Dedicated to innovation in aerospace
safetyinstitute

NLR-TP-2017-114 | March 2017

A safety impact quantification approach for early stage innovative aviation concepts

Application to a third pilot adaptive automation concept

CUSTOMER: Netherlands Aerospace Centre

NLR – Netherlands Aerospace Centre

Netherlands Aerospace Centre

NLR is a leading international research centre for aerospace. Bolstered by its multidisciplinary expertise and unrivalled research facilities, NLR provides innovative and integral solutions for the complex challenges in the aerospace sector.

NLR's activities span the full spectrum of Research Development Test & Evaluation (RDT & E). Given NLR's specialist knowledge and facilities, companies turn to NLR for validation, verification, qualification, simulation and evaluation. NLR thereby bridges the gap between research and practical applications, while working for both government and industry at home and abroad.

NLR stands for practical and innovative solutions, technical expertise and a long-term design vision. This allows NLR's cutting edge technology to find its way into successful aerospace programs of OEMs, including Airbus, Embraer and Pilatus. NLR contributes to (military) programs, such as ESA's IXV re-entry vehicle, the F-35, the Apache helicopter, and European programs, including SESAR and Clean Sky 2.

Founded in 1919, and employing some 650 people, NLR achieved a turnover of 73 million euros in 2014, of which three-quarters derived from contract research, and the remaining from government funds.

For more information visit: **www.nlr.nl**

EXECUTIVE SUMMARY

UNCLASSIFIED

A safety impact quantification approach for early stage innovative aviation concepts

Application to a third pilot adaptive automation concept

Problem area

In Europe's vision for aviation in 2050, the safety goal is to reduce the accident rate to less than one accident per ten million commercial aircraft flights. It is envisioned that the occurrence and impact of human error will be significantly reduced through new designs, training processes, and advanced decision support systems. Worldwide, considerable research and development is being undertaken towards improving aviation safety, including the SESAR and NextGen programs. To ensure efficient decision-making in such R&D programs, there is a need for methods which can provide feedback on the potential safety advantages of innovative aviation concepts at early stages of their development.

Description of work

This paper presents a straightforward approach for safety impact quantification of innovative aviation concepts in early development stages. The safety impact quantification approach provides a high-level and broad overview of the accident risk reduction that may be obtained by the novel concept. The approach uses a systematic assessment of change factors for base event probabilities in a total aviation system risk model, consisting of combinations of event sequence diagrams and fault trees.

Results and conclusions

The approach is illustrated in terms of the assessment of an innovative third pilot adaptive automation concept. The results indicate that this concept can effectively reduce the fatal accident risk.

Applicability

The approach supports safety impact quantification of innovative aviation concepts in early development stages.

REPORT NUMBER
NLR-TP-2017-114

AUTHOR(S)
S.H. Stroeve
J. Cahill
B.A. van Doorn

REPORT CLASSIFICATION
UNCLASSIFIED

DATE
March 2017

KNOWLEDGE AREA(S)
Safety

DESCRIPTOR(S)
accident risk
adaptive automation
safety

GENERAL NOTE

This report is based on a paper presented at the 6th SESAR Innovation Days, Delft, The Netherlands, November 8-10, 2016.

NLR
Anthony Fokkerweg 2
1059 CM Amsterdam
p) +31 88 511 3113 f) +31 88 511 3210
e) info@nlr.nl i) www.nlr.nl

Dedicated to innovation in aerospace
safetyinstitute

NLR-TP-2017-114 | March 2017

A safety impact quantification approach for early stage innovative aviation concepts

Application to a third pilot adaptive automation concepts

CUSTOMER: Netherlands Aerospace Centre

AUTHOR(S):

S.H. Stroeve	NLR
J. Cahill	Trinity College Dublin
B.A. van Doorn	NLR

NLR - Netherlands Aerospace Centre

This report is based on a paper presented at the 6th SESAR Innovation Days, Delft, The Netherlands, November 8-10, 2016.

The contents of this report may be cited on condition that full credit is given to NLR and the author(s).

CUSTOMER	**Netherlands Aerospace Centre**
OWNER	**NLR + partner(s)**
DIVISION NLR	**Aerospace Operations**
DISTRIBUTION	**Unlimited**
CLASSIFICATION OF TITLE	**UNCLASSIFIED**

APPROVED BY :		
AUTHOR	**REVIEWER**	**MANAGING DEPARTMENT**
S.H. Stroeve	External, anonymous reviewers for SESAR Innovation Days	A.D.J. Rutten
DATE 2 0 0 3 1 7	DATE 2 0 0 3 1 7	DATE 2 0 0 3 1 7

Summary

This paper presents a straightforward approach for safety impact quantification of innovative aviation concepts in early development stages. The safety impact quantification approach provides a high-level and broad overview of the accident risk reduction that may be obtained by the novel concept. The approach uses a systematic assessment of change factors for base event probabilities in a total aviation system risk model, consisting of combinations of event sequence diagrams and fault trees. The approach is illustrated in terms of the assessment of an innovative third pilot adaptive automation concept. The results indicate that this concept can effectively reduce the fatal accident risk.

Table of Contents

1 Introduction

In Europe’s vision for aviation in 2050 [1], the safety goal is to reduce the accident rate to less than one accident per ten million commercial aircraft flights. It is envisioned that the occurrence and impact of human error will be significantly reduced through new designs, training processes, and advanced decision support systems, e.g. for smart assistance of pilots and controllers. Worldwide, considerable research and development is being undertaken towards improving aviation safety, including the SESAR and NextGen programs.

To ensure efficient decision-making in such R&D programs, there is a need for methods which can provide effective feedback on the potential safety advantages that may be obtained by innovative aviation concepts at early stages of their development. The objective of this paper is to present a straightforward approach for obtaining such quantitative safety impact information of early stage aviation concepts and to illustrate this approach for an innovative aviation concept. Key elements of the approach are a total aviation system risk model [2] and systematic evaluation of changes in risk by stakeholder evaluation in a Community of Practice (COP) [3].

Section 2 describes the safety impact quantification approach for novel aviation concepts. Section 3 describes the innovative concept for improving aviation safety – namely, a third pilot adaptive automation concept. Section 4 presents the results of the safety impact quantification for the third pilot adaptive automation concept. Section 5 discusses the approach and the attained results.

2 Safety impact quantification approach

2.1 Total aviation system risk model

As a basis for the safety impact quantification approach a total aviation system risk model is used, which was developed in the CATS (Causal model for Air Transport Safety) and ASCOS (Aviation Safety and Certification of new Operations and Systems) projects [2, 4]. This total aviation system risk model represents 29 scenarios, which may lead to five types of aviation accidents, namely runway excursions, mid-air collisions, ground collisions, controlled flight into terrain, and loss of control in flight. The scenarios cover all types of accidents that have occurred in commercial air transport, with the exception of security related accidents (e.g. hijacks, terrorism and pilot suicide).

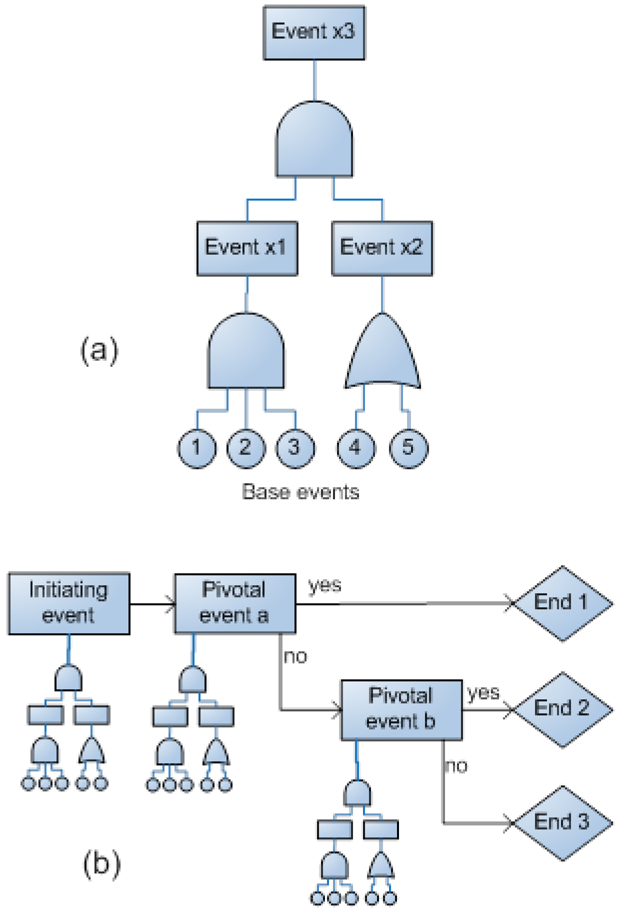

Figure 1: Generic representations of a fault tree (part a) and an event sequence diagram plus fault trees (part b).

Each scenario is structured by a combination of an event sequence diagram and one or more fault trees (Figure 1). An event sequence diagram describes potential sequences of events, starting from an initiating event, via a range of pivotal events, up to a number of end states. The horizontal and vertical arrows leaving a pivotal event represent affirmative and negative answers to its statement, respectively. Reasons for affirmative answers of the pivotal event statements and reasons for initiating events are represented by fault trees. A fault tree uses Boolean logic to combine events that lead to an affirmative answer of the pivotal event statement. The roots or starting points in a fault tree are called base events, the other are intermediate events.

The total aviation system risk model contains 425 base events and 51 end states. The particular structure of an event sequence diagram and its connected fault trees depends on the scenario considered. As an example, base events initiating the scenario “unstable approach” include “loss of visual”, “crosswind exceeded”, and “poor manual flight control causes unstable approach”. Pivotal events in this unstable approach scenario include “flight crew does not initiate missed approach”, “flight crew does not maintain control”, and “insufficient fuel for next approach”. Base events contributing to these pivotal events include “flight crew does not recognise unstable approach”, “AOA protection prevents missed approach”, “incorrect control”, and “aircraft executes multiple missed approaches”. End states of this scenario include “collision with ground”, “runway overrun”, and “aircraft enters new approach”.

In probabilistic risk assessment, probabilities are associated with the events in the fault trees and event sequence diagrams. As the probabilities of the intermediate events, initiating events, pivotal events, and end states are completely determined by the base event probabilities, such quantification ultimately comes down to setting values for the base event probabilities. For the ASCOS-CATS total aviation system risk model such parameter quantification was achieved by a combination of accident data and expert judgement. The model drew upon data from European commercial aviation accidents. Specifically, accidents occurring between 1995 to 2011 and involving fixed wing aircraft of more than 5701 kg maximum takeoff weight. These correspond with 502 accidents which occurred during 109 million flights.

The main outputs of the total aviation system risk model are frequencies of accidents and fatal accidents. Aviation accidents are occurrences in aircraft operations leading to fatal or serious injuries, to damage requiring major repair or replacement, or to missing or inaccessible aircraft [5]. Fatal accidents are accidents which resulted in one or multiple fatalities (within 30 days of the date of the accident). In this study, fatal accident frequencies were determined by using scenario-specific fatality factors of CATS.

2.2 Scoping

A scoping of the safety impact assessment is needed to focus on the appropriate types of accidents and to restrict the number of scenarios and base events that are studied in detail. It includes three steps: 1) choice of accident type and fatality level, 2) selection of risk-relevant scenarios or base events, and 3) identification of concept impressionable base events. A description of these steps is presented next and they are illustrated by the application in Section 4.

Choice of accident types and fatality level

The choice of accident type refers to the five types of aviation accidents (runway excursions, mid-air collisions, ground collisions, controlled flight into terrain, and loss of control in flight). It is determined which accident types are relevant for the novel concept.

The choice of the accident fatality level refers to the choice to consider accidents in general, or only fatal accidents in particular. This is an important distinction, since the overall frequency of accidents is two orders of magnitude higher than the overall frequency of fatal accidents, and there are differences up to four orders of magnitude for particular scenarios. The overall accident frequency is dominated by scenarios, such as “Cracks in aircraft pressure cabin”, “Fire, smoke, fumes on-board aircraft”, and “Conflict on taxiway or apron”, but these scenarios rarely lead to fatalities.

Selection of risk-relevant scenarios or base events

The total aviation system risk model consists of 29 scenarios and 425 base events. For efficiency, the scenarios and base events that are assessed in detail, need to be restricted. Such restriction can be achieved at the level of scenarios and/or at the level of individual base events. At the scenarios level, only those scenarios can be chosen which contribute to the overall (fatal) accident risk in current operations for a particular minimum extent. At the level of individual base events, the elasticities of changes in (fatal) accident risk due to changes in base event probabilities can be determined, and only base events with a risk elasticity above a certain threshold are maintained in the safety impact assessment.

Identification of concept impressionable base events

Following the selection of risk-relevant scenarios or individual base events in the previous scoping step, there typically is a range of base events for which it is manifest that they are not influenced in any way by the novel concept. As a structured way to exclude these base events, a number of base event exclusion assumptions are adopted. The remaining base events are indicated as concept impressionable, as they can in principle be influenced by the novel concept.

2.3 Assessment of change in accident risk

The assessment of change in (fatal) accident risk due to a novel concept is done in two consecutive steps: 1) assessment of change in base event probabilities, and 2) risk impact quantification.

Assessment of change in base event probabilities

The change in base event probabilities due to the novel concept is calculated using change factors. Denoting the probability of a base event i in current operations as $p_{i,C}^{b}$ and the probability of a base event in operations under the novel concept as $p_{i,N}^{b}$, a multiplicative change factor is $c_i^b = p_{i,N}^{b} / p_{i,C}^{b}$.

In support of the risk change assessment a range of values and associated terminology are defined for c_i^b in Table 1, based on earlier work on bias and uncertainty assessment in risk quantification of [6]. For example, if it is assessed that the probability of a base event has a “Small Increase” due to the novel concept, it means that its value is increased by a multiplicative factor 1.2; if the novel concept leads to a “Considerable Decrease” of the probability of a base event, its value is decreased by a factor 5.

Table 1: Definition of the change in the probability of a base event, using terminology and values of [6].

Qualitative term	**Value of change factor c_i^b**	
	Increase	**Decrease**
Neutral	1.0	1.0
Negligible	1.1	1/1.1 (0.91)
Small	1.2	1/1.2 (0.83)
Minor	1.5	1/1.5 (0.67)
Significant	2.25	1/2.25 (0.44)
Considerable	5	1/5 (0.20)
Major	10	1/10 (0.10)

The probability change factors c_i^b of all impressionable base events are determined in the safety assessment on the basis of information gathered in multiple workshops with members of the Community of Practice (COP) of the R&D program for the innovative concept. The COP refers to a broad group of stakeholders, who are involved in the development and evaluation of an innovative concept. For aviation, such a COP can involve a broad variety of stakeholders, such as multi-disciplinary researchers, technicians, pilots, air traffic controllers, and other representatives of aviation organisations. In the workshops the participants argue about the kinds of mechanisms facilitated by the innovative concept which may increase or decrease the probability of a particular base event in a scenario. On the basis of these argumentation they next express their opinion about the change factor of Table 1 which represents best the overall effect of these mechanisms. The safety assessment team uses all arguments and change factors derived in the COP workshops to assess an overall value of the probability change factor for each impressionable base event.

Risk impact quantification

The risk impact is evaluated at the level of individual scenarios and for the total risk. To determine the risk impact at the level of individual scenarios, the (fatal) accident probability is determined by the total aviation system risk model, using the new probabilities of all impressionable base events $p_{i,N}^b = c_i^b \cdot p_{i,C}^b$, and unchanged probabilities for all other base events. The overall (fatal) accident probability is determined by summation of the contributions of all scenarios. These include the scenarios that are assessed to be impacted by the novel concept, the scenarios that are assessed to be not impacted by the novel concept, and the low risk contributing scenarios for which changes were not assessed.

Optionally and additionally, the risk impact can be evaluated at the level of individual base events by combining the risk elasticity and change factor of a base event. Due to restrictions this option is not detailed in this paper.

3 Third pilot adaptive automation concept

To support flight safety and efficiency, a third pilot adaptive automation concept has been developed in the European FP7 project A-PiMod (Applying Pilot Models for Safer Aircraft). Its objective is to support adaptive distribution of tasks between the crew and automation, based on real-time analysis of the crew's cognitive state and behaviour, and on the risk associated with the mission.

As an argumentation basis, the execution of a flight is conceptualized at the following three levels [7]:

1. *Mission level.* The mission level is the highest level, which describes tasks to achieve a successful mission for flying from origin to destination, such as taxiing, takeoff, climb, en-route, approach, and landing, including specific route points. The flight plan describes these mission level tasks and it may be adapted during flight to cope with changing or unexpected circumstances.
2. *Cockpit level.* The cockpit level describes the tasks of the cooperative human and machine agents in the cockpit to achieve the mission level tasks. The cockpit level tasks include (1) mission monitoring and adaptation, (2) mission execution tasks for aviation, navigation, and communication, and (3) distribution of tasks between humans and automation.
3. *Agent level.* At the agent level the cockpit level tasks are executed by combinations of cockpit agents, including the pilot flying, pilot monitoring, and specific technical (automation) systems.

Building upon these flight execution levels, the architecture of the third pilot adaptive automation concept developed in the A-PiMod project (Figure 2) consists of the following eight joint human-software components:

1) The *Situation Determination at Mission Level* component determines the current state of the mission and provides the context in which it is executed.
2) The *Risk Assessment at Mission Level* component determines the risk of not being able to achieve the mission as intended.
3) The *Situation Modification at Mission Level* component modifies the mission to reduce the associated risk to an acceptable level.
4) The *Task Determination at Cockpit Level* component determines the tasks that the cockpit as a whole has to do in a given situation.
5) The *Situation Determination at Cockpit Level* assesses the state of the cockpit, addressing the availability and current capabilities of the two pilots and automation.
6) The *Task Distribution at Cockpit Level* produces possible distributions of tasks between the pilots and automation, and in coordination with the risk assessment at cockpit level component it proposes the best task distribution.
7) The *Risk Assessment at Cockpit Level* component assesses the risk of appropriate task completion for the possible task distributions, based on the crew state and automation functioning.
8) The *Crew State Inference* component monitors the crew in order to infer their intentions, situation awareness, and task-load.

In addition, the architecture includes the following two software modules for the human-automation interaction.

a) The *Human-Machine Multi-Modal Interface (HMMI)* facilitates the interaction between the pilots and the flight deck. It uses traditional input modalities as well as speech, gesture, touch and eye movements. Outputs are via dedicated displays for the mission and cockpit levels.

b) The *HMMI Interaction Manager* is the interface between the user and the adaptive automation technologies. It uses escalation strategies (i.e. notifications) if it detects via the crew state inference, that particular information is not perceived by the pilots.

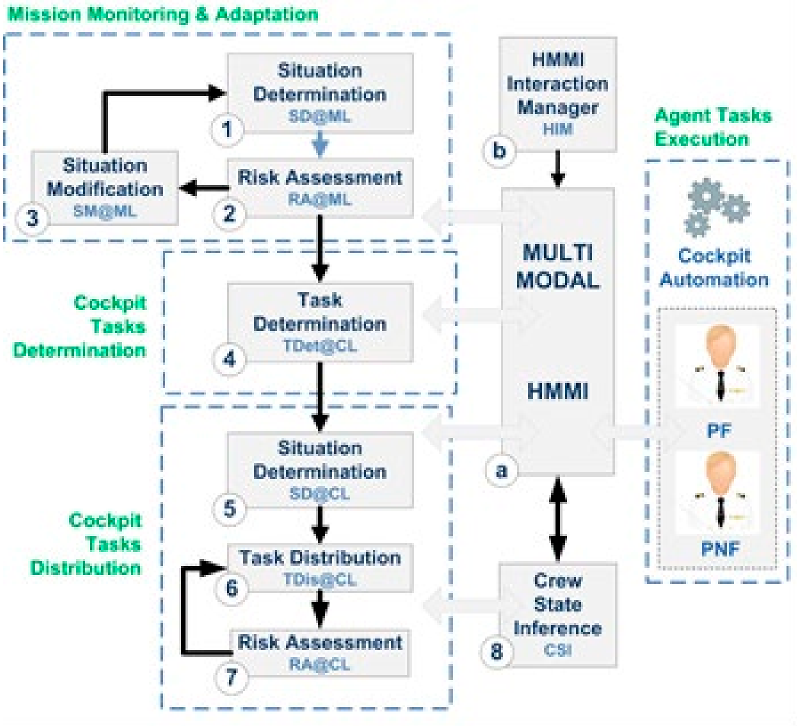
Mission Monitoring & Adaptation
Situation Determination SD@ML
1
Situation Modification SM@ML
3
Risk Assessment RA@ML
2
HMMI Interaction Manager HIM
b
Agent Tasks Execution
Cockpit Automation
MULTI MODAL
HMMI
Cockpit Tasks Determination
Task Determination TDet@CL
4
Situation Determination SD@CL
5
a
PF
PNF
Cockpit Tasks Distribution
Task Distribution TDis@CL
6
Risk Assessment RA@CL
7
Crew State Inference CSI
8

Figure 2: Architecture of the third pilot adaptive automation concept [7].

The notion of partnership between pilots and automation is central in the third pilot adaptive automation concept. The joint human-machine system continuously monitors the operational situation and the allied crew/automation/aircraft state, to determine the tasks the cockpit has to perform to achieve the mission goal, and the best task distribution between the crew and automation. Herein, the adaptive automation system can be seen as a third pilot, providing support to the pilots to ensure the completion of the mission level goal and to optimise flight safety. It provides extra information in relation to flight risks and potential courses of action, if required by crew.

Pilots are responsible and accountable for their decisions/actions. They are not mandated to follow the decision support and in most situations, the pilots have the final authority and can veto automation. However, in specific safety critical situations and when the pilots are not responding, the automation can take charge of the aircraft. In this way, the third pilot has three different operating modes: (1) passive support mode – monitoring only without crew notification and decision support, (2) active support mode - providing support and assistance to achieve the mission level goal, and (3) intervention/over-ride mode – taking charge of the aircraft control [8].

In the A-PiMod project specific tools were developed for the architecture, which were integrated and evaluated in a flight simulation environment; see [9] for more details. The safety impact quantification presented in the next section, however, is for the third pilot adaptive automation concept as such and does not consider any specific technical implementations.

4 Results

4.1 Scoping

All accident types of the total aviation system risk model are considered relevant for the third pilot adaptive automation concept. The safety impact quantification was achieved for fatal accidents rather than for aviation accidents in general, because these types of accidents are in line with the quantitative safety goal of [1]. In addition, they matter most for the perception of aviation safety, and they match best with the focus of the third pilot concept.

In this study an initial model restriction was achieved at the level of scenarios. We selected all scenarios that contribute at least 2% to the total fatal accident risk. As a result, 16 scenarios including 236 base events were retained and 13 scenarios including 189 base events were excluded. The remaining scenarios are listed in Table 2 and overall they contribute to 90% of the total fatal accident frequency.

Table 2: Scenarios of the total aviation system risk model that contribute at least to 2% of the total fatal accident frequency (per flight).

Code	Description	Fatal accident frequency	
S18	Engine(s) failure in flight	7.13E-08	18.0%
S19	Unstable approach	4.05E-08	10.2%
S35	TAWS alert	3.23E-08	8.2%
S32	Runway incursion	2.75E-08	7.0%
S26	Aircraft handling by flight crew inappropriate during landing roll	2.55E-08	6.5%
S27	Aircraft directional control related system failure during landing roll	2.42E-08	6.1%
S31	Aircraft are positioned on collision course in flight	2.36E-08	6.0%
S16	Airspeed, altitude or attitude display failure	2.31E-08	5.8%
S13	Flight control system failure	1.76E-08	4.4%
S06	Aircraft takes off with contaminated wing	1.49E-08	3.8%
S10	Pitch control problem during take-off	1.18E-08	3.0%
S09	Single engine failure during take-off	9.82E-09	2.5%
S25	Aircraft handling by flight crew inappropriate during flare	9.78E-09	2.5%
S14	Flight crew member incapacitation	9.64E-09	2.4%
S12	Flight crew member spatially disoriented	8.04E-09	2.0%
S03	Aircraft directional control by flight crew inappropriate during take-off	7.80E-09	2.0%
	13 other scenarios	3.82E-08	9.6%
	Total	3.96E-7	100%

For the identification of impressionable base events of the novel concept, 12 exclusion assumptions were identified. Examples are “the concept does not have any influence on base events that represent technical systems not being available or failing, or causes of technical failures (such as bad maintenance)” and “the concept does not have any influence on base events that are solely caused by ATC”.

Using these assumptions all 236 remaining base events were evaluated. It follows from this evaluation that 153 base events are not influenced by the third pilot adaptive automation concept. The exclusion of these base events implies that all base events of the following 6 scenarios are not influenced: S27, S06, S10, S09, S25, and S03. The remaining 83 base events may be influenced and they were assessed in detail.

4.2 Assessment of change factors of base events

In support of the assessment of the change factors, three workshops with experts were organized as part of the A-PiMod Community of Practice. One workshop involved 12 project partners with backgrounds in system development, human factors and safety analysis, and the other two workshops involved a total of 4 airline pilots. Although the experts knew about particular technical implementations of the adaptive automation concept, during these workshops it was stressed that the concept as such was assessed and not its particular implementations. In the sessions the experts provided their opinions on the potential safety negative and positive implications of the concept, and on the resulting change factors of the related base events using the terminology of T.

The results achieved in these sessions were used to assess the probability change factors for all concept impressionable base events. The details of the argumentation of this assessment are in [10]; some examples are provided next.

- A Significant reduction (factor 2.25) is expected in the probability of S13 base event “Conflicting course due to airspace infringement”. The system advises to take a different course if the aircraft is heading towards forbidden airspace (e.g. military zones). The system impact is limited by concurrently available support from air traffic controllers for avoiding airspace infringements.
- A Considerable reduction (factor 5) is expected in the probability of S13 base event “Conflicting course due to level bust”. There are a number of inputs that allow the system to detect and flag discrepancies, and to advise to level off.
- A Major reduction (factor 10) is expected in the probability of S14 base event “Simultaneous incapacitation of all flight crew members”. The system recognizes the incapacitation of the pilots and takes control of the aircraft.
- A Major reduction (factor 10) is expected in the probability of S19 base event “Flight crew fails to recognise unstable approach”. If the criteria for a stable approach are built into the third pilot system, it can tell the crew when they have not been met and advise to go around. The pilots in the COP sessions recognized that sometimes crew may have tunnel vision towards landing or may be pressed by ATC. The system supports the ending of such risky approaches.
- A Major reduction (factor 10) is expected in the probability of S19 base event “Flight crew fails to respond appropriately to unstable approach” (the crew has recognised the unstable approach but is not able to take appropriate action, i.e. initiate a missed approach). The third pilot system can support the pilots in conducting a missed approach and it may take over the control for flying the missed approach.
- A Small reduction (factor 1.2) is expected in the probability of S19 base event “Improper control exchange” (problem with the control roles of the pilots during approach). It is expected that pilots are typically well aware of their roles during this flight phase and that the task distribution function of the system has only a Small effect.
- A Major reduction (factor 10) is expected in the probability of S35 base event “Flight crew does not execute terrain avoidance manoeuvre successfully” (in case of a terrain avoidance alert). It is expected that the third pilot system takes control of the aircraft if the pilots don’t react properly to the terrain avoidance alert and gets the aircraft away from the terrain.

A main result in the assessment is that all base event probabilities were assessed to remain the same or to be reduced due to the novel concept. Although potential safety negative effects were noted for several situations in the COP sessions, the overall safety effect was never judged negatively for the concept.

Overall, the concept was assessed to lead to a reduction in base event probabilities for 46 of the 236 base events that were in the scope of the study, i.e. for 19% of these base events. With respect to the mechanisms by which the third pilot adaptive automation system supports flight safety, in almost all of these 46 base events the system can detect the safety critical situation considered (43 base events) and it can support the pilots in recovery actions (43 base events). In about half of the 46 base events, the system can support the pilots in avoiding an error (22 base events) that can lead to the safety critical situation.

4.3 Risk impact quantification

The fatal accident risk effects are shown in Table 3 for each of the scenarios that are in the scope of the assessment. It follows from this overview that there are 8 scenarios that profit from the third pilot adaptive automation concept, with a reduction of the probability of a fatal accident in the range from 41% to 93% per scenario with respect to the baseline condition. These reductions correspond with reductions of 2% to 13% with respect to the total fatal accident risk. Overall the fatal accident probability is reduced by 43% from 4.0E-7 per flight to 2.2E-7 per flight, where we made the conservative assumption that the 13 other scenarios (which were not assessed) do not contribute to any risk reduction. Comparing the fatal accident probability of the 16 scenarios that were assessed, shows that the summed fatal accident risk of this set of scenarios decreases from 3.6E-7 to 1.9E-7, being a reduction of 48%.

It follows from Table 3 that in the third pilot adaptive automation concept the scenarios that would contribute mostly to the overall fatal accident risk are different from those in the baseline. It is assessed that the fatal accident probability is strongly reduced for the top-3 of the baseline, especially the remaining contributions to the overall risk for S19 “Unstable approach” and S35 “TAWS alert” are expected to be very low. The new top-3 of scenarios in the novel concept consists of scenarios that are expected not to be influenced: S32 “Runway incursion”, S26 “Aircraft handling by flight crew inappropriate during landing roll” and S27 “Aircraft directional control related system failure during landing roll”.

Table 3: Fatal accident frequencies of scenarios in the baseline condition and in the novel third pilot adaptive automation concept.

Code	Scenario description	Fatal accident frequency (per flight)					
		Baseline		Novel concept		Change (%)	
		Freq.	**Perc.**	**Freq.**	**Perc.**	**Scen.**	**Total**
S18	Engine(s) failure in flight	7.1E-08	18.0%	2.1E-08	9.2%	-71%	-12.8%
S19	Unstable approach	4.1E-08	10.2%	2.9E-09	1.3%	-93%	-9.5%
S35	TAWS alert	3.2E-08	8.2%	3.2E-09	1.4%	-90%	-7.4%
S32	Runway incursion	2.8E-08	7.0%	2.8E-08	12.3%	0%	0%
S26	Aircraft handling by flight crew inappropriate during landing roll	2.6E-08	6.5%	2.6E-08	11.4%	0%	0%
S27	Aircraft directional control related system failure during landing roll	2.4E-08	6.1%	2.4E-08	10.8%	0%	0%
S31	Aircraft are positioned on collision course in flight	2.4E-08	6.0%	8.0E-09	3.6%	-66%	-3.9%
S16	Airspeed, altitude or attitude display failure	2.3E-08	5.8%	7.5E-09	3.4%	-67%	-3.9%
S13	Flight control system failure	1.8E-08	4.4%	1.0E-08	4.7%	-41%	-1.8%
S06	Aircraft takes off with contaminated wing	1.5E-08	3.8%	1.5E-08	6.6%	0%	0%
S10	Pitch control problem during take-off	1.2E-08	3.0%	1.2E-08	5.3%	0%	0%
S09	Single engine failure during take-off	9.8E-09	2.5%	9.8E-09	4.4%	0%	0%
S25	Aircraft handling by flight crew inappropriate during flare	9.8E-09	2.5%	9.8E-09	4.4%	0%	0%
S14	Flight crew member incapacitation	9.6E-09	2.4%	9.6E-10	0.4%	-90%	-2.2%
S12	Flight crew member spatially disoriented	8.0E-09	2.0%	6.4E-10	0.3%	-92%	-1.9%
S03	Aircraft directional control by flight crew inappropriate during take-off	7.8E-09	2.0%	7.8E-09	3.5%	0%	0%
	13 other scenarios (not assessed)	3.8E-08	9.6%	3.8E-08	17.0%	0%	0%
	Total	**4.0E-07**	**100%**	**2.2E-07**	**100%**		**-43%**

5 Discussion

In this paper we presented a straightforward approach for safety impact quantification of innovative aviation concepts in early stage development. Such an approach supports decision-making for early stage selection of safety-effective concepts. Next we discuss some main aspects and limitations of the approach and its results to the case study.

The basis of the approach is the total aviation system risk model, which is a combination of event sequence diagrams and fault trees for a range of safety-critical aviation scenarios. Event sequence diagrams and fault trees are well known and broadly used methods in safety assessment studies, which can be depicted and understood quite easily. On this basis, the total aviation system risk model provides a broad, structured and straightforward categorization of aviation accidents and their main causes, and an overview of the frequency by which they occur. This a valuable asset to assess potential safety improvements in early stage concept development.

On the basis of this risk model. the safety impact quantification approach provides a high-level, broad and rough overview of the accident risk reduction that may be obtained by the novel concept. Sources of uncertainty in the risk quantification include the following.

- There exists uncertainty in the total aviation system risk model. It is an extensive model, which consists of 29 scenarios with 425 base events and 51 accident end states. The quantification of the ASCOS-CATS model was achieved using data on 502 accidents and expert judgement, and using insights from earlier quantification of the CATS model with a broader world-wide scope. Given the model size, the limited data set and the use of expert judgement, the quantification results include some levels of uncertainty, especially for events with little associated accident data.
- There exists uncertainty due to the model structure. A key limitation of fault trees and event sequence diagrams is that these do not well represent the interactions and dynamics of agents in a sociotechnical system. Therefore, the risk implications of dynamic relations between events and actions of human operators and technical system in an operational context cannot be studied and understood in detail by such risk modelling [11].
- There exists uncertainty in the assessment of the change factors of the base event probabilities. The assessment has primarily been based on the feedback obtained from commercial pilots and system designers in the COP sessions. Some uncertainty is due to differences in opinion between the participants of these sessions. Most importantly, it is intrinsically difficult to judge the effect of dynamic scenarios and the performance of humans and systems herein. This is strengthened by the judgement of the novel concept rather than a less abstract specific implementation of the concept.

The particular levels of uncertainty due to above aspects have not been assessed, neither during the development of the total aviation system risk model, nor during the assessment of the change factors. A particular level of uncertainty is inherent in any safety risk assessment and it is typically more prevalent for early stage concepts. As long as the presence of uncertainty is realized and the results are being interpreted as indicative, this is acceptable in the early development phase.

As part of the development process of specific technical implementations of a concept, more detailed safety assessment studies would be needed during its subsequent development phases. Such safety assessment should consider in detail the performance of new technical systems, their interactions with human operators, and the role in the overall sociotechnical system. The analysis should be done in the context of specific scenarios and it should consider a broad range of hazards which may disturb the technical systems, the performance of the human operators, and the context of the flight operations. The safety assessment method applied should be commensurate with the characteristics of the scenario studied. For instance, to assess in detail the safety implications of scenarios during which the timing of interacting actors is critical, a dynamic safety assessment method is advised, such as agent-based dynamic risk modelling [11, 12].

The assessment of change in accident risk due to a novel concept used the assessment of multiplicative change factors by expert judgement in combination with the total aviation system risk model as a main method. The values and terminology of the change factors were based on earlier work on bias and uncertainty assessment in risk modelling [6]. In the current application for the assessment of change in base event probabilities using expert feedback (in the COP workshops), it was found that the system designers and pilots well understood the use of the change factors. The range and granularity of the change factors were mostly appropriate for this study, but it was noticed that the term Negligible (factor 1.1) was never used and that some pilots referred to an above Major (factor 20) effect for some base events. The lack of the use of the term Negligible may be due to the rather high conceptual level of the operation assessed, which made it difficult to distinguish with respect to Neutral and Small effects. In future assessments, a term for an above Major effect may be explicitly included, as it better reflects the option that the likelihood of particular events is very strongly suppressed.

Scoping was used to select the most risk-relevant scenarios and impressionable events. Such scoping was needed to downsize the number of base events to an amount that could be handled well in the sessions with experts. The selection of the most risk-relevant scenarios reduced the number of base events from 425 to 236, and the subsequent selection of impressionable base events further reduced the set to 83 base events. This set could be well handled in the sessions with experts.

The results attained for the third pilot adaptive automation concept indicate that it may facilitate a reduction in the probability of fatal accidents by 43% from 4.0E-7 to 2.2E-7 fatal accidents per flight. In addition to the overall impact on the fatal accident probability, the assessment also provided results for the contributions of scenarios. The largest reductions with respect to the total fatal accident risk were assessed for scenarios S18 “Engine(s) failure in flight”, S19 “Unstable approach”, and S35 “TAWS alert”. Complete development and operational introduction of the third pilot adaptive automation system for these scenarios thus is expected to have the largest impact on aviation safety.

High impact is expected in situations where the third pilot system takes control of the aircraft. Examples are events where pilots do not respond well to alerts to avoid collisions with terrain or other aircraft, and an event where pilots do not initiate a missed approach although they have been warned about an unstable approach condition. In such situations, the automation may need to take control of the aircraft without the consent of the pilots, since the required actions are time-critical and the pilots did not respond by themselves in first instance. Clearly, such taking over by automation is sensitive from different perspectives. (1) It implies a shift in responsibility from the pilots to the automation. (2) Such shift in responsibility means that the liability of aircraft and avionics manufacturers has to be studied carefully. (3) Such shift in responsibility would need to be accepted by the pilot, the aviation community and the travelling public. (4) The situations in which control would be taken over by the automation need to be defined and studied in large detail using appropriate methods for studying all kinds of combinations of events and the dynamics of the scenarios. Such detailed and well-validated understanding is a necessary condition for items 1 – 3 related to the shift in responsibility to be accepted. Only if all these sensitive aspects have been handled well, the large reductions in fatal accident risks associated with these situations may be achieved.

A further reduction of the fatal accident risk (e.g. towards the safety goal specified in [1]) can most effectively be attained by additional innovative approaches that can reduce the fatal accident probabilities of scenarios that are not influenced by the described third pilot adaptive automation concept. These scenarios most importantly consider landing and take-off operations, as well as runway incursion scenarios. For an advanced concept to be effective in these kinds of scenarios it should have the information and means to react and possibly take control very rapidly.

Overall, the safety impact quantification approach is a straightforward way to obtain quantitative insight in the safety implications of early stage aviation concepts. In later development phases, other dedicated methods are needed for more detailed safety assessment of the sociotechnical system. The new third pilot adaptive automation concept allows for improved partnership between pilots and automation, which is expected to significantly improve the safety of flight, especially in abnormal situations and crisis management.

Acknowledgements

This research was done as part of the European FP7 project A-PiMod (Applying Pilot Models for Safer Aircraft). We thank all members of the A-PiMod Community of Practice for their contributions to the sessions for the safety impact quantification.

6 References

[1] European Commission. Flightpath 2050: Europe's vision for aviation. Luxembourg; 2011.

[2] Roelen ALC, Verstraeten JG, Speijker LJP, Bravo Munoz S, Heckmann JP, Save L, et al. Risk models and accident scenarios in the total aviation system. 2014.

[3] Wenger E, McDermott RA, Snyder W. Cultivating communities of practice: A guide to managing knowledge. Boston, USA: Harvard Business Press; 2002.

[4] Ale BJM, Bellamy LJ, Cooke RM, Goossens LHJ, Hale AR, Roelen ALC, et al. Towards a causal model for air transport safety—an ongoing research project. Safety Science. 2006;44:657-73.

[5] ICAO. Annex 13: Aircraft accident and incident investigation. International Civil Aviation Organization; 2010.

[6] Everdij MHC, Blom HAP, Stroeve SH. Structured assessment of bias and uncertainty in Monte Carlo simulated accident risk. Proceedings 8th International Conference on Probabilistic Safety Assessment and Management, New Orleans, USA, 2006.

[7] Javaux D, Fortmann F, Mohlenbrink C. Adaptive human-automation cooperation: A general architecture for the cockpit and its application in the A-PiMod project. 7th International Conference on Advanced Cognitive Technologies and Applications (COGNITIVE 2015), 2015.

[8] Cahill J, Callari TC, Javaux D, Fortmann F, Hasselberg A. A-PiMod: a new approach to solving human factors problems with automation HCI International Toronto, Canada, 2016.

[9] A-PiMod project website. www.apimod.eu.

[10] Cahill J, Callari TC, Stroeve SH, Van Doorn BA. Overall evaluation of safety impact. A-PiMod project; D5.7; 2016.

[11] Stroeve SH, Blom HAP, Bakker GJ. Contrasting safety assessments of a runway incursion scenario: Event sequence analysis versus multi-agent dynamic risk modelling. Reliability Engineering & System Safety. 2013;109:133-49.

[12] Everdij MHC, Blom HAP, Stroeve SH, Kirwan B. Agent-based dynamic risk modelling for ATM: A white paper. Eurocontrol; 2014.

This page is intentionally left blank.

NLR

Anthony Fokkerweg 2
1059 CM Amsterdam, The Netherlands
p) +31 88 511 3113 f) +31 88 511 3210
e) info@nlr.nl i) www.nlr.nl