Quantitative Assessment for Organisational Security & Dependability

Yudistira Asnar
University of Trento
Trento, Italy
yudis.asnar@disi.unitn.it

Massimo Felici
Deep Blue S.r.l.
Roma, Italy
massimo.felici@dblue.it

Fabio Massacci
University of Trento
Trento, Italy
fabio.massacci@disi.unitn.it

Alessandra Tedeschi
Deep Blue S.r.l.
Roma, Italy
alessandra.tedeschi@dblue.it

Artsiom Yautsiukhin
University of Trento
Trento, Italy
evtiukhi@disi.unint.it

Abstract

There are numerous metrics proposed to assess security and dependability of technical systems (e.g., number of defects per thousand lines of code). Unfortunately, most of these metrics are too low-level, and lack on capturing high-level system abstractions required for organisation analysis. The analysis essentially enables the organisation to detect and eliminate possible threats by system re-organisations or re-configurations. In other words, it is necessary to assess security and dependability of organisational structures next to implementations and architectures of systems. This paper focuses on metrics suitable for assessing security and dependability aspects of a socio-technical system and supporting decision making in designing processes. We also highlight how these metrics can help in making the system more effective in providing security and dependability by applying socio-technical solutions (i.e., organisation design patterns).

1. Introduction

The design of secure and dependable systems requires a thoughtful analysis of the organisational and the social environments in which systems will operate. This is crucial especially for safety-critical domains, such as the Air Traffic Management (ATM) domain, that have to comply with stringent Security and Dependability (S&D) requirements [19]. In such domains, failures increase the risk of exposure for people and the environment. Research in requirements engineering stresses the importance of analysing S&D issues in the early phases and throughout the software development [10], [21]. Design patterns capturing organisational aspects support modelling and analysis of S&D issues arising in socio-technical settings. S&D patterns at the organisational level involve agents whose behaviour needs to be specified, constrained, predicted and guaranteed. Hence, it is necessary to support the deployment of S&D organisational patterns [26] by quantitative assessment of their impact, that is, how they affect S&D properties required at the organisational level. Therefore, there is a strong need for quantitative assessment of systems and their underlying design patterns in order to support monitoring and decision-making processes. Though there have been many proposals for metrics suitable for analysis of security and dependability at the technical level [16], [17]. However, there is yet little experience on metrics that focus on S&D *organisational* aspects.

This paper discusses metrics that can be used to estimate the level of protection (e.g., S&D properties) in organisations that rely on technical systems, that is, metrics that allow the analysis of properties related to organisational patterns. The work was conducted within the SERENITY project [2]. One of the industrial case studies used within the project was drawn from the Air Traffic Management (ATM) domain. The industrial scenarios supported the evaluation of a prototype adopting and implementing S&D organisational patterns tailored to specific domain requirements (e.g., compliance with ATM work practices). A quantitative account of the ATM scenario highlights how S&D patterns relate to and support organisational strategies that involve different artifacts. This stresses a relationship between quantitative observable organisational aspects (e.g., strategies, activities, uncertain events, etc.) and S&D patterns.

This paper is structured as follows. Section 2 briefly describes the ATM case study. Section 3 shows how a system can be modelled on organisational level and which concepts can be used for such modelling. Section 4 gives detailed description of metrics suitable for assessment of systems on organisational level. Section 5 presents our experience of using the metrics in a context of the case study. Section 6 discusses related work and draw some concluding remarks in Section 7.

2. The ATM Case Study

Air Traffic Management (ATM) system provides a set of ground-based services, such as giving air traffic instructions, air traffic planning and airspace management. These services

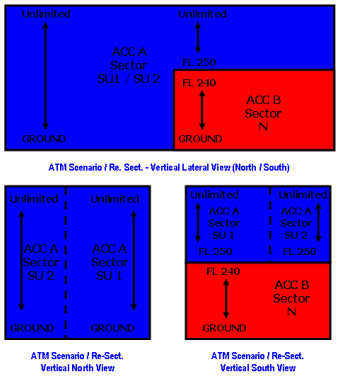

Figure 1. Different sectors' configurations

are performed by Air Traffic Controllers (ATCOs) that are orgnized into Airport Control Towers for the arrival and departure flight phases and Area Control Centres (ACCs) for the en-route flight phase. The airspace managed by an ACC is organised into several adjacent sectors with a predefined capacity (i.e., number of flights that can be managed safely) and operated by a team of two ATCOs: a Planning Controller (PC) and an Executive Controller (EC). They work together as a team and share the responsibility for safe operations of the sector. ECs monitor aircrafts in their sector and provide pilots with instructions. PCs assist ECs by arranging incoming traffic, coordinating entry exit flight-point and altitude with adjacent sectors. They also monitor the (incoming) traffic within their sector. Groups of neighbouring sectors are coordinated by a supervisor who is also responsible to define sectors configuration. Supervisors monitor, assist, and, if needed, temporarily take over the roles of ATCOs. Occasionally, air traffic may increase unexpectedly and then a number of measures needs to be put in place. Such measures may include cooperation between individuals or between organisations as such mediated by supervisors as their representatives. The ATM scenario involves an unexpected threat that requires subsequent re-sectorisations and a partial delegation of airspace in order to guarantee safety and performance. Figure 1 shows the different sectors' configurations.

The ATM scenario highlights useful information in order to design, develop and deliver a decision support system, which implements S&D patterns [26] as reaction mechanisms into the specific industry domain [7]. It provides examples of organisational patterns within the ATM domain. In particular, it describes how general organisational patterns have been recognised within the ATM scenario. Table 1 shows some examples of organisational patterns, which concern the ATM scenario.

Table 1. Examples of organisational patterns

Pattern Name	Pattern Description
Public Artefact	Shared resources are used to share information among several agents that carry on similar or related tasks.
Reinforcing Overlapping Responsibilities	Agents share the responsibility for achieving safety-critical tasks.
Artefact generation as an audit trail	There is the need to share information, keep track of modification and promoting non-repudiation.
Collaboration in Small Groups	complex activities critically require tight coordination among workers.
Multiple Representations of Information	Workers need to access the same information to achieve different results or to perform different, though related each other, activities.
Doing a Walkabout	Checking directly what is going on is important and strategic.

3. Modelling Organisational Structures

A socio-technical system from an organisational viewpoint is seen as a set of interacting agents (e.g., organisations, humans and systems). Each of them is in charge of a set of goals that must be accomplished whatever happens in the environment [4], [11]. At this level of modelling abstraction, it is useful to capture what is needed in order to achieve a specific goal: permissions, allocation of tasks or resources, execution dependencies and trust relations among actors. In order to describe organisation structures, we use SI* [11] which has a formal semantics based on either Datalog instances or satisfiability with mathematical decision procedures over the reals. Figure 2 summarises the main formal concepts (which have also a graphical notation) of SI*. Other methodologies, e.g., KAOS [25], similarly capture these concepts. This work is then relevant for other goal-driven methods – not just for SI*.

- A *goal* represents some strategic interests while a *task* is a specific process for satisfying a goal. A *softgoal* represents a qualitative objective.
- An *actor* models a generic entity with strategic goals, which can be either a *role* or an instance denoted as an *agent*
- The *execution dependency* (DE) relations indicates that one actor depends on the other in order to execute some tasks or use a resource (because of direct or indirect delegation).
- The relation *delegation of permission* (DP) transfer permissions between actors
- the *Trust relationship* between two actors indicates that one actor believes that the other will satisfy a goal, execute a task or deliver or a resource.
- *Event* is a positive or negative occurrence which may happen at some point of time.

Figure 2. Basic organisational concepts

The SI* tool[1] provides the possibility of checking whether a specific property is violated and selecting a pattern which

1. http://sesa.dit.unitn.it/sistar_tool/

can solve the problem. Unfortunately, simple model checking is not enough in the real situation. In fact, the assessment of most properties cannot be simply reduced to satisfaction problems (i.e., whether properties hold or not). Hence, quantitative assessment supports empirical analysis that highlight *how well* systems fulfil required S&D properties. Metrics allow us to assess whether the system and any relevant organisational patterns provide the required S&D properties. These measures may also guide analysts in selecting suitable organisational patterns. Finally, quantitative measures point out whether any S&D problem has been solved completely after installation of a pattern or additional solutions are still required. The rest of the article is devoted to these issues.

4. Metrics for Organisational S&D Analysis

Metric is a system of ways (and parameters) to measure particular properties of systems [5]. The term "system", here, refers to a system as a whole or a part of it (e.g., component). To avoid the confusion, we call the object of measurement as *Target of Evaluation (ToE)*. ToE refers to a part of a system under consideration which is also the main source of collected data. Organisational level operates with high level constructs (e.g., actors, goals, events, etc.). This means that ordinary low level systems (like firewalls, concrete operational system, cryptographical algorithm) cannot be considered as suitable ToEs for organisational level. Many problems can be identified on the highest level of design and solved before concrete implementation is determined (and save time, working time of designers and money). This means that the ToEs we can use should be also from the same level, i.e., implementation-independent. Most of the primitives used by *SI** can be considered as ToEs: actors, business objects (goals, tasks, resources), relationships and events. [2] At the level of organisation, these are the ToEs that need to be assessed by S&D metrics. The same observation is relevant for evaluation of organisational patterns [26].

Table 2 presents several examples of metrics assessing the property of ToEs previously presented in Figure 2. These metrics can be applied in various organisations. For instance, to measure the S&D relevance of a goal an organisation needs to define and assess the *value of a goal* or the criticality of an event can be assessed in terms of the loss introduced by the failures of goals or tasks to perform.

Note that some metrics do not measure S&D directly (e.g., *Value of goal*), but needed as building blocks for other metrics (e.g., *Total expected loss from an event*). ToE may be complex, i.e., consist of a set of similar constructs or several different constructs may form one ToE.

Example 1: Loss from an event metric measures the whole loss for the organisation caused by an event: several

2. These are also the same constructs used to capture S&D patterns presented in [26]

Table 2. Metrics for Organisational Level

Target of Evaluation	**Metric**
Goal	Value of goal
Set of *Goals, Tasks*	Loss caused by an event
Resources impacted by an *event*	Total expected loss from an event
Task, Resource	Complexity of task/resource
Actor fulfilling a set of *goals*	Workload of an actor
Event impacting *one goal* though failure of another *goal*	Probability of impact propagation
Event obstructing *a goal*	Frequency of events

goals, tasks and resources may be impacted by the *event*. This means that an analyst should consider all these constructs as one ToE when the metric is calculated. Moreover, the metric must be calculated for each event separately. This means that the event should be a part of the ToE as well.

In order to represent metrics uniformly, their definitions shall contain general information: the name of the metric and a short description of the ToEs. Moreover, each metric definition must contain a clear assessment methodology: procedure of measurement, formula for the calculation, and the procedure of re-measurement (if it is different with the initial one). In this work, we divide metrics into two levels:

Definition 1: Abstract metric is a metric which could be applied in various domains (i.e., organisations). *Instantiated metric* is an abstract metric that has been concretised to specific context and provides precise information about the metric.

There are different levels of details between the methodologies of an abstract metric and an instantiated one. Abstract metrics prescribe the baseline of the measurement procedure, while the instantiated ones detail the procedure according to the organisation settings. In other words, instantiated metrics are derived and detailed from the procedures of abstract metrics depending on the targeted context, on the usage of the selected metric and on the scopes of the assessment.

Besides having the detailed assessment procedure, instantiated metrics should specify the frequency of assessment (e.g., once, on demand, each month, etc.) and the threshold of the metric value. These aspects depend on the properties, ToEs, organisation, and on the specific needs of the evaluation.

Example 2: In the ATM scenario one may be interested in examining the *workload of an ATCO* (actor). The event of *workload overhead* is one type of ToE which is the subject for *frequency of event* metric.

Table 3 shows an example of metrics for the assessment of aspects related to the *Workload of an Actor*. Note that the structure of metrics has been adapted from [14]. It is essential to be aware how many workloads an actor is handling. If an actor is responsible for too many goals, then this tends to decrease the reliability of the actor. Moreover,

high workload causes stress for the actor and again makes him less reliable. In other words, less workload makes an actor more aware and, as the result, the system becomes safer.

Table 3. Example of an abstract metric

Element	Description
Name	Workload of an Actor
Description	Measures the assigned amount of work for an actor.
Procedure	Divide amount of work to be fulfilled by time to fulfill the work.
Time/ Frequency	Depends on the application domain.
Unit	Work/Hour
Thresholds	Depends on the application domain.
Notes	

The next section shows instances of metrics drawn from the ATM scenario. It highlights how metrics support quantitative assessment of relevant S&D properties from an organisational perspective.

5. Sample Evaluation Measurements

Quantitative assessment highlights the importance of metrics in Air Traffic Management (ATM) (e.g., see [1], [13]). In particular, it is possible to assess ATM systems in terms of, e.g., *safety*, *efficiency* and *capacity* [1], [13]. Quantitative assessment, therefore, enables the ATM domain to monitor ATM systems as a whole and to assess operational aspects (e.g., the introduction of new tools and procedures, etc.) continuously. The monitoring and management activities of ATM systems rely on quantitative assessment, which uses specific analytical tools and methodologies [3], [9]. The vast range of metrics identified in the ATM domain (e.g., see [8]) emphasises its complexity and socio-technical nature. A particular aspect in which quantitative assessment is particularly difficult concerns human factors. The investigation of accidents or degraded modes of operations stresses the *human-in-the-loop* aspects. Causal analyses and investigations highlight how *ATM failures* are often *organisational failures*. Essentially, the cause of accidents is complex and involves multiple responsibilities as characterised by hierarchical models (e.g., the cheese model). The classification, hence the quantitative assessment, of 'human errors' requires an analysis of interdependencies between different organisational factors.

This section provides some examples of metrics, which allow a quantitative assessment of organisational aspects that relate to dependability requirements. Table 4 shows the definition of *Number of Air Traffic Movements* that is a safety related metric (instantiated for different time period).

Note that this metric relates to the ATCOs' workload. Workload somehow is an indirect measure. It relates to the number of flights managed per hour (or other factors, e.g., number of routinary tasks if tasks are well-defined, numbers of communications, etc.). Number of Air Traffic Movements can actually be measured. For instance, it is possible to analyse different distributions of workload over the day. This is due to flight schedules. Thus, the workload would be high during peak-time (e.g., in the mornings or evenings with usual business flights). Of course, the workload, in this case, the number of flights per hour, depends on many factors (e.g., time of the day, distribution of flights, air traffic control centre, sector configuration). Different profiles correspond to different control centres and sectors. This is why ATCOs usually require training for the specific sector or ACC. Table 5 shows another example, the *en-route capacity*, which is related to efficiency and capacity properties.

Table 4. Air Traffic Movements

Element	Description
Name	Air Traffic Movements in Sector
Description	IFR Flights or segment of IFR Flights that could be managed by ACC in a hour.
Procedure	Count or use flight plans in the ACC system to predict the flights incoming in the sector
Time/ Frequency	Hourly
Unit	number of flights per hour
Thresholds	should not exceed En-Route Sector Capacity
Notes	Possible variation of ACC capacity up to about 410% from night to daily peak hours.

Table 5. En-Route Sector Capacity

Element	Description
Name	En-Route Sector Capacity
Description	Maximum number of flight that can be safely managed by the Air Traffic Controllers operating in an en-route sector.
Procedure	Defined in relation to the Sector characteristics (e.g., routes, airports, type of traffic, etc.)
Time/ Frequency	hourly
Unit	number of flights per hour
Thresholds	should not exceed 43
Notes	It could be seen as 'Workload of an Actor' Metric. This metric is related directly to defining the capacity of a sector and indirectly to the efficiency management of air traffic. Finally, it can also affect the safety of en-route flights

Both metrics are concerned with dependability aspects. Essentially, those metrics are described in terms of 'Frequency of an Event' ('flight arrival' event) and 'Workload of an Actor' (actor here is a group of actors managing the sector), respectively. Similar metrics have been used for the quantitative characterisation of the ATM scenario. The remainder of this section highlights how S&D organisational patterns enable safety and performance (i.e., support an increase of the air traffic capacity). It provides a quantitative account of the scenario unfolding. In particular, a quantitative analysis highlights how the scenario stresses the relationship between resilience strategies and dependability

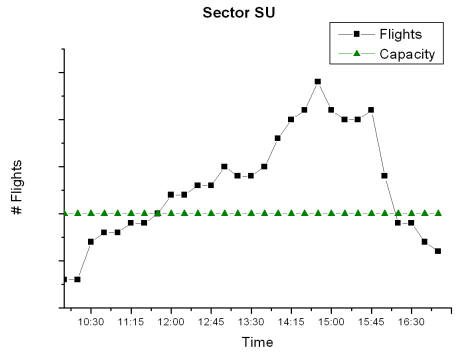

Figure 3. Traffic exceeding sector's capacity

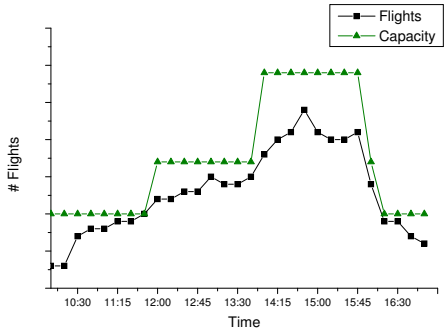

Figure 4. Resulting capacity

features (e.g., safety).

The analysis takes into account the dependability aspects with respect to traffic forecast (e.g., number of expected flights per hour), flights managed (e.g., number of current flights within a sector) and sector capacity (e.g., number of flights per time unit that are safely manageable). Note that some of these quantitative aspects relate to local physical constraints (e.g., sector characteristics) as well as to airspace regulations. For instance, the number of flights that is possible to accommodate per sector depends on the sector capacity and the constraining regulations (e.g., separation minima requirements). These measures point out how resilience strategies allow the modification of the operation profile (in terms of, sector capacity), hence the ability to accommodate an increasing and unusual traffic demand. Figure 3 depicts the traffic forecast (per hour-interval), flights accommodate (every 45'), and the sector SU capacity, respectively. It is evident in some period of time (i.e., 11.30-16.00) that the flight traffics exceeds the sector capacity.

After modifying the organisation structure (i.e., S&D patterns), the evaluation session guided the Air Traffic Controller. Although these decision strategies are coded in the ATM Internal Permanent Instructions (IPIs), the ATM toolset's functionalities support work practices (e.g., by reminding available strategies). Moreover, it supports the 'discovery' of emerging work practices (e.g., the combination of resectorisation and partial delegation). Figure 4 shows how the modification increases the overall capacity comparing the initial setting (in Figure 3).

6. Related work

There are a number of well-known and widely-used assessment methodologies for evaluation of technologies and management processes (e.g., Common Criteria (CC) [15] and Capability Maturity Model (CMM) series [12]). The levels assigned by the methods (evaluation assurance level for CC and maturity level for CMM) either appraise a specific software or organisational practices and, thus, cannot be used for high-level evaluation of organisational structure of a socio-technical system.

Penetration testing [18] is a well-known security analysis but the method depends very much on the experience of the penetrators. The method does not produce a metric but just a list of found breaches. Although number of the found breaches can be considered as a metric this method evaluates quality of a technology but not the organisational structure.

Using the received statistics and results of the penetration testing some methods calculate mean-time-to-breach metric [20], [22]. Mean-time-to-failure (MTTF), is used for evaluation of dependability. The biggest limitation of this metric is that its calculation is time-consuming [24]. Despite some limitations mean-time-to-breach and mean-time-to-failure metrics can be used on organisational level for assessing goals because the metrics are not connected with a specific technology and can be applied to a human being as well as to a technical system.

Risk analysis [23], [6] is an economical approach, which helps an analyst to understand the needs of a system, prioritise existing risks and justify investments in counter-measures. Typical metrics used for risk assessment are risk level, amount of damage caused by a single breach/failure occurrence and frequency of breach/failure occurrences. This approach is relevant for all levels of the design and some of our metrics were derived from it.

More metrics can be found in [16], [17]. Most of these metrics are technical and can be used to determine which aspects of the technical systems are required to be improved. However, there are many cases where the technical systems are operated correctly, but the organisation still suffers from failures. This can be caused by (negative) events that affect the organisation (e.g., aircraft accident, employees take holidays) or the users are overloaded. That is why we focused on metrics for organisational level of system design in this chapter.

7. Conclusion

This paper highlights how metrics can help to analyse S&D properties and judge if installation of S&D pattern solves the identified problem. In this work we focused on the possible metrics for evaluation of organisational level both at design or run-time. These metrics should be used to assess socio-technical systems from this level, to provide the most efficient support for system designers and administrators. We have defined how to represent the metrics on organisational level and have given several examples in general. However, these metrics should be instantiated for a particular organisation before putting them in practice. In our context, we used the ATM scenario from SERENITY project for specific monitoring and evaluation scopes and determined several metrics which can help to indicate early problems with S&D at organisation level.

Acknowledgement

This work has been partly supported by the projects EU-SERENITY and EU-MASTER.

References

[1] SECAM - Safety Efficiency and Capacity in ATM Methodologies. transport research fourth programme air transport **VII**65, eu (1998), 1998.

[2] Serenity project. `www.serenity-project.org/`.

[3] F. A. Administration. *Airspace Management Handbook*. The MITRE corporation, version 2.2 edition, 2005.

[4] Y. Asnar, P. Giorgini, F. Massacci, and N. Zannone. From trust to dependability through risk analysis. IEEE Computer Society Press, 2007.

[5] J. Bøegh, S. De Panfilis, B. Kitchenham, and A. Pasquini. A method for software quality planning, control, and evaluation. *IEEE Software*, 16(2):69–77, 1999.

[6] S. A. Butler. Security attribute evaluation method. Technical Report CMU-CS-03-132, Carnegie Mellon University, May 2003.

[7] V. Di Giacomo, et al. Using security and dependability patterns for reaction processes. In *Proceedings of the 19th International Conference on Database and Expert Systems Application, DEXA '08*, pages 315–319. IEEE Computer Society, 2008.

[8] Eurocontrol Performance Review Commission. Ace 2006 - atm cost-effectiveness 2006 benchmarking report, 2008.

[9] GAIN. *Guide To Methods & Tools for Safety Analysis in Air Traffic Management*, first edition edition, 2003.

[10] P. Giorgini, F. Massacci, J. Mylopoulos, and N. Zannone. Modeling security requirements through ownership, permission and delegation. In *Proceedings of the 13th IEEE International Requirements Engineering Conference (RE'05)*, pages 167–176, Washington, DC, USA, 2005. IEEE Computer Society.

[11] P. Giorgini, F. M. J. Mylopoulos, and N. Zannone. Requirements engineering for trust management: Model, methodology, and reasoning. *International Journal of Information Security*, 5:257–274, 2006.

[12] SEI. Capability maturity model (cmm).

[13] INTEGRA Project. EUROCONTROL CARE (Co-operative Actions of R&D in EUROCONTROL).

[14] ISM3 Consortium. *Information Security Management Maturity Model*.

[15] ISO/IEC. *Common Criteria for Information Technology Security Evaluation*. Common Criteria Project Sponsoring Organisations, 2.2 edition, January 2004.

[16] A. Jaquith. *Security metrics: replacing fear, uncertainty, and doubt*. Addison-Wesley, 2007.

[17] A. M. Johnson and M. Malek. Survey of software tools for evaluating reliability, availability, and serviceability. *ACM Comput. Surv*, 20(4), 1988.

[18] R. G. Johnston. Adversarial safety analysis: Borrowing the methods of security vulnerability assessments. *Journal of Safety Research*, 35(3):245–248, 2004.

[19] J.-C. Laprie and B. Randell. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1):11–33, 2004. Fellow-Algirdas Avizienis and Senior Member-Carl Landwehr.

[20] B. Littlewood, et al. Towards operational measures of computer security. *Journal of Computer Security*, 2:211–229, 1993.

[21] L. Liu, E. S. K. Yu, and J. Mylopoulos. Security and Privacy Requirements Analysis within a Social Setting. In *Proceedings of the 11th IEEE International Requirements Engineering Conference (RE'03)*, pages 151–161. IEEE Computer Society Press, 2003.

[22] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel. Time-to-compromise model for cyber risk reduction estimation. Springer-Verlag, 2005.

[23] G. Stoneburner, A. Goguen, and A. Feringa. Risk management guide for information technology systems. Technical Report 800-30, National Institute of Standards and Technology, 2001.

[24] W. Torell and V. Avelar. Mean time between failure: Explanation and standards. White Paper 78, APC, 2004.

[25] A. van Lamsweerde et al. From System Goals to Intruder Anti-Goals: Attack Generation and Resolution for Security Requirements Engineering. In *Proceedings of International Workshop on Requirements for High Assurance Systems (RHAS 2003)*, pages 49–56, 2003.

[26] Y. Asnar, et al. Secure and Dependable Patterns in Organizations: An Empirical Approach. In *Proc. of RE '07*. IEE CS Press, 2007.