Comparing Modelling Approaches in Aviation Safety

Tibor BOSSE[a] and Nataliya MOGLES[a]
[a] *Vrije Universiteit Amsterdam, Department of Artificial Intelligence*
de Boelelaan 1081a, 1081 HV Amsterdam, The Netherlands
{tbosse, nms210}@few.vu.nl

Abstract. Within open socio-technical systems, the quality of the system as a whole crucially depends on the joint performance and interaction of the individual agents involved. A domain where the study of this regulation is particularly complex is the domain of Air Traffic Management (ATM). The current paper compares four of the more influential modelling approaches within ATM, namely Event Trees, FRAM, STAMP, and the agent-based approach LEADSTO. This is done by applying the four approaches to a case study on retrospective modelling of a runway incursion incident that occurred in 1995. Based on this comparison, the pros and cons of the different approaches are discussed.

Keywords. aviation safety, modelling, agents, comparison

Introduction

For complex open systems consisting of multiple heterogeneous agents that are spatially distributed, regulation is an important issue. Whether it is an insurance company, an air traffic organisation, or a university, all of these systems cope with the challenge that their overall quality crucially depends on the joint performance and interaction of various loosely coupled entities, or agents. Important mechanisms to enforce regulation of open multi-agent systems are coordination, organisation, institutions and norms [17]. Indeed, many existing systems make use of these mechanisms. For example, contemporary airlines apply strict protocols for airline crew, maintenance technicians, and passengers, in order to ensure safe and efficient flights. Nevertheless, such regulations are no guarantee that all operations run smoothly. Especially for systems of which the performance depends on the interaction between a large number of heterogeneous autonomous agents, things can still go wrong. In such cases, rather than strictly following the prescribed rules, improvisation of individual agents may be needed to prevent failure.

A domain where this concept of improvisation is particularly relevant is the area of Air Traffic Management (ATM). According to Eurocontrol [19], ATM involves 'the process, procedures and resources which come into play to make sure that aircraft are safely guided in the skies and on the ground'. The ATM system as a whole is often referred to as an 'open socio-technical system'; it is called socio-technical because it involves both social agents (e.g., pilots and air traffic controllers) and technical components (e.g., aircraft and autopilots), and it is called open because it can be

influenced by external factors that cannot be entirely predicted before operation (e.g., the weather). Within the ATM domain, one of the main measures for success of the organisation is safety. However, it is impossible to always guarantee safety for all possible scenarios, due to the complex interplay of the different agents involved. For example, although currently still under investigation, the famous accident in 2009 of Air France Flight 447 seems to have been the consequence of a rare combination of factors, including inconsistent airspeed sensor readings, the disengagement of the autopilot, and the pilot pulling the nose of the plane back despite stall warnings [18]. In such cases, where safety is threatened by a combination of factors, *flexibility* of individual agents is sometimes preferred over predefined rule-based behaviour. This is also recognised by the field of Resilience Engineering, a scientific discipline that studies the design of socio-technical systems that are able to cope with unexpected disturbances, among others based on flexibility of the (human) agents involved [8].

However, due to the complexity of the ATM system and the variety of possible agent behaviours, studying the dynamics of potential accidents and incidents in aviation is a nontrivial issue. For these reasons, researchers in aviation are increasingly making use of techniques from computer science, including agent-based modelling approaches. Whilst analysis of aviation incidents was done traditionally via Event Trees [9], recently a number of alternatives have been proposed [2], [7], [11], each with their own advantages and drawbacks. For the analysis of accidents and incidents in aviation, roughly two types of analysis can be distinguished in the literature, namely *retrospective analysis* (or *accident analysis*) and *prospective analysis* (or *risk analysis*). Whilst the former has the goal to determine the cause of an accident that actually took place, the latter aims to assess the likelihood of the occurrence of future accidents. Hence, although both streams have similar purposes, a main difference is that in retrospective analysis the sequence of events that have happened is known, while in prospective analysis combinatorially many sequences of events are possible. The focus of this article is on retrospective modelling.

To gain more insight in the landscape of modelling approaches in aviation safety, and to explore the usefulness of those approaches for modelling of complex systems in general, the current paper makes a comparison between four of the most influential existing modelling approaches in aviation safety: Event Trees [9], FRAM [7], STAMP [11], and the agent based modelling and simulation approach [1], [2]. The comparison is done by applying the approaches to a concrete case study on retrospective modelling of a runway incursion incident at a European airport in 1995.

In this paper, Section 1 provides an overview of the state-of-the-art regarding modelling approaches in ATM. In Section 2, the scenario used within the case study is described. Next, Sections 3-6 demonstrate how this scenario is modelled according to the four respective approaches, and Section 7 compares the four approaches based on a number of criteria. Finally, Section 8 concludes the paper with a discussion.

1. Modelling Approaches in Air Traffic Management

Based on a discussion with experts within ATM safety analysis and on the literature study, four modelling approaches have been selected to be included within our retrospective comparison: Event Trees [9], FRAM [7], STAMP [11], and LEADSTO as an example of an agent-based modelling approach [2]. The reasons for selecting the

first three approaches for this comparison were twofold. First, they are considered to be amongst the most influential approaches in the field. And second, they are sufficiently different to result in an interesting comparison. The fourth approach (LEADSTO) was selected as an example of an agent-based modelling approach due to its expressiveness with respect to cognitive states and the possibility for both qualitative and quantitative representation. Together, the four selected approaches roughly cover the landscape of modelling approaches in ATM.

Traditionally, ATM safety analyses were commonly performed based on *Event Trees* [10] (and a related approach called Fault Trees [9]). Event Trees are based on graphical representations of Boolean logic relations between success and failure types of events. It is a bottom-up approach that starts with an initiating event and ends with its consequences. Event Trees can be quantified by associating with each branch a conditional probability, given the successes/failures associated with all branches leading up to it. The approach is still widely used, although there is an increasing awareness that it has some limitations, especially when it comes to analysing dynamic systems with time-dependent interactions (see [6] for an extensive argumentation).

The Functional Resonance Analysis Method (*FRAM*) [7] provides a framework for systemically describing and evaluating functions and performance variability within ATM systems. It is more a task-oriented than an agent-oriented approach. FRAM characterises socio-technical systems by the functions they perform rather than by how they are structured. For each function that is identified, six aspects are described, namely input, output, resources, control, precondition, and time. Dynamics are captured by modelling non-linear dependencies and performance variability of system functions. Based on this, the modeller can find combinations of variability of the functions that may lead to 'functional resonance', i.e. situations where the system loses its capability to safely manage variability.

The Systems-Theoretic Accident Model and Processes (*STAMP*) methodology [11] uses system and control theory to describe socio-technical organisations. In this methodology, an accident is not understood in terms of a series of events, but rather as the result of a lack of control or the constraints imposed on the system design and operations. STAMP uses system dynamics to describe interactions and dynamics between organisational processes and their effect on safety. The variables in these types of models are typically at an aggregated organisational level, rather than at the level of individuals in the organisation.

Finally, *LEADSTO* [2] is a formal language and software environment for modelling and simulation of dynamic processes in terms of both qualitative and quantitative concepts. The LEADSTO language is a declarative order-sorted temporal language, extended with quantitative notions like integer and real. Dynamic processes can be modelled in LEADSTO by specifying the direct temporal dependencies between state properties in successive states. In [4], an agent-based model has been developed based on LEADSTO, which specifies the behaviours of agents involved in ATM scenarios in terms of cognitive agent concepts like beliefs, expectations, actions and communications. This model is largely inspired by the multi-agent dynamic risk modelling (DRM) methodology [1], [16] for the evaluation of air traffic risk. Since the LEADSTO approach shows much overlap with the multi-agent DRM approach, it was decided to only include the former in our comparison, as an example instance of an agent-based approach. However, the use of agent-based modelling within ATM is widespread (see, e.g., [5], [14]), and the authors do not intend to claim that the LEADSTO approach is synonymous with the various agent-based approaches around.

All of these approaches share the standard assumptions of the agent paradigm, such as the idea to conceptualise the ATM system as a multitude of autonomous entities, and to analyse the system's overall dynamics as emerging from the individual agent processes and their interactions. However, a detailed comparison of the pros and cons of different agent-based approaches within ATM is beyond the scope of the current paper.

2. Case Study

To make a detailed comparison between the four modelling approaches feasible, each of them was applied to model a real world scenario, involving a runway incursion incident at a large European airport in 1995. This scenario was acquired based on a semi-structured interview with a two years retired pilot of a European civil aviation company. It involves a situation where a small mistake of one actor (a pilot) could have led to severe consequences at the level of the whole system, but was corrected by other actors (an air traffic controller and another pilot) such that a possible accident was prevented. This scenario was chosen because it includes a number of aspects that pose interesting challenges for our modelling languages, such as the interaction between multiple agents, and the notion of biased human decision making.

The incident took place during the departure of an Airbus A310 of a civil aviation company from one large airport in Europe, and is summarised below (for more details on the scenario and the interview, the reader is referred to [4]):

The Airbus was preparing for the departure: the pilot-in-command was sitting on the left and the co-pilot on the right seat in the cockpit and they were ready to start taxiing. They were supposed to taxi to runway 03 in the north-east direction. The Airbus received permission to taxi and started taxiing to its runway. Approximately at the same time, a military Hercules aircraft that was ready for the departure as well received permission to taxi in the north-west direction from its parking gate. The Hercules was supposed to take off from runway 36 that crossed with runway 03 that was designated for the Airbus. Both aircraft were taxiing to their runways. During the taxiing, the Airbus received its flight route from the air traffic controllers. Some time later, when the Airbus was near the runway designated for taking off, it switched from the taxiing radio frequency to the frequency of the Tower and received permission to line up on the assigned runway. The Hercules was still at the taxiing radio frequency and also received permission to line up, while at the same time the Airbus received permission to take off at the radio frequency of the Tower. However, due to unknown reasons1, the Hercules pilot interpreted his permission for lining up as permission for taking off and started taking off on runway 36. As a result of this mistake of the pilot of the Hercules, two aircraft were taking off simultaneously on crossing runways, and none of the crews were aware of that. The air traffic controllers in the Tower observed the conflicting situation and communicated a 'STOP' signal to the pilot-in-command of the Airbus, while the Airbus was still on the ground (but at high speed). The pilot had to make a quick decision about the termination of the take-off as there is a point in this process that one cannot safely do this anymore. After having analysed the situation, the pilot-in-command of the Airbus gave a command to the co-pilot (who controlled the aircraft) to abort the take-off and start braking on the runway. During braking, the crew of the Airbus saw the Hercules flying close in the air above their own aircraft at a distance of about 5 meters. The serious collision was prevented.

[1] This misinterpretation might be explained by the fact that the pilot of the Hercules got used to the routine procedure of taxiing from the same military parking place at this airport and perhaps also of taking off from the same runway. And in many past cases, the line up procedure was often immediately followed by taking off, as permissions for lining up and taking off were sometimes given simultaneously.

3. Event Trees

To model the case study described in Section 3 using Event Trees, a first step is to identify a number of events that are play a role in the scenario, with an emphasis on events of which their presence or absence potentially results in a hazardous event. In this case, such a hazardous event, which is represented at the leaves of the Event Tree (see Figure 1), is the occurrence of a collision. Regarding the events that might lead up to this collision, the following have been identified: 1) the Hercules pilot taking off without clearance, 2) the air traffic controller detecting the conflict, 3) the controller communicating 'STOP' to the Airbus, 4) the Airbus pilot receiving this signal, 5) the Airbus pilot executing an emergency stop. Note that the choice as to which events to include is fairly subjective, and largely depends on the purpose of the analysis. In the current paper, we have focussed on events related to the role of the human agents.

After the events have been identified, the next step is to place them in the correct chronological order (see the bold headings above Figure 1), and to connect them to each other via branches. While doing that, in principle two potential outcomes (success vs. failure) can be associated to event (note that their respective probabilities have been left out in Figure 1). After that, for each combination of success/failure combinations, the analyst should determine what is the outcome at the global level (in this case: 'collision' or 'no collision'). Eventually, this results in an intuitive, easy-to-read, tree-like structure that represents a number of alternative scenarios (together with an associated outcome) for the case study. In the case of Figure 1, the number of scenarios is six, corresponding to the six different paths from root to leaf. As an example, the concrete scenario describe in the previous section corresponds to the path 'occurrence-success-success-success-success-no collision'.

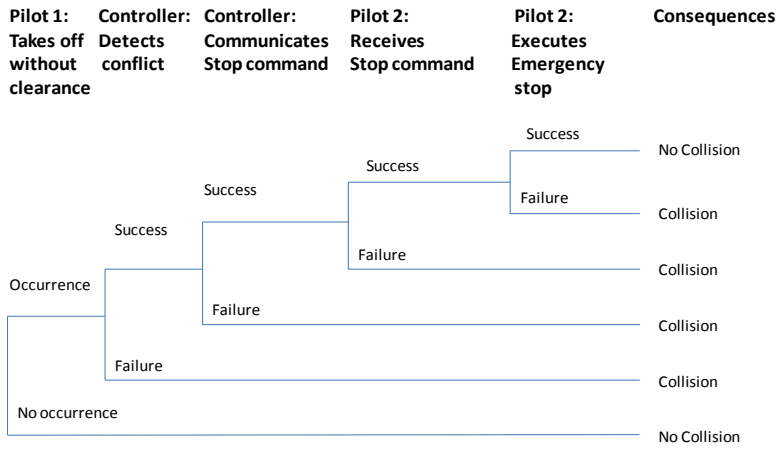


Figure 1. Event sequences related to the case study.

4. FRAM

This section describes how the case study can be modelled using FRAM. This method is an example of systemic accident modelling [7], [11]. Systemic models treat safety as an emergent property of systems as a whole, and try to find system-related vulnerabilities rather than failure of individual components. A FRAM analysis consists of four steps: 1) identification of essential system functions and characterization of each function by six basic parameters; 2) characterization of (context dependent) potential variability through common performance conditions (CPCs) and variability phenotypes; 3) defining the 'functional resonance' based on possible dependencies/couplings among functions and the potential for functional variability; 4) identification of barriers, or damping factors, that can reduce normal performance variability [7]. In this paper we focus on steps 1 and 3.

During step 1 six essential functions and their aspects related to the given incident were identified. The functions are grouped according to *operative areas*2:

-*Air traffic controllers:* Monitoring, Operational control commands issuing
-*Pilots:* Taxiing, Lining-up, Taking off, Stop taking off

There are no specified rules for the level of granularity of the functions in this analysis; global functions can be split up further into local ones when more detailed explanation of variability is required. Each function is characterised by six parameters: *input* I (which the function processes or transforms or that which starts the function), *output* O (which is the result of the function, either a specific output or product, or a state change), *preconditions* P (conditions that must exist before a function can be executed), *resources* R (what the function needs or consumes to produce the output), *time* T (temporal constraints affecting the function, e.g. with regard to starting time, finishing time, or duration) and *control* C (how the function is monitored or controlled). As an example, Table 1 illustrates the defined aspects and their descriptions of the function *Hercules Taking off*. Similar tables were developed for five other functions.

Table 1. Identification of function aspects; example for the function *Hercules Taking off*.

Function: Hercules Taking off	***Description***
Inputs	Commands of Air Traffic Controller Decision and intention to take off
Outputs	Aircraft takes off on a runway
Preconditions	Technical characteristics of aircraft
Resources	Pilot-flying, aircraft
Time	Temporal constraints based on flight schedule
Controls	Experience, expectations, training, decision making abilities, standard operating procedures (SOPs), language

[2] The FRAM methodology provides no explicit reference to agents; agency is described in terms of *operational areas* in FRAM.

In step 2, the potential for variability is described using a list of common performance conditions (CPCs), such as availability of equipment, available time and communication quality. Each CPC is then assigned one of three values: *Adequate*, *Inadequate* or *Unpredictable*, which correspond to increasing levels of performance variability. For example, for the function *Hercules Taking off* as performed by the pilot-flying of the Hercules aircraft, the CPC *communication quality* may be assigned the value *Inadequate*, since the pilot misinterpreted the line-up clearance. Due to space limitations, no further details of this step are shown here.

In step 3, links between functions are identified and an assessment is made of how coupling of functions can influence the spread of performance variability. The couplings between functions for our case study are depicted in Figure 2 (annotated with the relevant events). As shown in Figure 2, the output variability of function *Hercules Taking Off* was caused by the variability of the inadequate *control* aspect (C) of this function, namely learned routine and erroneous expectations of the Hercules pilot. At the same time the *Airbus Taking Off* function was executed normally by the Airbus pilots. Almost simultaneous execution of these two functions created the conflict situation as both aircraft were taking off on the intersecting runways. The execution of the *ATCo Monitoring* function by the tower air traffic controller resulted in the identification of the conflict situation that provides input to the *Operational control commands issuing* function. The output of the given function resulted in the generation of a stop command to the pilots of the Airbus aircraft. This output served as an input to the *Stop take off operation* function that was properly executed by the crew of the Airbus.

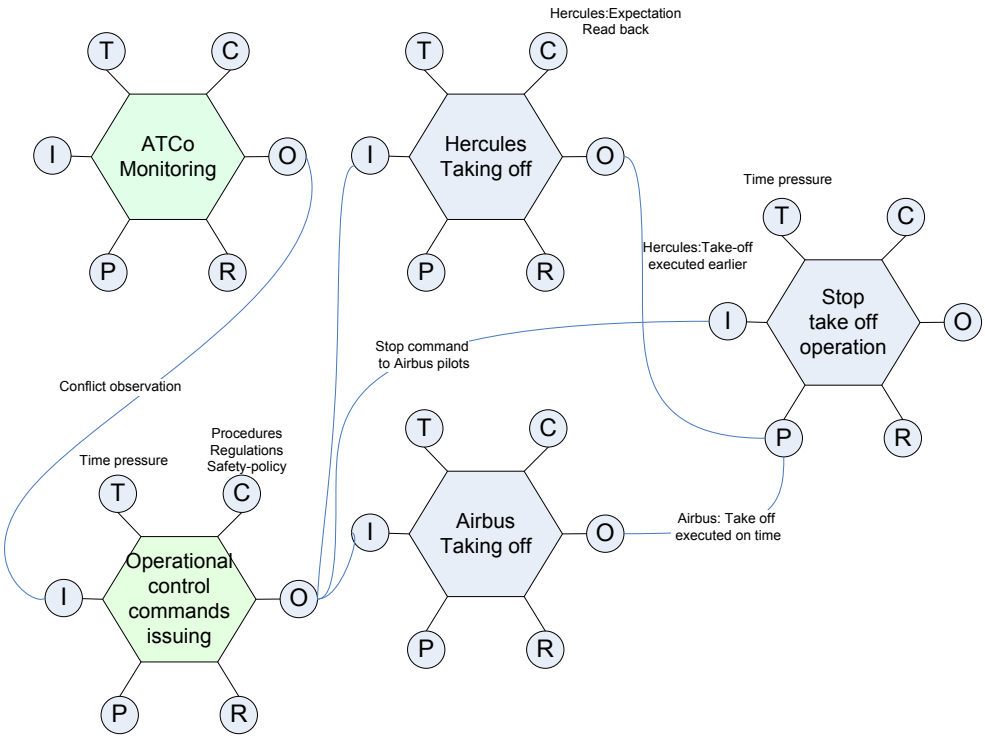


Figure 2. A FRAM instantiation with the incident data. Light-green hexagons correspond to the controllers' functions, grey hexagons correspond to the pilots' functions.

5. STAMP

The STAMP approach is also an example of systemic accident modelling that treats an accident as a result of failure of an entire system [11]. The approach comprises several steps according to the STAMP-based CAST methodology [12]: 1) Identify the system's hazards involved in the loss; 2) Identify the system's safety constraints; 3) Document the safety control structure; 4) Determine the proximate events leading to the loss; 5) Analyse the loss at the physical system level; 6) Analyse how each successive higher level of the system contributed to the inadequate control at a lower level; 7) Examine overall coordination and communication between the elements of the system; 8) Determine the dynamics and changes in the system and the safety control structure; 9) Generate recommendations. The analysis process is non-linear and there are no strictly defined requirements that one step must be completed before the next one is started [12]. The present study will focus on the first seven steps of the analysis. Further, according to the STAMP accident analysis methodology, each component of the system is described in terms of the following characteristics: safety requirements and constraints, controls, context (e.g., roles and responsibilities, environmental and behaviour-shaping factors), dysfunctional interactions and failures, reasons for the flawed control actions and dysfunctional interactions (e.g., control algorithm flaws, incorrect process models, inadequate coordination or communication, reference channel flaws, feedback flaws).

First, the general hierarchical control structure of air traffic operations in the country of the incident was constructed according to steps 3 and 7 listed above, starting from the government down to the aircraft (see Figure 3). The rectangles correspond to agents at different levels of aggregation. Control flows are represented by the solid or dotted lines and communication flow by the dashed lines.

At the highest level of this structure, the International Civil Aviation Organisation (ICAO) provides international standards for air traffic operations and communications. These guidelines are considered by local governments of the member-countries of the ICAO. Eurocontrol is a European organisation that provides safety guidelines for air traffic operations in Europe. The country where the incident occurred is a member of Eurocontrol. Recommendations concerning air traffic safety should be adopted by the governments of country-members of Eurocontrol. The government of the country participates in the decision-making processes that take part within the ICAO and Eurocontrol. This government provides the guidelines of the policy concerning transportation and funding for the airport and air traffic control organisations within the country.

At a lower level, the Ministry of Transport and Communications is responsible for making uniform rules and standards for air traffic operations and functioning of airports. Air navigation providers are responsible for work instructions, procedures and guidelines regarding functioning for air traffic controllers, while airports provide the facilities for air traffic controllers. Pilots are directly controlled by air traffic controllers that communicate clearances for different operations to the pilots. The operating

process of steering aircraft (see bottom of Fig. 3) is directly controlled by the pilots, using sensors and actuators. Airlines execute control over their pilots by means of setting general guidelines for the adherence for procedures and for aircraft exploitation. These guidelines are in turn provided by the government of the country in question. The connection between the government and the airlines is represented by a dotted line in Figure 3, as the airlines company may be from another country.

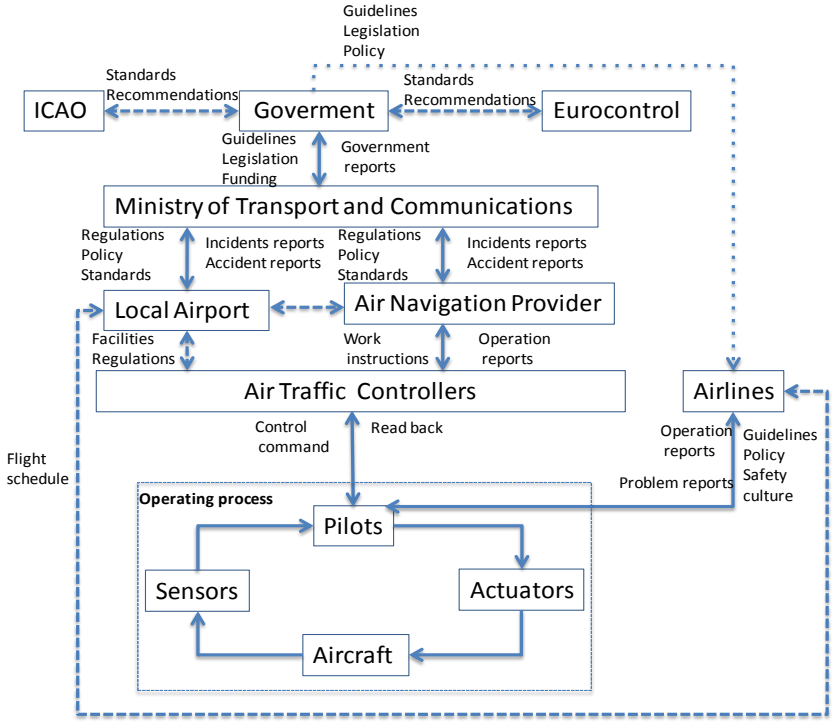


Figure 3. General hierarchical safety control structure for the case study.

Taking this general control structure into consideration along with the proximate events (in space and time) leading to the incident, a specific control structure for the incident was constructed (steps 4 and 5); see Figure 4. In this structure there are two proximate operating processes: pilots controlling the Airbus and pilots controlling the Hercules. Tower controllers are involved for giving instructions and commands to the pilots of both aircraft during the incident. The Airport Flight Operation Management department of the airport communicates flight schedule changes to the controllers and in collaboration with the Air Navigation Provider Management it defines runway usage depending on traffic flow, weather conditions and work activities in the airport.

The following safety constraint on the whole system according to step 1 of the STAMP methodology was identified: "The system safety control structure must prevent collision of aircraft". To achieve that, a safe aircraft separation should be maintained according to existing standards. This entails two main lower level constraints (step 2): 1) Air traffic controllers should monitor traffic flow, make plans and give instructions to the pilots, ensuring that the instructions are interpreted

properly; 2) Pilots should follow the commands of air traffic controllers and ensure that the commands are read back. Further analysis was performed to investigate the roles of human agents in maintaining the system's safety.

The key human components depicted in Figure 4 were selected for further analysis (steps 6 and 7): Airport Flight Operations Management, Air Navigation Provider Management, Tower Controllers, Airbus Pilot and Hercules pilot. For these components, their safety requirements and constraints, context, inadequate control actions and mental model flaws were identified. Due to the space limitations, only one example of this analysis -for the *Hercules Pilot* component- is shown in Figure 5.

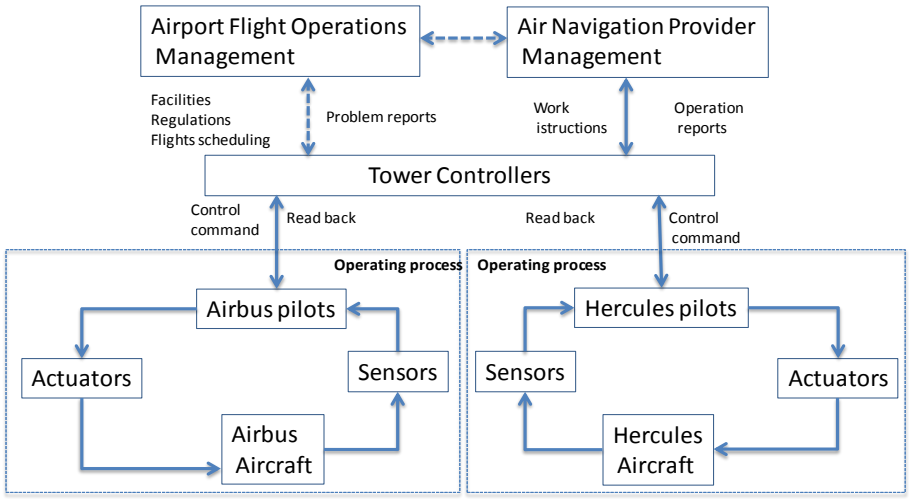


Figure 4. Proximate safety control structure based on the general control structure.

To analyse the dynamics of the system over time, the safety control structure constructed during the previous steps of the STAMP analysis can be mapped onto dynamic processes behind it (step 8). A schematic example of how this safety system can be modelled dynamically is presented in Figure 6. This dynamic model (which can be formalised in terms of differential equations if quantitative data are available) allows for investigation of safety controls that degrade over time due to changes in the system components' behaviour. For example, one can see in Figure 6 that a higher system safety status leads to a lower incident (or accident) rate, while at the same time a low incident rate results in high complacency, entailing less efforts to maintain situation awareness, which in turn may result in a higher incident accident rate.

6. LEADSTO

The specification of the case study in LEADSTO is described in detail in [4], and is summarised below. In LEADSTO, direct temporal dependencies between two state properties in successive states are modelled by *executable dynamic properties*. The

LEADSTO format is defined as follows. Let α and β be state properties as defined above. Then, the executable property $\alpha \rightarrow\!\!\!\!\rightarrow_{e, f, g, h} \beta$ means:

If state property α *holds for a certain time interval with duration g,*
then after some delay between e and f,
state property β *will hold for a certain time interval with duration h.*

Hercules Pilot

Safety requirements and constraints

- Ensure safety of the aircraft, its crew, cargo and passengers while piloting aircraft
- Complete a thorough pre-flight inspection of the aircraft
- Ensure all safety systems are working properly
- Ensure all information on the route, weather, passengers and aircraft is received
- Calculate the required runway distance depending on the weather conditions
- Consider the effects of wind and engine performance on the aircraft's fuel burn to ensure it reaches its destination safely
- Ensure the fuel levels balance safety with economy and supervise loading and fuelling of the aircraft
- Complete flight plans taking all information into consideration
- Communicate with air traffic control before take-off and during flight and landing
- Brief the cabin crew before the flight and maintaining regular contact throughout the flight
- Report and communicate problems arising during flight to air traffic controllers
- Ensure compliance of all laws and regulations
- Know all limitations applicable to the aircraft (max airspeeds for gear and flaps, max takeoff & landing weights, max temps for the engines, etc)
- Understand and interpret data from instruments and controls
- Understand and interpret instructions of air traffic controllers
- Follow commands of air traffic controllers
- Make regular checks on the aircraft's technical performance and position, on weather conditions and air traffic during flight
- Communicate with passengers using the public address system
- React quickly and appropriately to environmental changes and emergencies

Context

- Routine take off procedure at this non-busy European airport created an expectation that a line-up clearance is immediately followed by take off clearance

Inadequate control actions

- Non-compliance to take off procedure rules: pilot did not ensure that the read back of take off clearance was received by the tower controller

Mental Model Flaws

- Interpretation of line-up clearance as take off clearance

Figure 5. The role of the Hercules pilot in the incident.

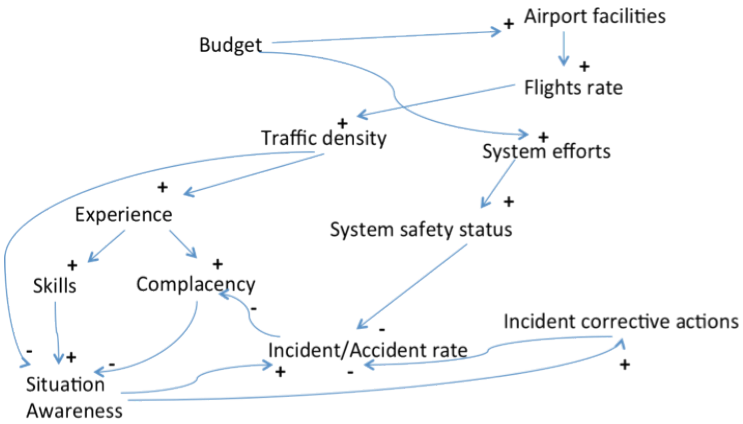
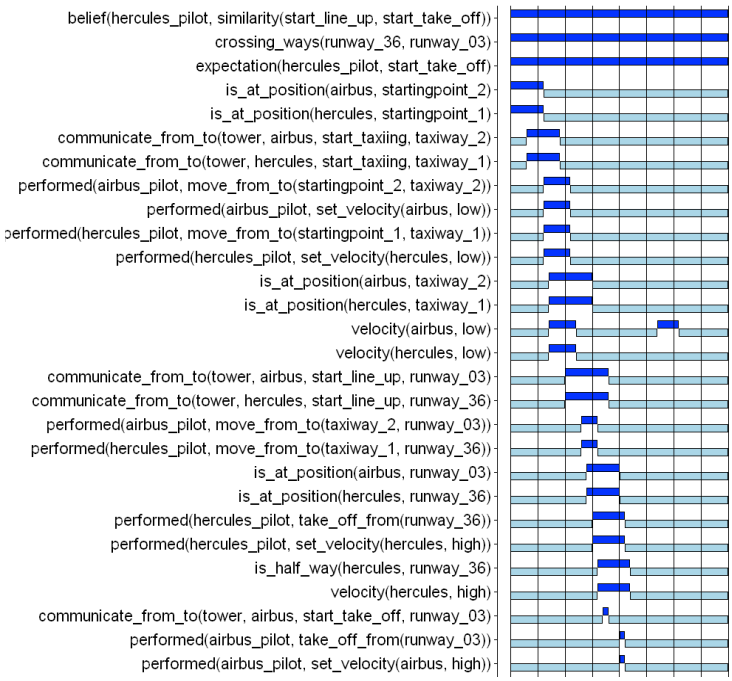


Figure 6. A simplified system dynamics model of the incident.

To formalise state properties, ontologies are specified in a (many-sorted) first order logical format: an ontology is specified as a finite set of sorts, constants within these sorts, and relations and functions over these sorts. For the ATM domain, the ontology contains n-ary predicates (or proposition symbols) such as is_at_position(A:AGENT, R:RUNWAY), belief(A:AGENT, I:INFO_EL) or expectation(A:AGENT, C:ACTION).



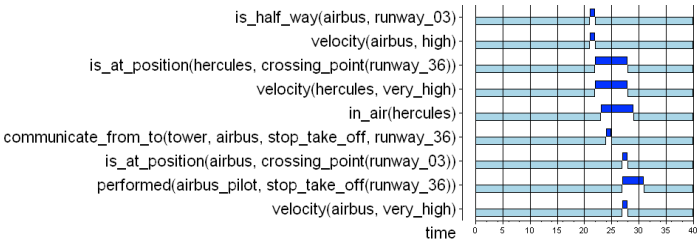


Figure 7. Example simulation run of the LEADSTO model

Next, the dynamics of the scenario are modelled by means of executable dynamic properties (EPs). These properties can be subdivided into four different categories, namely properties related to 1) belief formation, 2) communicative action generation, 3) physical action generation, and 4) information transfer. Some examples are the following (where for simplicity, the time parameters have been left out):

EP1 - Belief formation on roadway availability
observation(A:Agent, not_at_position(B:Agent, R:Roadway))
→ belief(A:Agent, is_available(R:Roadway))

EP3 - Communication Transfer
communicate_from_to(A:Agent, B:Agent, I:Action, R:Roadway) & is_pilot_of(P:Pilot, B:Aircraft)
→ incoming_communication(P:Pilot, I:Action, R:Roadway)

EP5 - Communication misinterpretation
incoming_communication(A:Agent, I1:Action, R:Roadway)
& belief(A:Agent, similarity(I1: Action, I2: Action)) & I1 ≠ I2 & expectation(A:Agent, I2:Action)
→ belief(A:Agent, I2:Action, R:Roadway)

EP16 - Take-off abort request communication
belief(tower, is_half_way(A:Aircraft, R1: Runway)) & belief(tower, is_half_way(B:Aircraft, R2: Roadway))
& belief(tower, crossing_ways(R1:Runway, R2:Roadway)) & belief(tower, velocity(B:Aircraft, high))
& not collision(A:Aircraft, B:Aircraft) & B ≠ A
→ communicate_from_to(tower, B:Aircraft, stop_take_off, R1:Runway)

Based on a specification of several EPs, the LEADSTO Simulation Environment [2] generates simulation runs. An example of such a simulation, which corresponds to the scenario of the case study, is shown in Figure 7. Here, the horizontal axis indicates a time line and the states that hold in the world are represented on the vertical axis. As shown, the pilot of the Hercules aircraft misinterprets the information communicated by the Tower because of an incorrect expectation (see atom expectation(hercules_pilot, start_take_off) at the top of the figure that is true during the whole simulation), and consequently initiates take-off without take-off clearance (see performed(hercules_pilot, take_off_from(runway_36)) from time point 15-21).

7. Comparison

To compare the four modelling approaches addressed, a number of criteria were identified using the classification frameworks presented in [3] and [10]. The three-dimensional framework described in [3] proposes classification of agent-based models across *time*, *process abstraction* and *agents clustering* dimensions. Within each dimension the 'grain size' of the representation is defined. The framework proposed in [10] describes models according to two dimensions: the scope (depth) and the purpose of a model. Some additional criteria were identified based on practical observations made during our incident analysis. All criteria are listed in Table 2. They can be roughly divided into two groups. The first group predominantly contains concepts that relate to the expressive power of the model:

- *Formalisation* indicates whether the model can be expressed in a formal language
- *Simulation* refers to the possibility of performing simulations of a model's behaviour over time
- *Time dynamics* indicates the possibility of expressing temporal aspects
- *Process abstraction level* refers to the 'grain size' of the real world processes that are represented by a model, e.g. physiological, cognitive, behavioural, or social [3]
- *Time abstraction level* refers to the 'grain size' of the temporal dimension (if any) represented by a model, e.g. local transitions between subsequent time points or global descriptions that cover the development of processes over longer time periods [3]
- *Agent clustering abstraction level* characterises the 'grain size' of the groups of agents considered within a model (e.g., individual or population-based) [3]
- *Qualitative representation* defines whether a model allows for qualitative representations of concepts (e.g., as in logic)
- *Quantitative representation* defines whether a model allows for quantitative representations of concepts (e.g., as in mathematics)
- *Agency* defines whether an approach differentiates between individuals or intelligent components that perform autonomous actions
- *Cognitive states representation* indicates whether an approach allows for the representation of cognitive states, such as beliefs, desires or intentions
- *Cognitive processes representation* implies that an approach is allows for the representation of cognitive processes, such as reasoning, creation of situation awareness, etc.
- *Probabilistic relations* refers to the possibility to model non-deterministic relations

The second group of criteria relates to the usage of the model:

- *Not time-consuming* means that the process of modelling does not take much time and effort
- *Usability* indicates whether the approach is easy to work with (i.e., user-friendly, also for laymen)
- *Bottom-up approach* indicates an approach where the 'model fits the data'; models within this approach are *descriptive* models [10]
- *Top-down approach* indicates an approach where the 'data fit the model'; models within this approach are *normative* models [10]

While modelling the case study using Event Trees, it became clear that the selection of relevant events is quite subjective and can be influenced by the hindsight: one identifies the events that are assumed to be the causes of an incident. Other possible alternative events are often not considered during this analysis. The outcome of this analysis is a sequence of relevant events that may or may not lead to an

accident/incident. It is obvious that Event Trees is a rather simplistic method regarding expressiveness. Though user-friendly and not time consuming (see Table 2), it has limitations w.r.t. modelling complex, non-linear processes on a formal level.

Application of the STAMP approach to the case study revealed considerable comprehensiveness and depth of the analysis, starting from the hierarchical control structure with the international organisations and government on the top to a thorough qualitative analysis of each component of the structure and the dynamics of system's processes. However, such analysis requires a vast amount of information not only in safety domain, but also regarding the cultural, historical and political context and the management and structure of all organisations involved, which may be quite time-consuming to obtain. Another problem with the accessibility of such information is that many issues related to organisational safety are company confidential. Hence, a STAMP-based analysis is not trivial to be applied by safety specialists. Indeed, Salmon et al. [13] state that the STAMP theory and analysis approach has not yet been accepted outside the academic circles. The hierarchical structure generated during this type of analysis can be regarded as a static organisational structure while the formal system's dynamic model is more process-based. In general, STAMP is a good approach w.r.t. the scope of the analysis and can be applied in modelling and simulation as it has a substantial formal basis as well. This method generates models at different levels of abstraction, both qualitative and quantitative.

Table 2. Comparison between modelling approaches.

Criterion	Event Trees	STAMP	FRAM	LEADSTO
Formalisation	-	+	-	+
Simulation	-	+	-	+
Time dynamics	+	+	-	+
Processes abstraction level	macro	mixed	micro	micro
Time abstraction level	micro	mixed	-	mixed
Agent clustering abstraction level	micro	mixed	-	mixed
Qualitative Representation	+	+	+	+
Quantitative Representation	-	+	-	+
Agency	+	+-	-	+
Cognitive states representation	-	+	-	+
Cognitive processes representation	-	-	+	+
Probabilistic relations	+	-	-	+
Not time-consuming	+	-	-	-
Usability	+	+-	+	-
Bottom-up approach	+	-	+	+
Top-down approach	-	+	-	-

As far as FRAM is concerned, its application demonstrated substantial flexibility in defining system's functions. There are no guidelines regarding granularity of relevant functions; the functions can be split or combined depending on the depth of analysis. Moreover, the notion of agency is often hidden in this analysis. Nevertheless, the outcome of the FRAM analysis is a quite comprehensive description of a system's functions, functions' variability and couplings between the functions. One significant disadvantage of this method is that it is not computational, hence it does not allow performing simulations. Some simple kind of simulation, however, is possible by showing multiple pictures with functions' couplings, annotated with time stamps.

Finally, LEADSTO may also be time-consuming (especially for non-experts), as it requires representation of the dynamics of a process in terms of a large number of relations between states over time. An advantage is that the modeller is free to define the desired level of abstraction. The output of the method is a dynamic multi-agent model, which can be used to generate detailed simulation traces. Another asset of this approach is that it allows for both quantitative and qualitative representation within one model and representation of both cognitive states and cognitive processes.

8. Discussion

This article presented a case-study based comparison of the retrospective modelling capabilities of four contemporary accident analysis methods: Event Trees, FRAM, STAMP and LEADSTO. The main contributions were: 1) models of the case study incident according to the four methodologies, 2) identification of key criteria for comparison and 3) comparison of the models based on these criteria and practical observations during the application of the given approaches.

Depending on the modelling purpose and importance of certain criteria, the analyst can select the most appropriate modelling approach. For instance, if the historical context of an organisation is crucial for understanding particular phenomena, the STAMP methodology is the most appropriate one. If one is predominantly interested in descriptive characteristics of organisational functions and their interactions without the direct necessity of performing simulations, then one would opt for the FRAM approach. For a quick superficial analysis of the events and the agents involved, the Event Tree approach the most appropriate one. Finally, LEADSTO offers the possibility to simulate cognitive processes at an individual level, although it requires some background knowledge on the formalism.

The main limitation of the current study is that the comparison of the approaches has been made by their application to only one incident. However, the basic characteristics of the approaches and their expressive capabilities become vivid even during their application to one case study.

The runway incursion incident described in this study is a vivid example of a system where coordination and communication between agents play a crucial role. In this example the interplay between poor communication and erroneous information processing human agent resulted in a serious incident, rather than the failure of an individual component. This paper demonstrated the extent to which the four approaches are able to grasp these dynamics of a complex socio-technical system.

Note that the current analysis focused on the analysis of an existing incident, i.e., on retrospective analysis. In follow-up research, it is worthwhile to compare the four modelling approaches on their prospective capabilities. Such a comparison might involve different evaluation criteria, such as the capability of the approaches to run large numbers of simulations (as in Monte Carlo simulation). In this respect it is of interest that [15] compares the prospective analysis capabilities of an event sequence based safety assessment versus an agent-based Dynamic Risk Modelling approach.

References

[1] H.A.P. Blom, G.J. Bakker, P.J.G. Blanker, J. Daams, M.H.C. Everdij, M.B. Klompstra: Accident risk assessment for advanced air traffic management. In: Donohue, G.L. and Zellweger, A.G. (eds.), *Air Transport Systems Engineering, AIAA* (2001), 463-480.

[2] T. Bosse, C.M. Jonker, L. van der Meij and J. Treur: A Language and Environment for Analysis of Dynamics by SimulaTiOn. *International Journal of AI Tools* **16 (3)** 2007, 435-464 (2007)

[3] T. Bosse, M. Hoogendoorn, M.C.A. Klein and J. Treur: A Three-Dimensional Abstraction Framework to Compare Multi-Agent System Model. In: Pan, J.-S., Chen, S.-M. and Nguyen, N.T. (eds.), *Proc. of the 2nd Int. Conference on Computational Collective Intelligence, ICCCI'10, Part I. LNAI,* vol. **6421**, Springer Verlag (2010), 306-319.

[4] T. Bosse and N. Mogles: Studying Aviation Incidents by Agent-Based Simulation and Analysis. In: Filipe, J. (ed.), *Proceedings of the Fifth International Conference on Agents and Artificial Intelligence, ICAART'13*. INSTICC Press (2013)

[5] S. Bouarfa, H.A.P. Blom and R. Curran: Airport Performance Modeling using an agent based Approach. *Proceedings of ATOS 2012*, Delft, The Netherlands (2012), 427-442.

[6] M.H.C. Everdij: Review of techniques to support the EATMP Safety Assessment Methodology. Report for EEC Safety Methods Survey project, Volume I and II (2004)

[7] E. Hollnagel, *Barriers and accident prevention*, Aldershot, Ashgate, 2004.

[8] E. Hollnagel, D.D. Woods and N. Leveson: *Resilience engineering: Concepts and precepts*. Ashgate, Aldershot, England, 2006.

[9] B. Kirwan: *A guide to practical human reliability assessment*, Taylor and Francis. 1994.

[10] J.-C. Le Coze, Disasters and organisations: From lessons learnt to theorising. *Safety Science* **46** (2008), 132-149.

[11] N. Leveson: A new accident model for engineering safer systems. *Safety Science* **42**, (2004), 237-270.

[12] N. Leveson. *Engineering a safer world: Systems thinking applied to safety*, MIT Press, 2011

[13] P.M. Salmon, M. Cornelissen and M. J. Trotter: Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP. *Safety Science* **50** (2012), 1158-1170.

[14] SESAR JU: Complex World Position Paper, Report D23.2, 21st December 2012 (2012)

[15] S.H. Stroeve, H.A.P. Blom and G.J. Bakker: Contrasting safety assessments of a runway incursion scenario: event sequence analysis versus multi-agent dynamic risk modelling, *Reliability Engineering and System Safety* **109**, (2013), 133-149.

[16] S.H. Stroeve, H.A.P. Blom and G.J. Bakker: Systemic accident risk assessment in air traffic by Monte Carlo simulation. *Safety Science* **47** (2009), 238-249.

[17] M. de Vos, N. Fornara, J.V. Pitt and G. Vouros, G. (eds.): Coordination, Organizations, Institutions, and Norms in Agent Systems VI. Springer LNAI, volume **6541** (2011)

[18] http://en.wikipedia.org/wiki/Air_France_Flight_447

[19] http://www.eurocontrol.int/articles/what-air-traffic-management