NLR Air Transport Safety Institute

Research & Consultancy

Executive summary

DEVELOPMENT OF A SAFETY ASSESSMENT METHODOLOGY FOR THE RISK OF COLLISION OF AN UNMANNED AIRCRAFT SYSTEM WITH THE GROUND

Problem area

Recent technological developments and increased utilization of Unmanned Aircraft Systems (UAS) have widened their application from military operations to also civil and commercial operations. UAS are most beneficial when they can share the whole airspace with manned aircraft. However, integration of UAS into non-segregated airspace is only viable if UAS operations are proved to be safe enough. The concern is that UAS operations could pose a safety problem for other aircraft and persons or property on the ground.

Description of work

The objective of this paper is to develop and apply a safety risk analysis methodology for the risk of collision of an Unmanned Aircraft System with the ground. The method provides insight into the probability of a UAS collision with the ground in relation with safety objectives and requirements. To better understand the differences between manned and unmanned aircraft, UAS performance characteristics are examined. This helps to clarify in which airspace classes the different available UAS may be able to fly. This concerns the broad range of size, various configurations and different performance characteristics. Next, causal models are developed for 15 accident scenario that may result in a collision with the ground. These causal models are represented as Event Sequence Diagrams (ESDs) and Fault Trees (FTs), and provide a logical structure showing how hazards and causal factors could combine to cause a collision with the ground. This approach utilizes the Causal model for Air Transport Safety (CATS) developed for the Dutch Ministry of Transport. Five specific UAS related ESDs are added to cover UAS specific hazards that do not exist in manned aircraft operation. Using the twenty ESDs, a UAS accident probability model for the risk of collision with the ground is developed.

Results and conclusions

A safety risk analysis methodology for the risk of collision of an Unmanned Aircraft System with the ground has been developed. Causal models are developed for each accident scenario that may result in a collision with the ground. The method has been applied to derive Safety Objectives for hazardous events related to UAS operations in non segregated airspace, performed with UAS that are equivalent with manned aircraft in category Certification Specifications (CS) 25. The Safety Objectives may be apportioned further (in a subsequent study) into Safety Requirements for each of the root causes, failures and causal factors underlying an accident scenario. The method provides insight into the probability of a UAS collision with the ground in relation with safety objectives. In third party risk analyses, usually *Societal risk* (to a group) and *Individual risk* (to individuals at a location) are evaluated. It is therefore recommended to further extend the developed method with an accident location model and an accident consequence model, in order to assess UAS third party risk in terms of these risk metrics.

Applicability

The developed methodology supports regulators with the setting of UAS safety objectives and safety requirements. It may also be used by applicants (UAS operators and manufacturers) for identification of UAS related hazards, causal factors, and accident scenarios. This paper illustrates the method for UAS operations performed with UAS that are equivalent with manned aircraft in category CS-25. For other types of UAS, it will be necessary to investigate if the ESDs developed in this paper still apply or whether or not further adaptations are required. It also remains to be investigated if the fact that a UAS does not carry passengers could allow for a less stringent Target Level of Safety than could apply for manned aviation.

NLR-TP-2011-325

Development of a safety assessment methodology for the risk of collision of an Unmanned Aircraft System with the ground

A.D. Ozuncer[1]
L.J.P. Speijker
J.A.A.M. Stoop[1]
R. Curran[1]

[1] Delft University of Technology

Customer	National Aerospace Laboratory NLR
Contract number	----
Owner	NLR + partner(s)
Division	Air Transport
Distribution	Unlimited
Classification of title	Unclassified
	August 2011

Approved by:

Author	Reviewer	Managing department
	R 10/08	

Content

Development of a safety assessment methodology for the risk of collision of an Unmanned Aircraft System with the ground

A.D. Ozuncer*, L.J.P. Speijker**, J.A.A.M. Stoop*, R. Curran*

* Delft University of Technology, ** National Aerospace Laboratory NLR

ABSTRACT

Recent technological developments and increased utilization of Unmanned Aircraft Systems (UAS) have widened their application from military operations to also civil and commercial operations. UAS are most beneficial when they can share the whole airspace with manned aircraft. However, integration of UAS into non-segregated airspace is only viable if UAS operations are proved to be safe enough. The concern is that UAS operations could pose a safety problem for other aircraft and persons or property on the ground [19].

The objective of this paper is to develop and apply a safety risk analysis methodology for the risk of collision of an Unmanned Aircraft System with the ground. Such method could support regulators with the setting of UAS safety requirements. It may also be used by applicants (UAS operators and manufacturers) for identification of UAS related hazards, causal factors, and accident scenarios. The method provides insight into the probability of a UAS collision with the ground in relation with safety objectives and requirements.

To better understand the differences between manned and unmanned aircraft, UAS performance characteristics are examined. This helps to clarify in which airspace classes the different available UAS may be able to fly. This concerns the broad range of size, various configurations and different performance characteristics (maximum takeoff weight, maximum flight altitude, endurance and maximum speed).

Next, causal models are developed for each accident scenario that may result in a collision with the ground. These causal models are represented as Event Sequence Diagrams (ESDs) and Fault Trees (FTs), and provide a logical structure showing how hazards and causal factors could combine to cause a collision with the ground. This approach utilizes the Causal model for Air Transport Safety (CATS) developed for the Dutch Ministry of Transport [1]. Specific UAS related ESDs are added to cover UAS specific hazards that do not exist in manned aircraft operation [12]. Using the newly developed ESDs, a UAS accident probability model is developed for determination of the frequency of occurrence of a UAS accident in relation with safety objectives and requirements.

In third party risk analyses, usually *Societal risk* (to a group) and *Individual risk* (to individuals at a location) are evaluated. It is recommended to extend the method with an accident location model and an accident consequence model, in order to assess UAS third party risk in terms of these risk metrics.

INTRODUCTION

The earliest area of usage of the unmanned aircraft systems is for military applications where these systems are used as expendable weapons or targets. Recent technological developments and increased utilization of Unmanned Aircraft Systems (UAS) have widened their application from military operations only to also civil and commercial operations. Research on UAS safety has been carried out with utilization of different approaches, focusing on the integration of UAS in non-segregated airspace [2, 3, 4, 5, 6, 14, 15, 16, 17, 18]. A problem area that has not yet been fully tackled – and to which this study will contribute to – is the derivation of a consistent set of safety objectives and safety requirements for the risk of collision of a UAS with the ground. One of the most significant challenges in the safety assessment of the ground collision risk of a UAS is the lack of past accident data. This creates a challenge, because it is to some extent uncertain which hazards and causes could lead to UAS accidents. A further challenge is the fact that regulations and standards for civil use of UAS are still under further development. Therefore, it is not yet possible to develop a very detailed concept of operation, and identification of the hazards and causes will – for the moment - have to stay at a relatively high level. Consequently, some general assumptions are to be made regarding the UAS itself and its operation. It is clear that it has to be shown that the current safety level does not decrease.

The objective of this paper is to develop and apply a safety assessment methodology for the risk of collision of a UAS with the ground. The method support regulators and applicants in the process for approval and certification of civil UAS use.

The next section introduces UAS and their performance characteristics. The paper continues with a description of the basic principles underlying the developed safety risk analysis methodology. This is followed by a description of the causal

models developed for each accident scenario that may result in a collision with the ground. Safety objectives and safety requirements are derived using a Target Level of Safety for the overall probability of ground collision. Finally, this paper provides conclusions, recommendations, and references.

UNMANNED AIRCRAFT SYSTEMS

An Unmanned Aircraft Systems is defined by ICAO as "an aircraft and its associated elements which are operated with no pilot on board" [7]. In order for UAS to integrate into non-segregated airspace and at non-segregated aerodromes, there shall be a pilot responsible for the UAS operation [7]. Therefore, for the purpose of this paper, it is assumed that there is a remote pilot, situated at a remote pilot station (e.g. a Ground Control Station (GCS)). The Unmanned Aircraft itself is one component of the UAS, which also includes other components such as the GCS, payload, data link and data storage system and other supporting equipment. The GCS is the brain of the whole system from where the flight control orders are sent to the unmanned aircraft and where potential sensor data is analyzed. There can be more than one remote pilot in the GCS. A data link and data storage system is facilitated by a two way communication link, an uplink and a downlink, between the unmanned aircraft and the GCS.

Considering UAS applications in the non-segregated airspace, the presence of various vehicle types, configurations and sizes should be recognized. The functional categories of UAS are derived from the past and current missions of these vehicles. In the light of past and present experience; one way to congregate the functional capabilities of UAS is through the following categories: Target and decoy, reconnaissance, combat, logistics, research and development and civil and commercial. Some UAS are capable to fulfill more than one functional capability while others are designed only to fulfill one specific mission. UAS can also be classified according to their size, range, and altitude. UVS International uses the following categories [8]: Nano, Micro, Mini, Close Range (CR), Short Range (SR), Medium Range (MR), Medium Range Endurance (MRE), Low Altitude Deep Penetration (LADP), Low Altitude Long Endurance (LALE), Medium Altitude Long Endurance (MALE), High Altitude Long Endurance (HALE), Unmanned Combat Aerial Vehicle (UCAV), Lethal (LETH), Decoy (DEC), Stratospheric (STRATO), Exo-stratospheric (EXO), Space (SPACE). Note that e.g. the Global Hawk and Euro Hawk fit in the HALE category, the Predator in the MALE category, the Sperwer in the MR category and the Geocopter GC-201 in category CR.

Figure 1 shows maximum operating altitude versus Maximum Take-Off Weight (MTOW) characteristics of thirteen different types of UAS and their operating airspace classes [8, 9] on the right side. Nano, micro and mini UAS are operated in uncontrolled airspace and at a relatively low altitude. CR, SR, MR, DEC and LETH UAS may fly in the airspace classes B, C, D and E. Generally, their altitude range stands between

3000m to 6300m. MALE type UAS mostly operate in airspace class A, while HALE types have the capability to operate above 18000 m in uncontrolled airspace. Although the HALE operating environment is uncontrolled airspace, they may have to pass the controlled airspaces (A, B, C, D and E) before reaching their operating altitude. Under these circumstances, these HALE UAS should also have the same safety considerations as the UAS which operate in the controlled airspace classes.
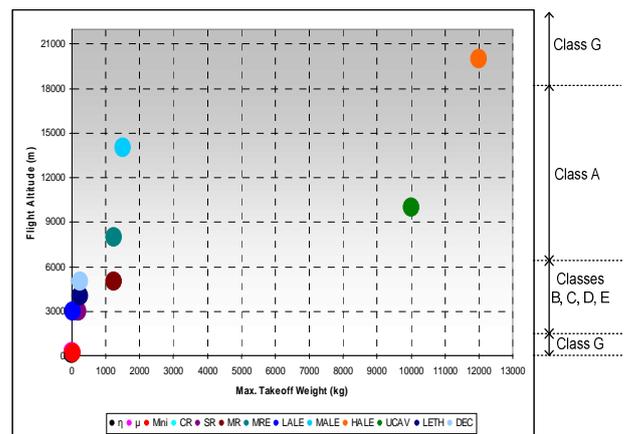
Figure 1 UAS flight altitude versus MTOW

Figure 2 sketches the relation between endurance and MTOW of the thirteen different UAS categories [8]. Nano and micro unmanned aerial vehicles have very low endurance times that can be measured with minutes. One can observe the increasing trend of the maximum endurance capability as the mass of the unmanned aircraft increases. UAS have a very wide range of endurance capability. While nano, mini and micro UAVs can be operated not exceeding a couple of hours, a strategic UAV can operate up to 36 hours.
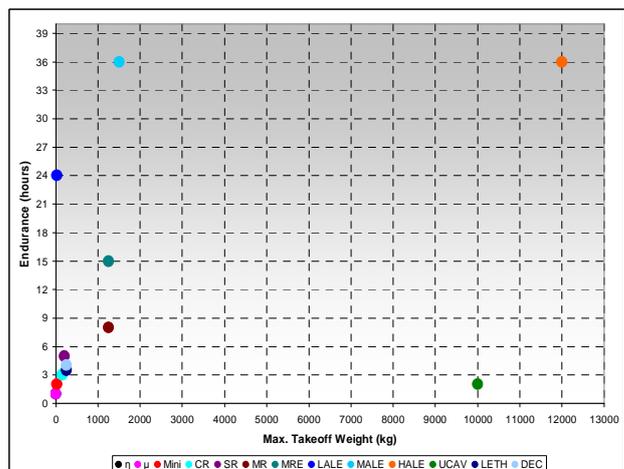
Figure 2 UAS endurance versus MTOW

Figure 3 shows the relationship between maximum speed and maximum altitude of different size classes of unmanned aircraft systems [8]. The maximum speed interval for various mini UAS vary between 220-250 km/h. CR, SR, MR, MRE and LALE type UAS do not have high velocity (changes between 120-350 km/h) compared to MALE and HALE. At the altitudes at which CR, SR, MR, MRE and LALE type of UAS fly, manned aircraft speeds can be reached. The cruise speed of MALE and HALE is significantly higher than that of other UAS.
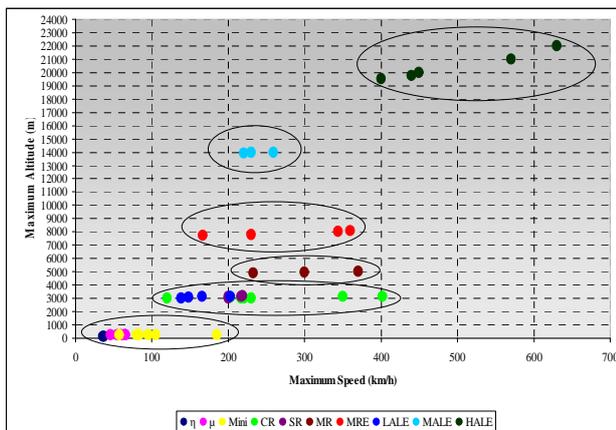
Figure 3 UAS maximum speed versus maximum altitude

SAFETY METHODOLOGY

A generic process for the safety assessment of ATM systems usually deals with three subsequent questions [10]:
▪ How safe does the system needs to be?
▪ How safe can the system be?
▪ How safe is the implemented system?

Implementation and transfer to operations is not within the scope of this paper. Therefore, in this paper the focus will be on the establishment of a Target Level of Safety (TLS), the associated Safety Objectives (SOs) and Safety Requirements (SRs) for the risk of collision of a UAS with the ground. This may subsequently be used by manufacturers and operators as guidance for implementation and transfer to UAS operations.

To determine how safe the system needs to be, Safety Objectives are specified on the basis of an overall TLS. A SO is a qualitative or quantitative statements that defines the maximum frequency or probability at which a hazard can be accepted to occur. To determine how safe the system can be, the SOs are apportioned into Safety Requirements for each of the hazards and causes underlying an event for which a SO is specified. Although the SRs may include organizational, operational, procedural, functional, performance, and interoperability requirements or environment characteristics,

they are usually allocated to the system elements, i.e. specify the risk level to be achieved by the system elements.

Our proposed method follows exactly the same process, but derives the TLS, SOs, and SRs for the collision risk of UAS with the ground from the existing Causal model for Air Transport Safety (CATS) [1], which was originally developed for commercial air transport operations. The proposed approach for the setting of UAS safety requirements uses Event Sequence Diagrams (ESDs) and Fault Trees (FTs), and is proposed to consist of the following sequential steps [12]:
1. Define the scope of the UAS accident probability model, including type of operation, assumptions, limitations, etc.
2. Identify relevant incident/accident and accident avoidance scenarios for UAS based on literature and safety studies.
3. Select ESDs from CATS that are valid for UAS as well.
4. Modify selected ESDs for UAS operations, if necessary.
5. Develop ESDs for scenarios unique to UAS operations.
6. Select, modify and/or develop Fault Trees for each of the events in the UAS related ESDs.
7. Set a Target Level of Safety for the overall probability of occurrence of a UAS collision with the ground.
8. Derive Safety Objectives for each of the end-events ground collision' in all the ESDs developed for UAS.
9. Derive Safety Requirements for each of the hazards and causes represented in the FTs.

An advantage of this approach is that utilization of ESDs will visually demonstrate event series that lead to an accident. For the same reason, utilization of fault trees demonstrates cause and effect relationship of hazardous events. A generic ESD with FTs is given below. Each ESD consists of several events:
• One initiating event;
• Several end-events, which are the end state of a sequence of events, and;
• One or more pivotal events (failures of so-called 'barriers') with fault trees.
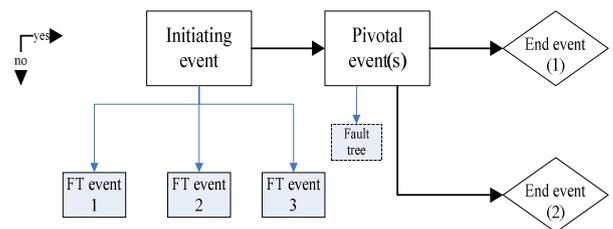
Figure 4 Generic ESD with fault trees

In this paper, the initiating event is defined as the first event of the accident scenario which commences the series of events leading to collision with ground. Accident scenarios end up with collision with ground end events and accident avoidance scenarios end up with no ground collision end events.

The total probability of collision of a UAS with the ground is equal to the sum of the collision with ground probabilities of each accident scenario, which should be smaller than the TLS.

In this paper, the safety objectives pertain to the initiating and pivotal events of the event sequence diagrams and represent the maximum allowed probability that is necessary to be met by the safety requirements. Determined Safety Requirements relate to various components of unmanned aircraft systems and they represent the maximum failure frequency that UAS components are allowed to have in order to assure that the risk of a collision with the ground does not exceed a defined TLS.

GROUND IMPACT RISK ANALYSIS

In this paper, ground impact risk represents the risk of a UAS collision with the ground. This type of risk includes UAS collision with earth, sea or other obstacles. A possible ground collision might cause damage to the aircraft, damage to the obstacles, injuries and/or fatalities. Ground impact risk analysis is performed via causal models which are developed for each accident scenario that may result in a collision with the ground.

Some assumptions have been adopted in the qualitative development phase of the Event Sequence Diagrams to maintain the general applicability of the developed methodology to a wide range of UAS. These assumptions are considered necessary as they constrain the complexity of the system or because of the limited information on available and/or currently used systems in unmanned aviation. The following general assumptions have been made:
- The UAS is to a large extent equivalent with manned aircraft in category Certification Specifications (CS)-25.
- The UAS comprises one Ground Control Station (GCS) and at least one remote pilot who are located at the GCS.
- The following communications links are available:
  o Air-ground link between the GCS and the aerial vehicle for command and control;
  o Air-ground link between ATC and the aerial vehicle for traffic surveillance;
  o Communication link(s) between the UAS remote pilots and ATC.
- The UAS flight may cross multiple ATC control sectors.
- The UAS may carry different payloads, but is not used to transport passengers.
- Both night and day UAS operations are considered.
- The UAS uses runways for take off and approach/landing.
- The UAS comprises a single engine and fixed wing.
- The UAS has fire detection, warning and extinguishing systems onboard.
- The UAS is able to fly in icing conditions.
- The UAS is used for civil and commercial IFR operations.

In addition to the above, 3 modelling assumptions are made:
- There are no dependencies between the different ESDs.
- Pivotal events cannot occur 'partially'; these events are described as either happening (yes) or not happening (no).

ACCIDENT SCENARIOS

Aviation accidents tend to result from a combination of many different causal factors (human errors, technical failures, environmental and management influences) in certain characteristic accident categories (loss of control, collision, fire etc), whose causes and consequences differ according to the phase of flight in which they occur (taxi, take-off, en-route etc). The CATS project approached this complexity by developing 33 separate causal models for each accident category in commercial air transport [7]. A review of the original 33 CATS scenarios has yielded fifteen relevant ESDs applicable to UAS operations. The ESDs which do not have a "collision with ground" end event are eliminated for the scope of this research. Five further UAS specific ESDs can be added to cover UAS specific hazards that do not exist in manned aircraft operation. The result is provided in Table 1. Note that the total collision with ground probability of the whole system is equal to the sum of the collision with ground probabilities of each accident scenario.

Table 1 UAS hazards that might result in a ground collision

#	Name of the Event Sequence Diagrams
5	Operation of UAS by remote pilot inappropriate
6	UAS takes off with contaminated wing
7	Weight and balance outside limits (takeoff)
8	UAS encounters performance decreasing windshear
11	Fire on board UAS
12	Remote pilot spatially disorientated
13	Flight control system failure
14	Remote pilot(s) incapacitation
15	Anti-ice system not operating
16	Flight instrument failure
17	UAS encounters adverse weather
18	UAS engine failure
19	Unstable approach
21	Weight and balance outside limits (approach/landing)
37	Wake vortex encounter
40	UAS Positional information system failure
41	UAS Data link failure
42	Unnatural conditions in UAS Ground Control Station
43	UAS Mid air collision
44	A part of the UAS falls down

Assuming that the future UAS operation will have to be at least as safe as commercial air transport in the current manned aviation system [11], it is possible to derive SOs for each ESD using the quantified CATS [1]. The collision with the ground end event's SOs, are used as the starting point to calculate SOs for the pivotal events, other end events and the initiating event in the event sequence diagram. Figures 5 to 24 demonstrate the ESDs with their safety objectives located at the top of the

event boxes. The SOs for the end-event "ground collision" of the ESDs are indicated with red color. The pivotal events' SOs that are determined via assumptions, are indicated with a blue color. A conservative approach is followed when making assumptions for the SO of pivotal events which are dependent on the behavior of the remote pilot(s). The human error probability of remote pilot depends on many factors, including the skill level, training, and performance of critical tasks. When it is highly likely that a remote pilot will fail to regain control of the aircraft after a certain sequence of events, it is assumed he will. Hence, a failure probability of 1 is then used. It is furthermore assumed that practicable safety requirements for a remote pilot may not be more stringent than in the order of about 10^{-3} probability of failure per flight. Practicable safety requirements for system failures may be as stringent as about 10^{-7} failure probability per flight. Therefore, when making assumptions, the SOs of the pivotal events that are dependent on human behavior are set to the lesser stringent values, while the SOs for pivotal events that are related to system failures are set to be more stringent. This way of balancing the SOs is expected to result in a realistic set of safety objectives and safety requirements, with the highest likelihood that all requirements are practicable and achievable.

A total of 23 accident and 34 accident avoidance scenarios are represented by these 20 ESDs. Accident scenarios end up with 'collision with ground' end events and accident avoidance scenarios end up with 'no ground collision' end events. Note that the latter may, besides nonhazardous consequences such as 'UAS continues flight' or 'UAS continues landing roll', also contain hazardous consequences that are not in the scope of an end event 'UAS ground collision' (e.g. aircraft continues flight damaged). These ESDs are visualised in 20 Figures, and explained in the following pages. Note that Safety Objectives are determined for each of the events in the ESDs. The overall Target Level of Safety is equal to the sum of the SOs of the end-events "ground collision" of all the different ESDs.

The initiating event of ESD 5 occurs as a result of remote pilots' takeoff commencing while the UAS is not properly configured for takeoff. The following pivotal and end events are represented in Figure 5 respectively. Take-off configuration warning is regarded as a determinative event because of an unsuccessful one causes a ground collision.

The initiating event of ESD 6 occurs as a result of remote pilots' takeoff commencing while aircraft wing, horizontal stabilizer, tail and/or flight control surfaces are contaminated with frost, ice, slush or snow. The following series of events in the scenario are represented in order in Figure 6.

The initiating event of ESD 7 describes the situation where the centre of gravity or weight of UAS differs from the remote pilots' expectations such that remote pilots have to take additional action to maintain control of the aircraft. This ESD only applies to takeoff. Figure 7 shows the subsequent events in the scenario.
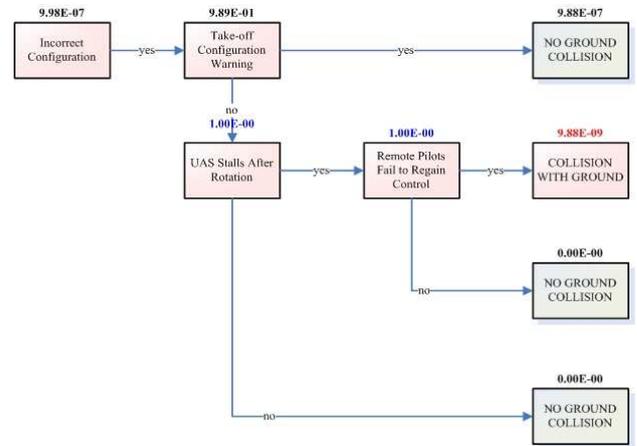
Figure 5 Operation by remote pilot(s) inappropriate
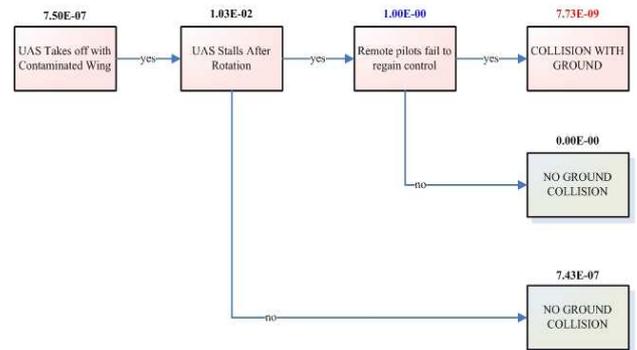
Figure 6 UAS takes off with contaminated wing
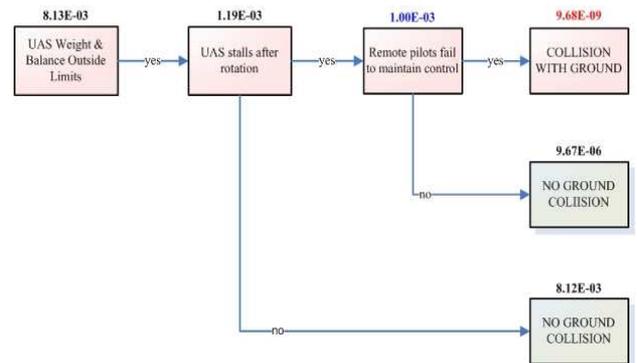
Figure 7 Weight/balance outside limits (takeoff)

Figure 8 describes the situation where the UAS encounters an increase in tailwind or a decrease in headwind after rotation. The occurrence probability of a performance decreasing windshear is determined based on the probability data but occurrence due to wake vortex is excluded.
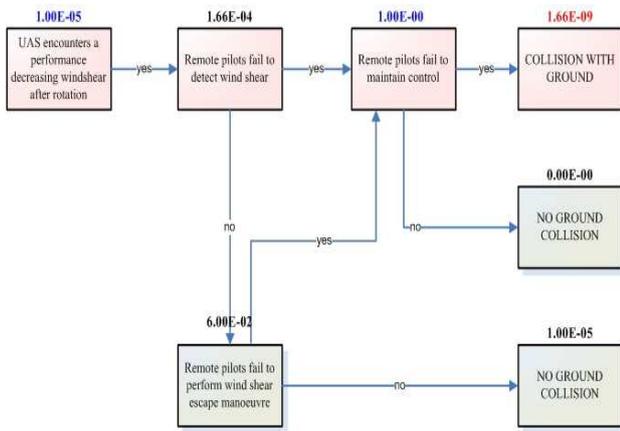
Figure 8 Encountering performance decreasing windshear

The initiating event in ESD 11 describes the situation where a combustible substance onboard the UAS is burning (see Fig. 9). It is assumed that the UAS has fire detection and/or fire warning system which warns remote pilots who are located at the GCS and also a fire extinguishing system installed onboard that can be controlled and activated by GCS.
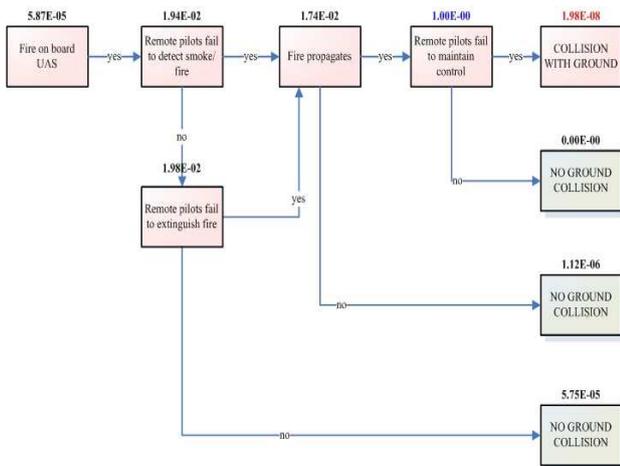
Figure 9 Fire on board UAS

The initiating event of ESD 12 refers to the situation where remote pilots are spatially disoriented owing to unsuccessful attitude guidance and lack of visual orientation following by lack of autopilot control. According to Figure 10 after remote pilots are spatially disoriented, the type of the end event depends on the success of remote pilots to maintain control.

The initiating event of ESD 13 describes the situation where a flight control system failure occurs. Once there is a flight control system failure, type of the end event generally depends on the remote pilots' success to maintain control (see Fig. 11).
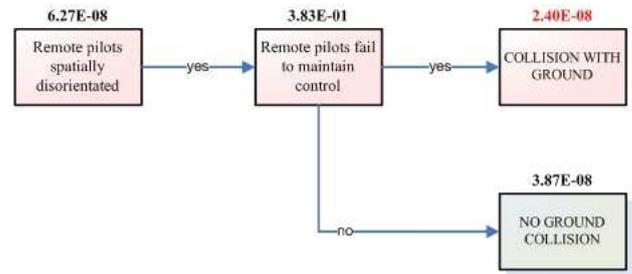
Figure 10 Remote pilots spatially disoriented
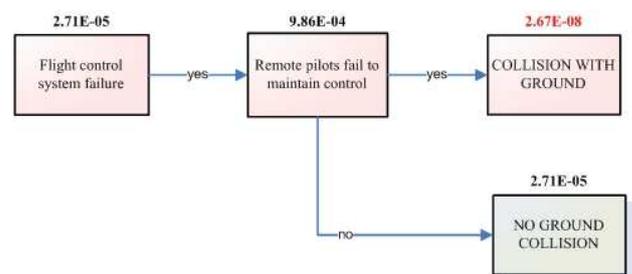
Figure 11 Flight control system failure

The initiating event of ESD 14 describes the situation where any required remote pilot is unable to perform the prescribed flight duties as a result of reduced medical fitness (medical illness or injuries). Once the remote pilots fail to maintain control due to incapacitation, the type of the end event depends on the success or failure of the auto recovery module to maintain control (see Fig. 12).
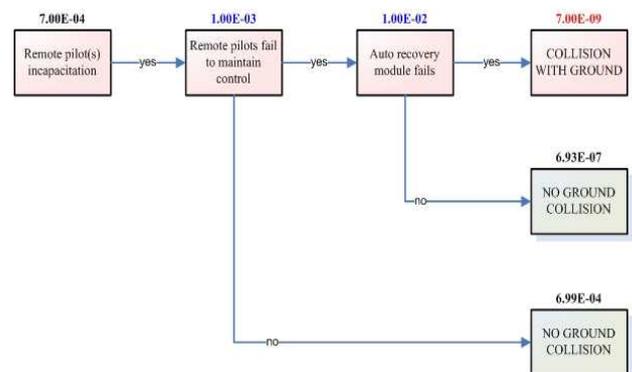
Figure 12 Remote pilot(s) incapacitation

The initiating event of ESD 15 describes the situation where UAS' anti ice system does not operate while it flies in severe icing conditions that might exceed the UAS' certification envelope and cause ice accretion on the outside structure of UAS. Icing of the pitot static system is not covered in this ESD. The following series of events in the scenario are represented in order in Figure 13.
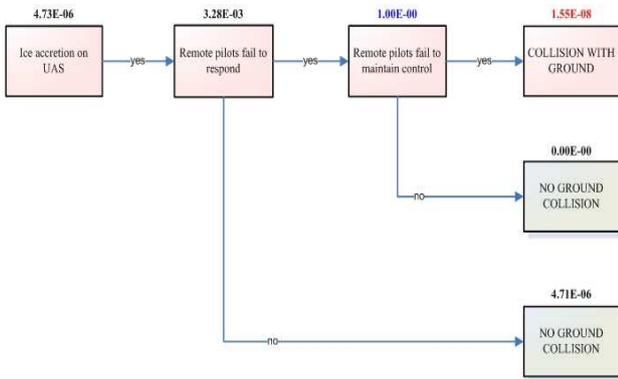
Figure 13 Anti icing system not operating

The initiating event of ESD 16 describes the situation where any flight instrument fails to display flight data, i.e. airspeed, altitude and/or attitude. According to Figure 14, after a flight instrument failure occurs, the type of the end event depends on the success of the remote pilots to maintain control.
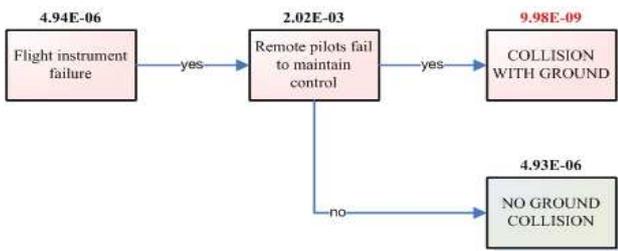
Figure 14 Flight instrument failure

The initiating event in ESD 17 describes the situation where UAS encounters with severe turbulence or unfavourable weather conditions which may result in structure overstress. The following events of the scenario are represented in Figure 15 with their consequences.
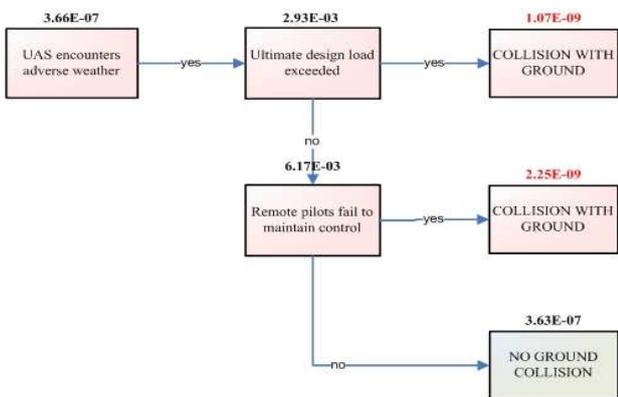
Figure 15 UAS encounters adverse weather

The initiating event in ESD 18 describes the situation of a significant thrust loss from the propulsion system. For the purpose of this ESD, only engine failures during climb, en-route or approach phases are considered and engine detachment cases are included. Engine fires are excluded due to their previous incorporation in ESD 11. Following series of events in the scenario are represented in order in Figure 16.
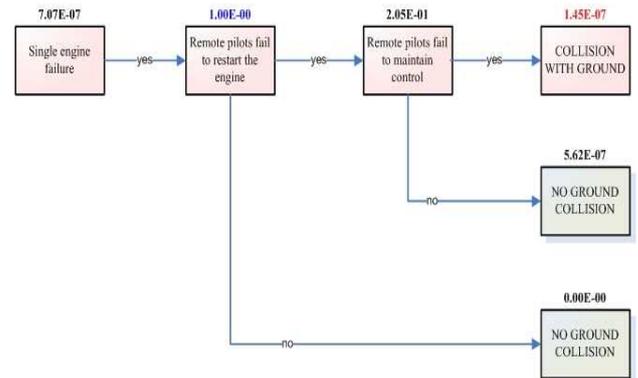
Figure 16 Single engine failure

Figure 17 shows ESD 19. The initiating event in ESD 19 describes the situation where one or more of the flight parameters are set out incorrectly by the remote pilots that result in an unstable approach. Initiation and execution of a missed approach is done to achieve a flight in safe conditions in a safe state.
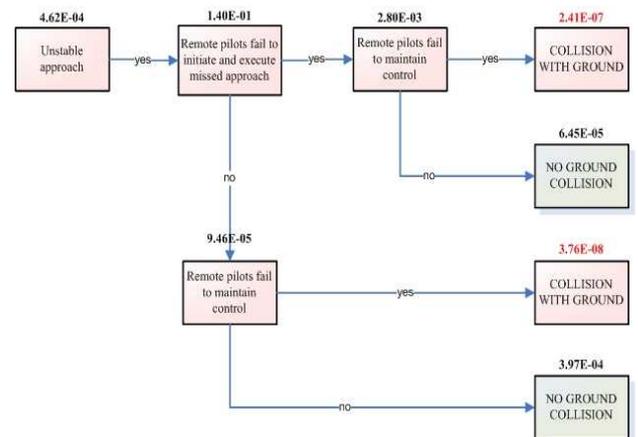
Figure 17 Unstable approach

The initiating event of ESD 21 describes the situation where the centre of gravity or weight of UAS differs from the remote pilots' expectations such that remote pilots have to take additional action to maintain control of the aircraft. This ESD only applies to the approach and landing phase. Figure 18 shows the subsequent events in the scenario.
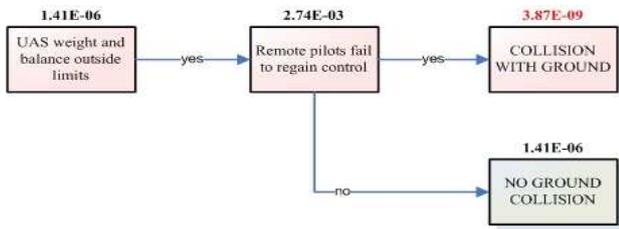
Figure 18 Weight/balance outside limit (approach/landing)

The initiating event of ESD 18 describes the situation where UAS encounters the wake vortex of a preceding aircraft such that noticeable deviations from the UAS' initially intended flight path or attitude occur. Figure 19 shows the following events in the scenario.
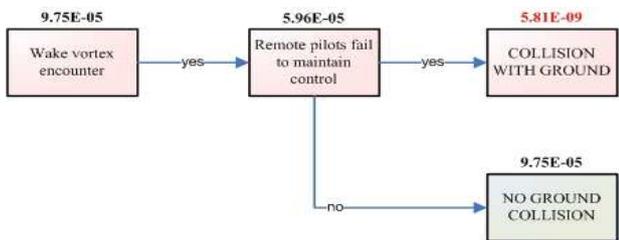
Figure 19 Wake vortex encounter

Figure 20 shows ESD 40. The initiating event describes the situation where the actual location of UAS differs from the location displayed in the GCS due to a failure in the positional information system of UAS. The pivotal event "remote pilots' loss of situational awareness" is defined as the situation where remote pilots' mental picture of UAS' position in the horizontal or vertical plane does not correspond with the actual position.
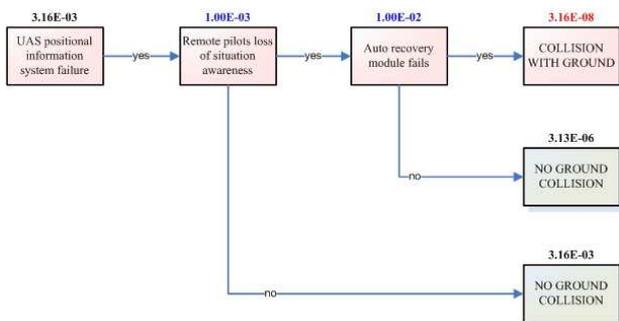
Figure 20 UAS positional information system failure

The initiating event of ESD 41 describes the situation where there is a failure in the Air Data Terminal (ADT) and/or Ground Data Terminal (GDT), which subsequently leads to the loss of data link implying that the remote pilot(s) cannot communicate with the aircraft. Following series of events in the scenario are represented in order in Figure 21.
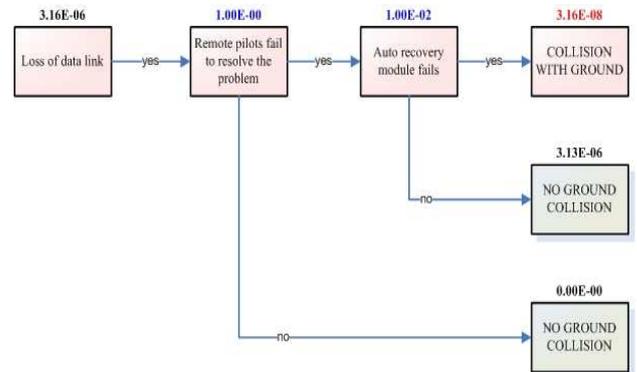
Figure 21 UAS data link failure

The initiating event of ESD 42 describes the situation where GCS encounters severe conditions such as fire and/or weather related disasters, i.e. flood, thunderstorms unexpectedly. Figure 22 represents the following series of events in the scenario.
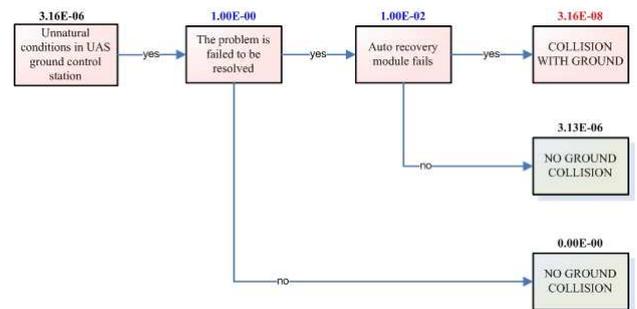
Figure 22 Unnatural conditions in the UAS GCS

The initiating event of ESD 43 represents a mid air collision where the flight trajectory of a UAS intersects with the flight trajectory of a manned aircraft. The pivotal event "parts of the aircrafts fall down" is defined as the situation where UAS manages to continue flight after a mid air collision but the collision causes detachment of some aircraft parts which lead to a ground collision when they fall down (see Fig. 23).

The accident scenario of ESD 44 is represented in Figure 24 and it only deals with the situation where a part of UAS falls down while it is flying due to maintenance and/or design failure, maneuver outside the flight envelope, severe turbulence conditions or cargo fall.
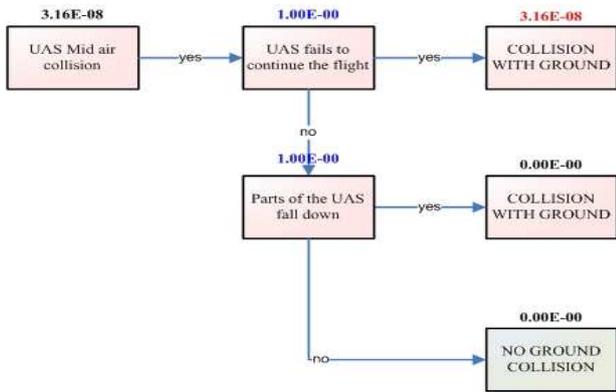
Figure 23 UAS mid air collision
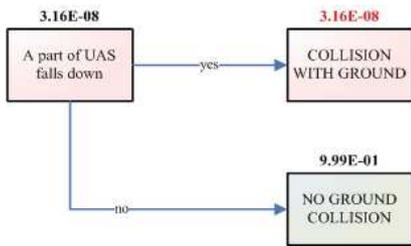
Figure 24 A part of the UAS falls down

SAFETY OBJECTIVES

The SO calculations are initiated with the presence of a TLS. Calculations are carried out from the right side of each ESD to the left side (starting from the end events). A SO is obtained for all of the initiating and pivotal events that might lead to a ground collision, using the assumption that the future UAS operation will have to be at least as safe as commercial air transport in the current manned aviation system. The Safety Objectives, which are represented by the initiating and pivotal events of the ESDs, are determined and summarized in Table 2. Since some events are repeated several times with different SOs in different ESDs (i.e. remote pilots fail to maintain control) their most stringent SO values are listed only.

Table 2 List of the UAS safety objectives

NAME	SO
Incorrect configuration (per takeoff)	9×10^{-7}
Take Off Configuration Warning (TOCW) (per takeoff with incorrect configuration)	9×10^{-1}
UAS stalls after rotation (per takeoff continuation with TOCW failure)	1×10^{0}
Remote pilot(s) fail to regain control (per stall after takeoff continuation with TOCW failure)	1×10^{0}
UAS takes off with contaminated wing (per takeoff)	7×10^{-7}

UAS stalls after rotation (per takeoff with ice on wings)	1×10^{-2}
Remote pilot(s) fail to regain control (per takeoff with ice on wings)	1×10^{0}
UAS weight and balance outside limits (per takeoff)	1×10^{-6}
UAS stalls after rotation (per takeoff outside the limits)	1×10^{-3}
Remote pilot(s) fail to maintain control (per stall after takeoff outside limits)	1×10^{-3}
UAS encounters a performance decreasing windshear after rotation (per takeoff)	1×10^{-5}
Remote pilot(s) fail to detect wind shear (per takeoff with windshear encounter)	1×10^{-4}
Remote pilot(s) fail to perform windshear escape maneuver (per windshear detection)	6×10^{-2}
Remote pilot(s) fail to maintain control (per windshear detection &/ avoidance failure)	1×10^{0}
Fire on board UAS (per flight)	5×10^{-5}
Remote pilot(s) fail to detect smoke/fire (per fire onboard)	1×10^{-2}
Remote pilot(s) fail to extinguish fire (per fire onboard)	1×10^{-2}
Fire propagates (per developed fire onboard)	1×10^{-2}
Remote pilot(s) fail to maintain control (per propagated fire on board)	1×10^{0}
Remote pilot spatially disoriented (per flight)	6×10^{-8}
Remote pilot(s) fail to maintain control (per spatial disorientation)	3×10^{-1}
Flight control system failure (per flight)	2×10^{-5}
Remote pilot(s) fail to maintain control (per system control failure)	9×10^{-4}
Remote pilot(s) incapacitation (per flight)	7×10^{-4}
Remote pilot(s) fail to maintain control (per incapacitation)	1×10^{-3}
Auto recovery module fails (per flight)	1×10^{-2}
Ice accretion on UAS (per flight)	4×10^{-6}
Remote pilot(s) fail to respond (per ice accretion)	3×10^{-3}
Flight instrument failure (per flight)	4×10^{-6}
Remote pilot(s) fail to maintain control (per instrument failure)	2×10^{-3}
UAS encounters adverse weather (per flight)	3×10^{-7}
Ultimate design load exceeded (per adverse weather conditions)	2×10^{-3}
Remote pilot(s) fail to maintain control (per adverse weather conditions)	6×10^{-3}
Single engine failure (per flight)	7×10^{-7}
Remote pilot(s) fail to restart the engine (per single engine failure)	1×10^{0}
Remote pilot(s) fail to maintain control (per total power loss)	2×10^{-1}
Unstable approach (per landing)	4×10^{-4}
Remote pilot(s) fail to initiate and execute missed approach (per unstable approach)	1×10^{-1}

Remote pilot(s) fail to maintain control (per failure to execute missed approach)	2×10^{-3}
Remote pilot(s) fail to maintain control (per missed approach)	9×10^{-5}
UAS weight and balance outside limits (per approach)	1×10^{-6}
Remote pilot(s) fail to regain control (per approach with weight and balance problem)	2×10^{-3}
Wake vortex encounter (per flight)	9×10^{-5}
Remote pilot(s) fail to maintain control (per wake encounter)	5×10^{-5}
Positional information system failure (per flight)	3×10^{-3}
Remote pilot(s) loss of situational awareness (per flight)	1×10^{-3}
Loss of data link (per flight)	3×10^{-6}
Remote pilot(s) fail to resolve the problem (per flight)	1×10^{0}
Unnatural conditions in the GCS (per flight)	3×10^{-6}
The problem is failed to be resolved (per flight)	1×10^{0}
UAS Mid air collision (per flight)	3×10^{-8}
UAS fails to continue flight (per flight)	1×10^{0}
Parts of the UAS falls down (per flight)	1×10^{0}
A part of UAS falls down (per flight)	3×10^{-8}

SAFETY REQUIREMENTS

Safety requirements are determined via the utilization of fault trees that are generated under the initiating and pivotal events. A fault tree structure has one top gate at the top and several root causes at the bottom. The top gate of a fault tree is either the pivotal event or the initiating event of an ESD. The root causes are usually human related, system related or task related. In the scope of this research, the failure frequency of a root cause in a fault tree represents the safety requirement which is defined as the maximum allowable failure frequency that a specific system, task or human act needs to have. Human related safety requirements usually pertain to erroneous operator acts or the remote pilot incapability and restrict them to a certain failure rate per certain flight hours. Human related safety requirements are usually less stringent than system related safety requirements. The latter are usually related to system incapacities, failures or system shutdowns. Task related safety requirements mostly relate to erroneous, unperformed or insufficient task-based acts, which may include the contribution of an operator and/or a system.

Determination of the SRs can be considered beneficial for manufacturers and rule making authorities. SRs are "serving tools" for the manufacturers since they represent the maximum allowable failure frequency that a specific system needs to have. A relatively high value of SRs stands for a less restrictive safety standard and a small value of SRs stands for a relatively more restrictive safety standard. Under the

circumstances where there is lack of regulations, SRs establishment would also provide insight to the rule making authorities via demonstrating which kind of tasks and/or systems have a high failure frequency under the predefined conditions. Lastly, SRs may determine the kind and level of training that a UAS remote pilot needs to receive.

An example of how to interfere Safety Requirements for root causes is provided in Figure 25 and Table 3 below. The example reflects the root causes for pivotal event 'UAS weight and balance outside limits (take off)'. It is outside scope of this paper to include all FTs (note that reference 12 does provide the full details on the derivation of about 140 SRs).
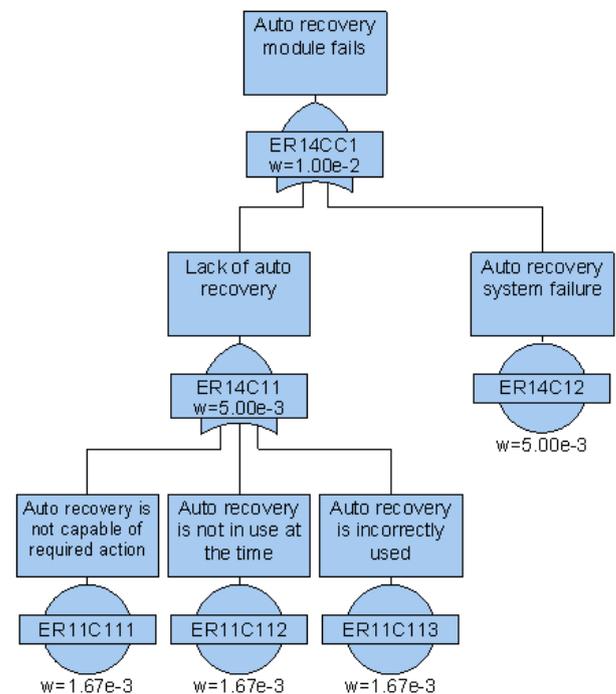
Figure 25 Example fault tree "auto recovery module fails"

Table 3 Example Safety Requirements for root causes

Root causes	SRs
Auto recovery is not capable of required action (per flight)	1.67×10^{-3}
Auto recovery is not in use at the time (per flight)	1.67×10^{-3}
Auto recovery is incorrectly used (per flight)	1.67×10^{-3}
Auto recovery system failure (per flight)	5.00×10^{-3}

RISK MITIGATION MEASURES

Some of the Safety Objectives derived in this research are relatively stringent. It is therefore relevant to identify some mitigation measures that could help to reduce or cope with the root causes of UAS hazards and risks. Utilization of control system redundancy management can mitigate the risk of flight control system failures, and make it easier to demonstrate that the associated SOs will be met. Additionally, utilization of caution and warning indicators may help to eliminate certain hazards or identify risks in an early stage. An example of the utilization of caution and warning indicators has already been used in the ESD 'Fire onboard UAS' by assuming presence of fire detection, warning and extinguishing systems onboard. Another important risk mitigation measure could be setting of waypoints which can help prevent or delay potential remote pilots' spatial disorientation problems [13] and/or their loss of situational awareness during the flight. Other risk mitigation measures could be route changes, safe location of GCS and multiple flight planning. Route changes would help prevent the unfavorable operational weather conditions such as lightening, rain, wind speed aloft and turbulence level. Locating the GCS at a safe place i.e. a location where the earthquake frequency and severity is low enough, could help to cope with the effects of unexpected conditions and/or natural disasters happening at the location of GCS. Multiple flight planning could be another risk mitigation measurement which would affect the ESDs 'Unstable Approach', 'UAS Engine Failure', and 'Remote Pilots Spatially Disoriented'. Evaluation of the impact of the above risk mitigations on the risk of a ground collision would be a topic for further study.

SUMMARY/CONCLUSIONS

Although UAS are mainly used in segregated airspace, the integration of UAS in non-segregated airspace is coming closer. To better understand the differences between manned and unmanned aircraft, UAS performance characteristics are examined. This helps to clarify in which airspace classes the different available UAS may be able to fly. This concerns the broad range of size, various configurations and different performance characteristics (maximum takeoff weight, maximum flight altitude, endurance and maximum speed).

A safety risk analysis methodology for the risk of collision of an Unmanned Aircraft System with the ground has been developed. Causal models are developed for each accident scenario that may result in a collision with the ground. These causal models provide a logical structure, showing how hazards and causal factors could combine to cause a collision with the ground. This approach utilizes the CATS developed for the Dutch Ministry of Transport [1]. The method has been applied to derive Safety Objectives for hazardous events that may lead to a collision with the ground, under the assumption that the level of safety should be equivalent to that of current commercial air traffic operations. The method has been applied to derive Safety Objectives for hazardous events related to commercial UAS operations, performed with a UAS that is equivalent with manned aircraft in category CS-25. The Safety Objectives may be apportioned further (in a subsequent study) into Safety Requirements for each of the root causes, failures and causal factors underlying an accident scenario. The method provides insight into the probability of a UAS collision with the ground in relation with safety objectives.

The developed methodology supports regulators with the setting of UAS safety objectives and safety requirements. It may also be used by applicants (UAS operators and manufacturers) for identification of UAS related hazards, causal factors, and accident scenarios. This paper illustrates the method for commercial UAS operations performed with UAS that are to a large extent equivalent with manned aircraft in category CS-25. For other UAS types, it will be necessary to investigate if the ESDs developed in this paper still apply or whether further adaptations are required. It also remains to be investigated if the fact that a UAS does not carry passengers could allow for a less stringent TLS than for manned aviation.

In third party risk analyses, usually *Societal risk* (to a group) and *Individual risk* (to individuals at a location) are evaluated. It is recommended to extend the method with an accident location model and an accident consequence model, in order to assess UAS third party risk in terms of these risk metrics.

REFERENCES

1. B. Ale, L.J. Bellamy, R.M. Cooke, M. Duyvis, D. Kurowicka, P.H. Lin, O. Morales, A. Roelen, J. Spouge; Causal model for air transport safety - Final Report, 2009.
2. Kuchar, J., Safety Analysis Methodology for Unmanned Aerial Vehicle (UAV) Collision Avoidance Systems, 6th USA / Europe Seminar on Air Traffic Management Research and Development, Baltimore, MD, 2005.
3. Clothier, R, Walker, R, Fulton, N, Campbell, D. A Casualty Risk Analysis For Unmanned Aerial System (UAS) Operations Over Inhabited Areas, AIAC12 – Twelfth Australian International Aerospace Congress,2nd Australasian Unmanned Air Vehicles Conference, 19 – 22 March 2007.
4. Luxhøj, J. Safety Risk Analysis of Unmanned Aircraft Systems (UAS) Integration into the National Airspace System (NAS): Phase 1 Final Report, Department of Transportation. Federal Aviation Administration, 2008.
5. Oztekin, A, and Luxhøj, J. Hazard, Safety, Risk and Uncertainity Modeling of the Integration of Unmanned Aircraft Systems into the National Airspace, 26th International Congress of the Aeronautical Sciences (ICAS) 2008.
6. Clothier, R, and Walker, R. Determination and evaluation of UAV safety objectives, Proceedings of 21st International Unmanned Air Vehicle Conference, Bristol, United Kingdom, pp. 18.1-18.16., 2006.

7. ICAO; Unmanned Aircraft Systems (UAS), Circular 328-AN/190, ISBN 978-92-9231-751-5.
8. UVS International; Unmanned Aircraft Systems Yearbook, 8th Edition, 2010/2011
9. FAA Airspace Classifications, Chapter 8, the National Airspace System.
10. EUROCONTROL; Safety Assessment Methodology, Version 2.1, November 2006.
11. UAV Task-Force Final Report, A Concept For European Regulations For Civil Unmanned Aerial Vehicles (UAVs), The Joint JAA/EUROCONTROL Initiative on UAVs, 11 May 2004.
12. A.D. Ozuncer; Development of a Safety Assessment Methodology for the Risk of Collision of a Unmanned Aircraft System with the Ground, MSc thesis, 2011.
13. Benson, A.J.; Spatial disorientation – a perspective, in RTO HFM Symposium on Spatial Disorientation in Military Vehicles: Causes, Consequences and Cures, La Coruna, Spain, 15-17 April 2002, RTO-MP-086.
14. R.E. Weibel, R.J. Hansman; Safety considerations for operation of Unmanned Aerial Vehicles in the National Airspace System, Report No. ICAT-2005-1, March 2005.
15. EUROCONTROL; Unmanned Aircraft Systems - ATM Collision Avoidance Requirements (Phase 1), Edition 1.2, 14 December 2009, CND/CoE/CNS/09-156.
16. EUROCONTROL; Specifications for the Use of military Unmanned Aerial Vehicles as Operational Air Traffic outside segregated Airspace, 2007.
17. H. de Jong (DFS), R. Priego Lopez (ISDEFE), Scope of risks and safety criteria, INOUI D5.0b, 27 March 2009.
18. D. Durrett, H. de Jong (DFS), J. Tattersall (Rheinmetall); Functional Hazard Analysis, INOUI D5.2, 29 June 2009.
19. L.J.P. Speijker, X. Lee, R. van de Leijgraaf; Framework for Unmanned Aircraft Systems Safety Risk Management, NLR-TP-2011-324, August 2011.

CONTACT INFORMATION

The author may be contacted at aysedenizozuncer@gmail.com and/or Valckenierstraat 39, 1018 XE Amsterdam, Netherlands. The co-authors may be contacted as follows:

L.J.P. (Lennaert) Speijker, NLR, Anthony Fokkerweg 2, 1059 CM, Amsterdam, Netherlands, speijker@nlr-atsi.nl

J.A.A.M. (John) Stoop, TU Delft, Kluyverweg 1, 2629 HS Delft, Netherlands, J.A.A.M.Stoop@tudelft.nl

R. (Ricky) Curran, TU Delft, Kluyverweg 1, 2629 HS Delft, Netherlands, R.Curran@tudelft.nl

ACKNOWLEDGMENTS

ABBREVIATIONS

ADT	Air Data Terminal
ATC	Air Traffic Control
ATM	Air Traffic Management
CATS	Causal model for Air Transport Safety
CR	Close Range
CS	Certification Specifications
DEC	Decoy
ESD	Event Sequence Diagram
EXO	Exo-stratospheric
FTA	Fault Tree Analysis
GCS	Ground control station
GDT	Ground Data Terminal
HALE	High altitude long endurance
ICAO	International Civil Aviation Organization
IFR	Instrument Flight Rules
LADP	Low altitude deep penetration
LALE	Low altitude long endurance
LETH	Lethal
MALE	Medium altitude long endurance
MR	Medium range
MRE	Medium range endurance
MTOW	Maximum take-off weight
SO	Safety Objective
SPACE	Space
SR	Short range
SRs	Safety requirements
STRATO	Stratospheric
TLS	Target level of safety
TOCW	Take Off Configuration Warning
UAS	Unmanned aircraft systems
UCAV	Unmanned combat aerial vehicle