates how pilot incapacitation and pilot homicide-suicide can be detected and prevented in a future design concept for commercial RCO. The recovery of the single-piloted aircraft represents the main issue which has to be solved (Harris 2007; Stanton et al. 2016). It has not been evaluated for any of the design recommendations of RCO in commercial aviation yet, neither through modelling nor in empirical studies. Thus, we modelled the hazard of pilot incapacitation and homicide-suicide in a possible future concept of RCO. The hazard analysis considered the proposals of new advanced automation systems together with an operational concept of a remote ground-based support. Here, we used the System-Theoretic Accident Model and Processes (STAMP) and System-Theoretic Process Analysis (STPA) to include human behaviour in a systems theory hazard analysis of the conceivable complex sociotechnical system of commercial RCO (Leveson 2004a; Leveson 2011; Leveson 2017). Furthermore, STAMP and STPA have been rarely applied in a predictive context to evaluate future designs of complex sociotechnical systems (Fleming et al. 2013; Grant et al. 2018; Leveson 2015). There are notable exceptions, such as the STAMP analysis of a rapid decompression event for SPO (Revell et al. 2018). This major advantage of STPA enables evaluating a design concept such as a RCO in early stages of the development process. Following the system-theoretical rationale, we provide a new way of looking at the widely debated issue of pilot incapacitation in RCO in a modelling study.

2 Method

STAMP and STPA have been applied mostly retrospectively to a series of incidents and accidents in aviation and aerospace

Table 1 Additional automation tools which fit into a thinkable design RCO

Upper level function	System	Function(s)
Pilot health monitoring system		Monitors pilot health via physiological sensors
Aircraft systems monitoring	OTDS (On-board Threat Detection System)[a]	Detect unauthorised access, dangerous materials or suspicious human activity (from NAV, A/C systems, FCS, surveillance). Forwards information to the TARMS.
	TARMS (Threat Assessment and Response Management System)[a]	Alerts crew, evaluates threat situation and recommends possible responses to deal with; Can conclude that cockpit crew is no longer in control of aircraft.
	EAS (Emergency Avoidance System)[a]	Disables all unauthorised inputs (flight controls and aircraft systems) and protects aircraft systems (electrics, hydraulics, engine power);
	FRF (flight reconfiguration function)[a]	Allows an automated landing at a secure airport in case of the single-pilot aircraft having been out of control.

The pilot health monitoring system remains unspecified

[a] SAFEE (Gaultier and SAFEE Consortium 2008; Laviv and Speijker 2007)

as well as in transport and military, whereas the predictive use of both methods is less widespread in the peer-reviewed literature (e.g. Allison et al. 2017; Fleming and Leveson 2014; Ishimatsu et al. 2014; Leveson 2004b; Plioutsias et al. 2017; Revell et al. 2018; Rong and Tian 2015). STAMP as a causal model of its corresponding hazard analysis STPA uses the basic tenet of systems theory to explain accidents and their causality holistically (Leveson 2017). Systems theory proposes safety as a control problem rather than a component reliability problem (Rasmussen 1997). In STAMP, a sociotechnical system is defined as several interrelated components which are related to each other by both feedforward and feedback loops of information and control. Safety is achieved by keeping the components' behaviour and state in an acceptable range of system operations. In other words, adequate safety constraints have to be enforced. Thus, the basic concepts of STAMP are hierarchical safety control structures, safety constraints and process models.

In general, systems theory assumes a hierarchical risk management in which a complex system is embedded (Rasmussen 1997). This covers legislators, managers, work planners and operators across different systemic levels. In STAMP, two basic control structures represent the development and operation of a system. Whilst both structures may change over time, safety must not be adversely affected. Safety constraints enforce control at, and across, each level of both structures to create the emergence of system safety (Leveson 2004a). Safety constraints can be standards and redundancy in design, fail-safe design, standardised processes and operating procedures, regulations and laws and social and organisational culture. The safety constraints define the relationships between the system components' variables to keep the system in a non-hazardous (i.e. safe) state. The system components include human and technical system components. For example, commercial flight operations comprise pilots and aircraft systems among others which are all regulated and checked (Harris and Stanton 2010).

An accident occurs if the safety constraints are inadequately enforced or if there is a lack of adequate safety constraints. Human controllers or automated controllers can enforce safety constraints (Leveson 2017). A controller can control a process and influence a system's state according to the control action via actuators. A sensor provides feedback about the process' state. Leveson (2004a) assumed the controller to have goals, the ability to ascertain and affect the system's state, and a mental or formal process model which depends on the controller's nature. These characteristics of a controller are essential for the logic of a process model. This model describes a controlled process as the interaction of controllers with the process by enforcing a control action and receiving feedback about the process' state (Leveson 2017). Each component of the hierarchical safety control structure enforces control actions via which it controls a process. The control actions can be either safe or unsafe at every level. The unsafe control actions in STAMP are analysed by the corresponding hazard analysis technique STPA.

STPA can describe an accident before it occurs in a formal model, requiring only a conceptual design of system operations and the scenario of the safety critical event (Leveson 2011). The predictive use of this analysis in the early conceptual design stages of a system provides information to guide the design process. Potential sources for accidents can be eliminated or controlled. In doing so, STPA contributes to a most cost-effective way of designing safer systems. Therefore, we applied STPA to the hazard of incapacitation events in imaginable future RCO. Furthermore, STPA provides some additional advantages compared to traditional reliability analysis methods. These traditional methods, for example the fault tree analysis or the HAZOP (Hazard and Operability) techniques, typically model only a single chain of events (Aven

2015; Dunjóa et al. 2010; Geymar and Ebecken 1995; Stanton and Harvey 2017). By contrast, STPA focuses on the whole complex sociotechnical system at all levels. The operating processes and corresponding control actions of all involved agents are modelled for a causal scenario of an incident or accident. For example, we analysed the exemplary cases of pilot incapacitation and homicide-suicide (see Table 2) under RCO conditions according to STPA. Firstly, four types of Unsafe Control Actions (UCAs) were identified for the given system and scenario under analysis (Leveson 2011; Leveson 2017):

1. Control action is not provided;
2. Unsafe control action is executed;
3. Control action is applied too early or too late;
4. Control action is applied for too short or too long.

Secondly, each control loop was examined to reason how the UCAs could occur. The hierarchical safety control structure was considered to identify how control might degrade and how system resilience could be improved. This detection of the weaknesses in safety constraints helps to anticipate incidents and accidents in existent or planned designs of complex sociotechnical systems.

We used official reports, regulations, guidelines, aviation training textbooks and a Flight Crew Operating Manual to construct the hierarchical control structure of RCO (Airbus

Table 2 The incidents' and accidents' causal scenarios transferred to future RCO in STAMP and STPA

Type		Flight	Year	Short summary
In-flight incapacitation	Subtle	Air Canada Rouge (scheduled flight)	2008	During cruise, the FO left the flight deck for several times, did not follow the standard operating procedures, took a controlled rest and finally became belligerent and uncooperative. The Captain called the cabin crew to secure the incapacitated pilot away from the controls. He diverted the flight to Shannon due to better weather conditions and landed the aircraft safely.
	Obvious	China Airlines CI681	2001	Thirty minutes after take-off, the Captain did not react to flight operations anymore. The FO carried out the crew incapacitation procedure, turned back to Taiwan Taoyuan International Airport and landed the aircraft safely. The Captain had died from an acute cardiac artery occlusion.
		Ryanair (scheduled flight)	2011	Thirty minutes after take-off, the FO felt ill and the captain took over control. Afterwards, he did not react anymore and eventually fainted. The Captain called the cabin crew to carry out the crew incapacitation procedure, declared a medical emergency and diverted to the adjacent Girona Airport safely.
		Etihad Airways ETD308	2012	During the approach to Abu Dhabi International Airport, the Captain's (PF) speech became incoherent and tone of voice unusual during conversation. He slumped down in his seat. Thus, the FO took over control after having tried to wake up the Captain in vain. He called the cabin crew to take care of the Captain, declared an emergency to approach control and landed the aircraft safely. The Captain had sustained an antiphospholipid syndrome leading to an embolic and loss of consciousness.
Pilot homicide-suicide		Japan Airlines JL350	1984	During final approach to Tokyo Haneda Airport, the Captain jumped out of his seat and babbled incomprehensibly when reaching the DA. The FO and flight engineer pulled him back into his seat. Then, the Captain cancelled the autopilot, retarded thrust to idle/reverse and pushed forward yoke. Although the FO tried to pull back the controls, the McDonnell Douglas DC-8-61 crashed into Tokyo Bay before reaching the runway. The Captain had a premedical history of a delusional schizophrenia.
		Germanwings U9525	2015	During descend the Captain of Germanwings flight 4U9525 left the flight deck. After FO locking the door, the FO selected open descent mode, an altitude of 100 ft, and a speed of 350 kt at the autopilot. He did not answer to a ring of the buzzer of the door, several knocks, several calls from ATC, a radio call from another airliner's crew and violent blows against the door. Finally, the airplane crashed into the French Alps. The copilot had suffered from a mental disorder with psychotic symptoms.

DA, Decision Altitude; *FO*, First Officer; *PF*, Pilot Flying; *PM*, Pilot Monitoring. For full outline of the incident/accident, refer to the given referenced official report (Aircraft Investigation Unit Ireland [AAIU] 2008; Aircraft Accident Investigation Committee 1984; Aviation Safety Council China 2001; Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile [BEA] 2016; Comisión de Investigación de Accidentes e Incidentes de Aviación Civil [CIAIAC] 2011; UAE General Civil Aviation Authority [UAE GCAA] 2012)

2011; Oxford Aviation Academy 2008). Table 2 lists all incidents and accidents reports of which we transferred to the time course of happenings to RCO. Four cases of pilot incapacitation were merged to create a general process model. Pilot homicide-suicide had to be considered on its own because each case shows a unique multifactorial causation (Kenedi et al. 2016; Schmid et al. 2018). For example, the cockpit crew members of Japan Airlines 350 (JL350) had actively intervened in suicidal actions of the captain during approach. They had tried to prevent the plane from crashing (Aircraft Accident Investigation Committee 1984). Most of the passengers and all of the crew survived. By contrast, Germanwings flight 4U9525 ended as fatal crash without survivors (BEA 2016). We merged all information with an anticipated design concept for RCO how it might be introduced beside MCO in the future. All outputs from the analysis were verified through consultation with a commercial pilot (age 28 years, male; Commercial Pilot Licence [CPL], frozen Air Transport Pilot Licence [ATPL]; 1400 of 1800 flying hours at Boeing B737-800) from one of the larger European airlines. This Subject Matter Expert (SME) was introduced to the methodology, the preliminary design concept and findings during a video conference. His suggestions were incorporated into the results.

3 Results

3.1 A design approach to Reduced-Crew Operations

A possible future design concept of RCO required for STPA includes the following agents: the single-pilot, an aircraft including its automation, the remote-copilot at a Ground Station (GS) connected via data-link and ATC. In addition, we specified conceivable characteristics of ground support and advanced automation systems which deal with monitoring and detection of incapacitation(s). These agents are sufficient to model any in-flight incapacitation. Their composition is similar to that proposed in other design concepts of RCO (Lachter et al. 2017; Schmid and Korn 2017; Stanton et al. 2016). Other possible agents are omitted in this paper. During departure and approach, the remote-copilot supports the single-pilot in-flight planning and navigation as Pilot Monitoring (PM). These flight phases are associated with a high workload and therefore support would be mandatory (European Commission 2015; Federal Aviation Administration [FAA] 2001). It is assumed that these periods of the high workload will remain in RCO because it is anticipated that the airport-related preconditions for departure and arrival will remain largely unchanged. Hence, the remote-copilot supports each single-pilot aircraft successively, of which he can serve 4–6 aircraft during departure/arrival (Koltz et al. 2015). During the cruise, the single-pilot is supported remotely as needs arise (Schmid and Korn 2017). The pilot on the aircraft can call for assistance or take-over of control via the remote-copilot call lever in any phase of flight. Both functions for immediate recovery from any safety critical event are available to the single-pilot throughout all flight phases. Typical applications might be high-workload situations, technical failures and health issues. Normal events, like going to the lavatory, taking a nap and eating, would require only a temporary take-over of control.

We assumed three functions of additional automation systems that would be required to recover from any incapacitation. Firstly, a pilot health monitoring system should be capable of evaluating the single-pilot's physiological state. Secondly, aircraft systems monitoring should assess entries into aircraft systems in the search for critical and unauthorised deviations from the flight plan and safe flight operations. Third, and finally, an affiliated system can disable all unauthorised inputs at airside and transfer control to the GS and the remote-copilot. We modelled systems similar to those proposed in the European Union (EU) projects (Advanced Cockpit for Reduction of Stress and Workload [ACROSS] 2016; Gaultier and SAFEE Consortium 2008). Table 1 summarises some of the details of these systems. We adapted their functions by adding dual-graded alert management to integrate them into the concept of RCO. Subsequent events release dual-graded alerts:

1. Critical physiological state/suspicious entries into aircraft systems;
2. In-flight incapacitation based on physiological variables/cockpit crew is no longer in control of the aircraft.

It is anticipated that the single-pilot aircraft would automatically connect to the GS via data-link. The first type of alert would involve the remote-copilot to support as PM. By contrast, the second type would completely handover control to the GS. The single-pilot can also manually initiate support or handover by the GS. Finally, the remote-copilot can also switch control from the air if he deems necessary in emergencies. Otherwise, the single-pilot has authority and control of the aircraft unless a loss of control occurs. It is also anticipated that a backup GS with the same systems monitors several GSs in order to provide redundancy in case of fire or terror attack.

Figure 1 shows the hierarchical organisation of a proposed commercial RCO in a safety control structure. RCO could be embedded next to MCO by introducing the required technologies and procedures. The flight crew consisting of a single-pilot and (optional) remote-copilot remains on the crew level. The remote-copilot at the GS is linked via data-link to the single-pilot and aircraft systems. A remote-copilot centre serves as a facility at airports to organise ground support and corresponding technical infrastructure on the ground. It provides space for airlines to operate a reduced-crew fleet. The safety constraints on all other levels will be extended to

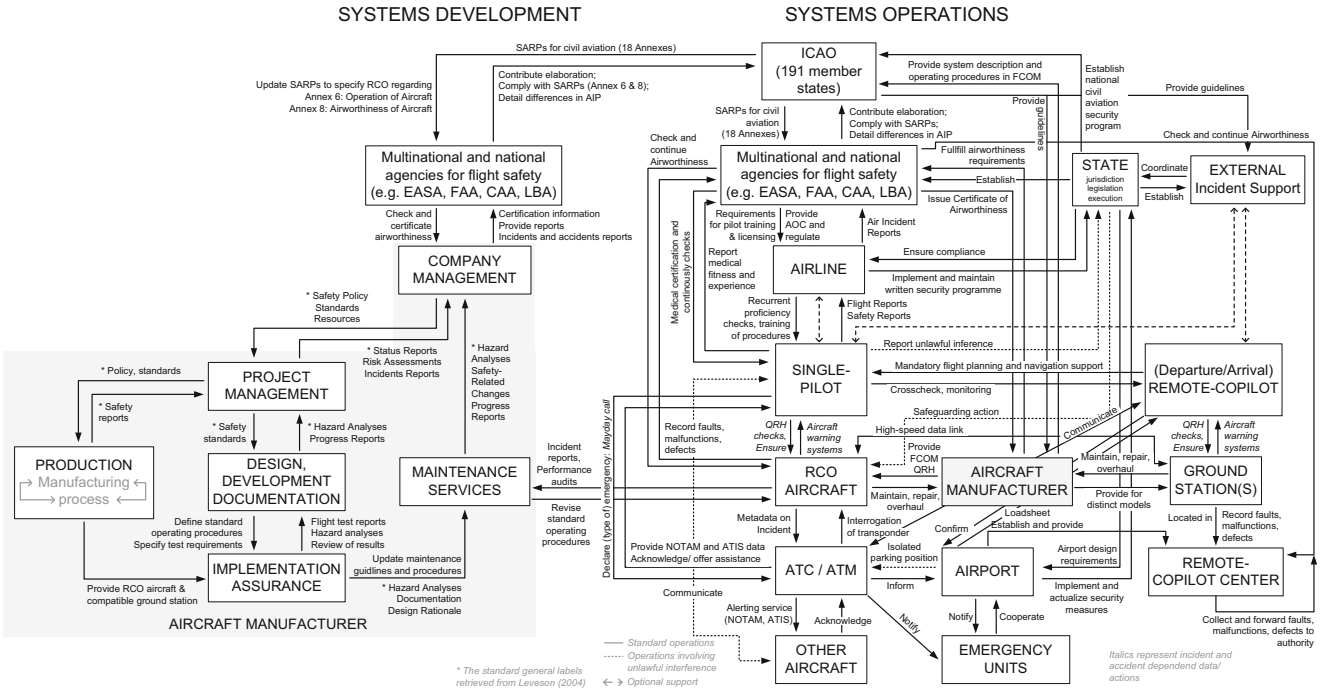

Fig. 1 The hierarchical safety control structure of system development and system operations of RCO in commercial aviation

include commercial RCO in the future. For example, both the single-pilot and remote-copilot could be commercial pilots who have undergone additional training to receive a licence as RCO pilot. They would need to perform their jobs in a shift of several months to keep their skills up to date as well as annual refresher training and testing. The entire design approach assumes reliable and secure data-links with backups as a necessary prerequisite (Schmid and Korn 2018).

Currently, the hierarchical safety control structure of MCO does not include commercial RCO. Only one legislative step has been initialized towards considering commercial RCO yet. The US Congress had recently launched the FAA Reauthorization Act H.R.4 incorporating a research and development programme for single-piloted cargo aircraft assisted by remote piloting (FAA Reauthorization Act of 2018 (H.R.4) 2018). Stanton et al. (2016) predicted that cargo operations would most likely be the first commercial flights for the RCO concept. They have gone on to consider the implications for distributed crewing (Stanton et al. 2019). As reaction, the pilots' community has however opposed this development. They fear a loss of safety in regulations and airline culture driven by premature technology for RCO which could affect systems (cyber)security (Cargo Airlines Respond to FAA Reauthorization Section 744 Language 2018). Hence, they implored Congress to reject the relevant section 744. Nevertheless, experts have fostered the planned programme to investigate the safety issues of RCO. Although the bill has passed the Senate, the research programme was taken out in the final version (FAA Reauthorization Act of 2018 (H.R.302) 2018). Before the current hierarchical organisation of commercial aviation can progress towards RCO in the end, research issues, such as pilot incapacitation, have to be addressed.

3.2 Pilot incapacitation

We assessed the four exemplary cases of pilot incapacitation including the obvious and subtle subtype against the concept of RCO previously introduced in Table 2. In doing so, we identified the following common control actions:

1. Detect adverse health condition of single-pilot;
2. Remote-copilot to take control;
3. Reorganise the cockpit and land aircraft safely;

   (a) Call cabin crew to conduct crew incapacitation procedure;
   (b) Declare an emergency ("Mayday") and inform on crew incapacitation; and
   (c) Land aircraft safely.

The control actions for the remote-copilot at the GS remain similar to those in MCO (ICAO 2012a). Figure 2 shows the corresponding course of interactions between an incapacitated single-pilot, a remote-copilot, aircraft and optional support. In general, the single-pilot can proactively ask for support and/or handover control if they feel unwell. Furthermore, they can voluntarily request medical incident support and advice on health issues. The two-communication rule would be maintained. If the single-pilot does not self-report an adverse

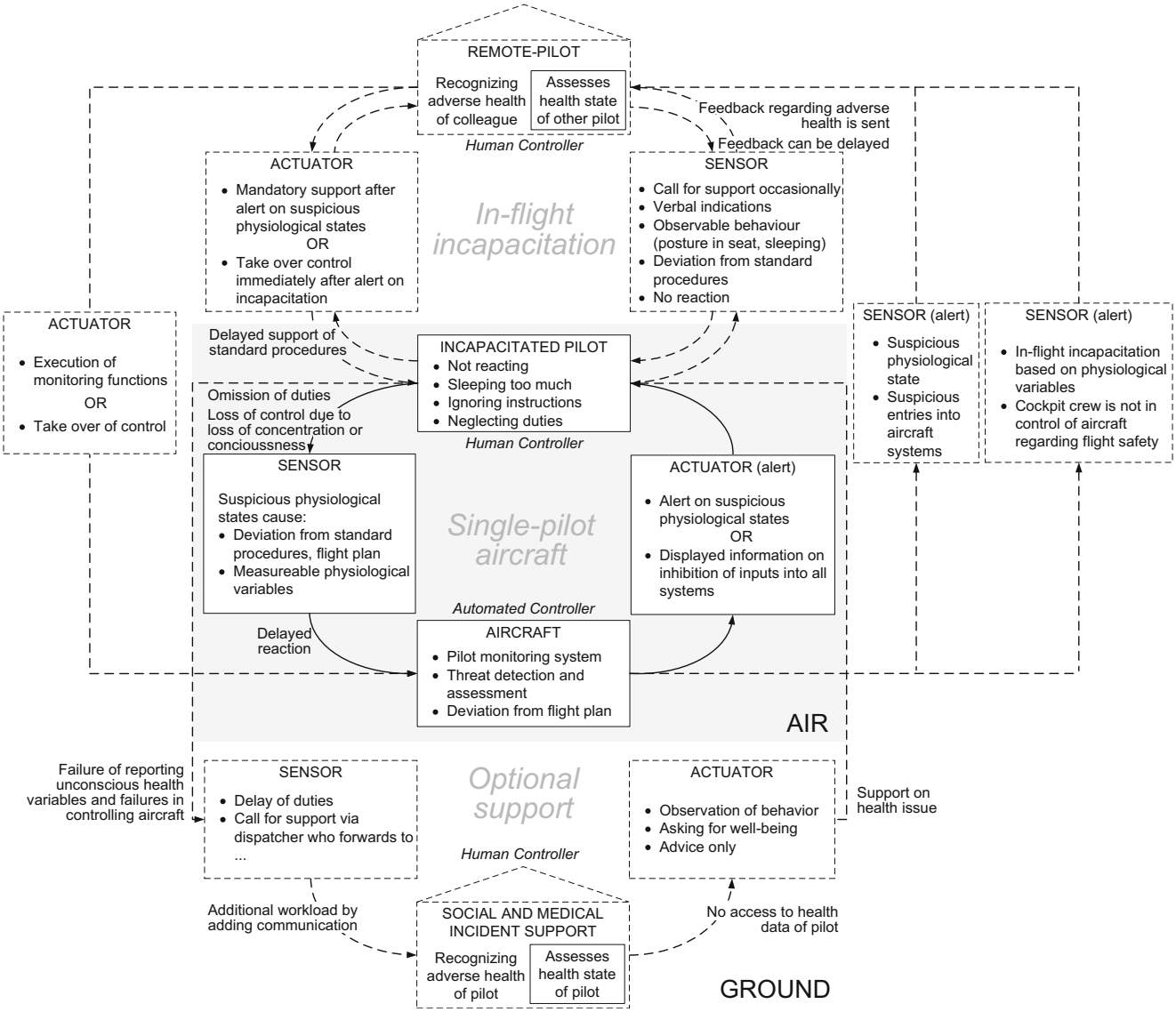

Fig. 2 UCAs and control loops for pilot incapacitation in general in RCO

physiological state, the pilot health monitoring system detects and evaluates the hazard. The system's dual-graded alert management handles a decrease in physiological health of the single-pilot by involving ground support. The remote-copilot is connected to either support the single-pilot in situations of a degraded cognitive and/or physical capability or to take over control completely if control is lost. The recovery of the single-pilot aircraft from both critical events is initiated by automation. In addition, subtle incapacitation eliciting procedural deviations and abnormalities could be detected by the aircraft systems monitoring function. This monitoring system either indicates suspicious operations or a complete loss of control regarding flight safety. The two types of reactions involving the remote-copilot remain the same: support or take-over of control depending on criticality for flight safety. Hence, all manifestations of an incapacitation were attempted to be covered by both monitoring systems in this design approach. Advanced automation tools would complement the control actions in RCO and should consequently enable the recovery from a single-pilot incapacitation. After a handover of control to the ground due to incapacitation, the remote-copilot lands the aircraft at the nearest viable alternate airport.

3.3 Pilot homicide-suicide

Pilot homicide-suicide is different to cognitive and physical incapacitation because it represents a deliberate and intentional action to crash an aircraft. Both JL350 and 4U9525 represent homicide-suicides with an airline pilot as the perpetrator but they differ in terms of their causation and outcome (as shown in Table 2). Taken together with the formal emergency procedures for crew incapacitation and guidelines on incapacitation (Airbus 2011; ICAO 2012a), the following common

control actions could be identified in a transfer of both crash scenarios to RCO:

1. Detect adverse health condition of single-pilot;
2. Remote-copilot to take control;
3. Detect homicidal-suicidal intent; and
4. Bring aircraft to a safe landing by control from GS;

   (a) Disable all unauthorised inputs and protect aircraft systems;
   (b) Declare emergency ("Mayday") and inform on homicidal-suicidal intent;
   (c) Inform cabin crew; and
   (d) Land aircraft safely.

Assuming a single-pilot would behave like the incapacitated captain of JL350 in RCO, the course of action and corresponding UCAs are presented in Table 3 and feedback loops in Fig. 3. Advanced automation could have alerted the GS in two cases depending on its operating rules. Firstly, the hazardous holding on the outbound flight might have caused an alert on suspicious entries into aircraft systems. This would have established assistance by a remote-copilot who may (or may not) have reported it depending on whether or not they suspected the hazardous state of the single-pilot. Such alerts of suspicious entries might be collected, but only after a distinct frequency of abnormal events, compulsory preventive measures could be undertaken. For example, an appointment for an additional specific aeromedical checkup can be arranged in case of abnormalities. Secondly, the pilot health monitoring system would have immediately detected the UCA of the single-pilot jumping up from the seat during approach and concluded a loss of control in connection with other systems, e.g. the On-board Threat Detection System (OTDS). Thus, the Emergency Avoidance System (EAS) would have disabled all inputs from airside to protect its systems. Another system would have switched control to the ground to the GS for the rest of the flight. Hence, the captain's actions to crash the aircraft would have had no effect on flight operations.

The possible control actions against hazardous events of GWI18G are similar to JL350 in RCO (Fig. 4; Table 4). Firstly, the short-time selection of 100 ft on the outbound flight would have caused an automatic alert of suspicious human activity by aircraft systems monitoring. The assigned remote-copilot could have assisted until the situation is reported under control. Depending on the hazard classification of this event, it is either collected in a database (as mentioned previously) or leads to a compulsory appointment with a pilot support programme member. However, a break from duty is unlikely. Secondly, OTDS and Threat Assessment and Response Management System (TARMS) would have immediately detected the hazardous autopilot selections of 100 ft,

Table 3 UCAs and safety constraints generated for control loop of "remote-copilot at GS", "suicidal single-pilot" for JAL 350 transferred to in RCO

Control action/feedback	1. Control action is not provided	Safety constraints 1	2. Unsafe control action is executed	Safety constraints 2
(1) Detect adverse health condition of single-pilot	(1) No report on hazardous operation to management	*Missing information regarding hazardous holding: not clear if detectable by proposed systems*		
(2) Remote-copilot to take control			(2) Captain ignoring call out of DA and radio altimeter warning; (4) Captain jumping up at DA and babbling incomprehensibly	(3) Recognising call out of DA and radio altimeter warning; (5) Alert on suspicious human activity
(3) Detect homicidal-suicidal intent	(9) Captain tries to cancel autopilot, push forward yoke and retards thrust in vain	(8) Remote-copilot took over control; Aircraft systems monitoring	(5) Alert on suspicious human activity (*already in place*)	(6) TARMS: conclusion that nobody is in control of aircraft; (7) Displayed information on inhibition of inputs into all systems; Warning of loss of control by single-pilot
(4) Bring aircraft to a safe landing by control from GS				
(4a) Disable all unauthorised inputs and protect aircraft systems			(7) EAS disables all unauthorised inputs and protects aircraft systems	(8) Remote-copilot takes over control; Improved aeromedical decision-making

The numbers inside the table refer to the time course of UCAs in the process model of Fig. 3. JAL 350 modelled in RCO. Control actions (4b)–(4c) were omitted because we assume them to be conducted safely and successfully

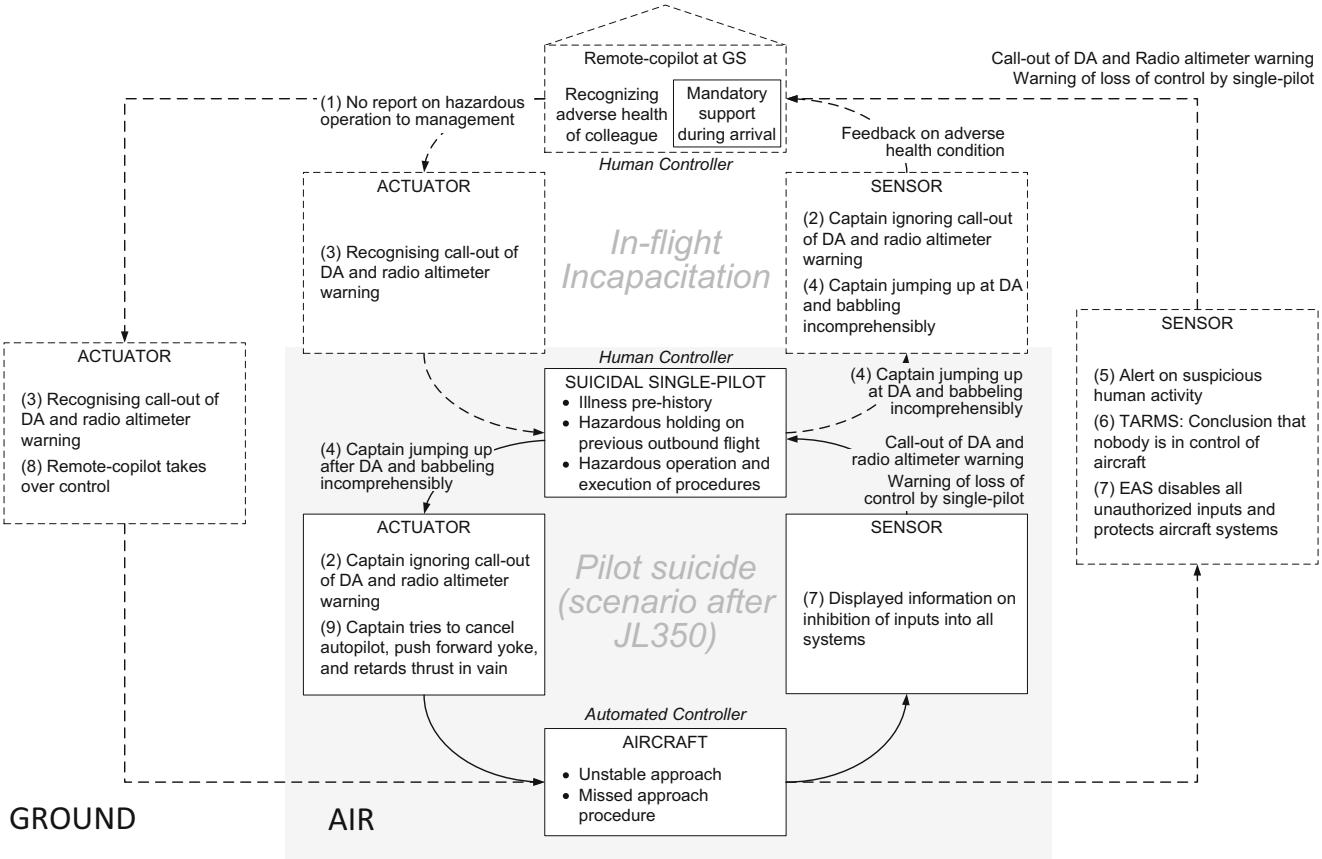

Fig. 3 UCAs and control loops for a pilot homicide-suicide in RCO based on the real-world model of JL350 transferred to RCO

the open descent as vertical mode, thrust mode idle and a speed of 308 kt as loss of control. Thus, EAS would have disabled all unauthorised inputs to protect aircraft systems on airside. Subsequently, command and control would have been transferred to the remote-copilot at the GS.

In summary, both pilot homicide-suicides can be anticipated as hazardous for safe flight operations. Hence, they are conceptually preventable in the proposed design approach for RCO. Subsequent to a detection of pilot incapacitation and/or an attempt for homicide-suicide, several actions are anticipated. The remote-copilot could land the aircraft safely by using an autoland function. He could also monitor the activation of the FRF and EAS. Both would control and land the aircraft automatically at an airport. Although TARMS and EAS are proposed for normal flight crew on-board (Gaultier and SAFEE Consortium 2008), they remain a solution to react to hazardous flight operations in RCO detect by an aircraft systems monitoring. Of course, the ground infrastructure would have to be added into the systems. Hence, TARMS and EAS can enable recovery from hazardous reduced-crew flight operations in off-nominal situations or emergencies. The present paper has focused on how a single-pilot aircraft can be protected from the emergencies of in-flight incapacitation and exemplary cases of homicide-suicide.

4 Discussion

A predictive use of STAMP and STPA to a design concept of RCO including remote support has shown that incapacitation and homicide-suicide can be detected and prevented in the present modelling approach. This concept required the application of a pilot health monitoring system and a detection system for suspicious entries into aircraft systems (Table 1; Benitez et al. 2018; Matessa et al. 2017). Both systems were considered in the present design approach based on research's solutions for different applications in aviation. New systems have already been proposed in EU projects and integrated into the approach (Laviv and Speijker 2007). Furthermore, affiliated systems are needed to protect aircraft systems by disabling all inputs on airside and land the aircraft safely at an adjacent airport. Here, the remote-copilot could land the aircraft by autoland or an alternate control system (e.g. FRF) takes over control to land the aircraft automatically.

Both system solutions proposed for detection and subsequent recovery from incapacitation or severe security intrusions (except hacking) into aircraft systems provide the opportunity for a comparable resilience of RCO to contemporary MCO (Stanton et al. 2016). The new design approach manages off-nominal situations and emergencies comparable to

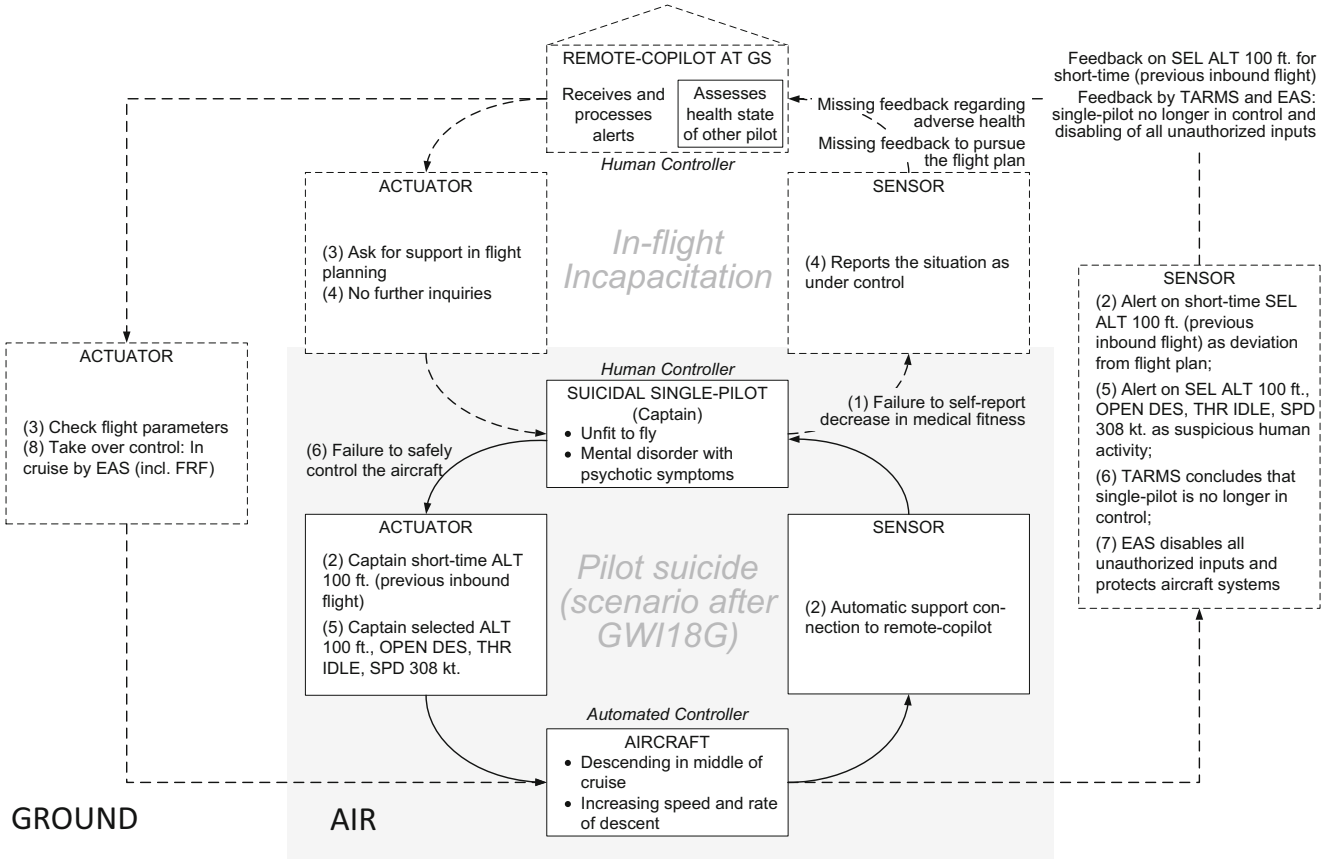

Fig. 4 UCAs and control loops for a pilot homicide-suicide in RCO based on the real-world model of GWI 18G transferred to RCO

the National Aeronautics and Space Administration's (NASA's) ConOps (Johnson et al. 2012; Lachter et al. 2017). In the latter one, dedicated support would be assigned to the single-pilot aircraft in high-workload and urgent situations among which are adverse physiological states, suspicious entries into aircraft systems, incapacitation and loss of control (Brandt et al. 2015; Dao et al. 2015; Lachter et al. 2014; Ligda et al. 2015). It was suggested combining an autoland procedure with new automation technology to enable a safe automated landing. They have not made any further specific design recommendations yet. The decision for procedures after the detection of incapacitation or loss of control depends on the interactions between the reliability of the technical systems and reliability of the data-link. Here, the two biggest hazards in RCO could coincide in time: the presence of both pilot incapacitation and a data-link failure (Driscoll et al. 2017a). An autoland technology on-board was proposed for data-link loss or disconnection (Lachter et al. 2017). The autoland system on-board could be applied in the case of in-flight incapacitation as well. If the data-link is sufficient reliable (Schmid and Korn 2018), the remote-copilot could also conduct the autoland from the ground in combination with automation tools reviewed above (Table 1). This represents an additional option depending on the data-link's bandwidth, reliability and security.

The specific application of such a pilot health and aircraft system monitoring system to RCO has not been modelled nor empirically evaluated. Nonetheless, similar applications were already investigated for use in MCO. The STAMP models presented provide first insights into how these new types of automation systems could be integrated into a concept of RCO. In doing so, we employed dual-graded alert management with affiliated recovery systems for both specific types of monitoring systems to adapt it to the two types of remote support by PM or PF. Any alert management would have to be fitted to the specific health and systems monitoring technology. Nonetheless, empirical data regarding the precise in-flight application of both types of monitoring technology are not available (Maiolo et al. 2017) and only validated regarding their technical feasibility in assessment (Oliveira et al. 2012) rarely during simulated flight (e.g. Çakır et al. 2016; Gaultier and SAFEE Consortium 2008). Thus, we discuss the risks involved with the use of both kinds of system support mechanisms on a conceptual level.

At first, most approaches to pilot health monitoring include physiological measures for cognitive capacity or workload but they do not suggest a specific response for crew members of commercial aircraft. For example, Maiolo et al. (2017) only demonstrated the technical operation of a wireless wristband to monitor cardiac activity and gesture recognition off-flight.

Table 4 UCAs and safety constraints generated for control loop of "remote-copilot at GS", "suicidal single-pilot" for Germanwings flight transferred to in RCO

Control action/ feedback	1. Control action is not provided	Safety constraints 1	2. Unsafe control action is executed	Safety constraints 2
(1) Detect adverse health condition of crewmember	(1) Failure to self-report decrease in medical fitness of single-pilot; (4) Reports the situation as under control	Self-report decrease in medical fitness; (3) Ask for support in-flight planning; (3) Check flight parameters; (4) No further inquiries	(2) Captain short-time SEL ALT 100 ft (previous inbound flight); (4) No further inquiries; (5) Captain selected ALT 100 ft OPEN DES, THR IDLE, SPD 308 kt.	(2) Alert on short-time SEL ALT 100 ft (previous inbound flight) as deviation from flight plan; (3) Check flight parameters; (3) Ask for support in-flight planning; (5) Alert on SEL ALT 100 ft, OPEN DES, THR IDLE, SPD 308 kt as suspicious human activity
(2) Remote-copilot to take control	Failure to safely control the aircraft by remote-copilot	The assessment of premedical history as context cannot be served by remote-copilot		
(3) Detect homicidal-suicidal intent	Missing feedback to pursue the flight plan	Pursue flight plan; Safety recommendations regarding aeromedical decision-making after GWI18G	(5) Captain selected ALT 100 ft. OPEN DES, THR IDLE, SPD 308 kt.	(5) Alert on SEL ALT 100 ft, OPEN DES, THR IDLE, SPD 308 kt as suspicious human activity; (6) TARMS concludes that single-pilot is no longer in control
(4) Bring aircraft to a safe landing by control from GS				
(4a) Disable all unauthorised inputs and protect aircraft systems	(6) Failure to safely control the aircraft	(7) EAS disables all unauthorised inputs and protects aircraft systems (8) Take over control: In cruise by EAS (incl. FRF)	(7) EAS disables all unauthorised inputs and protects aircraft systems	(8) Take over control: In cruise by EAS (incl. FRF)

The numbers inside the table refer to the time course of UCAs in the process model of Fig. 4. The accident of Germanwings flight GWI18G from Barcelona to Düsseldorf (BEA, 2016) was modelled with the tripartite concept of RCO assumed to be valid in commercial aviation. Italics represent a possible safety constraint which was recommended after this accident (EASA 2015; EASA 2016a; 2016b)

The system had around 90% reliability of assessing physiological signals. The monitoring system by Oliveira et al. (2012), using oximetry and corporal temperature measurement, was found to assess both physiological parameters reliable during glider flight. A classification of physiological parameters to assess the pilot's workload or health state and to relate this to their ability to control the aircraft safely is missing in all these systems. Hence, no conclusion can be drawn on the pilot's cognitive state and the control of the aircraft, although a relation of these parameters to workload exists in general (Young et al. 2015). Functional near-infrared spectroscopy (fNIRS) can be used to passively monitor cognitive load during simulated and real flight with an accuracy of workload classification between 76 and 92% but a limited predictive value of 68% for expected workload levels (Çakır et al. 2016; Gateau et al. 2018). Thus, relating physiological measures and psychological states of human subjects remains a challenging undertaking for integrating it into sociotechnical systems. Until this issue is solved entirely, the practical application remains risky due to the technologies' lower maturity in further signal attribution in the operational context of aviation. Conclusions regarding the pilot's ability to control an aircraft independent of the situation were not investigated for these systems. This seems to be the reason why further applications of pilot monitoring technologies to influence flight procedures on the base of these data have almost not been investigated yet. In all examples, the assessment of physiological signals was found to be reliable whereas the subsequent classification of the pilot's physiological state regarding flight safety was either omitted, neglected or less satisfactory. In sum, current technology monitoring pilot's physiology remains at low levels of technological maturity for the transition to commercial RCO.

In contrast, aircraft systems monitoring has evolved further in terms of system integration into simulations of commercial airliners' flight deck. ACROSS' (ACROSS Consortium 2016) and SAFEE's systems (Table 1; OTDS, TARMS, EAS supplemented by FRF; Gaultier and SAFEE Consortium 2008; Laviv and Speijker 2007) can validly detect hazardous entries into aircraft systems, warn, take over control whilst protecting aircraft systems and land the aircraft autonomously. For example, the OTDS prototype employed detection algorithms based on basic behaviour detection principles and suitable indicators for suspicious behavioural patterns. The ability of TARMS to evaluate different security hazards subsequently was evaluated. Although the system suggested different courses of actions, the pilots doubted the TARMS' interpretation and decision-making. This issue of lack of trust in

interpretation was also apparent in the present theoretical analysis of JL350 regarding the hazardous holding on the previous flight (Table 3) and of GWI81G regarding the short-time selection of ALT 100 ft on the outbound flight (Table 4). Here, both deviations from normal operations would have been very presumably detected by a system protecting the aircraft from unauthorised operations as a deviation from the current valid flight plan and trajectory. The risk in the interpretation of such hazardous entries into aircraft systems is as follows. The SME of this study remarked that although the selection of 100 ft at a cruise flight level of 38,000 ft would be considered as an abnormal event with caution, it would be challenging to evaluate such detection even as a human pilot involved in-flight operations. At this point, a solution has to be found because automation depending on predefined values remains risky in terms of limited interpretability. A possible solution is to monitor the time period of the hazardous aircraft system's state and define an emergency based on additional measures. In contrast, other situations are easily to detect as hazards in which control can be automatically switched to ground. Among these is the long-term selection of the lowest possible altitude of the Flight Management System (FMS) of GWI18G and jumping off the seat during the approach of JL350. In the end, ambiguous detections of deviations from predefined norms of safe flight operations which do not immediately lead to a loss of control on airside followed by apparent danger remain challenging in integrating into a software solution that should assist or even take over the decision on switching control to ground. Connection to remote ground-based support does not guarantee the detection of malicious behaviour. Here, a system-theoretic view remains important because additional factors must be considered in system design, such as personal data protection. Observing the health data of the single-pilot too closely could lead to a lack of trust between the air and ground pilots.

Hence, we may indicate the technology for aircraft systems monitoring as under development for RCO (Harris 2007) because in general, the technology exists whereas it has only be tailored specifically to RCO. In sum, the predictive STAMP and STPAs of pilot incapacitation and homicide-suicide stimulate the debate about how to encounter these events in RCO by providing a comprehensive structured framework. Here, we encourage community proceeding research regarding the data these systems assess with relation to the operational context of operating an aircraft. This basic requirement has to be solved before considering the integration of such technologies into practical development.

Against this emerging background of RCO, some changes to the higher managerial levels of commercial aviation in the future might be required to improve the safety of flight operations, because the hierarchical safety control structure usually adapts over time (Leveson 2004a). The regulations regarding the two communication rule (ICAO 2012a) and aeromedical decision-making (Evans 2016) will remain because both represent effective countermeasures against in-flight incapacitation. The two communication rule is well established in practice (Schmid and Stanton 2018; Schmid et al. 2018) whereas the aeromedical services have been improving in Europe as reaction to the Germanwings crash in 2015 (EASA 2016a). In the future, aeromedical services might apply enhanced methods for diagnosis when compared with contemporary medical services. Pilot homicide-suicide has remained thankfully a very rare event throughout the history of aviation (Aviation Safety Network 2015; Kenedi et al. 2016). We anticipate that the current preventive enhancement of countermeasures, such as an additional psychological checkup and other services, provides a solid base to diminish this risk (EASA 2016a). For example, a proactive and non-punitive support programme will assist pilots in any issues which might potentially affect their fitness to fly whilst keeping data confidential and protected (European Commission 2018). Further possible influences of the incapacitation rate in future by a growing demand for air travel and better aeromedical services have not been investigated yet (Airbus 2018; Boeing 2018). Whereas the preconditions and upper level regulations in RCO remain similar, the cases of incapacitations might climb in total due to an increase in flight operations. This aspect has not been taken into account in any discussions on RCO yet.

The new infrastructure of RCO will serve as the driver of all changes in the hierarchical safety control structure of commercial air operations which we introduced above in the present operational concept. An old issue which might become more relevant in RCO is trust especially in a new advanced automation system which monitors pilot and system, and actively influences system operations (Ashleigh and Stanton 2001; Hoffmann et al. 2013; Lee and See 2004; Walker et al. 2016). It is crucial to enable safe operations. For example, trust in an assistance tool called the "Autonomous Constrained Flight Planner" aiming to improve flight planning of a remote-operator in RCO was found to be dependent from several different factors like transparency and risk of the recommended potential diversions (Brandt et al. 2017; Lachter et al. 2017; Sadler et al. 2016). The sociotechnical system of commercial aviation continues to evolve towards the future of RCO. All systems levels, including human-, automation- and environment-related factors, can potentially affect trust (Schaefer et al. 2016). A policy on data processing, storage, use and recording of alerts has led to the pilot's fear of loss of licence. The (multi)national aviation

authorities would face the challenge of integrating RCO into policy and operational practice.

5 Conclusions

In this paper, we have taken step towards applying the contemporary ideas on pilot health monitoring and implementation of additional automation tools to a possible future of RCO. STAMP and STPA have been used predictively which is rather novel to human systems integration. The models have shown how the application of specific advanced automation systems could prevent an incident resulting from incapacitation of the single-pilot on-board. The sociotechnical system even handles the rarer event of a pilot homicide-suicide. Hence, the concept on how to prevent a crash due to a purely human loss of control of the single-pilot extends existing function allocations of RCO. By considering the system-theoretic approach, we could take the whole system and identify stakeholders affected into account. These results stimulate debate about progressing to RCO in the future and encourage further development of operational procedures and technologies for specific use in commercial RCO. A limitation of the system-theoretic model and analyses of the scenarios of pilot incapacitation and homicide-suicide is that the predictions have not yet been validated empirically. An experimental flight simulation setup with standard methods is planned for future studies. Nonetheless, the functions of the single additional automation tools have been validated in case of the EU projects and look promising for RCO. In contrast, the pilot health monitoring systems require further research. Here, the research is rather fragmented at present, resulting in varied solutions which focus on different measures and responses. With the concept of RCO, residual issues of trust in the automation tools, the distributed crew member and the reliability of datalink remain. If all these issues are resolved, then RCO could indeed become a viable future concept of operations for commercial aviation.

Acknowledgements We would like to thank the anonymous commercial pilot for validating the results during two video conferences.

Abbreviations ACROSS, Advanced Cockpit for Reduction of Stress and Workload; ATC, Air Traffic Control; ATPL, Air Transport Pilot Licence; BEA, Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile; ConOps, Concept of Operations; CPL, Commercial Pilot Licence; EAS, Emergency Avoidance System; EASA, European Aviation Safety Agency; EU, European Union; FAA, Federal Aviation Administration; FE, Flight Engineer; FMS, Flight Management System; fNIRS, functional Near-Infrared Spectroscopy; FRF, Flight Reconfiguration Function; GS, Ground Station; HAZOP, Hazard and Operability Analysis; ICAO, International Civil Aviation Organization; MCO, Multi-Crew Operations; NASA, National Aeronautics and Space Administration; OTDS, On-board Threat Detection System; PM, Pilot Monitoring; RCO, Reduced-Crew Operations; SAFEE, Security of Aircraft in the Future European Environment; SARPs, Standards and Recommended Practices; SME, Subject Matter Expert; SPO, Single-Pilot Operations; STAMP, System-Theoretic Accident Model and Processes; STPA, System-Theoretic Process Analysis; TARMS, Threat Assessment and Response Management System; UCAs, Unsafe Control Actions

References

ACROSS Consortium (2016) Incapacitated crew: Emergency Aircraft Control System (EACS). European Commission, Bruessels, Belgium

Air Accident Investigation Unit Ireland (2008) Synoptic report. Incident. Boeing 767–333. Dublin, Ireland

Airbus (2011) Airbus A380 Flight Crew Operating Manual. Airbus S.A.S., Blagnac Cedex, France

Airbus (2018) Global networks, global citiziens: 2018-2037. Global Market Forecast. Airbus S.A.S., Blagnac Cedex, France

Aircraft Accident Investigation Committee (1984) Japan Airlines Corporation Douglas DC–61 JA 8061 Tokyo International Airport (Haneda) Offshore Navigation May 16, 1982 Aircraft accident investigation report: a statement and summary, vol 58–3. Ministry of Land and Transport, Tokyo, Japan

Allison CK, Revell KM, Sears R, Stanton NA (2017) Systems Theoretic Accident Model and Process (STAMP) safety modelling applied to an aircraft rapid decompression event. Saf Sci 98:159–166. https://doi.org/10.1016/j.ssci.2017.06.011

Ashleigh MJ, Stanton NA (2001) Trust: key elements in human supervisory control domains. Cogn Tech Work 3:92–100. https://doi.org/10.1007/PL00011527

Aven T (2015) Risk analysis, 2nd edn. Wiley, Chichester, UK

Aviation Safety Council China (2001) A serious incident involving a: China Airlines B-18503, A300-600R aircraft, while flying from Chiang Kai Shek International Airport to Ho Chi Minh City, Vietnam, the pilot became incapacitated during flight. Aviation Safety Council, New Taipei, China

Aviation Safety Network (2015) List of aircraft accidents and incidents intentionally caused by pilots. http://news.aviation-safety.net/2015/03/26/list-of-aircraft-accidents-and-incidents-deliberately-caused-by-pilots/. Accessed 7 Sept 2017

Benitez DM, del Corte Valiente A, Lanzi P (2018) A novel global operational concept in cockpits under peak workload situations. Saf Sci 102:38–50. https://doi.org/10.1016/j.ssci.2017.09.028

Bilimoria KD, Johnson WW, Schutte PC (2014) Conceptual framework for single pilot operations. In: Proceedings of the International Conference on Human-Computer Interaction in Aerospace. HCI-Aero '14. ACM, New York, NY, USA. https://doi.org/10.1145/2669592.2669647

Boeing (2018) Commercial Market Outlook: 2018-2037. Boeing, Seattle, WA, USA

Boy GA (2016) Flexibility. In: Boy GA (ed) Tangible interactive systems: grasping the real world with computers. Human–Computer Interaction Series. Springer International Publishing, Cham, Switzerland, pp 107–129. https://doi.org/10.1007/978-3-319-30270-6_6

Brandt SL, Lachter J, Battiste V, Johnson W (2015) Pilot situation awareness and its implications for single pilot operations: analysis of a human-in-the-loop study. Procedia Manuf 3:3017–3024. https://doi.org/10.1016/j.promfg.2015.07.846

Brandt SL, Lachter J, Russell R, Shively RJ (2017) A human-autonomy teaming approach for a flight-following task. In: Baldwin C (ed) Advances in neuroergonomics and cognitive engineering: Proceedings of the AHFE 2017. Advances in intelligent systems

and computing, vol 586. Springer International Publishing, Cham, Switzerland, pp 12–22. https://doi.org/10.1007/978-3-319-60642-2_2

Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile (2011) Incidents in air transport: flight crew incapacitation. BEA France, Le Bourget, France

Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile (2016) Final report: accident on 24 March 2015 at Prads-Haute-Bléone (Alpes-de-Haute-Provence, France) to the Airbus A320-211 registered D-AIPX operated by Germanwings. BEA France, Le Bourget, France

Çakır MP, Vural M, Koç SÖ, Toktaş A (2016) Real-time monitoring of cognitive workload of airline pilots in a flight simulator with fNIR optical brain imaging technology. In: Schmorrow D, Fidopiastis CM (eds) Foundations of augmented cognition: neuroergonomics and operational neuroscience. Lecture notes in artificial intelligence, vol 9743. Springer International Publishing, Cham, Switzerland, pp 147–158. https://doi.org/10.1007/978-3-319-39955-3_14

Cargo Airlines Respond to FAA Reauthorization Section 744 Language (2018) Air Line Pilots Association, International, Washington, DC, USA

Comisión de Investigación de Accidentes e Incidentes de Aviación Civil (2011) Final report: incident involving Boeing 737-800, EI-EKB Ryanair and Boeing 767-300, N366AA American Airlines, Barcelona airport, 14 April 2011. Ministerio de Fomento, Madrid, Spain

Dao A-QV, Koltai K, Cals SD, Brandt SL, Lachter J, Matessa M, Smith DE, Battiste V, Johnson WW (2015) Evaluation of a recommender system for single pilot operations Procedia Manuf 3:3070–3077 :https://doi.org/10.1016/j.promfg.2015.07.853

Deutsch S, Pew RW (2005) Single pilot commercial aircraft operation. BBN Technologies, Cambridge, MA, USA

Driscoll K, Roy A, Ponchak DS (2017a) Cyber safety and security for reduced crew operations (RCO). Paper presented at the 30th Digital Avionics Systems Conference DASC, St. Petersburg, FL, USA,

Driscoll K, Roy A, Ponchak DS, Downey AN (2017b) Cyber safety and security for reduced crew operations (RCO). Paper presented at the Aerospace Conference, 2017 IEEE, Big Sky, MT, USA

Dunjóa J, Fthenakis V, Vílcheza JA, Arnaldosa J (2010) Hazard and operability (HAZOP) analysis. A literature review. J Hazard Mater 53:19–32. https://doi.org/10.1016/j.jhazmat.2009.08.076

Embraer SA (2015) Phenom 300. São José dos Campos, Brazil

European Aviation Safety Agency (2015) Task force on measures following the accident of germanwings flight 9525: Final Report. European Aviation Safety Agency, Cologne, Germany

European Aviation Safety Agency (2016a) Aircrew medical fitness: implementation of the recommendations made by the EASA-led Germanwings Task Force on the accident of the Germanwings Flight 9525 vol 14/2016. European Aviation Safety Agency, Cologne, Germany

European Aviation Safety Agency (2016b) Minimum cockpit occupancy. European Aviation Safety Agency, Cologne, Germany

European Commission (2015) Commission Regulation (EU) No 965/2012 Off J Eur Union 55

European Commission (2018) Commission Regulation (EU) 2018/1042 Off J Eur Union:188/183–188/188

Evans ADB (2016) Aeromedical risk: a numerical approach. In: Gradwell DP, Rainford DJ (eds) Ernsting's Aviation and Space Medicine, 5th edn. CRC Press, Boca Raton, FL, USA, pp 373–384

Evans S, Radcliffe S-A (2012) The annual incapacitation rate of commercial pilots. Aviat Space Environ Med 83:42–49. https://doi.org/10.3357/asem.3134.2012

Evans ADB, Evans S, Harper G (2016) International regulation of medical standards. In: Gradwell DP, Rainford DJ (eds) Ernsting's Aviation and Space Medicine, 5th edn. CRC Press, Boca Raton, FL, USA, pp 357–371

FAA Reauthorization Act of 2018 (H.R.302) (2018). Congress, Washington DC, USA

FAA Reauthorization Act of 2018 (H.R.4) (2018). Congress, Washington, D.C., USA

Federal Aviation Administration (2001) Instrument Flying Handbook. FAA-H-8083-15. U.S. Department of Transportation, Washington, D.C., USA

Fleming CH, Leveson NG (2014) Improving hazard analysis and certification of integrated modular avionics. J Aerosp Inf Syst 11:397–411. https://doi.org/10.2514/1.i010164

Fleming CH, Spencer M, Thomas J, Leveson N, Wilkinson C (2013) Safety assurance in NextGen and complex transportation systems. Saf Sci 55:173–187. https://doi.org/10.1016/j.ssci.2012.12.005

Gateau T, Ayaz H, Dehais F (2018) In silico vs. over the clouds: on-the-fly mental state estimation of aircraft pilots, using a functional near infrared spectroscopy based passive-BCI. Front Hum Neurosci 12:1–14. https://doi.org/10.3389/fnhum.2018.00187

Gaultier D, SAFEE Consortium (2008) SAFEE (Security of Aircraft in the Future European Environment): Final Publishable Report. SAGEM Défense Sécurité

Geymar JAB, Ebecken NFF (1995) Fault-tree analysis: a knowledge-engineering approach. IEEE Trans Reliab 40:37–45

Graham J, Hopkins C, Loeber A, Trivedi S (2014) Design of a single pilot cockpit for airline operations. Paper presented at the Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA,

Grant E, Salmon PM, Stevens N, Goode N, Read GJM (2018) Back to the future: what do accident causation models tell us about accident prediction? Saf Sci 104:99–109. https://doi.org/10.1016/j.ssci.2017.12.018

Harris D (2007) A human-centred design agenda for the development of single crew operated commercial aircraft. Aircr Eng Aerosp Tech 79:518–526. https://doi.org/10.1108/00022660710780650

Harris D, Stanton NA (2010) Aviation as a system of systems: preface to the special issue of human factors in aviation. Ergonomics 53:145–148. https://doi.org/10.1080/00140130903521587

Hinkelbein J, Dambier M, Glaser E, Landgraf H (2008) Medical Incapacitation im Cockpit - Inzidenz, Ursachen und Folgen Flugmedizin. Tropenmedizin · Reisemedizin 15:14–19. https://doi.org/10.1055/s-2008-1075813

Hoffmann RR, Johnson M, Bradshaw JM, Underbrink A (2013) Trust in automation. IEEE Intell Syst 28:84–88. https://doi.org/10.1109/MIS.2013.24

International Civil Aviation Organization (2012a) Manual of civil aviation medicine. ICAO, Montréal, Canada

International Civil Aviation Organization (2012b) Manual of procedures for establishment and management of a state's personnel licensing system, 2nd edn. ICAO, Montréal, Canada

Ishimatsu T, Leveson NG, Thomas JP, Fleming CH, Katahira M, Miyamoto Y, Ujiie R, Nakao H, Hoshino N (2014) Hazard analysis of complex spacecraft using Systems-Theoretic Process Analysis. J Spacecr Rockets 51:509–522. https://doi.org/10.2514/1.a32449

Johnson WW, Lachter J, Feary M, Comerford D, Battiste V, Mogford R (2012) Task allocation for single pilot operations: a role for the ground. In: Proceedings of the International Conference on Human-Computer Interaction in Aerospace. HCI-Aero '12. ACM, New York, NY, USA

Kenedi C, Friedman SH, Watson D, Preitner C (2016) Suicide and murder-suicide involving aircraft. Aerosp Med Hum Perform 87:388–396. https://doi.org/10.3357/amhp.4474.2016

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. https://doi.org/10.1016/j.promfg.2015.07.948

Lachter J, Brandt SL, Battiste V, Ligda SV, Matessa M, Johnson WW (2014) Toward single pilot operations: developing a ground station.

In: Proceedings of the International Conference on Human-Computer Interaction in Aerospace. HCI-Aero '14. ACM, New York, NY, USA. https://doi.org/10.1145/2669592.2669685

Lachter J, Brandt SL, Battiste V, Matessa M, Johnson WW (2017) Enhanced ground support: lessons from work on reduced crew operations. Cogn Tech Work 19:279–288. https://doi.org/10.1007/s10111-017-0422-6

Laviv O, Speijker LJP (2007) SAFEE - Security of Aircraft in the Future European Environment. National Aerospace Laboratory NLR, Amsterdam, Netherlands

Lee JD, See KA (2004) Trust in automation: designing for appropriate reliance. Hum Factors 46:50–80. https://doi.org/10.1518/hfes.46.1.50_30392

Leveson NG (2004a) A new accident model for engineering safer systems. Saf Sci 42:237–270. https://doi.org/10.1016/s0925-7535(03)00047-x

Leveson NG (2004b) Role of software in spacecraft accidents. J Spacecr Rockets 41:564–575. https://doi.org/10.2514/1.11950

Leveson NG (2011) Engineering a safer world: systems thinking applied to safety. MIT Press, Cambridge, MA, USA

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

Leveson NG (2017) Rasmussen's legacy: a paradigm change in engineering for safety. Appl Ergon 59:581–591. https://doi.org/10.1016/j.apergo.2016.01.015

Ligda SV, Fischer U, Mosier K, Matessa M, Battiste V, Johnson WW (2015) Effectiveness of advanced collaboration tools on crew communication in reduced crew operations. In: Harris D (ed) Engineering psychology and cognitive ergonomics. Lecture notes in artificial intelligence, vol 9174. Springer International Publishing, Cham, Switzerland, pp 416–427. https://doi.org/10.1007/978-3-319-20373-7_40

Maiolo L, Maita F, Castiello A, Minotti A, Pecora A (2017) Highly wearable wireless wristband for monitoring pilot cardiac activity and muscle fine movements. In: 2017 IEEE International Workshop on Metrology for AeroSpace (MetroAeroSpace). IEEE, Padua, Italy, pp 271–275. https://doi.org/10.1109/MetroAeroSpace.2017.7999578

Malik A, Gollnick V (2016) Impact of reduced crew operations on airlines – operational challenges and cost benefits. Paper presented at the 16th AIAA Aviation Technology, Integration, and Operations Conference, Washington, D.C., USA. AIAA 2016-3303. https://doi.org/10.2514/6.2016-3303

Matessa M, Strybel T, Vu K, Battiste V, Schnell T (2017) Concept of operations for RCO/SPO. NASA, Moffett Field, CA, USA

Norman RM (2007) Economic opportunities and technological challenges for reduced crew operations. Boeing, Seattle, WA, USA

Oliveira LML, Rodrigues JJPC, Mação BM, Nicolau PA, Zhou L (2012) A WSN solution for light aircraft pilot health monitoring. In: Wireless Communications and Networking Conference (WCNC). pp 119–124. https://doi.org/10.1109/wcnc.2012.6213959

Oxford Aviation Academy (2008) Air Law. ATPL Ground Training Series, vol 1, 4 edn. Oxford Aviation Academy (UK), Shoreham, UK

Plioutsias A, Karanikas N, Chatzimichailidou MM (2017) Hazard analysis and safety requirements for small drone operations: to what extent do popular drones embed safety? Risk Anal:1–23. https://doi.org/10.1111/risa.12867

Rasmussen J (1997) Risk management in a dynamic society: a modelling problem. Saf Sci 27:183–213. https://doi.org/10.1016/S0925-7535(97)00052-0

Revell KM, Allison C, Sears R, Stanton NA (2018) Modelling distributed crewing in commercial aircraft with STAMP for a rapid decompression hazard ergonomics (in press). https://doi.org/10.1080/00140139.2018.1514467

Rong H, Tian J (2015) STAMP-based HRA considering causality within a sociotechnical system: a case of Minuteman III missile accident. Hum Factors 57:375–396. https://doi.org/10.1177/0018720814551555

Sadler G et al. (2016) Effects of transparency on pilot trust and agreement in the autonomous constrained flight planner. Paper presented at the IEEE/AIAA 35th Digital Avionics Systems Conference (DASC), Piscataway, NJ, USA,

Schaefer KE, Chen JYC, Szalma JL, Hancock PA (2016) A meta-analysis of factors influencing the development of trust in automation. Hum Factors 58:377–400. https://doi.org/10.1177/0018720816634228

Schmid D, Korn B (2017) A tripartite concept of a remote-copilot center for commercial single-pilot operations. Paper presented at the AIAA SciTech 2017 Forum, Grapevine, TX, USA,

Schmid D, Korn B (2018) The operational issue of an airliner's reduced-crew caused by data-link break-up to remote support. Proc Hum Factors Ergon Soc Annu Meet 62:71–75. https://doi.org/10.1177/1541931218621016

Schmid D, Stanton NA (2018) How are laser attacks encountered in commercial aviation? A hazard analysis based on systems theory. Saf Sci 110:178–191. https://doi.org/10.1016/j.ssci.2018.08.012

Schmid D, Vollrath M, Stanton NA (2018) The System Theoretic Accident Modelling and Process (STAMP) of medical pilot knock-out events: pilot incapacitation and homicide-suicide. Saf Sci 110:58–71. https://doi.org/10.1016/j.ssci.2018.07.015

Schmitt D-R, Többen H, Philippens H (2010) Passivation of misused aircraft to protect passengers, airports and infrastructure. In: Grant I (ed) 27th Congress of the International Council of Aeronautical Sciences. Optimage, Edinburgh, UK, pp 1–3

Stanton NA, Harvey C (2017) Beyond human error taxonomies in assessment of risk in sociotechnical systems: a new paradigm with the EAST 'broken-links' approach. Ergonomics 60:221–233. https://doi.org/10.1080/00140139.2016.1232841

Stanton NA, Harris D, Starr A (2016) The future flight deck: modelling dual, single and distributed crewing options. Appl Ergon 53:331–342. https://doi.org/10.1016/j.apergo.2015.06.019

Stanton NA, Plant KL, Revell KMA, Griffin TGC, Moffat S, Stanton MJ (2019) Distributed cognition in aviation operations: a gate-to-gate study with implications for distributed crewing. Ergonomics (in press). https://doi.org/10.1080/00140139.2018.1520917

UAE General Civil Aviation Authority (2012) Air accident investigation sector: pilot incapacitation. Abu Dhabi, United Arab Emirates

Walker GH, Stanton NA, Salmon PM (2016) Trust in vehicle technology. Int J Veh Des 70:157–182. https://doi.org/10.1504/IJVD.2016.074419

Young MS, Brookhuis KA, Wickens CD, Hancock PA (2015) State of science: mental workload in ergonomics. Ergonomics 58:1–17. https://doi.org/10.1080/00140139.2014.956151