Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

## Executive summary

# Organizational safety modelling and analysis of an air traffic application

## EUROCONTROL CARE Innovative Research III


**Problem area**
It is now generally well realized that the level of safety of air traffic operations depends on the constraints and resources set by people working at the blunt end (e.g. managers), which determine the working conditions and thereby the performance of people (e.g. pilots, controllers) who are directly controlling potentially hazardous processes at the sharp end. Notwithstanding the recognition of the importance of organizational processes for safe operations, formal models describing organizational processes and their effect on safety-relevant scenarios are largely lacking in the current air traffic risk assessment practice.

**Description of work**
As a way forward for the description of organizational processes and inclusion thereof in air traffic safety assessment methods, NLR and Vrije Universiteit Amsterdam collaborate in an Eurocontrol CARE Innovative Research III project. The objective of this research project is to enhance safety analysis of organizational processes in air traffic by development of formal approaches for modelling, simulation and analysis of organizational relationships and processes. This report presents a new approach to this end.

**Results and conclusions**
The applied approach describes a formal organization in three views: (1) organization-oriented view, describing roles, their interactions and authority relations, (2) performance-oriented view, describing goals and performance indicators, and (3) process-oriented view, describing tasks, processes, resources and their relations. A fourth agent-oriented view represents the link between the role-based formal organizational model and the agents that fulfil the roles. The performance of the agents is determined by the formal organization, but also influenced by the stochastic dynamics of interacting agents. With these four interrelated views a broad scope of organizational modelling is achieved. The modelling approach supports safety assessment by identification of inconsistencies and evaluation of safety-relevant performance both at the level of the formal organization and at the level of interacting agents.

**Applicability**
This research supports safety modelling and assessment of organizational processes.



**Report no.**
NLR-CR-2007-457



**Author(s)**
S.H. Stroeve
A. Sharpanskykh
H.A.P. Blom



**Report classification**
UNCLASSIFIED

**Date**
November 2007

**Knowledge area(s)**
Safety & Security

**Descriptor(s)**
Safety
Modelling
Organization

Nationaal Lucht- en Ruimtevaartlaboratorium, National Aerospace Laboratory NLR

Anthony Fokkerweg 2, 1059 CM Amsterdam,
P.O. Box 90502, 1006 BM Amsterdam, The Netherlands
Telephone +31 20 511 31 13, Fax +31 20 511 32 10, Web site: www.nlr.nl

Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-CR-2007-457

# Organizational safety modelling and analysis of an air traffic application

## EUROCONTROL CARE Innovative Research III

S.H. Stroeve, A. Sharpanskykh* and H.A.P. Blom

*Vrije Universiteit Amsterdam

| | |
|---|---|
| Customer | Eurocontrol |
| Contract number | C06/12396BE |
| Owner | Eurocontrol |
| Division | Air Traffic |
| Distribution | Unlimited |
| Classification of title | Unclassified |
| | November 2007 |

Approved by:

| Author | Reviewer | Managing department |
|---|---|---|
| | | |

## Summary

This report presents results of year-1 research in the EUROCONTROL CARE Innovative Research III project on safety modelling and analysis of organizational processes in air traffic. It is the objective of this research project to enhance safety analysis of organizational processes in air traffic by development of formal approaches for modelling, simulation and analysis of organizational relationships and processes. These approaches should explicitly relate organizational processes at the blunt end (e.g. management, regulation) with working processes at the sharp end where accidents may occur.

The year-1 research includes a literature survey (Stroeve et al., 2007), leading to identification of promising approaches, and application of the most viable approach to an air traffic case on safety occurrence reporting (this report).

The applied approach describes a formal organization in three views: (1) organization-oriented view, describing roles, their interactions and authority relations, (2) performance-oriented view, describing goals and performance indicators, and (3) process-oriented view, describing tasks, processes, resources and their relations. A fourth agent-oriented view represents the link between the role-based formal organizational model and the agents that fulfil the roles. The performance of the agents is determined by the formal organization, but also influenced by the stochastic dynamics of interacting agents. With these four interrelated views a broad scope of organizational modelling can be achieved. The modelling approach supports safety assessment by identification of inconsistencies and evaluation of safety-relevant performance both at the level of the formal organization and at the level of interacting agents.

# Contents


**1 Introduction 8**

**2 Air traffic case 11**

**3 Development of an organizational model 13**

3.1 Introduction 13
3.2 Step 1: Identification of organizational roles 14
3.3 Step 2: Identification of interactions between roles and with the environment 16
3.4 Step 3: Identification of requirements for roles 21
3.5 Step 4: Identification of organizational performance indicators and goals 23
3.6 Step 5: Identification of resources 31
3.7 Step 6: Identification of organizational tasks and relations between tasks, resources and goals 32
3.8 Step 7: Identification of authority relations 36
3.9 Step 8: Identification of the flows of control 38
3.10 Step 9: Identification of allocation, characteristics and behaviour of agents 40
3.11 Step 10: Identification of organizational constraints 43
3.12 Organizational model of informal reporting of occurrences 45

**4 Consistency analysis of the organizational model 47**

4.1 Consistency analysis of the performance-oriented view 47
4.2 Consistency analysis of the process-oriented view 49
4.3 Consistency analysis of the organization-oriented view 50

**5 Agent-based simulation of the organizational model 52**

5.1 LEADSTO simulation technique 52
5.2 Simulation results for safety occurrence reporting 54

**6 Discussion 56**

**7 References 59**

**Appendix A Temporal Trace Language 62**

Appendix B Details of the formal organizational model 64

Appendix C Model details for informal discussion of occurrences 88

## Abbreviations

| | |
|---|---|
| ANSP | Air Navigation Service Provider |
| AODU | Airport Operation Design Unit |
| ATC | Air Traffic Control |
| ATO | Air Traffic Organization |
| CST | Controllers Supervision Team |
| EMATC | Executive Management ATC |
| NODT | New Operation Design Team |
| OAU | Operation Assessment Unit |
| ODU | Operation Design Unit |
| OMT | Operation Management Team |
| RIAS | Runway Incursion Alert System |
| SIU | Safety Investigation Unit |
| SMU | Safety Management Unit |
| TCU | Tower Control Unit |

# 1 Introduction

In complex and distributed organizations like the air traffic industry, safe operations are the result of interactions between many entities of various types at multiple locations. Such organizations can be described at various aggregation levels. At a high aggregation level such a description discerns companies/corporations (e.g. air traffic control centres, airlines, airports, regulators), zooming in at lower aggregation levels it discerns departments/groups (e.g. safety department, control tower group, operational management team), and at the lowest aggregation level it distinguishes the performance of single human operators executing organizational tasks in their organizational habitats, usually including knowledge and procedure intensive interactions with technical systems and other human operators (e.g. pilots, air traffic controllers, maintenance personnel, supervisors). In safety-focused organizations like airlines and air traffic control centres, it is important to have a good understanding of the organizational structures and dynamics at the different aggregation levels, since misconceptions and inconsistencies in the organizational structure and dynamics may contribute to the development of incidents and accidents.

The importance of proper organizational processes for the safety of complex operations is currently well realised. It is generally acknowledged that the level of safety achieved in an organization depends on the constraints and resources set by people working at the blunt end (e.g. managers, regulators), which determine the working conditions of practitioners who are directly controlling hazardous processes at the sharp end (e.g. pilots, controllers, physicians). The well known Swiss cheese model of Reason (1997) illustrates that accidents may occur if multiple holes, reflecting active failures and latent conditions in an organization, are aligned. Messages similar to those of Reason (1997) have been put forward by Turner (1978) and Pidgeon and O'Leary (2000) in their man-made disasters theory. The man-made disasters theory states that, despite the best intentions of all involved, the objective of safely operating technological systems could be subverted by some very familiar and 'normal' processes of organizational life. Man-made disasters theory highlights how system vulnerability often arises from unintended and complex interactions between contributory preconditions, each of which singly would be unlikely to lead to an accident. Also Perrow (1984) provided early descriptions of accidents as the consequence of complex interactions in sociotechnical systems and considers such accidents to be 'normal'.

In the literature and in the risk assessment practice, the recognition of the importance of organizational processes for safe operations has mostly been accommodated by high-level conceptual models and to some extent by organizational influencing factors in accident models. Predominantly, formal risk assessment approaches focus on fault/event tree type of analysis, which uses sequential cause-effect reasoning for accident causation. Recent views on accident causation indicate that these types of accident models may not be adequate to represent the complexity of modern socio-technical systems (Hollnagel 2004, Leveson 2004, Sträter 2005, Hollnagel et al. 2006, Le Coze 2005, Reason et al. 2006). Limitations of frequently applied accident models as fault/event trees include the difficultness to represent the large number of dynamic interdependencies between organizational entities and their restrictive error-view on human performance.

To adequately account for the effects of the complexity of socio-technical organizations in safety assessment, above recent views indicate that we need analysis approaches that account for the variability in the performance of interacting organizational entities and the emergence of safety occurrences from this variability. In the terminology of Hollnagel (2004) this is a systemic accident model. The systemic view considers accidents as emergent phenomena from the variability of an organization and thus passes the limitations of sequential accident models in accounting for the dynamic and non-linear nature of the interactions that lead to accidents. In current risk assessment practices, formal models that describe the variability of organizational processes and its effect on safety-relevant scenarios are largely lacking.

As a way forward for description of organizational structures and processes and inclusion thereof in air traffic safety assessment methods, NLR and Vrije Universiteit Amsterdam collaborate in an Eurocontrol CARE Innovative Research III project. It is the objective of this research project to enhance safety analysis of organizational processes in air traffic by development of formal approaches for modelling, simulation and analysis of organizational relationships and processes. These models should describe the organization at different aggregation levels and should lead to emergent safety issues as result of performance variability and interactions of organizational entities. In other words, it is intended to develop an approach for systemic accident modelling of air traffic organizational processes.

The first phase of this research project consists of (1) a literature survey on safety modelling and analysis of organizational processes, and (2) a first application of identified methods to a safety-relevant organizational process in air traffic. The literature survey is reported in (Stroeve et al., 2007). It follows from the literature survey that the organizational modelling framework proposed by Popova and Sharpanskykh (2007e) presents the widest repertoire of multi-agent organizational modelling features of the methods considered. Therefore, this framework has been chosen to study the possibilities of organizational modelling in an air traffic case.

The current report describes the modelling process and model results. Section 2 introduces the case study. Section 3 describes the steps in the development of the organizational model for the air traffic case. Section 4 presents methods and results for consistency analysis of the organizational model. Section 5 presents methods and results for agent-based simulation of the organizational model. Section 6 presents a discussion and recommendations for further research.

# 2 Air traffic case

In this report we study the possibilities of organizational modelling in air traffic for the case of reporting and management of safety occurrences during taxiing operations across and near an active runway of a fictitious major airport. It is considered that the runway crossing operation has recently been developed in relation with new infrastructure on the airport. The runway considered has a complex surrounding taxiway structure, it is in use for take-offs and it may be crossed by taxiing aircraft. Traffic movements on the runway and surrounding taxiways are under control of, respectively, a runway controller and ground controllers.

In this operational context safety-relevant events may occur. For the purpose of this study, we consider the following safety-relevant events:

*a.* Aircraft rejects take-off as result of a runway incursion;
*b.* Taxiing aircraft stops progressing on the runway crossing only after the stopbar and due to a call by the runway controller;
*c.* Taxiing aircraft makes wrong turn and progresses towards the runway crossing;
*d.* Taxiing aircraft makes wrong turn and progresses on a wrong taxiing route that is not a runway crossing;
*e.* Taxiing aircraft has switched to a wrong frequency;
*f.* Taxiing aircraft initiates to cross due to misunderstanding in communication.

To support effective safety management, such events should be reported by the involved pilots and controllers. In the air traffic case, we consider that reporting of safety occurrences can be done either via formal organizational lines or via informal coordination. The formal organization considers safety occurrence reporting at the air traffic control centre and at airlines, the informal path considers coordination between air traffic controllers.

The formal safety occurrence reporting at the air traffic control centre starts by the creation of a notification report by the involved controller(s). This notification report is examined and possibly improved by the supervisor. The notification report is processed by the safety investigation unit of the air traffic control centre. The severity of the occurrence is assessed and a description of the event is stored in a safety occurrences database. In the case of single severe occurrences or in the case of a consistent series of less severe occurrences, the safety investigation unit may initiate an investigation for possible causes that may pinpoint to problems in the operations. The results of such an investigation are reported to the operation management team at the air traffic control centre. On the basis of such reporting, the operation management team may decide on a change process of the operation. This may have to be formally approved by the executive management of the air traffic control centre.

The organization of the safety occurrences processing at the airline starts with a notification report created by the pilots. This notification report may be provided to the airline's safety management unit or it may be directly provided to the regulator. The airline's safety management unit examines and potentially improves the report and it informs the regulator about safety occurrences at the airline. The regulator may decide on further investigation of safety occurrences by the regulator itself or by a facilitated external party. Involved airlines and air traffic control centre are informed by the regulator about the investigation results, which may indicate safety bottlenecks in the operation.

The informal safety occurrence reporting path at the air traffic control centre considers that controllers discuss during breaks the occurrences that happened in their control shifts. If they identify potential important safety issues they inform the head of controllers, who is a member of the operation management team. The operation management team may decide on further investigation of the potential safety issue. The results of such investigation are handled as in the formal safety occurrence reporting path.

The development of a formal organizational model along the methods of (Popova and Sharpanskykh 2007e) for the incident reporting mechanisms in the context of the newly designed taxiing operations is presented next in Section 3. The prime aim of this modelling is to analyse the possibilities of air traffic organizational modelling for safety assessment. This will be illustrated by evaluation of inconsistencies in the organization and simulation-based results for the effectiveness of incident reporting mechanisms.

# 3 Development of an organizational model

## 3.1 Introduction

For the development of a formal organizational model in the case study considered in this report, the formal framework for organization modelling and analysis is used (Popova and Sharpanskykh 2007e). This framework introduces four interrelated views on organizations:

- The *organization-oriented view* describes organizational roles, their authority, responsibility and power relations;
- The *performance-oriented view* describes organizational goal structures, performance indicators structures, and relations between them;
- The *process-oriented view* describes organizational functions and processes, how they are related, ordered and synchronized and the resources they use and produce;
- The *agent-oriented view* describes agents' types with their capabilities, models of agent behaviour based on social theories, and principles of allocating agents to roles.

A formal organizational model comprises the specifications of all these views.

In (Popova and Sharpanskykh 2007e) a number of general methodological guidelines in the form of design steps for creating a formal organizational model using the framework from (Popova and Sharpanskykh 2007e) have been identified. By executing these steps, parts of an organizational model corresponding to the specifications of different views of the framework are described. Furthermore, some steps aim at the establishing of relations between the specifications of different views (i.e., between different parts of an organizational model). In general, the designer has freedom to apply these steps in different sequences. The description of the design procedures that are applied for creating a formal organizational model for the case study considered in this report, is given in Table 1.

*Table 1: Overview of steps in organizational modelling and their relation with the views considered.*

| Step | Name | View | | | |
|---|---|---|---|---|---|
| | | Organization | Performance | Process | Agent |
| 1 | Identification of organizational roles | x | | | |
| 2 | Identification of interactions between roles and with the environment | x | | | |
| 3 | Identification of requirements for roles | x | | | x |
| 4 | Identification of organizational performance indicators and | | x | | |

| | | | | | |
|---|---|---|---|---|---|
| | goals | | | | |
| 5 | Identification of resources | | x | | |
| 6 | Identification of organizational tasks and relations between tasks, resources and goals | | x | x | |
| 7 | Identification of authority relations | x | | x | |
| 8 | Identification of flows of control | | | x | |
| 9 | Identification of allocation, characteristics and behaviour of agents | | | | x |
| 10 | Identification of organizational constraints | x | x | x | x |

Via steps 1-8 and 10 the formal organisation is specified, i.e. the organization as it is prescribed in formal organizational documents (e.g. organizational charts, job descriptions, procedures, regulations). In contrast, step 9 aims at the identification of possible (realistic) variations and deviations of/from the prescribed organizational structure and behaviour that may be attributed to agents allocated to the organizational roles.

The development of an organizational model according to these modelling steps for the air traffic case on safety occurrence reporting is presented next. First, Sections 3.2 to 3.11 present the model development for the formal occurrence reporting paths, subsequently, Section 3.12 describes the additional model elements for the informal occurrence reporting paths. Modelling details are provided in Appendices A, B and C.

### 3.2 Step 1: Identification of organizational roles

In this step organizational roles are identified, both simple and composite ones and subrole-relations between them are established. By performing this step a part of the specification for the organization-oriented view is described.

A role represents a (sub-)set of functionalities of (part of) an organization, which are abstracted from specific agents who fulfil them. Each role can be composed by several other roles, until the necessary detailed level of aggregation is achieved, where a role that is composed of (interacting) subroles, is called a composite role. At the highest aggregation level, the whole organization can be represented as one role. Each role has an input and an output interface, which facilitate in the interaction (communication) with other roles. Graphically, a role is represented as an ellipse with white dots (input interfaces) and black dots (output interfaces); see e.g. Figure 2 on page 17.

The conceptualized environment represents a special component of an organization model. To model the environment either an aggregated view may be taken (e.g., to represent the global behaviour of markets) or a more elaborated specification of the environment may be created. In the latter case, the internal specification for the environment can be specified using an existing world ontology. It can be also defined by a set of objects with certain properties and states and with causal relations between objects. In general, no particular restrictions on the representation of the environment are imposed by the framework. Similarly to roles, the environment has input and output interfaces, which facilitate in the interaction with roles of an organization. Graphically, the environment is depicted as a rectangle with rounded corners (see e.g. Figure 3f on page 18).

In the case for the organization of air traffic, roles are represented at three aggregation levels. Table 2 shows all the generic roles. Based on these generic roles, role instances may be defined for particular applications. For instance, different number of instances of the role Airline may be considered.

*Table 2: Identified organizational roles at three aggregation levels.*

| Level 1 | Level 2 | Level 3 |
|---|---|---|
| Air Navigation Service Provider | ATC Executive Management | - |
| | Operation Management Team | Team Member (CSU) |
| | | Team Member (ODU) |
| | | Team Member (Systems) |
| | | Team Member (Maintenance) |
| | | OMT Leader |
| | Operation Assessment Unit | Operation Analyst |
| | | Head OAU |
| | Operation Design Unit | Operation designer |
| | | Head of ODU |
| | Safety Investigation Unit | Safety Investigator |
| | | Head of SIU |
| | Tower Control Unit | Ground Controller |
| | | Runway Controller |
| | | Tower Controllers Supervisor |
| | | Env (Environment) |
| | Controllers Supervision Team | Controllers Supervisor |
| | | Head of Controllers |
| Airport | Airport Operation Design Unit | Airport Operation Designer |
| | | Head AODU |
| | Airport Management | - |
| Airline | Airline Management | - |

| | | |
|---|---|---|
| | Safety Management Unit | - |
| | Crew | Pilot in command |
| | | Second Pilot |
| | | Env (Environment) |
| Regulator | - | - |
| New Operation Design Team | Design Team Manager | - |
| | ANSP design representative | - |
| | Airport design representative | - |
| | Airline representative | - |

### 3.3 Step 2: Identification of interactions between roles and with the environment

In this step, interaction relations between roles, roles and the environment are identified. To enable interaction, for each role interfaces specified by interaction ontologies are identified. This step, as well as step 1, contributes to the development of the organizational specification for the organisation-oriented view.

**Interaction relations between roles and with the environment**

Relations between roles are represented by interaction and interlevel links:

- An *interaction link* represents an information channel between two roles at the same aggregation level. Graphically, it is depicted as a solid arrow, which denotes the direction of possible information transfer (see e.g. Figure 2 on page 17).
- An *interlevel link* connects a composite role with one of its subroles. It represents information transition between two adjacent aggregation levels. Graphically, it is depicted as a dashed arrow, which shows the direction of the interlevel transition (see e.g. Figure 2 on page 17).

To enable the interaction between subroles of two composite roles, interaction roles may be defined. Such interaction roles consist of the representatives of both composite roles that interact with each other on behalf of the corresponding composite roles.

Agents allocated to organizational roles may be capable of interacting with the environment. On the one hand, they are capable of observing states and properties of objects in the environment; on the other hand, they can act or react and, thus, affect the environment. Roles interact with the environment by means of environment interaction links. Graphically, this links are depicted as dotted arrows, which denote the direction of possible information transfer.

For the air traffic organizational model, relations between roles can be depicted at the three identified aggregation levels. The interaction relations between the roles at aggregation level 1 of the complete air traffic organization are depicted in Figure 1. The subroles of the role ANSP are depicted at aggregation level 2 in Figure 3 and at aggregation level in Figure 3. The subroles of the role New Operation Design Team, the role Airport and the role Airline are depicted Figure 4, Figure 5 and Figure 6, respectively; these subroles include definitions at aggregation levels 2 and 3. Note that in principle the environment may be included in almost every composite role of the air traffic organizational model, as almost all of these roles and their subroles interact with the environment in reality. However, for the purposes of this case study, only the interactions of the controllers and the pilots with the environment are modelled explicitly.

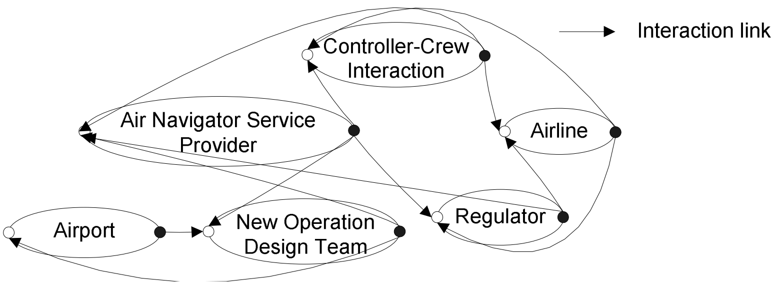


*Figure 1: The interaction relations between the generic roles at the aggregation level 1*

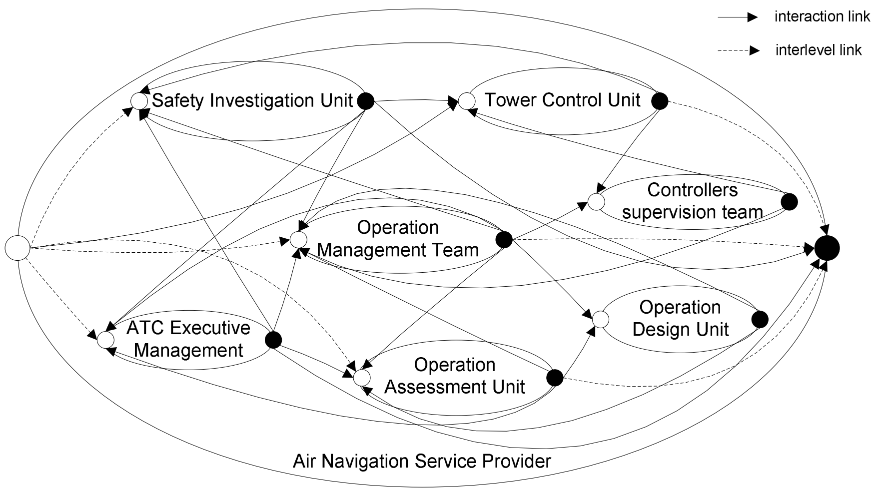


*Figure 2: The interaction relations between the subroles of the role Air Nativation Service Provider at the aggregation level 2*

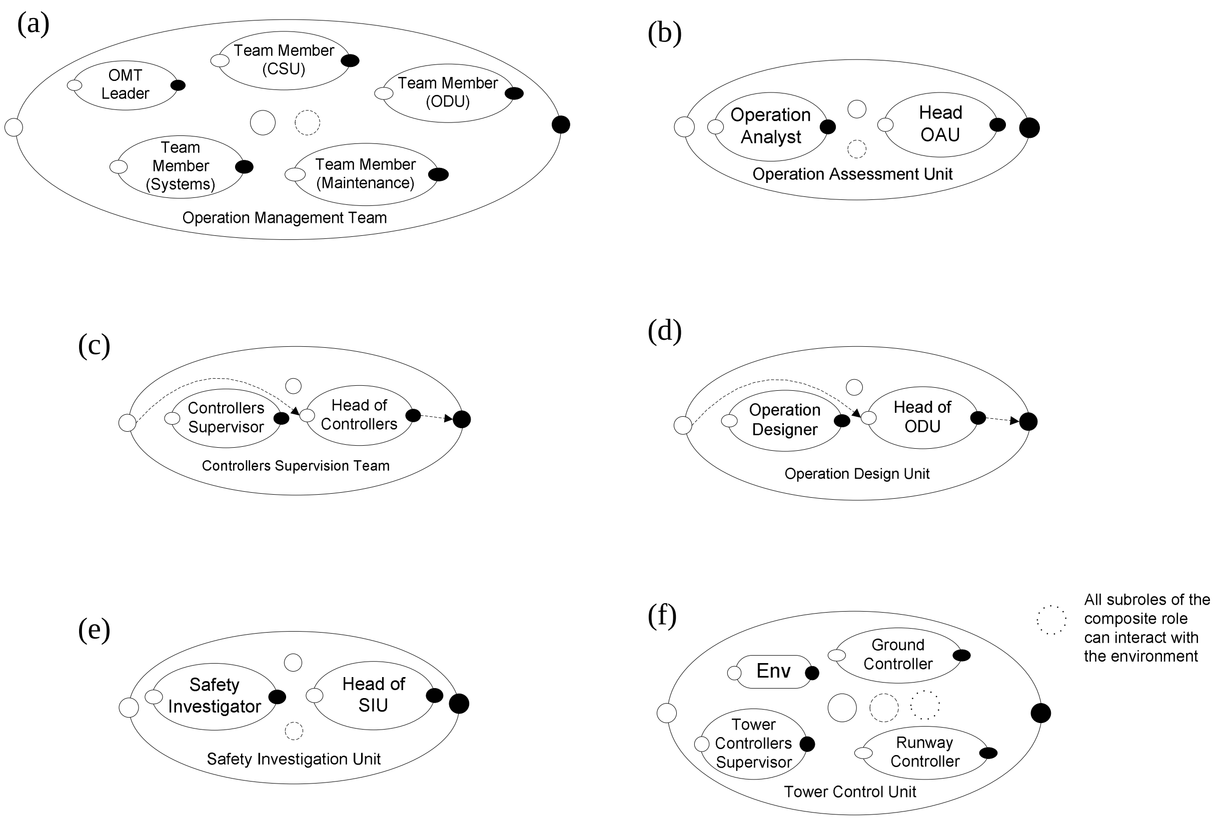


*Figure 3: The interaction relations between the subroles of the ANSP at aggregation level 3: (a) Operation Management Team, (b) Operation Assessment Unit, (c) Operation Design Unit, (d) Controllers Supervision Team, (e) Safety Investigation Unit, (f) Tower Control Unit.*

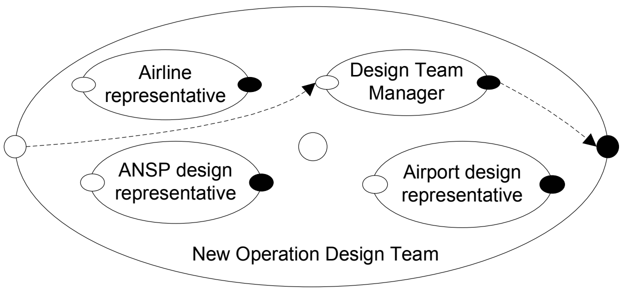


*Figure 4: The interaction relations between the subroles of the role New Operation Design Team at the aggregation level 2.*

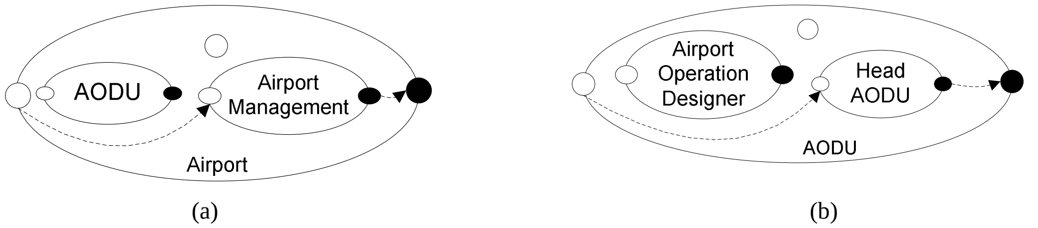


*Figure 5: The interaction relations between the subroles of the role Airport at aggregation level 2 (a) and of its subrole Airport Operation Design Unit at aggregation level 3 (b)*

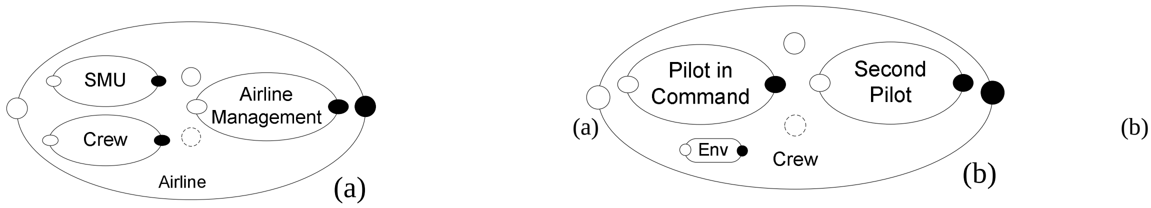


*Figure 6: The interaction relations between the subroles of the role Airline at aggregation level 2 (a) and of its subrole Crew at aggregation level 3 (b)*

To enable the interaction between the controllers of the ANSP and the pilots of the Airline the role Controller-Crew Interaction is introduced. This role consists of the subroles the Aircraft's Controller, who performs the constant monitoring and control over the aircraft and the Crew Representative role that interacts with the controllers on behalf of the aircraft's crew, when the contact is required. This interaction role is depicted at the aggregation level 2 in Figure 7

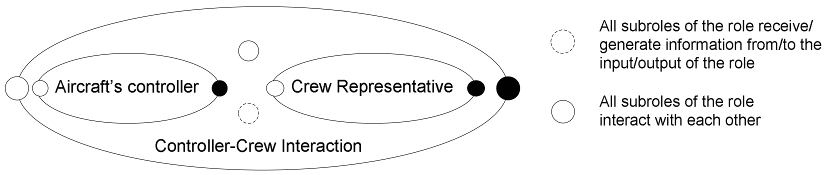


*Figure 7: The additional role for the interaction between the ANSP and the Airline composite depicted at the aggregation level 2*

**Ontologies**

The interfaces of roles are described in terms of interaction (input and output) ontologies: a vocabulary or a signature specified in order-sorted logic. An ontology contains objects that are typed with sorts, relations, and functions. Generally speaking, an input ontology determines what types of information are allowed to be transferred to the input of a role, and an output ontology predefines what kinds of information can be generated at the output of a role.

For each role, three types of ontologies are specified: an input ontology, an output ontology and an internal ontology. Input and output ontologies are often referred to as interface ontologies, which are used to describe interactions with other roles. An internal ontology is used to specify internal states of agents allocated to roles.

For specifying communications, the interface ontologies for all roles include the following predicate:

communication_from_to: ROLE x ROLE x MSG_TYPE x CONTENT

where the first argument denotes the role-source of information, the second argument denotes the role-recipient of information, the third argument denotes the types of the communication (which may be one of the following {observe, inform, request, decision, readback}) and the fourth argument denotes the content of the communication. The sort ROLE is a composite sort that comprises all subsorts of the roles of particular types (e.g., CONTROLLER, PILOT). The sort CONTENT is also the composite sort that comprises all names of terms that are used as the communication content. Such terms are constructed from sorted constants, variables and functions in the standard predicate logic way. For example, a set of functions that are used to construct the content of communications generated by the controller role of at its output is given in Table 3. For instance, to specify the communication of the decision of the agent allocated to the Aircraft's Controller role on the request for the clearance to cross the runway rw from the agent allocated to the role Crew Representative the following relation is used:

communication_from_to(Aircraft's Controller, Crew Representative, decision, instruction(position_and_hold, rw))

*Table 3: A set of functions that belong to the output ontology of the role Controller.*

| Function | Short description |
|---|---|
| aircraft_approaches_to: AIRCRAFT x REGION → CONTENT | Specifies an aircraft that approaches to a sector or a runway |
| aircraft_moved_from_to: AIRCRAFT x REGION x REGION → CONTENT | Specifies an aircraft that moved from one region to another |
| aircraft_at: AIRCRAFT x REGION → CONTENT | Identifies an aircraft situated in a certain sector or on a certain runway |
| instruction: INSTRUCTION_TYPE x RUNWAY → CONTENT | Specifies an instruction (i.e., a clearance to cross, a clearance to take off, an instruction to position and hold) to a crew |
| change_frequency_to: FREQUENCY → CONTENT | Identifies a new frequency for a crew |
| clear_of_the_runway: AIRCRAFT x RUNWAY → CONTENT | Specifies that an aircraft is clear of a runway |
| notification_report_for: REPORT x INCIDENT → CONTENT | Specifies a notification report for an incident |
| start_execution: PROCESS → CONTENT | Specifies a process being executed by the role |

| | |
|---|---|
| start_monitoring: PROCESS → CONTENT | Specifies a process being monitored by the role |
| finish_execution: PROCESS → ACTION_TYPE | Specifies the process execution finished by the role |
| finish_monitoring: PROCESS → ACTION_TYPE | Specifies the process monitoring finished by the role |
| performed_action: ACTION_TYPE → CONTENT | Specifies an action of the role |
| transfer_control_over: AIRCRAFT → CONTENT | Specifies that the transfer of control over an aircraft |

An ontology mapping associated with an interlevel link may be used for representing mechanisms of information abstraction. These mechanisms can be applied for transmitting (or generating) partial, aggregated or generalized information to the input (or from the output) of a role. For example, a version of the incident notification report 1 provided by the ANSP role to the Regulator may differ (can be more abstracted) from the original received by the role OMT within the ANSP.

In the model of the formal organization there is no distortion in the data transfer between roles; distortion may, however be included in agent-based modelling. To specify beliefs of agents that are allocated to roles, the following predicate is used:

belief: BEL_TYPE x ROLE x CONTENT,

where the first argument specifies the belief type from the set {observed, requested, requested_by, informed, informed_by, decision_provided, decision_provided_by}, the second argument specifies the role that initiated the belief creation, and the third argument specifies the content of the belief. For example, the following relation represents the belief of the agent allocated to the Crew Representative role about the decision position and hold received from the Aircraft's Controller role:

belief(decision_provided_by, Aircraft's Controller, instruction(position_and_hold, rw))

Ontologies of all other roles are constructed in a similar way.

### 3.4 Step 3: Identification of requirements for roles

In this step the requirements for each role at the lowest aggregation level are identified. By execution of this step a relation is created between the specifications of the organisation-oriented and the agent-oriented views.

For each role, requirements on knowledge, skills and personal traits of the agent implementing the role may be defined. Knowledge-related requirements usually define facts and procedures with respect to organizational tasks that must be well understood by an agent.

Skills describe developed abilities of agents to use effectively and readily their knowledge for tasks performance. In the literature (Pinder 1998) four types of skills relevant in the organizational context are distinguished: technical (related to the specific content of a task), interpersonal (e.g., communication, cooperation), problem-solving/decision-making and managerial skills (e.g., budgeting, scheduling, hiring). More specific requirements may be defined on skills reflecting their level of development, experience and the context in which these skills were attained.

Personal traits may also influence the successfulness of the execution of tasks. The traits are divided into five broad categories discovered in psychology (Katz and Kahn 1966): openness to experience; conscientiousness - the trait of being painstaking and careful, or the quality of acting according to the dictates of one's conscience.; extroversion – the trait that appears in the act, state, or habit of being predominantly concerned with and obtaining gratification from what is outside the self; agreeableness – the trait that is defined as a tendency to be pleasant and accommodating in social situations, and neuroticism – the trait that is defined as an enduring tendency to experience negative emotional states. Some agent's traits may mediate the attainment of agent's skills. For example, extroversion and agreeableness play an important role in building interpersonal skills.

To enable testing (or estimation) of skills and knowledge, every particular skill and knowledge is associated with one or more performance indicators (e.g., the skill 'typing' is associated with the performance indicator "the number of characters per minute"). Notice that some indicators may be soft (not directly measurable) (such as the level of flexibility); the value of such indicators may be established by indirect evidences (e.g., from the agent's history and achievements). Moreover, a skill may be associated with a compound performance indicator built as a weighed expression on simple performance indicators. In some cases agent personal traits may be evaluated through psychological tests and by consultations with agents' referees.

As an example, in the air traffic organizational model the following requirements for the air traffic controller role are defined:

a. Passed a rigid medical examination.
b. 2 or 4 year college degree before initiation of ATC training.
c. Thorough knowledge of the air traffic management system and the flight regulations.
d. Computer training.
e. Air traffic control training.
f. Excellent listening and communication skills.
g. Quick decision-making skills.
h. Ability to stand stress.
i. Good short-term memory capabilities.

The measure of the level of development may be associated with (some) capabilities. For example, controllers may differ in the amount of hours that they spent for air traffic control training. This may be expressed by assigning corresponding development levels of this capability to the controllers.

### 3.5 Step 4: Identification of organizational performance indicators and goals

In this step, organizational goals, performance indicators and relations between them and organizational roles are identified. By performing this step a complete specification for the performance-oriented view is specified. Furthermore, this step establishes relations between the specifications for the performance-oriented and organisation-oriented views. This section subsequently describes goals, performance indicators and relations between goals and performance indicators.

**Goals**

A goal describes a desired state or development that is aimed to be achieved by a role or an agent. A goal is characterized by the following aspects: (1) name; (2) priority; (3) horizon; (4) ownership; (5) perspective; (6) hardness; and (7) negotiability.

1. *Name*. The name / description of the goal.
2. *Priority*. Priority is defined by a range of natural numbers or by qualitative terminology such as {very high, high, medium, low, very low}. In this case study the range [1, 3] is used, where 3 corresponds to the highest priority.
3. *Horizon*. Horizon specifies within which time interval or at which time point, the goal is supposed to be satisfied: (a) long-term goal; (b) mid long-term goal; (c) short-term goal.
4. *Ownership*. Ownership can be organizational, i.e. belonging to an organizational role, or individual, i.e. belonging to an agent. Usually, organizational goals have a high level of priority. Goals of agents may comply with organizational goals to a varying degree. The priority of individual goals may depend on the company policy: some companies may assign lower priority to individual goals than to organizational ones; others may decide to involve and motivate the agents by taking into account their goals and avoiding conflicts that may exist between individual and organizational goals.
5. *Perspective*. Perspective (for organizational goals) defines, which point of view is described by the goal: e.g. of management, of a supplier; of a customer; or of the society. Even though all organizational goals belong to the organization itself, they can reflect the point of view of an external party which desires the organization to perform in a certain way. For example, the society wants the organization to obey society's norms and values. It may be beneficial for the company to adopt goals desired by other parties, e.g. to conform to the relevant laws. Different points of view can be conflicting, e.g. the desire for low prices by customers and high profit by management. Conflicts should be recognised during the design phase and made explicit in order to deal with them, e.g. the definition of goal priorities.
6. *Hardness*. Hardness distinguishes hard and soft goals. Satisfaction of hard goal can be clearly established and is indicated by the labels: satisfied > undetermined > failed. The satisfaction of a soft goal cannot be clearly established. We use the term satisficing to indicate an acceptable degree of satisfaction of a soft goal. Soft goals are given labels that

correspond to their degrees of satisficing/denial with a natural order between the labels: satisficed > weakly_satisficed > undetermined > weakly_denied > denied.

7. *Negotiobility*. By negotiability goals are divided into non-negotiable (i.e., need to be satisfied, no compromise is possible) and negotiable (negotiation is possible in case of conflicts with other goals). This can be used for conflict resolution at the design phase.

Table 4 shows some examples of the goals formulated in the air traffic organizational model. A complete list of its goals is specified in Appendix B.1. Table 5 shows some examples of the characteristics of the goals in the model; a complete list is specified in Appendix B.1.

*Table 4: Examples of goals and performance indicators of the air traffic organizational model*

| # | Goal | Performance indicator |
|---|---|---|
| 3 | It is required to achieve a high level of quality of the internal investigation of a new operation | The level of quality of the internal investigation of a new operation |
| 3.1 | It is required to achieve a high level of thoroughness of the internal investigation of a new operation | The level of thoroughness of the internal investigation of a new operation |
| 3.2 | It is required to maintain a high professional level of operation analysts | The professional level of operation analysts |
| 3.3 | It is required to maintain up-to-date knowledge of norms, standards and statistics used for the evaluation of a new operation | Knowledge of norms, standards and statistics used for the evaluation of a new operation |
| 4 | It is required to achieve a satisfactory realization of the high level requirements and their refinements in the concept of a new operation | The realization of the high level requirements and their refinements in the concept of a new operation |
| 4.1 | It is required to achieve a satisfactory realization of the safety-related requirements in the concept of a new operation | The realization of the safety-related requirements in the concept of a new operation |
| 4.2 | It is required to achieve a satisfactory realization of the capacity- and volume-related requirements in the concept of a new operation | The realization of the capacity- and volume-related requirements in the concept of a new operation |
| 4.3 | It is required to achieve a satisfactory realization of other types of requirements in the concept of a new operation | The realization of other types of requirements in the concept of a new operation |
| 4.4 | It is required to achieve great involvement of the experts (e.g., controllers) possessing knowledge in the domain of the operation in the process of | The involvement of the experts possessing knowledge in the domain of the operation in the process of |

| | | |
|---|---|---|
| | operation design | operation design |
| 16 | It is required to maintain a high level of robustness and unambiguousness of the control (coordination) structure for the execution of tasks | The level of robustness and unambiguousness of the control (coordination) structure for the execution of tasks |
| 16.1 | It is required to maintain a high level of robustness and unambiguousness of the control (coordination) structure for the execution of tasks in standard conditions | The level of robustness and unambiguousness of the control (coordination) structure for the execution of tasks in standard conditions |
| 16.2 | It is required to maintain a high level of robustness and unambiguousness of the control (coordination) structure for the execution of tasks in exceptional conditions | The level of robustness and unambiguousness of the control (coordination) structure for the execution of tasks in exceptional conditions |

*Table 5: Examples of characteristics of the goals in the air traffic organizational model.*

<table>
<tr><th>#</th><th>Priority (max -3)</th><th>Horizon</th><th>Ownership</th><th>Perspective</th><th>Hardness</th><th>Negotiability</th></tr>
<tr><td>1</td><td rowspan="4">2</td><td rowspan="19">short-term</td><td rowspan="4">ATCEM, OMT</td><td rowspan="4">management</td><td rowspan="8">soft</td><td rowspan="4">neg.</td></tr>
<tr><td>1.1</td></tr>
<tr><td>1.2</td></tr>
<tr><td>1.3</td></tr>
<tr><td>2</td><td rowspan="2">3</td><td>NODT, Regulator, Airport, ANSP</td><td rowspan="2">management, customer</td><td rowspan="2">non-neg.</td></tr>
<tr><td>2.1</td><td>Airport, ANSP</td></tr>
<tr><td>3</td><td rowspan="8">2</td><td>OAU, NODT</td><td rowspan="11">management</td><td rowspan="11">neg.</td></tr>
<tr><td>3.1</td><td rowspan="3">OAU</td></tr>
<tr><td>3.2</td><td rowspan="2">hard</td></tr>
<tr><td>3.3</td></tr>
<tr><td>4</td><td rowspan="5">NODT</td><td rowspan="6">soft</td></tr>
<tr><td>4.1</td></tr>
<tr><td>4.2</td></tr>
<tr><td>4.3</td></tr>
<tr><td>4.4</td><td>1</td></tr>
<tr><td>5</td><td>2</td><td>Regulator, NODT</td></tr>
</table>

| | | | | | | |
|---|---|---|---|---|---|---|
| 6 | 3 | | NODT, OAU, Regulator, Airport, ANSP | management, customer | | |
| 6.1 | | | Airport, ANSP | management | | non-neg. |
| 7 | 2 | | NODT | | | neg. |
| 7.1 | | | | | | |
| 7.2 | | | | | | |
| 7.3 | | | | | | |
| 8 | | | NODT, ATCEM, OMT | | | |
| 8.1 | | long-term | NODT | | hard | non-neg. |
| 8.2 | | short-term | | | soft | neg. |
| 8.3 | | | | | hard | |
| 9 | | | NODT, OAU, Regulator | | soft | |
| 9.1 | | | NODT, OAU | | hard | |
| 9.2 | | | NODT | | | |
| 9.3 | | | Regulator | | | |
| 9.4 | | | OAU | | | |

**Goal structures**

Goals can be refined into more specific goals, thus, forming goal structures. Since goals in the modelling framework can be of two types: hard and soft, different types of refinement relations are considered.

*Hard goals*

Hard goals can be refined by, respectively, AND and OR relations:

- The expression is_refined_to: GOAL × AND_GOAL_LIST means that only if all the goals in the list are satisfied then the goal in the first argument is satisfied. For example, the hard goal 16 from Table 4 can be refined into goals 16.1 and 16.2, i.e., is_refined_to(goal 16, L), where L is the and-goal list that comprises goals 16.1 and 16.2.
- If several refinements are defined, they are considered as alternatives connected by OR, i.e. they allow multiple possibilities to satisfy the goal.

*Soft goals*

The process of refinement of soft goals distinguishes two types or relations, which are expressed by the following relations; here the goal in the second argument is soft and the goal in the first argument can be soft or hard:

- satisfices: GOAL × GOAL: The first goal strongly contributes in a positive way to the satisficing of the second goal. If the first goal is satisfi(c)ed and any other influences are ignored then the second goal is considered satisficed. For example, in the context of the case study, goal 3.1 " It is required to achieve a high level of thoroughness of the internal investigation of a new operation" satisfices goal 3 "It is required to achieve a high level of quality of the internal investigation of a new operation".
- contributes_to: GOAL × GOAL: The first goal contributes positively to the satisficing of the second goal, however might not be enough to satisfice it. In the context of the case study, goal 4 "It is required to achieve a satisfactory realization of the high level requirements and their refinements in the concept of a new operation" contributes to goal 5 "It is required to achieve a high level of quality of the external investigation of a new operation". This relation exists, because a set of requirements properly identified and elaborated in a concept of a new operation in most cases influences positively the quality level of an external investigation of a new operation, however, still does not suffice for the satisficing of the goal 4.

The precise meanings of satisficing and contribution relations are defined through propagation rules. These rules are used to determine the degree of satisfaction/satisficing of a higher level goal based on the available information about the degrees of satisfaction/satisficing of lower level goals in its refinement. Lower level goals can be combined using AND relations or balanced contributions.

- In an AND-list, the label of a higher level goal is the minimum label propagated from the list of lower level goals, using the relation between labels of lower and upper level goals of Table 6. As an example of the refinement approach, consider the refinement of soft goal 3 of the air traffic organizational model in Figure 8. Goal 3 is refined into the AND-list that consists of goals 3.1, 3.2, 3.3 and 4. Given the labels of the subgoals as shown in Figure 8, the degree of satisfaction/satisficing of the goal 3 is the minimum of the propagated values of the subgoals: goal 3.1 – weakly_denied, goals 3.2 and 3.3 – satisfied, and goal 4 – weakly_denied.
- In the balanced contribution approach, the labels of the lower level goals are quantified and the resulting label of the higher level goal is based on their weighted average, taking into account weights for the level of influence of each lower level goal to the higher level goal. For instance, the quantification scale for the propagated labels may be: satisficed = 2, weakly_satisficed = 1, undetermined = 0, weakly_denied = -1, denied = -2.

*Table 6: Propagated labels for a higher level goal based on the labels of lower level goals.*

| **Label of lower level goal** | **Resulting higher level goal** | |
|---|---|---|
| | **satisfices** | **contributes_to** |
| satisficed / satisfied | satisficed | weakly_satisficed |
| weakly_satisficed | weakly_satisficed | undetermined |

| | | |
|---|---|---|
| undetermined | undetermined | undetermined |
| weakly_denied | weakly_denied | undetermined |
| denied / failed | denied | weakly_denied |

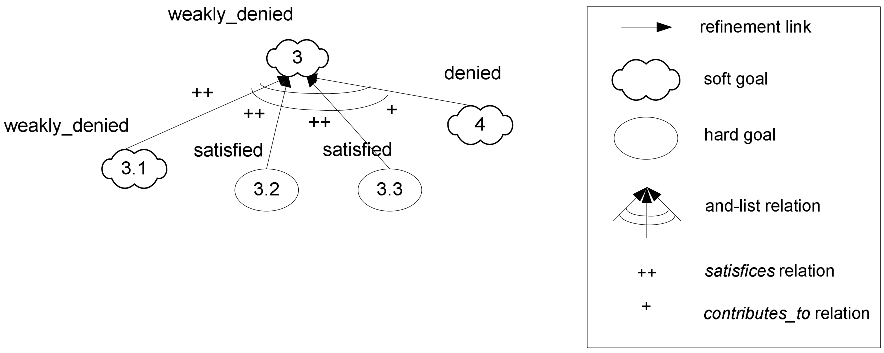


*Figure 8: Example of the refinement of goal 3 by an AND-list of subgoals.*

When a goal is refined in one list only then the influence calculated using the described above rules defines the satisficing label of the goal. In addition a goal may be refined into alternative influence lists related by OR. In such situations we use the following strategy: first the influences of the AND and balanced lists are calculated separately and then the highest label among them is assigned to the higher level goal.

Usually, high level goals of a company are of a strategic (long-term) type. Such goals are often made operational by refining them into lower level tactical (short-term) goals. In such a way a goal-structure is created by a top-down design process. The refinement of goals may proceed until subgoals are found, which could be realized by (possibly single) lowest-level tasks from the task hierarchy. In practice, the top-down design approach is often combined with the bottom-up approach, which is performed by aggregation of goals. For example, subgoals can be identified by asking "how" questions about the goals already determined, and parent goals are identified by asking "why" questions. The goal structure of the air traffic organizational model is depicted in Figure 9.

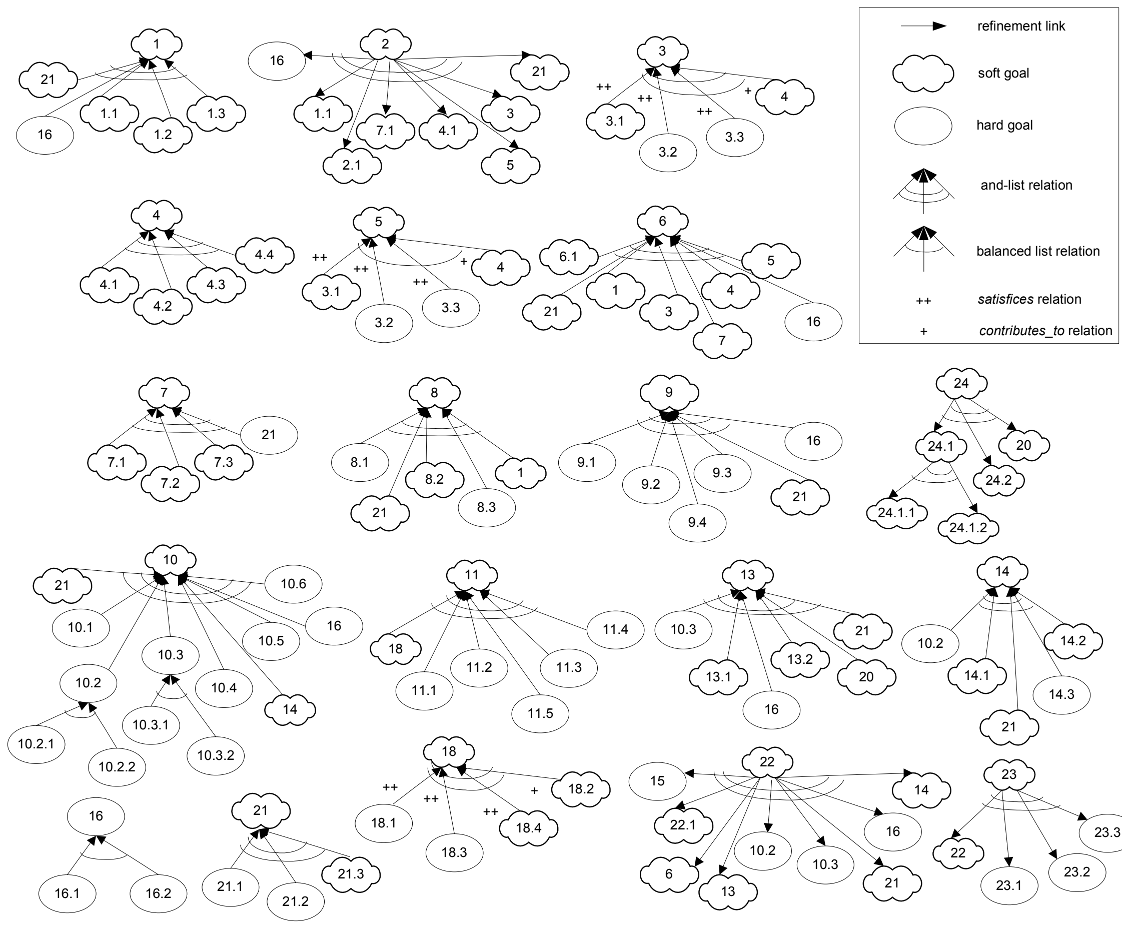


*Figure 9: The goal structure in the air traffic organizational model.(Links without indication are of the type satisfices.)*

**Performance indicators**

Performance indicators are quantitative or qualitative indicator that reflects the state/progress of the company, unit or individual. A performance indicator can be soft or hard. A soft performance indicator is difficult to measure directly and usually specified by a qualitative expression, e.g. customer's satisfaction, company's reputation, employees' motivation. A hard performance indicator is well measurable and usually expressed quantitatively, e.g., number of customers, number of landing aircraft, or average time to cross an active runway. The set of performance indicators that can be defined for one organization can be very large and it is often not feasible to monitor all of them. Therefore the companies select a subset of indicators, called key performance indicators, that can give a representative picture of the performance and the costs of measuring and monitoring are reasonable.

The process of extracting the performance indicators from source documents involves asking the question: What should be measured / observed to ensure the requirements in the document? Performance indicators are often represented by nouns in the text; modifiers such as adjectives give information about the type, scale of measurement and what is considered a desirable value of the performance indicator (used in performance indicator expressions, goal patterns and goals), e.g., the job description requires a crew 'to maintain a high level of collaboration during decision making' then 'the level of collaboration during decision making' is a performance indicator and 'high' – its desired value.

Often the performance indicators that can be extracted from documents such as the mission statements and policies are soft and difficult to assess. In order to evaluate such a performance indicators it is usually beneficial to find a closely related hard indicator that can be measured instead and that can give an impression on the state of the soft one. For example, customer satisfaction cannot be measured directly but it is possible to design questionnaires to collect information on customer's opinion.

Some examples of the performance indicators of the air traffic organizational model are shown in Table 4. A complete list of its performance indicators is specified in Appendix B.1.

**Relations between performance indicators**

Three types of relations between performance indicators are defined: causing, correlated and aggregation_of; they are elaborated on next.

- causing: PI × PI × {very_pos, pos, neg, very_neg}: The first performance indicator causes change in the same direction (positive) or opposite direction (negative) to the second performance indicator. For example, in the air traffic organizational model the performance indicator "the completeness and accuracy of the identification of high level safety-related requirements for a new operation from all parties involved into the operation" causes a positive change of the performance indicator "the level of safety of a new implemented operation".
- correlated: PI × PI × {pos, neg}: The first performance indicator is correlated positively or negatively to the second performance indicator. For example, in the air traffic organizational model, the performance indicators "the development and assessment time of a new operation" and "the level of quality of the internal investigation of a new operation" are related by a positive correlation relation.
- aggregation_of: PI × PI: The first performance indicator is an aggregation of the second performance indicator. For example, in the air traffic organizational model, the performance indicator "the development and assessment time of a new operation" is the aggregation of the performance indicators "the development time of the concept of a new operation", "the time for an external assessment of a new operation" and "the time for an internal assessment of a new operation".

The relations between the performance indicators in the air traffic organizational model are depicted in Figure 10.

Using the standard procedure from the sorted first-order predicate logic, terms and formulae over sort PI can be built, expressing different types of mathematical relations between performance indicators. For instance, performance indicator expressions can be defined over performance indicators, which is a mathematical statement over a performance indicator containing >, ≥, =, < or ≤. A performance indicator expression can be evaluated to a numerical, qualitative or Boolean value for a time point, for the organization, unit or agent. Performance indicator expressions are used to define goal patterns which are properties that can be checked to be true or false for the organization, unit or individual at a certain time point or period. Examples of performance indicator expressions are: "maintained the number of ground controller agents allocated to each sector ≥ 1" and "achieved that time to generate a decision about the clearance issuing for an aircraft ≤ 5 seconds".

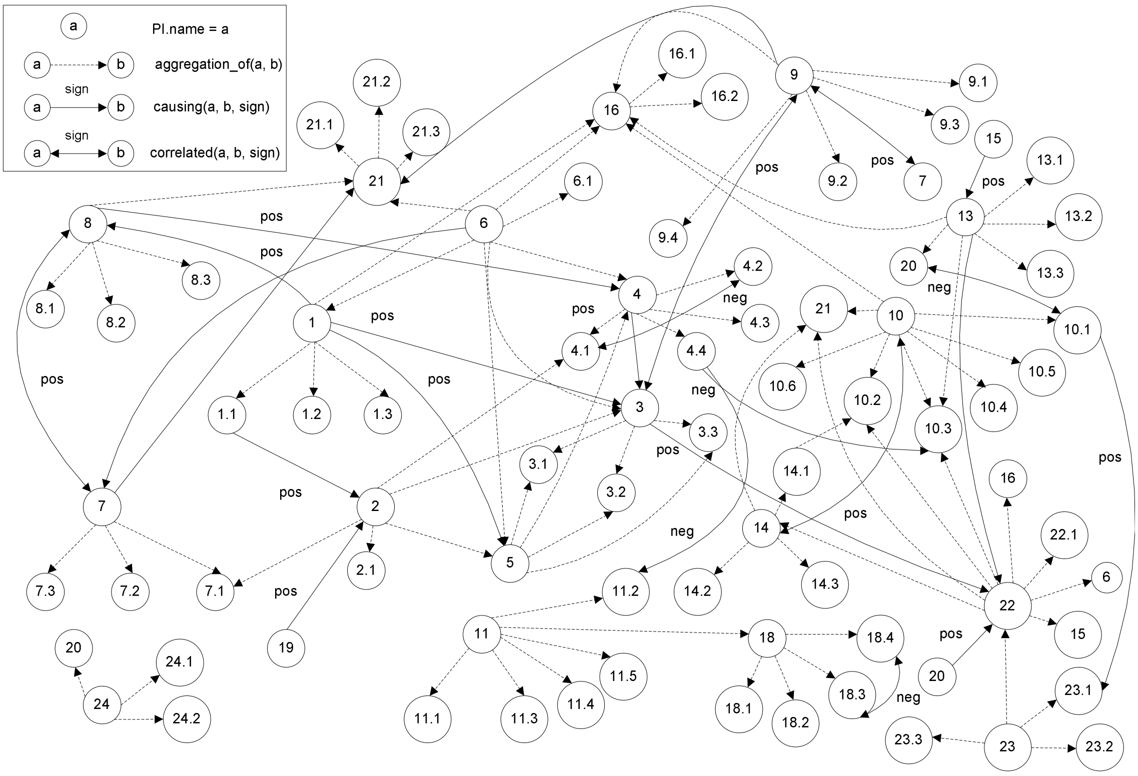


*Figure 10: Relations between the performance indicators in theair traffic organizational model.*

### 3.6 Step 5: Identification of resources

In this step organizational resource types and resources are identified, and characteristics for them are provided. It is part of the process-oriented view.

Resources describe a wide range of materials and data, such as tools, supplies, components and digital artefacts. Types of resources are characterized in the model by:

- name;
- category – discrete or continuous;
- measurement unit;
- expiration duration – the time interval during which a resource type can be used.

Specific resources represent instances of resource types and inherit their characteristics. In addition to the inherited characteristics, the specific resources also are characterized by a (specific) name and an amount. Examples of resource types in the air traffic organizational model are provided in Table 7.

*Table 7: Examples of resource types in the air traffic organizational model.*

| Name | Category | Measurement unit | Expiration duration |
|---|---|---|---|
| Airport's diagram | Discrete | Item | Conditional: until any changes in the airport's layout are performed |
| Aircraft | Discrete | Item | Depending on the aircraft's type |
| Runway Incursion Alert System (RIAS) | Discrete | Item | 10 years |
| Radar | Discrete | Item | 10 years |
| Communication R/T system | Discrete | Item | 10 years |
| Incident classification database | Discrete | Item | Conditional: until any changes are introduced |
| Clearance to cross a runway | Discrete | Item | Conditional: until the runway is crossed by the aircraft that received the clearance |
| An incident investigation report | Discrete | Item | 50 years |

For some application areas it is important to keep track of where the resources are at certain time points. For modelling such information the concept of a location is used which for example can represent the available storage facilities. Processes can add or remove resource types from locations which can be specified using the predicates: process_adds_resource_type_to: PROCESS × RESOURCE_TYPE × LOCATION × VALUE and process_rem_resource_type_from: PROCESS × RESOURCE_TYPE × LOCATION × VALUE where the last argument specifies the amount of the added or removed resource type. Resources are considered removed at the starting time point of the corresponding process and are added at the ending time point of the process.

### 3.7 Step 6: Identification of organizational tasks and relations between tasks, resources and goals

This section describes how the static part of a specification for the process-oriented view is defined. This part identifies organisational tasks, their characteristics and relations between them and defines relations between tasks and resources. Furthermore, this step relates each task to a goal and thereby establishes a connection between the process-oriented view and the performance-oriented view.

A task represents a function performed in the organisation and is characterized by a name and by maximal and minimal durations. Examples of the tasks in the air traffic organizational model are shown in Table 8; a complete overview is in Appendix B.3.

Tasks can range from very general to very specific. General tasks can be decomposed into more specific ones using AND- and OR-relations and thereby form hierarchies. In Figure 11 the decompositions of the composite tasks are depicted. Note that two sets of tasks {4.7, 4.4, 5.4, 5.3, 5.1} and {4.7, 4.4, 5.2, 5.4} define the alternative refinements of the task 5.

Every task performed in an organization should contribute to the satisfaction of one or more organizational goals. Goals are related to tasks by the relation is_realizable_by: GOAL x TASK_LIST: The goal in the first argument is realizable by the list of tasks in the second argument. Table 8 shows relations between the lowest level tasks and goals. Sets of goals that correspond to higher level tasks are formed by combination of all goals that correspond to the subtasks of these tasks.

*Table 8: Examples of tasks in the air traffic organizational model, their characteristics and the relations to the goals.*

| # | Task name | Short description | Durations |
|---|---|---|---|
| 4 | Incident reporting management based on the data provided by a controller | The incident reporting loop initiated by a (runway or ground) controller. | Min: 1 day<br>Max: 160 days |
| 4.1 | Create a notification report | When a controller observes an occurrence that may be classified as an incident/accident, s/he is obliged to create a notification report. | Min: 1 min<br>Max: 2 hours |
| Goal: 17, 18.2, 19, 20 | | | |
| 4.2 | Preliminary processing of a notification report | A notification report created by a controller is examined and improved by his/her supervisor. The occurrence described in the report is classified. | Min: 1 min<br>Max: 2 days |
| Goal: 19, 13.3, 20 | | | |
| 4.3 | Making decision about the investigation necessity based on the provided notification report | The decision about investigation of the occurrence depends on its perceived severity in relation with earlier occurrences as specified in Table 9. | Min: 1 day<br>Max: 30 days |
| Goal: 19, 20 | | | |
| 4.4 | Investigation of the occurrence based on the notification report | During the investigation the (possible) causes of the incident/accident are identified, and based on the investigation results recommendations are provided. | Min: 3 days<br>Max: 90 days |
| Goal: 18.3, 18.4, 20 | | | |
| 4.5 | Discussion of the intermediate occurrence investigation results | The intermediate results of the investigation are provided to the OMT of the ANSP. | Min: 1 day<br>Max: 15 days |

| | | | |
|---|---|---|---|
| Goal: 11.5, 12 | | | |
| 4.6 | Reviewing of the occurrence investigation results | The Executive Board of the ATC reviews the incident/accident investigation results. | Min: 5 min<br>Max: 4 hours |
| Goal: 11.5, 12, 20 | | | |
| 4.7 | Distribute the occurrence investigation report among all concerned roles | - | Min: 1 hour<br>Max: 15 days |
| Goal: 21.2, 21.3, 21.1 | | | |
| 5 | Incident reporting management based on the data provided by a crew | The incident reporting loop initiated by a crew. | Depends on the durations of subtasks |
| 5.1 | Create a notification report and provide it to the SMU | When a pilot (a crew) observes an occurrence that may be classified as an incident/accident, s/he is obliged to create a notification report, which may be further provided to the SMU of the airline by which the pilot is employed. | Min: 2 hours<br>Max: 2 days |
| Goal: 14.1, 14.3, 17, 18.2, 19, 14.2, 20 | | | |
| 5.2 | Create a notification report and provide it to the regulator | A notification report created by a pilot may be provided directly to the regulator. | Min: 1 day<br>Max: 14 days |
| Goal: 14.1, 14.3, 17, 18.2, 19, 14.2, 20 | | | |
| 5.3 | Process a notification report and provide it to the regulator | A notification report created by a pilot (a crew) is examined and improved by the SMU and provided further to the regulator for further investigation. | Min: 1 day<br>Max: 90 days |
| Goal: 19, 20 | | | |
| 5.4 | Making decision about the investigation necessity and about the role-investigator | The decision is based on the notification report and the choice of the role-investigator is based on the severity of the incident/accident (see Table 9), the availability of roles and the competences of the available roles. | Min: 1 day<br>Max: 30 days |
| Goal: 18.3, 18.4, 20 | | | |

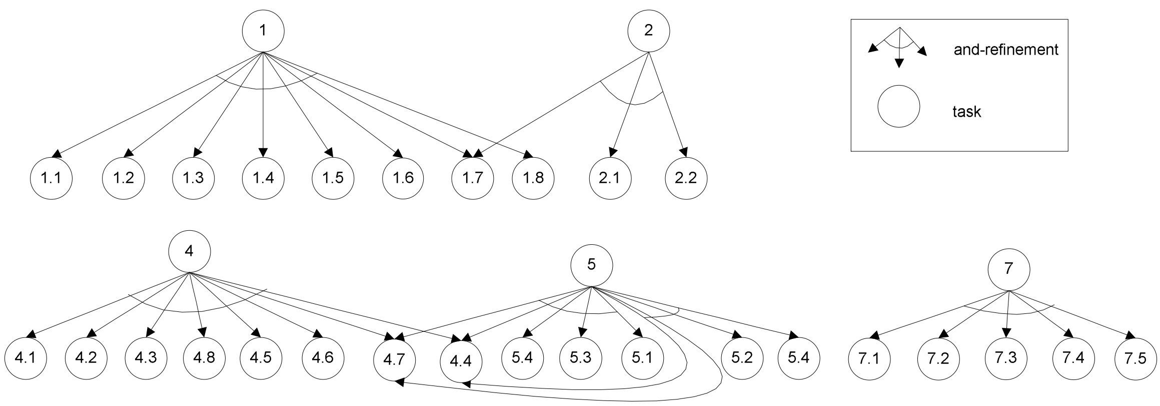


*Figure 11: Composition of tasks in subtasks.*

*Table 9: Assumed number of events that is required to decide on a safety investigation on the type of event.*

| Event | | Number of occurrences for investigation |
|---|---|---|
| **ID** | **Description** | |
| *a* | Aircraft rejects take-off as result of a runway incursion | 1 |
| *b* | Taxiing aircraft stops progressing on the runway crossing only after the stopbar and due to a call by the runway controller | 3 |
| *c* | Taxiing aircraft makes wrong turn and progresses towards the runway crossing | 6 |
| *d* | Taxiing aircraft makes wrong turn and progresses on a wrong taxiing route that is not a runway crossing | 55 |
| *e* | Taxiing aircraft has switched to a wrong frequency | 55 |
| *f* | Taxiing aircraft initiates to cross due to misunderstanding in communication | 6 |

**Relation tasks and resources**

Organizational tasks use, consume and produce resources of different types. In the modelling approach, the predicates task_uses, task_consumes, task_produces: TASK × RESOURCE_TYPE × VALUE indicate resource types that are input or output of tasks with their prescribed amounts. Table 10 shows examples of resource-task relations. Appendix B.3 provides an overview of all resource-task relations in the air traffic organizational model. Note that only the relations between the simple tasks and resource types are shown. The resource types that are used/consumed/produced by a composite task comprise all the resource types that are used/consumed/produced by all the subtasks of this task.

*Table 10: Examples of relations between tasks and resources in the air traffic organizational model.*

| Task | Task uses | Task produces |
|---|---|---|
| 4.1 | the observation from the environment of an occurrence that may be classified as an incident/accident, the incident classification database | a notification report |
| 4.2 | a notification report | a processed notification report |
| 4.3 | a processed notification report | a decision on the initiation of the occurrence investigation |
| 4.4 | a processed notification report, additional data about the occurrence (optional) | an incident investigation report |
| 4.5 | a processed notification report, an incident investigation report, occurrence statistics | recommendations based on the incident investigation report |
| 4.6 | an incident investigation report | directions to redesign some operation(s) (optional) |
| 4.7 | an incident investigation report, the list of all | - |

| | | |
|---|---|---|
| | concerned roles | |
| 5.1 | the observation from the environment of an occurrence that may be classified as an incident/accident, the incident classification database | a notification report |
| 5.2 | the observation from the environment of an occurrence that may be classified as an incident/accident, the incident classification database | a notification report |
| 5.3 | a notification report | a processed notification report |
| 5.4 | a (processed) notification report | a decision on the initiation of the occurrence investigation, a decision concerning the role-investigator |

## 3.8 Step 7: Identification of authority relations

In this step authority relations (i.e., formal power relations) of an organisation are identified: superior-subordinate relations on roles with respect to tasks, responsibility relations, control for resources, authorization relations. By execution of this step the remaining part of a specification of the organisation-oriented view is described (other parts are specified by steps 1-3).

**Task authorization and responsibility**

Organisational roles may have different rights and responsibilities with respect to different aspects of task execution. This is represented in the organizational modelling approach by the following relations:

- is_authorized_for: r:ROLE x aspect: ASPECT x a:TASK, which denotes that role r is authorized for an aspect of task a;
- is_responsible_for: r:ROLE x aspect:ASPECT x a:TASK, which denotes that role r is responsible for an aspect of task a.

These relations account for the following task aspects:

- *Execution.* Authorization/responsibility for execution implies that a role is authorized/responsible for task execution according to existing standards and guidelines. Whenever a problem, a question or a deviation from the standard procedures occurs, the role must report about it to the role(s) authorized for making technological/managerial (depending on the problem type) decisions and must execute the decision(s) that follow.
- *Monitoring.* Monitoring implies passive observation of (certain aspects of) task execution, without intervention.
- *Consulting*. Recommendation and voluntary acceptance of advices.
- *Making technological decisions*. Technological decisions concern technical questions related to the task content and are usually made by technical professionals. The decision must be followed.

- *Making managerial decisions.* Managerial decisions concern general organizational issues related to the task (e.g., the allocation of employees, task scheduling, the establishment of performance standards, provision of resources, presenting incentives and sanctions). Managers of different levels (i.e., from the lowest level line managers to strategic apex (top) managers) may be authorized for making different types of managerial decisions varying from in scope, significance and detail. The decision must be followed.
- *User defined aspect*. Other specific aspects for a particular organization.

Notice that other aspects of task execution described in the managerial literature (e.g., control, supervision) can be represented as a combination of already introduced aspects. In particular, control can be seen as the conjunction of monitoring and making technological and/or managerial decisions aspects; supervision can be defined as the combination of consulting and control. Furthermore, the designer is given the possibility to define his/her own aspects and to provide an interpretation to them.

Examples of responsibility relations in the air traffic organizational model are presented in Table 11; a complete list is specified in Appendix B.4.

*Table 11: Examples of the responibility relations in the air traffic organizational model.*

<table>
<tr><th>Task</th><th>Execution</th><th>Monitoring</th><th>Consulting</th><th>Technological decisions</th><th>Managerial decisions</th></tr>
<tr><td>4.1</td><td colspan="5">Runway or Ground Controller</td></tr>
<tr><td>4.2</td><td colspan="5">Tower Controllers Supervisor</td></tr>
<tr><td>4.3</td><td colspan="5">SIU</td></tr>
<tr><td>4.4</td><td>Safety Investigator</td><td colspan="2">Head SIU</td><td>Safety Investigator</td><td>Safety Investigator, Head SIU</td></tr>
<tr><td>4.5</td><td colspan="5">OMT</td></tr>
<tr><td>4.6</td><td colspan="5">ATCEM</td></tr>
<tr><td>4.7</td><td colspan="5">OMT</td></tr>
<tr><td>4.8</td><td>Safety Investigator or Regulator</td><td colspan="2">OMT, ATCEM</td><td>Safety Investigator, Regulator</td><td>OMT, ATCEM</td></tr>
<tr><td>5.1</td><td colspan="5">Crew</td></tr>
<tr><td>5.2</td><td colspan="5">Crew</td></tr>
<tr><td>5.3</td><td colspan="5">SMU</td></tr>
<tr><td>5.4</td><td colspan="5">Regulator</td></tr>
</table>

**Assigning tasks authorization and responsibility**

Some roles are authorized to make managerial decisions for authorizing/disallowing other roles for certain aspects with respect to task execution. The authorization/ disallowance actions are specified by the following relations:

authorizes_for: r1:ROLE x r2:ROLE x aspect: ASPECT x a:TASK: role r1 gives the authority for aspect of task a to role r2.

disallows: r1:ROLE x r2:ROLE x aspect: ASPECT x a:TASK: role r1 denies the authority for aspect of task a for role r2.

To make a role responsible for a certain aspect of the task, another role besides the authority to make managerial decisions should also be the superior of the role with respect to the task. Superior-subordinate relations with respect to organizational tasks are specified by:

is_subordinate_of_for: r1: ROLE x r2: ROLE x a:TASK.

Responsibility is assigned/retracted using the following relations:

assigns_responsibility_to_for: r1: ROLE x r2:ROLE x aspect: ASPECT x a:TASK: role r1 assigns the responsibility for aspect of task a to role r2.

retracts_responsibility_from_for: r1: ROLE x r2:ROLE x aspect: ASPECT x a:TASK: role r1 retracts responsibility from role r2 for aspect of task a.

Using these relations superiors may delegate/retract (their) responsibilities for certain aspects of tasks execution to/from their subordinates, and may restrict themselves only to control and making decisions in exceptional situations. Table 12 shows the superior-subordinate relations of the roles with respect to the tasks in the air traffic organizational model.

*Table 12:Superior-subordinate relations of the roles with respect to the tasks in the air traffic organizational model.*

| Subordinate role | Superior role | Task |
|---|---|---|
| ANSP design representative | Design Team Manager | 7.1, 7.3 |
| Airport design representative | Design Team Manager | 7.1, 7.3 |
| Airline representative | Design Team Manager | 7.1, 7.3 |
| OMT | ATCEM | 7.2, 7.4 |
| OAU | OMT | 7.2, 7.4 |
| Operation Analyst | Head OAU | 7.2, 7.4 |
| Runway Controller | Tower Controllers Supervisor | 1.4 |
| Ground Controller | Tower Controllers Supervisor | 1.1 |
| Runway Controller | Tower Controllers Supervisor | 1.5 |
| Runway Controller | Tower Controllers Supervisor | 2.2 |
| Runway Controller | Tower Controllers Supervisor | 4.1 |
| Safety Investigator | Head SIU | 4.4, 6 |
| OMT | ATCEM | 4.4, 6 |
| SIU | OMT | 4.4, 6 |

### 3.9 Step 8: Identification of the flows of control

In this step the dynamic part of specification for the process-oriented view is described. This is achieved by the definition of workflows that represent temporal execution sequences of processes of an organisation in particular scenarios. Logical expressions for the definitions of workflows and examples of formal specifications of workflows in the air traffic organizational model are described in Appendix B.5. Graphical definitions of workflows in the air traffic organizational model are shown in Figure 12 to Figure 15.

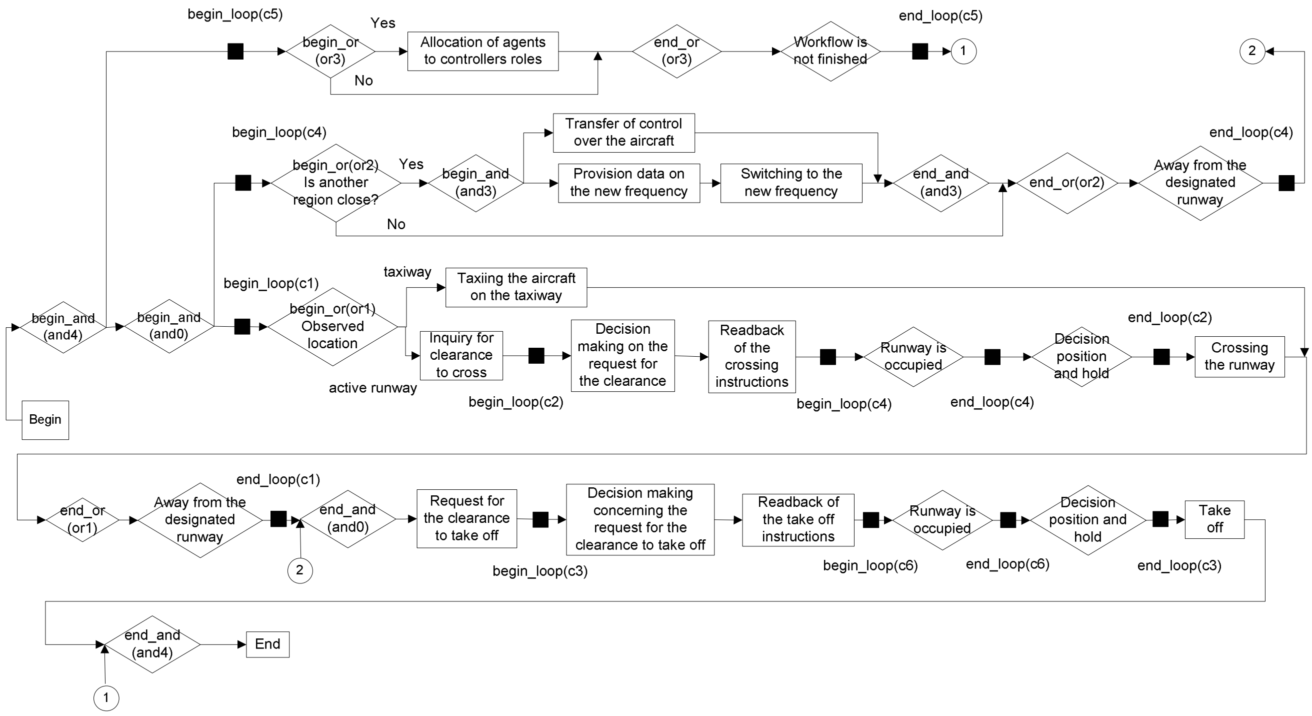


*Figure 12: Workflow for an aircraft taxiing to and taking-off from a designated runway.*

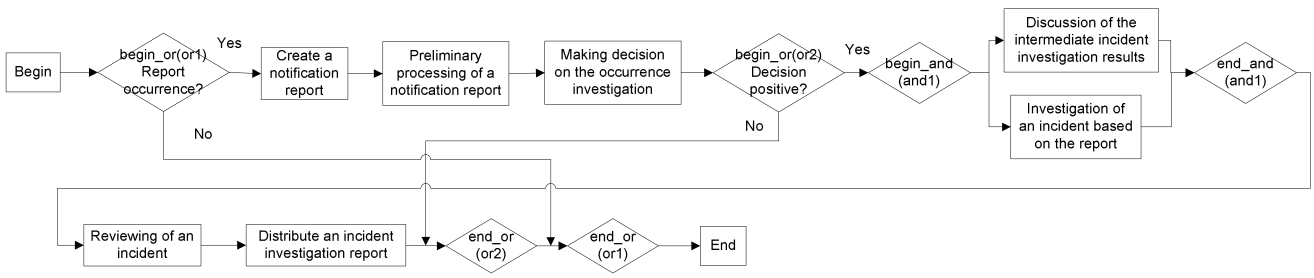


*Figure 13: Workflow for management of controller incident reporting*

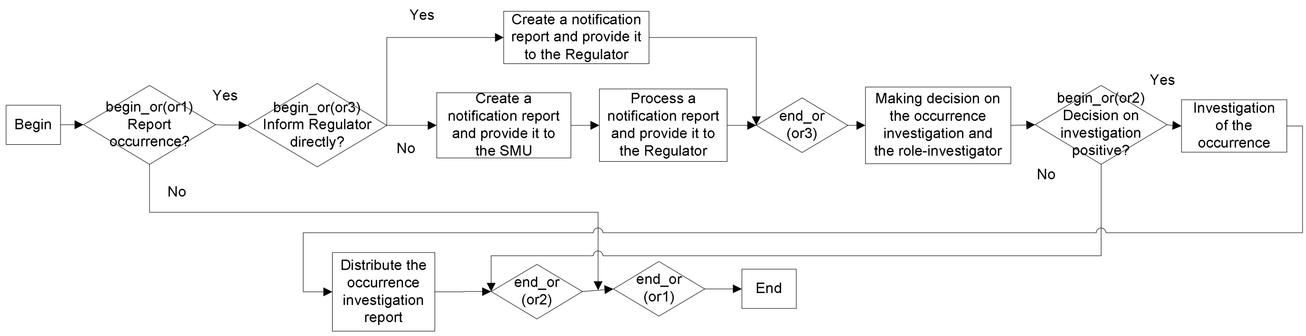


*Figure 14: Workflow for management of aircraft crew incident reporting*

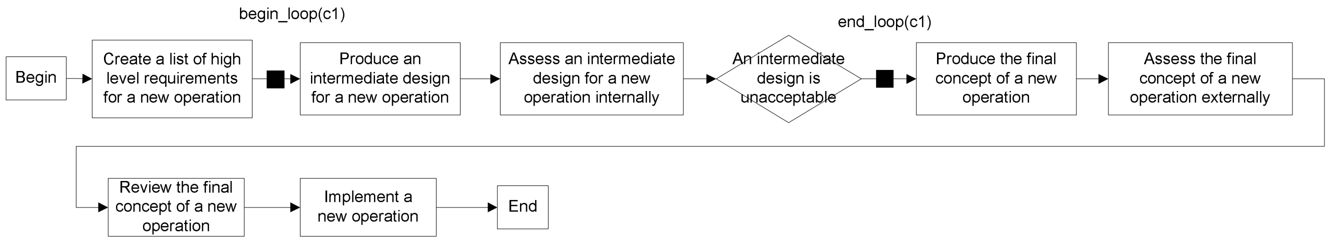


*Figure 15: Workflow for development and implementation of a new operation.*

## 3.10 Step 9: Identification of allocation, characteristics and behaviour of agents

The performance variability in an organisation is the result of the behaviour of agents that are allocated to organizational roles. In this step, the characteristics and behaviour of agents allocated to organisational roles are described.

In this section general characteristics determining agent behaviour are described. In addition, any deviation of agent behaviour from the organisational scenarios is possible to specify. Usually the dynamics of agents is defined depending on a particular scenario and on the purposes of analysis.

**Agent types and agent allocation**

Agents are characterized by capabilities (knowledge / skills), personal traits and internal goals (see also Section 3.4). Table 13 shows the types of agents and the range of values of their characteristics for the air traffic organizational model. Note that in general for the identified types of agents more characteristics can be specified, however, for the purposes of simulations performed in the frames of the considered case study, the identified set of characteristics of each agent type is sufficient. Note that for particular types of analysis (e.g. analysis of decision making processes) the identified characteristics can be further refined in more specific ones.

In general, the specification of internal attitudes and dynamics of agents is not limited to any particular theory. Instead, a modeller is given freedom to choose a suitable theoretical basis depending on the purpose of modelling.

The principles of allocation of agents to organizational roles may vary between organizations (e.g., allocation based on equality, seniority or stimulation of novices). In general, agent allocation depends on how well the agent's characteristics (i.e., capabilities and traits) and goals fit with the role specification and the requirements. In practice this implies that an agent is only allocated to a role when it satisfies all the requirements identified for this role.

*Table 13: Types of agents and potential values of their characteristics in the air traffic organizational model*

| Agent Type | Characteristic | Possible values |
|---|---|---|
| Controller | decision-making skills | {bad, good, excellent} |

| | | |
|---|---|---|
| | passed a rigid medical examination | {yes, no} |
| | the number of years of college education before initiation of ATC training | [2, 4] |
| | knowledge of the air traffic management system and the flight regulations | {bad, good, excellent} |
| | number of hours of computer training | any number |
| | number of hours of air traffic control training | any number |
| | listening and communication skills | {bad, good, excellent} |
| | ability to stand stress | {yes, no} |
| | short-term memory capabilities | {bad, good, excellent} |
| Controller Manager | the same charactistics as for the controller type | |
| | controllers management skills | overall development level: [1, 4] |
| Pilot | control of aircraft | development level: [1, 4] |
| | decision-making skills | {bad, good, excellent} |
| | passed a rigid medical examination | {yes, no} |
| | knowledge of the flight regulations | {bad, good, excellent} |
| | number of hours of computer training | any number |
| | listening and communication skills | {bad, good, excellent} |
| | short-term memory capabilities | {bad, good, excellent} |
| Regulator | decision-making skills | {bad, good, excellent} |
| | knowledge of general safety standards, requirements and regulations for the execution of flight operations | {bad, good, excellent} |
| | analytic skills | {bad, good, excellent} |
| | level of proficiency of use of a safety assessment framework | {no, low, high} |
| | listening and communication skills | {bad, good, excellent} |
| Safety Investigator | the same as for the regulator type | |
| SIU Manager | the same as for the regulator type | |
| | safety investigators management skills | overall development level: [1, 4] |
| Manager | decision-making skills | {bad, good, excellent} |
| | employee management skills | {bad, good, excellent} |
| | listening and communication skills | {bad, good, excellent} |
| | ability to stand stress | {yes, no} |

**Agent behaviour**

The behaviour of an agent is considered as goal-driven. In this case study only the goals of agents that are in line with the organizational goals are taken into account, i.e., the goals related to a role, to which an agent is allocated are also attributed to the agent (see Table 5 on page 25). For example, since goal 1 is attributed to roles ATCEM and OMT, therefore all agents allocated to the roles within ATCEM and OMT strive to achieve goal 1.

The internal states of agents allocated to organizational roles are represented as beliefs. A belief of an agent is created based on one of the following events:

(a) observation from the environment: a belief state is generated after the agent observed some occurrence in the environment;
(b) a communication provided to/obtained from another agent: belief states are changed for the agents involved in the communication;
(c) an action performed by the agent in the environment: a belief state is changed after the agent performed an action.

Formal representation of belief update functions is described in Appendix B.6.

In addition to the general belief update functions, specific rules defining for the belief states of agents in the air traffic organizational model are presented below.

1. When an agent allocated observes that an aircraft moved from some region reg1 to another region reg2, and the agent has the belief that the aircraft is in the region reg1, then this belief becomes invalid at the next time point.
2. When an agent observes that an aircraft moved from some region reg1 to another region reg2, and the agent has the belief that the aircraft is approaching to the region reg2, then this belief becomes invalid at the next time point.
3. If an agent has a belief that a clearance to cross/takeoff from some runway is provided to some aircraft, then this belief will be invalid after the agent has observed that the aircraft has crossed/took off from the runway.
4. A belief of an agent that a clearance to cross/takeoff is provided to some aircraft becomes invalid 2 minutes after the time point of its generation.
5. A belief of an agent that a position and hold instruction is provided to some aircraft becomes invalid after the agent has observed that the clearance to cross/take off is provided to this aircraft.
6. In case an agent-pilot has a false belief about the frequency of the controller guiding his/her aircraft, and some agent-controller informs the agent about the correct frequency, then this belief becomes invalid.
7. In case an agent-pilot has a false belief about the position of his/her aircraft and some agent-controller informs the agent about his/her correct position, then this belief becomes invalid.

Concerning the recognition and reporting of events by controllers and cockpit crews it is assumed in the model that the probabilities of recognition and reporting depend on the events and the agent considered as specified in Table 14. Furthermore, the possibility to recognize an event is considered to depend on the particular type of controller (runway/ground) and the particular type of crew (taxiing/taking-off aircraft) as specified in Table 15.

*Table 14: Assumed probability values for the observation and the registration of safety-relevant events (see Section 2) by controllers and crews.*

| Event | Probability of correct event recognition, when it occurred | | Probability of event reporting, when it has been observed | |
|---|---|---|---|---|
| | by a controller | by a crew | by a controller | by a crew |
| *a* | $1 - 10^{-5}$ | $1 - 10^{-5}$ | $1 - 10^{-5}$ | $1 - 10^{-5}$ |
| *b* | $1 - 10^{-5}$ | $1 - 10^{-5}$ | 0.99 | 0.99 |
| *c* | 0.99 | 0.98 | 0.9 | 0.9 |
| *d* | 0.95 | 0.8 | 0.5 | 0.5 |
| *e* | 0.7 | 0.9 | 0.5 | 0.5 |
| *f* | 0.99 | 0.9 | 0.99 | 0.99 |

*Table 15: Observation possibilities of safety-relevant events (see Section 2) by agents fulfilling the organizational roles. In the model 'yes'/'maybe' means that the event can be recognized, 'no' means it cannot be recognized by the agent.*

| Event | Recognition of event by | | | |
|---|---|---|---|---|
| | Runway controller | Ground controller | Crew of a taxiing aircraft | Crew of a taking-off aircraft |
| *a* | yes | no | yes | yes |
| *b* | yes | maybe | yes | maybe |
| *c* | yes | maybe | maybe | no |
| *d* | no | maybe | maybe | no |
| *e* | maybe | maybe | maybe | no |
| *f* | yes | no | maybe | maybe |

## 3.11 Step 10: Identification of organizational constraints

In this step general and domain-specific constraints on the concepts and relations from particular or multiple views of the organizational model are identified. The constraints are divided in two groups:

1. *Generic constraints* that need to be satisfied by any specification of a view or by a combined organizational specification; Two types of generic constraints are considered: (a) structural integrity and consistency constraints based on the rules of the specification composition; (b) constraints imposed by the physical world. Examples of generic constraints are: "not consumed resources become available after all processes are finished" and "non-sharable resources cannot be used by more than one process at the same time".
2. *Domain-specific constraints* are dictated by the application domain and may be changed by the designer. Domain-specific constraints can be imposed by the organization, external parties or the physical world of the specific application domain. Two examples of the

domain-specific constraints are the following: "the amount of driving hours for each driver should not exceed 6 hours per day" (imposed by a law), "agent A has no access to resource of type rt" (imposed by the organization).

Many of the environmental conditions in which an organization operates can be represented by both generic and domain-specific constraints.

A set of constraints imposed on an organizational specification is represented by a logical theory that consists of formulae constructed in the standard predicate logic way from the terms of the dedicated language of the view (and of TTL if temporal relations are required).

The purpose of the formulation of the constraints is, to define key markers for desired behaviour in the organization. The satisfaction of the constraints of the organizational model can be evaluated in analysis and simulation of the model.

**Constraints of the air traffic organizational model**

For the air traffic organizational model, a range of constraints has been identified. Below, a number of examples of constraints are specified. Appendix B.7 shows the full list of constraints identified as formal definitions of these constraints in TTL.

*Constraint 1.*

Each instruction of the controller guiding an aircraft provided to the crew of the aircraft should be read back by one of the pilots within 10 seconds.

*Constraint 2.*

Before performing the crossing or taking off pilots must visually check for conflicting traffic regardless of clearance.

*Constraint 3.*

Both pilots should monitor the frequency when a clearance is called for to ensure that both pilots hear the taxi clearance.

*Constraint 6.*

Each observed incident/accident should be reported by a crew.

*Constraint 12.*

A controller is not allowed to issue any new clearances for some runway until this runway is vacated by the aircraft that had received the last clearance from the controller.

*Constraint 13.*

As soon as a runway is vacated and some aircraft(s) is (are) waiting for the clearance for this runway, the controller responsible for the runway should provide a clearance to one of the waiting aircrafts.

*Constraint 14.*

If a controller cannot reach an aircraft taxiing in the sector for which this controller is responsible, s/he should contact the controller of the sector from which the aircraft came.

*Constraint 15.*

Each observed incident/accident should be reported by a controller.

### 3.12 Organizational model of informal reporting of occurrences

In the development of a model for informal discussion and reporting of safety-related occurrences by groups of controllers we introduce additional roles that are presented in Table 16. The interaction relations between the introduced roles and the formally defined structure of ANSP role are given in Figure 16.

The role Discussion addresses discussion during shifts by controllers of observed occurrences and the identification of potential safety-related problems in such discussion. The subroles Participant 1…N represent the participants of a discussion. Since different numbers of participants may be involved in discussions at different time points, also the number of instances of the role Participant in the role Discussion changes over time. The controller with the highest influence level among the controllers is also allocated to the role Influential Participant. This most influential controller agent provides the interaction of the role Discussion with the role Problem Communication role by allocation to the role Problem Informant. By interaction with role Information Recipient, to which the same agent as for role Head of Controllers is allocated, the Problem Informant propagates the information about the safety-related problem identified in Discussion role further through the managerial hierarchy. This is performed by the information path (i.e., the interaction and interlevel relations) specified in the formal organization between role Head of Controllers and the subroles of OMT and ATCEM roles. When the identified potential safety-related problem is considered at the level of management, it may result into the initiation of an investigation. The process of investigation and the subsequent processes are performed as it is prescribed by the formal incident reporting organization.

Details about tasks, authority relations, agents' influence and performance in informal discussions and additional constraints are presented in Appendix C.

*Table 16: Additional roles for the informal incident reporting path.*

| Level 1 | Level 2 | Level 3 |
|---|---|---|
| ANSP | Discussion | Influential Participant |
| | | Participant 1… N |
| | Problem Communication | Problem Informant |
| | | Information Recipient |

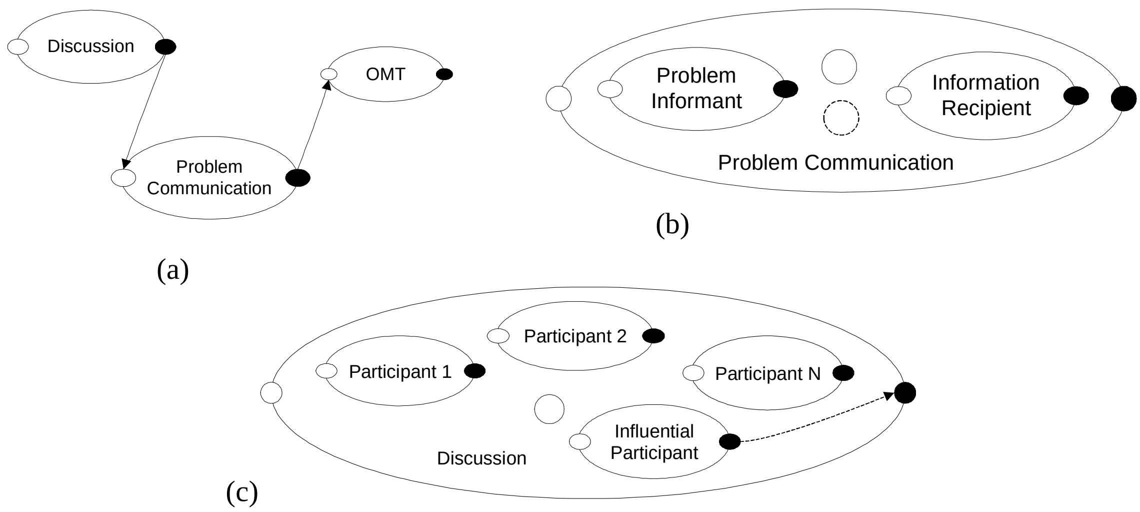


*Figure 16: The interaction relations between (a) the additional roles for informal incident reporting at aggregation level 2,(b) the subroles of the role Problem Communication at aggregation level 3, and (c) the subroles of the role Discussion at aggregation level 3 .*

# 4 Consistency analysis of the organizational model

The framework of (Popova and Sharpanskykh, 2007e) contains a set of automated formal techniques for analysis of organizational specifications. The performance-, process- and organization-oriented views are supported by consistency verification techniques. By applying this analysis type the correctness of a specification of a particular view with respect to the corresponding set of constraints can be established. In logical terms, a specification of a view is correct if the corresponding theory of constraints *T* is satisfied by this specification, i.e., all sentences in *T* are true in the many-sorted first-order structure(s) corresponding to the specification. This type of analysis is described in Section 4.1 to 4.3. Next, Section 5 presents a simulation-based analysis approach for the agent-oriented view.

## 4.1 Consistency analysis of the performance-oriented view

**Consistency of performance indicators**

Based on the formal definitions of relations between performance indicators, all types of relations between the performance indicators can be reduced to causality relations (Popova and Sharpanskykh 2007b). Such a reduction enables the inference of new relations in a performance indicators structure from the existing ones. In general, the inference rules specified in the form

causing(p1, p2, s1) & causing(p2, p3, s2) ⇒ causing(p1, p3, s3),

where p1, p2 and p3 are performance indicators and s1, s2, s3 are of sort SIGN={very_neg, neg, pos, very_pos}. Specific inference rules are provided in Table 17, in which s3 values are given in the cells on the intersection of columns containing s1 values with rows containing s2 values. The verification of the consistency of a performance indicators structure is performed by checking constraints based on these inference rules.

*Table 17: Inference rules for causal relationships.*

| **s2** | **s1** | | | |
|---|---|---|---|---|
| | **Very negative** | **Negative** | **Positive** | **Very positive** |
| **Very negative** | Very positive | Very positive | Very negative | Very negative |
| **Negative** | Very positive | Positive | Negative | Very negative |
| **Positive** | Very negative | Negative | Positive | Very positive |
| **Very positive** | Very negative | Very negative | Very positive | Very positive |

As an example of a consistency check for the air traffic case, consider the relation between PI3 “the level of quality of the internal investigation of a new operation”, PI9 “the development and assessment time of a new operation” and PI7 “the level of elaboration of the high level requirements for a new operation”. In the performance indicator structure, PI3 correlates positively with PI9 and PI9 correlates positively with PI7. If there would be a negative causality relation between PI3 and PI7, there would be an inconsistency.

Consistency analysis for the performance indicator structure presented in Section 3.5 shows that it is consistent.

**Consistency of goals**

A consistency check for goal and performance indicator structures can be performed in a semi-automated way, based on the following principle. If goals are related by a refinement relation, then the performance indicators corresponding to these goals are related by a causality relation. To determine the type of causality, goal expressions can be analyzed. If the performance indicator expressions for goals related by refinement, contain an equality relation (“=”) over comparable (or opposite) measures of degrees (i.e. high/low, maximal/minimal) of some variables, then the corresponding performance indicators are probably related by positive (or negative) causality relation. Comparison functions (i.e., ‘>’,’<’) or change functions (i.e., ‘increased’, ‘decreased’) in performance indicator expressions can be treated in a similar way. Given a functional relation between performance indicators (on which goals in a refinement are based), the type of the causality relation can be determined and used for identifying inconsistencies in the goal structure. Note that since the designer has much of freedom in specifying goal expressions, there is no guarantee that inconsistencies identified in a performance indicator structure are valid. Therefore, all automatically identified inconsistencies in goal and performance indicator structures still need to be confirmed by the designer.

This type of analysis for the goal and the performance indicators structures specified in the case study (Section 3.5) results in the identification of the goal conflicts shown in Table 18. The goals that are in conflict cannot be satisfied (satisficed) at the same time. For example, goal 3 “It is required to achieve a high level of quality of the internal investigation of a new operation” and the goal 9 “It is required to minimize the development and assessment time of a new operation” are in conflict, since the corresponding performance indicators “quality of the internal investigation of a new operation” and “the development and assessment time of a new operation” are related by the positive causality relation, and the corresponding goal patterns are based on the opposite types of functions: maximize (i.e., to achieve a high level) and minimize.

*Table 18: Automatically identified conflicts between goals.*

| **Goal** | | **Conflicting goals** | |
|---|---|---|---|
| **No.** | **Description** | **No.** | **Description** |
| 4.1 | It is required to achieve a satisfactory realization of the safety-related requirements in the concept of a new operation | 4.2 | It is required to achieve a satisfactory realization of the capacity- and volume-related requirements in the concept of a new operation |
| 4.4 | It is required to achieve great involvement of the experts (e.g., controllers) possessing knowledge in the domain of the operation in | 10.3 | It is required to maintain a high (sufficient) level of proficiency of controllers |
| | | 11.2 | It is required to maintain the regular |

| | | | |
|---|---|---|---|
| | the process of operation design | | monitoring of flight data to identify potential hazards and to improve the safety |
| 9 | It is required to minimize the development and assessment time of a new operation | 3 | It is required to achieve a high level of quality of the internal investigation of a new operation |
| | | 7 | It is required to achieve a high level of elaboration of the high level requirements for a new operation |
| 10.1 | It is required to maintain a high level of conformance of all roles involved in air traffic management to the formal norms and regulations defined for their tasks | 20 | It is required to maintain a sufficient level of autonomy of decision making and the operation execution for the roles involved in air traffic management |

For organization models that do not allow conflicts, consistency of a model can be achieved by applying conflict resolution techniques (Van Lamsweerde, Darimont, and Letier, 1998). The common strategy for conflict resolution is based on weakening of goal expressions. This can be achieved by weakening boundary conditions in the performance indicator expressions; by introducing so-called ‘organizational slacks’. Furthermore, the value of the goal priority may be adapted in the process of conflict resolution. In general, organization goals have the higher priority than individual goals of agents. Therefore, in order to fit into the organization, an agent sometimes may need to adjust its own goals to the organizational ones. On the other hand, sometimes priorities of goals of an agent (e.g., important customer, government) can be so high that the organization decides to revise its goal structure to ensure the satisfiability of agent goals. For negotiable goals, conflicts can be solved by negotiations among the stakeholders, to whom the goals are related (Sycara, 1988).

### 4.2 Consistency analysis of the process-oriented view

In the process-oriented view, structural consistency constraints are defined for the three types of structures applied: workflow, task and resource hierarchies. Verification of these constraints on process-oriented specifications is supported by automatic tools (Popova and Sharpanskykh, 2007c). Verification of the correctness of a specification is performed during or at the end of the design process, depending on the type of constraint. Syntactical check of a specification and verification of generic constraints are performed at each design step.

Workflow specifications can be represented and analyzed at different levels of abstraction. In general, the verification of higher-level specifications is computationally cheaper than that of more detailed lower-level specifications. A high-level workflow specification can be refined to a lower level by using the hierarchy of tasks, on which the processes of the workflow are based. In such a case, the correctness verification of the obtained workflow is guaranteed without additional verification. The verification of interaction relations in composite (multi-level, hierarchical) organizational structures is addressed in (Jonker et al., 2007). The algorithms developed for the verification of constraints of different types in the proposed framework are more efficient than general-purpose methods for verifying specifications, e.g. (Clarke, Grumberg, and Peled, 2000).

The consistency analysis shows that the structures of resources and tasks identified in the case study (see Section 3.7) are correct with respect to the generic constraints defined in the process-oriented view.

Regarding the consistency between the goal and task structures (see Section 3.7), it follows from the analysis that all but one constraint is not satisfied. In particular, the following generic constraint defined over both the process-oriented and the performance-oriented views is not satisfied by the task specification: "Each organizational goal should be related to at least one organizational task and each task should contribute to the satisfaction of at least one organizational goal." The automated analysis shows that goal 4.4 "It is required to achieve great involvement of the experts (e.g., controllers) possessing knowledge in the domain of the operation in the process of operation design" does not have a corresponding task. In reality such a goal may be satisfied in an ad-hoc way, without following any particular procedures or regulations.

The automated analysis shows that the flows of control developed in Section 3.9 are consistent with the generic constraints defined in the process-oriented view. Furthermore, the process-oriented specifications satisfy all the relevant domain-specific constraints defined in step 10: constraints 1 and 6 defined on the crew-related processes and constraints 12, 13 and 15 defined for the controller-related processes. Establishing the satisfaction of all other identified constraints can be performed in simulation of organizational scenarios.

### 4.3 Consistency analysis of the organization-oriented view

The organization-oriented view identifies sets of generic consistency constraints on both interaction structures of roles (Jonker et al., 2007) and on formal authority relations (Sharpanskykh 2007a) between roles.

In general, examples of possible conflicts on interaction relations between roles are:

- Existence of a subrole in a composite role that is not related to any other subrole of this role;
- The information type outputted by some role is not in the ontology of the role-recipient (which may mean that this information either should not be sent by the role or other role cannot access the sent information, or roles use different terminology);
- Roles involved in the execution of some task do not interact (may be a problem when they need to interact);
- A communication path does not exist when it should, or does exist when it should not;
- A subrole belongs to two roles at the same time;
- Roles related by a superior-subordinate relation do not interact, whereas they should;

- A role supervising the execution of some process does not interact with a role performing the process, whereas it should;
- A role responsible for consulting some other role about process execution does not interact with the role performing the process;
- A role responsible for making technological/managerial decisions w.r.t. a process is not communicating with the role responsible for the process execution;
- Delays in interactions between agents allocated to roles, e.g. due to inefficient work coordination, physical remoteness etc.;
- A controller issued a clearance to an aircraft for some runway, when another aircraft still occupied this runway;
- After an aircraft has vacated a runway, a controller did not provide a clearance to any of the aircrafts waiting to cross/take off from this runway;
- Pilots did not interact during the execution of some task (some subtask of taxiing);
- Information about an incident observed by some crew was not propagated outside of role Crew;
- Assignment of responsibility to a role that is not authorized for the task's aspect;
- A role with more than two direct superior roles (at the same level of the authority hierarchy) may cause a problem when these roles have different opinions on a task-related decision;
- Conflict between a goal requiring some level of autonomy for a role and a strict authority structure that doesn't allow realizing this goal;
- Responsibility/authorization for some aspect of a task is provided to a role for some time interval and after finishing this interval the role still acts as if the responsibility is still provided.

For the case study, automatic verification of the interaction relations between the roles (defined in Section 3.3) show that they are consistent with the constraints.

The responsibility relations of the roles with respect to the identified tasks (Section 3.8) are also defined in an unambiguous way. For each aspect of each identified task the responsible role(s) is (are) assigned.

There is no formal consistency check to evaluate whether the requirements for roles (Section 3.4) properly reflect the capabilities agents need for effective and efficient accomplishment of the corresponding tasks.

# 5 Agent-based simulation of the organizational model

## 5.1 LEADSTO simulation technique

Based on the various views of the organizational model, simulation can be performed in which different types of agents are allocated to the organizational roles. By considering different simulation scenarios, a range of aspects of the organization can be evaluated using the dedicated language and corresponding tool LEADSTO (Bosse et al., 2005). The LEADSTO language is a sublanguage of TTL that enables modelling direct temporal dependencies between state properties in successive states (i.e. dynamic properties).

Dynamic properties specified in LEADSTO can be executed and can often easily be depicted graphically. The format is defined as follows. Let α and β be state properties of the form 'conjunction of atoms or negations of atoms', and e, f, g, h non-negative real numbers. In the LEADSTO language the notation $\alpha \twoheadrightarrow_{e, f, g, h} \beta$ (also see Figure 17), 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 of length h.*

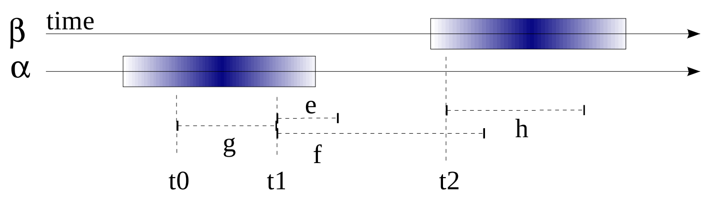


*Figure 17: Timing relationships in LEADSTO*

For example, the dynamic property

> 'if agent A observes that it is dark in the room for 0.5 time points, then after one time point s/he switches on a lamp'

is expressed in LEADSTO as:

input(A, observed(dark_in_room)) $\twoheadrightarrow_{1, 1, 0.5, 1}$ action(A, switch_on_lamp)

The simulation tool provides the possibility to generate the simulation results in the form of a trace. For example, based on the property above the trace is obtained given in Figure 18. Here, the time frame is depicted on the horizontal axis. The names of predicates are shown on the vertical axis. A dark box on top of the line indicates that the predicate is true during that time period.

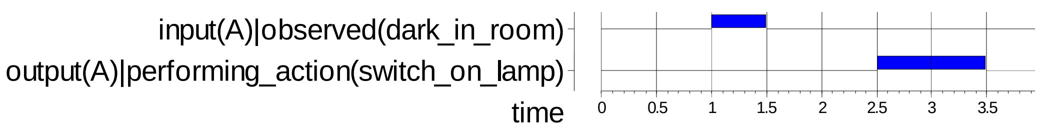


*Figure 18: Example visualisation of a trace*

LEADSTO allows specifying probabilistic rules, in which probability values can be assigned to different consequents of the same antecedent. For example, ‘if agent A observes that it is dark in the room for 0.5 time points, then after one time point s/he switches on the lampA with the probability 0.6 and switches on the lampB with the probability 0.4’

input(A, observed(dark_in_room)) $\twoheadrightarrow_{1,\ 1,\ 0.5,\ 1}$ prob(action(A, switch_on_lampA), 0.6) & prob(action(A, switch_on_lampB), 0.4)

Traces can be used for the validation of specifications by checking dynamic properties in the environment TTL Checker (Bosse et al., 2006) (see Figure 19). Such properties should be specified in TTL and may be expressed using the concepts and the relations defined in different views. The TTL checker environment consists of two closely integrated tools: the Property Editor and the Checker Tool. The Property Editor provides a user-friendly way of building and editing properties in TTL. By means of graphical manipulation and filling in forms a TTL specification can be constructed. TTL specifications may also be provided as plain text. User interaction with the tools involves three separate actions:

(1) Loading, editing, and saving a TTL specification in the Property Editor (see Figure 19).

(2) Loading and inspecting traces to be checked by activating the Trace Manager. Both, traces produced by simulations and empirical traces can be used for verification. Empirical traces provided to the TTL Checker may be obtained by formalizing empirical data from log-files produced by information systems or from results of experiments.

(3) Checking a property against a set of loaded traces by the Checker Tool. The property is compiled and checked, and the result is presented to the user.

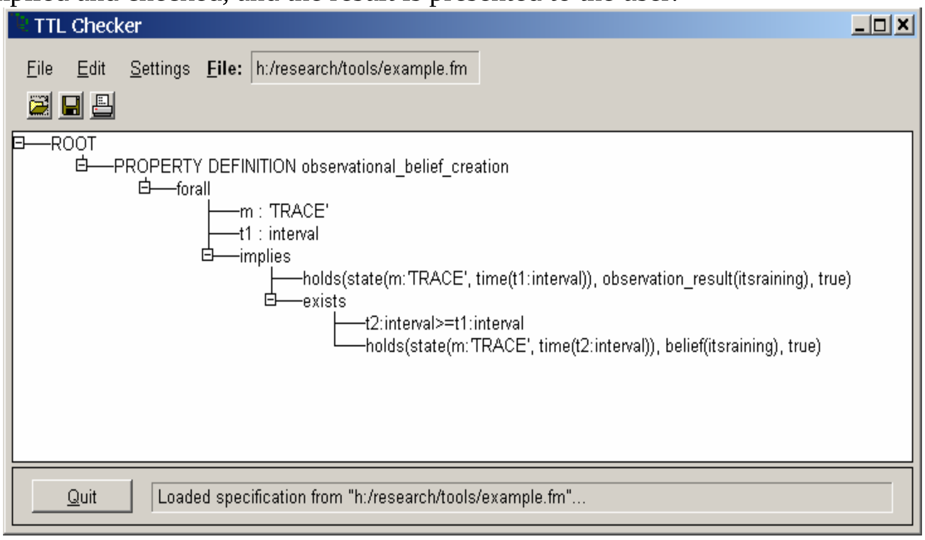


*Figure 19: The TTL Checking Environment*

Given a trace and a formalized property as an input, the automatic verification software generates a positive or negative result. A positive decision confirms that the property holds with respect to the given trace. In case of a negative decision, the software explains why the property does not hold.

Simulation based on a correct and valid specification can also be used for predictions on the organization's behaviour in different environmental conditions and with different agents as well as for investigating theories from the social sciences. The application of this technique will be illustrated in the context of the considered case study in the following section.

## 5.2 Simulation results for safety occurrence reporting

Based on the organizational simulation model defined in Section 3 for safety occurrence reporting, the simulation tool LEADSTO has been applied to perform 100 simulations with a simulation time of maximum 3 years (12 operational hours per day) each. If the formal or informal safety occurrence reporting leads to the identification of a safety problem and a further investigation thereof, the simulation is halted. For simulation performance reasons, the simulation step for the formal incident reporting case equals 1 day, whereas the simulation step for the informal incident reporting equals 1 hour. The latter simulation step value is explained by the necessity to simulate each shift and break time of controllers, whereas for the former case an aggregated view on reporting may be taken without the loss of preciseness, when occurrences are registered and considered on daily basis.

The simulation results for both formal and informal reporting cases are presented in Table 19. The mean time value of the identification of a safety related problem with respect to some event type in the third column is calculated over all traces, in which the occurrences of events of this type caused the incident investigation. The corresponding standard deviation in the fourth column is calculated over the same set of traces.

*Table 19: Results of the simulation experiments.*

| Event | Percentage of traces, in which based on the event type the investigation began | | Mean time value of the recognition of a safety problem (days) | | Standard deviation of time of the recognition of a safety problem (days) | |
|---|---|---|---|---|---|---|
| | Formal | Informal | Formal | Informal | Formal | Informal |
| *a* | 22% | 21% | 155.1 | 134.9 | 59.9 | 56.82 |
| *b* | 5% | 15% | 168.1 | 123.9 | 81.6 | 48 |
| *c* | 28% | 50% | 194.6 | 149.61 | 49.8 | 43.9 |
| *d* | 0% | 0% | - | - | - | - |
| *e* | 0% | 3% | - | 278.9 | - | 49.6 |
| *f* | 45% | 11% | 185.9 | 184.7 | 50.1 | 38 |
| total | 100% | 100% | 180.79 | 150.4 | 55.1 | 53.98 |

Table 19 shows that for both the formal and informal handling of safety occurrences in all simulation traces a safety investigation is initiated, but the mean time until start of the investigation is 181 days in the formal case, whereas it is 150 days in the informal case. Considering the simulation results for the particular events, the mean time of recognition is smaller for all event types in the informal reporting path.

A main reason underlying the difference in the time until recognition of the safety problem is that situations like event *b* (“Taxiing aircraft stops progressing on the runway crossing only after the stopbar and due to a call by the runway controller”) and event *c* (“Taxiing aircraft makes wrong turn and progresses towards the runway crossing”) are often recognized by both ground and runway controllers and thus feed common situation awareness on safety-critical aspects in informal discussions, whereas such events are just single occurrence reports in the formal incident reporting case.

# 6 Discussion

In this report we have presented the first results of a new approach for systemic accident modelling of organizational processes in air traffic, based on the organizational modelling approach of Popova and Sharpanskykh (2007e). This systemic modelling approach provides a broad scope description of the ‘system’ (i.e. the organization) and the variance in its performance. The analysis of the model is focussed on obtaining inconsistencies in the model and evaluating emergent safety-relevant characteristics. Systemic accident modelling can be contrasted with sequential or epidemiological accident modelling approaches, which merely use influencing factors to represent the effect of organizational factors on risk levels.

The organization is modelled according to four interrelated views that account for a variety of organizational aspects. Three of these views have a distinct focus on the formal organization and describe the organizational structure (roles, their interactions, authority relations and resources), the organizational behaviour (processes in an organization and their relations), and the organizational goal-related performance (goals, performance indicators). The fourth view describes the link between the role-based formal organizational model and the agents that used to perform the roles. The performance of the agents is determined by the formal organization, but also influenced by the stochastic dynamics of interacting agents. Variations in the agents’ performance (e.g. tasks are done slower/quicker, tasks are omitted, tasks are done in varying order, etc.), variations in environmental conditions and variations in interactions between agents all have effect on the overall performance of the organization. With these four interrelated views a broad scope of organizational modelling can be achieved.

It follows from the literature survey (Stroeve et al., 2007), that the modelling approach used has the broadest scope of the multi-agent modelling methods identified. In relation with the safety literature, we note that many risk assessment methods have a purely functional focus, which only consider malfunctioning of functions in an operation. It is questionable whether methods with such a limited focus can support effective risk assessment of organizational processes. In contrast, the methods presented in this paper also include functional aspects in the process-oriented view, but they extend the focus extensively to the four interrelated views on organizational modelling.

For broad scope organizational modelling it is important that the methods well support managing a potentially complex model. An issue herein is the level of scalability of the modelling methods. In the approach portrayed, the organization can be modelled at various aggregation levels and particular aspects of the model can be included or excluded at the different aggregation levels, depending on the goal of the study. Modelling tools support automatic expression of relations between model aspects at high and low aggregation levels.

Explanatory ease and usability of the modelling methods is supported by various graphical interfaces and the application of generic templates.

This modelling approach provides a framework to address well-known important contributors to the safety in an organization: human performance/error and organizational/safety culture. The formal organizational model provides a broad scope description of organizational aspects that form the working context of the humans in the organization (e.g. tasks, hierarchy, responsibilities and goals). This working context also represents the prescribed behaviouristic aspect of organizational culture. The agent-oriented view provides the means to describe (the variability of) human performance in interaction with other agents and in the working contexts of the agents. Here, the effect of organizational/safety culture can be described by its influence on the level of performance variability.

This modelling approach provides a framework to address well-known important contributors to the safety in an organization: human performance/error and organizational/ safety culture. The formal organizational model provides a broad scope description of organizational aspects that form the working context of the humans in the organization (e.g. tasks, hierarchy, responsibilities and goals). This working context also addresses aspects of organizational/safety culture, such as information streams, working conditions, management involvement and safety-related behaviour. The agent-oriented view provides the means to describe (the variability of) human performance in interaction with other agents and in the working contexts of the agents. Here, the effect of organizational/safety culture can be described by its influence on the level of performance variability.

The modelling approach supports safety assessment by identification of misconceptions or inconsistencies both at the level of the formal organization for the range of views considered, and at the level of agents by the evaluation of safety-relevant performance in multi-agent simulations. In particular, the consistency analysis identified conflicts at the level of organizational goals, which stem from the tension between capacity and safety objectives of the organization. The presented simulation results indicate the potential strength of informal coordination for safety occurrence reporting. It is noted that the validity of the model has not been evaluated. The prime goal in the research phase presented is the inventory of the possibilities of organizational modelling and the links with safety assessment, rather than the particular outcomes of the model analysis.

The study presented in this report is a first step towards multi-agent systemic accident modelling for organizational processes. This first step has identified a new approach and clarified the types of results that can be attained. The proposed follow-up research aims to lay more direct links with the needs in safety cases for organizational processes and to develop an advanced organizational safety model that addresses those needs. As a basis for this, identification of objectives for further organizational modelling is intended, which will take into account needs from risk assessment cycles and safety case development. This may include the identification of objectives for laying explicit relations with human performance/error and organizational/safety culture. We intend to further increase the validity of the organizational safety model by incorporating more specific knowledge of relevant organizational processes. Building forward on the results achieved, such specific knowledge will be integrated in the organizational model, and model analysis and simulation results will be achieved for the advanced organizational model.

# 7 References


Allen JF (1983). Maintaining knowledge about temporal intervals. *Communications of the ACM*, 26, pp. 832–843.

Bosse T, Jonker CM, van der Meij L, Sharpanskykh A, Treur J (2006). Specification and Verification of Dynamics in Cognitive Agent Models. In: *Proceedings of the Sixth Int. Conf. on Intelligent Agent Technology, IAT'06,* IEEE Computer Society Press, pp. 247-254.

Bosse T, Jonker, CM, van der Meij L, Treur J (2005). LEADSTO: a Language and Environment for Analysis of Dynamics by SimulaTiOn. In: Proceedings of MATES'05. LNAI 3550, edited by T. Eymann et al., Springer Verlag, pp. 165-178.

Clarke EM, Grumberg O, Peled DA (2000). Model Checking, MIT Press.

Galbraith JR (1978). *Organization design*, Addison-Wesley Publishing Company, London Amsterdam Sydney

Hollnagel E (2004). Barriers and accident prevention. Ashgate, Aldershot, England

Hollnagel E, Woods DD, Leveson N (eds.) (2006). Resilience engineering: Concepts and precepts. Ashgate, Aldershot, England

Jonker CM, Sharpanskykh A, Treur J, Yolum P (2007). A Framework for Formal Modeling and Analysis of Organizations, Applied Intelligence, 27(1), pp. 49-66.

Katz D, Kahn R. (1966) The social psychology of organizations. Wiley, New York.

Lawler EE (1973). Motivation in Work Organisations, Cole Publishing.

Le Coze J (2005). Are organizations too complex to be integrated in technical risk assessment and current safety auditing? Safety Science 43:613-638

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

Mintzberg H (1979). The Structuring of Organizations, Prentice Hall, Englewood Cliffs

Perrow C (1984). Normal accidents: Living with high-risk technologies. Basic Books, New York, USA

Pidgeon N, O’Leary M (2000). Man-made disasters: why technology and organizations (sometimes) fail. Safety Science 34:15-30

Pinder CC (1998). Work motivation in organizational behavior. Upper Saddle River, NJ: Prentice-Hall.

Popova V, Sharpanskykh A (2007a). Formal Modelling of Goals in Agent Organizations. In Proceedings of Agent Organizations: Modelling and Simulation Workshop during the 20th International Joint Conference on Artificial Intelligence (IJCAI’07)

Popova V, Sharpanskykh A (2007b). Modeling Organizational Performance Indicators. In Proceedings of International Modeling and Simulation Multiconference, invited session on Agent Based Modeling and Simulation, in Industry and Environment, SCS Press

Popova V, Sharpanskykh A (2007c). Process-Oriented Organization Modeling and Analysis. In Proceedings of the 5th International Workshop on Modelling, Simulation, Verification and Validation of Enterprise Information Systems (MSVVEIS 2007), INSTICC Press

Popova V, Sharpanskykh A (2007d). Formal Analysis Of Executions Of Organizational Scenarios Based On Process-Oriented Models. In Proceedings of 21st EUROPEAN Conference on Modelling and Simulation ECMS 2007, SCS Press

Popova V, Sharpanskykh A (2007e). A Formal Framework for Modeling and Analysis of Organizations. In: Proceedings of the Situational Method Engineering Conference, ME'07, Springer Verlag.

Reason J (1997). Managing the risk of organizational accidents. Ashgate, Aldershot, England

Reason J, Hollnagel E, Paries J (2006). Revisiting the Swiss cheese model of accidents. Eurocontrol, EEC Note no. 13/06

Scott WG, Mitchell TR, Birnbarum PH (1981). Organization theory: a structural and behavioural analysis, Richard D. Irwin inc., Illinois, USA.

Sharpanskykh A (2007a). Authority and its Implementation in Enterprise Information Systems. In Proceeding of the 1st International Workshop on Management of Enterprise Information Systems, MEIS 2007, INSTICC Press.

Sharpanskykh A (2007b). Modeling of Agents in Organizational Context. In: Proceedings of the 5th International Central and Eastern European Conference on Multi-Agent Systems, Springer Verlag.

Sharpanskykh A, Treur J (2006). Verifying Interlevel Relations within Multi-Agent Systems. In: Proceedings of the 17th European Conference on Artificial Intelligence, ECAI'06. IOS Press, 2006, pp. 290-294.

Sträter O (2005). Cognition and safety: An integrated approach to system design and assessment. Ashgate, Aldershot, England

Stroeve SH, Sharspanskykh A, Blom HAP (2007). Literature survey of safety modelling and analysis of organizational processes: Eurocontrol CARE Innovative research III. National Aerospace Laboratory NLR, report CR-2007-156

Sycara, K (1988). Resolving Goal Conflicts via Negotiation: In Proceedings of the Seventh National Conference on Artificial Intelligence, pp. 245-250.

Turner BA (1978). Man-made disasters. Wykeham Science Press, London, UK

Van der Aalst WMP, Ter Hofstede AHM, Kiepuszewski B, Barros AP. (2003). Workflow patterns, Distributed and Parallel Databases, 14(3), pp. 5–51.

Van Lamsweerde A, Darimont R, Letier E (1998). Managing Conflicts in Goal-Driven Requirements Engineering. IEEE Transaction on Software Engineering, vol. 24(11) 908-926.

Vroom VH (1964). Work and motivation. Wiley, New York.

# Appendix A Temporal Trace Language

The first-order sorted predicate logic serves as a formal basis for defining dedicated modelling languages for each view. These languages provide high expressivity for conceptualizing a variety of concepts and relations and allow expressing both quantitative and qualitative aspects of different views. Syntactically each language is defined by a signature that specifies the vocabulary to represent and reason about a system. It comprises sets of sorts (types), sorted constants, functions and predicates.

To express temporal relations in specifications of the views, the dedicated languages of the views are embedded into the Temporal Trace Language (TTL) (Sharpanskykh and Treur 2006), which is a variant of the order-sorted predicate logic. In TTL the organizational dynamics are represented by a trace, i.e. a temporally ordered sequence of states. A state of a system at a certain point in time is an indication of which of the state properties of the system and its environment are true (hold) at that time point. State properties are specified using the dedicated language(s) of the view(s). To express state properties the language TTL includes special sorts, such as: TIME (a set of linearly ordered time points), STATE (a set of all state names of an agent system), TRACE (a set of all trace names; a trace or a trajectory can be thought of as a timeline with for each time point a state), and STATPROP (a set of all state property names).

A state of a system is related to a state property via the satisfaction relation |= formally defined as a binary infix predicate (or by holds as a binary prefix predicate). For example, "in the output state of agent A in trace γ at time t property p holds" is formalized by state(γ , t, output(A)) |= p. Both state(γ , t, output(A)) and p are terms of the TTL language. In general, TTL terms are constructed by induction in a standard sorted predicate logic way from variables, constants and functional symbols typed with TTL sorts. Dynamic properties are expressed by TTL-formulae defined by:

(1) If $v_1$ is a term of sort STATE, and $u_1$ is a term of the sort STATPROP, then holds($v_1$, $u_1$) is an atomic TTL formula.

(2) If $\tau_1$, $\tau_2$ are terms of any TTL sort, then $\tau_1 = \tau_2$ is an atomic TTL formula.

(3) If $t_1$, $t_2$ are terms of sort TIME, then $t_1 < t_2$ is an atomic TTL formula.

(4) The set of well-formed TTL-formulae is defined inductively in a standard way based on atomic TTL-formulae using boolean propositional connectives and quantifiers.

For example, the dynamic property

> "in any trace γ, if at any point in time t1 agent A observes that it is dark in the room, then there exists a point in time t2 after t1 such that at t2 in the trace agent A switches on a lamp".

is expressed in formalized form as:

∀t1 [ state(γ, t1, input(A)) |= observed(dark_in_room) ⇒

∃t2 ≥ t1 state(γ, t2, output(A)) |= performing_action(switch_on_lamp) ]

Notice that also within states statements about time can be made (e.g., in state properties representing memory). To relate time within a state property to time external to states a functional symbol present_time is used.

# Appendix B Details of the formal organizational model

## B.1 Safety-relevant events

The air traffic case considers occurrences for taxiing traffic near an active runway with a traffic flow of 30 aircraft per hour during 12 hours per day. Table 20 shows the safety-relevant events that are form the contextual condition for the organizational model. It also shows the probability values assumed for the safety-relevant events and the resulting mean times between occurrences for the assumed traffic flow.

*Table 20: Probability values assumed for events occurrences and the associated mean time between occurrences for a traffic flow of 360 aircraft per day.*

| Event | | Assumed probability (per taxi operation) | Mean time between events (days) |
|---|---|---|---|
| ID | Description | | |
| *a* | Aircraft rejects take-off as result of a runway incursion | 5e-6 | 556 |
| *b* | Taxiing aircraft stops progressing on the runway crossing only after the stopbar and due to a call by the runway controller | 2e-5 | 139 |
| *c* | Taxiing aircraft makes wrong turn and progresses towards the runway crossing | 1e-4 | 28 |
| *d* | Taxiing aircraft makes wrong turn and progresses on a wrong taxiing route that is not a runway crossing | 2e-4 | 13.9 |
| *e* | Taxiing aircraft has switched to a wrong frequency | 1e-3 | 2.8 |
| *f* | Taxiing aircraft initiates to cross due to misunderstanding in communication | 1e-4 | 28 |

## B.2 Goals and performance indicators

Table 21 shows the complete list of goals and performance indicators of the air traffic organizational model. Table 22 shows the complete list of the characteristics of the goals in the air traffic organizational model.

*Table 21: Complete list of goals and performance indicators of the air traffic organizational model.*

| # | Goal | Performance indicator |
|---|---|---|
| 1 | It is required to achieve a high level of completeness and accuracy of the identification of high level requirements for a new operation from all parties involved in the operation | Completeness and accuracy of the identification of high level requirements for a new operation from all parties involved in the operation |
| 1.1 | It is required to achieve a high level of completeness and accuracy of the identification of high level safety-related requirements for a new operation from all parties involved into the operation | Completeness and accuracy of the identification of high level safety-related requirements for a new operation from all parties involved into the operation |

| | | |
|---|---|---|
| 1.2 | It is required to achieve a high level of completeness and accuracy of the identification of high level capacity- and volume-related requirements for a new operation from all parties involved into the operation | Completeness and accuracy of the identification of high level capacity- and volume-related requirements for a new operation from all parties involved into the operation |
| 1.3 | It is required to achieve a high level of completeness and accuracy of the identification of all other high level requirements for a new operation from all parties involved into the operation | Completeness and accuracy of the identification of all other high level requirements for a new operation from all parties involved into the operation |
| 2 | It is required to achieve a high level of safety of a new implemented operation | Level of safety of a new implemented operation |
| 2.1 | It is required to achieve a high level of safety of the implementation of a new operation | Level of safety of the implementation of a new operation |
| 3 | It is required to achieve a high level of quality of the internal investigation of a new operation | The level of quality of the internal investigation of a new operation |
| 3.1 | It is required to achieve a high level of thoroughness of the internal investigation of a new operation | Level of thoroughness of the internal investigation of a new operation |
| 3.2 | It is required to maintain a high professional level of operation analysts | Professional level of operation analysts |
| 3.3 | It is required to maintain up-to-date knowledge of norms, standards and statistics used for the evaluation of a new operation | Knowledge of norms, standards and statistics used for the evaluation of a new operation |
| 4 | It is required to achieve a satisfactory realization of the high level requirements and their refinements in the concept of a new operation | Realization of the high level requirements and their refinements in the concept of a new operation |
| 4.1 | It is required to achieve a satisfactory realization of the safety-related requirements in the concept of a new operation | Realization of the safety-related requirements in the concept of a new operation |
| 4.2 | It is required to achieve a satisfactory realization of the capacity- and volume-related requirements in the concept of a new operation | Realization of the capacity- and volume-related requirements in the concept of a new operation |
| 4.3 | It is required to achieve a satisfactory realization of other types of requirements in the concept of a new operation | Realization of other types of requirements in the concept of a new operation |
| 4.4 | It is required to achieve great involvement of the experts (e.g., controllers) possessing knowledge in the domain of the operation in the process of operation design | Involvement of the experts possessing knowledge in the domain of the operation in the process of operation design |
| 5 | It is required to achieve a high level of quality of the external investigation of a new operation | Level of quality of the external investigation of a new operation |
| 6 | It is required to achieve a high level of effectiveness and efficiency of a new introduced operation | Level of effectiveness and efficiency of a new introduced operation |
| 6.1 | It is required to achieve a high level of accuracy of the implementation of the concept of a new operation | Level of accuracy of the implementation of the concept of a new operation |
| 7 | It is required to achieve a high level of elaboration of the high level requirements for a new operation | Level of elaboration of the high level requirements for a new operation |
| 7.1 | It is required to achieve a high level of elaboration of the identified high level safety-related requirements for a new operation | Level of elaboration of the identified high level safety-related requirements for a new operation |
| 7.2 | It is required to achieve a high level of elaboration of the identified high level capacity-related requirements for a new operation | Level of elaboration of the identified high level safety-related requirements for a new operation |
| 7.3 | It is required to achieve a high level of elaboration of | Level of elaboration of the other |

| | | |
|---|---|---|
| | the other identified high level requirements for a new operation | identified high level requirements for a new operation |
| 8 | It is required to achieve a high level of productivity of the collaboration within the New Operation Design Team during the development of the concept for a new operation | Level of productivity of the collaboration within the New Operation Design Team during the development of the concept for a new operation |
| 8.1 | It is required to maintain a high professional level of the members of the team | Professional level of the members of the team |
| 8.2 | It is required to maintain constructive discussions during the development of a new operation | Discussions during the development of a new operation |
| 8.3 | It is required to maintain a high level of consideration of the opinions of different members of the team | Level of consideration of the opinions of different members of the team |
| 9 | It is required to minimize the development and assessment time of a new operation | Development and assessment time of a new operation |
| 9.1 | It is required to maintain a frequent collaboration between the New Operation Design Team and the Operation Assessment Unit of the Air Navigation Service Provider during the development of the concept for a new operation | Collaboration between the NODT and the OAU of the ANSP during the development of the concept for a new operation |
| 9.2 | It is required to minimize the development time of the concept of a new operation | Development time of the concept of a new operation |
| 9.3 | It is required to minimize time for an external assessment of a new operation | Time for an external assessment of a new operation |
| 9.4 | It is required to minimize time for an internal assessment of a new operation | Time for an internal assessment of a new operation |
| 10 | It is required to maintain a high level of safety of execution of tasks related to the air traffic management | Level of safety of execution of tasks related to the air traffic management |
| 10.1 | It is required to maintain a high level of conformance of all roles involved into the air traffic management to the formal norms and regulations defined for their tasks | Level of conformance of all roles involved into the air traffic management to the formal norms and regulations defined for their tasks. |
| 10.2 | It is required to maintain a high (sufficient) level of proficiency of pilots | Level of proficiency of pilots |
| 10.2.1 | It is required to maintain a high (sufficient) level of proficiency of pilots operating in regular conditions | Level of proficiency of pilots operating in regular conditions |
| 10.2.2 | It is required to maintain a high (sufficient) level of proficiency of pilots operating in non-stationary (hazardous) conditions | Level of proficiency of pilots operating in non-stationary (hazardous) conditions |
| 10.3 | It is required to maintain a high (sufficient) level of proficiency of controllers | Level of proficiency of controllers |
| 10.3.1 | It is required to maintain a high (sufficient) level of proficiency of controllers operating in regular conditions | Level of proficiency of controllers operating in regular conditions |
| 10.3.2 | It is required to maintain a high (sufficient) level of proficiency of controllers operating in non-stationary (hazardous) conditions | Level of proficiency of controllers operating in non-stationary (hazardous) conditions |
| 10.4 | It is required to maintain the high quality and reliability of communication lines between roles that are supposed to communicate during the execution of the tasks related to the air traffic management | Quality and reliability of communication lines between roles that are supposed to communicate during the execution of the tasks related to the air traffic management |
| 10.5 | It is required to maintain the high quality and | Quality and reliability of |

| | | |
|---|---|---|
| | reliability of communication lines between the roles involved into the air traffic management and the environment | communication lines between the roles involved into the air traffic management and the environment |
| 10.6 | It is required to maintain the high quality and reliability of the hardware used in the air traffic control management | Quality and reliability of the hardware used in the air traffic control management |
| 11 | It is required to maintain an up-to-date set norms and regulations that ensure the safe execution of the air traffic management tasks | Set norms and regulations that ensure the safe execution of the air traffic management tasks |
| 11.1 | It is required to maintain a sufficient proficiency level of regulators and other norm- and regulation-makers | Proficiency level of regulators and other norm- and regulation-makers |
| 11.2 | It is required to maintain the regular monitoring of flight data to identify potential hazards and to improve the safety | Regularity of the monitoring of flight data to identify potential hazards and to improve the safety |
| 11.3 | It is required to maintain the regular investigation of potential safety hazards | Investigation of potential safety hazards |
| 11.4 | It is required to maintain the regular performance of risk assessment of operations. | Performance of risk assessment of operations |
| 11.5 | It is required to maintain a timely update of norms and regulations based on investigation reports | Timeliness of update of norms and regulations based on investigation reports |
| 12 | It is required to maintain a consistent set of norms and regulations for the execution of the air traffic control management tasks | Consistency of a set of norms and regulations for the execution of the air traffic control management tasks |
| 13 | It is required to maintain a high level of effectiveness and efficiency of the work organization within the Tower Control Unit | Level of effectiveness and efficiency of the work organization within the Tower Control Unit |
| 13.1 | It is required to maintain effective coordination of the task execution within the Tower Control Unit | Coordination of the task execution within the Tower Control Unit |
| 13.2 | It is required to maintain high flexibility of the task allocation to the controllers within the Tower Control Unit | Flexibility of the task allocation to the controllers within the Tower Control Unit |
| 13.3 | It is required to maintain a high level of collaboration within the Tower Control Unit | Level of collaboration within the Tower Control Unit |
| 14 | It is required to maintain a high level of effectiveness and efficiency of the work organization of the crew of an aircraft | Level of effectiveness and efficiency of the work organization of the crew of an aircraft |
| 14.1 | It is required to maintain a high flexibility of the task distribution between the pilots of a crew | Flexibility of the task distribution between the pilots of a crew |
| 14.2 | It is required to maintain a high level of collaboration between the pilots of the crew | Level of collaboration between the pilots of the crew |
| 14.3 | It is required to maintain a high level of collaboration during decision making in the crew | Level of collaboration during decision making in the crew |
| 15 | It is required to maintain the timely execution of the processes of the air traffic management | Timeliness of the execution of the processes of the air traffic management |
| 16 | It is required to maintain a high level of robustness and unambiguousness of the control (coordination) structure for the execution of tasks | Level of robustness and unambiguousness of the control (coordination) structure for the execution of tasks |
| 16.1 | It is required to maintain a high level of robustness and unambiguousness of the control (coordination) structure for the execution of tasks in standard conditions | Level of robustness and unambiguousness of the control (coordination) structure for the execution of tasks in standard |

| | | |
|---|---|---|
| | | conditions |
| 16.2 | It is required to maintain a high level of robustness and unambiguousness of the control (coordination) structure for the execution of tasks in non-stationary (exceptional) conditions | Level of robustness and unambiguousness of the control (coordination) structure for the execution of tasks in non-stationary (exceptional) conditions |
| 17 | It is required to maintain timely reporting of incidents/hazards | Timeliness of reporting of incidents/hazards |
| 18 | It is required to maintain timeliness and a high quality of the incident investigation | Timeliness and quality of the incident investigation |
| 18.1 | It is required to maintain a high proficiency level of incident investigators | Proficiency level of incident investigators |
| 18.2 | It is required to maintain a sufficient level of details of (incident/hazard) notification reports | Level of details of (incident/hazard) notification reports |
| 18.3 | It is required to maintain the timely investigation of an incident/hazard | Timeliness of the investigation of an incident/hazard |
| 18.4 | It is required to maintain a high level of thoroughness of the incident investigation | Level of thoroughness of the incident investigation |
| 19 | It is required to maintain a high level of recognition of actual incidents/hazards from the potential ones | Level of recognition of actual incidents/hazards from the potential ones |
| 20 | It is required to maintain a sufficient level of autonomy of decision making and the operation execution for the roles involved into the air traffic management | Level of autonomy of decision making and the operation execution for the roles involved into the air traffic management |
| 21 | It is required to maintain unambiguousness, consistency, correctness and timeliness of information exchanged between agents | Unambiguousness, consistency, correctness and timeliness of information exchanged between agents |
| 21.1 | It is required to maintain a high level of unambiguousness and consistency of information exchanged between agents | Unambiguousness and consistency of information exchanged between agents |
| 21.2 | It is required to maintain the timely provision of information to all agents that require this information | Timeliness of the provision of information to all agents that require this information |
| 21.3 | It is required to maintain the high correctness of information exchanged between agents | Correctness of information exchanged between agents |
| 22 | It is required to achieve a highly expeditious flow of air traffic at an airport | Flow of air traffic at an airport |
| 22.1 | It is required to maintain a high level of efficiency of scheduling of the aircrafts (for taxiing, departures, arrivals) at an airport | Level of efficiency of scheduling of the aircrafts (for taxiing, departures, arrivals) at an airport |
| 23 | It is desired to increase the volume of passengers, departing/arriving from/to an airport | Volume of passengers, departing/arriving from/to an airport |
| 23.1 | It is required to minimize the execution time of the air traffic management tasks | Execution time of the air traffic management tasks |
| 23.2 | It is desired to maximize the territory of an airport | Territory of an airport |
| 23.3 | It is desired to maintain low prices for services | Prices for services |
| 24 | It is desired to maintain a high level of job satisfaction of agents fulfilling the roles in all organizations | Level of job satisfaction of agents fulfilling the roles in all organizations |
| 24.1 | It is desired to maintain a sufficient level of motivation of every employee | Level of motivation of every employee |
| 24.1.1 | It is desired to maintain a sufficient level of autonomy for every employee | Level of autonomy for every employee |

| | | |
|---|---|---|
| 24.1.2 | It is desired to maintain a sufficient amount of feedback for every employee | Amount of feedback for every employee |
| 24.2 | It is desired to achieve that an effective reward system is developed | Effectiveness of the organization reward system |

*Table 22: Complete list of the characteristics of the goals in the air traffic organizational model.*

| # | Priority (max -3) | Horizon | Ownership | Perspective | Hardness | Negotiability |
|---|---|---|---|---|---|---|
| 1 | 2 | short-term | ATCEM, OMT | management | soft | neg. |
| 1.1 | | | | | | |
| 1.2 | | | | | | |
| 1.3 | | | | | | |
| 2 | 3 | | NODT, Regulator, Airport, ANSP | management, customer | | non-neg. |
| 2.1 | | | Airport, ANSP | | | |
| 3 | 2 | | OAU, NODT | management | | neg. |
| 3.1 | | | OAU | | | |
| 3.2 | | | | | hard | |
| 3.3 | | | | | | |
| 4 | | | NODT | | soft | |
| 4.1 | | | | | | |
| 4.2 | | | | | | |
| 4.3 | | | | | | |
| 4.4 | 1 | | | | | |
| 5 | 2 | | Regulator, NODT | | | |
| 6 | 3 | | NODT, OAU, Regulator, Airport, ANSP | management, customer | | |
| 6.1 | | | Airport, ANSP | management | | non-neg. |
| 7 | 2 | | NODT | | | neg. |
| 7.1 | | | | | | |
| 7.2 | | | | | | |
| 7.3 | | | | | | |
| 8 | | | NODT, ATCEM, OMT | | | |
| 8.1 | | long-term | NODT | | hard | non-neg. |
| 8.2 | | short-term | | | soft | neg. |
| 8.3 | | | | | hard | |
| 9 | | | NODT, OAU, Regulator | | soft | |
| 9.1 | | | NODT, OAU | | hard | |
| 9.2 | | | NODT | | | |
| 9.3 | | | Regulator | | | |
| 9.4 | | | OAU | | | |
| 10 | 3 | long-term | TCU, SCU, SIU, Airline | management, customer | soft | non-neg. |
| 10.1 | | | | | hard | |
| 10.2 | | | Pilot in Command, Second Pilot | | | |
| 10.3 | | | TCU, CSU | management | | |
| 10.4 | | | TCU, CSU, SIU, Airline | | | |
| 10.5 | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 10.6 | | | | | | |
| 11 | | | SIU, Regulator | | soft | |
| 11.1 | | | | | | |
| 11.2 | | | SIU | | | neg. |
| 11.3 | 2 | | | | hard | |
| 11.4 | | | SIU, Regulator | | | |
| 11.5 | | | | | | |
| 12 | 3 | | | | | non-neg. |
| 13 | | | TCU, CSU | | | |
| 13.1 | | | | | | |
| 13.2 | | | TCU | | | |
| 13.3 | 2 | | | | soft | |
| 14 | | | Pilot in Command, Second Pilot | | | |
| 14.1 | | | | | | |
| 14.2 | | | | | | |
| 15 | 3 | | Airline, TCU, CSU, SIU | management, customer | | neg. |
| 16 | | | | | hard | |
| 16.1 | | | All roles | | | |
| 16.2 | 2 | | | | | |
| 17 | | | TCU, Airline | | | |
| 18 | | | | | soft | |
| 18.1 | 3 | | | | hard | non-neg. |
| 18.2 | 2 | | SIU, Regulator | | soft | |
| 18.3 | 3 | | | | hard | |
| 18.4 | | | | | soft | |
| 19 | 2 | | TCU, SIU, Regulator | | hard | neg. |
| 20 | | | TCU, SIU, Crew, SIU | management | soft | |
| 21 | | | | | | |
| 21.1 | | | All roles | | hard | non-neg. |
| 21.2 | | | | | | |
| 21.3 | | | | | | |
| 22 | | | Airline, TCU, CSU | | | |
| 22.1 | 3 | | TCU, CSU | | soft | |
| 23 | | | Airline, TCU, CSU, Airport, OMT, ATCEM | | | |
| 23.1 | | | TCU, CSU, OMT, ATCEM | | | neg. |
| 23.2 | 2 | | Airport, ATCEM, Airline | | hard | |
| 23.3 | 3 | | Airport, ATCEM, Airline | management, customer | | |
| 24 | 2 | | All roles | management | soft | |

## B.3 Tasks

Table 23 shows the complete list of tasks in the air traffic organizational model, their characteristics and the goals contributed to by the tasks. Table 24 shows an overview of the resource types used and produced by the tasks.

*Table 23: The tasks in the air traffic organizational model, their characteristics and the goals contributed to by the tasks.*

| # | Task name | Short description | Durations |
|---|---|---|---|
| 1 | Taxiing the aircraft to the designated runway | Taxiing the aircraft on the taxiways and through the runways to the designated runway according to the taxiing instructions provided to the crew | Depends on the durations of subtasks |
| 1.1 | Taxiing the aircraft on a taxiway | - | Depends on a particular taxiway |
| Goal: 13.2, 14.1, 14.3, 24.1.1, 14.2, 23.1, 20 | | | |
| 1.2 | Switching to the frequency of another controller | The action of switching to the frequency of the controller, who will continue the guidance of an aircraft | Min: 1 sec<br>Max: 5 sec |
| Goal: 14.1, 14.3, 14.2 | | | |
| 1.3 | Inquiry for the clearance for crossing an active runway | An inquire to the controller currently guiding the aircraft | Min: 2 sec<br>Max: 5 sec |
| Goal: 14.1, 14.3, 14.2 | | | |
| 1.4 | Making and communicating the decision on a request for crossing a runway | The decision on a request from a crew for crossing an active runway is made by the controller currently guiding the aircraft of the crew | Min: 3 sec<br>Max: 11 sec |
| Goal: 13.1, 22.1, 24.1.1, 23.1, 20 | | | |
| 1.5 | Crossing a runway | - | Min: 30 sec<br>Max: 60 sec |
| Goal: 14.1, 14.3, 23.1, 14.2, 20 | | | |
| 1.6 | Provision of data about a new frequency to a crew | The data are provided to the aircraft's crew by the controller currently guiding the aircraft before the aircraft is handed over to another controller | Min: 2 sec<br>Max: 6 sec |
| Goal: 10.1 | | | |
| 1.7 | Readback of a pilot of the controller's instructions | All instructions provided by controllers to a crew should be read back by one of the pilots of the crew and corrected by the controller if necessary | Min: 2 sec<br>Max: 6 sec |
| Goal: 14.1, 14.3, 21.1, 21.3, 14.2 | | | |
| 1.8 | Transfer of control over an aircraft between controllers | The transfer of control is performed by means of strips that are handed over between the controllers | Min: 2 sec<br>Max: 5 sec |
| Goal: 13.1, 13.3, 23.1 | | | |
| 2 | Acquiring a takeoff allowance | When an aircraft is close to the designated runway the crew initiates the acquiring of the allowance for takeoff from the Runway Controller responsible for the runway | Depends on the durations of subtasks |
| 2.1 | Request for clearance to take off | The request is communicated by the aircraft's crew to the Runway Controller of the designated runway | Min: 2 sec<br>Max: 5 sec |
| Goal: 14.1, 14.3, 14.2 | | | |
| 2.2 | Making and | The decision is made by the controller | Min: 3 sec |

| | | | |
|---|---|---|---|
| | communicating the decision on a request for takeoff | responsible for the runway | Max: 11 sec |
| Goal: 13.1, 22.1, 24.1.1, 23.1, 20 | | | |
| 3 | Take off | - | Min: 30 sec<br>Max: 60 sec |
| Goal: 10.1, 14.1, 14.3, 15, 20, 23.1, 14.2, 13.2 | | | |
| 4 | Incident reporting management based on the data provided by a controller | The incident reporting loop initiated by a (runway or ground) controller | Min: 1 day<br>Max: 160 days |
| 4.1 | Create a notification report | When a controller observes an occurrence that may be classified as an incident/accident, s/he is obliged to create a notification report | Min: 1 min<br>Max: 2 hours |
| Goal: 17, 18.2, 19, 20 | | | |
| 4.2 | Preliminary processing of a notification report | A notification report created by a controller is examined and improved by his/her supervisor. The occurrence described in the report is classified. | Min: 1 min<br>Max: 2 days |
| Goal: 19, 13.3, 20 | | | |
| 4.3 | Making decision about the investigation necessity based on the provided notification report | If the occurrence is of a high severity, the incident/accident investigation will be initiated. The lower the level of severity of the occurrence, the less the chance that the occurrence will be immediately investigated | Min: 1 day<br>Max: 30 days |
| Goal: 19, 20 | | | |
| 4.4 | Investigation of the occurrence based on the notification report | During the investigation the (possible) causes of the incident/accident are identified, and based on the investigation results recommendations are provided | Min: 3 days<br>Max: 90 days |
| Goal: 18.3, 18.4, 20 | | | |
| 4.5 | Discussion of the intermediate occurrence investigation results | The intermediate results of the investigation are provided to the OMT of the ANSP | Min: 1 day<br>Max: 15 days |
| Goal: 11.5, 12 | | | |
| 4.6 | Reviewing of the occurrence investigation results | The Executive Board of the ATC reviews the incident/accident investigation results | Min: 5 min<br>Max: 4 hours |
| Goal: 11.5, 12, 20 | | | |
| 4.7 | Distribute the occurrence investigation report among all concerned roles | - | Min: 1 hour<br>Max: 15 days |
| Goal: 21.2, 21.3, 21.1 | | | |
| 5 | Incident reporting management based on the data provided by a crew | The incident reporting loop initiated by a crew | Depends on the durations of subtasks |
| 5.1 | Create a notification report and provide it to | When a pilot (a crew) observes an occurrence that may be classified as an | Min: 2 hours<br>Max: 2 days |

| | | | |
|---|---|---|---|
| | the SMU | incident/accident, s/he is obliged to create a notification report, which may be further provided to the SMU of the airline by which the pilot is employed | |
| Goal: 14.1, 14.3, 17, 18.2, 19, 14.2, 20 | | | |
| 5.2 | Create a notification report and provide it to the regulator | A notification report created by a pilot may be provided directly to the regulator | Min: 1 day<br>Max: 14 days |
| Goal: 14.1, 14.3, 17, 18.2, 19, 14.2, 20 | | | |
| 5.3 | Process a notification report and provide it to the regulator | A notification report created by a pilot (a crew) is examined and improved by the SMU and provided further to the regulator for further investigation | Min: 1 day<br>Max: 90 days |
| Goal: 19, 20 | | | |
| 5.4 | Making decision about the investigation necessity and about the role-investigator | The decision is based on the notification report and the choice of the role-investigator is based on the severity of the incident/accident, the availability of roles and the competences of the available roles | Min: 1 day<br>Max: 30 days |
| Goal: 18.3, 18.4, 20 | | | |
| 6 | Identification of hazards, safety problems and trends | Once in three months the SIU of the ANSP performs an investigation on the collected notification reports and the occurrence investigation results. The aim of this investigation is to identify safety hazards, problems and trends | Min: 20 days<br>Max: 30 days |
| Goal: 11.3, 11.4, 15, 11.2, 20 | | | |
| 7 | Design and evaluate a new operation | - | Depends on the durations of subtasks |
| 7.1 | Produce an intermediate design for a new operation | During the development of the concept of a new operation a number of intermediate design concepts are produced which are provided for the further evaluation | Depends on the particular operation. For the operation “runway introduction”:<br>Min: 2 weeks<br>Max: 1 month |
| Goal: 4.1, 4.2, 4.3, 7.1, 7.2, 7.3, 8.1, 8.2, 8.3, 9.1, 9.2, 24.1.1, 20 | | | |
| 7.2 | Assess an intermediate design for a new operation internally | The internal evaluation of an intermediate design within the ANSP | Min: 2 days<br>Max: 1 week |
| Goal: 3.1, 9.1, 9.4, 20 | | | |
| 7.3 | Produce the final concept of a new operation | Based on the previous intermediate design concepts and the results of the internal evaluation, the final concept of operation is produced | Min: 4 days<br>Max: 2 week |
| Goal: 4.1, 4.2, 4.3, 7.1, 7.2, 7.3, 8.1, 8.2, 8.3, 9.2, 20 | | | |
| 7.4 | Assess the final concept of a new operation externally | The final concept of a new operation is assessed externally | Min: 2 week<br>Max: 1 month |
| Goal: 3.1, 3.2, 3.3, 9.3, 5, 20 | | | |
| 7.5 | Review the final concept of a new operation | - | Min: 3 days<br>Max: 1 week |
| Goal: 4.1, 4.2, 4.3, 6.1, 20 | | | |
| 8 | Implement a new | - | Depends on the particular |

| | | | |
|---|---|---|---|
| | operation | | operation. For the operation "runway introduction":<br>Min: 3 month<br>Max: 1 year |
| Goal: 2.1, 20 | | | |
| 9 | Create a list of high level requirements for a new operation | This task precedes and produces an input for the final concept development task. Both safety and performance-related goals should be reflected in the requirements. | Min: 1 month<br>Max: 3 month |
| Goals: 1, 20 | | | |
| 10 | Schedule training for a pilot | - | Min: 1 min<br>Max: 5 min |
| Goal: 10.2, 14, 20 | | | |
| 11 | Schedule training for a controller | - | Min: 1 min<br>Max: 5 min |
| Goals:10.3, 20 | | | |
| 12 | Schedule training for an operation analyst | - | Min: 1 min<br>Max: 5 min |
| Goals: 3.2, 20 | | | |
| 13 | Schedule training for a safety investigator | - | Min: 1 min<br>Max: 5 min |
| Goal: 18.1, 11.1, 20 | | | |
| 14 | Get training | - | Depends on the particular training type |
| Goal: 10.2, 14, 10.3, 3.2, 18.1, 11.1 | | | |
| 15 | Allocation of agents to controllers roles | - | Constantly |
| Goal: 13.2, 16, 20 | | | |

*Table 24: The resource types used and produced by tasks.*

| Task | Task uses | Task produces |
|---|---|---|
| 1.1 | the airport's diagram, the taxi instructions for the flight, compass, radar, visual observations, aircraft | the aircraft's trajectory on the airdrome |
| 1.2 | data about the new frequency | - |
| 1.3 | the observation of the close proximity of the active runway to be traversed, the taxi instructions for the flight, communication R/T system | a request to the Runway Controller responsible for the runway for the clearance for crossing the runway |
| 1.4 | data about the current state of the runway, a request from the aircraft's crew to the Runway Controller responsible for the runway for the clearance for crossing the runway, communication R/T system | the instruction to the crew (which may be 'position and hold' (wait) or 'the clearance to cross is provided') |
| 1.5 | the clearance from the Runway Controller for crossing the runway, the airport's diagram, the taxiing instructions, compass, radar, visual observations, aircraft | the pilot's report 'clear of the runway' to the Runway Controller controlling the runway |
| 1.6 | the observation that the aircraft is approaching to the margins the current sector, the data about the controller of the adjoining region (i.e., a sector or a runway), communication R/T systems | data about the frequency of the controller of the adjoining sector |
| 1.7 | the controller's instruction, communication R/T systems | the correct readback of the controller's instruction |

| | | |
|---|---|---|
| 1.8 | the observation that the aircraft is approaching to the margins the current sector, the data about the controller of the adjoining region (i.e., a sector or a runway) | the strip with the aircraft's details provided to the controller, who will be guiding the aircraft |
| 2.1 | the observation of the close proximity of the designated runway, communication R/T systems | a request to the Runway Controller of the designated runway for the clearance to take off |
| 2.2 | data about the current state of the runway, a request to the Runway Controller of the designated runway for the clearance to take off, communication R/T systems | the instruction to the crew (which may be 'position and hold' (wait) or 'the clearance to takeoff is provided') |
| 3 | the clearance from the Runway Controller to takeoff, compass, radar, visual observations, aircraft, RIAS | the pilot's report 'clear of the runway' to the Runway Controller controlling the runway |
| 4.1 | the observation from the environment of an occurrence that may be classified as an incident/accident, the incident classification database | a notification report |
| 4.2 | a notification report | a processed notification report |
| 4.3 | a processed notification report | a decision on the initiation of the occurrence investigation |
| 4.4 | a processed notification report, additional data about the occurrence (optional) | an incident investigation report |
| 4.5 | a processed notification report, an incident investigation report, occurrence statistics | recommendations based on the incident investigation report |
| 4.6 | an incident investigation report | directions to redesign some operation(s) (optional) |
| 4.7 | an incident investigation report, the list of all concerned roles | - |
| 5.1 | the observation from the environment of an occurrence that may be classified as an incident/accident, the incident classification database | a notification report |
| 5.2 | the observation from the environment of an occurrence that may be classified as an incident/accident, the incident classification database | a notification report |
| 5.3 | a notification report | a processed notification report |
| 5.4 | a (processed) notification report | a decision on the initiation of the occurrence investigation, a decision concerning the role-investigator |
| 6 | Collected notification reports, incident/accident investigation reports, occurrence statistics | a report on the identified safety hazards, problems and trends |
| 7.1 | a list of high level requirements for a new operation, (optional) results of the internal assessment of the previous intermediate design concepts for a new operation, (optional) the previous intermediate design concept for a new operation. | an intermediate design concept for a new operation |
| 7.2 | an intermediate design for a new operation, the evaluation framework | the results of the internal assessment of an intermediate design for a new operation |
| 7.3 | operation requirements, the current intermediate design for a new operation | the final concept of a new operation |
| 7.4 | the final concept of a new operation, the evaluation framework | the results of the external assessment of the final concept of a new operation |

| | | |
|---|---|---|
| 7.5 | the final concept of a new operation, the results of the internal assessment of the final concept of a new operation, the results of the external assessment of the final concept of a new operation | a permission/prohibition for the implementation of a new operation |
| 8 | the permission for the implementation of a new operation, the final concept of a new operation | the new operation implemented |
| 9 | - | a list of high level requirements for a new operation |
| 10 | data about a pilot | training scheduled for a pilot |
| 11 | data about a controller | training scheduled for a controller |
| 12 | data about an operation analyst | training scheduled for an operation analyst |
| 13 | data about a performance investigator | training scheduled for a performance investigator |
| 14 | data about a scheduled training | - |
| 15 | Data about the available agents and their workload, data about the roles that have to be allocated | - |

## B.4 Authority relations

Table 25 shows all responsibility relations in the air traffic organization model.

*Table 25: The responsibility relations in the air traffic organization model.*

| Task | Execution | Monitoring | Consulting | Technological decisions | Managerial decisions |
|---|---|---|---|---|---|
| 1.1 | Crew | Runway Controller, Tower Controllers Supervisor | Runway Controller | Crew | Runway Controller, Tower Controllers Supervisor |
| 1.2 | Crew | | Runway Controller | Crew | |
| 1.3 | Crew | | | | |
| 1.4 | Runway Controller | Tower Controllers Supervisor | Tower Controllers Supervisor, other Runway and Ground Controllers | Runway Controller | |
| 1.5 | Crew | Runway Controller | Runway Controller, Tower Controllers Supervisor | Crew | Crew, Runway Controller, Tower Controllers Supervisor |
| 1.6 | Runway or Ground Controller | Tower Controllers Supervisor | | Runway Controller | |
| 1.7 | Pilot | Runway or Ground Controller | | | |
| 1.8 | Aircraft's controller (i.e., | Tower Controllers Supervisor | | Aircraft's controller | |

| | | | | |
|---|---|---|---|---|
| | controller currently responsible for the aircraft) | | | |
| 2.1 | Crew | | | |
| 2.2 | Runway Controller | Tower Controllers Supervisor | Runway Controller | |
| 3 | Crew | Runway Controller | Crew | Crew, Runway Controller |
| 4.1 | Runway or Ground Controller | | | |
| 4.2 | Tower Controllers Supervisor | | | |
| 4.3 | SIU | | | |
| 4.4 | Safety Investigator | Head SIU | Safety Investigator | Safety Investigator, Head SIU |
| 4.5 | OMT | | | |
| 4.6 | ATCEM | | | |
| 4.7 | OMT | | | |
| 4.8 | Safety Investigator or Regulator | OMT, ATCEM | Safety Investigator, Regulator | OMT, ATCEM |
| 5.1 | Crew | | | |
| 5.2 | Crew | | | |
| 5.3 | SMU | | | |
| 5.4 | Regulator | | | |
| 6 | Regulator | | | |
| 7.1 | New Operation Design Team | | | |
| 7.2 | Operation Analyst | Head OAU | Operation Analyst | Head OAU |
| 7.3 | New Operation Design Team | | | |
| 7.4 | Regulator | | | |
| 7.5 | OMT, ATCEM, Airport Management | | | |
| 8 | Airport | | | |
| 9 | OMT, ATCEM, Airport Management, Airline Management | | | |
| 10 | Airline Management | | | |
| 11 | Tower Controllers Supervisor | | | |
| 12 | Head OAU | | | |
| 13 | Head SIU | | | |
| 14 | Pilot, Controller, Operation Analyst, Safety. Investigator | Airline Management, Tower Controllers Supervisor, Head OAU, Head SIU | | |
| 15 | Tower Controllers Supervisor | | | |

### B.5 Workflows

A workflow is defined by a set of (partially) temporally ordered processes. Each process, except for the special ones with zero duration introduced below, is defined using a task as a template and all characteristics of the task are inherited by the process. This is specified using the predicate: is_instance_of: PROCESS × TASK. Decisions are also treated as processes that are associated with decision variables taking as possible values the possible decision outcomes.

A workflow starts with the process BEGIN and ends with the process END; both have zero duration. The (partial) order of execution of processes in the workflow is defined by sequencing, branching, cycle and synchronization relations (referred to as ordering relations) specified by the designer.

A sequencing relation is specified by the predicate starts_after: PROCESS × PROCESS × VALUE expressing that the process specified by the first argument starts after the process specified by the second argument with the delay expressed by the third argument, represented graphically by solid arrows between the processes (see Figure 12 on page 39). For each process p, different from BEGIN and END at least two sequencing constraints are defined, which specify the process that precedes p and the process which follows after p.

Synchronization relations define temporal relations between processes that are executed in parallel (e.g. starts_with, finishes_with, starts_during: PROCESS × PROCESS). An example of such a relation is shown by a dashed line between the beginnings or endings of the processes in Figure 12 on page 39, meaning that the connected processes should start or finish simultaneously. Taken together, synchronization and sequencing relations allow specifying all cases of interval relations defined in (Allen 1983).

Branching relations are defined over and- and or-structures. An and(or)-structure with name id, starts with the zero-duration process begin_and(id) (begin_or(id)) and finishes by the zero-duration process end_and(id) (end_or(id)). These special processes are represented graphically by rhombuses. Our treatment of AND-structures is similar to the parallel split pattern combined with all types of the merge pattern from (van der Aalst et al. 2003), represented in our case by an and-condition. The first processes in every branch of an and-structure start at the same time. For each and-structure a condition is defined (and_cond: AND_STRUCTURE × CONDITION_EXPRESSION), which determines when the process p following after the and-structure may start. The following types of conditions may be used: (1) constant any: meaning that as soon as all processes of one of the branches finish, the process p starts; (2) constant all: meaning that as soon as all processes of all branches finish, the process p starts; (3) a condition expressed by a logical formula constructed from the functions finished, not_finished: PROCESS → {true, false} using Boolean connectives ∨ and ∧.

For every or-structure a condition is defined (or_cond: OR_STRUCTURE × CONDITION_EXPRESSION), based on which it is determined which branches of the or-structure will start. The condition may consist only of a condition variable or it may be a disjunction of conjunctions of expressions in the form condition_variable [OP value], where OP∈{=, ≠, <, >}, and value belongs to the domain of the condition variable. The following types of condition variables can be used: (1) a decision variable; (2) a variable over the sort that includes all states of a certain object in the environment, e.g. market conditions, customer demand, taxes, weather conditions, etc.; (3) a variable over the sort that includes all values of certain characteristic of an object in the environment. For an or-structure branches are specified that correspond to all possible values of the condition expression, using the predicate or_branch: OR_COND_VALUE × PROCESS, which expresses that the branch of the or-structure that begins with the process specified in the second argument corresponds to the value of the condition expression specified in the first argument. An or-branch may correspond to the constant other, which should be interpreted as all other values from the domain of the condition variable. Our treatment of or-structures allows realizing both exclusive and multiple-choice patterns from (van der Aalst et al. 2003).

Cycle relations are defined over loop-structures with conditions that realize cycle patterns from (van der Aalst et al. 2003). For every loop-structure a Boolean condition (loop_cond: LOOP × CONDITION_EXPRESSION) and the maximal number of times of the loop execution (loop_max: LOOP × VALUE) are specified. No cycles were identified for the running example.

*Workflow for aircraft taxiing to and taking off from designated runway*

Below a formal specification in the vocabulary specified is given of the workflow for an aircraft taxiing to and taking off from a designated runway. Graphically this workflow is specified in Figure 12 on page 39.

is_instance_of(Allocation of agents to controllers roles, Allocation of agents to controllers roles)
is_instance_of(Transfer of control over the aircraft, Transfer of control over an aircraft between controllers)
is_instance_of(Provision data on the new frequency, Provision of data about a new frequency to a crew)
is_instance_of(Switching to the new frequency, Switching to the frequency of another controller)
is_instance_of(Taxiing the aircraft on the taxiway, Taxiing the aircraft on a taxiway)
is_instance_of(Inquire for clearance to cross, Inquiry for the clearance for crossing an active runway)
is_instance_of(Repeated inquiry for clearance to cross, Inquiry for the clearance for crossing an active runway)
is_instance_of(Decision making on the request for the clearance, Making and communicating the decision on a request for crossing a runway)
is_instance_of(Readback of the crossing instructions, Readback of a pilot of the controller's instructions)
is_instance_of(Readback of the take off instructions, Readback of a pilot of the controller's instructions)
is_instance_of(Crossing the runway, Crossing a runway)
is_instance_of(Request for the clearance to take off, Request for clearance to take off)
is_instance_of(Decision making concerning the request for the clearance to take off, Making and communicating the decision on a request for takeoff)
is_instance_of(Take off, Take off)
starts_after(begin_and(and4), begin, 0)

starts_after(begin_loop(c5), begin_and(and4), 0)

loop_cond(c5, “workflow is not finished”)

loop_max(c5, 50)

starts_after(begin_or(or3), begin_loop(c5), 0)

or_cond(or3, “A new allocation of agents controllers to roles?”)

or_branch(or3, yes, Allocation of agents to controllers roles)

or_branch(or3, no, end_or(or3))

starts_after(end_or(or3), Allocation of agents to controllers roles, 0)

starts_after(end_loop(c5), end_or(or3), 0)

starts_after(end_and(and4), end_loop(c5), 0)

and_cond(and4, all)

starts_after(begin_and(and0), begin_and(and4), 0)

starts_after(begin_loop(c4), begin_and(and0), 0)

starts_after(begin_or(or2) ,begin_loop(c4), 0)

or_cond(or2, “is another region close?”)

or_branch(or2, yes, begin_and(and3))

or_branch(or2, no, end_or(or2))

starts_after(Transfer of control over the aircraft, begin_and(and3), 5)

starts_after(end_and(and3), Transfer of control over the aircraft, 0)

starts_after(Provision data on the new frequency, begin_and(and3), 1)

starts_after(Switching to the new frequency, Provision data on the new frequency, 1)

starts_after(end_and(and3), Switching to the new frequency, 0)

and_cond(and3, all)

starts_after(end_or(or2), end_and(and3), 0)

starts_after(end_loop(c4), end_or(or2), 0)

loop_cond(c4, “away from the designated runway”)

loop_max(c4, 5)

starts_after(end_and(and0), end_loop(c4), 0)

and_cond(and0, all)

starts_after(begin_loop(c1), begin_and(and0), 0)

loop_cond(c1, “away from the designated runway”)

loop_max(c1, 7)

starts_after(begin_or(or1), begin_loop(c1), 0)

or_cond(or1, “observed location”)

or_branch(or1, taxiway, Taxiing the aircraft on the taxiway)

or_branch(or1, active runway, Inquire for clearance to cross)

starts_after(end_or(or1), Taxiing the aircraft on the taxiway, 0) starts_after(begin_loop(c2), Inquire for clearance to cross, 0)

loop_cond(c2, "decision position and hold")

loop_max(c2, 4)

starts_after(Decision making on the request for the clearance, begin_loop(c2), 0)

starts_after(Readback of the crossing instructions, Decision making on the request for the clearance, 1)

starts_after(begin_loop(c4), Readback of the crossing instructions, 0)

loop_cond(c4, "runway is occupied")

loop_max(c4, 1000)

starts_after(end_loop(c4), begin_loop(c4), 1)

starts_after(end_loop(c2), end_loop(c4), 0)

starts_after(Crossing the runway, end_loop(c2), 8)

starts_after(end_or(or1), Crossing the runway, 0)

starts_after(end_loop(c1), end_or(or1), 0)

starts_after(end_and(and0), end_loop(c1), 0)

starts_after(Request for the clearance to take off, end_and(and0), 1)

starts_after(begin_loop(c3), Request for the clearance to take off, 0)

loop_cond(c3, "decision position and hold")

loop_max(c3, 4)

starts_after(Decision making concerning the request for the clearance to take off, begin_loop(c3), 0)

starts_after(Readback of the take off instructions, Decision making concerning the request for the clearance to take off, 1)

starts_after(begin_loop(c6), Readback of the take off instructions, 0)

loop_cond(c6, "runway is occupied")

loop_max(c6, 1000)

starts_after(end_loop(c6), begin_loop(c6), 1)

starts_after(end_loop(c3), end_loop(c6), 0)

starts_after(Take off, end_loop(c3), 8)

starts_after(End, Take off, 0)

### B.6 Agents' performance

A belief of an agent is created based on one of the following events:

1. observation from the environment: a belief state is generated after the agent observed some occurrence in the environment;
2. a communication provided to/obtained from another agent: belief states are changed for the agents involved in the communication;
3. an action performed by the agent in the environment: a belief state is changed after the agent performed an action.

Consider the rules of the generation of a belief state for all three types of events.

For the events of the type (a) a belief state is generated at the next time point after the agent observed some occurrence in the environment. Thus, for the agent allocated to a role r1 the following rule holds:

∀γ: TRACE ∀content_var:CONTENT ∀t1:TIME holds(state(γ, t1, input(r1)), communication_from_to(env, r1, observe, content_var))) ⇒

holds(state(γ, t1+1, internal(r1)), belief(observed, env, content_var))

Here the sort CONTENT is formed based on the functions defined in Table 3on page 20. In such a way, beliefs about all events represented by the functions in Table 3 can be generated.

When the agent ag1 that fulfils the role r1 informs some information to the agent ag2 that fulfils the role r2, then the belief states are created for both agents: for ag1 – about sending information when it is sent and for ag2 – about receiving information, when it is received:

For sending information of type CONTENT:

∀γ: TRACE ∀content_var:CONTENT ∀t1:TIME holds(state(γ, t1, output(r1)), communication_from_to(r1, r2, inform, content_var))) ⇒

holds(state(γ, t1+1, internal(r1)), belief(informed, r2, content_var))

For receiving information of type CONTENT:

∀γ: TRACE ∀content_var:CONTENT ∀t1:TIME holds(state(γ, t1, input(r2)), communication_from_to(r1, r2, inform, content_var))) ⇒

holds(state(γ, t1+1, internal(r2)), belief(informed_by, r1, content_var))

The belief generation rules for other types of communication acts (request and decision_made) are defined in a similar way. E.g., if one agent requests some information from another agent, then the belief states are created for both agents: for the agent-requester – about sending the request when it is sent, for the agent- recipient – about the receipt of the request when it is received.

For the events of the type (c) a belief state is generated at the next time point after the agent has performed some action. Thus, for the agent allocated to a role r1 the following rule holds:

∀γ: TRACE ∀act:ACTION ∀t1:TIME holds(state(γ, t1, output(r1)), performed_action(act)) ⇒

holds(state(γ, t1+1, internal(r1)), belief(performed_by, r1, act))

Here the sort ACTION consists of all types of actions performed by agents in the case study represented by the tasks from the sort TASK.

A belief state of an agent allocated to a role r1 persists until it is invalidated. An invalid belief is specified by the predicate belief_invalid: BEL_TYPE x ROLE x CONTENT. To specify the persistency rule for a belief of an agent allocated to a role r1 with the content content_var the following rule is used:

∀γ: TRACE ∀content_var:CONTENT ∀t1:TIME ∀bel:BEL_TYPE holds(state(γ, t1, internal(r1)), belief(bel, r1, content_var) ∧ ¬ belief_invalid(bel, r1, content_var)) ⇒
holds(state(γ, t1+1, internal(r1)), belief(bel, r1, content_var))

### B.7 Constraints

The complete list of constraints identified for the air traffic organizational model is given below.

*Constraint 1.*

Each instruction of the controller guiding an aircraft provided to the crew of the aircraft should be read back by one of the pilots within 10 seconds.

Formally:

∀γ: TRACE ∀ct_var: MSG_TYPE ∀content_var:CONTENT ∀t1:TIME holds(state(γ, t1, input(Crew Representative)), communication_from_to(Aircraft's Controller, Crew_Representative, ct_var, content_var)) ⇒ ∃t2 ≤ t1+10 holds(state(γ, t2, output(Crew Representative)), communication_from_to(Crew Representative, Aircraft's Controller, readback, content_var))

*Constraint 2.*

Before performing the crossing or taking off pilots must visually check for conflicting traffic regardless of clearance.

Formally:

∀γ: TRACE ∀content_var:CONTENT ∀t1:TIME ∀clear_var:CLEARANCE ∀runway_var: RUNWAY holds(state(γ, t1, internal(Crew)), belief(decision_provided_by, Aircraft's Controller, instruction(clear_var, runway_var)) ∧ belief(observed, env, runway(runway_var, clear)) ⇒ holds(state(γ, t1+1, output(Crew)), begin_execution(cross_runway(runway_var)))

*Constraint 3.*

Both pilots should monitor the frequency when a clearance is called for to ensure that both pilots hear the taxi clearance.

Formally:

∀γ: TRACE ∀t1, t2:TIME t2 > t1 ∀clear_var:CLEARANCE ∀runway_var: RUNWAY ∀instr_var: INSTRUCTION_TYPE ∀ag1, ag2: AGENT
holds(state(γ, t1, output(Crew Representative)), communication_from_to(Crew Representative, Aircraft's Controller, request, instruction(clear_var, runway_var))) &
holds(state(γ, t2, input(Crew Representative)), communication_from_to(Aircraft's Controller, Crew Representative, decision, instruction(instr_var, runway_var))) &

holds(state(γ, t1, env, agent_plays_role(ag1, Pilot in Command) ∧ agent_plays_role(ag2, Second Pilot)) &
⇒ ∀t3 t2 > t3 > t1 holds(state(γ, t3, env), agent_plays_role(ag1, Crew Representative) ∧
agent_plays_role(ag2, Crew Representative))

*Constraint 4.*
When an aircraft is approaching to an active runway, the pilots should cease all processes not related to the taxiing.
Formally:
∀γ: TRACE ∀t1, t2: TIME t2 > t1 ∀acraft_var:AIRCRAFT ∀clear_var:CLEARANCE ∀runway_var: RUNWAY ∀ag1, ag2: AGENT ∀p1: TAXIING_AIRCRAFT ∀r1: ROLE
holds(state(γ, t1, env), aircraft_approaches_to(acraft_var, runway_var) ∧ agent_plays_role(ag1, Pilot in Command) ∧ agent_plays_role(ag2, Second Pilot)) ⇒
holds(state(γ, t1, env), process_execution(p1, Pilot in Command) ∧ process_execution(p1, Second Pilot) ∧ ¬∃p2: PROCESS p2≠p1 process_execution(p2, r1) ∧ (agent_plays_role(ag1, r1) ∨ agent_plays_role(ag2, r1)))

*Constraint 5.*
In case the pilots have different beliefs about certain objects or events related to the taxiing or taking off tasks, one of the pilots should contact the controller currently guiding the aircraft for the clarification.

This rule should be specified by several constraints, one of which is the following:
If pilots have different beliefs about the received clearance, they should contact the Aircraft's Controller again.
This and the following constraints are formalized in a similar way as the previous constraints.

*Constraint 6.*
Each observed incident/accident should be reported by a crew.

*Constraint 7.*
The pilots of the crew should verbally share relevant information with each other.

*Constraint 8.*
Any information received or transmitted during the absence of one of the crew members should be provided to him/her upon his/her return.

*Constraint 9.*

If a pilot is revealed/reveals himself/herself from the allocation to the role Crew Representative that constantly monitors the frequency of the Aircraft's Controller role, then this pilot should inform all other crew members about this.

In the following consider some of the constraints obtained from the regulations related to the functioning of a controller:

*Constraint 10.*
A shift of a controller consists of three sessions. The duration of each session is 1 hour. After each session the obligatory break follows, which lasts for 1 hour.
Formally:

∀r1:CONTROLLER ∀a1:AGENT ∀t1:TIME ∀proc1:PROCESS holds(state(γ, t1, env), is_responsible_for(r1, execution, proc1) ∧ is_instance_of(proc1, control_region) ∧ agent_allocated(ag1, r1)) ⇒
[ holds(state(γ, t1+3600, env), agent_released_from(ag1, r1)) ∧
[sum([t2: TIME], case(holds(state(γ, t2, env), agent_allocated(ag1, r1)), 1, 0) < 10800 ⇒ holds(state(γ, t1+7200, env), agent_allocated(ag1, r1)) ] ]

*Constraint 11.*
A controller may guide maximum five aircrafts at the same time.

*Constraint 12.*
A controller is not allowed to issue any new clearances for some runway until this runway is vacated by the aircraft that had received the last clearance from the controller.

*Constraint 13.*
As soon as a runway is vacated and some aircraft(s) is (are) waiting for the clearance for this runway, the controller responsible for the runway should provide a clearance to one of the waiting aircrafts.

*Constraint 14.*
If a controller cannot reach an aircraft taxiing in the sector for which this controller is responsible, s/he should contact the controller of the sector from which the aircraft came.

*Constraint 15.*
Each observed incident/accident should be reported by a controller.

One of the constraints for the tower controllers supervisor is the following:

*Constraint 16.*

Perform the allocation of agents-controllers to the aircraft monitoring processes in such a way that the number of processes executed at the same time by each controller is less than six.

Several constraints describe the required common allocations of agents:

*Constraint 17.*

At any time point one of the roles of type CONTROLLERS_SUPERVISOR should have the common allocation with the role Tower Controllers Supervisor.

Formally:

∀γ:TRACE ∀t1:TIME ∃ag1: AGENT ∃r1: CONTROLLERS_SUPERVISOR holds(state(γ, t1, env), agent_plays_role(ag1, r1) ∧ agent_plays_role(ag1, Tower Controllers Supervisor))

*Constraint 18.*

At any time point the role Aircraft's Controller should have the common allocation with one of the roles of the type CONTROLLER.

*Constraint 19.*

At any time point the role Crew Representative should have the common allocation with one of the roles of the type Pilot.

*Constraint 20.*

At any time point the role Head ODU should have the common allocation with the role Team Member (ODU).

*Constraint 21.*

At any time point the role Head of Controllers should have the common allocation with the role Team Member (CSU).

*Constraint 22.*

At any time point the role Airport design representative of the role NODT should have the common allocation with one of the roles of type Airport Operation Designer.

*Constraint 23.*

At any time point the role ANSP design representative of the role NODT should have the common allocation with one of the roles of type Operation Designer.

Furthermore, one more general constraint for the allocation of agents to any role is defined:

*Constraint 24.*

A prerequisite for the allocation of an agent to a role is the existence of a mapping between the capabilities and traits of the agent and the role requirements.

# Appendix C Model details for informal discussion of occurrences

## C.1 Tasks

Table 26 shows the additional tasks identified in the informal incident reporting path. In contrast with the formal tasks in the organization presented in Table 23 on page 71, no formal prescriptions on the execution of these tasks exist. Tasks 16 to 19 all contribute to the satisfaction of safety-related goals 1.1, 3, 5, 10, 18 (see Table 21 on page 64). Table 27 shows an overview of the resource types used and produced by the tasks.

*Table 26: The tasks of the informal incident reporting path.*

| # | Task | Description | Duration |
|---|---|---|---|
| 16 | Discussion about occurrences | Discussion of occurrences observed during shifts by controllers | Varies for each set of controllers |
| 17 | Decision making about the propagation of identified safety issue(s) to the managerial level | Controllers decide jointly if safety-related issues identified during the discussion should be propagated to the level of management | Min: 1 min<br>Max: 3 min |
| 18 | Consideration of the identified issue(s) at the level of management | The members of OMT and ATCEM consider the issues identified by the controllers | Min: 10 min<br>Max: 1 hour |
| 19 | Decision making about the initiation of the occurrence investigation process based on the identified issue(s) | An occurrence investigation begins when the members of OMT and/or ATCEM believe that the investigation may identify/confirm some safety-related problems | Min: 2 min<br>Max: 5 min |

*Table 27: The relations between the tasks of the informal incident reporting path and the resources.*

| Task | Task uses | Task produces |
|---|---|---|
| 16 | Observations of occurrences of different types by controllers | A possible safety-related issue |
| 17 | A possible safety-related issue | the decision about the propagation of the identified issue to the management |
| 18 | A possible safety-related issue, the concept of the operation related to the issue | the results of the discussion on the identified issue |
| 19 | A possible safety-related issue, the concept of the operation related to the issue | the decision about the beginning of the occurrence investigation |

The processes of the informal incident reporting path are executed as represented by the workflow in Figure 20.

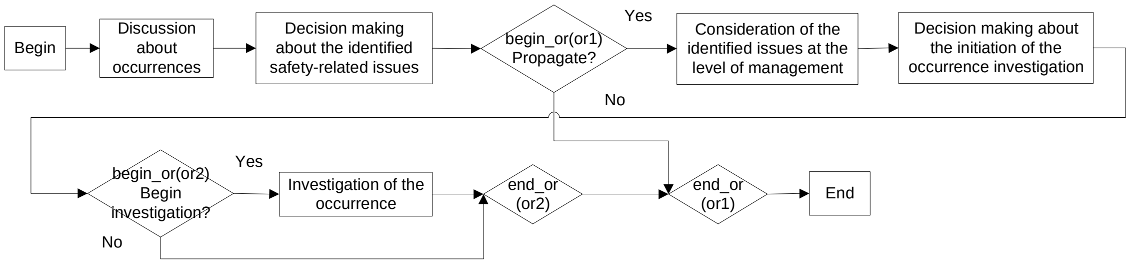


*Figure 20: The workflow for the informal incident reporting path*

## C.2 Authority relations

The authority relations are defined in Table 28 and Table 29. Part of these relations refers to tasks that link with the formal organization, in particular the decision about the beginning of an occurrence investigation is to be made by management layer (OMT and ATCEM roles). Another part of these relations (for tasks 16 and 17) is regulated by informal authority (or influence) relations that exist in the ANSP. In here, the level of influence of an agent-controller plays an important role in the propagation of information about a potential safety problem to the management level of the organization. The employed influence model is presented as part of Appendix C.3.

*Table 28: The responsibility relations of the roles on different aspects of the tasks of the informal incident reporting path and the resources.*

| Task | Execution | Monitoring | Consulting | Technological decisions | Managerial decisions |
|---|---|---|---|---|---|
| 16 | Controllers involved in the discussion (i.e., Participant 1, …, Participant N), Tower Controllers Supervisor | | | | |
| 17 | | | | | |
| 18 | OMT, ATCEM | | | | |
| 19 | | | | | |

*Table 29: The superior-subordinate relations in the informal incident reporting path*

| Subordinate role | Superior role | Task |
|---|---|---|
| OMT | ATCEM | 18, 19 |

## C.3 Agents' performance

The simulations consider 7 agent controllers in the context of the aerodrome operations and incidents that may occur. In Table 30, the assumed aggregated skills and their development levels are presented for the considered agents controllers. All the agents-controllers possess the aggregated air traffic control skill (atc), which allows them to be assigned to role instances of either runway or ground controller roles. For this case study, two interacting role instances of the generic role ground controller are defined at the level of the instantiated role interaction model. Each role instance is responsible for one of the sectors of the aerodrome. Furthermore, each role instance inherits the types of behaviour and relations to other roles defined for the generic role ground controller. Similarly, one role instance of the generic role runway controller is defined that is responsible for the runway investigated in the case study. For investigating different types of occurrences, for each aircraft involved into an occurrence (e.g., incident or accident) a role instance of the generic role crew is introduced. For example, for the occurrence type "Aircraft rejects take-off as result of a runway incursion" two role instances of role crew are introduced: one – for the crew of the aircraft crossing the runway and one – for the crew of the aircraft that takes off. It is assumed that role instances representing the crews of different aircrafts do not interact directly with each other.

The agent ag_controllerG also possesses the skill "employee management", which allows allocating this agent to the role Tower Controllers Supervisor. At the beginning of each day, three controllers are chosen randomly to be allocated to the ground controllers and the runway controller roles.

*Table 30: Agents-controllers considered in the simulation case study.*

| Agent Controller | Skills development level |
|---|---|
| ag_controllerA | atc (2) |
| ag_controllerB | atc (3) |
| ag_controllerC | atc (2) |
| ag_controllerD | atc (4) |
| ag_controllerE | atc (3) |
| ag_controllerF | atc (4) |
| ag_controllerG | employee management(4)<br>atc (4) |

The development level of the skills related to air traffic control forms the basis for influence relations (i.e., informal power). The higher the skill development level of an agent-controller, the more influence this agent has in the ANSP organization. The relations between the skill development levels and the levels of influence assumed in this study are given in Table 31

*Table 31: The correspondence relations between the development levels of the aggregated air traffic management skills and the influence levels.*

| The level of development of the aggregated skill | Influence level |
|---|---|
| atc (2) | 0.3 |
| atc (3) | 0.6 |
| atc (4) | 1 |

**Modelling informal discussions**

Informal incident reporting by agents controllers is performed when a sufficient number of occurrences of some type have been observed and discussed by the agents. The combined influence level of the controllers involved in the discussion about potential safety-relevant issues increases the chance of a positive decision about the propagation of an identified issue by the controllers through the informal path. For this the motivation model introduced in (Sharpanskykh 2007b) is used, which is shown in Figure 21.

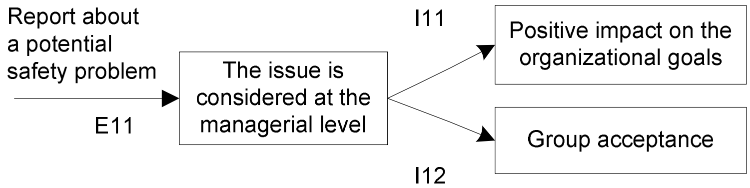


*Figure 21: The motivation model of a representative of a group of controllers for reporting about a potential safety problem*

The motivation force to report about a possible problem is determined using follwoing general motivation model from (Vroom, 1964):

$$F_i = f\left(\sum_{j=1}^{n} E_{ij} \times V_j\right), \quad V_j = \sum_{k=1}^{m} V_{jk} \times I_{jk}$$

Here, $E_{ij}$ is the strength of the expectancy that act i will be followed by outcome j; $V_j$ is the valence of first-level outcome j; $V_{jk}$ is the valence of second-level outcome k that follows first-level outcome j; $I_{jk}$ is perceived instrumentality of outcome j for the attainment of outcome k.

In the air traffic model, two instrumentalities I11 and I12 are considered to be high (=0.9), as the controllers involved in the discussion believe that the identified safety related issue will contribute to the satisfaction of the organizational safety-related goals (i.e., goals 1.1, 3, 5, 10, 18, 24) and that they will be acknowledged for that (i.e., goal 24). Both second-order outcomes (positive impact on the organizational goals and group acceptance) have a high level of priority for the controllers (valence value = 1).

Expectancy E11 is proportional to the influence levels of the controllers in the discussion as well as to the quotient of the number of occurrences required for the investigation and the number of occurrences observed by the controllers involved in the discussion so far:

$$E11(occur\_type, CD) = ac(occur\_type) \times \sum_{C_i \in CD} influence\_level(C_i),$$

where CD is the set of the controllers involved in the discussion and ac(occur_type) is defined as:

$$ac(occur\_type) = \begin{cases} 1, & N(occur\_type) \leq N(occur\_type)_{curr} \\ \dfrac{N(occur\_type)_{curr}}{N(occur\_type)}, & N(occur\_type) > N(occur\_type)_{curr} \end{cases}$$

with N(occur_type) the number of occurrences of the type occur_type required for the investigation and $N(occur\_type)_{curr}$ the number of occurrences of the type occur_type observed by the controllers involved in the discussion so far.

Thus, the motivation force to report about a possible problem based on the observations of events of type occur_type is F(occur_type, CD) = 1.8* E11(occur_type, CD). If F(occur_type, CD) > 1.8, the problem will be reported to the Head of Controllers by a controller representative (e.g., the controller with the highest influence level) of the group of the controllers involved into the discussion. After that, the problem will be discussed at the nearest OMT meeting. In the model it is assumed that this discussion will always result in a detailed investigation of the problem.

### C.4 Constraints

The formally defined work regulations for controllers are determined by the constraints 10-16 from Section 3. A number of additional constraints are imposed on the allocation of agents to the roles in the informal incident reporting:

*Constraints 25.* The same agent should be allocated to both Information Recipient and Head of Controllers roles.

*Constraints 26.* The same agent should be allocated to both Influential Participant and Problem Informant role.

*Constraints 27.* The agent-controller that has the highest influence level among the agents allocated to the subroles of the Discussion role should be also allocated to Influential Participant role.