Reliability Engineering and System Safety 140 (2015) 37–52

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

The risk of an air accident as a result of a serious incident of the hybrid type

Jacek Skorupski [1]

Warsaw University of Technology, Faculty of Transport, Warszawa, Poland

ARTICLE INFO

Article history:
Received 12 September 2014
Received in revised form
16 March 2015
Accepted 21 March 2015
Available online 31 March 2015

Keywords:
Air traffic safety
Incidents and accidents analysis
Petri net model

ABSTRACT

Safety in air traffic is a multilayered concept and consists of many safety barriers. The practical side of increasing safety is mainly based on analysing the causes of accidents and incidents. This analysis leads to finding gaps in the safety structure and to developing corrective recommendations in order to eliminate them. In this paper we indicate that this practice is insufficient. Most incidents could transform into accidents with fatalities. The standard method of investigating incidents does not answer the question as to whether safety barrier is permanent or whether it was activated accidentally. This paper proposes a new method for analysing incidents aimed at finding their consequences rather than their causes. This makes it possible to find areas that need improvement. Stochastic, timed, coloured Petri nets were used for the analysis. There are three types of air traffic incidents, distinguished according to events that lead to a transformation of an incident into an accident: causal and temporal. The hybrid case, in which both types are important, has been discussed in detail. The method is useful in evaluating the current level of safety in air traffic. Applicability of this method has been shown on the example of the runway incursion problem.

1. Introduction

Safety in air traffic is a multilayered concept and consists of many safety barriers: organisational, technical and procedural barriers. Their task is to protect participants of the transport process from events with potentially catastrophic consequences. Traffic accident investigations are conducted in terms of searching for the reasons and circumstances that were favourable for these events. The present studies were carried out within the existing organisational structures that make use of well-established and legally sanctioned methods and procedures ([20,32]), which are directed at determining the causes of accidents and making preventive recommendations aimed to eliminate them, and indirectly to prevent the occurrence of analogous events in the future. Of course, incidents (serious incidents) are also examined in the same way. This examination of incidents, as is the case for accidents, is focused on searching for the reasons why they occurred.

In this paper a new method of traffic incident analysis is proposed. This method is based on an exploration of the possible scenarios for the development of an incident and on checking what other effects it could bring about. This approach allows us to evaluate and to verify whether any particular case of an incident that did not transform into an accident was the result of hedging activities or whether this was pure coincidence. In the latter case one should suggest preventive recommendations relating to those scenarios that did not actually occur. In other words, there is a common belief that safety barriers will work forever and that they will work in slightly different circumstances, such as worse weather conditions or worse technical conditions of the vehicle, etc. However, the fact that the safety barriers worked during a particular incident does not guarantee that they will work in any other case. This applies especially to complex systems working in the long time horizon, assuming that they can be subjected to threats which we are currently not even able to imagine. A similar approach is presented in works on resilience engineering [30,11]. A somewhat similar approach was recently presented by Khakzad et al. [38].

In this paper we propose a quantitative analysis of scenarios in which serious incidents could have transformed into accidents but did not do so. The proposed approach is illustrated by air traffic examples. Due to the special role of airports in logistics chains, the analysis was carried out for an aerodrome traffic incident. The studied case belongs to the class of so-called Runway Incursions (RIs). The International Civil Aviation Organization (ICAO) defines these as "any occurrence at an aerodrome involving the incorrect presence of an aircraft, vehicle or person on the protected area of a

E-mail address: jsk@wt.pw.edu.pl
[1] Warsaw University of Technology, Faculty of Transport, ul. Koszykowa 75, 00-662 Warszawa, Poland. Tel.: +48 22 234 7339.

http://dx.doi.org/10.1016/j.ress.2015.03.031
0951-8320/

surface designated for the landing and take-off of aircraft" ([33]). The most common RI types are:

- take-off without the air traffic controller's (ATC) permission
- aircraft runway crossing after landing contrary to ATC clearance
- issued ATC taxi clearance in conflict with other ATC clearance
- unauthorised runway incursion of people, vehicles or animals.

There are many factors that affect this type of event, e.g. weather, the airport's configuration, conditional control clearances, simultaneous use of intersecting runways, phraseology, the use of several languages for controller-pilot communication, workload, etc. It constitutes a broad class of occurrences, with possible consequences of a most serious nature, thus much attention in the activities of organisations responsible for the safety of air traffic is devoted to it. According to Eurocontrol statistics for the period 2008–2011, the number of RIs was close to 0.06 per 10,000 flights [18,19]. According to the U.S. FAA (Federal Aviation Administration) ([23]), in the airspace of the United States from 2004 to 2007, 1353 RIs were recorded for about 248 million take-offs and landings, which gives an average of $5.46 \cdot 10^{-6}$ per flight, i.e. a similar likelihood of this phenomenon as in Europe.

The current strategy of the European Aviation Safety Agency (EASA) is to focus on five key operational problems in air traffic—the so-called "top five". These also include runway incursions (RIs). The analysed incident that is a typical representative of the RI category applies to taxiing against ATC permission along with crossing a runway that is in use. Contributory factors are also typical, such as outdated maps, poor situational awareness and communication errors. The proposed method can be applied to a whole runway incursion class of occurrences. It can be used not only for error detection but also for error recovery [40].

In Europe, EUROCONTROL Safety Regulatory Requirements (ESARRs) have been developed which discuss various aspects that affect the overall level of safety in air traffic. The European Organization for the Safety of Air Navigation EUROCONTROL has undertaken efforts to develop standardised methods and tools of risk management, particularly to determine the acceptable (tolerable, target) level of safety [16]. At present, the ESARR regulations are a part of the European Community Law, thus they have increased legal effect. This has been possible thanks to the Single European Sky (SES) initiative and to transposition works performed mainly in the years 2007–2011. The European regulations [21] divide events with the participation of ATM (Air Traffic Management) into five categories:

- accidents, which include: mid-air collisions, collisions on the ground, controlled flight into terrain (CFIT), total loss of flight control
- serious incidents: a significant loss of separation (separation of less than half the allowable minima), and neither the crew nor the air traffic controller is able to recover from the situation, cases when the aircraft changes its flight path in such a way that in order to avoid a collision an abrupt manoeuvre is required
- major incidents: a significant loss of separation, but with the crew or the ATC controlling the situation, a minor loss of separation (separation greater than half the minima), with the crew and the controller unable to recover from the situation
- significant incidents: an increase in the workload of air traffic controllers and flight crew, a minor loss of separation, with the crew or ATC controlling the situation and fully able to recover from the situation
- incidents without direct impact on safety.

Regulations [21] require that member states determine the current level of safety (CLS) and then make their evaluations by comparing them to the target level of safety (TLS). TLS and CLS are usually defined as the quotient of the number of accidents divided by the number of flight hours or, simply, the number of flights [17]. These regulations define the tolerable level of risk just for the "accidents". If the current level of safety is worse than the TLS, one must propose solutions to improve it. At the moment, TLS is understood as the maximum value of the probability of an accident; for commercial aircraft it was adopted as being equal to $1.55 \cdot 10^{-8}$ accident on a flight hour, or $2.31 \cdot 10^{-8}$ accident on a flight [17]. CLS forecasts should be made with respect to any change (technical or organisational) in the air traffic management system. The task of determining the current level of safety can be difficult in practice. For small- or medium-sized countries the annual number of operations is small and the number of accidents per year is often zero (or at most a few). This prevents accurate determination of CLS.

One method of solving this problem is to determine the level of safety on the basis of data on air incidents which are obviously more frequent than air accidents [14]. Unfortunately, the target level of safety for that category of events has not been specified. It has been planned that the standard will be defined in the future, but it is not certain whether such a standard could be practically accepted as air traffic incidents are very different in nature and the severity of effects is also different. Also, the combined examination of all incidents prevents one from understanding the real causes that led to them.

Another method is to treat a serious incident as "a partial accident". By knowing the number of serious incidents and the likelihood of their transformation into accidents we can estimate the number that might be called the expected value of the number of accidents. The method of incidents analysis as proposed in this paper allows one to estimate the probability of the transformation of an incident into an accident.

The latter method is based on the number of serious incidents and the likelihood of their transformation into accidents. The objective of this paper is to develop a new method for the analysis of incidents—focused on exploring the consequences and not the causes. An accident model is created based on the model of a real incident and by taking incident development scenarios into account. Its analysis allows us to estimate the probability of the conversion of an incident into an accident as well as the probability that the scenario will take place.

The work is structured as follows: Section 2 briefly presents the specificity of the problem of air traffic safety in the vicinity of an airport. Also, some works on the modelling of traffic safety in the airport area are discussed. This section provides a classification of major incidents in transport into three groups along with references to literature and a selection of serious incidents with hybrid characteristics as the object of interest in this work; Section 3 presents an overview of the Petri nets; Section 4 describes the method of analysing the likelihood that a serious incident will turn into an accident; Section 5 presents a comprehensive example of applying the proposed method of analysis. Real data from a serious air traffic incident which occurred in 2006 at Warsaw Chopin Airport was used for this purpose. Petri nets modelling the actual incident and also the accident into which the incident could be transformed were shown. Results of the simulation research of the model is discussed; Section 6 provides a summary and the conclusions.

2. Airport traffic safety modelling—Literature review

2.1. Airport operations and air traffic control

The airport is a separate area on land, water or another surface which is intended for the arrival, departure and surface movement

of aircraft. The airport is a complex object of clearly distinguished elements and the relationships between them, therefore it is a system. The area of the airport is the part of controlled airspace in which the majority of the flight operations is concentrated in.

Airport traffic includes all operations related to aircraft landing, taxiing, ground handling, taxiing again and take-off. Landing is a series of transition operations moving the aircraft from flight to ground operations. Touchdown is followed by the roll on the runway where speed reduction takes place. When the speed is adequate, taxiing on the taxiway to the apron occurs. The taxiway provides a connection between certain parts of the airport, usually between the aprons and places of access to the runway. After the ground service, the aircraft commander reports to the tower control (TWR) as ready for take-off. After receiving clearance, the aircraft performs taxiing. Then, the aircraft receives permission for line-up on the runway and subsequently receives clearance for take-off. Next, take-off and the climb take place. After reaching a height of 2000 ft, control of the aircraft is transferred to an area control centre (ACC).

Safe organisation and management of the take-off and landing operations are the responsibility of the tower control (TWR). In full configuration, the TWR consists of four positions ([33]):

- TWR controller—the controller ensures separations between aircraft on approach as prescribed by the regulations, he/she provides pilots with ACC permissions to perform the flight and allows take-offs and landings to take place
- Ground controller (GND)—is responsible for the ground movement of aircraft within the taxiways and runways
- Tower flight data controller—arranges the exchange of information with other supervisory authorities and in consultation with the TWR controller supports the movement of ground vehicles at the airport
- Delivery controller—with access to the flight plans database he/she receives permission from the ACC and provides it to the flight crew.

2.2. The causes of incidents and accidents

As has been shown by numerous examples, airport traffic is so complex and so dependent on many unpredictable factors that accidents will sometimes occur in this area. One of the major causes of the problems is the pilot and controller workload [46] so the CD&R (Conflict Detection and Resolution) systems are progressively implemented [58]. It is affected by many contributing factors, and avoidance of such events is a major challenge for all services supervising the air traffic in the airport. The main problems in their work are:

- a large number of objects that must be managed, which forces the distribution of tasks between several services—inadequate coordination of their activities is often the cause of an air incident [68]
- the crucial role of a human who, acting under conditions of a shortage of time or under stress, makes mistakes arising from shortcomings in training [24,25], sensory deficiencies, the inability to correctly process an excessive number of signals and information [1]
- the large dynamics of events which make the time to work out a decision and to carry it out very short and the consequences of even small mistakes—huge
- the variety of objects under management—aircraft, vehicles, or ground maintenance equipment.

A major challenge for the safety of airport traffic has been the increasing range of implementations of automated systems. In [4] the acceptable level of automation was analysed. This approach increases the chances of effective implementation of automated support systems in air traffic management. One of the most serious causes of incidents and accidents is the human factor. In [39], cases of similar mistakes made by controllers were examined. It was found that a systemic approach needs to include human and organisational considerations as well as technical and procedural ones [10]. If not, the problem, or even a more complex variant, is likely to recur. Similar results were obtained in [60,49].

2.3. Methods of air traffic events modelling

Numerous attempts have been undertaken to develop effective models of airport elements which would enable an analysis of the impact of various organisational activities on the safety of airport traffic. These use various methods of mathematical modelling, which include, among others, dynamical programming, fuzzy sets, queuing models, and hierarchical Bayesian models. In [12], a dynamic programming approach was used for airport capacity allocation. In [31], hierarchical Bayesian modelling was used to gain a better understanding of the impact of new safety measures on mitigating rare and extreme events. An interesting approach to the problem of modelling airport operations was presented in [50]. On the basis of the fuzzy sets theory, a model for determining runways in use was elaborated. It could help controllers evaluate their own solutions or provide suggestions of new solutions to this problem. A multi-criteria analysis of the causes of a serious air traffic incident was presented in [63]. An interesting attempt to analyse airport traffic safety was presented in the work [2]. The location and consequences of accidents were studied, and in particular aircraft overruns, veer-offs, and obstacle striking.

2.4. Petri nets in air traffic processes modelling

Convenient tools for analysis of traffic processes in transport are Petri nets. Some examples in airport safety analysis include [9,53,69]. Most of them, however, concerns the modelling of en-route air traffic [51,52,45,3]. The general approach to using coloured Petri nets in modelling aircraft operations can be found in [22]. In [53], a model of forward-looking planning of the arrival process at the airport is presented. It is implemented in CPN Tools (as in the current study), thus indicating the usefulness of this package in simulation analysis of air traffic in the vicinity of the airport. A similar issue has been discussed in [6], where the authors present the Petri net to model simultaneous instrument approaches on the converging runway combination 19R and 22 at Schiphol. Coloured Petri nets with the use of the CPN Tools package were also used to model one-runway operations in [41], which was continued in [42]. Stroeve et al. [65,66], used Petri net modelling for risk assessment of runway incursion scenarios. A similar approach was implemented in [26]. Petri nets were also used to represent human factors problems during accident analysis [37].

Petri nets have also been used to analyse various aspects of traffic problems in other modes of transport. In [59], the general concept of modelling traffic processes in transport was described. Similarly, for instance [27] dealt with maritime traffic, and [34] with rail traffic.

2.5. Modelling tool—CPN Tools 4.0

In this paper an analysis was carried out using the CPN Tools 4.0 package [54,70,36]. It allows for easy simulation of the model in the form of a Petri net. By using monitors (connected with transitions or places) provided by this package it was possible to record a number of characteristics of the system that were necessary for determining the likelihood of an incident–accident

transformation. CPN Tools is gaining increasing recognition among researchers using Petri nets. This is mainly because it offers a combination of graphical network editor, simulator and analysis capabilities in the state space. CPN Tools also allows to create a hierarchical network with multiple page synchronisation mechanisms. Additionally, it supports REAL and TIME colour sets and has good support for timed analysis. CPN Tools uses the CPN ML language to specify declarations and net inscriptions. This language is an extension of the functional programming language Standard ML that was developed at the University of Edinburgh. From the point of view of modelling incidents of the hybrid type (as in this paper), CPN Tools 4.0 provides an excellent tool that allows one to easily take into account both the dynamic nature of events and also static logical conditions. This is a key feature of the method proposed in this paper.

2.6. Quantitative analysis of air traffic incidents

The problem of investigating incidents and accidents was analysed in [64]. It was noted that contemporary methods of analysing the causes of accidents are not fully proactive. More general comments on the lessons to be learned from accident analysis can be found in [44]. Roelen et al. [56] suggested the need to use multiple methods simultaneously. Building a model that represents possible causal event sequence scenarios that include technical, human and organisational factors is a huge task and requires a combination of detailed knowledge of all aspects of the system, the processing of huge amounts of data, a substantial mathematical background and the ability to capture all of this in a user-friendly software tool to be used by safety analysts [65,66]. Recently, Ford et al. [24,25] analysed some issues regarding the instrumentation and monitoring of surface movements to determine the symptoms of increased collision potential. Similar work on monitoring movements was conducted at Heathrow [29].

While analysing the risk of occurrences with the use of an event tree or a fault tree there are many elements whose probabilities we do not know [67]. In addition, events are dependent on one another, which makes analysis more difficult. In the literature we can find many attempts to determine the likelihood of an accident, including the use of Petri nets. The most developed method in this area is the method of risk analysis called TOPAZ [5,7]. This method allows for a quantitative analysis of the process leading up to the accident. It is a safety assessment methodology designed for the evaluation of existing or future ATM operational concepts. It is based on a stochastic modelling approach. The main idea is to assess accident risk in a cycle that consists of four sequential stages, i.e. identification of operation and hazards, mathematical modelling, accident risk assessment, and feedback to operational experts.

2.7. Types of air traffic incidents

If we look at the reports of committees investigating the causes of traffic incidents which occurred in the vicinity of airports (in procedures of taxiing, take-off, approach and landing), we will see that there are three main types of air traffic incidents. This division was made with regard to the nature of the factors necessary to transform an incident into an accident. Determining these factors is a typical element of the report prepared by an accident investigation committee.

1. Incidents in which the conversion of an incident into an accident depends on the occurrence of certain events. This group includes those incidents in which all temporal sequences indicate the occurrence of an accident, but the activation of a safety barrier prevents it from happening. In the case of such incidents, the most efficient method of research is analysis of the event tree (ETA), which allows to specify scenarios leading up to the accident and then to determine the probabilities of these scenarios. This method was used in [61], where usefulness of Petri nets for an analysis of similar cases was shown. In a situation where some of the events in the tree are related to human error, we have to determine their likelihood by using expert judgment [57]. This leads to an uncertainty, mainly of a linguistic nature, which can lead to searching for solutions in the field of fuzzy systems [15]. Such an approach, based on an analysis of event trees with fuzzy probabilities, was used in [47]. It has been shown that elimination of one of the safety barriers leads to an accident. Moreover, the fuzzy probability of such an elimination was calculated. It was pointed out that, unfortunately, the recommendations arising from the standard procedure of searching for the causes of incidents do not relate at all to this important issue.
2. Incidents in which the conversion into an accident depends on a favourable or unfavourable time sequence, whereas all the premises necessary for the accident have, in fact, taken place. This case was analysed in [62]. In this example of an air traffic incident a fundamental role is played by time dependencies. The probability that two aircraft taking off will be at an intersection of the runways is in this case equal to 1. Only the time when they reach this point decides whether an accident will occur or not. In [62], both analytical and simulation methods for determining the probability of an accident were shown.
3. Incidents of a hybrid nature in which the conversion of an incident into an accident needs both the existence of a sequence of additional events and some specific time dependencies between events. This is the general case and will be discussed in detail later in this paper.

3. Petri nets

In many types of systems, Petri nets provide a convenient way of analysis. Many applications may be found in software engineering where they are used particularly to describe concurrent systems. There is a large range of literature on this subject, e.g. [55,35,13], which also contains an extensive bibliography of the topic. In this paper an example of using Petri nets for modelling air traffic safety problems is shown, but a similar approach can be applied to other modes of transport.

The basis for building a Petri net is a bipartite graph containing two disjoint sets of vertices called places (designated by circles) and transitions (rectangles). The arcs in this graph are directed. A characteristic feature of the graph used in Petri nets is that the arcs have to combine different types of vertices. Below are presented brief definitions of timed and coloured Petri nets used in this paper.

A *timed Petri net* (TPN) is described as [48]:

$$S_T = \{P, T, I, O, H, \tau, M_0\} \tag{1}$$

where P—set of places, T—set of transitions, $T \cap P = \varnothing$, I, O, H, are functions, respectively, of input, output and inhibitors, $I, O, H: T \to B(P)$, where $B(P)$ is the superset over the set P.

Given a transition $t \in T$, it can be defined as:

$t^+ = \{p \in P : I(t,p) > 0\}$—input set of transition t
$t^- = \{p \in P : O(t,p) > 0\}$—output set of transition t
$t^o = \{p \in P : H(t,p) > 0\}$—inhibition set of transition t
$\tau : T \to \mathbb{R}_+$—delay function, specifying static delay $\tau(t)$ of transition t

$M_0 : P \to \mathbb{Z}_+$ is the initial marking, i.e. a function assigning an integer to a place. We also say that the marking specifies the number of tokens assigned to each of the places. Initial marking, along with the rules governing the dynamics of the net, i.e. the

rules of marking changes, determine all possible reachable markings.

Transition t is called active in marking M if and only if:

$$\forall p \in t^+, \qquad M(p) \geq I(t,p) \wedge \forall p \in t^o, \qquad M(p) < H(t,p) \tag{2}$$

Firing of transition t, active in marking M, removes from any place p belonging to the set t^+ as many tokens as function $I(t,p)$ determines. At the same time it adds to any place p from the set t^- as many tokens as determined by the $O(t,p)$ function. This means the firing of transition t will change actual marking to M' such that

$$M' = M + O(t) - I(t) \tag{3}$$

This relationship is written briefly $M[t\rangle M'$. We then say that M' is reachable directly from M. If the $M \to M'$ transformation requires firing a sequence of transitions σ, then we say that M' is reachable from M and denote $M[\sigma\rangle M'$.

Characteristics on transitions may determine the time associated with the firing of the transition in different ways. In particular, this value may be described by a deterministic or a random variable with a given probability distribution. In the latter case we can talk about the stochastic network.

Coloured Petri nets (CPNs) have the ability to define tokens of different types. A token type is called a colour. Each place in the coloured net is assigned a set of colours that it can store. Expressions are assigned to arcs and transitions that allow to manipulate various types of tokens. It is possible to combine the idea of CPNs and TPNs.

The airport traffic model presented in this paper can therefore be written as

$$S_{AT} = \{P, T, I, O, H, M_0, \tau, X, \Gamma, C, G, E, R, r_0, B\} \tag{4}$$

where $M_0 : P \to \mathbb{Z}_+ \times R$—initial marking, $\tau : T \times P \to \mathbb{R}_+$—delay function, specifying the static delay $\tau(t)$ of transition t moving tokens to place p, $X : T \times P \to \mathbb{R}_+$—random variable, describing the random time of carrying out transition t leading to place p, Γ—nonempty, finite set of colours, C—function determining what colour of tokens can be stored in a given place: $C : P \to \Gamma$, G—function defining the conditions that must be satisfied for the transition before it can be fired; these are the expressions containing variables belonging to Γ, for which the evaluation can be made, giving as a result a Boolean value, E—function describing the so-called weight of arcs, i.e. expressions containing variables of types belonging to Γ for which the evaluation can be made, giving as a result a multiset over the type of colour assigned to a place that is at the beginning or the end of the arc, R—set of timestamps (also called time points) closed under the operation of addition, $R \subseteq \mathbb{R}$, r_0—initial time, $r \in R$, $B : T \to \mathbb{R}_+$—function determining the priority of transition t; this function applies only for transitions that are simultaneously active; in this situation a free choice of transition to be fired is possible.

In the presented method of analysis the most important property of the Petri net is the reachability of selected states (markings) from the initial marking M_0. It allows to assess the probability and time of transition to those selected markings. Particularly important are the dead markings because they illustrate the final situations in which we can assess whether the traffic process will result in a collision or the traffic process was safe. This allows to quantify the probability of an accident and thus the level of traffic process safety.

In the following sections of the paper the term "marking" and "state" will be understood as synonyms and will be identified with the nodes of the reachability graph.

As was mentioned earlier, reachability graph G is the basic tool for quantitative analysis of the safety of traffic processes in transport as modelled by using Petri nets:

$$G = \langle M, T, S \rangle \tag{5}$$

where M—set of nodes reachable from the initial marking M_0, corresponding to the Petri net markings (states of the traffic process), T—set of arcs illustrating direct reachability between markings, labelled by the names of the transitions, S—ternary relation $S \subseteq M \times T \times M$, satisfying the condition.

$$\forall (M_1, t, M_2) \in S : \; M_1[t\rangle M_2 \tag{6}$$

This graph often contains an enormous number of states, which makes it difficult to analyse, thus its reduction is necessary. The method of construction of the reachability graph will be presented based on an example of a simple Petri net as shown in Fig. 1. This net is used only to illustrate the process of creating the reachability set and reachability graph. It is in no way connected with the example of the incident discussed later in this work. The places $P = \{P1, \ldots, P8\}$ are marked as circles, and transitions $T = \{T1, \ldots, T7\}$ as rectangles. White rectangles stand for timed transitions which are characterised by their duration. Black rectangles are immediate transitions. The Petri net is coloured, so each place has a specific colour that it can store. Set Γ is equal to $\{A = \mathbb{R},\ B = \mathbb{Z}_+,\ C = \mathbb{Z}_+\}$. This example of the Petri is TPN with timestamps connected with tokens.

The set of all possible states, called the reachability set, corresponding to this net is presented in Table 1. For each marking, places having tokens are specified, and so is the number of tokens; for example, for marking M_4 notation $p_2 + p_3 + 2p_7$ means that the state M_4 corresponds to a situation in which there is one token in each of the places p_2 and p_3 and there are two tokens in place p_7. In addition, for each

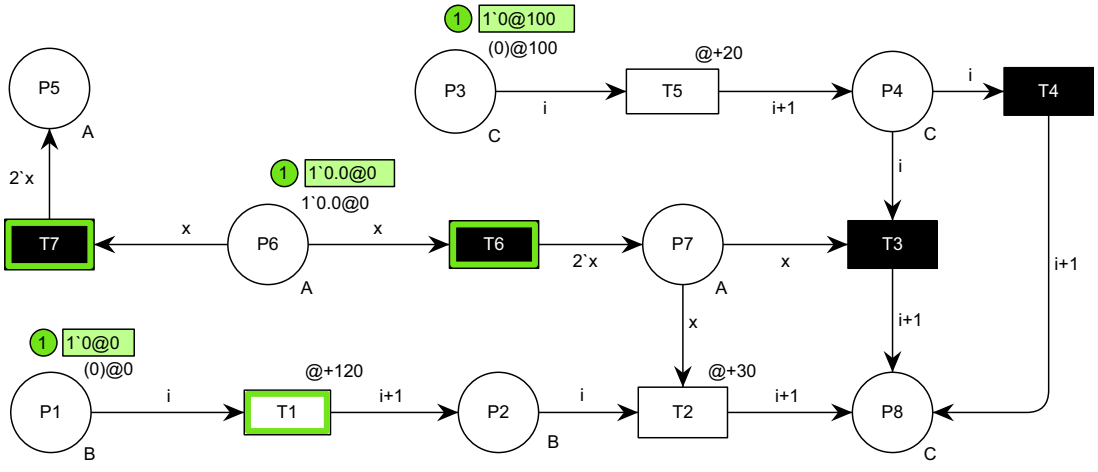

Fig. 1. Example of a coloured, timed Petri net.

marking its liveness are determined. Dead states are marked with the letter D. These are states in which no transition is enabled. They are particularly important in a quantitative analysis of the safety of traffic processes as they allow to assess the effects of a given scenario of the development of a traffic situation.

The reachability graph corresponding to the example Petri net is shown in Fig. 2. The essence of this graph is to determine which transition needs to be fired in order for the system to change from one marking to another. Vertices that do not have successors correspond to dead states.

4. Method of incident analysis

As is widely known, air traffic occurrences are almost always the result of a combination of many different factors. During the development of a dangerous situation in time there are also inhibitory factors that hinder or prevent this process. Preliminary analysis of various air traffic occurrences indicates that for events classified as serious incidents there would be sufficient occurrence of only one additional conducive factor or the termination of only one inhibiting factor and a serious incident could have become an accident. There are also incidents where all factors determining the existence of the accident are present and only a lucky time sequence of events causes that that accident in fact does not occur. Such incidents may also be evaluated against the probability of becoming accidents with the use of the method introduced in this paper. This is possible through the use of timed, coloured Petri nets.

4.1. Purpose and scope of the analysis

The method presented in this paper is based on analysing only those additional factors or time dependencies that determine transformation from serious incident into the accident. We do not need to consider events and scenarios (and their probabilities), which led to a serious incident. Because serious incident had occurred! These events are usually several dozen, many of them related to the human factor and very difficult to determine. A characteristic feature of a serious incident is, that its transformation into an accident requires only additional one or two events. And only the probability of that one or two events requires the calculation. This definitely reduces the scope of analysis and also reduces the uncertainty of risk estimation. At the same time this approach is adequate to achieve the goals of analysis, i.e. to determine the probabilistic dependencies between a serious incident and an air accident. As a result of finding such a relationship it would be possible to estimate the number of accidents just on the basis of knowing the number of incidents.

Table 1
Reachability set for an example Petri net.

M_0	$p_1+p_3+p_6$		M_1	$p_2+p_3+p_6$		M_2	$p_1+p_3+2p_7$	
M_3	$p_1+p_3+2p_5$		M_4	$p_2+p_3+2p_7$		M_5	$p_2+p_3+2p_5$	
M_6	$p_2+p_4+2p_7$		M_7	$p_2+p_4+2p_5$		M_8	$p_2+p_7+p_8$	
M_9	$p_4+p_7+p_8$		M_{10}	$p_2+2p_7+p_8$		M_{11}	$p_2+2p_5+p_8$	D
M_{12}	$2p_8$	D	M_{13}	p_7+2p_8	D			

4.2. General assumptions

1. We analyse only serious air traffic incidents that are characterised by only one additional adverse event that would be necessary to cause an accident. We do not study the probability of occurrence of an incident but the probability of its transformation into an accident. By knowing the number of serious incidents and the likelihood of their transformation into an accident, one can estimate the expected number of accidents.
2. Each incident that is analysed can be classified into one of the pre-defined causal groups.
3. We have a description of the time dependencies of the activities of individual participants of the event.
4. Adverse development of the events could in a real situation lead to an accident instead of an incident.
5. A hybrid case is considered. It is one in which the transformation of an incident into an accident needs additional events of a logical nature and a specific time sequence of events.

4.3. Representation of air traffic processes by a Petri net

The following methodology of analysing air traffic processes in terms of Petri net elements was adopted:

(a) The set of places P corresponds to traffic situations in which a plane can be found during normal traffic. These situations refer both to the location of the plane in the airspace as well as to the issue of specific permits (clearances). Set P may include, e.g. situations such as: aircraft ready for take-off, occupied runway, plane at the intersection of runways, taxiing started, etc. Additional elements of this set are situations describing the state of the environment, such as: less than 400 m of visibility, ATC controller is busy, the pilot of another aircraft is watching the situation on the manoeuvring area, etc. The traffic situation may relate to a single aircraft which is modelled with the occurrence of a single token in place $p \in P$. It may also involve many planes simultaneously; then the number of aircraft is modelled with

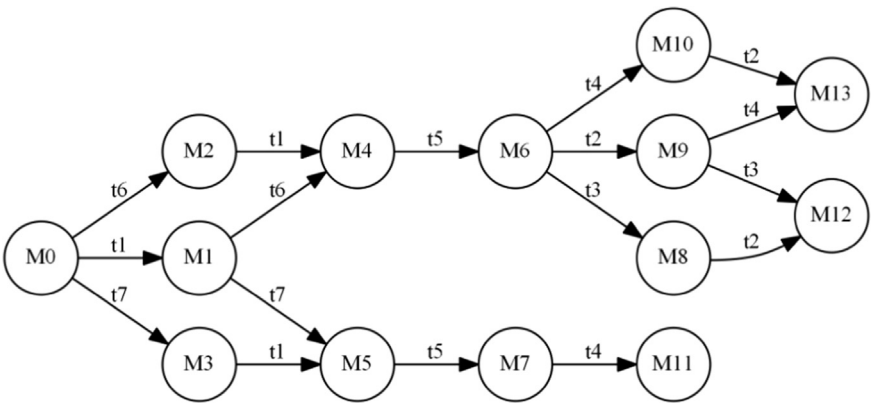

Fig. 2. Reachability graph for an example Petri net.

more tokens ($M(p) > 1$). Since the traffic situation refers to a specified airspace which has limited capacity, places in the model will be characterised by capacity K.

(b) The set of transitions T corresponds to the set of events (actions) that change the traffic situation, particularly affecting the safety of manoeuvres. These are events such as: ATC controller allows for take-off, plane taxiing on a certain taxiway, plane does not stop the actual manoeuvre. These events can be characterised by two values: the time of their duration and the priority, defined by the probability of events taking place that can occur simultaneously. Activation of transition depends on the presence of an adequate number of tokens in the input places but may also depend on the occurrence of certain additional conditions, particularly those characterising the time of appearance of tokens in the input places. The rules of activation and firing of transitions determine the dynamics of the researched process. In this case a stochastic Petri net was used. The term "stochastic" means that the time delays occurring in the net are partially random values of given probability distributions; the network structure itself, however, is deterministic.

(c) The input function I defines traffic situations that determine the occurrence of certain events. Output function O defines what event (action) must occur to change the status of the analysed system, and the inhibitor function H specifies traffic situations that must not exist in order for certain events to occur. In many cases, functions I and O take values that are greater than 1, which means that not only is the existence of certain traffic situations necessary, but also the fact that a sufficient number of objects take place in these situations. This is signalled by a sufficient number of tokens in specified places of the net.

(d) The initial marking M_0 defines the traffic situation in which we begin the analysis, and the current marking M describes the current state of the system (process). If the time dependencies play a significant role in traffic situation development, the marking must be supplemented by a timestamp for each of the tokens. The existence of different types of objects (e.g. aircraft of different weight categories) determines the use of a coloured Petri net, thus of tokens of different colours. In this case, traffic situations (places of the net) must also be characterised by the type of token.

An analysis which aims to determine the probabilistic relationship between a serious incident and an accident in air traffic may proceed along two lines:

1. Based on the structure of the corresponding Petri net, by modelling the investigated serious incident and hypothetical accident, one can determine the reachability graph. Its analysis allows for an analytical determination of the desired probability.
2. Simulations of a serious incident represented by a Petri net along with recording the probability of staying in different states of the system. In particular, it may be interesting to observe how often the system passes to the so-called dead markings which correspond to the transition of an incident into an accident. This frequency will give the searched probability.

4.4. The algorithm of the method

The overall algorithm of the method is as follows:

1. Creation of a model of a serious air traffic incident as a Petri net. It is necessary to take into account all of the events (leading to or inhibiting the incident) and the time relations between them. Proper determination of the time sequence of these events can be obtained by:
   a. Defining the time of transition firing as a deterministic value corresponding to the actual duration of the modelled events
   b. using inhibitor arcs or transitions priorities; they do not allow the firing of transitions before a specified physical situation is completed, i.e. until another traffic event occurs
   c. a combination of both methods.
2. Reduction of the network, which consists in eliminating places and transitions that do not affect the transformation of the incident into an accident. Arcs that are adjacent to the removed places and transitions are also removed. This step in the method allows for a significant reduction in the number of states considered in the later stages.
3. Determining scenarios transforming an incident into an accident. These scenarios must take into account both the appearance of additional events and the absence of inhibiting events. Scenarios selection is important for the method, as scenarios should recognise hardware failures, wrong decisions on the part of the controller and pilot, failure to comply with controller recommendations, lack of situational awareness, and adverse environmental conditions, including the weather. On the other hand, one should not unduly expand the area of analysis beyond factors that are closely related to the incident and process of its transformation into an accident.
4. Creation of a model of an accident by taking into account reduction of the network and all the possible scenarios as defined in step 3. This step requires the identification of nodes and arcs that must be added to the network. For newly added elements it is necessary to determine their characteristics, among others:
   a. for places—capacity, colour, initial marking
   b. for transitions—firing conditions, execution time
   c. for arcs—weights and characteristics depending on the type of network, particularly those that are important for the coloured network.

   In this step of the algorithm one should also consider which elements of the network are to be stochastic and one should take into account the relevant characteristics of random variables of the transition execution time. The aim of this procedure is mainly randomisation of the time sequence mentioned in step 1 of the algorithm. Besides introducing the random component to the time of transition firing, also the removal of most inhibitor arcs serves this purpose. The last part of this step of the algorithm is to determine the initial marking M_0.
5. Determining the reachability set and the reachability graph of the developed Petri net. This step of the algorithm is also a part of the model validation. It is necessary to check whether for all dead states it is possible to determine if there has been a transformation of an incident into an accident. If not, we are dealing with a situation that requires a return to step 4 of the algorithm and we need to re-examine the structure of the network in order to eliminate any errors.
6. Extraction of system states which represent a transformation of an incident into an accident. It is recommended to form a structure of the model in such a way that it will not be possible to continue firing transitions at a time when it is already known that in the course of the simulation the accident occurred or that the conversion of an incident into an accident is impossible. In other words, it is recommended to achieve a situation where the final states of analysis will be dead states.
7. Reduction of the reachability graph which is necessary in the case of analytical approach.
8. Analytical or simulation determination of the total probability of reaching states representing the accident. In this paper we use a simulation method involving repeated execution of the simulation experiment. The frequency of reaching the accident

markings is the desired probability of a serious air traffic incident transformation into an accident.

5. Example—Serious air traffic incident no. 270/06

A serious incident that took place in September 2006 at Warsaw Chopin Airport will be presented as an example to illustrate the method of analysis. Two aircraft, Airbus A320 and Embraer EMB170, were the participants, and the cause of the incident was classified as a "human factor" and causal group H4 —"procedural errors". All of the circumstances of the incident, the activities of the pilots and ATC services and the time dependencies between the events are described in the protocol of the Commission examining the causes of the incident [8].

5.1. Description of the circumstances of the incident

The crew of the Airbus (A320) was approved by ground controller GND to taxi via taxiway A, then taxiway E to the runway threshold RWY 29 (Fig. 3). The pilot acknowledged the permission properly, but then taxied incorrectly, i.e. by taxiway A4 straight to the runway, rather than turning left into taxiway E1 and then via taxiway E2 and E3 to the runway threshold. At the same time the Embraer aircraft (EMB170) began take-off on runway RWY 29. Taxiing by A4 resulted in a safety hazard for take-off on runway RWY 29. In this situation the airport tower controller TWR issued the command to stop to the EMB170 crew. The same decision was made by the ground controller for A320. Both crews performed the command.

A description of the circumstances of the incident as set out in the statement of the Civil Aviation Authority does not specify what kind of actions were planned by the A320 crew. These actions were inhibited by the proper operation of both air traffic controllers, but the plans are crucial for the analysis of a situation which could consequently have led to an accident. It is not clear whether the A320 crew was about to cross runway RWY 29 and then taxi to the threshold via taxiways A5, A6 and L or via the runway itself. It is not clear where the A320 aircraft stopped, i.e. on runway RWY 29, in front of it or behind it. For the purposes of this study it is assumed that the intention of the A320 crew was to cross runway RWY 29 and to taxi via taxiways A5, A6 and L to the threshold of runway RWY 29. It is also assumed that the decision to stop A320 took place just before incursion of the runway under consideration took place. This assumption results in an expansion of the area of analysis because it requires consideration of the:

- potential errors by the GND controller
- possibility of rejection to stop A320
- relationship between the moments of reaching the intersection of a taxiway with runway RWY 29 for both aircraft.

This is the widest possible area of analysis in this case. It is reflected in the presented scenarios of incident continuation.

5.2. Model of the incident

Air event 270/06 was classified as a serious incident due to the fact that continuation of A320's taxiing and EMB170's take-off could have led to a crash. The factors contributing to formation of the event include:

- Crew A320 failed to follow the GND controller's clearance by taxiing on the wrong taxiway despite a proper understanding (repeating) of the clearance

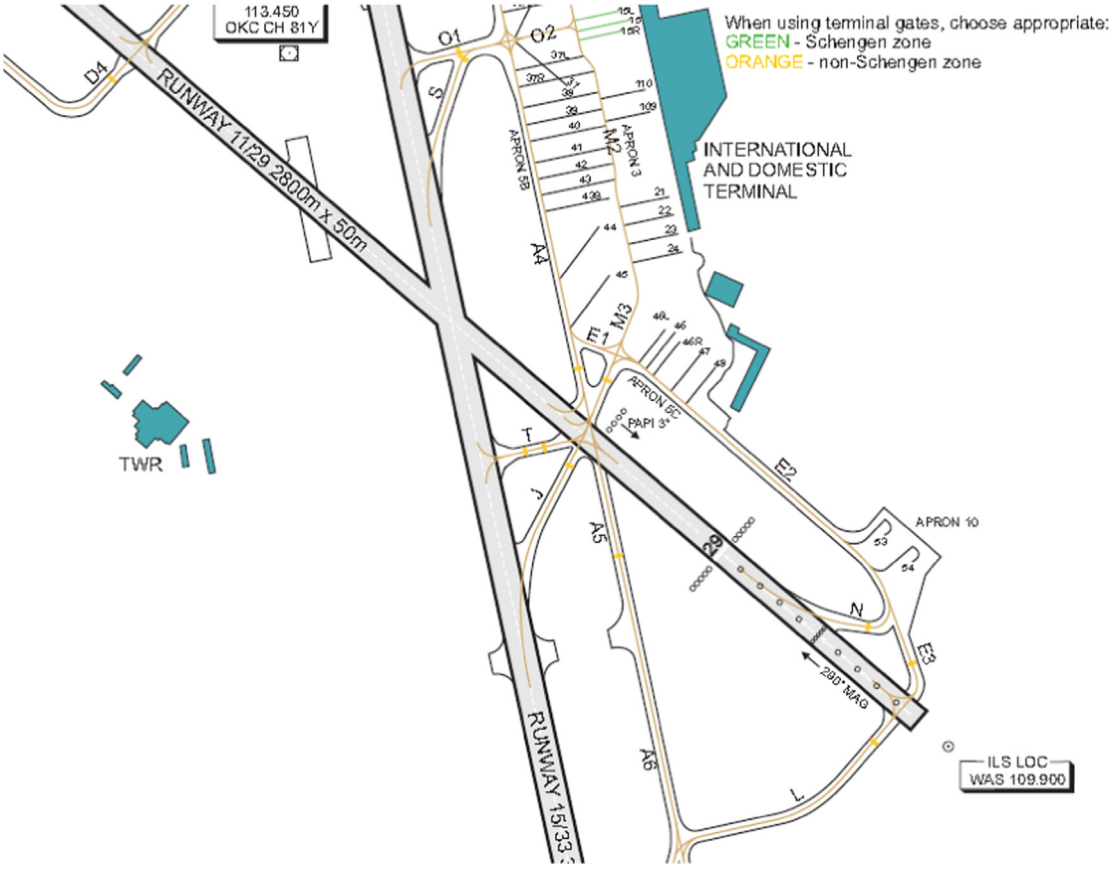

Fig. 3. Warsaw Chopin Airport—aerodrome chart.

– Crew A320 probably failed to read the NOTAM informing about changes in taxiing procedures
– Construction work was being performed at the airport
– Jeppesen maps were outdated; they did not represent the real situation at the airport which was connected with the construction work.

Factors inhibiting the conversion of an incident into an accident in this case were:

– A320's movements were properly monitored by the ground traffic controller
– The traffic situation around the airport was properly monitored by the tower controller; this allowed him/her to notice the incorrect manoeuvre of the A320 crew
– The controllers and crews of both aircraft responded appropriately to the events as they happened.

Both procedures (A320's taxiing and EMB170's taxiing and beginning the take-off) did in fact take place simultaneously and independently of each other. Only the final decisions of the TWR and GND controllers to retain both aircraft resulted from observation of the activities of both aircraft. A model of a serious incident as a coloured Petri net is shown in Fig. 4. This model is the realisation of step 1 of the method's algorithm (Section 4.4).

Determining the model of the incident should be followed by a reduction of the appropriate Petri net by considering the possible consequences of the incident (step 2 of the algorithm). For this particular incident model a reduction is not possible. However, in the general case, this step of the algorithm often allows a significant reduction of the area of analysis.

Model of the incident is the starting point for further analysis and may be useful particularly for practitioners from ANSPs (Air Navigation Service Providers) involved in the analysis of the causes of air traffic events. However, the occurred incident can be also represented by the accident model as will be explained in Section 5.5.1.

5.3. *Determining accident scenarios and the model of the accident*

In the analysis of the likelihood of incident 270/06 being converted into an accident, one needs to consider both the additional events and the time dependencies. It is therefore the most general case.

In the analysed air event we may distinguish several scenarios leading to the transformation of the incident into an accident (step 3 of the method):

Scenario 1 (S_1). The GND controller after issuing taxi clearance and making sure that the A320 crew properly understood it (which occurred in the actual case as the crew correctly repeated the clearance) does not monitor the actual execution of this procedure. In fact, this also corresponds to the situation when the GND controller notices incorrect taxiing and issues the command to stop the taxiing, although it will be too late and there will be no opportunity to avoid A320 runway incursion.
Scenario 2 (S_2). The TWR controller only deals with observation of his/her own area of responsibility and does not pay attention to the taxiway, and therefore does not see the risk in EMB170's take-off. In fact, this also corresponds to the situation when the TWR controller notices incorrect taxiing and issues a command to interrupt the take-off but it will be too late and there will be no possibility to stop the EMB170 aircraft from reaching the collision point.
Scenario 3 (S_3). The crew of either aircraft involved in the incident do not respond to a command to stop the actual procedure. In reality, this corresponds to the situation when the crew's reaction time is too large and the aircraft cannot be stopped before the collision point.
Scenario 4 (S_4). Weather conditions (visibility) are so weak that it is impossible to observe the actual traffic situation. This applies to both controllers. In the present case the weather conditions were good, but if the same traffic situation occurred in poor visibility then the probability of an accident instead of an incident would have been much greater.
Scenario 5 (S_5). None of the aircraft crews notes a conflict situation. In this particular incident there was a timely intervention of the controllers, so action based on either pilot's own observation and recognition of the conflict was not necessary. However, in many real-world situations the aircraft crew notices the threat first and undertakes appropriate preventive action. In the accident model, scenario S_5 will be represented by the times at which the flight crews notice a threat. If this time is too large, it will not be able to stop the aircraft before the collision point.
Scenario 6 (S_6). The time sequence of events (taxiing and take-off times) is such that the A320 plane makes a runway RWY 29 incursion at precisely the same moment when EMB170, while taking off, passes it, thus causing a crash.

As one can see, in scenarios S_1–S_3 and S_5, it is most important if it is possible to stop the aircraft before the collision point. These are binary events—either the aircraft stops or it does not stop. However, the process that determines this is dynamic. It is required to consider both the response time of individual

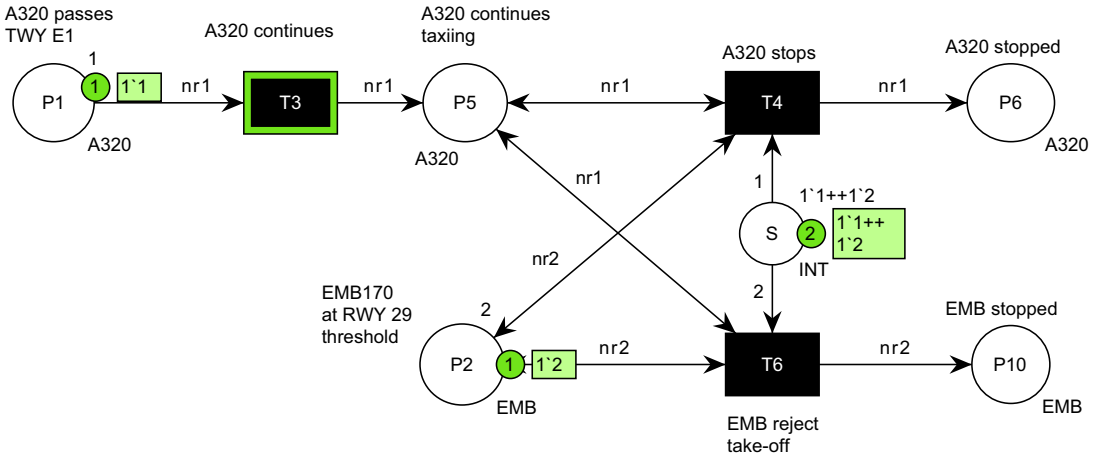

Fig. 4. Model of serious incident 270/06.

controllers and crews but also of the dynamic characteristics (speed, accelerations and decelerations) of aircraft movements. The model takes into account all of these dynamic elements, but the end result is the logical (binary) event—the conflict point is either occupied or not. Scenario S_4 will not be assessed probabilistically, as this analysis makes sense in a general risk assessment; it does not in the case of studying a particular incident where the weather conditions are known. However, the case of insufficient visibility is possible in reality and has a significant impact on the final result of traffic occurrence. The model assumes in scenario S_4 that the conditions are sufficient or insufficient—without probabilistic analysis. Scenario 6 requires an analysis of the time dependencies between the planes involved in the incident. We denote by X_1 a random variable describing the time at which A320 enters the runway, while by X_2 a random variable indicating the time at which the EMB 170 aircraft reaches the intersection of runway 29 with taxiway A4. The condition for an accident to occur is to implement scenario 6. Scenarios 1–5 modify the probability of scenario 6. Of course, we should consider not so much the equality of X_1 and X_2 but rather if the difference between them is less than a given limit.

After determining the accident scenarios the network should be extended with elements allowing for consideration of scenarios leading to accidents. This extension entails the need to modify the set of arcs. In this case the model must also take into account modifications resulting from the change of the process synchronisation method, i.e. from synchronisation of events to time synchronisation.

The Petri net modelling the process which might result in an air traffic accident (step 4 of the method) is shown in Figs. 5–9. It is a hierarchical network consisting of five pages. The page titled *Traffic* contains the initialisation part and a fragment of the model mapping the situation when both planes continue their movements. It is worth noting that the arcs outgoing from transition t_0 to places p_1 and p_2 explicitly define the fact that the taxiing aircraft and taking off aircraft at roughly the same time are in the conflict zone. The page titled *Weather* is responsible for checking the weather conditions. In this paper it is assumed that the situations of good and bad visibility are analysed separately. The page titled *GND Monitor* is responsible for mapping the activities of the GND controller and the crew of the taxiing A320 aircraft. The transition t_{10}, along with its output arc leading to place p_{12} are responsible for determining the random time after which the controller (function *GND_rt*) or pilot (function *A320_st*) notice the threat. In the former case, the possibility of stopping the aircraft before the collision point is also determined by the random crew reaction time (as determined by the function *A320_rt*). The page titled *TWR Monitor* is responsible for mapping the corresponding actions of the TWR controller and the crew of the taking off EMB170 aircraft. In the case when the conflict is recognised and the decision to begin a rejected take-off procedure is taken, the fragment of the model on the *EMB stop* page is responsible for verifying the possibility of stopping the aircraft before the collision point.

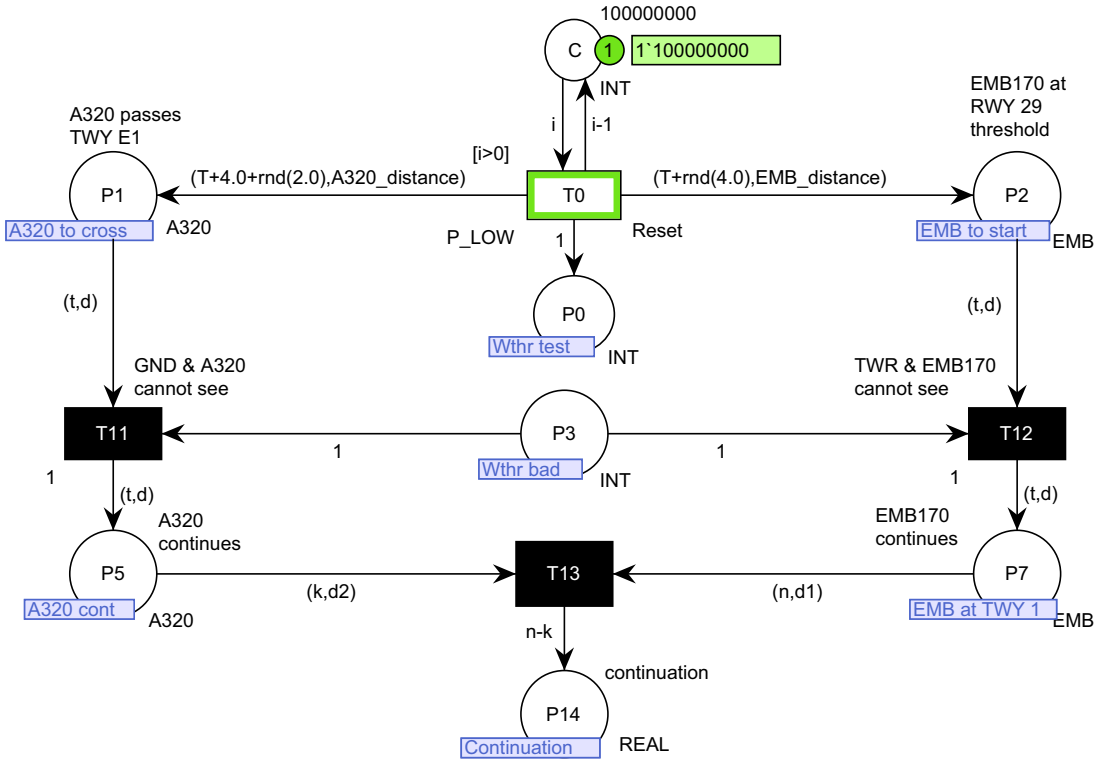

Fig. 5. Main page (*Traffic*) of the model of the accident raised from serious incident 270/06.

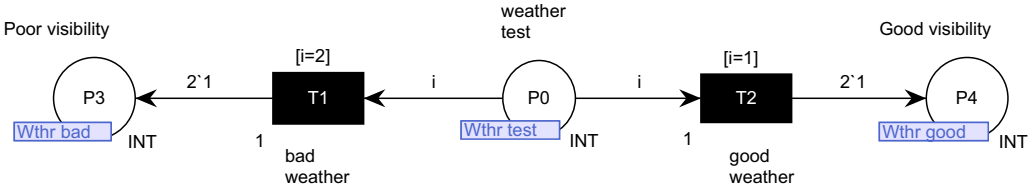

Fig. 6. Page *Weather* of the model of the accident raised from serious incident 270/06.

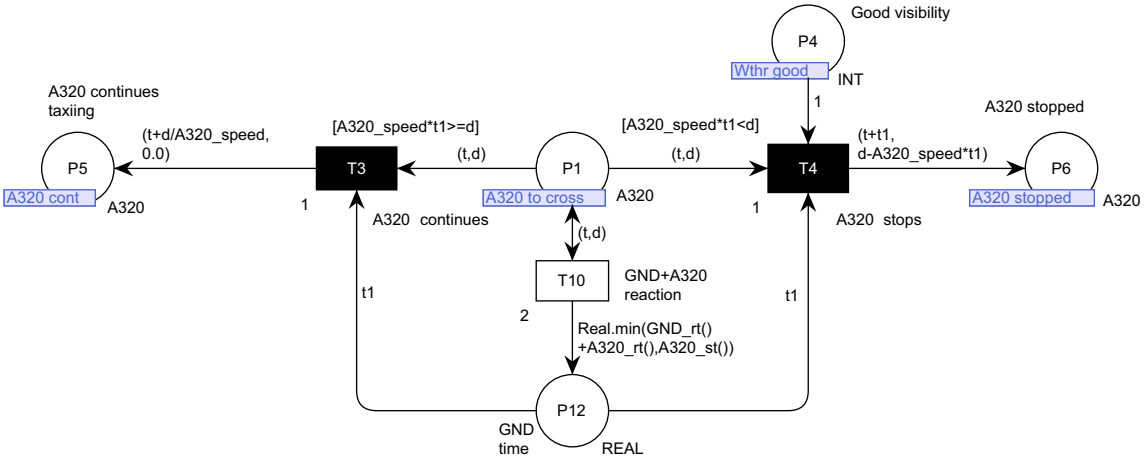

Fig. 7. Page *GND Monitor* of the model of the accident raised from serious incident 270/06.

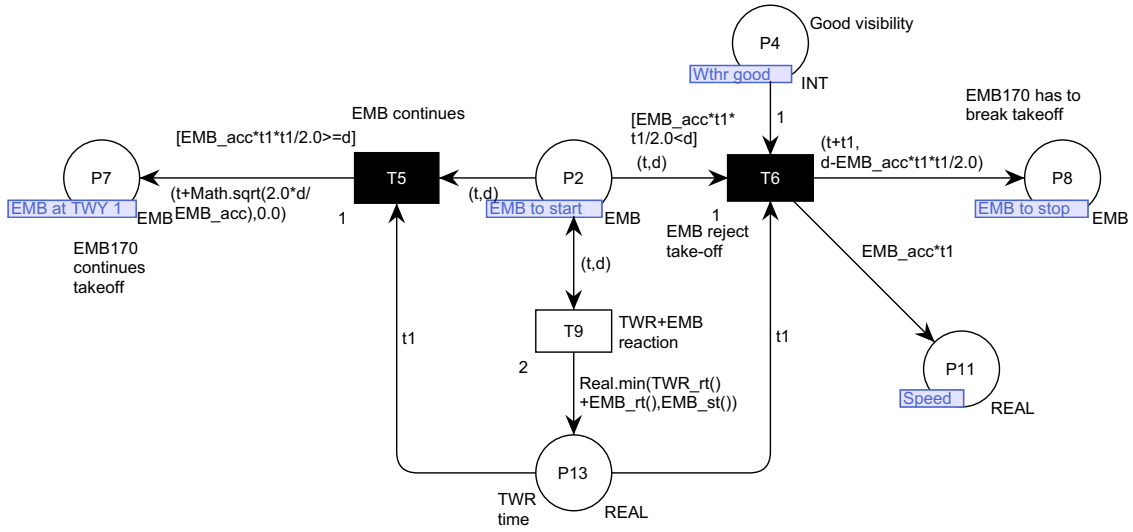

Fig. 8. Page *TWR Monitor* of the model of the accident raised from serious incident 270/06.

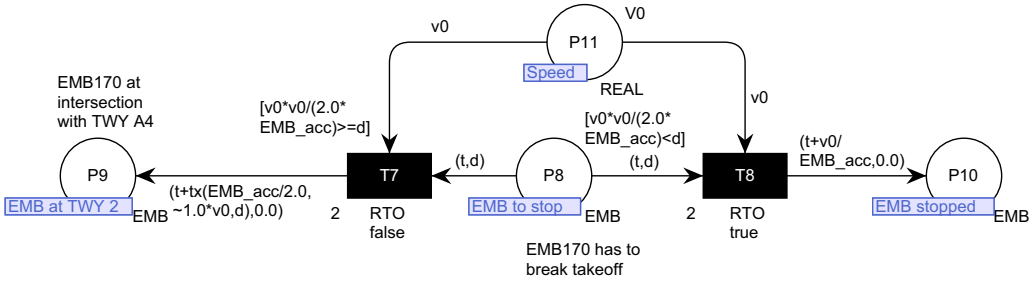

Fig. 9. Page *EMB stop* of the model of the accident raised from serious incident 270/06.

Relations between the pages are implemented using *fused places*. These places are labelled in the bottom left-hand corner. All places marked with the same label are the same. It is a coloured net containing four sets of colours:

- $A320 = \mathbb{R} \times \mathbb{R}$—the set corresponding to traffic situations of the A320 aircraft; the first number represents the timestamp assigned to a token in the place and the second number represents the distance to the collision point
- $EMB = \mathbb{R} \times \mathbb{R}$—the set corresponding to traffic situations of the EMB170 aircraft; the first number represents the timestamp assigned to a token in the place and the second number represents the distance to the collision point
- $INT = \mathbb{Z}$—the set used for the simulations counter and for describing the weather conditions
- $REAL = \mathbb{R}$—the set used for storing calculated aircraft speeds and random pilot and controller reaction times.

The use of colours with a timestamp allows to track the time of transition execution, and thus for an analysis of the timing between the events. This enables an accurate simulation of the course of the modelled event.

Designations of places are as follows: p_0—"weather test", p_1—"A320 passes TWY E1", p_2—"EMB170 at RWY 29 threshold", p_3—"poor visibility", p_4—"good visibility", p_5—"A320 continues taxiing", p_6—"A320 stopped", p_7—"EMB170 continues take off", p_8—"EMB170 has to break take off", p_9—"EMB170 at intersection with TWY A4, "p_{10}—"EMB170 stopped", p_{11}—"speed", p_{12}—"GND time", p_{13}—"TWR time", p_{14}—"continuation".

The set of transitions contains the following elements: t_0—"reset", t_1—"bad weather", t_2—"good weather", t_3—"A320 does not interrupt taxiing", t_4—"A320 interrupts taxiing", t_5—"EMB170 does not interrupt take-off", t_6—"EMB170 interrupts take-off", t_7—"rejected take-off unsuccessful", t_8—"rejected take-off successful", t_9—"TWR and EMB170 reaction", t_{10}—"GND and A320 reaction", t_{11}—"GND and A320 cannot see", t_{12}—"TWR and EMB170 cannot see", t_{13}—"distance".

The occurrence of scenarios S_1, S_3 and S_5 corresponds to the firing of transition t_3. The occurrence of scenario S_2, S_3 and S_5 corresponds to the firing of transitions t_5 and t_7. The firing of transition t_1 corresponds to the occurrence of scenario S_4.

5.4. Reachability set and reachability graph construction

The set of markings that are reachable from the initial marking M_0 is shown in Table 2, and the reachability graph is in Fig. 10 (step 5 of the method). The final (dead) states are indicated with the letter D. In determining the reachability set, the activation and firing sequences were defined with taking into account the laps of local simulation time.

The most important states (final states, marked with the letter D in Table 2) in terms of risk analysis of accident resulting from incident 270/06 are shown in Table 3. Other states and insignificant places are omitted.

System states M_{23}, M_{25}, M_{26} and M_{27} represent safe situations in which at least one of the aircraft stopped before the runway–taxiway intersection. States M_{18}, M_{28} and M_{29} represent cases in which both aircraft reach the intersection. This statement represents the implementation of point 6 of the algorithm.

5.5. Determining the probability of incident to accident conversion

Determining the likelihood of conversion of the incident into an accident (step 8 of the method) will be made by using the simulation. Analytical method together with an example of the reachability graph reduction (step 7 of the method) will be the subject of another publication.

5.5.1. Determining the probability by simulation

We can use the simulation method, which involves the repeated execution of transitions (starting from the initial marking), including all random events, and observing the results. These results are treated as a random sample for a group of experiments. In this case, these experiments can be equated with multiple executions of an identical serious incident and observing how often it transforms into an accident.

Simulation analysis requires determining the time necessary to execute timed transitions. In the model of the incident these values are constant. The adoption of these values also in the accident model allows one to represent the occurred incident. This applies to the model parameters calculated by the functions *GND_rt*, *A320_rt*, *A320_st*, *EMB_st*, *TWR_rt* and *EMB_rt*. To represent the occurred incident by the accident model the values returned by these functions must be constant like in the real incident. In the model of the accident they are random variables. These variables are determined by the time necessary for the crew to recognise the conflict, or to react to the warning coming from the outside. Analyses of the problems of human perceptual capabilities and the reaction time fall within the area of psychology and are beyond the scope of this work. However, to illustrate the proposed method these values have been estimated by the experts—an experienced air traffic controller and the pilot of a military transportation aircraft. The experts identified the expected values of these times. These values are presented in Table 4. It was also assumed that these random variables are described by exponential distribution. In Table 4, data derived from the author's own measurements of the aircraft taxiing process at Chopin Airport in Warsaw is also presented. The measurements were completed from May to November of 2012. And so, the (t_0, p_1) arc's characteristics are equal to the actual taxiing time of aircraft A320 from parking position no. 33 via taxiway A to the A4–E1 taxiway crossing. For aircraft EMB 170, the (t_0, p_2) arc's characteristics correspond to the measured taxiing time from parking position no. 46 to the position before the runway 29 threshold plus the time to line up on the runway and be ready for takeoff. Using a constant T makes it easier to notice the small difference in the time of appearance of the two aircraft in the conflict zone. The term $rnd(x)$ means the execution of a self-written computer code generating an adequate random variable with an expected value equal to x. In the presented simulation results the value generated by $rnd(x)$ is based on the exponential distribution, however, other distributions may be applied. The algorithm truncates the tails of the distributions in accordance with the observations and measurements of the actual values. Due to paper volume limitations, the detailed statistical analysis was omitted. All of this made it possible to estimate the characteristics of the timed transitions and thus allowed to find the sought probabilities by simulation. However, one should bear in mind that these are largely expert estimates and further research should be carried out in this area, including with the use of formal methods [43,28].

The hierarchical net shown in Figs. 5–9 was subjected to an experiment which consisted in execution of 10^8 simulation runs. In the case of the analysis carried out in good visibility conditions, the state M_{18} did not appear. The state M_{28} was reached in 342,945 cases, and the state M_{29} in 138,682 cases. These are the cases in

Table 2
Reachability set for a model of accident arising from incident 270/06.

M_0	$p_0+p_1+p_2$		M_1	$p_1+p_2+2p_4$		M_2	$p_1+p_2+2p_3$	
M_3	$p_1+p_2+2p_4+p_{13}$		M_4	$p_1+p_2+2p_4+p_{12}$		M_5	$p_2+p_3+p_5$	
M_6	$p_1+p_3+p_7$		M_7	$p_1+p_4+p_8+p_{11}$		M_8	$p_1+2p_4+p_7$	
M_9	$p_2+p_4+p_6$		M_{10}	$p_2+2p_4+p_5$		M_{11}	p_5+p_7	
M_{12}	$p_1+p_4+p_{10}$		M_{13}	$p_1+p_4+p_9$		M_{14}	$p_1+p_4+p_8+p_{11}+p_{12}$	
M_{15}	$p_1+2p_4+p_7+p_{12}$		M_{16}	$p_2+p_4+p_6+p_{13}$		M_{17}	$p_2+2p_4+p_5+p_{13}$	
M_{18}	p_{14}	D	M_{19}	$p_1+p_4+p_{10}+p_{12}$		M_{20}	$p_1+p_4+p_9+p_{12}$	
M_{21}	$p_6+p_8+p_{11}$		M_{22}	$p_4+p_5+p_8+p_{11}$		M_{23}	$p_4+p_6+p_7$	D
M_{24}	$2p_4+p_5+p_7$		M_{25}	p_6+p_{10}	D	M_{26}	$p_4+p_5+p_{10}$	D
M_{27}	p_6+p_9	D	M_{28}	$p_4+p_5+p_9$	D	M_{29}	$2p_4+p_{14}$	D

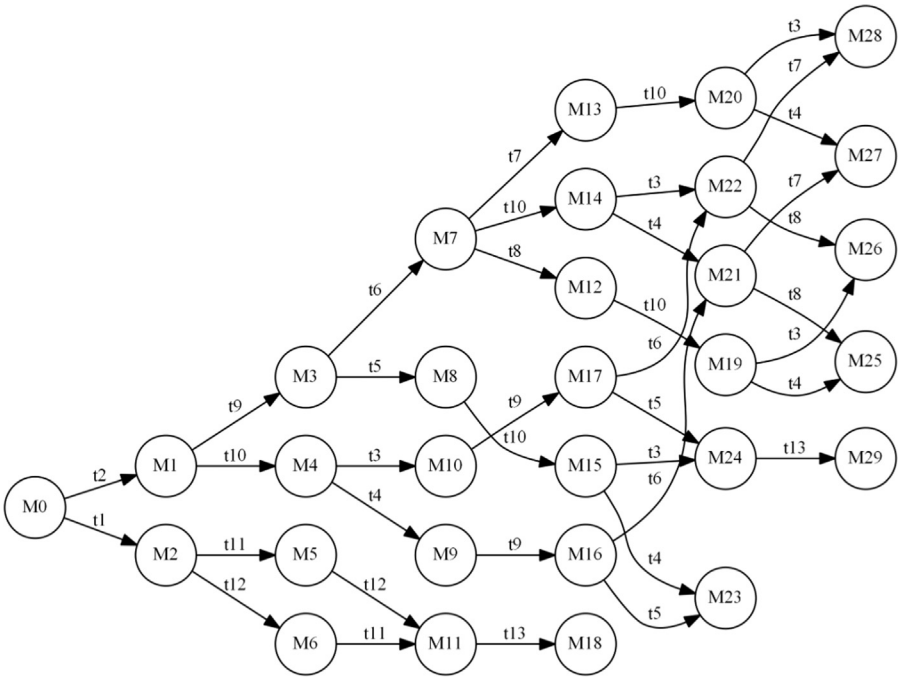

Fig. 10. Reachability graph for a model of accident arising from incident 270/06.

Table 3
Selected states of the system (in model of accident resulting from incident 270/06).

	p_4 Good visibility	p_5 A320 continues taxiing	p_6 A320 stopped	p_7 EMB170 continues take-off	p_9 EMB170 at intersection with TWY A4	p_{10} EMB170 stopped	p_{14} Continuation
M_{18}							1
M_{23}	1		1	1			
M_{25}			1			1	
M_{26}	1	1				1	
M_{27}			1		1		
M_{28}	1	1			1		
M_{29}	2						1

Table 4
Times determining the intensities of transitions in the model of the accident.

Parameter	Time [s]
GND controller reaction	10
A320 crew reaction	2
TWR controller reaction	10
EMB170 crew reaction	2
TWR-EMB170 transmission	2
A320 own observation	15
EMB170 own observation	15
(t_0, p_1)	$200+rnd(2)$
(t_0, p_2)	$196+rnd(4)$

Table 5
Results of simulation for the transition to final states.

Final state	Accident	Probability	
		good weather	bad weather
M_{18}	Accident	0	$9.298 \cdot 10^{-1}$
M_{18}	Safe	0	$7.02 \cdot 10^{-2}$
M_{23}	Safe	$1.588 \cdot 10^{-2}$	0
M_{25}	Safe	$8.643 \cdot 10^{-1}$	0
M_{26}	Safe	$7.578 \cdot 10^{-2}$	0
M_{27}	Safe	$3.921 \cdot 10^{-2}$	0
M_{28}	Accident	$2.806 \cdot 10^{-4}$	0
M_{28}	Safe	$3.149 \cdot 10^{-3}$	0
M_{29}	Accident	$2.45 \cdot 10^{-4}$	0
M_{29}	Safe	$1.142 \cdot 10^{-3}$	0

which both aircraft appeared at the intersection of the runway and taxiway. Only in some of them was the difference in the time of occupation of the conflict point less than 5 s, which was adopted as the limit to qualify the event as an accident. This value is the result of the analysis of the distance that A320 aircraft covers in the collision zone and its speed. This analysis takes into account the dimensions of the plane and the angle at which it crosses the runway. There were 52,561 of such cases. This means that the probability obtained by simulation is $P_{I\to A} = 5.256 \cdot 10^{-4}$. In the case of analysis for poor visibility conditions, the only final state is M_{18}, while the probability of conversion of the incident into an accident is $P_{I\to A} = 0.93$.

Also, the analysis of final states that occurred during the transformation of the incident into an accident is interesting. The results are shown in Table 5.

The simulation results show that in good weather conditions $P(M_0[\sigma\rangle M_{28}) = 3.429 \cdot 10^{-3}$, $P(M_0[\sigma\rangle M_{29}) = 1.387 \cdot 10^{-3}$. State M_{18} was not observed. Final states marked as safe depict cases in which scenarios leading to the transformation from an incident into an accident occurred, but the time dependencies were such that there

Table 6
Dependence of the probability of an accident on: (a) the time until the A320 crew recognises a conflict, (b) the time until the EMB170 crew recognises a conflict, (c) the time until the TWR controller recognises a conflict.

(a) A320 recognition of conflict [s]	3	6	9	12	15	18	21	24	27
Probability of accident $\left[\cdot 10^{-4}\right]$	0.014	0.661	2.421	4.152	5.256	6.843	7.691	8.264	8.635
(b) EMB170 recognition of conflict [s]	3	6	9	12	15	18	21	24	27
Probability of accident $\left[\cdot 10^{-4}\right]$	0.012	0.533	1.634	3.517	5.256	6.775	7.919	9.308	10.09
(c) TWR controller recognition of conflict [s]	2	4	6	8	10	12	14	16	18
Probability of accident $\left[\cdot 10^{-4}\right]$	0.021	1.132	2.283	3.684	5.256	6.618	8.392	9.291	10.19

was no collision of aircraft. In particular, this concerns the case when EMB170, taking off, passed the intersection with taxiway TWY A4 before the taxiing aircraft A320 reached this place. Of course, it should be noted that these situations are also extremely dangerous and should be avoided.

5.5.2. Sensitivity analysis

The model developed here in the form of a Petri net allows to define the relationship between the probability of an incident–accident transformation and the many factors that were included in the analysis. This section presents this relationship for the time at which the flight crews or the TWR controller recognise a conflict. The results are shown in Table 6 and come from a simulation approach.

The probability of an incident–accident transformation changes approximately linearly with respect to each of the three factors as listed in Table 6. As can be seen, there is a potential to increase safety by enhancing situational awareness manifested by shortening the time to recognition of a dangerous situation. For very large values of that time, which in practice corresponds to the lack of a response, the probability of an accident stabilises at a constant level.

6. Summary and conclusions

In the paper the method of analysing the relationship between a serious air traffic incident and accident was presented. The starting point for this analysis was the assumption that a serious incident describes a situation in air traffic in which only one or two additional adverse events are sufficient to cause an accident. The paper focuses on the model development and the method to estimate the probability of transformation of an incident into an accident.

In the analysed example (a real air traffic incident) there are six scenarios which lead to the transformation of an incident into an accident. Of these, five relate to events of a certain probability, and one relates to specific time dependencies between the events. This is the most general case—an incident of a hybrid type. In the paper an algorithm for the construction of an appropriate, coloured, timed, stochastic Petri net model of accident was proposed. The model may be examined analytically and with the use of the simulation technique. The latter method allowed to determine the probability of an incident–accident conversion. However, we should remember that in both cases they are based on expert assessments, thus it would be advisable to perform further measurements and tests in order to increase the accuracy of the input data. The simulation time for 10^8 experiments is approximately 20–30 min for a medium-class personal computer. Therefore, the simulation method seems to be a reasonable approach to the analysis of a serious incident of the hybrid type.

The developed method is general and may help to forecast the number of accidents on the basis of the number of incidents (serious incidents) in air traffic. This was checked on a serious incident of the class of runway incursion. Development of such a method is an important step towards using the TLS concept in the practice of air traffic management (ATM). It is also crucial to the airport safety management system (SMS). As was shown in the simulation analysis, the probability of the transformation of analysed incident of the runway incursion type into an accident is of the order of $5 \cdot 10^{-4}$. As was indicated in Section 1, the runway incursion rate in Europe is of the order of $6 \cdot 10^{-6}$. By taking both of these figures into account we obtain that the expected number of accidents of this specific type can be estimated at $3 \cdot 10^{-9}$ accident on a flight. To compare this with the Eurocontrol TLS value ($2.31 \cdot 10^{-8}$ accident on a flight) we must have similar estimates for other types of incidents. Of course, the TLS value $2.31 \cdot 10^{-8}$ applies to the entire flight, so in the case of the analysis of incidents of the RI class only we should take only its part for comparison. This type of analysis will be carried out in future publications.

This paper is a continuation of research aimed at finding a method for effective analysis of incident–accident transformations. For accidents depending on the occurrence of certain additional events [61] or depending on a favourable or unfavourable time sequence [62]—the best method is to examine the model analytically. For the hybrid case (as in this paper, incident no. 270/06)—the simulation method seems to be efficient. The use of the proposed method may be of practical significance. On the one hand, it can assist in safety management systems by providing an approach to determine the CLS in cases when there are no air traffic accidents in the country. On the other hand, it is a proactive approach; this may be stated since we are not analysing what has already happened but rather what might happen. In this way we anticipate threats even before they appear. Quantitative estimates also allow to assess how probable these risks are. Moreover, this approach is consistent with the resilience engineering approach as proposed by Holnagel et al. [30], i.e. it seeks to answer the question whether the system will retain the ability to work in the long term if faced with threats which are currently not even possible to be imagined. The proposed method is going in the same direction—to assess whether, and with what probability, in the case of accident scenarios the system will switch to a safe state. If not, then we can offer early intervention, which will improve the resilience of the system.

References

[1] Ahlstrom U. Work domain analysis for air traffic controller weather displays. J Saf Res 2005;36:159–69.
[2] Ayres Jr. M, Shirazi H, Carvalho R, Hall J, Speir R, Arambula E, et al. Modelling the location and consequences of aircraft accidents. Saf Sci 2013;51(1):178–86.
[3] Bakker G, Klein Obbink B, Klompstra M, Blom H. DCPN specification of a free flight air traffic operation, working document. Technical report. Amsterdam, The Netherlands: National Aerospace Laboratory NLR; 2004.
[4] Bekier M, Molesworth BRC, Williamson A. Tipping point: The narrow path between automation acceptance and rejection in air traffic management. Saf Sci 2012;50(2):259–65.
[5] Blom HAP, Bakker GJ, Blanker PJG, Daams J, Everdij MHC, Klompstra MB. Accident risk assessment for advanced air traffic management. In: Donohue GL, Zellweger AG, editors. Air transport systems engineering. AIAA; 2001. p. 463–80.
[6] Blom, H., Klompstra, M., Bakker, B. (2001b). Accident risk assessment of simultaneous converging instrument approaches. In: Fourth USA/Europe Air Traffic Management R&D seminar Santa Fe.

[7] Blom, HAP, Stroeve, SH, De Jong, HH Safety risk assessment by Monte Carlo simulation of complex safety critical operations, In: F. Redmill, T. Anderson editors, Developments in risk-based approaches to safety. Proceedings of the fourteenth safety-critical systems symposium, Bristol, U.K., 7–9 February 2006, Springer; 2006.
[8] Civil Aviation Authority. Statement no. 81 of President of the Office of Civil Aviation in Poland from 4th of September 2008 on Air Event no. 270/06, Warsaw; 2008.
[9] Davidrajuh R, Lin B. Exploring airport traffic capability using Petri net based model. Expert Syst Appl 2011;38(9):10923–31.
[10] Dekker SWA. Reconstructing human contributions to accidents: the new view on error and performance. J Saf Res 2002;33:371–85.
[11] Dekker S, Hollnagel E, Woods D, Cook R. Resilience engineering: new directions for measuring and maintaining safety in complex systems. Lund University School of Aviation; 2008.
[12] Dell'Olmo P, Lulli G. A dynamic programming approach for the airport capacity allocation problem. IMA J Manage Math 2003;14:235–49.
[13] Diaz M. Petri nets. Fundamental models, verification and application. London: John Wiley and Sons; 2009.
[14] Dong-bin L, Xiao-hao X, Xiong L. Target level of safety for Chinese airspace. Saf Sci 2009;47(3):421–4.
[15] Dubois D, Prade H. On the relevance of non-standard theories of uncertainty in modelling and pooling expert opinions. Reliab Eng Syst Saf 1992;36:95–107.
[16] EUROCONTROL. Risk assessment and mitigation in ATM. Eurocontrol safety regulatory requirement ESARR4, Edition 1.0, Eurocontrol Safety Regulation Commission, Brussels; 2001.
[17] EUROCONTROL. A method for States to determine national ATM safety minima, Eurocontrol Safety Regulation Commission, Brussels; 2004.
[18] EUROCONTROL. EVAIR safety bulletin, no. 8, Bruxelles; 2012.
[19] European Aviation Safety Agency. European aviation safety plan 2013–2016, Koeln; 2012.
[20] European Union. (2010). Regulation (EU) no 996/2010 of the European Parliament and of the Council of 20 October 2010 on the investigation and prevention of accidents and incidents in civil aviation and repealing Directive 94/56/EC, Off J Eur Union, L 295/35.
[21] European Union. (2011). Regulation (EU) No 1035/2011 of European Commission of 17 October 2011 laying down common requirements for the provision of air navigation services and amending Regulations (EC) No 482/2008 and (EU) No 691/2010, Off J Eur Union L 271/23.
[22] Everdij, M, Blom, H. Modelling hybrid state Markov processes through dynamically and stochastically coloured Petri nets. EU IST Programme: distributed control and stochastic analysis of hybrid systems supporting safety critical real-time systems design (HYBRIDGE Project); 2004.
[23] Federal Aviation Administration. National runway safety plan 2009–2011, Washington DC; 2009.
[24] Ford J, Henderson R, O'Hare D. The effects of Crew Resource Management (CRM) training on flight attendants' safety attitudes. J Saf Res 2014;48:49–56.
[25] Ford, AT, Waldron, TP, Borener, S. Relating airport surface collision potential to taxiway geometry and traffic flow. In: Fourteenth AIAA aviation technology, integration, and operations conference, Atlanta; 2014.
[26] Fota, N Everdij, M, Stroeve, SH, Kråkenes, T, Herrera, I, Quiñones, J, et al. Using dynamic risk modelling in Single European Sky Air Traffic Management Research (SESAR), In: Nowakowski, T. editor, Safety and reliability: methodology and applications—proceedings of the European safety and reliability conference, ESREL 2014; 2015. p. 729-737.
[27] Gudelj A, Kezic D, Vidacic S. Marine traffic optimization using Petri Net and genetic algorithm. Promet—Traffic Transp 2012;24(6):469–78.
[28] Hanea DM, Jagtman HM, van Alphen LLMM, Ale BJM. Quantitative and qualitative analysis of the expert and non-expert opinion in fire risk in buildings. Reliab Eng Syst Saf 2010;95:729–41.
[29] Heathrow Airside Operations Flight Performance (FP) Team. Flight performance annual report, London; 2013.
[30] Holnagel E, Woods DD, Leveson N. Resilience engineering: concepts and precepts. Aldershot: Ashgate Publishing; 2006.
[31] Horowitz BM, Santos JR. Runway safety at airports: a systematic approach for implementing ultra-safe options. J Air Transp Manage 2009;15:357–62.
[32] International Civil Aviation Organisation. Aircraft accident and incident investigation. In: International standards and recommended practices, Annex 13 to the convention on international civil aviation; 2001.
[33] International Civil Aviation Organisation Procedures for air navigation services—rules of the air and air traffic services, DOC 4444-RAC/501, 15th ed.; 2007.
[34] Ishak SZ, Yue WL, Somenahalli S. Level crossing modelling using Petri nets approach and Π–tool. Asian Transp Stud 2010;1(2):107–21.
[35] Jensen K. Coloured Petri nets. Basic concepts, analysis methods and practical use. Berlin: Springer Verlag; 1997.
[36] Jensen K, Kristensen LM, Wells L. Coloured Petri nets and CPN tools for modelling and validation of concurrent systems. Int J Softw Tools Technol Trans 2007;9(3-4):213–54.
[37] Johnson C. The application of Petri nets to represent and reason about human factors problems during accident analyses. In: Palanque P, Bastide R, editors. Design, specification and verification of interactive systems '95. Springer-Verlag/Wien; 1995. p. 93–112.
[38] Khakzad, N., Khan, F., Paltrinieri, N., On the application of near accident data to risk analysis of major accidents, Reliab Eng Syst Saf 126: 116–125.
[39] Kirwan B. Incident reduction and risk migration. Saf Sci 2011;49(1):11–20.
[40] Kontogiannis T. A systems perspective of managing error recovery and tactical re-planning of operating teams in safety critical domains. J Saf Res 2011;42:73–85.
[41] Kovacs, A, Nemeth, E, Hangos, K. Coloured Petri net model of a simple runway (research report SCL-001/2004); 2004.
[42] Kovacs, A, Nemeth, E, Hangos, K. Modeling and optimization of runway traffic flow using coloured Petri nets. In: Proceedings of the fifth international conference on control and automation Budapest, Hungary; 26–29 Jun, 2005. p. 881–886.
[43] Kurowicka D, Cooke R, Goossens L, Ale B. Expert judgment study for placement ladder bowtie. Saf Sci 2008;46:921–34.
[44] Le Coze JC. What have we learned about learning from accidents? Post-disasters reflections Saf Sci 2013;51(1):441–53.
[45] Lesire, C, Tessier, C. Particle Petri nets for aircraft procedure monitoring under uncertainty. In: Proceedings 26th international conference on application and theory of Petri nets (ATPN), editors G. Ciardo, P. Darondeau, Lecture notes in computer science (LNCS), vol. 3536, 2005, p. 329–348. Springer-Verlag.
[46] Lin CJ, Lin P, Chen H, Hsieh M, Yu H, Wang EM, et al. Effects of controller-pilot communication medium, flight phase and the role in the cockpit on pilots' workload and situation awareness. Saf Sci 2012;50(9):1722–31.
[47] Lower M, Magott J, Skorupski J. Air traffic incidents analysis with the use of fuzzy sets. In: Rutkowski L, et al., editors. ICAISC 2013, Part I, LNAI 7894. Berlin Heidelberg: Springer; 2013. p. 306–17.
[48] Marsan MA, Balbo G, Conte G, Donatelli S, Franceschinis G. Modelling with generalized stochastic Petri nets. Torino: Universita degli Studi di Torino, Dipartamento d'Informatica; 1999.
[49] Mearns K, Kirwan B, Reader TW, Jackson J, Kennedy R, Gordon R. Development of a methodology for understanding and enhancing safety culture in air traffic management. Saf Sci 2013;53(0):123–33.
[50] Netjasov, F. Fuzzy expert model for determination of runway in use case study: Airport Zurich. In: First international conference on research in air transportation ICRAT 2004, Zilina, Slovakia; November 22–23, 2004. p. 59–64.
[51] Netjasov, F., Vidosavljevic, A., Tosic, V., Everdij, M., Blom, H., Development, validation and application of stochastically and dynamically coloured Petri net model of ACAS operations for safety assessment purposes, Transp Res: Part C: Emerg Technol, 33, 167–195.
[52] Oberheid, H. A coloured Petri net model of cooperative arrival planning in air traffic control. In: Proceedings of the seventh workshop and tutorial on practical use of coloured Petri nets and the CPN Tools, editor K. Jensen, Department of Computer Science, University of Aarhus, Denmark, 2006, p. 177–196.
[53] Oberheid H, Söffker D. Cooperative arrival management in air traffic control—a coloured Petri net model of sequence planning. In: Hee K, Valk R, editors. Applications and theory of Petri nets. Berlin Heidelberg: Springer; 2008. p. 348–67.
[54] Ratzer, A.V., Wells, L., Lassen, H.M., Laursen, M., Qvortrup, J.F., Stissing, M.S., et al. CPN Tools for editing, simulating, and analysing coloured Petri nets. In: Proc. of 24th international conference on applications and theory of Petri nets (Petri Nets 2003), lecture notes in computer science 2679; 2003. p. 450–462.
[55] Reisig W. Understanding Petri nets. Modeling techniques, analysis methods, case studies. Berlin: Springer Verlag; 2013.
[56] Roelen ALC, Lin PH, Hale AR. Accident models and organisational factors in air transport: The need for multi-method models. Saf Sci 2011;49(1):5–10.
[57] Rogerson EC, Lambert JH. Prioritizing risks via several expert perspectives with application to runway safety. Reliab Eng Syst Saf 2012;103:22–34.
[58] Ruiz S, Piera MA, Del Pozo I. A medium term conflict detection and resolution system for terminal maneuvering area based on spatial data structures and 4D trajectories. Transp Res: Part C: Emerg Technol 2013;26:396–417.
[59] Skorupski, J. Petri nets as a tool for modelling the traffic processes in transport (Sieci Petriego jako narzędzie do modelowania procesów ruchowych w transporcie). Scientific Works of Warsaw University of Technology, Transport, 78, 2011a; 69-77.
[60] Skorupski J. Modelling of traffic incidents in transport. In: Weintrit A, editor. Transport systems and processes—marine navigation and safety of sea transportation. London: CRC Press/Taylor & Francis; 2011. p. 25–32.
[61] Skorupski J. Method of analysis of the relation between serious incident and accident in air traffic. In: Berenguer C, editor. Advances in safety, reliability and risk management. London: CRC Press/Taylor & Francis; 2011. p. 2393–401.
[62] Skorupski, J. Risk analysis of incident–accident transformation in air traffic. In: Eleventh international probabilistic safety assessment and management conference and the annual European safety and reliability conference 2012 (PSAM11 ESREL 2012); 2012. p. 4849–4857.
[63] Skorupski J. Multi-criteria group decision making under uncertainty with application to air traffic safety. Expert Syst Appl 2014;41(16):7406–14.
[64] Stoop J, Dekker S. Are safety investigations pro-active? Saf Sci 2012;50(6):1422–30.
[65] Stroeve SH, Blom H, Bakker GJ. Systemic accident risk assessment in air traffic by Monte Carlo simulation. Saf Sci 2013;47:238–49.
[66] Stroeve SH, Blom H, Bakker GJ. Contrasting safety assessments of a runway incursion scenario: Event sequence analysis versus multi-agent dynamic risk modelling. Reliab Eng Syst Saf 2013;109:133–49.
[67] Tamasi G, Demichela M. Risk assessment techniques for civil aviation security. Reliab Eng Syst Saf 2011;96:892–9.

[68] Wang Y, Vormer F, Hu M, Duong V. Empirical analysis of air traffic controller dynamics. Transp Res: Part C: Emerg Technol 2013;33:203–13.
[69] Werther, N, Moehlenbrink, C, Rudolph, M. Colored Petri Net based formal airport control model for simulation and analysis of airport control processes. In: Vincent G. Duffy editor. Proceedings of the first international conference on digital human modeling (ICDHM'07); 2007. p. 1027–1036.
[70] Westergaard, M., Kristensen, LM. The access/CPN framework: a tool for interacting with the CPN Tools simulator. In: Proc. of 30th international conference on applications and theory of Petri nets (Petri Nets 2009). Lecture notes in computer science 5606; 2009. p. 313–322.