Safety modelling and analysis of organizational processes in air traffic

Sybert H. Stroeve, Alexei Sharpanskykh, Henk A.P. Blom

***Abstract*— This paper presents the results of the first year 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, leading to identification of promising approaches, and application of the most viable approach to an air traffic case on safety occurrence reporting. 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.**

***Index Terms*—Safety, Organization, Air Traffic, Modelling**

I. 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 crucial 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 [1] illustrates that accidents may occur if multiple holes, reflecting active failures and latent conditions in an organization, are aligned. Early ideas about the evolution of accidents in complex sociotechnical systems have also been put forward by Turner [2] and Perrow [3].

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 [4]-[10]. Limitations of frequently applied accident models as fault/event trees include the difficulty to represent the large number of dynamic, non-linear 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 views indicate that we need analysis approaches that account

Manuscript received 15 November 2007. This work was supported by the EUROCONTROL CARE Innovative III project.

S.H. Stroeve is with the Air Traffic Safety Institute of National Aerospace Laboratory NLR, Amsterdam, The Netherlands; e-mail: stroeve@nlr-atsi.nl.

A. Sharpanskyks is with the Agent Systems Research Group of Vrije Universiteit, Amsterdam, The Netherlands; e-mail: sharp@few.vu.nl.

H.A.P. Blom is with the Air Traffic Safety Institute of National Aerospace Laboratory NLR, Amsterdam, The Netherlands; e-mail: blom@nlr-atsi.nl.

for the variability in the performance of interacting organizational entities and the emergence of safety occurrences from this variability. In the terminology of Hollnagel [4] 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 year 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. This paper describes both aspects of the first year. Section 2 provides an overview of approaches identified in the literature and our view how these can be used for systemic accident modelling of organizational structures and processes. Section 3 introduces an air traffic case for safety occurrence reporting and describes the development of an organizational model for this case. Section 4 presents the kinds of results that are obtained by the organizational modelling approach. Section 5 provides a discussion. Section 6 presents ideas for future research.

II. Literature Survey on Modelling of Organizational Safety

As a basis for the research on safety modelling and analysis of organizational processes, a wide-scope literature survey has been done [11]. This survey considers a variety of sources and viewpoints, which are presented in the following list.

- *Accident models*, describing views and models for accident causation in an organizational context. These models include sequential, epidemiological and systemic accident models.
- *Human performance and human error*, describing human performance in an operational context and the effect of its variability on the evolution of safety-relevant events. There exists a large volume of research on human factors and its relation to safe operations. Historically, there has been a considerable emphasis on human error and its analysis in sequential and epidemiological accident models. In systemic accident modelling the focus is not on human error as such, rather the effects of variability in human performance are analysed for the role of the human in the organization.
- *Organizational and safety culture*, describing culture in an organization and its effect on safety. These aspects can be seen as conceptional reflections on the variability in work processes, i.e. as moderators of the variability in the human performance. In other words, they reflect the impact on “the way we do things around here”, which is an informal, behaviour focused notion of organizational culture [12].
- *Multi-agent models*, describing models of agents and their interactions for the representation of emergent behaviour in complex multi-agent systems.
- *Organization theory*, describing views on structures and dynamics of human organizations using methods from a wide variety of disciplines as economics, psychology, sociology, political science, anthropology, and system theory; related practical disciplines include human resources and industrial and organizational psychology.
- *Enterprise architectures*, describing enterprise-wide, integrating modelling frameworks used to represent and manage business processes, information systems and personnel.

The first three aspects considered in above list belong to the core of safety science and are well known by researchers in ATM safety. The last three aspects are less well known and consider descriptions of formal structures and relations in organizations, as well as multi-agent models to evaluate complex dynamic interactions of organizational entities. These latter aspects will be further worked upon in this paper.

Multi-agent models

Within our systemic accident modelling view for organizational processes, multi-agent modelling plays a key role between a formal description of the structure and relations of an organization, on the one hand, and the stochastic dynamics of interacting organizational agents, on the other hand. Here, incidents and accidents can be considered as emergent phenomena from the variability of the agents’ performance in the organizational context. In agent-based modelling the following aspects are relevant: agents, environment, organization and implementation (see Figure 1).

- An agent is generally defined as an active object with the ability to perceive, reason and act. To this end, agents may have intrinsic models addressing the agent’s internal representations of the external world (e.g. memory or belief states), motivational and intentional attitudes (e.g. wishes, desires, intentions, goals) and mechanisms for reasoning about its intrinsic states and evaluation of possible behavioural strategies for the future. Agents may interact with other agents, e.g. via collaboration or competition.

- The environment of an agent may include both passive and active entities (other agents). Here, agents act in and receive information from.
- The multi-agent organization specifies the structure and protocols of interactions between agents. These structures may be intentionally designed or they may emerge from repeated patterns of interactions among agents. Organizational structures include hierarchies, holarchies, coalitions, teams, congregations and federations. Depending on the type of an organizational structure, agents are provided different degrees of autonomy at various aggregation levels of the organizational structure.
- An agent-based modelling approach may be supported by a software implementation.

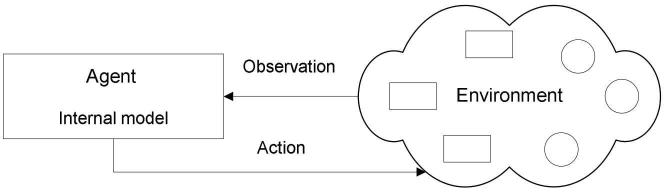

Figure 1: The classical model of an agent situated in the environment, which includes other agents and passive objects.

As part of the literature review [11], an evaluation of a number of multi-agent design methodologies has been done regarding above multi-agent system characteristics. Table 1 shows the main results of this evaluation; more details can be found in [11]. It follows from this evaluation that the organizational modelling framework of [13] presents the widest repertoire of relevant aspects for multi-agent modelling of organizations. Therefore this framework has been chosen to study the possibilities of organizational modelling in the air traffic safety context of this paper.

Table 1. Summary of characteristics for multi-agent system methodologies. A '+' denotes that a characteristic is addressed in the methodology, '-' denotes that a characteristic is not considered.

Method	Environment	Agents		Organization		Implemen-tation
		Internal models	Inter-action	Structure	Dynamics	
[14]	-	-	+	+	-	-
[15]	-	-	+	+	-	+
[16]	+	-	+	+	+	-
[17]	-	+	+	+	-	+
[18]	-	+	+	+	+	+
[19]	+	+	+	-	-	+
[13]	+	+	+	+	+	+

Organizational modelling framework

The foundation of the performance of agents within an organization is specified by the formal organization. This encompasses a definition of the hierarchical structures, interactions, procedures, regulations, goals and performance indicators of the organization as formally described. In other words, it describes the organization as it should be according to its formal definitions. The formal organization can be specified at different aggregation levels, ranging from general regulations for the whole organization to specific prescriptions for particular roles and their interaction with other roles that occur in the executions of work processes. Analysis of processes and relations both at the same aggregation level and across different levels may show potentially safety-critical inconsistencies.

The organizational modelling framework of [13] considers the following four interrelated views to formally describe an organization and link it to a description of performance variability of a multi-agent system:

1. The *organization-oriented view* describes a functional decomposition of an organization by a composite structure of roles at various aggregation levels. These roles are abstracted from particular agents that may fulfil them, e.g. business unit, department, manager or operator. The organization-oriented view describes interactions between roles and specifies the authority relations in an organization: superior-subordinate relations on roles with respect to tasks, responsibility relations, authorization relations and control for resources.
2. The *performance-oriented view* describes the goals of the organizational roles in a goal structure of generic and specific goals. It uses performance indicators as measures of goal achievement for organizational roles.
3. The *process-oriented view* describes tasks and processes in the organization. It specifies static and dynamic relations between processes, e.g. decomposition, ordering and synchronization, and the resources used and produced.
4. The *agent-oriented view* describes the link between the role-based formal organizational model and the agents that are to perform the roles. It formulates agents' types, their capabilities, their behaviour, and the principles of allocating agents to roles. The agent-oriented view crosses the description of the formal organization and the description of performance variability. On the one hand, the performance and interactions of agents are regulated by the formal organization. On the other hand, the dynamics and stochastic aspects of interacting agents contribute to the performance variability in an organization.

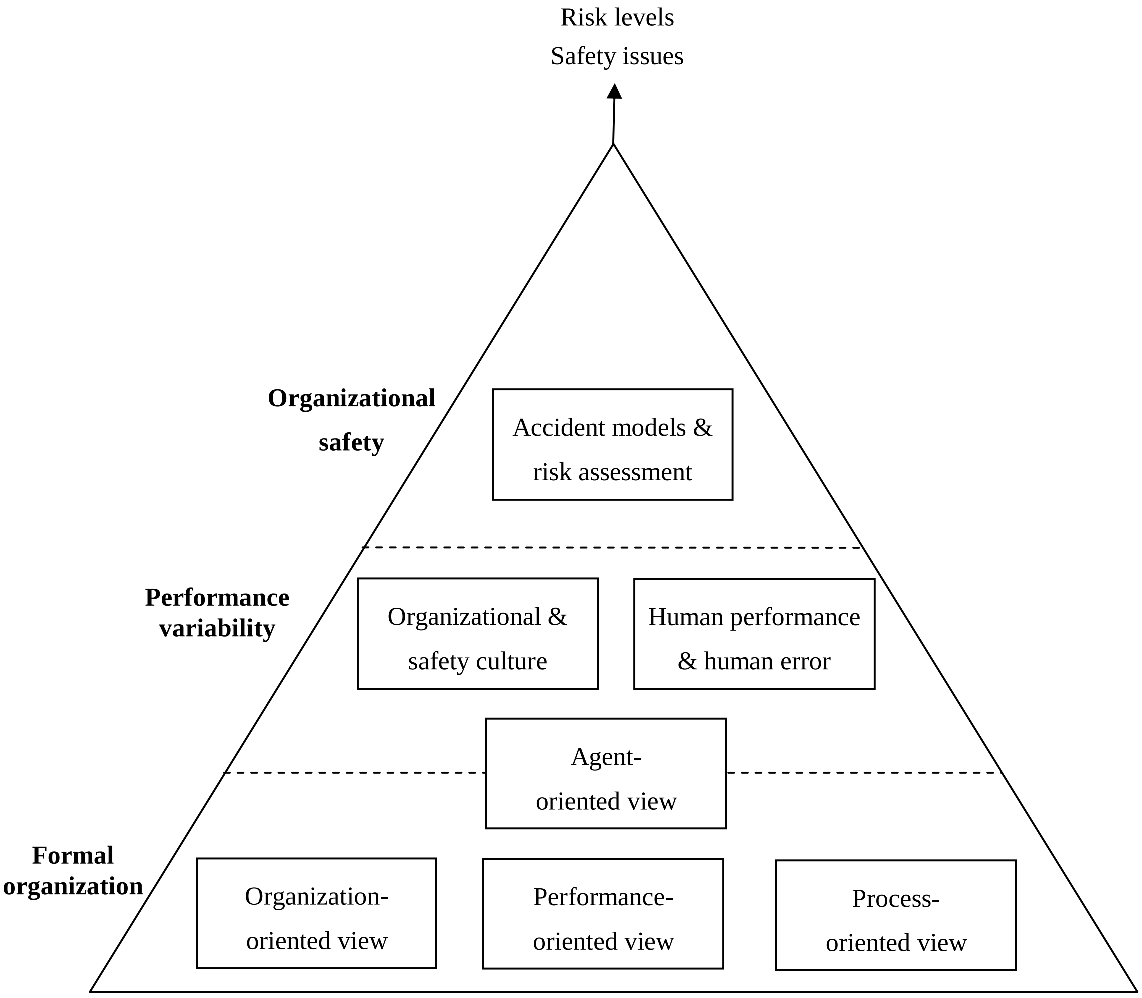

Figure 2: Organizational safety pyramid.

To illustrate the main aspects of an organizational systemic accident model discussed in this section, we use a three-layered organizational safety pyramid shown in Figure 2. It describes the main aspects contributing to safety of organizational processes and the evaluation thereof:

- *Formal organization*, using the organization-, performance- and process-oriented views, as well as the agent-oriented view for the connection to the next level;
- *Performance variability*, describing human performance & error, and the moderating effect of organizational & safety culture;
- *Organizational safety*, describing the result of the various sources of performance variability in the organizational context on the development of safety events.

Although this safety pyramid looks similar to the classical safety pyramid of Heinrich [20], it follows from above explanation that the reasoning behind it is quite different from the relation between unsafe acts, incidents and accidents considered in the classical safety pyramid.

III. ORGANIZATIONAL MODELLING OF AN AIR TRAFFIC CASE

In this section we describe the development of an organizational model according to the four views of [13] for an air traffic case on safety occurrence reporting. First we give a high-level description of the case, subsequently the development of the organizational model is described in a number of steps.

High level description of air traffic case on safety occurrence reporting

We study the possibilities of organizational modelling in air traffic for the case of reporting and management of safety occurrences during taxiing operations near an active runway of a fictitious major 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 a runway controller and ground controllers, respectively. In this operational context safety-relevant events may occur, e.g. ‘taxiing aircraft makes a wrong turn and progresses towards the runway crossing’, ‘taxiing aircraft has switched to a wrong frequency' or 'taxiing aircraft initiates to cross due to misunderstanding in communication'. To support 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.

Model development steps

The development of the organizational model is done in a number of steps specified in Table 2. Steps 1 to 9 are performed subsequently and contribute to one view or the combination of two views. Step 10 may be done after a particular step or after a combination of steps, depending on the type of constraint considered. In all steps, first-order sorted predicate logic serves as a formal basis for defining dedicated modelling languages [21] and temporal relations are specified by the Temporal Trace Language [22].

Table 2: 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	Specification of interactions between roles and with the environment	x			
3	Identification of requirements for roles	x			x
4	Identification of organizational performance indicators and goals		x		
5	Specification of resources			x	
6	Identification of organizational tasks and relations between tasks, resources and goals		x	x	
7	Specification of authority relations	x		x	
8	Specification of flows of control			x	
9	Specification of allocation, characteristics and behaviour of agents				x
10	Identification of generic and domain-specific organizational constraints	x	x	x	x

Step 1: Identification of organizational roles

In this step, organizational roles are identified. 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; a role that is composed of (interacting) subroles is a composite role. At the highest aggregation level, the whole organization can be represented as one role. The refined role structures may correspond to organizational constructs such as groups, units, departments, managers, operators, etc. Since roles are represented by a composite structure, interactions between roles can be represented at different levels of abstraction.

For the air traffic case, the roles Air Navigation Service Provider (ANSP), Airport, Airline, Regulator and New Operation Design team are considered at the highest aggregation level (see also Figure 3). The composition of these roles is considered up to two additional aggregation levels. Aggregation level 2 consists of 16 roles that mostly refer to units and teams in the organization (see Figure 4 for the level-2 roles in the ANSP). Aggregation level 3 consists of 22 roles at the level of single humans (see Figure 5 for some examples of level-3 roles in the ANSP).

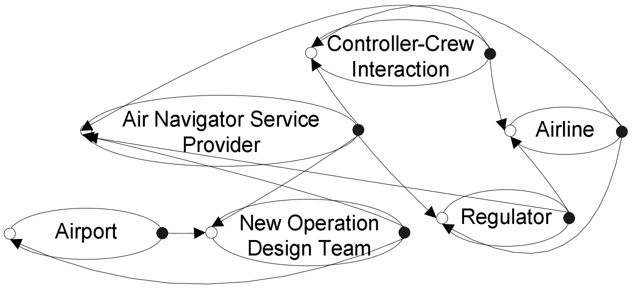

Figure 3: The interaction relations between the generic roles at aggregation level 1

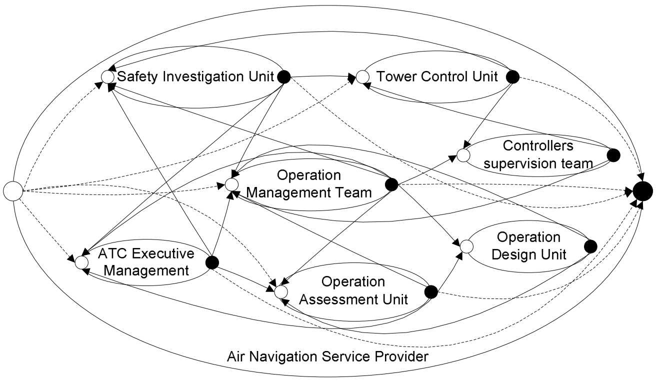

Figure 4: The interaction relations between the subroles of the role Air Nativation Service Provider at aggregation level 2

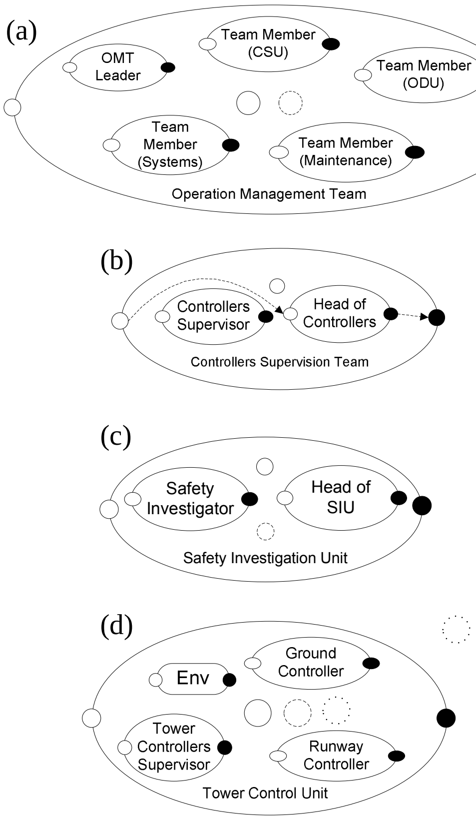

Figure 5: Examples of interaction relations between the subroles of the ANSP at aggregation level 3: (a) Operation Management Team, (b) Controllers Supervision Team, (c) Safety Investigation Unit, (d) Tower Control Unit.

Step 2: Specification of interactions between roles and with the environment

In this step, interaction relations between roles and with the environment are identified. Furthermore, the vocabulary of interactions (interaction ontology) is defined. Together with Step 1, it contributes to the organization-oriented view.

For the air traffic organizational model, relations between roles exist 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 3. Subroles of the role ANSP are depicted at aggregation level 2 in Figure 4 and at aggregation level in Figure 5. Relations between roles at the same aggregation level are represented by interaction links, relations between composite roles and subroles are represented by interlevel links.

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 organization-oriented and the agent-oriented views.

For each role, requirements on knowledge, skills and personal traits of the agent implementing the role are defined.

- Knowledge-related requirements 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. Four types of generic skills are distinguished that are relevant in an organizational context [23]: 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). Requirements on skills can be defined that reflect their level of development, experience and the context in which these skills were attained.
- Personal traits may influence the successfulness of task execution. The traits are divided into five broad categories [24]: openness to experience, conscientiousness, extroversion, agreeableness and neuroticism.

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 performance-oriented and organization-oriented views.

A goal is characterized by the following aspects: name, priority (high, medium, low, etc.), horizon (time interval in which the goal is supposed to be satisfied), ownership (role, agent), perspective (point of view described by the goal, e.g. management, supplier, etc.), hardness (clearness of satisfaction of a goal, i.e. hard or soft), and negotiability (whether negotiation is possible in case of conflicts with other goals).

Goals can be refined in goal structure, which defines relations between goals and sub-goals, expressing rules for goal satisfaction. For instance, in the partial goal structure of the air traffic organizational model shown in Figure 6, goal 3 “It is required to achieve a high level of quality of the internal investigation of a new operation” requires sufficient fulfilment of sub-goals 3.1 “It is required to achieve a high level of thoroughness of the internal investigation of a new operation”, sub-goal 3.2 “It is required to maintain a high professional level of operation analysts” and sub-goal 3.3 “It is required to maintain up-to-date knowledge of norms, standards and statistics used for the evaluation of a new operation”, and goal 3 is supported by 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”. The developed air traffic organizational model contains 21 goals and 60 sub-goals.

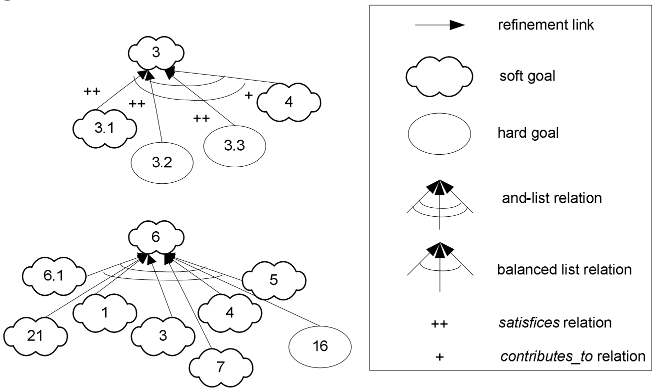

Figure 6: Part of the goal structure in the air traffic organizational model.

Performance indicators are goal-associated quantitative or qualitative expressions of the state/progress of a role or agent. Performance indicators can be soft or hard. A soft performance indicator is difficult to measure directly and is 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. A number of relations can be defined between performance indicators: causal, correlation and aggregation. Figure 7 shows graphical representation of the relations between performance indicators in the air traffic organizational model. Here, examples of the types of relations are:

- Causality – indicator 1.1 “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 indicator 2 “The level of safety of a new implemented operation”;
- Correlation – indicator 9 “The development and assessment time of a new operation” correlate positively with indicator 3 “The level of quality of the internal investigation of a new operation”;
- Aggregation – indicator 9 “The development and assessment time of a new operation” is an aggregation of indicator 9.2 “The development time of the concept of a new operation”.

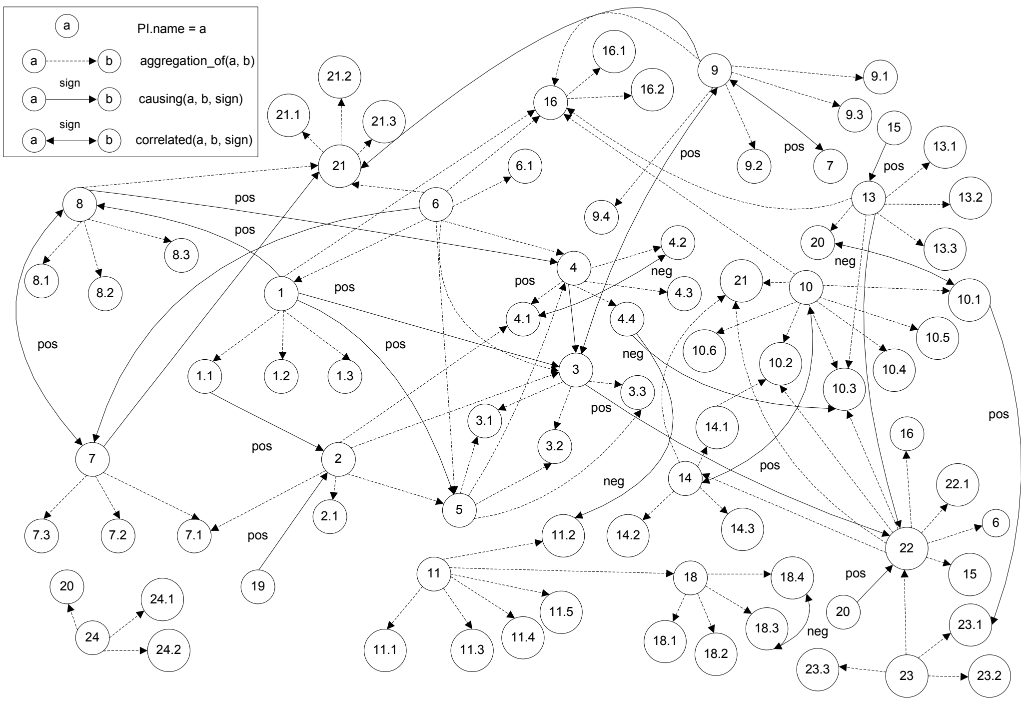

Figure 7: Relations between the performance indicators in the air traffic organizational model.

Step 5: Specification of resources

In this step organizational resources are defined. Resources describe a wide range of materials and data, such as tools, supplies, components and digital artefacts. Resources are characterized by name, category (discrete/continuous), measurement unit, expiration duration and amount. This step is part of the process-oriented view.

Examples of resources in the air traffic case are aircraft, radar system, incident database, incident investigation report and R/T system.

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

This step identifies organizational tasks, their characteristics and relations, 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 organization and is characterized by a name and by minimum and maximum durations. 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. For every task it is indicated to which organizational goals they contribute. For every task it is indicated which kinds and quantities of resources it uses, consumes and produces.

The model contains 15 general tasks and 26 specific tasks. Examples of tasks in the air traffic case are: creation of a notification report, preliminary processing of a notification report, making decision about the investigation necessity based on the provided notification report, investigation of the occurrence based on the notification report.

Step 7: Specification of authority relations

In this step authority relations (formal power relations) of an organization are identified: superior-subordinate relations on roles with respect to tasks, responsibility relations, control for resources, authorization relations. Authorization and responsibility relations are defined with respect to task execution, task monitoring, consulting, technological decision-making and managerial decision-making.

In the model responsibilities are defined for all tasks. For example, the following responsibilities of roles are defined with respect to the task “Investigation of the occurrence based on the notification report”: for task execution and technological decisions the Safety Investigator is responsible, for monitoring, consulting and managerial decisions the Head Safety Investigation Unit is responsible.

Step 8: Specification of 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 organization in particular scenarios. Figure 8 shows an example of the workflow for the processing of incident reporting by a controller.

Step 9: Specification of allocation, characteristics and behaviour of agents

In the context of organizational modelling, the performance variability in an organization is the result of the behaviour of agents that are allocated to organizational roles. In Step 9, the characteristics and behaviour of agents allocated to organizational roles are described. The characteristics describe knowledge, skills, personal traits and internal goals of the agents.

In the context of the air traffic case, the following types of agents are defined: Controller, Controller Manager, Pilot, Regulator, Safety Investigator, and Manager. For example, the agent type Controller may have the following characteristics: decision-making skills, passed a rigid medical examination, number of years of college education before initiation of ATC training, knowledge of the air traffic management system and flight regulations, number of hours of computer training, number of hours of air traffic control training, listening and communication skills, ability to stand stress, and short-term memory capabilities. By assigning different values to the identified characteristics different instances of the agent type Controller can be specified.

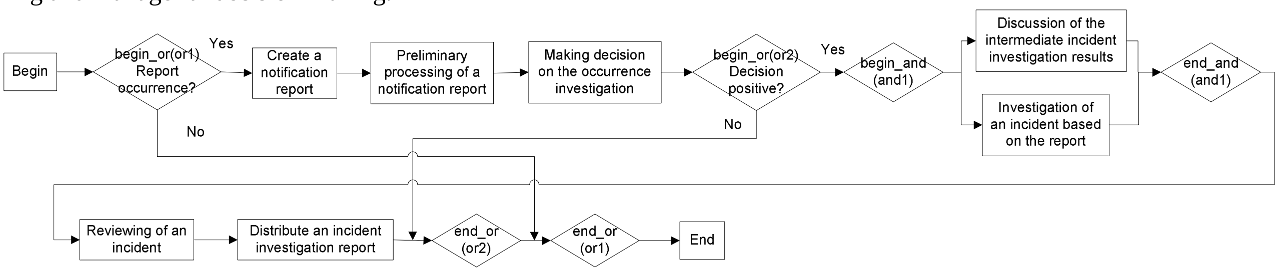

Figure 8: Workflow for management of controller incident reporting.

The behaviour of agents is considered to be goal-driven. In the case study the agents' goals are consistent with the organizational goals. 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:

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

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

Step 10: Identification of generic and domain-specific organizational constraints

Within every view and across views of the organizational modelling framework, a set of structural and behavioural constraints can be defined (see Figure 9). 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. 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. Generic constraints can be structural integrity and consistency constraints based on the specification rules of the composition, or constraints imposed by the physical world.
2. Domain-specific constraints are imposed by the organization, external parties or the physical world of the specific application domain.

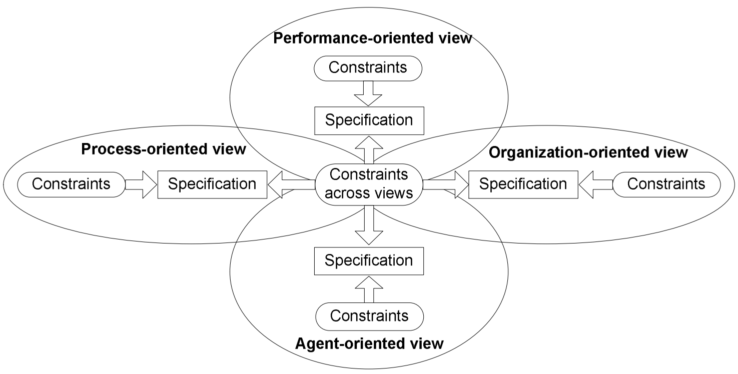

Figure 9: Constraints in the organizational modelling framework.

Examples of constraints in the various views for the air traffic case are:

- Generic structural integrity constraint in the performance-oriented view: "If performance indicator A causes a positive change of indicator B, and indicator B causes a positive change of indicator C, then indicator A causes a positive change of indicator C".
- Generic constraint in the process-oriented view: "Not consumed resources become available after all processes are finished".
- Domain specific constraint in the process-oriented view: "Each active runway should not be used by more than one aircraft at the same time".
- Generic constraint in the organization-oriented view: "Each role may be a subrole of one complex role at most".
- Domain specific constraint in the organization-oriented view: "The pilots of the crew should verbally share relevant information with each other".
- Generic constraint in the agent-oriented view: "To be allocated to a role, an agent should possess all the required knowledge and the development levels of skills, and the required traits".
- Domain specific constraint over combined process-oriented, organization-oriented and agent-oriented views: "Each observed incident/accident should be reported by a controller".

IV. Organizational analysis results

For analysis of the developed organizational model two types of techniques can be applied [13]:

1. Checking the consistency and correctness of organization models. This analysis type focuses on verification of the model specification for the particular views. 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. For this analysis, techniques based on first-order sorted predicate logic are used.
2. Verification by simulation. The second type addresses the validation of constraints on single or combined specifications of different views by simulations. In such simulations, agents are allocated to particular organizational roles.

Next, the types of results that can be achieved by these analysis techniques are presented for the four organizational modelling views.

Organization-oriented view

The organization-oriented view identifies sets of generic consistency constraints on both interaction structures of roles [25] and on formal authority relations [26] between roles. Examples of possible conflicts on interaction relations between roles include:

- Roles involved in the execution of a task do not interact (may be a problem when they need to interact).
- A communication path does not exist at all when it should exist.
- The role which supervises the execution of some process should interact with the role performing the process.

Examples of possible conflicts on authority relations between roles include:

- A role has more than two direct superior roles (at the same level of the authority hierarchy); this 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 does not 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 acts as if the responsibility is still provided.

Performance-oriented view

For analysis of the performance-oriented, view consistency checks can be performed for the goal and performance indicator structures [27]. For example, goal 3 “It is required to achieve a high level of quality of the internal investigation of a new operation” and goal 9 “It is required to minimize the development and assessment time of a new operation” are in conflict. This conflict has been detected since the corresponding performance indicators “Quality of the internal investigation of a new operation” and “Development and assessment time of a new operation” are related by a positive causality relation, and the corresponding goal patterns are based on opposite types of functions to either maximize or minimize the performance indicator.

Process-oriented view

In the process-oriented view structural consistency constraints are defined for workflow, task and resource hierarchies [28]. Automated algorithms are available for the verification of these constraints on process-oriented specifications.

The verification of the correctness of a specification is performed during or at the end of the design process, depending on the type of constraint. Some domain-specific constraints might not (yet) be satisfied for incomplete specifications. The designer can choose when they should be checked. The syntactical check of a specification and the verification of generic constraints are performed at each design step.

Examples of types of inconsistencies that can be identified by these techniques are:

- A process is not finished before a dependent process has commenced.
- Processes try to share a non-sharable resource (e.g. a runway).
- A resource is located at a non-accessible place.
- A pilot is assigned to multiple simultaneous flights.
- Particular information types may not be used by tasks (security/privacy).

Agent-oriented view

In the agent-oriented view, the dynamic interactions of agents allocated to the roles in the organization are evaluated in varying contextual conditions. For the air traffic case described in Section 3, simulation models have been developed for the formal and informal reporting of incidents during taxiing operations [29]. These simulation models represent the behaviour of agents for the roles considered (e.g. controllers, pilots, safety investigator) in the context of six types of safety occurrences that may happen during taxiing. The events considered are:

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.

In the model, the formal and informal handling of these events may lead to a start of a safety investigation and thereby to the identification of safety-critical aspects in the operation. In both the formal and informal approaches, the severity of the event has impact on the decision to initiate an investigation; in particular, less severe events require more occurrences.

Table 3: Results of the agent-based simulations.

Event	Fraction of traces with start of investigation given the event type		Mean time before start of safety investigation (days)	
	Formal	Informal	Formal	Informal
a	22%	21%	155	135
b	5%	15%	168	124
c	28%	50%	195	150
d	0%	0%	-	-
e	0%	3%	-	279
f	45%	11%	186	185
total	100%	100%	181	150

For the formal and informal cases, 100 simulations have been performed with 12 operational hours per day and a maximum simulation time of 3 years. Main results of these simulations are shown in Table 3. The results shown are the fractions of cases in which an investigation is initiated given a sufficient number of occurrences of a particular event and the mean time until start of the investigation. 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. A main reason underlying this difference is that events like *b* and *c* 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.

V. Discussion

In this paper 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 [13]. 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 perform the roles. The performance of the agents is determined by the formal organization, but it is 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 [11], 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 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. The presented results show various forms of inconsistencies and 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.

VI. Future research

The study presented in this paper 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. Next year's research can be organized along the steps in the original project planning [30].

The identification of objectives for further organizational modelling is done in WP3 'Identification of application and analysis objectives'. The identification of objectives for organizational modelling will be based on 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. To assure a sufficient knowledge base we will consider in

WP3 what issues should be considered in the air traffic case for the advanced organizational model.

In WP4 'Organizational safety model & simulation of advanced air traffic application' the advanced organizational model will be developed in the context set. Building forward on the results achieved, more specific knowledge will be integrated in the organizational model. Model analysis and simulation results will be achieved for the advanced organizational model.

VII. Publications in the Project

The first year of research has resulted in reports [11][29] and a research paper published at the EUROCONTROL Safety R&D Seminar 2007 [31]. The project has contributed to the PhD research of Alexei Sharpanskykh and associated research papers [13][26][28][32][33][34].

Acknowledgement

We would like to thank Barry Kirwan for stimulating comments and discussions.

References

[1] Reason J. Managing the risk of organizational accidents. Ashgate, Aldershot, England, 1997
[2] Turner BA. Man-made disasters. Wykeham Science Press, London, UK, 1978
[3] Perrow C. Normal accidents: Living with high-risk technologies. Basic Books, New York, USA, 1984
[4] Hollnagel E. Barriers and accident prevention. Ashgate, Aldershot, England, 2004
[5] Leveson N. A new accident model for engineering safer systems. Safety Science 42:237-270, 2004
[6] Sträter O. Cognition and safety: An integrated approach to system design and assessment. Ashgate, Aldershot, England, 2005
[7] Hollnagel E, Woods DD, Leveson N (eds.). Resilience engineering: Concepts and precepts. Ashgate, Aldershot, England, 2006
[8] Le Coze J. Are organizations too complex to be integrated in technical risk assessment and current safety auditing? Safety Science 43:613-638, 2005
[9] Reason J, Hollnagel E, Paries J. Revisiting the Swiss cheese model of accidents. Eurocontrol, EEC Note no. 13/06, 2006
[10] Blom HAP, Bakker GJ, Blanker PJG, Daams J, Everdij MHC, Klompstra MB. Accident risk assessment for advanced air traffic management. In: Donohue GL and Zellweger AG (eds.), Air Transport Systems Engineering, AIAA, pp. 463-480, 2001
[11] Stroeve SH, Sharpanskykh A, Blom HAP. Literature survey of safety modelling and analysis of organizational processes: Eurocontrol CARE Innovative research III. National Aerospace Laboratory NLR, report CR-2007-156, 2007
[12] Hopkins A. Studying organizational cultures and their effects on safety. Safety Science 44:875-889, 2006
[13] Popova V, Sharpanskykh A. A Formal Framework for Modeling and Analysis of Organizations. In: Ralyte, J., Brinkkemper, S., Henderson-Sellers, B. (eds.), Proceedings of the Situational Method Engineering Conference, ME'07, Springer Verlag, 2007
[14] Zambonelli F, Jennings NR, Wooldridge M. Developing multi-agent systems: the Gaia Methodology, ACM Transactions on Software Engineering and Methodology, vol. 12 (3): 317-370, 2003
[15] Ferber J, Gutknecht O. A meta-model for the analysis and design of organizations in multi-agent systems. In: Proceedings of Third International Conference on Multi-Agent Systems (ICMAS'98), IEEE Computer Society, 128-135, 1998
[16] Omicini, A. (2000). SODA: Societies and infrastructures in the analysis and design of agent-based systems. In: Proceeding of AOSE 2000, 185–193
[17] Hannoun M, Boissier O, Sichman JS, Sayettat C. MOISE: An Organizational Model for Multi-agent Systems. In Proceedings of the International Joint Conference, 7th Ibero-American Conference on AI: Advances in Artificial Intelligence, LNCS, vol. 1952, 156 – 165, 2000
[18] Bresciani P, Giorgini P, Giunchiglia F, Mylopoulos J, Perini A. Tropos: An Agent-Oriented Software Development Methodology, Journal of Autonomous Agent and Multi- Agent Systems, vol. 8(3): 203-236, 2004
[19] Brazier FMT, Dunin-Keplicz B, Jennings N, Treur J. DESIRE: Modelling Multi-Agent Systems in a Compositional Formal Framework. International Journal of Cooperative Information Systems, 6: 67-94, 1997
[20] Heinrich HW. Industrial accident prevention: A scientific approach. McGraw-Hill Book Cie, New York, 1931
[21] Manzano M. Extensions of First Order Logic, Cambridge University Press, 1996
[22] Sharpanskykh A, Treur J. Verifying Interlevel Relations within Multi-Agent Systems. In: G. Brewka, S. Coradeschi, A. Perini, P. Traverso (eds.), Proceedings of the 17th European Conference on Artificial Intelligence, ECAI'06. IOS Press, 290-294, 2006
[23] Pinder CC. Work motivation in organizational behavior. Upper Saddle River, NJ: Prentice-Hall, 1998
[24] Katz D, Kahn R. The social psychology of organizations. Wiley, New York, 1966
[25] Jonker, CM Sharpanskykh A, Treur J, Yolum P. A Framework for Formal Modeling and Analysis of Organizations, Applied Intelligence 27(1): 49-66, 2007
[26] Sharpanskykh A. Authority and its Implementation in Enterprise Information Systems. In: Sadiq, S., Reichert, M., Schulz, K., Trienekens, J., Moller, C., and Kusters, J. (eds.), Proceeding of the 1st International Workshop on Management of Enterprise Information Systems, MEIS 2007, INSTICC Press, 33-43, 2007
[27] Popova V, Sharpanskykh A. Modelling Organizational Performance Indicators. In: Barros, F. et al. (eds.): Proceedings of the International Modeling and Simulation Multiconference IMSM'07, SCS Press, 165-170, 2007
[28] Popova V, Sharpanskykh A. Process-Oriented Organization Modeling and Analysis. In: J.C.Augusto, J. Barjis, U. Ultes-Nitsche (eds.), Proceedings of the 5th International Workshop on Modelling, Simulation, Verification and Validation of Enterprise Information Systems (MSVVEIS 2007), INSTICC Press, 114-126, 2007
[29] Stroeve SH, Sharpanskykh A, Blom HAP. Organizational safety modelling and analysis of an air traffic application: Eurocontrol CARE Innovative research III. National Aerospace Laboratory NLR, report CR-2007-457, 2007
[30] Stroeve SH. Safety modelling and analysis of organizational processes in air traffic: Proposal for Eurocontrol CARE Innovative Research III. National Aerospace Laboratory NLR, memorandum ATSF-2006-102, September 2006
[31] Stroeve SH, Sharpanskykh A, Blom HAP. Systemic safety modelling and analysis of organizational processes in air traffic. EUROCONTROL Safety R&D Seminar, Rome, Italy, 24-26 October 2007
[32] Popova V, Sharpanskykh A. Formal analysis of executions of organizational scenarios based on process-oriented Models. In: F. Barros et al. (eds), Proceedings of 21st European Conference on Modelling and Simulation ECMS 2007, SCS Press, 36-44, 2007.
[33] Sharpanskykh, A. Modeling of Agents in Organizational Context. In: H-D. Burkhard, G. Lindeman, L. Varga, R. Verbrugge (eds.), Proceedings of the 5th International Central and Eastern European Conference on Multi-Agent Systems, LNAI 4696, Springer Verlag, 193-204, 2007.
[34] Sharpanskykh, A. Agent-based Modeling of Human Organizations. In: F.Amblard (ed.), Proceedings of the 4th European Social Simulation Association Conference, 335-347, 2007.