



Executive summary

Safety risk analysis of runway incursion alert systems in the tower and cockpit by multi-agent systemic accident modelling

Problem area

Runway incursion is broadly recognised as an important safety issue. Runway incursion alert systems in air traffic control towers and cockpits are intended to reduce runway incursion risk. It is, however, not well known how effective these alert systems can be. Analysis of their effectiveness is challenging, because of the context-dependent distributed and dynamic interactions of multiple human operators and technical systems in a runway incursion scenario. Recent views in the safety literature indicate that for risk assessment of such complex scenarios, we need systemic accident modelling, which considers accidents as emergent phenomena from the performance variability of a system.

Description of work

This paper uses multi-agent situation awareness as a prime concept for systemic accident modelling of a runway incursion scenario. In the multi-agent situation awareness model a single representation is used for both situation awareness of humans and technical systems. The modelled situation awareness is a dynamic entity, including information attitudes (belief) and pro-attitudes (intent). Stochastic effects in

situation awareness updating processes and the dynamic interactions between agents are contributors to the performance variability in the systemic accident model.

Results and conclusions

Accident risk results are provided for the effectiveness of alert systems in the tower and cockpit in good and reduced visibility conditions, and for two cases of pilot situation awareness errors. The results of the Monte Carlo simulations indicate that runway incursion alert systems may lead to a large reduction in conditional collision risk during reduced visibility conditions. Here, ATC runway incursion alerts enable a risk reduction of about one order of magnitude and cockpit alerts enable a risk reduction of about two orders of magnitude. In good visibility conditions, the effectiveness of runway incursion alert systems in reducing the conditional collision risk values is considerably less. Nevertheless, a significant risk reduction can still be attained by cockpit alert systems for situations in which the crew of the taxiing aircraft is lost.

Applicability

Safety of aerodrome operations.

Report no.

NLR-TP-2007-563

Author(s)

S.H. Stroeve
G.J. Bakker
H.A.P. Blom

Report classification

UNCLASSIFIED

Date

July 2007 July 2007

Knowledge area(s)

Safety & Security

Descriptor(s)

accident risk assessment
runway incursion
alert systems
multi-agent modelling

Safety risk analysis of runway incursion alert systems in the tower and cockpit by multi-agent systemic accident modelling

Nationaal Lucht- en Ruimtevaartlaboratorium, National Aerospace Laboratory NLR

Anthony Fokkerweg 2, 1059 CM Amsterdam,
P.O. Box 90502, 1006 BM Amsterdam, The Netherlands

Telephone +31 20 511 31 13, Fax +31 20 511 32 10, Web site: www.nlr.nl



NLR-TP-2007-563

Safety risk analysis of runway incursion alert systems in the tower and cockpit by multi-agent systemic accident modelling

S.H. Stroeve, G.J. Bakker and H.A.P. Blom


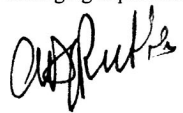
This report is based on a paper presented at the 7th USA/Europe Air Traffic Management R&D Seminar, Barcelona, Spain, 2-5 July 2007.

This report may be cited on condition that full credit is given to NLR and the authors.

This publication has been refereed by the Advisory Committee AIR TRANSPORT.

| | |
|-------------------------|---------------|
| Customer | NLR |
| Contract number | ---- |
| Owner | NLR |
| Division | Air Transport |
| Distribution | Unlimited |
| Classification of title | Unclassified |
| | December 2007 |

Approved by:

| | | |
|--|----------|--|
| Author  24-1-08 | Reviewer | Managing department  |
|--|----------|--|

Summary

Runway incursion alert systems in air traffic control towers and cockpits are intended to reduce runway incursion risk. Analysis of the effectiveness of such systems is challenging, because of the context-dependent distributed and dynamic interactions of multiple human operators and technical systems in a runway incursion scenario. Recent views in the safety literature indicate that for risk assessment of such complex scenarios, we need systemic accident modelling, which considers accidents as emergent phenomena from the performance variability of a system. This paper uses multi-agent situation awareness as a prime concept for systemic accident modelling of a runway incursion scenario. Accident risk results are provided for the effectiveness of alert systems in the tower and cockpit for various contextual conditions.

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 7 |
| 2 | Runway incursion scenario | 9 |
| 2.1 | Aerodrome layout | 9 |
| 2.2 | Weather conditions | 9 |
| 2.3 | Human operators | 9 |
| 2.4 | Crossing procedure | 9 |
| 2.5 | ATC alerts | 10 |
| 2.6 | Cockpit alerts | 10 |
| 2.7 | Communication/Navigation/Surveillance | 10 |
| 2.8 | Runway incursion case | 10 |
| 3 | Accident modelling paradigms | 12 |
| 3.1 | Sequential / Epidemiological models | 12 |
| 3.2 | Systemic accident models | 13 |
| 4 | Multi-agent situation awareness | 15 |
| 4.1 | Human cognition | 15 |
| 4.2 | Distributed artificial intelligence | 15 |
| 4.3 | Socio-technical organizations | 16 |
| 5 | Multi-agent SA accident model | 17 |
| 5.1 | Multi-agent SA component and dynamics | 17 |
| 5.2 | Multi-agent systemic accident modelling | 18 |
| 6 | Monte Carlo simulation | 22 |
| 7 | Discussion | 24 |
| | References | 27 |



Abbreviations

| | |
|---------|--|
| ADS-B | Automatic Dependent Surveillance-Broadcast |
| A-SMGCS | Advanced Surface Movement Guidance and Control Systems |
| ATC | Air Traffic Control |
| FRAM | Functional Resonance Accident Model |
| GPS | Global Positioning System |
| HMI | Human Machine Interface |
| ICAO | International Civil Aviation Organization |
| NASA | National Aeronautics and Space Administration |
| R/T | Radio Transmitter |
| SA | Situation Awareness |
| STAMP | Systems-Theoretic Accident Model and Processes |
| TOPAZ | Traffic Organization and Perturbation AnalyZer |
| VHF | Very High Frequency |



This page is intentionally left blank.

1 Introduction

Runway incursion is broadly recognised as an important safety issue and several guidelines and safety programmes have been put forward in an effort to reduce this risk [1], [2], [3]. In addition to procedure and training related measures, research and development is done on new technology in the aircraft, air traffic control (ATC) tower, ground vehicles and aerodrome. Part of these systems aim to reduce the probability of runway incursion by enhancing situation awareness, providing improved guidance on the aerodrome and supporting efficient communication. Other systems aim to reduce the consequences of a runway incursion by alerting one or more involved operators.

This latter class most notably includes runway incursion alert systems. Alert systems directed to the controller are commercially available and alert systems directed to the pilots are the subject of research and development (e.g. NASA Runway Incursion Prevention System [4]). Despite the availability of such commercial and experimental systems, their effectiveness in reducing accident risk and the conditions under which these systems can be effective are not well known in the ATM safety literature.

Assessment of runway incursion risk and of the effectiveness of related alert systems is complex, due to the large number of human operators, aircraft and supporting technical systems on the aerodrome, the large number of interactions between those agents, the dynamics of the agents and the range of potential performance deviations of these agents. Therefore, we need risk assessment approaches which can address this complexity of aerodrome operations.

Recently, there has been a considerable impetus in safety science by approaches for risk assessment by systemic accident models [5], [6], [7]. Systemic accident models describe the performance of a system as a whole, rather than on the level of events that may go wrong and related cause-effect mechanisms, such as in e.g. fault and event trees. The systemic approach considers accidents as emergent phenomena from the variability in the performance of interacting entities in an organization. As part of continuing research on risk evaluation of complex multi-agent organizations, we presented earlier a multi-agent situation awareness modelling approach and showed how this can be effectively used for risk assessment of a runway incursion scenario involving ATC runway incursion alerting [8], [9]. In [10] we showed that this risk assessment approach is a systemic accident model.

The accident risk results presented in [8] were achieved for a runway incursion scenario in good visibility and involving an ATC runway incursion alert system. Those results showed that the effectiveness of ATC runway incursion alerts for lowering the accident risk is very small. In subsequent work [10], we showed that the effectiveness of ATC alerts in reduced visibility can be considerable. The development of runway incursion alerts in the cockpit is motivated by the expectation that these alerts will be more effective than ATC alerts, since they

by-pass the alert response and instruction time of the controller. In this paper we evaluate this expectation by expanding the model with cockpit alerts and presenting the accident risk results that follow from Monte Carlo simulation.

The organization of this paper is as follows. Section 2 describes the aerodrome operation for which we assess runway incursion risk aspects. Section 3 introduces accident modelling paradigms and argues what type of model is needed for risk assessment of complex operations. Section 4 proposes the concept of multi-agent situation awareness as key element in systemic accident modelling. Section 5 describes how this concept is effectively applied in an accident model of the runway incursion scenario. Section 6 provides results of Monte Carlo simulation for the accident model, which show the effectiveness of ATC tower and cockpit runway incursion alert systems. Section 7 discusses the methods and results for risk assessment of aerodrome operations.

2 Runway incursion scenario

2.1 Aerodrome layout

We consider a departure runway with a complex surrounding taxiway structure, including a taxiway crossing the runway at a distance of 1000 m from the runway threshold. The runway crossing may be used for taxiing between the aprons and a second runway, according to a runway crossing procedure that will be outlined later. The runway crossing has stopbars at 153 m from the runway centreline, which are remotely controlled by the runway controller.

2.2 Weather conditions

The operation is considered under limited weather conditions, in particular without wind and for the following two visibility conditions.

- *Visibility condition 1*: unrestricted visibility range; implying that pilots as well as controllers can visually observe the traffic situation. This is in line with visibility condition 1 of ICAO's A-SMGCS manual [11].
- *Visibility condition 2*: visibility range between 400 m and 1500 m; implying that controllers cannot visually observe the traffic and pilots are not always able to see the conflicting aircraft during the initial part of the take-off run. The lower limit of this visibility range (400 m) is equal to the upper limit of the runway visible range of visibility condition 3 indicated in [11]; the upper limit (1500 m) is chosen for this study (no value is given in [11]).

2.3 Human operators

The main human operators involved in the runway crossing operation are the pilots of the taking-off aircraft, the pilots of the taxiing aircraft, the runway controller and the ground controllers responsible for traffic on nearby taxiways. The pilots are responsible for safe conduct of the flight operations and should actively monitor for potential conflicting traffic situations. The runway controller is responsible for safe and efficient traffic handling on the runway and the runway crossings. The ground controllers are responsible for safe and efficient traffic handling on taxiways in the surrounding of the runway.

2.4 Crossing procedure

Aircraft may taxi across the active runway via the following procedure. The control over the taxiing aircraft is transferred from the responsible ground controller to the runway controller (including a change of the R/T frequency). Taking into consideration the traffic situation, the runway controller specifies a crossing clearance to the taxiing aircraft and switches off the remotely controlled stopbar. The crew of the taxiing aircraft acknowledges the clearance and initiates taxiing across the runway. The crew reports when the taxiing aircraft has vacated the

runway, upon which the control over the aircraft is transferred from the runway controller to the responsible ground controller.

2.5 ATC alerts

The runway controller has the disposition of alerts that intend to reduce the risk of runway incursion. These alerts are based on ground radar tracking data and consist of audible warnings and an indication on the ground surveillance display. A runway incursion alert is presented when an aircraft is crossing the runway in front of an aircraft that has initiated to take-off. A stopbar violation alert is presented when an aircraft crosses an active stopbar in the direction of the runway.

2.6 Cockpit alerts

Both the crews of the taking off and the taxiing aircraft have the disposition of cockpit runway incursion alerts. The cockpit runway incursion alert systems use satellite-based position estimation systems in each aircraft, and data-link communication of this navigation data between the aircraft. The cockpit alerts are thus independent from the ATC alerts. The cockpit runway incursion alert systems provide an aural alert if a runway incursion conflict is detected. These systems use a generic approach for runway incursion zone monitoring, which leads to an alert when a taxiing aircraft is within a specified distance from the runway and the other aircraft has initiated the take-off [4].

2.7 Communication/Navigation/Surveillance

Communication between controllers and crews is via VHF R/T communication systems. The pilots use their knowledge on the aerodrome layout and maps for taxiing. Ground radar tracking data of all aircraft and sufficiently large vehicles on the airport surface is shown on HMI's of the tower controllers. Both the runway controller and the pilots have alert systems, as described above.

2.8 Runway incursion case

We consider a runway incursion case in which an aircraft is taxiing across the active departure runway over the taxiway at 1000 m from the runway threshold, while it should not. This is due to the situation awareness of the crew of the taxiing aircraft, which is either that crossing of the runway is allowed, or the pilots think to be taxiing on a regular taxiway that does not cross the runway (i.e. they are lost). An overview of the main agents and their interactions in the runway incursion scenario is shown in Figure 1. The pilot not flying is not considered as agent in the current model of the runway incursion scenario; this is discussed in Section 7.

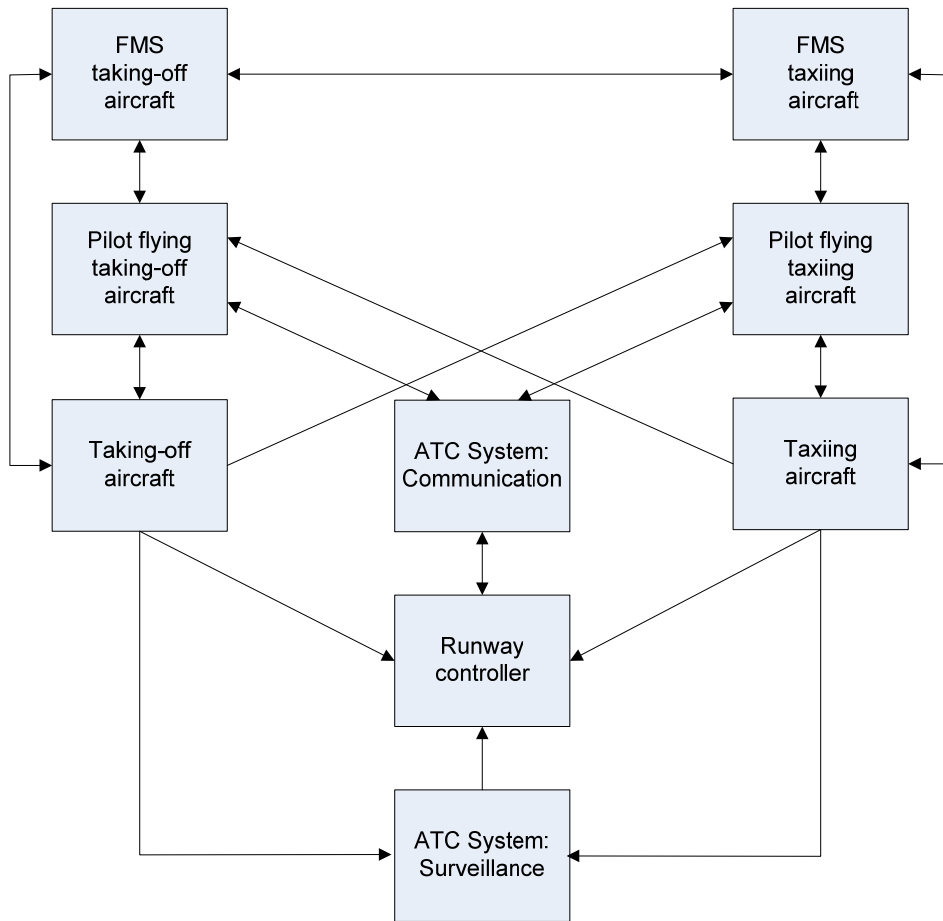


Figure 1: Main interactions between agents in the runway incursion scenario.

3 Accident modelling paradigms

3.1 Sequential / Epidemiological models

Safety risk assessment and management in the air traffic industry as well as in other industries have to a large extent been based on two paradigms for accident causation, namely (1) sequential accident models and (2) epidemiological accident models [5]. Sequential accident models describe an accident as the result of a sequence of events that occur in a specific order; examples are the domino theory, event trees, fault trees and networks models. Epidemiological accident models describe an accident in analogy with the spreading of a disease, i.e. as the outcome of a combination of factors, such as performance deviations, environmental conditions, barriers and latent conditions. Examples of epidemiological models are the “Swiss cheese” model [12] and Bayesian belief networks [13]. Both sequential and epidemiological accident models rely on cause-effect propagation in accidents and give a fixed representation of relations between failures, errors and contextual conditions. Predominantly, they represent relations between probabilities of event occurrences that are cause-effect implied. They do not address emergent behaviour due to interactions between entities.

For safety assessment of air traffic, these two types of accident models are used extensively. Sequential accident models are commonly known and applied in aviation. Fault and event trees are often applied in system dependability and safety requirement studies for air traffic [14], [15]. Epidemiological accident models have recently been used in air traffic safety assessment methods such as the Human Factors Analysis and Classification System [16] and Bayesian belief networks for air transport safety [13], [17].

Recent views on accident causation indicate that the sequential and epidemiological accident models may not be adequate to represent the complexity of modern socio-technical systems [5], [6], [7], [18]. Key determinants of this complexity include the number and variety of organizational entities (human, groups, technical systems), the number and types of interdependencies between organizational entities, the degree of distribution of the entities (single/multiple locations), the types of dynamic performance of the entities (static/slow/fast), and the number and types of hazards in the organization. Figure 1 well illustrates the complexity of the interactions between agents in the runway incursion scenario. Limitations of sequential and epidemiological accident models include the difficultness to represent the large number of interdependencies between organizational entities and the dynamics of these interdependencies. Since the focus on failures in sequential and epidemiological accident models is there also used for the evaluation of human performance, the roles of humans are practically restricted to making errors and resolving safety-critical situations.

3.2 Systemic accident models

Quite a different approach is followed in a third type of accident model [5]: systemic accident modelling. The systemic accident model view considers accidents as emergent phenomena from the performance variability of a system. Here the term 'system' is used in a broad sense as an organization of interacting humans and technical systems, i.e. a joint cognitive system [19]. The performance of a joint cognitive system is variable due to external noisy influences and the interactions between its entities. In particular, Hollnagel [5] argues that in daily practice, humans do not always work strictly according to rules and procedures, but adapt their performance according to the perceived requirements set by the working context. In other words, human performance must be variable to handle efficiently the complex interactions in a socio-technical environment. Hollnagel also argues that the combined and coupled performance variability in an organization may lead to functional resonance, i.e. enlarged deviations in performance from normal practice, which may be a source of accident causation. In a systemic framework, accident prevention is based on finding dependencies in a socio-technical organization that may lead to functional resonance, and monitoring and controlling such critical dependencies. As a basis for the analysis and understanding of complex systems, Pariès [20] points out that we should relate its micro and macro levels its micro and macro levels, such that macro level properties emerge from assembling micro level properties. This view is in line with multi-agent modelling, which considers the local perspective and behaviour of agents, and the emergence of overall behaviour due to the distributed agent interactions [21], [22]. Above views indicate that for risk assessment of complex organizations (such as air traffic) we need approaches that account for the variability in their multi-agent performance and the emergence of safety occurrences from this variability.

Systemic accident models have their origins in cybernetic control theory and chaos theory. Recent developments in systemic accident modelling include Functional Resonance Accident Model (FRAM), Systems-Theoretic Accident Model and Processes (STAMP) and Traffic Organization and Perturbation AnalyZer (TOPAZ). FRAM uses a functional representation of an operation and describes performance variability based on a number of characteristics of each function (input, output, resources, time, control and preconditions) and the interactions with other functions [5]. A qualitative analysis is used to evaluate safety-critical conditions where the interdependencies in a FRAM network may give rise to functional resonance. STAMP is based on system and control theory, and uses the key principle that accidents may occur as the result of a lack of control constraints imposed on the system design and on operations [7]. STAMP applications have mostly focussed on interactions at higher organizational levels than the human-system level. STAMP supports quantitative evaluation of risk levels as function of organizational processes, but not at the level of accident probability. The TOPAZ methodology is based on stochastic system and control theory, and employs the

basic principle that accidents may result from stochastic and dynamic interactions between agents in a traffic scenario. It uses integration with a qualitative safety risk assessment cycle, mathematical modelling, Monte Carlo simulation and uncertainty evaluations to analyse the safety of air traffic operations up to the level of accident probability [23], [24], [25], [26]. Multi-agent situation awareness is a key concept in TOPAZ [8], [9]. The following sections discuss this concept and its integration in a systemic accident model.

4 Multi-agent situation awareness

4.1 Human cognition

From human factors studies it is well known that lack of proper situation awareness is an important contributor to the occurrence of incidents and accidents [27], [28]. Situation awareness has been defined in the literature as a state or as a process [29]. The best known and most influential definition is the state-oriented one of Endsley [27]: *Situation awareness is the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.* In this definition, situation awareness is a dynamic state of knowledge which discerns three levels:

1. perception of elements in the environment,
2. comprehension of the current situation,
3. projection of the future status.

The process of achieving, acquiring and maintaining situation awareness is referred to as situation assessment [27]. Situation assessment processes depend on a range of human performance characteristics [30] and may lead to incomplete or inaccurate situation awareness at the three indicated levels. At level 1, a person may wrongly or not perceive task-relevant information, depending on aspects as signal characteristics, perception strategies and expectations. At level 2, a person may wrongly interpret perceived information, for instance due to miss-use or non-existence of proper mental models of the environment. At level 3, a person may wrongly predict a future status, for instance due to a lack of good mental model or memory limitations.

For a group of interacting humans the concept of team situation awareness is used [27]. In addition to the cognitive processes as perception, comprehension and projection, acquiring team situation awareness depends on team processes such as communication and coordination. Team situation awareness may be seen as individual situation awareness plus a number of processes to share part of the individual situation awareness with team members. In teams, the situation awareness of individual members may be affected as result of imperfect communication and coordination processes, or due to information transfer processes based on inappropriate situation awareness.

4.2 Distributed artificial intelligence

In the field of distributed artificial intelligence, human mentalistic notions similar to that of situation awareness are used. Ascription of mental qualities to technical systems is recognised as useful for analysis of complex systems, even if a complete and accurate description of the system is available. The human mentalistic notions are then abstractions, which provide a

convenient and familiar way of describing, explaining and predicting behaviour of complex systems [21]. The two most important types of attitudes are

- *information attitudes*: belief, knowledge; and
- *pro-attitudes*: desire, intention, obligation, commitment, choice, etc.

In distributed artificial intelligence, an *agent* is known as a computational mechanism with these attitudes that exhibits a high degree of autonomy, performing actions in its environment based on information (sensors, feedback) received from the environment. A *multi-agent* environment is defined broadly as a situation with more than one agent, where agents interact with one another, and there are constraints such that agents may not know everything about the world that other agents know [22].

4.3 Socio-technical organizations

For risk assessment of socio-technical organizations, the performance of human operators, technical systems and their interactions must be accounted for. In this context of socio-technical organizations, we use the term agent from the field of distributed artificial intelligence in a broad sense to represent technical systems as well as human operators. Furthermore, we broaden the term situation awareness from the field of human factors to represent the state of human operators as well as technical systems. We coin the term multi-agent situation awareness to stress the union of both disciplines in representation of information attitudes and pro-attitudes in an environment of interacting human operators and technical systems [8], [9].

5 Multi-agent SA accident model

5.1 Multi-agent SA component and dynamics

The main agents and interactions in the model of the runway incursion alerts case are shown in Figure 1. These agents include both the aircraft taking-off and taxiing, the aircrafts' pilots flying, the aircrafts' flight management systems (including GPS receiver, ADS-B system, incursion alert system), the runway controller and the ATC system (including surveillance systems, communication systems, airport manoeuvre control systems, airport configuration, environmental conditions).

In a multi-agent environment such as in Figure 1, a single agent may have situation awareness about each agent, i.e. in an environment of n agents the situation awareness of agent k at time t is

$$\sigma_{t,k} = [\sigma_{t,k}^1, \dots, \sigma_{t,k}^j, \dots, \sigma_{t,k}^n]$$

Agents are not omniscient; situation awareness components may be unknown. The situation awareness $\sigma_{t,k}^j$ includes information attitudes, such as beliefs concerning identify, state and mode of an agent; this part is named 'state situation awareness'. Additionally, the situation awareness $\sigma_{t,k}^j$ includes a pro-attitude [21] regarding the intent of agent j ; this part is named 'intent situation awareness'. The intent situation awareness includes anticipated modes, states and related times. Details on the mathematical representation of situation awareness can be found in [8], [9]. Table 1 shows examples of situation awareness components of the agents considered in the runway incursion example.

As is stipulated by the time index t , the situation awareness is a dynamic state. A general update process for the situation awareness is:

$$\sigma_{t'+\tau} = f^{\text{SA update}}(\sigma_{t'}, \mathcal{E})$$

where t' is a trigger time of the updating process, τ is the duration of the updating process and \mathcal{E} denotes stochastic effects that influence the updating process. In [8], [9] we distinguished three types of updating processes, depending on the information transfer between the involved agents:

- Reasoning: process in which the SA of an agent is updated without any interaction with other agents;
- Observation: process in which the SA of an agent is updated via a unidirectional information flow from another agent;
- Communication: process in which the SA of an agent is updated via a bidirectional information flow with another agent, which may also lead to a change in the SA of the other agent.

Examples of specific situation awareness updating processes for the runway incursion accident model are shown in Table 1.

Table 1: Examples of situation awareness aspects and situation awareness updating processes for the runway incursion scenario (see also Figure 1).

| Agent | Situation awareness aspects | Situation awareness updating processes |
|-------------------------|---|--|
| PF taking-off aircraft | <ul style="list-style-type: none"> • Identity, mode, position, velocity of own and other aircraft • ATC clearance • Mode of cockpit alert • Next waypoint | <ul style="list-style-type: none"> • Visual observation • Auditory monitoring • Speech communication • Conflict recognition & reaction |
| PF taxiing aircraft | <ul style="list-style-type: none"> • Identity, mode, position, velocity of own and other aircraft • ATC clearance • Mode of controlled stopbar • Mode of cockpit alert • Next waypoint | <ul style="list-style-type: none"> • Visual observation • Auditory monitoring • Speech communication • Conflict recognition & reaction |
| Runway controller | <ul style="list-style-type: none"> • Identity, mode, position, velocity of aircraft • Mode of controlled stopbar • Modes of ATC alerts • Next waypoints of aircraft | <ul style="list-style-type: none"> • Visual observation • Auditory monitoring • Speech communication • Conflict recognition & reaction |
| FMS taking-off aircraft | <ul style="list-style-type: none"> • Identity, mode, position, velocity of own and other aircraft • Aerodrome geometry data • Mode of cockpit alert | <ul style="list-style-type: none"> • Satellite position estimation • Data-link communication • Alert setting process |
| FMS taxiing aircraft | <ul style="list-style-type: none"> • Identity, mode, position, velocity of own and other aircraft • Aerodrome geometry data • Mode of cockpit alert | <ul style="list-style-type: none"> • Satellite position estimation • Data-link communication • Alert setting process |
| ATC system | <ul style="list-style-type: none"> • Position, velocity of aircraft • Aerodrome geometry data • Modes of ATC alerts | <ul style="list-style-type: none"> • Ground radar tracking • Alert setting process |
| Taking-off aircraft | <ul style="list-style-type: none"> • Position, velocity of own aircraft | <ul style="list-style-type: none"> • Aircraft dynamics |
| Taxiing aircraft | <ul style="list-style-type: none"> • Position, velocity of own aircraft | <ul style="list-style-type: none"> • Aircraft dynamics |

5.2 Multi-agent systemic accident modelling

The systemic accident model view considers accidents as emergent phenomena from the variability of a (joint cognitive) system. In the context of a multi-agent organization this variability is due to the variability in SA updating processes. The variability of SA updating processes is described in various modes of the agents, which represent situations in which there may be considerable differences between the SA updating processes. Table 2 describes selected

modes of the runway incursion alerts case. For ease of discussion, we distinguish nominal and non-nominal modes.

In nominal modes, the SA updating processes are frequently occurring processes with variations within a normal range. Examples of these variations consider (see also Table 1 and Table 2) the usual accuracy of visual observation by a controller, the typical visual monitoring frequency of pilot, or the normal accuracy of a surveillance system. Although these variations are considered normal, in combination with the variations in related multi-agent interactions they may lead to safety-critical situations, i.e. provide considerable contributions to the overall risk level.

Non-nominal modes describe more seldom situations and related SA updating processes. Table 2 provides a range of examples for the runway incursion alerts case. Such non-nominal situations often reflect degradation or non-functioning of a technical system, or an erroneous interpretation of reality by a human operator. These types of events are similar to failures and errors such as typically considered in sequential and epidemiological accident models. However, in the current systemic accident model these events are not directly associated with risk levels, but they indicate how related situation awareness updating processes are affected. These afflictions of the situation awareness updating processes may then induce a risk increase. Thus, the risk levels emerge from the variability of the agents' performance and interactions in the accident model.

Table 2: Examples of mode-dependent SA updating processes.

| Component | Mode | Impact on SA updating processes |
|--|------------------|--|
| Agent: Flight Management System Taxiing / Taking-off Aircraft | | |
| ADS-B Receiver | <i>Nominal</i> | Information is received with a normal sampling rate |
| | <i>Interrupt</i> | Information is received after a prolonged time |
| | <i>Down</i> | ADS-B receiver does not function |
| ADS-B Transmitter | <i>Up</i> | Information is transmitted with a normal sampling rate |
| | <i>Down</i> | ADS-B transmitter does not function |
| GPS Receiver | <i>Nominal</i> | Information is received with a normal sampling rate and accuracy |
| | <i>Interrupt</i> | Information is received after a prolonged time |
| | <i>Down</i> | GPS receiver does not function at all |
| Airport Map Database | <i>Correct</i> | Airport map database is correct for the specific airport |
| | <i>Incorrect</i> | Airport map database is erroneous for the specific airport, leading to lack of runway incursion alerting |
| Runway Incursion Alert Avionics | <i>Up</i> | Runway incursion alert avionics system is working nominally |



| | | |
|---|--|--|
| Availability | <i>Down</i> | Runway incursion alert avionics system is not working, leading to lack of runway incursion alerting |
| Agent: Pilot Flying Taxiing Aircraft | | |
| State Situation Awareness PF | <i>Intent SA = Proceed Taxiway</i> | Pilot believes to be taxiing on a normal taxiway, while actually proceeding toward a runway crossing; leading to sub-optimal visual monitoring |
| | <i>Intent SA = Cross Runway</i> | Pilot believes that crossing of the runway is allowed, while actually it is not allowed |
| Agent: ATC System | | |
| Surveillance Tracking | <i>Up</i> | ATC surveillance data is provided at normal rates and accuracy |
| | <i>Down</i> | ATC surveillance data is not provided |
| ATC Runway Incursion Alert System | <i>Up</i> | ATC runway incursion alerts are provided according to normal settings |
| | <i>Down</i> | ATC runway incursion alerts are not provided |
| R/T Communication Systems | <i>Up</i> | Tower-cockpit communication is supported normally |
| | <i>Delaying</i> | Tower-cockpit communication is delayed |
| | <i>Down</i> | No tower-cockpit communication |

As a basis for the Monte Carlo simulations of the air traffic scenario, the qualitative descriptions of the situation awareness updating processes in Table 1 and Table 2 are further detailed in mathematical models, which uniquely define the stochastic dynamics of the related agents (human operators and technical systems). These models are specified by a compositional specification approach using a stochastic dynamic extension of the Petri net formalism [31]. Within this Petri net formalism a hierarchically structured representation of the agents in the air traffic scenario is developed, including key aspects of agents, modes within these key aspects, dynamics within these modes and interactions between these model elements (see [10] for examples). The choice of parameter values for the simulation model is typically based on a variety of sources, such as technical system specifications, scientific expertise and literature on safety and human factors, searches in incident databases, interviews with operational experts, measurement data from real operations, measurement data from real-time simulations, and simulation results from other relevant models. In practice, limited data on appropriate parameter values is available for the contextual conditions considered, leading to a probability density function / confidence interval of possible parameter values. Typically, the mean of this interval is chosen for the simulation model and an analysis of the effect of the uncertainty in the parameter value on the risk is included in a bias and uncertainty assessment [26]. If the



uncertainty in the parameter value has a significant effect on the risk, an additional effort may be done to attain a better estimate.

6 Monte Carlo simulation

In this section we provide the results of Monte Carlo simulations with the model developed. The collision risks are simulated conditional on the visibility condition and the situation awareness of the pilot flying of the taxiing aircraft, which represents the intention to either continue taxiing on the current regular taxiway or to cross the runway. The conditional collision risks achieved in the Monte Carlo simulations for the multi-agent dynamic risk model are shown in Figure 2 and Figure 3 for visibility conditions 1 and 2, respectively. For both visibility conditions and intent situation awareness cases, the conditional collision risks are shown for the situation without alert systems ('None'), with an ATC alert system only ('ATC'), with cockpit alert systems only ('A/C'), and with both ATC and cockpit alert systems ('ATC+A/C').

The Monte Carlo simulation results in Figure 2 show that for an unrestricted visibility range (visibility condition 1) the conditional collision risk strongly depends on the situation awareness of the pilot flying of the taxiing aircraft. This difference is mainly caused by the improved (more frequent) monitoring strategy in the model for the case that the pilot intends to cross the runway compared to the case that the pilot intends to proceed on a regular taxiway. The Monte Carlo simulation results show that the effectiveness of the ATC alerts in visibility condition 1 is very small. In this situation the conflict has almost always been recognised by the pilots of one or both aircraft before the controller has the chance to react to the alert and instruct the pilots, and in the remaining cases the controller can usually not timely warn the pilots. The results indicate that in visibility condition 1, the effectiveness of the cockpit alerts is higher than ATC alerts for the situation where the pilots of the taxiing aircraft are not aware to be taxiing towards the runway. Here a quick cockpit alert may timely warn the crew of the taxiing aircraft. Furthermore, the effectiveness of ATC alerts in addition to cockpit alerts seems limited.

For a visibility range between 400 and 1500 m (visibility condition 2), the Monte Carlo simulation-based risks are quite different. Firstly, it follows from comparison of Figure 2 and Figure 3, that the conditional collision risks are considerably higher in the reduced visibility condition. Secondly, it can be observed in Figure 3 that similar conditional collision risks are obtained for both the cases of situation awareness of the pilot flying of the taxiing aircraft. In this visibility condition, the improved monitoring strategy of the pilot does not support early-stage recognition of the conflict. Thirdly, the ATC alerts enable a significant reduction in the conditional collision risk. Here, the conflict can often not be recognised by the pilots at an early stage and the alerts reduce the conflict detection time for the controller. Fourthly, the cockpit alerts result in a major reduction of the conditional collision risk. In this case, the conflict recognition time is further reduced by direct notification of the pilots. Fifthly, the alerts are more effective in the case where the pilot is intending to cross. This is due to the model aspect that in this case the aircraft may initiate taxiing from stance, thereby increasing the time before

it reaches the collision critical zone on the runway. Sixthly, the effectiveness of the ATC alerts in addition to the cockpit alerts is limited.

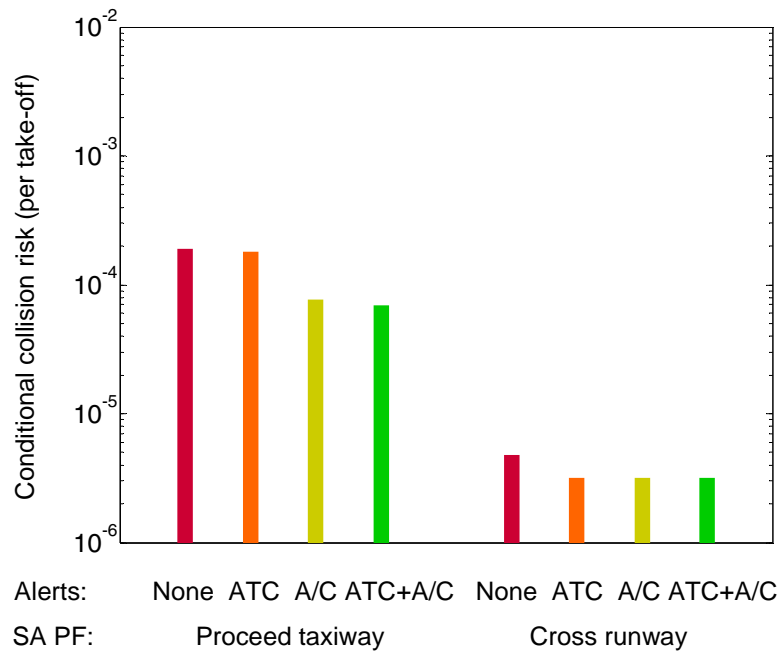


Figure 2: Estimated conditional collision risks in good visibility.

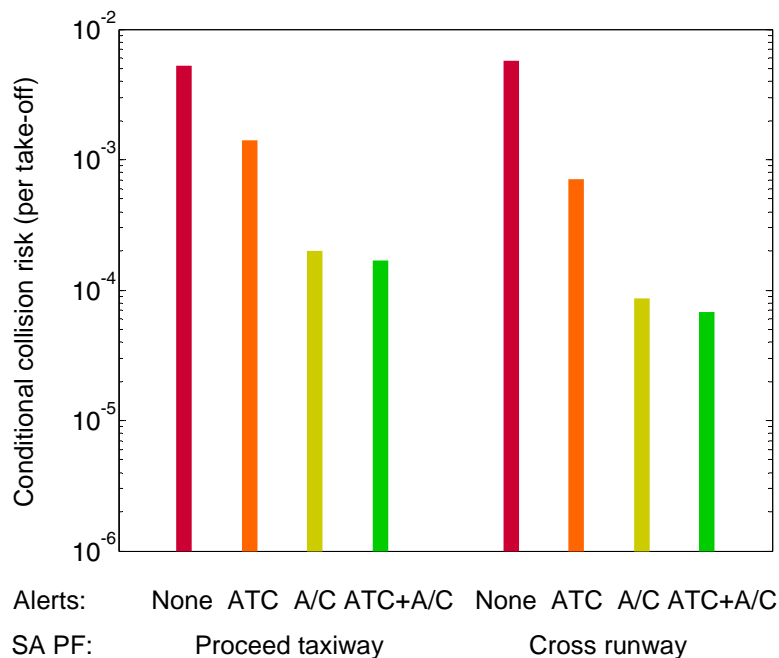


Figure 3: Estimated conditional collision risks in reduced visibility (400-1500 m).

7 Discussion

In this paper multi-agent situation awareness is used as a key concept for systemic accident modelling of complex socio-technical organizations. Important aspects of this method are illustrated by a safety evaluation of the effectiveness of tower and cockpit alerts in a runway incursion scenario.

In the multi-agent situation awareness model a single representation is used for both situation awareness of humans and technical systems. The modelled situation awareness is a dynamic variable, which considers information attitudes (belief) and pro-attitudes (intent), and is being changed by updating functions. Stochastic effects in these updating processes (e.g. perceptual noise, decision variance, duration until update) and the dynamic interactions between the agents are contributors to the performance variability in this systemic accident model.

The common notion of situation awareness for both humans and technical systems makes it a very suitable model for analysis of a joint cognitive system. A safety assessment ideally should address the performance of a joint cognitive system including all relevant humans and technical systems, rather than the performance of a (new) technical system and its direct interactions with humans / other systems. The suitability of the multi-agent situation awareness model is illustrated by the runway incursion alerts case. Here, the performance of a wide range of human operators and technical systems is considered, such as pilots, runway controller, tower and cockpit alert systems, communication systems, surveillance systems, etc. Therefore, we can assess the effectiveness of the tower and cockpit alert systems in reducing the accident risk of the runway incursion scenario in the context of the performance of the involved human operators, i.e. given that an accident would not have been prevented by the involved pilots or controller.

This kind of analysis of the effectiveness of a single agent (e.g. an alert system) in the context of a multi-agent organization with complex interactions is very difficult to achieve by sequential or epidemiological accident models. These models are not well suited for the dependent dynamics of the agents in this type of traffic scenario. For instance, in order to analyse the effectiveness of an ATC alert by these models, we would require data like 'the probability that an alerted controller warns the pilots when the taxiing aircraft is at position X and given that the crews of the taxiing aircraft as well as the taking-off aircraft have not yet detected the conflict either visually or via a cockpit alert.' Since these kinds of conditional probabilities can usually not be obtained, one typically has to assume that events/entities happen/act independently from each other and in a fixed sequence.

Systemic accident modelling is being broadly recognised as an important new stream for risk assessment [6]. Within the class of systemic accident models there are various ways to represent the performance variability of joint cognitive systems, main recent developments

include FRAM [5], STAMP [7] and TOPAZ [23]. The multi-agent situation awareness model presented in the current paper is part of TOPAZ and differs considerably from the other approaches. FRAM uses a functional decomposition of operations (which may include several agents in a function) and describes performance variability based on a number of characteristics of each function and the interactions with other functions. FRAM does not use mathematical modelling, Monte Carlo simulation or risk quantification. STAMP is based on system and control theory, where accidents may occur as the result of a lack of control constraints. Use of STAMP has focussed on interactions at a higher organizational level rather than the human-system level addressed in the multi-agent situation awareness model. STAMP does not use Monte Carlo simulation to evaluate stochastic variations. STAMP provides quantitative risk levels as function of organizational processes, but not at the level of accident probability.

The conditional collision risks that follow from the Monte Carlo simulations depend on the assumptions adopted in the mathematical model and simulation process. These assumptions address, for instance, airport specific aspects (e.g. traffic density, traffic characteristics, runway and taxiway geometry), human performance characteristics (e.g. monitoring intervals, alert reaction times, conflict detection strategy), performance of runway incursion alert systems (e.g. alert threshold distances, conflict detection settings), and exclusion of agents (e.g. exclusion of pilots not flying). In a risk assessment for a specific operation at a particular airport, its specific characteristics should be accounted for in dedicated Monte Carlo simulations, as well as included in a bias and uncertainty assessment of the Monte Carlo simulation-based results. Such a bias and uncertainty assessment evaluates the effects of the assumptions on the bias and uncertainty in the risk level via a number of steps, including a risk sensitivity analysis [26]. For assumptions with a large potential effect on the risk, additional parameter value sources or an enhanced model structure may be strived for in a subsequent risk assessment cycle. For instance, in a bias and uncertainty assessment of a runway incursion scenario without alerts [10], the effect on the risk of the neglect of the pilot not flying of the taxiing aircraft was assessed to be more than 30%. On basis of such insight, it may be considered to explicitly represent in follow-up research the pilot not flying as agent in the model and team situation awareness of the cockpit crew. The results of the current study are derived for a generic runway crossing operation on a taxiway at 1000 m from the runway threshold and do not include an assessment of uncertainty and potential bias in the results.

The results of the Monte Carlo simulations indicate that runway incursion alert systems may lead to a large reduction in conditional collision risk during reduced visibility conditions. Here, ATC runway incursion alerts enable a conditional risk reduction of about one order of magnitude and cockpit alerts enable a conditional risk reduction of about two orders of magnitude. In good visibility conditions, the effectiveness of runway incursion alert systems in reducing the conditional collision risk values is considerably less. Nevertheless, the Monte



Carlo simulations indicate that a significant reduction in the conditional risk can still be attained by cockpit alert systems for situations in which the crew of the taxiing aircraft is lost and aware to be taxiing on a normal taxiway rather than a runway crossing. Since the likelihood of good visibility is typically much larger than of reduced visibility, cockpit alerts may thus also support a considerable risk reduction due to use in good visibility for cases where pilots are lost during taxiing.

References

- [1] ICAO. *Manual for preventing runway incursions*. Doc 9870, AN/463, first edition, 2006
- [2] Eurocontrol. *European action plan for the prevention of runway incursions*, release 1.1. August 2004
- [3] FAA. *Despite significant management focus, further actions are needed to reduce runway incursions*. Report AV-2001-066, 26 June 2001
- [4] Cassell R, Evers C, Esche J, Sleep B. *NASA Runway Incursion Prevention System (RIPS) Dallas-Fort Worth demonstration performance analysis*. Report NASA/CR-2002-211677, June 2002
- [5] Hollnagel E. *Barriers and accident prevention*. Ashgate, Hampshire, UK, 2004
- [6] Hollnagel E, Woods DD, Leveson N (eds.). *Resilience engineering: Concepts and precepts*. Ashgate, Aldershot, England, 2006
- [7] Leveson N. A new accident model for engineering safer systems. *Safety Science* 42:237-270, 2004
- [8] Stroeve SH, Blom HAP, Van der Park MNJ. Multi-agent situation awareness error evolution in accident risk modelling. *Proceedings of the 5th USA/Europe ATM R&D Seminar*, Budapest, Hungary, 2003
- [9] Blom HAP, Stroeve SH. Multi-agent situation awareness error evolution in air traffic. *Proceedings 7th Conference on Probabilistic Safety Assessment & Management*, Berlin, Germany, 2004
- [10] Stroeve SH, Blom HAP, Bakker GJ. Safety risk impact analysis of an ATC runway incursion alert system. *Eurocontrol Safety R&D Seminar*, Barcelona, Spain, 25-27 October 2006.
- [11] ICAO. *Advanced Surface Movement Guidance and Control System (A-SMGCS) Manual*. Doc 9830, AN/452, first edition, 2004
- [12] Reason JT, *Managing the risk of organizational accidents*. Ashgate Publishing Limited, Aldershot, UK, 1997
- [13] Kardes E, Luxhoj JT. A hierarchical probabilistic approach for risk assessments of an aviation safety product folio. *Air Traffic Control Quarterly* 13(3):279-308, 2005
- [14] Eurocontrol. *Air navigation system safety assessment methodology*. SAF.ET1.ST03. 1000-MAN-01, edition 2.0, 2004
- [15] EUROCAE. ED78A *Guidelines for approval of the provision and use of ATS supported by data communication*. 2000
- [16] Wiegmann DA, Shappel SA. Human error analysis of aviation accidents: Application of the Human Factors Analysis and Classification System (HFACS). *Aviation, Space, and Environmental Medicine* 72(11):1006-1016, 2001
- [17] Ale BJM, Bellamy LJ, Cooke RM, Goossens LHJ, Hale AR, Roelen ALC, Smith E. Towards a causal model for air transport safety - an ongoing research project. *Safety Science*, Volume 44, Issue 8, Pages 657-673, 2006
- [18] Sträter O. *Cognition and safety: An integrated approach to system design and assessment*. Ashgate Publishing Limited, Hampshire, England, 2005

- [19] Hollnagel E, Woods DD. *Joint cognitive systems: Foundations of cognitive systems engineering*. CRC Press, Boca Raton (FL), USA, 2005
- [20] Pariès J. Complexity, emergence, resilience... In: Hollnagel E, Woods DD, Leveson N (eds.). *Resilience engineering: Concepts and precepts*. Ashgate, Aldershot, England, 2006
- [21] Wooldridge M, Jennings N. Intelligent agents: Theory and practice. *Knowledge Engineering Review* 10(2), 1995
- [22] Panait L, Like S. Cooperative multi-agent learning: The state of the art. *Autonomous Agents and Multi-Agent Systems* 11: 387-434, 2005
- [23] Blom HAP, Bakker GJ, Blanker PJG, Daams J, Everdij MHC, Klompstra MB. Accident risk assessment for advanced air traffic management. In: Donohue GL and Zellweger AG (eds.), *Air Transport Systems Engineering*, AIAA, pp. 463-480, 2001
- [24] Blom HAP, Daams J, Nijhuis HB. Human cognition modelling in air traffic management safety assessment. In: Donohue GL and Zellweger AG (eds.), *Air Transport Systems Engineering*, AIAA, pp. 481-511, 2001
- [25] Blom HAP, Stroeve SH, De Jong HH. Safety risk assessment by Monte Carlo simulation of complex safety critical operations. In Redmill F, Anderson T (eds.), *Developments in risk-based approaches to safety*, Springer-Verlag, London, 2006
- [26] Everdij MHC, Blom HAP, Stroeve SH. Structured assessment of bias and uncertainty in Monte Carlo simulated accident risk. *Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management*, May 14-18 2006, New Orleans, USA
- [27] Endsley MR. Towards a theory of situation awareness in dynamic systems. *Human Factors* 37(1): 32-64, 1995
- [28] ESSAI project team. *Orientation on situation awareness and crisis management*. National Aerospace Laboratory NLR, Report NLR-TR-2000-668, 2000.
- [29] Rousseau R, Tremblay S, Breton R. Defining and modeling situation awareness : A critical review. Banbury S, Tremblay S (eds.), *A cognitive approach to situation awareness: Theory and application*, pp. 3-21. Ashgate, Aldershot, UK, 2004
- [30] Wickens CD, Holland JG. *Engineering psychology and human performance*. Prentice-Hall, Upper Saddle River (NJ), USA, 2000
- [31] Everdij MHC, Klompstra MB, Blom HAP, Klein Obbink B (2006b). Compositional specification of a multi-agent system by stochastically and dynamically coloured Petri nets. In: Blom HAP, Lygeros J (eds.), *Stochastic Hybrid Systems*, LNCIS 337, Springer-Verlag, pp. 325-350