Introducing the Common Non-Functional Ontology

Vandana Kabilan[1], Paul Johannesson[1], Sini Ruohomaa[2], Pirjo Moen[2], Andrea Herrmann[3], Rose-Mharie Åhlfeldt[4], and Hans Weigand[5]

[1] Department of Computer and Systems Sciences, Royal Institute of Technology and Stockholm University vandana@dsv.su.se,pajo@dsv.su.se
[2] Department of Computer Science, University of Helsinki sini.ruohomaa@cs.helsinki.fi,pirjo.moen@sc.helsinki.fi
[3] University of Heidelberg Andrea.Herrmann@informatik.uni-Heidelberg.de
[4] University of Skövde rose-mharie.ahlfeldt@his.se
[5] Tilburg University H.weigand@uvt.nl

Enterprise systems interoperability is impeded by the lack of a cohesive, integrated perspective on non-functional aspects (NFA). We propose to respond to the fragmentation in NFA research by supporting a shared, common understanding. For this purpose:- first, we propose a common NFA ontology, which generalizes and integrates the different non-functional aspects under a common top-level ontology. Second, we introduce a series of specialized ontologies on specific non-functional aspects, such as trust, risk, privacy, threat and misuse. By fostering a consensual and shared view of the non-functional aspects domain, we aim to move closer to enhancing semantic enterprise interoperability. This shared perspective on *what* non-functional aspects are and *how* they relate to the other 'functional' aspects of enterprise systems, is the key towards enterprise interoperability.

1 Introduction

Non-functional aspects (NFAs) have a key role in establishing, conducting and maintaining inter-enterprise interoperability [1]. The ill-toned naming of these properties reflects well the neglect they have long suffered in software design and development. Issues related to such aspects like trust, security, privacy, contracts or quality of service are often left unaddressed till late in the software development process. However, in the context of enterprise interoperability, these aspects and the organisational policies that they form span across a wide range of business activities. Therefore, they must be considered and integrated into the enterprise system modeling,along with the other traditionally accepted 'functional aspects'. In this respect, some of the key research problems identified are:

- Existence of a fragmented definition of *what* non-functional aspects are.
- Unclear vision on *how, when* or *where* these aspects should be integrated into the enterprise system modelling.

To resolve the above mentioned issues, we first need to establish a shared understanding of *what* Non-Functional Aspects are, *how* they influence the business processes and *how* they should be connected to the business models. One such way would be to capture the aforementioned knowledge as an ontology. Gruber's [5] definition of an ontology states: *Ontology is a specialization of a conceptualisation.* The fundamental objective behind the design of ontology is to conceptualise the domain of interest. Some other objectives for designing and using ontologies have been put forward by Noy and McGuinness [13] as:

- To make explicit implicit domain knowledge.
- To promote easy and shared understanding.
- To support reusability and interoperability.

Thus, the research problem addressed in this paper is on capturing and making explicit the implicit knowledge surrounding the non-functional aspects.We propose to capture and represent this shared conceptualisation as a set of ontologies. The researchers involved in this conceptualisation are experts from different non-functional aspect domains. Thus, the proposed ontologies are in themselves a product of consensus. We discuss more on our research methodology in Section 2. In this paper, we propose a Common NFA Ontology as a top level generic ontology, to which a number of individual Non-Functional ontologies are related. Our research has led us to establish a number of individual Non-Functional ontologies like trust, privacy, threat and misuse, information security, quality of service, digital rights management, business contracting, contract-related risks and so on. However, due to limitation of space, we present an overview of only a selected number of these.
The focus of this paper is to introduce the top level generic ontology - the Common NFA Ontology. We exemplify the utility of the proposed Common NFA ontology by describing how it is "specialised" in the individual sub ontologies. Note that the description given for each of the sub ontoloy is neither complete or exhaustive, but only an illustrative extract of the main concepts from each of them. We begin by a short discussion on our research methodology including the ontology design strategy adopted in Section 2. We present the Common NFA Ontology in Section 3. We present the overview of the Trust Ontology in Section 3.1, Threat and Misuse Ontology in Section 3.2, Business Contract Risk Ontology in Section 4, and Privacy Ontology in Section 5. We discuss the results and utility of our work in Section 6 and conclude in Section 7.

2 Research Methodology

To the best of our knowledge, no previous research exists that captures and models the different non-functional aspects within one common ontology. Our collective group of expert researchers carried out a state-of-the-art research survey for the different non-functional aspects. Initial results were published in TG7 Roadmap [1]. To analyse and represent the gathered knowledge, we reviewed different ontology design methodologies like those proposed by Gruninger and Uschold [17], Noy and McGuinness [13], Guarino [6] , Fernandez et al. [3] and Nicola and Missikoff [2]. We found the UPON methodology, based on the Unified Software Developement Process [9], simple to adopt within the diverse group of researchers, most of whom were not ontology experts. A first sketch of each of the non-functional aspects was carried out using the storyboard writing phase as proposed by the UPON. Next, a common template for capturing the main concepts, definitions and relationships to generate a glossary (again UPON) was suggested. A main instrument in the methodology of our work was a case study scenario of a typical enterprise system, which was carefully analysed from different non-functional aspect perspectives. Based on intial results of this analysis and further discussions, a first preliminary conceptual model for each individual sub ontology was proposed. After this 'glossary' building phase, the work was again reviewed for duplicacy and redundancy. Building on the case study analysis, detailed conceptual models for each of the sub ontologies was constructed.

3 Introducing the Common NFA Ontology

Our approach is to reuse existing ontologies as far as possible. Therefore, we chose to begin our work on the Common NFA Ontology by basing it on another accepted specification, namely the Business Motivation Model(BMM) [4]. Some of our reasons for choosing this particular standard may be summarised as:

- BMM identifies factors that motivate and influence a business enterprise and its goals.
- BMM identifes key business concepts like actors and business elements that are influenced by the above mentioned factors.
- BMM relates the key relationships between the influencing factors and the business concepts.

All the above reasons are useful in defining how non-functional aspects (influencing factors) may have an impact on or be related to the identifed key business concepts.

In Figure 1 we see the conceptual model of our Common NFA Ontology. As said before, the Common NFA Ontology extends the basic BMM.(The shaded

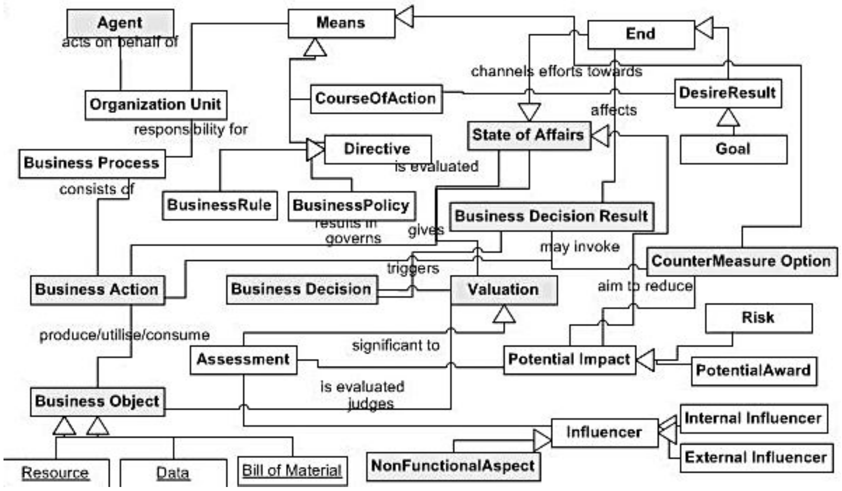

Fig. 1. Common NFA Ontology- Conceptual Model

concepts are those that have been introduced by us). We begin by first reviewing some of the existing concepts defined in BMM and thereafter, proceed to the new additions. We use the `type text font` to denote concept classes. Stereotypes of the Common NFA used in the sub ontologies also include the parent class in paranthesis, wherever applicable, if not stated explicitly.

3.1 BMM Revisited

A basic notion in BMM (Figure 1)is that of a `goal`, which expresses something a business seeks to accomplish, a desired future state of affairs or condition. Examples of goals are being the market leader in an industry or having a profit of more than one million euros. Furthermore, there are `means` , i.e. something that can be used to achieve a goal. `Means` can take different forms, they can be instruments, devices, capabilities or methods. A `means` states what an `organisation` will do or use to achieve a `goal`, while a `goal` tells what the `organisation` views as desirable. There are two main kinds of `means`, `course of action` and `directive` such as `business rules` and `policies`. Then there are `influencers`, i.e. things that can impact an enterprise in its employment of `means` or achievement of `goals`. Note that an `influencer` expresses an objective state of affairs, it just exists, and there is nothing the `organisation` can do about this. In contrast, a `goal` is something that an `organisation` decides about - it wants to accomplish the `goal`. Similarly, a `means` is something that the `organisation` chooses itself - it decides to use a `means` to achieve a `goal`. it is useful to distinguish between two types of influencers, `external` and `internal`. An `external influencer` exists outside the organisational boundaries of an enterprise, e.g. a competitor that is taking market shares from an enterprise. There are also internal influencers that exist within an enterprise. It could be a habit, i.e. a customary practice or use. Influencers can be positive or negative, they can make it easier or more difficult to achieve a goal. In fact, the same influencer may make it easier to achieve one goal and at the same time make it more difficult to achieve another goal. In order to tell how an influencer impacts a goal or a means, we use assessments. For example, we say that an influencer is a threat for achieving a certain goal, or an opportunity to employ a certain means. Other examples are strengths and weaknesses.

3.2 Common NFA Ontology

We begin by introducing the concept of business object in the Common NFA. Business objects refer to any object or resource that is of some value to an organisation. For examples- goods or services that are being traded, purchase orders, contracts, customers and ERP systems. Business objects also include less tangible objects like data,information and digital rights. Business process acts on or utilises or consumes or produces these business objects. Therefore, these business objects undergo some change of state, which we can qualitatively or quantitatively measure, to result in a state of affairs. Some states of affairs are planned and desired like goals, whereas other state of affairs are unplanned and even unwanted such as quality deficiencies and business damages. Business process are affected by internal as well as external influencers, therefore the business objects are also affected. Non-Functional Aspects like trust, risk, quality of service are all kinds of influencers. These influencers act indirectly to produce undesireable effects on the expected outcome of business processes, thereby affecting the goals for an organisation. Hence, it is required to assess whether this state of affairs is desired or not. For this purpose, we introduce the notion of a valuation in the Common NFA ontology. A valuation is usually done by an organisation, but it may also be done by an outside (external) agent. The valuation is an evaluation done on a business object, its current state and its planned state to give a value result. For example, if the goal had been to increase sales by ten percent and the current monthly balance sheet indicates a loss of five percent, then the valuation would provide the evaluated value result that there is a net loss and no growth in sales. If the value result indicates that the current state of affairs is undesirable or unacceptable then appropriate measures need to be set in motion to counteract these ill-effects. This is decided by a business decision. The business decision is a central concept in our Common NFA Ontology. The business decision is based on the valuation, the prescribed set of goals, available means and the expected state of affairs. The business decision result of such organisational decision making could involve a change in policy, directive, adoption of some new means. These are termed as countermeasures. The countermeasure

has to realise the business decision result, that is, it imposes some modified requirements on the enterprise. We introduce a countermeasure option as a kind of means that an organisation unit may adopt to specifically address any negative potential impact that any internal or external influencer may produce on the defined Objectives and Goals. Positive impacts, that is, potential awards are also incentives or factors that influence business goals and policies. In most non function aspect scenarios, it is the incentive of potential awards that motivate an enterprise, like improved customer satisfaction leading to more revenue is the potential award for implementing better quality of service(non-functional aspect). We see, thus, that the non-functional aspects often lead to qualitative performance indicators rather than quantitative aspects.
We shall in the following sections, present some of the non-functional aspects as individual ontologies.

4 Trust Ontology

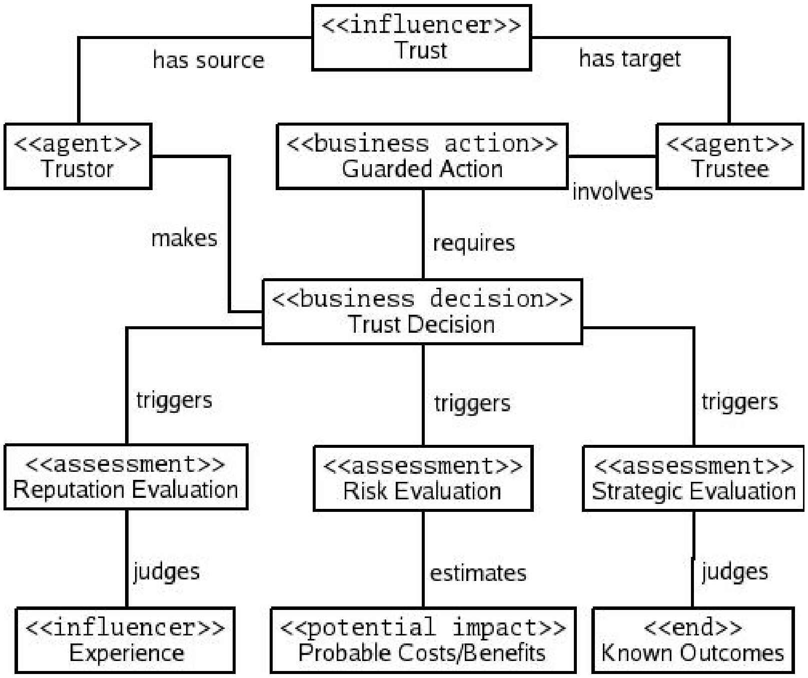

Fig. 2. Excerpt from Trust Ontology

The first subontology describes the multifaceted phenomenon of trust between organisations. Trust has business relevance to an organisation in two different contexts: as a `trustor(agent)` and as a `trustee(agent)`. In the `trustor`'s role, an `agent` representing the `organisation` tries to determine whether it is beneficial for the `organisation` to trust another `organisation` (or `agent`, as the case may be) in a particular context. In the `trustee`'s role, the `organisation` and its representatives try to encourage the trust of other `organisations` and `agents` by various `means`. In our trust ontology, we focus on describing the `trustor` role.

Definitions of trust in the literature vary according to the context they are used in [12, 15, 18]. Some research efforts focus on trust as a subjective belief about positive attributes of the trustee. From the management perspective, however, a more concrete approach is beneficial. We define trust as- *The extent to which the trustor is willing to participate in a given business action with a given trustee, considering the risks and incentives involved.* This definition of trust includes the subjective belief as one motivator to trust, while other motivators may depend on the general context as well. The trust ontology built on this conceptual approach is depicted in Figure 2.

`Trust` is a strong `influencer` between the `Trustor` and `Trustee`. It is the basis for `Trust Decisions` that concern the participation in certain `Guarded Actions(business actions)`. The general trustworthiness of the trustee is built on `Experience(influencer)`, which can be gained internally or reported by external sources. The body of experience is assessed in a `Reputation Evaluation(assessment)`. For example, a number of experiences on the trustee delivering excellent quality products but the being late can be evaluated as a low trustworthiness on timeliness, but high on quality products. The context determines which of these attributes would be more important for a given `Trust Decision.`

Participation in a `Guarded Action` also involves `Probable Costs/Benefits` (potential impact) depending on the behaviour of the trustee and the estimated cost or benefits resulting from it. These are assessed in a tactical `Risk Evaluation`(assessment), which aims to determine what the probabilities and effects of different outcomes are. There are also some `Known Outcomes(end)` that depend only on the `business decision`. For example, following or violating a contract that governs the `Guarded Action` leads to— the cost of a contract violation may be lower than the predicted outcome of doing business with an ill-reputed trustee, but it must be evaluated as a part of the `Trust Decision`.

5 Business Contract Risk Ontology

The primary goal for Enterprise systems is to conduct profitable business with other enterprises. Such transactions are covered by legal contracts and other regulatory bodies. The Multi Tier Contract Ontology [10] is one of many contemporary researches in the field of conceptualising the domain of business contracts from different perspectives. We do not discuss those "functional"

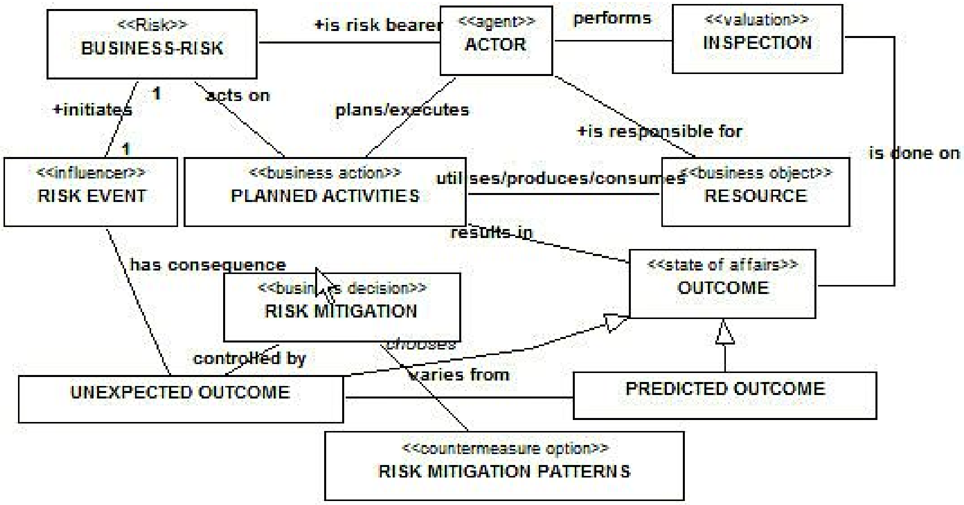

Fig. 3. Excerpt from Business Contract Risk Ontology

aspects in this paper. Instead, we focus on one of the non- functional aspects related to the business contract and the enterprise— that of Business Risks undertaken in a given contract. Business contracts act to specify expected behavior, describes course of actions for possible non-conformance to agreement. But they also state explicitly the kinds of risks undertaken and determine the options available for resolving situations, in the event such a risk is actualised. Mechanisms for assessing and controling such risks has been discussed by Kabilan and Weigand [11]. We capture some of these concepts in our non-functional sub-ontology for Business Contract Risk. The contracts are aimed to split such ”risks” on who will bear it, how much, to what extent and so forth.

`Business Risk (Assessment)` acts `on` a set of `planned activities` which utilizes or consumes and produces a set of `Resources (business objects)`. This `business risk` is always borne by an `actor(agent)` who acts on behalf of the enterprise concerned. Every `business process` or action is expected to result in a certain `outcome (State of Affairs)`. This `outcome` may be the expected result, in which case all is well, and we have `predicted outcome(outcome)`. The `outcome` may be `unexpected outcome` in the eventuality of an undesired result. For example, in the case of a loss of revenue(`unexpected outcome`) due to currency fluctuation (`external influencer`) the `risk event` is the change of currency rate. In short,the `business risk` is said to occur when there is a `planned activity` which does not produce the `predicted outcome` or Results. The `outcome` is inspected `valuation` by the `actor` to ascertain whether the `unexpected outcome` is an acceptable `state of affairs` or not. The `business decision` involved is the `risk` mitigation control. This requires that a countermeasure be adopted to limit the effects of the risk.

6 Threat and Misuse Ontology

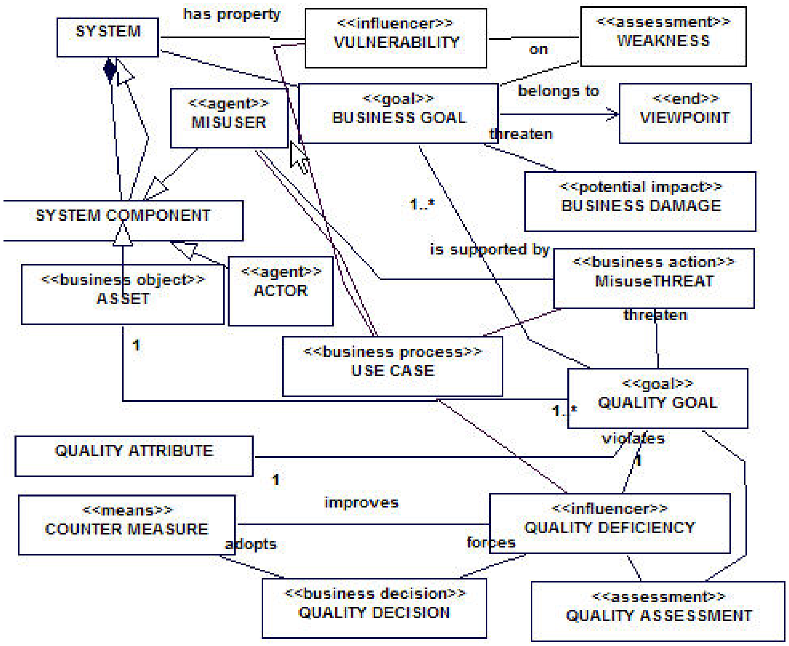

Fig. 4. Excerpt from Threat and Misuse Ontology

A central concept in the Threat and Misuse ontology[7, 8] is system, which is the entity that can be misused and threatened. A system does not include only software, hardware and networks, but also facilities, organisation, administrators, maintainers and users. A system can be decomposed into components that are themselves systems, thereby forming a hierarchy. Components of a system that need to be protected are called assets. In the ontology, we introduce a class system with a subclass system component. Three subclasses of system components are identified: asset, actor, misuser.

There are two kinds of goals for a system, business goals and quality goals. A business goal is a goal on the business level and tells why a system is introduced and used. A quality goal describes a general non-functional requirement that a system has to satisfy, and it is composed of one asset and one quality attribute. Some high level examples of quality attributes are reliability, usability, portability and efficiency. Note that, in contrast to BMM, we here make explicit which system a particular goal is defined for.

It may be the case that a goal is not fulfilled for some reason; such a situation is called a quality deficiency if it concerns a quality goal and a business damage if it concerns a business goal. For example, if there is a quality goal of high availability of data, there may be quality deficiencies like corrupted data or manipulation of data and hardware.

Business and quality goals may be directly threatened by certain business actions, which are called misuses.The actor(agent) who carries out this misuse is therefore a misuser. An example could be unauthorized access to classified data. Vulnerability(influencer) is a property of a component of a system that makes it vulnerable(weakness) to threats, e.g. a design flaw or a flaw in the software development process. Misuses, vulnerabilities, and quality deficiencies can be grouped together into misuse cases that describe entire scenarios of misuses. Such a scenario(called the misuse case includes a misuser who exploits some vulnerability of a system and carries out a misuse resulting in a quality deficiency. Misuses can be countered by means of countermeasures, which are requirements on a system, its development, maintenance or operation, which support quality goals. Countermeasures are aimed at detecting, preventing or mitigating misuse cases.

7 Privacy Ontology

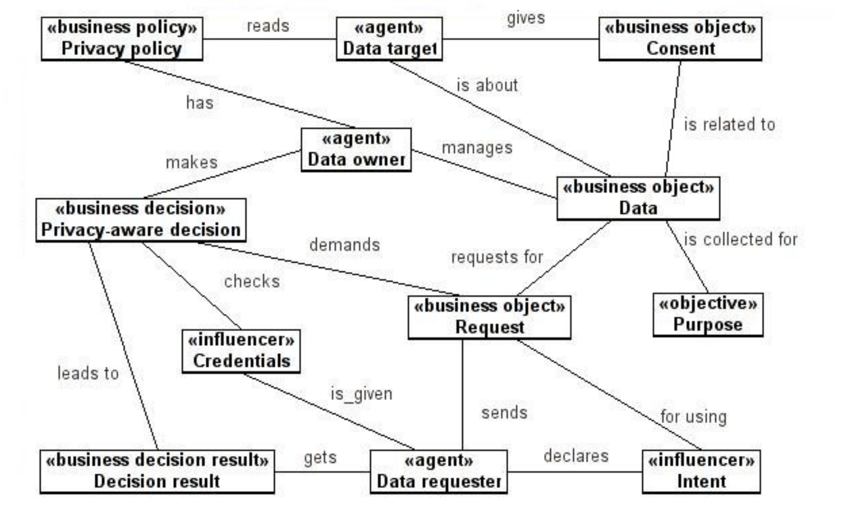

Fig. 5. Excerpt from Privacy Ontology

In this global age, when more and more enterprises are conducting business via the Internet and other electronic media, also privacy and information security come to the forefront. Of these two important non-functional aspects we consider in this section issues related to privacy of information and data that an enterprise processes. Every enterprise has to be aware of the governing privacy laws, privacy recommendations [16, 14] and its own policy on how it will handle requests for data/information. For example, if the enterprise is requested for some specific data regarding some person or enterprise, it is the onus of the enterprise owning this data to take a privacy-aware decision based on the background of who is sending the request, and for what purpose the request is being made. To give an example, if the enterprise is given a request for a photograph of one of its own employees, it is the duty of the enterprise to check (a) if it has a policy that it may give out such photographs to external agencies without the permission of the employee (whose photograph it is) or check if the employee has given her consent on an external access on the photograph, (b) check the credentials of the agency making such a request, and (c) assess the stated use (intent) of the requester. The privacy ontology in Figure 5 deals primarily with the non-functional aspect of how data in information systems are used in specific contexts. Every organisation should have a privacy policy that protects the data(business object) which is owned by the data owner(agent). Note that the business object and agent(actor) are the concepts identified from our Common NFA Ontology (Figure 1)- Another actor in this ontology is the Data Requester, who is the actor who wishes to procure the data and use it for a specific purpose. The data that is requested is usually about some actor, agent, or business enterprise. In our model, these are modeled as the Data Targets. The story begins with the Data Owner collecting the data about the data targets for a stated purpose(objective). The data target has to give its consent on how the data can be used, so that no privacy laws, regulations etc. are violated. The Consent may be stereotyped as a Business Object , and the process by which data target gives its consent as a business process. The Data owner has a privacy policy that it follows whenever a Data requester sends in a Request for Data. The Data requester sends a Request (stereotyped as a Business Object and also states his Intent for the use of the requested Data. The Intent is modelled as an Influencer. The Data owner, on receipt of the request makes a Privacy-aware decision, modelled as a business decision, processing the request based on the privacy policy, the Consent of the Data target, and the credentials and the stated intent of the Data requester. Also the Purpose the data was originally collected for can influence the privacy-aware decision. The Privacy-aware decision result, stereotyped as a business decision result, can be either request granted or denied. The Data requester is informed of the subsequent decision.

8 Discussion of Results

In this paper, we have discussed only the overview of the individual sub ontologies. Hence detailed description of all the concepts, their usage has not been in the scope. A detailed technical description of each individual NFA ontology will be discussed in separate papers. The Common NFA is still evolving and this process is visualized to be an iterative one. Some of the future work envisioned are:

- To incorporate all non-functional aspects sub-ontologies.
- To carry out field studies and apply the proposed set of ontologies in other domains.
- To align with business process modelling and other efforts at enterprise interoperability.

9 Conclusion

As stated in Section 1, our objective was to establish a shared explicit model for non-functional aspects. In this paper, we have elucidated on the top level generic ontology, Common Non-Functional Ontology. We have illustrated its utility by means of some individual non-functional ontologies. Our next step is to put forward specific details and descriptions of each sub- ontology along with instantiated facts from our ongoing case study analysis. The Common NFA and its related sub-ontologies, shall form a knowledge base which can be used for fostering interoperability, and resuse across enterprise systems.

References

1. INTEROP-NoE Task Group 7. Roadmap for tg7: Interoperability challenges of trust, confidence, security and policies, 2005. URL `http://interop-noe.org/backoffice/deliv/DTG7.1/`.
2. A. De Nicola and M. Missikoff. A proposal for a unified process for ontology building: Upon. In *Lecture Notes in Computer Science, Volume 3588,Pages 655 – 664*. Springer Verlag, 2005.
3. M. Fernandez, A. Gomez-Perez, and N. Juristo. Methontology: From ontological art towards ontological engineering. In *Proceedings of Symposium on Ontological Engineering of AAAI Stanford, California*, 1997.
4. Object Management Group. Business motivation model (bmm) specification. draft adopted specification 2006-07-01. http://www.omg.org/docs/dtc/06-07-01.pdf, 2006.
5. TR. Gruber. Toward principles for the design of ontologies used for knowledge sharing. In *Presented at the Padua workshop on Formal Ontology, March 1993*, 1993.
6. N. Guarino. Formal ontology and information systems. In *Proceedings of Formal Ontology and Information Systems(FOIS 1998), pp-3–15*. IOS Press, 1998.

7. A. Herrmann and B. Paech. Quality misuse. In *Workshop on Requirements Engineering for Software Quality(RFSQ),Foundations of Software Quality,pp 193–199*. Essener Informatik Berichte, 2005.
8. A. Herrmann, J. Rueckert, and B. Paech. Exploring the interoperability of web services using moqare. In *Proceedings of First International Workshop on Interoperability Solutions to Trust, Security, Policies and QoS for Enhanced Enterprise Systems(IS-TSPQ)*, 2006.
9. I. Jacobson, G. Booch, and J. Rumbaugh. *The Unified Software Development Process.* Addison Wesley, USA, 1999.
10. V. Kabilan and P. Johanesson. Semantic representation of contract knowledge using multi-tier contract ontology. In *Proceedings of Semantic Web and Databases workshop, (SWDB 2003)*, 2003.
11. V. Kabilan and H. Weigand. Value-model based risk assessment and contract drafting. In *Proceedings of First International Workshop on Interoperability Solutions to Trust, Security, Policies and QoS for Enhanced Enterprise Systems(IS-TSPQ)*, 2006.
12. D. Harrison McKnight and Norman L. Chervany. Trust and distrust definitions: One bite at a time. In *Trust in Cyber-societies: Integrating the human and artificial perspectives*, volume LNCS 2246/2001, pages 27–54. Springer-Verlag, 2001.
13. N. Noy and DL. McGuiness. Ontology development 101: A guide to creating your first ontology. Technical report, Stanford University, 2001.
14. Working Party on Information Security OECD and Privacy. Privacy online: policy and practical guidance. Technical report, OECD, 2003.
15. Sini Ruohomaa and Lea Kutvonen. Trust management survey. In *Proceedings of the iTrust 3rd International Conference on Trust Management, 23–26, May, 2005, Rocquencourt, France*, pages 77–92. Springer-Verlag, LNCS 3477/2005, May 2005.
16. European Union. Directive 95/46/ec. The Official Journal of The European Communities, 1995.
17. M. Uschold and M. Gruninger. Ontologies principles, methods and applications. *The Knowledge Engineering Re-view 11(2): 93–136*, 1996.
18. Lea Viljanen. Towards an ontology of trust. In *Proceedings of the 2nd International Conference on Trust, Privacy and Security in Digital Business (TrustBus'05)*, 2005.