DYNAMIC BUSINESS TRANSACTIONS CONTROL
An Ontological Example: Organizational Access Control with DEMO

Sérgio Guerreiro[1], André Vasconcelos[2,3] and José Tribolet[2,3]
[1]*Universidade Lusófona de Humanidades e Tecnologias, Escola de Comunicação, Artes Arquitectura e Tecnologias da Informação, Campo Grande 376, 1749-024 Lisbon, Portugal*
[2]*CODE, Center for Organizational Design & Engineering, INOV, Rua Alves Redol 9, Lisbon, Portugal*
[3]*Department of Information Systems and Computer Science, Instituto Superior Técnico, UTL, Lisbon, Portugal*

Keywords: Control, DEMO, Observation, Ontology, RBAC, White-box.

Abstract: This paper discusses the need to design control in the dynamic business transactions (DBT) of an enterprise. The concepts offered by the classical dynamic control systems (DSC) field are useful for identifying the main constructs. However, the complexity that today exists in the DBT is too high to be solely controlled by the analytical DSC approaches. A white-box ontology-based approach, supported by DEMO, is used to identify the core concepts required to enforce control in a DBT. Organizational access control exemplifies our proposal.

1 INTRODUCTION

This paper addresses the problem of enforcing control in the activity of the organizations. In general terms, it is related with the ability to drive, with a bounded effort, the operation of the enterprise towards a stable state whenever occur changes or perturbations. We are focusing in this issue but with a specialized view, which is how to enforce control in the transactions that operates in a real run-time organizational environment, in order to face the misalignments between the operational conditions and the references defined by the organizational models. The way that this specific research problem is being located is innovative because it considers that nevertheless the quality of the models definition that the organizations have, they are not enough to guarantee the actors follow them in the reality. Hence, a continuous observation of the operation is needed to identify the misalignments with the models and then to take corrective actions when needed.

From the foundations of the software engineering point of view, the adaptability quality of the software when facing change is broadly referenced, *e.g.*, the recommended practices for software requirements IEEE 830-1998 (IEEE830, 1998) identifies *"adaptability as non-functional properties of a system that should be included directly in its design"*. Roger Pressman, in (Pressman, 1992), a consensual classical reference in software engineering, states that *"the adaptability quality is classical identified as the aim in minimizing the software deterioration due to change"*. More contemporary in the normalized systems theory presented by Mannaert *et al.*, in (Herwig and Verelst, 2009) (Mannaert et al., 2008), a strong focus is given to the adaptability of a system: *"a design pattern needs to be stable with respect to anticipated changes"*. From the organizations point of view, Jan Dietz in (Dietz, 2006) refers that Enterprise Engineering (EE) is composed of the following missions: Enterprise Ontology (EO), Enterprise Architecture (EA) and Enterprise Governance (EG). From our perspective, we argue that software systems perform a key role in the operation of the organizations, however, if we want to control the fulfillment of the organizational goals by its persons and machines within the stated complexity, then the technological independent approaches from the enterprise engineering field (based in white-box solutions), such as DEMO ontology (Dietz, 2006), should be used to define comprehensiveness, coherent, conciseness and consistent (C4-ness) designs of the organization. Basically, it is a matter of abstraction, we cannot handle all the complexity directly at the software engineering level. Control in organizations is not only concerned with the electronic artifacts but rather with the communication between persons and between persons and machines, within public or private companies. It is interesting to notice that this concern is not recent, early in 1965, Emery and Trist (Emery and

Guerreiro S., Vasconcelos A. and Tribolet J..
DYNAMIC BUSINESS TRANSACTIONS CONTROL - An Ontological Example: Organizational Access Control with DEMO.
DOI: 10.5220/0003702905490554
In *Proceedings of the International Conference on Knowledge Engineering and Ontology Development* (SSEO-2011), pages 549-554
ISBN: 978-989-8425-80-5

Trist, 1965) refer that a company is a open system where its behavior is only explained when analysed in conjunction with its interactions with the surrounding environment. Later in 1978, Geert Hofstede's work, in (Hofstede, 1978), proposes that control should be formed and evaluated as a homeostatic model rather than a cybernetic model. Homeostatic control model considers that there are a large number of interrelated cybernetic systems within an organization, executing different business services and working side-by-side which usually involves communication between Humans and machines. Much more recently, José Tribolet and Rodrigo Magalhães, in the reference (Tribolet and Magalhães, 2007) also state that agility and real-time reconfiguration capability (Santos, 2007) are requirements to the maintenance of the organizations. Yet, the understanding and definition of the degrees of freedom between the DBT, the functional capabilities and the hierarchical power must be deeper researched. Also recently, Jan Hoogervorst (Hoogervorst, 2009), in the EG field, states that the increasingly complexity is characterised by an increase that follows the size of organizations. Thus, precise models that are able to deal with this complexity without exploding in terms of size are needed. By other words, the models should be able to follow, at the same pace, the increase in the size of companies.

The research related with the enforcement of the control in organizations require an investigation process that is incremental throughout time and that is obtained by a bottom-up, and step by step, knowledge acquisition. Our aim in this research is to acquire knowledge regarding the integration of the actual enterprise ontology state of the art with the access control modes to obtain a contemporary EG solution. In line, this paper presents the result of a set of steps to design an EG solution in the ontological field. The steps are integrated in a research process where the former iterations affected the remain ones. It allow the interaction of the work with the community while developing the solution, thus making alignment with the academic and entrepreneurial reality, and also allowed the researchers to learn from the errors while developing the theoretical and experimental artifacts. We clarify that this research does not follow a pure design-science research (DSR). Piirainen *et al.*, in the reference (Piirainen et al., 2010), studies the DSR developments stating that the following steps are required: identify an IT organizational problem, the aim is to identify and solve real problems that exist in the daily life of the organizations; demonstrate that no solution exists; develop IT artifact that addresses this problem; rigorously evaluate the artifact; articulate the contribution to the IT knowledge base and community; explain the implications of IT management and also to the reality of the enterprise. Actually, this paper uses the identification of organizational problem, the development of ontological artifacts to address the problem and then the rigorously evaluation, using argumentation, of the artifacts combined with some other steps.

The remaining of the paper is organized as follow. Section 2 identifies the typical perspective where the dynamic systems control is used. Then, section 3 proposes a feedback loop applied to the DBT. Section 4 exemplifies the DBT control using an access control approach. Finally, section 5 concludes the paper.

This work was partially supported by a PhD scholarship, SFRH/BD/43252/2008, FCT, MCTES, and also supported by PTDC/CCI-COM/115897/2009, MOBSERV.

2 DYNAMIC SYSTEMS CONTROL

The aim of controlling dynamic systems is to gain efficiency in their operation, thus achieving the same results but with less resources usage. From a historical point of view, the first significant work in automatic control was James Watt's centrifugal governor for the speed control of a steam engine in the eighteenth century (Ogata, 1997). Since then, major advances have been made in the research of the systems control theory, many of them were driven by the advent of the digital computers. It worth noticing that control systems are mainly developed by the automation field, raised by the need to implement automatic supervision since the industrial revolution. A control approach is composed of two main parts: *(i)* the *controller* and *(ii)* the *controlled process*. The controller is responsible to control the process, where a feedback control system is the system that maintains a prescribed relationship between the output and the reference input by comparing them and using the difference[1] as a means of control (Ogata, 1997; Franklin et al., 1991). This difference occurs because of two reasons: *(i)* the interaction of the controlled process with the *exogenous*[2] factors (for instance, a disturbance) and *(ii)* the *endogenous* factors (for instance, a breakdown). Along with this consideration, it is remarked that to control a process using the dynamic systems control concepts it is demanded the full dynamic specification of the process, mainly using analytical approaches. Once the dynamic of the process

[1] Sometimes also referred as innovation.

[2] Originating from outside and endogenous from within.

is presented then the controller is designed and fine-tuned to deliver a finite and bounded process output with a set of finite and bounded control initiatives.

Returning to the organizations field, the analytical models to express its functioning are not available, due to its complexity and with the intertwined human activity that exists in reality. Our knowledge about these phenomena's is only partial. Therefore we are not able to follow a similar research path as the one followed by the classical DSC. Yet, the DSC concepts are engineering-based founded and forms a relevant starting point to identify what is desirable to achieve in the scope of organizations. From the other hand, control exists in all areas of expertise, and conversely, it is not exclusive to DSC. Nonetheless, the advances of control concepts in the enterprise engineering field of expertise are still not defined in a consensual way, neither are proposed with an essential ontological perspective. Thus, the DSC approaches presented in this paper aims at identifying the concepts that are useful for the development of the control concepts in the enterprise engineering scope.

3 DYNAMIC BUSINESS TRANSACTIONS FEEDBACK CONTROL

Actually, considering DEMO (Dietz, 2006), it already controls the DBT in organizations, because it guarantees that the transactions are formed accordingly with an essential ontology that is compatible with the communication and production, acts and facts, that occurs in the reality between actors of the different layers of the organization *(D-, I- or B-)*[3]. Hence, when a DBT is fully DEMO compatible then we have the assurance that the designed communication and production, acts and facts, will replicate the set of possible combinations that the actors do in reality. Steven Kervel, in his references (Kervel, 2011; Kervel, 2009), in fact, proposes to control the operation of the transactions using a state machine, based in the Ψ-theory[4] of DEMO, that keeps track of the allowed states where a DBT is. In other words, when a DBT is correctly designed regarding the desire of the organization and when the actors executes their actions in respect with the designed DBT then the problem is supposed to be solved. However, in this paper we state that this is not the case in most of the situations. Most of the times the actors do not follow the designed DBT, in fact, they execute parts of the business that is again probably compatible with DEMO but it is not what has been previously defined by the organization. Having this kind of situations in mind, then we propose a solution that observe the operation and that actuates over the DBT models.

In more detail, the function of controlling a dynamic system requires the following aspects:

1. the *ex-post*[5] observation;
2. the actuation;
3. the *ex-ante* knowledge regarding the dynamics of the system to be controlled;
4. the *ex-ante* references specification;
5. the controller which might be composed of different layers of competence.

Our proposal combines these concepts with the actual knowledge offered by the Enterprise Engineering field in order to develop control functions applied to the companies. The dynamic of the organizations is captured by the transactional design and operation. A transaction is defined by the transaction axiom of Ψ-theory. Furthermore, we settled that a separation between the transactional models definition and the transactional instances must be considered in order to differentiate the reference from the operation and thus identifying the innovation. The transaction axiom is considered to be the organizational throughput, without it the organization does not exist. The importance that is attributed to the transactional concern justifies the first option to bound the solution to the observability to the operation of the transactions.

In line with the previous considerations, we remark that this solution nevertheless being located in the ontological field it is detailed enough to be a solid starting point to allow its implementation by the software engineering field. For the reason of having a normalized approach the solution is designed with the DEMO ontology and is also to be used in the DEMO models. In practice, it does not redefine the DEMO ontology, but rather defines a set of control patterns that should be included in the DEMO models whenever EG is alleged.

Figure 1 presents two control diagrams that have

[3]The organization of every enterprise can be conceived as a layered nesting of three parts, called aspect organizations: the **B-organization**, the business actions take place. It consists of B-actors and B-transactions; the **I-organization**, supporting infological actions take place. It consists of I-actors and I-transactions; the **D-organization**, supporting datalogical actions take place. It consists of D-actors and D-transactions.

[4]Ψ-theory that stands for *PSI:* Performance in Social Interaction (Dietz, 2006)

[5]The term *ex-post* is defined by the expression: "after the event", conversely, *ex-ante* is defined by the expression: "before happening".

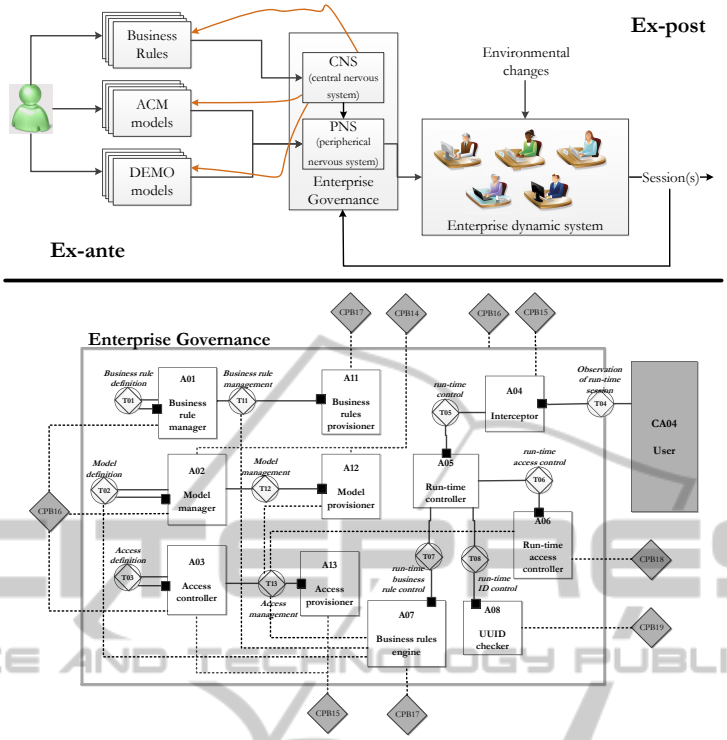

Figure 1: Comparison between the initial proposed control and the obtained ontological control. *In the top:* using free design figures. *In the bottom:* the ISM ontological control design that is obtained in the end of DEMO methodology execution.

the previous 5 concerns in mind. In the top of the Figure an information flow is designed using a non formal specification. The aim is to share the idea of a feedback loop in the scope of the organization operation. Only informal blocks and arrows are used to express correspondingly the control components and the information flow that exists. The solution controls the activity of the actors, checking misalignment between the *ex-ante* models and *ex-post* observations. A session execution includes all the *ex-post* observations in a real organizational environment and is used to trigger the EG kernel. EG check the misalignments and the result is one of the following counterparts: *(i)* a permission or denial of access to the activities that are being executed in the current session and / or *(ii)* a change to the *ex-ante* models. The first counterpart is based on the ability to control using a systemic view of the transactions of what is being done and if that complies with the *ex-ante* DEMO and access control models. The result obtained is only a grant or a revoke to execute the actor's activities. The second counterpart is based in the ability to control using a systemic view of the historical transactions of what is being done and if that complies with the *ex-ante* business rules. The result is one of the following actions: a change in the business rules, a change in the DEMO model or a change in the access control model.

In the bottom of the Figure 1, an Organization Construction Diagram (OCD) from DEMO is depicted to specify the actors, the production and coordination banks, the boundary and the information flow. The same concepts presented in the top of the figure are also herein expressed. But more detail regarding the involved transactions of the ontology are identified. Some few considerations are made regarding this model. An information link exists between A12 and T13 to obtain the access configuration from the DEMO model definition during the configuration phase of the references. The A07 has three information links to the T11, T12 and T13. They correspond to the control action that are taken when any misalignment occur. T11 corresponds to a self-change in a business rule, T12 corresponds to a change in the DEMO model to be controlled, it is expected to be performed by the model manager which is a person and T13 that corresponds to a change in the access management. *CPB16* refers to the Period that the EG is being considered, by other words a time frame where the control makes sense, hence a information link exists with its boundary, meaning that all the actors and transactions are supported in this composite production bank.

4 ORGANIZATIONAL ACCESS CONTROL EXAMPLE

This section exemplifies the proposed ontological design in the scope of an organizational access control system. Nevertheless the development of the role-based access control (RBAC) concepts, from the access control modes (ACM) community, this approach is only helpful for specifying and implementing the structural security access concerns for a single organizational silo (Sandhu et al., 2000). Typically, the ACM follows predefined policies that are applied to a specific application layer of an organization. Examples of such approach are the discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), time-role-based access control (TRBAC), Orcon or Chinese wall (Ferraiolo et al., 2001; Ferraiolo et al., 2007). In this scope, we are proposing, in Figure 2, the WOSL (Dietz, 2005) design of RBAC access integrated with the DEMO ontology.

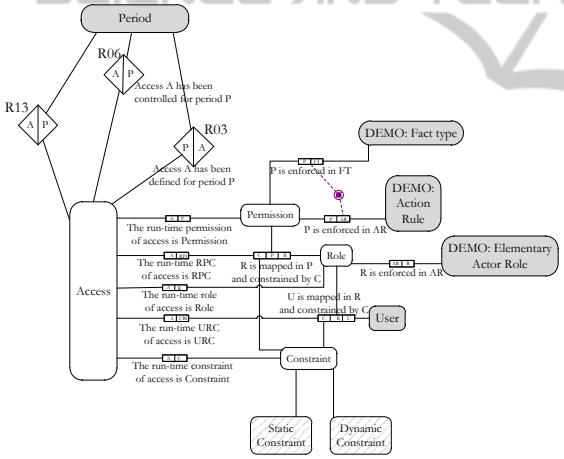

Figure 2: WOSL for governance enforcement in DEMO ontology: the RBAC state space representation.

The User is an external category that is related by a ternary fact type with its Role and its Constraint. A Role is related by a ternary fact type with its Permission and also with its Constraint. A Constraint is specialized by the categories Dynamic Constraint and Static Constraint representing design restrictions that allow configurable access authorization, *e.g.*, separation of duties. The first one is calculated online and is related with the Session enforcement by a binary fact type and the second is calculated offline related with the Model also by a binary fact type. The Access category keeps the state of the *access configuration* and corresponds exactly to the five reference laws declaration with: *(i)* the Permission; *(ii)* the Role; *(iii)* the Constraint; *(iv)* the fact type regarding the constrained mapping between the Role and the Permission and *(v)* the fact type regarding the constrained mapping between the User and the Role.

From the other hand, in the right part of Figure 2, the integration between the Access and the DEMO concepts is formally defined by:

(i) **a binary fact type relating the Role and the *DEMO:Elementary Actor Role***, this relation is not established with the DEMO composite actor roles because they are outside the scope of the organization;

(ii) **a binary fact type relating the Permission and *DEMO: Fact type***, where a fact type is considered as an entity that is able to be created, removed or updated in some way during the DBT execution;

(iii) **a binary fact type relating the Permission and *DEMO: Action rule***, where an action rule is considered as an entity that executes an atomic part of the DBT;

(iv) **a mutual exclusive law between Permission with *DEMO:Fact type* and *DEMO:Action rule*,** theoretical in this way we are controlling the permission to the DEMO action rule that are specified in the action rules specification (ARS) and to the DEMO Fact type in the state model (SM). However in practice if the transactions are properly decomposed to only handle a fact type inside each action rule then it is enough to integrate the Permission with the DEMO action rule.

Conversely to classical approaches in the scope of security, the explained integration between Access and DEMO allows not only to enforce the access control in the invocation of the DBT but, by the contrary, it allows a run-time control of all the action rules and fact types that are used within all the scope of the DEMO DBT instantiation. This approach has the advantage of fine-control the access of each user to the artifacts and also in the capability of changing the configuration in run-time with a direct consequence in the execution of the DBT. For instance, when some kind of action is taken in reaction to a session condition is order to conform with the business rule, model definition or access definition that are provisioned.

As one could notice a intertwined between the RBAC implementation and the constructs of DEMO models exists in this proposal. One clear advantage of using this proposal is to obtain the RBAC role and permission automatically from the previous designed DEMO models. Which means that only the assignment of each user to a role must be done by the organization.

5 CONCLUSIONS

Actually, the capability to fine-grained control the access to the artifacts of an organization, or even, the capability to define and implement business rules, are most of the times, decoupled from the enterprise design. The practical consequence of this decoupling, is *(i)* the duplication of effort in the control and models design counterparts and *(ii)* with the designed models not aligned with control. Nowadays, a change in the control requires a change in the model design, and *vice versa*. Integrating the access control at the models design enables a fine-grained access control to the artifacts directly in the design with a perfect alignment that enables the continuous changes throughout time. Moreover, this integration enables a full observability of the operation of the enterprise and thus allows the enforcing of business rules that are able to react in run-time based in the actual and historical observations. As a consequence of this, the business rules are kept as directions that are truly followed by the organization.

This paper defeat a completely different approach when compared with non ontological models or even with models that are solely black-box oriented. We accept that in order to understand control it is correct to view the models and the control principles using a black-box approach, yet the white-box concepts that relate the separation from the controller and the controlled process should be researched and precisely ontological specified if a real implementation is expected. It is not enough to consider only the black-box approach. On the other hand, a white-box approach enables *(i)* the continuous observation of the design restrictions of the run-time DBT from the inside and then *(ii)* to actuate with a change in the DBT models when needed. In the limit, parts of the control could be performed by automatic systems rather than exclusively performed by actors.

For short, our approach represents an effort for conceptualizing the control patterns that should be included in the design of the real systems that supports the organization. Moreover, the control concepts presented herein are directly related with the EG area regarding the lower level of governance for a DBT. For other aspects of the organization, other control layers should be further considered. Despite the concepts that are presented in this paper, further research is needed to design a full ontology for the control of the DBT. In particular the concepts of business rules enforcement. It is also needed to develop automatic tools to design and validate the ontological models.

REFERENCES

Dietz, J. L. G. (2005). A world ontology specification language. pages pp. 688699. OTM Workshops.

Dietz, J. L. G. (2006). *Enterprise Ontology: Theory and Methodology*. Springer.

Emery, F. and Trist, E. (1965). *The Causal Texture of Organizational Environments*. Systems Thinking, Frederick Emery edition.

Ferraiolo, D., Kuhn, D., and Chandramouli, R. (2007). *Role-Based Access Control*. ArtechHouse, 2nd edition edition.

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., and Chandramouli, R. (2001). Proposed nist standard for role-based access control. *ACM Trans. Inf. Syst. Secur.*, 4(3):224274.

Franklin, G. F., Powell, J. D., and Emami-Naeini, A. (1991). *Feedback Control of Dynamic Systems*. Addison-Wesley Publishing Company, second edition.

Herwig, M. and Verelst, J. (2009). *Normalized Systems: Recreating Information Technology based on Laws forSoftware Evolvability*. Koppa.

Hofstede, G. (1978). The poverty of management control philosophy. *The Academy of Management Review*, 3(3):450461.

Hoogervorst, J. A.(2009). Enterprise Governance and Enterprise Engineering. The Enterprise Engineering Series. Springer Science.

IEEE830 (1998). Ieee recommended practice for software requirements specifications.

Kervel, S. (2009). Enterprise ontology driven information system engineering. In: Presentation given at CIAO!

Kervel, S. (2011). *forthcoming in, Phd Thesis regarding DEMO processor*. PhD thesis, Delft University of Technology, Netherlands.

Mannaert, H., Verelst, J., and Ven, K. (2008). Exploring the concept of systems theoretic stability as a starting point for a unified theory on software engineering. *Software Engineering Advances, International Conference on*,0:360366.

Ogata, K.(1997). *Modern control engineering*. Prentice-Hall, Inc.

Piirainen, K., Gonzalez, R.,and Kolfschoten, G. (2010). Quo vadis,design science? a survey of literature. In Winter, R.,Zhao,J., and Aier, S., editors, *Global Perspectives on Design Science Research*, volume 6105 of *Lecture Notes in Computer Science*, pages 93108. SpringerBerlin/Heidelberg.

Pressman, R. S. (1992). *Software Engineering, A practitioners Approach*. McGraw Hill Book Company Europe,third edition.

Sandhu, R., Ferraiolo, D., and Kuhn, R. (2000). The nist model for role-based access control: towards a unified standard. In *Proceedings of the fifth ACM workshop on Role-based access control*, RBAC00, pages4763, NewYork, NY, USA. ACM.

Santos, C. A. L. d.(2007). *Modelo Conceptual para Auditoria Organizacional Contínua com Análise em Tempo Real*. PhD thesis, Universidade Técnica de Lisboa, Instituto Superior Técnico.

Tribolet, J. and Magalhães, R. (2007). *Ventos de Mudança*, chapter Engenharia Organizacional: das partes ao todo e do todo às partes na dialéctica entre pessoas e sistemas. Editora Fundo de Cultura. Brasil. in Portuguese.