

D'AUBETERRE, FERGLE, Ph.D. A Design Theory for Secure Semantic eBusiness Processes (SSeBP). (2008)

Directed by Dr. Rahul Singh and Dr. Lakshmi Iyer. 214 pp.

This dissertation develops and evaluates a Design theory. We follow the design science approach (Hevener, et al., 2004) to answer the following research question: *“How can we formulate a design theory to guide the analysis and design of Secure Semantic eBusiness processes (SSeBP)?”* Goals of *SSeBP* design theory include (i) unambiguously represent information and knowledge resources involved in eBusiness processes to solve semantic conflicts and integrate heterogeneous information systems; (ii) analyze and model business processes that include access control mechanisms to prevent unauthorized access to resources; and (iii) facilitate the coordination of eBusiness process activities-resources by modeling their dependencies.

Business processes modeling techniques such as Business Process Modeling Notation (BPMN) (BPMI, 2004) and UML Activity Diagrams (OMG, 2003) lack theoretical foundations and are difficult to verify for correctness and completeness (Soffer and Wand, 2007). Current literature on secure information systems design methods are theoretically underdeveloped and consider security as a non-functional requirement and as an afterthought (Siponen et al. 2006, Mouratidis et al., 2005).

SSeBP design theory is one of the first attempts at providing theoretically grounded guidance to design richer secure eBusiness processes for secure and coordinated seamless knowledge exchange among business partners in a value chain. *SSeBP* design theory allows for the inclusion of non-repudiation mechanisms into the

analysis and design of eBusiness processes which lays the foundations for auditing and compliance with regulations such as Sarbanes-Oxley.

SSeBP design theory is evaluated through a rigorous multi-method evaluation approach including descriptive, observational, and experimental evaluation. First, *SSeBP* design theory is validated by modeling business processes of an industry standard named Collaborative Planning, Forecasting, and Replenishment (CPFR) approach. Our model enhances CPFR by incorporating security requirements in the process model, which is critically lacking in the current CPFR technical guidelines. Secondly, we model the demand forecasting and capacity planning business processes for two large organizations to evaluate the efficacy and utility of *SSeBP* design theory to capture the realistic requirements and complex nuances of real inter-organizational business processes. Finally, we empirically evaluate *SSeBP*, against enhanced Use Cases (Siponen et al., 2006) and UML activity diagrams, for informational equivalence (Larkin and Simon, 1987) and its utility in generating situational awareness (Endsley, 1995) of the security and coordination requirements of a business process.

Specific contributions of this dissertation are to develop a design theory (*SSeBP*) that presents a novel and holistic approach that contributes to the IS knowledge base by filling an existing research gap in the area of design of information systems to support secure and coordinated business processes. The proposed design theory provides practitioners with the meta-design and the design process, including the system components and principles to guide the analysis and design of secure eBusiness processes that are secure and coordinated.

A DESIGN THEORY FOR SECURE SEMANTIC EBUSINESS PROCESSES (SSEBP)

by
Fergle D'Aubeterre

A Dissertation Submitted to
The Faculty of The Graduate School at
The University of North Carolina at Greensboro
in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

Greensboro
2008

Approved by

Rahul Singh, Ph.D.

Committee Co-Chair

Lakshmi Iyer, Ph.D.

Committee Co-Chair

To my wife, *Neliana*, daughter, *Ana Sofia*, and family. For their support, encouragement, and patience

APPROVAL PAGE

This dissertation has been approved by the following committee of the Faculty of The Graduate School at the University of North Carolina at Greensboro.

Committee Co-Chair: _____

Committee Co-Chair: _____

Committee Members: _____

Date of Acceptance by Committee

Date of Final Oral Examination

ACKNOWLEDGEMENTS

I would like to thank my advisors Dr. Rahul Singh and Dr. Lakshmi Iyer for their guidance, support, and patience. Dr. Singh has taught me that good research must address relevant problems while maintaining theoretical soundness. From Dr. Iyer I have learned the importance of tackling research problems from different angles. They have been encouraging mentors and supporting friends and I hope to maintain their friendship for a long time.

I want to express my gratitude to all my committee members, Dr. Ruth King, Dr. A. F. Salam, and Dr. Richard Ehrhardt, for their time, support, and critical suggestions in the development of this research. Special thanks are in order to Barry Marcus and Lynne Hammer. Without their help, accessing the right information would have been a difficult activity. I want to thank my classmates, faculty members, and staff at the Information Systems and Operations Management department for their support and friendship.

I would like to acknowledge and thank my wife Neliana, for her unconditional support and understanding. I am indebted to her for the wonderful job she has done as a wife and mother. Without her by my side, I would not have been able to achieve my personal and academic endeavors. I am grateful for my little princess, Ana Sofía, who gives me the inspiration to keep trying and never give up. Also, I would like to express my gratitude to my parents and family for their love and constant support during my life. Finally, my sincere thanks to Dr. Rebeca Torres-Rivera, Sra. Sue C. Herman, Roxana Vargas, and all of those people that helped our family during this voyage toward a better future.

TABLE OF CONTENTS

	Page
LIST OF TABLES	vii
LIST OF FIGURES.....	viii
CHAPTER	
I. INTRODUCTION.....	1
1.1. Research Problem and Its Importance.....	2
1.2. Research Question.....	5
1.3. Research Evaluation.....	7
1.4. Research Contributions.....	8
1.5. Dissertation Organization.....	9
II. THEORETICAL FOUNDATIONS.....	10
2.1. Design Science Paradigm.....	10
2.2. Kernel Theories.....	15
2.2.1. Kernel Theories for the Application Knowledge Domain.....	16
2.2.2. Kernel Theories for the Information Systems Knowledge Domain.....	36
III. DESIGN OF SECURE SEMANTIC EBUSINESS PROCESSES DESIGN THEORY.....	57
3.1. Meta-Requirements for a Secure Semantic eBusiness Processes Design Theory.....	57
3.2. Meta-Design for a Secure Semantic eBusiness Processes Design Theory.....	58
3.3. Design Method for a Secure Semantic eBusiness Processes Design Theory.....	65
3.3.1. Design Process for a Secure Semantic eBusiness	

Processes Design Theory	67
IV. EVALUATION OF THE SECURE SEMANTIC EBUSINESS PROCESS DESIGN THEORY	70
4.1. Descriptive Evaluation of the Secure Semantic eBusiness Processes Design Theory	74
4.1.1. Collaborative Planning, Forecasting, and Replenishment (CPFR) Approach	74
4.2. Observational Evaluation of the Secure Semantic eBusiness Processes Design Theory	86
4.2.1. Applying the Secure Semantic eBusiness Processes Design Theory: A Case Study	87
4.3. Experimental Evaluation of the Secure Semantic eBusiness Process Design Theory	102
4.3.1. Research Model	104
4.3.2. Experimental Design.....	107
4.3.3. Data Analysis	121
V. CONCLUSION	140
5.1 Implications	147
5.1.1. Theoretical Implications	147
5.1.2. Practical Implications	148
5.2. Limitations	152
5.3. Future Research	155
REFERENCES.....	158
APPENDIX A. CPFR PARTNERSHIPS.....	173
APPENDIX B. DESCRIPTION LOGICS.....	175
APPENDIX C. IRB APPROVAL.....	179
APPENDIX D. EXPERIMENT MATERIAL.....	183

LIST OF TABLES

	Page
Table 1. Dependencies among multiple resources and multiple activities	26
Table 2. Kernel Theories from the Application Domain applied in SSeBP.	36
Table 3. Enriched- Use Case (Adopted from Siponen et al., 2006).....	52
Table 4. Kernel Theories from the IS Knowledge Domain applied in SSeBP.	56
Table 5. DL Representation of concepts and relationships in the SSeBP model.....	61
Table 6. Graphical Representations for an SSeBP	69
Table 7. CPFR Business Processes (Source: CPFR Technical Specifications, VICS 1999)	77
Table 8. Security analysis for role-activity-resource permissions for the CPFR's generate order business process	82
Table 9. Security Analysis for role-activity-resource permissions for the <i>Organization</i> <i>A's Create Order Forecast and Generate Order processes</i>	94
Table 10. Experimental Design.....	114
Table 11. Sample Sizes Used in Literature	116
Table 12. Gender Distribution.....	122
Table 13. Age Distribution.....	122
Table 14. Educational Level Distribution	123
Table 15. Primary Occupation Distribution	123
Table 16. Level of Experience using System Development Methodologies (SDM)	124
Table 17. Level of Experience using UML- Activity Diagrams	124
Table 18. Level of Experience using UML- Use Case	125
Table 19. Descriptive Statistics for the Enriched-Use Case combined with UML-Activity Diagram.....	126
Table 20. Descriptive Statistics for the SSeBP Design artifacts	126
Table 21. Results for the subjects' perceptions about the two methods	127
Table 22. Test of hypotheses summary	132
Table 23. SSeBP Design Theory Evaluation Results.....	139
Table 24. A Design Science approach for SSeBP.....	146

LIST OF FIGURES

	Page
Figure 1. Components of a Design Theory (Adapted from Walls et al. 1992; Khatri et al., 2006; and Vaishnavi et al. 2006).....	11
Figure 2. Summary of Relevance// Rigor of this Research (Adapted from Hevner et al. 2004)	14
Figure 3. The Secure Semantic eBusiness Process Design Theory (adopted and extended from Singh and Salam, 2006 and Kishore et al., 2006)	60
Figure 4. Coordinates Relationships between Activities and Resources	63
Figure 5. <i>Permits</i> Relationships	64
Figure 6. Create Order Forecast and Generate Order Processes Data Flow (Adapted from CPFR Technical Specifications, VICS 1999)	79
Figure 7. Consistency and Integrity Checks Results.....	80
Figure 8. Semantic activity-resource coordination in <i>Create Order Forecast/Generate Order Processes</i>	84
Figure 9. Organization A's Semantic activity-resource coordination For Generate//Create Order Forecast.....	95
Figure 10. Research Model to Test Security Awareness	105
Figure 11. Enriched- Use Case for the “create order forecast” business process	108
Figure 12. UML- Activity Diagram for the “create order forecast” business process.....	109
Figure 13. SSeBP Role-Activity-Resource Permissions for the “create order forecast” business process.....	111
Figure 14. SSeBP Secure Activity Resource Coordination for the “create order forecast” business process.....	112
Figure 15. SSeBP Design Theory Kernel Theories.....	141

CHAPTER I

INTRODUCTION

In this global economy, the unit of competition is no longer a single organization but a network of collaborating organizations that have the common business goal of creating valuable customer propositions. Inter-organizational business processes allow collaborating organizations to provide complementary services through networks of collaborating organizations (Sawhney and Parikh, 2001; Dyer, 2000). Organizations engaged in collaborative inter-organizational business processes need to share information and knowledge to increase their partners' knowledge base and competitiveness (Raghu and Vinze, 2007; Tallman et al., 2004; Loebecke et al., 1999; Lorange, 1996). In this context, the resource-based view of the firm with focused capabilities is replaced by a network of organizations with a focal enterprise that coordinates resources of collaborating organizations to execute eBusiness processes (Sawhney and Parikh, 2001). Organizations require that their business processes can exchange information and knowledge resources in a secure and coordinated manner within and across partner organizations.

As organizations become increasingly distributed, their reliance on inter-organizational information flows with partner organizations is integral to any eBusiness

processes. Cooperative inter-organizational knowledge sharing can increase partners' knowledge base and competitiveness. This view is consistent with the knowledge-based view of the firm (Grant, 1996). For this research, the view that information and knowledge sharing occurs in a Business Process context is adopted (Raghu and Vinze, 2007; Singh and Salam, 2006).

1.1. Research Problem and Its Importance

In establishing an agenda for IT research in heterogeneous and distributed environments, March et al. (2000) recognize the complexity involved in sharing knowledge in business organizations. Organizations engaged in collaborative inter-organizational processes continue to deal with several issues related to the seamless flow of information and knowledge resources in an eBusiness Process. For instance, fragmented and heterogeneous IT infrastructures negatively affect the information flows and activity coordination among business partners (Rai et al., 2006; Barua et al. 2004; Sambamurthy et al. 2003). Interoperability problems arise from the lack of standards to describe products and services, business processes, and security policies that guide access to information and knowledge resources. These create difficulty in integrating heterogeneous systems within and across organizations. The lack of interoperability standards and supporting technologies make collaborating organizations expend considerable resources to avoid interoperability problems. A 2004 NIST study estimated annual interoperability costs for all business data flows among companies in the

transportation, electronic, and construction/building management supply chains to be \$5 billion, \$3.9 billion, and \$15.8 billion, respectively. These frequently lead to inter-organizational processes to be performed outside the systems. Semantic interoperability is one of the most important research issues in the context of heterogeneous and distributed systems and still represents technical challenges that prevent collaborative organizations from sharing knowledge.

Likewise, it has been recognized that information security and systems integration are among the key issues for IT executives (Luftman et al., 2006). Semantic interoperability problems frequently lead to inter-organizational information and knowledge exchange being done manually and outside the systems for both routine processes and problem resolution (van der Aalst and Kumar, 2003). Without the appropriate security controls for these manual interventions, they lead to unauthorized access of resources. The 2006 CSI/FBI Computer Crime and Security Survey identifies that authorization violations are the second largest cause of economic losses (Gordon et al., 2006). The lack of appropriate access control mechanisms on the information and knowledge exchange among business activities leaves organizations vulnerable to various information assurance threats and prevents them from engaging in collaborative eBusiness processes. Unfortunately, those issues still remain open and prevent organizations from realizing the benefits of seamless flow of information and knowledge resources in an eBusiness process.

Coordinating complex inter-organizational processes requires knowledge-driven coordination structures to determine knowledge sources and decision authority (Anand

and Mendelson, 1997). Similarly, a central issue in inter-organizational knowledge sharing is the nature of the knowledge exchange, including what knowledge is to be shared and under what conditions (Loebecke et al., 1999). Given the risks associated with knowledge sharing, it can only take place in a secure environment. Research on security of distributed business processes lacks an integrative business process perspective on secure information and knowledge sharing (Oh and Park, 2003). Local security policies are not designed for distributed resource sharing. Global policies do not consider impediments to local access control of resources (Sandhu et al., 1996). Centralized mechanisms fail to capture the distributed nature of systems support required for inter-organizational business processes. Extant literature does not *explicitly* consider or systematically represent *component knowledge* of resources such as descriptions of product knowledge and skills; *process knowledge* including process workflow models and coordination structures; and *security knowledge* of authorized access for activities to resources within and across organizations. A holistic consideration of *component*, *process* and *security* knowledge in the design of information systems to support secure and coordinated business processes is critical to inter-organizational eBusiness processes.

Software engineering methodologies conceptualize security requirements as non-functional requirements (Mouratidis et al., 2005). They do not fully integrate security in all systems development phases (Lee et al., 2002; Apvrille and Pourzandi, 2005). This creates a gap between systems development and security of systems (van Wyk and McGraw, 2005). Systems development methodologies incorporate security requirements as an afterthought at the implementation stage, resulting in a less secure system

(Choobinedh et al., 2007). Information systems methodology that includes security aspects in all stages is still needed (Baskerville, 1988). Siponen et al. (2006) argue that existing secure information systems design methods fail to satisfy secure systems design requirements and proposed a design theory for secure information systems (SIS) design methods. They identify a meta-notation to incorporate security policies and restrictions to enhance use-case descriptions. There is a need for theoretical grounded IS security methods and tools (Choobinedh et al., 2007). Soffer and Wand (2007) state that existing process modeling techniques are driven by practice and lack of theoretical principles, which impede the verification of the "correctness" of process models. Soffer and Wand (2007) propose a goal-driven multi-process analysis approach that is based on the Generic Process Model (GPM) to design and analyze processes; however, their approach fails to incorporate eBusiness processes security requirements and component knowledge into the eBusiness process analysis and modeling. Existing methods in the design of secure information systems lack a conceptualization of secure business process.

1.2. Research Question

Design science is a problem-solving paradigm that enhances understanding of a problem domain by developing purposeful design artifacts that address important and relevant organizational problems (Hevner, et al., 2004). Design theories are normative theories that provide guidance to practitioners to effectively develop new systems and inform researchers by suggesting testable research hypotheses (Markus et al., 2002). Design theories must be based on kernel theories and must be evaluated to demonstrate

their quality and utility to solve relevant problems in the problem domain (Walls et al. 1992; Hevner et al. 2004). Current literature on secure information systems design methods is theoretically underdeveloped (Choobinedh et al., 2007) and does not meet the goals of a secure information systems design method (Siponen et al. 2006). Moreover, business processes modeling techniques such as Business Process Modeling Notation (BPMN) (BPMI, 2004), Event-Driven Process Chains Diagrams (EPC) (Scheer, 1999) and the UML Activity Diagrams (OMG, 2003) lack of theoretical foundations; as a result, the verification of the resultant business processes is difficult to attained (Soffer and Wand, 2007).

This dissertation develops and evaluates a *Design theory*. Specifically, we follow a design science approach to answer the following research question: *How can we formulate a design theory to guide the analysis and design of Secure Semantic eBusiness processes?* The proposed Secure Semantic eBusiness Processes (SSeBP) design theory provides design principles, including modeling concepts and grammar, for the design and development of secure eBusiness processes. The goals of *SSeBP* design theory are to unambiguously represent information and knowledge resources involved in eBusiness processes to solve semantic conflicts and to integrate heterogeneous information systems; to enable the analysis and modeling of access control mechanisms to prevent unauthorized access to resources; and, to facilitate the coordination of eBusiness process activities-resources by modeling their dependencies. The design theory proposed in this dissertation is the first attempt in providing theoretically grounded guidance to design richer secure eBusiness processes for secure seamless knowledge exchange among

business partners of a value chain. *SSeBP* design theory is well grounded in kernel theories and is evaluated using a rigorous approach.

1.3. Research Evaluation

The proposed Secure Semantic eBusiness Processes (SSeBP) design theory is evaluated through a multi-method evaluation approach that includes descriptive, observational, and experimental evaluation. First, principles and knowledge representation mechanisms of SSeBP design theory are applied to critical business processes of an industry standard named Collaborative Planning, Forecasting, and Replenishment (CPFR). SSeBP design method is used to analyze CPFR business processes and to show how CPFR models can be mapped and enhanced by the application of the SSeBP design theory. Second, SSeBP design theory is applied to a case study to illustrate the applicability of SSeBP design theory to map real core business processes of an organization to resolve semantic conflicts and enable the exchange of component, process and security knowledge. Finally, using situational awareness theory (Endsley, 1995) SSeBP artifacts are empirically evaluated against the Enriched-Use Case (Siponen et al., 2006) and standard UML activity diagram. A detailed experimental design and hypotheses that demonstrates the utility of SSeBP is described. Hypotheses that establish informational equivalence (Larkin and Simon, 1987) and measure the level of security awareness generated by the SSeBP design theory are formulated and tested.

1.4. Research Contributions

Specific contributions of this dissertation are to develop a design theory (SSeBP) that presents a novel and holistic approach that contributes to the IS knowledge base by filling an existing research gap in the area of design of information systems to support secure and coordinated business processes. SSeBP provides practitioners with the modeling concepts and grammar and with the design process, including the system components and principles to guide the crafting of secure eBusiness processes that are semantically rich, highly coordinated and seamlessly integrated. SSeBP design theory presents an integrative approach that contributes to the IS knowledge base by filling an existing research gap in the area of design of information systems to support secure and coordinated business processes. We demonstrate how SSeBP utilizes emerging technologies to solve semantic conflict issues, to prevent unauthorized access to resources, to foster knowledge exchange, and to integrate heterogeneous systems.

Organizations will benefit from SSeBP in several ways. SSeBP design process provides organizations a set of principles and procedures to analyze and design secure eBusiness process. These facilitate the management of analysis and development activities and will result in more secure eBusiness processes. SSeBP allows management to analyze and define the relationships between organizational roles and the activities that they perform. This leads to assurance of segregation of duty in the context of eBusiness processes. SSeBP enables information and knowledge resources to be represented in a standard and unambiguous machine readable format. Common ontologies provide the foundation for semantic conflict resolution and seamless flow of information and

knowledge among heterogeneous systems involved in an eBusiness process. In SSeBP, roles specify organizational functions responsible for specific activities. This allows for the inclusion of non-repudiation mechanisms into the analysis and design of eBusiness processes. Non-repudiation mechanisms lay the foundations for auditing, which is needed for compliance with regulations such as Sarbanes-Oxley and HIPAA.

1.5.Dissertation Organization

The dissertation is organized following design science research guidelines (Hevner et al., 2004; Walls et al., 1992). Chapter two presents the theoretical foundations including the description of the research method, and the kernel theories from the problem domain and the IS application domain. In Chapter three, the SSeBP design theory is developed, including the conceptual SSeBP meta-requirements; the SSeBP meta-design; and the SSeBP design method. Chapter four presents the evaluation design for assessing the utility of the proposed design theory. Finally, chapter five summarizes the main aspect of the *SSeBP* design theory, and presents the theoretical and practical implications, limitations of the study, and directions for future research.

CHAPTER II

THEORETICAL FOUNDATIONS

This chapter presents the design science paradigm based on the perspectives of Walls et al. (1992), Hevner et al. (2004), March and Smith (1995) and Vaishnavi et al. (2006). It also establishes the *SSeBP* design theory's kernel theories from the application domain and for the IS Knowledge Domain.

2.1.Design Science Paradigm

The design science paradigm has its roots in the engineering and the sciences of the artificial (Simon, 1996). Design science research addresses classes of problems that solve relevant and unsolved problems, or solve problems in a more effective and efficient manner. In other words, design science is a fundamentally problem-solving paradigm (Hevner et al., 2004). Design theory is a prescriptive theory that integrates normative and descriptive theories into design paths to produce the artifact (Walls et al., 1992). A design theory includes the design product or artifact and design process to produce it (Walls et al., 1992). Figure 1 describes the components of a design theory.

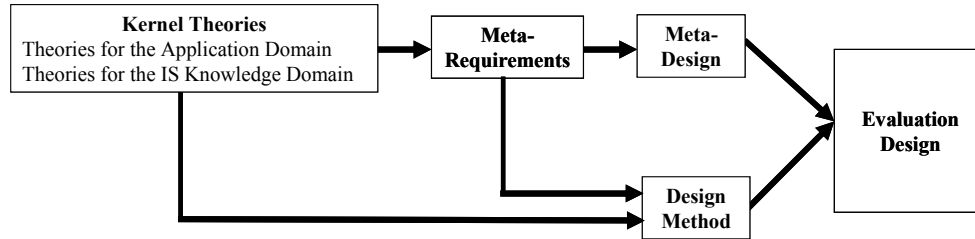


Figure 1. Components of a Design Theory (Adapted from Walls et al., 1992; Khatri et al., 2006; and Vaishnavi et al., 2006)

Walls et al. (1992, p. 42) state that “design” is both a noun and a verb and therefore design is both a product and a process. Design as a product can be defined as “a plan of something to be done or produced”. In the context of IS design science research that product is the IT artifact. Design as a process can be defined as “to so plan and proportion the parts of a machine or structure that all requirements will be satisfied”. In other word the process is the method used to produce the IT artifact in a way that the meta-requirements are satisfied.

Hevner et al., (2004) note the similarity between a *design artifact* and *IS Design Theory* (Walls et al., 1992). The meta-design describes a class of artifacts and a set of systems principles to select systems features that meet meta-requirements (Markus et al., 2002). Kernel theories from the application domain are applied, modified and/or extended (Hevner et al. 2004) to develop the theoretical basis for the meta-requirements and meta-design. Markus et al. (2002) refer to design process as principles that guide artifact development.

Gregor (2006) identifies the nature of theory in IS research and develops a taxonomy for classifying IS theories. Based on the goals of the theories (i.e.: analysis and description, explanation, prediction, and prescription), Gregor classifies IS theories into five types of theories namely theory for analyzing, theory for explaining, theory for predicting, theory for explaining and predicting, and theory for design and action. In particular, we are interested in the characteristics of theory for design and action since in this research we attempt to develop a design theory for Secure Semantic eBusiness processes. According to Gregor, design and action theories provide explicit prescriptions (e.g.: methods, techniques, principles of form and function) for constructing an artifact. We refer the interested reader to Gregor (2006) for a detail description of each theory type. A design theory can be understood as solutions for specialized classes of IS problems (Markus et al., 2002; Walls et al., 1992). These solutions are constructed artifacts that address “wicked problems” (Hevner et al., 2004). In order to consider a design theory to be complete, it has to exhibit the following set of characteristics (Walls et al, 1992):

- 1) *Design theories must deal with goals as contingencies*
- 2) *A design theory can never involve pure explanation or prediction*
- 3) *Design theories are prescriptive*
- 4) *Design theories are composite theories which encompass kernel theories from natural science, social science and mathematics*
- 5) *While explanatory theories tell "what is", predictive theories tell "what will be", and normative theories tell "what should be", design theories tell "how to/because"*
- 6) *Design theories show how explanatory, predictive, or normative theories can be put to practical use.*
- 7) *Design theories are theories of procedural rationality (Simon 1981)*

Hevner et al. (2004) propose a conceptual framework for understanding, executing, and evaluating IS research combining behavioral-science and design-science paradigms. The framework involves the following components:

- i) Environment: it defines the scope of the problem domain. It includes organizations, technology, and people.
- ii) IS Research: it is conducted by applying behavioral science, through the use of theories that explain or justify the business problem, and design science to address the building and evaluation of artifacts designed to meet the identified business need.
- iii) Knowledge Base: it encompasses all the theoretical foundations, including the research methodologies and the kernel theories.

Basically, Hevner et al. (2004) propose a research cycle that involves the identification of a relevant business problem that is solved by designing an IT artifact, which is evaluated using the appropriate methods and context; so that new addition to the IS knowledge base and environment can be done. Now, we apply Hevner et al. (2004) framework for information system research to show (figure 2) how our research is both relevant and rigorous and contribute to the IS knowledge base by solving an important kind of business problem.

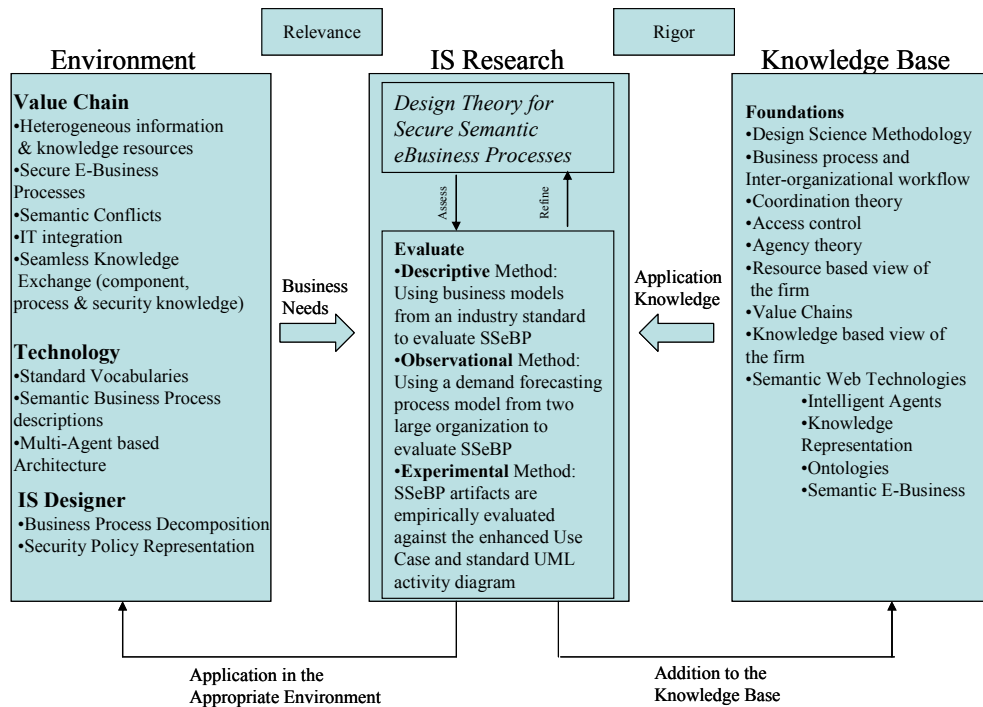


Figure 2. Summary of Relevance// Rigor of this Research (Adapted from Hevner et al. 2004)

Benbasat and Zmud (2003) suggest that the IT artifact and its immediate nomological network should be the core of IS research. Hevner et al. (2004) highlights that the main contribution of design science research is the IT artifact per se. Several controversial IT artifact definitions exist in the literature. We refer the interested reader to Alter (2006) for a compendium of IT artifact definitions. Recently, Baskerville et al. (2007) state that the IT artifact is the instantiation of a design theory. In a more broadly sense, Hevner et al. (2004, pp. 77) define an IT artifact as “constructs (vocabulary and symbols), models (abstraction and representations), methods (algorithms and practices), and instantiations (implemented and prototype systems)”. In this research, we adopt the

Hevner et al. (2004) IT artifact definition and argue that a design theory must provide constructs, models, or methods that guide the design and instantiation of novel IT artifacts. As a sidebar, Baskerville et al. (2007) emphasize the importance that design theories represent for the IS field, and as many other IS researchers (e.g.: Hevner et al., 2004; Gregor, 2006; Benbasat and Zmud, 2003), they argue that design science research is receiving a lot of attention because it is conceived as one of the way to address the issues related to “the small degree of utilization [of IS research by the practitioner community] and relevance of IS research”.

In this research, the perspectives of Walls et al. (1992), Hevner et al. (2004), March and Smith (1995) and Vaishnavi et al. (2006) are integrated in developing a design theory for Secure Semantic eBusiness Process (SSeBP) needed to guide the design and analysis of secure eBusiness processes. The following sections present the theoretical foundations from the kernel theories for the application domain and for the IS Knowledge Domain.

2.2. Kernel Theories

It has been recognized that knowledge resources must be shared to be useful and applicable (Raghu and Vinze, 2007). When knowledge is exchanged in a systematically way, it might increase collaborating partners’ knowledge base and their competitiveness (Loebecke et al. 1999). The knowledge-based view of the firm (Grant, 1996) considers knowledge as a strategic resource. Integrating information and knowledge resources

across a value chain requires secure access to preserve local security access control (SAC) requirements and autonomy. Activities of organizations are inter-connected and require multiple constraints for appropriate access control to information resources (Oh and Park, 2003). Current inter-organizational integration models suffer from a lack of knowledge sharing in a secure coordinated manner (Singh et al., 2005). In the proposed design theory for Secure Semantic eBusiness Processes (SSeBP), the central unit of analysis is the eBusiness processes, which span within and across organizations. SSeBP considers information and knowledge as the primary resources pertinent to the problem domain. SSeBP incorporates coordination of *component knowledge*, *process knowledge* and *security knowledge* for integrated inter-organizational eBusiness processes. Security is an integral part of the value activities of a business enterprise; in SSeBP, security access control (SAC) policies determine an activity's access to resources.

2.2.1. Kernel Theories for the Application Domain

Kernel theories from the application domain organize and structure constructs in the application domain, while kernel theories of IS Domain provides the representations and techniques that form the basis for artifact development. IS problem solving applies the IS domain knowledge and concepts to the theories of the application domain and advances knowledge in both domains (Khatri et al., 2006). Theories for the application domain relates to what Hevner et al. (2004) call the “environment”. These provide the “why” and the “what” for the development of SSeBP design theory. In this dissertation, the theories for the application domain include the Resource Based View (RBV) of the

firm, business process and inter-organizational workflows, coordination theory, access control, and situational awareness theory.

2.2.1.1. Resource Based View of the Firm

The resource-based view (RBV) of the firm provides a useful framework to identify resources that provide firms with competitive advantages. The resource-based view of the firm is based on two fundamental assumptions: 1) strategic resources owned by firms are heterogeneous within an industry or group (resource heterogeneity); and 2) such resources may not be perfectly mobile across firms, so that heterogeneity can be long lasting. These two assumptions are used to explain sources of sustained competitive advantage (Barney, 1991). Barney (1991) states that firm's resources can be sources of potential competitive advantages, if they possess the following four attributes: 1) the resources must be *valuable*; 2) they must be *rare* among a firm's current and potential competition; 3) they must be *imperfectly imitable*, and 4) they must be *non-substitutable*. The logic behind the RBV of the firm is that if a firm has a resource that is owned by several other competing firms that resource cannot be a source of competitive advantage. On the other hand, if a firm owns a rare and immobile resource, in the sense that firms without such resource incur in a cost disadvantage when they try to obtain, develop, and use it, in comparison with the firm that already has the resource, then we can say that the firm that possesses that resource can have a sustained competitive advantage (Mata et al. 1995). While the RBV of the firm considered the individual firm as unit of competition, in this research we focus on the *value chain*, where a focal firm is embedded in a network

of collaborating firms that have the common business goal of creating valuable customer propositions. This view is consistent with Porter's framework (1985) of value activities and value chain and it is consistent with Sawhney and Parikh's view (2001) of inter-organizational processes that allow collaborating organizations to provide complementary services through networks of collaborating organizations. Daft (1983) states that "firm resources include all assets, capabilities, organizational processes, firm attributes, information, knowledge, etc. controlled by a firm that enable the firm to conceive and implement strategies that improve its efficiency and effectiveness". In this research, we are interesting in *knowledge resources* and we recognize knowledge as a vital resource that must be shared in a secure and systematically way with partner organizations of a value chain. This view is consistent with the knowledge-based view of the firm (Grant, 1996), which considers knowledge as a strategic resource.

It has been recognized that knowledge resources must be shared to be useful and applicable (Raghu and Vinze, 2007). Knowledge exchange can increase collaborating partners' knowledge base and their competitiveness (Loebecke et al. 1999; Lorange, 1996). Hult et al. (2004) identify that knowledge development and exchange could positively impact supply chain performance. Simonin (1999) studies knowledge transfer in strategic alliances and its impacts on collaborative outcomes and explains that *knowledge ambiguity* negatively affects knowledge transfer. Hamel (1991) identifies that knowledge format is directly related to ease of transfer. Tallman et al. (2004) show that knowledge transferability directly affects firm's performance. Likewise, firms can obtain significant and sustainable improvements in their performance by developing supply

chain process integration capabilities (Rai et al., 2006). It is clear that extant literature recognizes that knowledge exchange and supply chain integration affect firms overall performance and their competitiveness. However, there is a lack of research in the areas of how knowledge exchange can be done in a systematic way and the kind of knowledge that can be shared in the context of an information supply chain. In this context, it is important to understand the nature of the knowledge and how inter-organizational information systems exchange knowledge.

Tallman et al. (2004) examine the role of knowledge exchange for competitive advantage of a cluster of organizations and note that simpler, codified and less tacit *component knowledge* is amenable to knowledge exchange. Raghu and Vinze (2005) highlight that knowledge sharing, when knowledge is not systematically stored, requires of special communication and collaborative mechanisms. Although knowledge exchange is central for inter-organizational collaboration, we recognize that all knowledge cannot be explicated and be effectively represented and reasoned with using decidable and complete computational techniques. This research uses an explicit definition of knowledge declarative enough for standards-based knowledge representation languages and can be processed using agent-based reasoning mechanisms to reach useful inferences. These pragmatic restrictions on knowledge are made for practical reasons to build effective and practical knowledge-based systems that are both viable and useful. We focus on *Component knowledge*, including descriptions of skills, technologies, tangible resources, consumer and product knowledge; and *Process knowledge*, typically embedded in the process models of workflow management systems as coordination

knowledge for complex processes. An inter-organizational eBusiness process view of knowledge integration incorporates management of *component knowledge* and *process knowledge* for knowledge integration across inter-organizational systems.

While cooperative inter-organizational knowledge sharing can increase business partners' competitiveness, organizations are very selective about the nature of knowledge resources shared. When knowledge resources are a primary concern, managing cooperative relationships is frequently a process of managing knowledge flows (Badaracco, 1991). Central to inter-organizational knowledge management (KM) is the nature of the knowledge exchange, what knowledge is to be shared and under what conditions (Loebecke et al., 1999). In this context, SSeBP design theory must consider the nature of the knowledge exchange needed for collaborating organizations to achieve inter-organizational eBusiness processes objectives. In particular, the *SSeBP* design theory must focus on methods for knowledge representation and exchange mechanisms that allow for its appropriate exchange and use in the inter-organizational eBusiness process context. In addition, the SSeBP design theory must support transparent exchange of machine-interpretable and unambiguous knowledge required to develop viable inter-organizational eBusiness relationships. This allows for knowledge to be interpreted by software and shared using automated reasoning mechanisms to reach useful inferences.

The resource-based view (RBV) of the firm (Wernerfelt, 1984) and the knowledge based theory (Grant, 1996) provide a useful framework to identify resources that provide firms competitive advantage. While RBV considers the individual firm as

unit of competition, in this research we focus on business processes in a *value chain*, where a focal firm is embedded in a network of collaborating firms that have the common business goal of creating valuable customer propositions.

In summary, in this dissertation, we complement the RBV of the firm (Barney, 1991), Porter's framework (1985) of value chain, the knowledge-based view of the firm (Grant, 1996), and inter-organizational value chain view (Sawhney and Parikh, 2001) to understand the nature of knowledge exchange in an eBusiness process.

2.2.1.2. Business Process and Inter-organizational Workflow

In this research, we take the view that an eBusiness process is a set of coordinated activities enacted by humans or software agents that exchange knowledge resources to achieve business objectives. This is consistent with extant literature. Davenport and Short (1990, p.12) define business process as “logically related task performed to achieve a define business outcome”. Swaminathan and Tayurs (2003, p. 1380) state that eBusiness process is “a business process that uses the Internet or other electronic medium as a channel to complete business transactions”. eBusiness is an approach to achieving business goals where information and knowledge exchange technology enable business activities in and across organizations and support decision making underlying these activities (Holsapple and Singh 2000). In addition, according to agency theory (Jensen and Meckling, 1976), an agent represents an entity's interests and fulfills responsibilities on its behalf. Therefore, it is essential for an SSeBP design theory to recognize that

eBusiness Processes are the context where relevant information and knowledge exchange occurs so that business goal can be attained and that business enterprises, human actors (agents) or software agents are responsible carry out the various activities to achieve such organizational and system goals.

As organizations become increasingly distributed, their reliance on inter-organizational information and knowledge flows with partner organizations is integral to eBusiness processes. Here workflows establish the logical order of execution between individual business activities in business processes within and across organizations. Inter-organizational workflow generally involves communications among business partners whose information systems are different. In addition, such communications are made difficult due to two facts. First, there is not a single way to represent the information and knowledge to be exchange. Second, partner's process information and knowledge are hidden from each other (van der Aalst and Kumar. 2003). Basu and Kumar (2002) identify that when mapping or translation of data and process information is required, mechanisms that ensure the semantic integrity of the information and rules for mapping it correctly are mandatory. *Process knowledge* represents a business process in a form that consists of a network of activities and their relationships, criteria to indicate the start and the termination of the process, and information about the individual activities, including participants and data, and their coordination (WfMC, 1996). In this context, SSeBP must rely on *Process knowledge* to orchestrate and integrate disparate business activities within and across organizations.

Nowadays, businesses are moving from EDI to Web-based approaches. In fact, many firms have adopted eBusiness model to improve their collaborative capabilities (Segars and Chatterjee, 2003). The reason of such movement is that EDI supports dyadic relationship while web-based approaches enable many-to-many relationships (Wafa et al., 2005). In addition, while organizations can obtain long-term cost saving from EDI, EDI does not provide a strategic advantage (Benjamin et al., 1990). Finally, even though EDI enables the exchange of transactional data among trading partners, EDI does not allow the exchange of detailed process-level information (van der Aalst and Kumar 2003). Here an SSeBP must provide means to seamlessly represent and exchange *Process Knowledge* among trading partners. Although technology such as eXtensive Markup Language (XML) has emerges as the main mechanism to exchange data electronically among trading partners, most workflow-management systems use proprietary formats which prevents exchange of workflow instances between systems of different vendors. In addition, emerging XML standards such the XML Common Business Library (xCBL) by CommerceOne, the Partner Interface Process (PIP) blueprints by RosettaNet, the Universal Description, Discovery and Integration (UDDI), the Electronic Business XML (ebXML) and other initiatives address only the exchange of data among business partners but do not take into account the control flow among them (van der Aalst and Kumar, 2003). Moreover, there is a lack of a unifying model for workflow modeling (Basu and Kumar, 2002). van der Aalst and Kumar (2003) develop a language called eXchangeable Routing Language (XRL), which is based on XML and allows trading partners to describe workflow process schemas to enable flexible documents routing. Here, it is vital

for an SSeBP to enable the exchange of not only data but also information and knowledge resources, including *Component and Process Knowledge*, among trading partners, while flexible control flow mechanisms are provided.

The notion of coordination is embedded in the ideas of workflow and automated workflow management systems since they essentially deal with issues of task-task and task-resource dependencies and their coordination (Kishore et al., 2004). In other words, *workflow* is a *coordinated* set of *business activities* performed by various actors or agents necessary to complete a business process. Coordination requirements need to be met, while activities are executed to achieve a business process. Here, workflows are subsumed in *Process Knowledge* through the coordination relationships between the dependent businesses activities in an eBusiness process. In this dissertation, we posit that inter-organizational workflow and eBusiness processes provide an integrative and holistic framework to integrate and coordinate *knowledge resources*.

2.2.1.3. Coordination Theory

Business processes comprise activities and require coordination mechanisms to manage their dependencies (Malone et al. , 1987). Effective coordination of business activities by managing their inter-dependencies is critical for effective inter-organizational eBusiness processes across the value-chain. Coordinating complex inter-organizational eBusiness processes requires an integrated view of the complete eBusiness process and knowledge-driven coordination to determine decision authority over

distributed knowledge resources (Anand and Mendelson 1997). In this context, for an SSeBP design theory to enable effective inter-organizational eBusiness processes, it must provide coordination mechanisms that effectively manage the dependencies that exist among activities and resources of an eBusiness processes.

Malone et al., (2003), Malone et al.(1999), and Malone and Crowston (1994) develop an interdisciplinary coordination theory drawing from various disciplines including computer science, organization theory, operations research, economics, linguistics, and psychology. They define coordination theory as a *body of principles about how the activities of separate actors can be coordinated* and they define coordination as *managing dependencies among activities*. Malone and Crowston (1994) explain that goals, activities, actors, and interdependencies are the main components of the coordination theory, where actors perform interdependent activities to achieve goals. Such actors face coordination problems derived from the dependencies that constrain how activities can be executed. Activities implement coordination methods to address coordination problems. Two key aspects of coordination theory are the processes of goal selection and goal decomposition. Here, a process of choosing a goal is followed by decomposing that goal into activities such that the selected goal can be attained (i.e.: top-down goal decomposition) (Malone and Crowston, 1994).

Malone et al., (2003) provide a taxonomy of dependencies among activities and resources. Dependencies among multiple resources and multiple activities are shown in Table 1 adapted from Malone et al. (2003). Here, Malone et al. (2003) defines resources as anything that can be used or affected by activities.

Dependency Type	Description
<i>Flow Dependency</i>	A resource is the effect of one activity and a precondition of another, typical of producer/consumer dependence where a resource may either be produced by or consumed by a business activity.
<i>Fit Dependency</i>	Two activities result in a common resource, e.g., two or more parts must ‘fit’ to produce the end product; hence the notion of ‘ <i>fit</i> ’ dependency among activities and output resources.
<i>Sharing Dependency</i>	Two activities have the same resource as a precondition.

Table 1. Dependencies among multiple resources and multiple activities

Crowston and Osborn (2003) identify that dependencies among resources or among activities can exist. First, it is possible that a *simultaneity* dependency exists among tasks when “one task might require the concurrent execution of another task, or several tasks might have to be performed all at the same time”. Second, a *composition* dependency exists when “both tasks and resources can be thought of as forming decomposition hierarchies: higher-level tasks can be decomposed into subtasks and an object into components”. Third, an *integration* dependency exists when the integration of multiple tasks’ results is required to accomplish some effect.

Coordination theory provides an approach to understand and study business processes. Crowston and Osborn (2003) show how coordination theory can be utilized to develop process descriptions and redesign. They develop a technique that involves six steps namely: *setting process boundaries, collecting data, identifying actors and*

resources, identifying activities, identifying dependencies, and verifying a model. Basically, actors, activities and resources are identified; and processes are decomposed into activities so that dependencies among activities and resources are identified and analyzed. The *SSeBP* design theory uses the notion of *activity-resource* dependency where activities have a *sharing, flow* or *fit* dependency with a resource. This notion of the coordination constructs are based on Malone et al. (2003) and are similar to those in van der Aalst and Kumar (2003). *SSeBP* design theory utilizes these coordination constructs to develop the activity-resource coordination in the process knowledge representation of eBusiness processes using semantic technologies.

Complexities of coordinating inter-organizational processes require knowledge-driven coordination structures to determine decision authority and knowledge sources (Anand and Mendelson 1997). Even though access control research is extensive, there is paucity in the research on information assurance of distributed eBusiness processes that provides a holistic, business process perspective (Oh and Park, 2003). Centralized mechanisms for information assurance fail to capture the distributed nature of systems support required for inter-organizational eBusiness processes. An organization will lose its competitive advantage if it fails to protect its externalized knowledge (Lee et al., 2005). In this regard, McGaughey (2002) correctly identifies the types of organizational interventions necessary that is “what” interventions are available but fails to point out the more important issue of “how” such interventions can be realistically achieved specifically for the codified knowledge and information resources in the context of the extended enterprise. Carpenter and Janson (2004) point the need for cooperating

organizations (that want to exchange information and knowledge resources) to be able to specify which of their users should be able to have what rights to access which of their resources under what circumstances.

2.2.1.4. Access Control

Sharing valuable information and knowledge resources entails the risks of possible unauthorized access and usage that may lead to foregone returns on information and knowledge assets. Research has identified that the most common security techniques and/or mechanisms used to overcome information security issues are the following: authentication mechanisms, authorization, access control, data integrity and data confidentiality policies, integrity of transactions and communications, non-repudiation, end-to-end integrity and confidentiality of message, audit trail, and distributed enforcement of security policies. Here, communication security addresses confidentiality and integrity of the data transmitted as well as non-repudiation, while access control addresses authentication, separation of duty (SOD), and delegation (Joshi et al 2001; Oh and Park 2003). The main objective of access control is, based on business rules, to grant or deny the access requested from a particular user. Access control requirements vary from one environment to another. In the enterprise environment, access control must maintain high degree of information sharing and strong confidentiality (Oh and Park, 2003). Moreover, Basu and Kumar (2002) highlight that current workflow systems must incorporate the organizational structure by allowing the representation of rules and policies and ensure that security policies are not breached. In this context, the *SSeBP*

design theory must provide a basis to represent sophisticated access control and security requirements for eBusiness processes. Specifically, the *SSeBP* design theory must incorporate business rules embedded in security policies that govern the access to knowledge resources within in and across of the value chain in the context of eBusiness processes.

Several access control models have been proposed to secure distributed applications. Here we present the main characteristics of the main access control models namely: discretionary access control (DAC) model, the mandatory access control (MAC) model, the role-based access control (RBAC) model, and the task-role-based access control (T-RBAC). Discretionary Access Control (DAC) and mandatory access control (MAC) are the traditional access control models. DAC models use access authorization rules for each subject and object in the system. Even though DAC policies are very flexible and mostly used on Web-based application, they have some security flaws. Under DAC model, data from object can be copied to another object without having the right authorization; as a result, the security of the system is compromised. In the MAC model, predefined sensitivity levels are used to categorize each subject and object. An advantage of the MAC model is that it allows for controlling information flows; so that confidentiality and integrity of the information are guaranteed (Joshi et al., 2001). A drawback of MAC models is the lack of flexibility; therefore, they cannot be applied successfully where trading partners use different security policies and systems.

Regarding the RBAC models, they classify the elements of the system into users, roles, permission, operations, and objects (system resources). The primary benefit of

RBAC over previous security mechanisms such as mandatory access control and discretionary access control is the ability of RBAC to accommodate the changing roles of users. RBAC adds *roles* as a layer of abstraction to simplify the association between *users/actors* (agents) and *permission*. Access control policies that specify users' permissions to specific system resources are defined through the relationships between users, roles and permissions. Sandhu et al. (1996) define a family of RBAC models that include role hierarchies and constraints that allow system administrators to assign users permissions to system resources using roles. Roles are organized and managed using role hierarchies that define the inheritance structure of roles. Role hierarchies for an organization commonly reflect the organizational structures and the hierarchy of responsibility in the organization. Constraints add pragmatic consideration and exceptions to the relationships role hierarchies and are a useful tool in implementing organizational policy for access to system resources (Park et. al, 2001). Because permissions to users are assigned through roles, the administration is made easier (Bhatti et al., 2004). Role-Based Access Control (RBAC) facilitates security administration by allowing organizations to centrally manage and control access to information and processing resources. It is important to mention that the National Institute of Standards and Technology (NIST) adopted RBAC as a National Standard in 2004 (csrc.nist.gov/rbac). Furthermore, the security literature is rich in the mechanisms and extensions of the RBAC (Sandhu, et. al., 1996). However, RBAC does not incorporate the content and context of the information workflow and does not separate task from role (Oh and Park 2003). Here, the *SSeBP* design theory must incorporate roles, permissions,

access, and security of resources: information and knowledge, from a dynamic eBusiness process perspective.

The task-role-based access control (T-RBAC) model extents RBAC into an enterprise environment. Under T-RBAC users are related to permission (access right) through a role and task; permissions are assigned to tasks, and task are assigned to roles. Task is not a sub-role; in fact, four classes of tasks are defined: i) class private (*P*): the permissions for the tasks in the class *P* are non-inherited by the ancestor job positions or business roles. They are mainly dominated by passive control principles; ii) class supervision (*S*): the permissions for the tasks in the class *S* are inherited by the ancestor job positions or business roles. They are mainly dominated by passive control principles and are related to management or supervision. Neither Classes *S* nor *P* belong to a business process; iii) class workflow (*W*): the permissions for the tasks in the class *W* are non-inherited by the ancestor job positions or business roles. They are mainly dominated by active control principles and belong to a business process; and iv) class approval for activity (*A*): Class *A* exhibits characteristics of class *S* and class *W*. The permissions for the tasks in the class *A* are inherited by the ancestor job positions or business roles and are dominated by active control principles. Oh and Park (2003) discuss the characteristics of information sharing and access control in organizations:

1. Information is characterized by information sharing.
2. Information resources are accessed by many agents as they are produced and consumed in the activities of a process

3. Environmental changes, and consequent changes in activities necessitate dynamic management of access rights to information resources. This makes administration of access control challenging.
4. Additionally, an organization may incur significant cost without appropriate and timely authorization for activities to access information artifacts. Authorized access to information resources is based on job position and assigned organizational roles since separation of duty is an important security principle.

Based on the analysis of access control literature, an SSeBP must allow for the separation of duties (DOS) and incorporate agents, activities, permissions, and resources (information and knowledge) in the context of a eBusiness process. In addition, it is imperative that an SSeBP enables the representation and enforcement of multiple constraints for granting the appropriate access to information and knowledge resources involved in an eBusiness process. In other words, SSeBP must provide an integrative framework for *component, process, and Security knowledge*.

2.2.1.5. Situational Awareness Theory

Situational Awareness (SA) is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status within the near future. Endsley (1995) defined three level of situational awareness (SA). The first level of SA is the ability to perceive the status, attributes and dynamics of relevant elements in the environment and forms a basis for decision making. The Second level of SA goes beyond awareness, into comprehension

and includes an understanding of the significance of elements for pertinent goals. A novice may achieve the same Level of SA as an expert, but fall short of also being able to integrate various data elements along with pertinent goals to comprehend the situation. At the highest level, SA includes the ability to project the future actions of the elements in the environment within temporal constraints of the problem domain forms. This is achieved through knowledge of the status and dynamics of the elements and comprehension of the situation, achieved through the first and second levels of SA.

Conceptual modeling is the activity of formally describing aspects of the physical and social world around us for purposes of understanding and communication (Mylopoulos, 1992). In this dissertation, we apply SA theory to define and measure the levels of situational awareness of security policies and constraints generated by using the SSeBP conceptualization of a secure ebusiness process.

Table 2 summarizes the kernel theories from the application domain and their application to SSeBP design theory.

Kernel Theory	Description	Application in SSeBP
Resource-Based View of the Firm; Impact of knowledge, and knowledge sharing, on competitive advantage (Wernerfelt, 1984; Dyer 2000; Tallman <i>et al.</i> , 2004; Loebecke <i>et al.</i> , 1999)	<p>Knowledge is considered a source of competitive advantage.</p> <p>Organizations must manage explicit knowledge sharing mechanisms with partner organizations to enact business processes in the extended enterprise.</p> <p>Cooperation through knowledge sharing may increase each partner's knowledge and therefore their competitiveness.</p>	<p>Knowledge sharing may be governed by, and helps form, contractual relationships between partner organizations.</p> <p>Knowledge sharing in supply chains is recognized to enhance competitive advantage of the supply chain as a whole.</p> <p>Actors use Information and knowledge resources to make decisions and reach useful inferences in performing their activities and accomplish their goals.</p>
Knowledge based view of the firm (Grant, 1996)	Knowledge is consider as a strategic resource	<i>Knowledge resources</i> are vital resources that must be shared in a secure and systematically way with partner organizations of a value chain.
Value Chain and networks of collaborating organizations (Porter, 1985; Sawhney and Parikh, 2001)	<p>Porter's framework (1985) of value activities and value chain to generate valuable customer propositions.</p> <p>Inter-organizational processes that allow collaborating organizations to provide complementary services through networks of collaborating organizations.</p>	<p><i>Value chain</i> as unit of competition.</p> <p>A focal firm is embedded in a network of collaborating firms that have the common business goal of creating valuable customer propositions.</p>

Kernel Theory	Description	Application in SSeBP
<p>Business Process and Interorganizational Workflow (van der Aalst and Kumar, 2003; WfMC, 1996)</p>	<p>A business process is “<i>a sequence of activities with distinct inputs and outputs and serves a meaningful purpose in an organization or between organizations</i>”. (WfMC, 1996)</p> <p>Workflows are a systematic representation of business process (van der Aalst and Kumar, 2003)</p>	<p>Business processes are deterministic, action-event sequences in workflow systems</p> <p>Activities and resources must be coordinated in order for an (extended) enterprise to enact business processes</p> <p>Coordination involves <i>managing dependencies among activities</i>.</p> <p>Process knowledge including coordination mechanisms and control structures manage business activities.</p>
<p>Agency Theory (Jensen and Meckling, 1976)</p>	<p>An agent represents an entity’s interests and fulfills responsibilities on its behalf</p>	<p>In a business enterprise, human actors (agents) or software agents carry out the various activities to achieve organizational/system goals.</p>
<p>Coordination Theory (Malone et al., 2003; Kishore et al., 2006; van der Aalst and Kumar, 2003)</p>	<p>Processes are decomposed into activities organized by generalization-specialization hierarchies and require coordination mechanisms for their management.</p>	<p>Coordination is the management of dependencies among activities.</p> <p>Activities have sharing, flow or fit dependency with resources.</p> <p>An activity either consumes or produces resources. An activity cannot produce or consume another activity.</p>

Kernel Theory	Description	Application in SSeBP
Access Control (Role Based Access Control (RBAC)) The National Institute of Standards and Technology (NIST), 2004; Oh and Park, 2003, Sandhu et al., 1996)	Access control policies specify users' permissions to specific system resources through relationships between users, roles and permissions. Permission to resources is based on user role. Roles specify organizational functions responsible for specific activities and provide repudiation and auditing.	<i>Roles</i> abstract business activities needed to achieve business process goals. Roles are assigned to actors expected to perform the business activities. Security Knowledge, SAC policies, defines users' permissions to resources. <i>Roles</i> are central to both eBusiness processes and RBAC for authorized resource access.
Situational Awareness (SA) Theory (Endsley, 1995)	Situational Awareness (SA) theory provides a framework for measuring people level of perception, comprehension, and prediction of their environment.	SSeBP leads to better security awareness about the security policies and constraints involved in an eBusiness process.

Table 2. Kernel Theories from the Application Domain extended and applied in SSeBP.

2.2.2. Kernel Theories for the Information Systems Knowledge Domain

Following Hevner et al. (2004) design science approach, we identify the kernel theories from the IS knowledge domain and derive the technical foundations for the SSeBP design theory. Theories for the IS domain relates to the “knowledge base” identified in Hevner et al. (2004). The SSeBP design theory requires of standardized

vocabulary and technologies to support transparent and secure exchange of machine-interpretable and unambiguous knowledge to develop viable inter-organizational eBusiness processes. Information and knowledge transparency for concurrent coordinated responses from trading partners require ontological descriptions of knowledge domains (i.e.: component, process, and security knowledge) in the context of eBusiness processes.

It has been recognized that candidates for applications of Semantic eBusiness include supply chain management and eMarketplaces (Sing et al., 2005). Here, we apply the semantic web technologies in conjunction with the vision of Semantic eBusiness to develop the *SSeBP* design theory. Developments in semantic technologies make semantic web content unambiguously computer-interpretable and amenable to agent interoperability and automated reasoning techniques (McIlraith et. al., 2001). Ontology-based representation of eBusiness processes lends specificity to representation of relevant knowledge domains. This allows for knowledge to be *interpreted by software and shared using automated reasoning mechanisms to reach useful inferences*. Built on Resource Description Framework (RDF) and Description Logics (DL), the Web Ontology Language (OWL) is a W3C standard for semantic knowledge representation. Semantic Web technologies provide semantic knowledge representation and exchange mechanisms for developing secure semantic eBusiness Processes. Next, we describe the semantic web technologies that form the technical foundations for the *SSeBP* design theory. These provide the “how” for the development of the *SSeBP* design theory. In this dissertation, the theories for the IS knowledge domain include semantic web, Semantic eBusiness,

Ontologies, Description Logic (DL), Intelligent Agents, Functional View of knowledge and secure information systems methods.

2.2.2.1. Semantic Web

The Semantic Web is an extension of the current Web in which information is given “*well-defined meaning*” to allow machines to “*process and understand*” the information presented to them (Berners-Lee et al., 2001). The Semantic Web vision comprises *Ontologies* for common semantics of representation and ways to interpret ontology; *Knowledge Representation (KR)* for structured collections of information and inference rules for automated reasoning in a single system; and *Intelligent Agent* to collect content from diverse sources and exchange data enriched with semantics (Berners-Lee et al., 2001). This vision provides the foundation for the SSeBP design theory proposed in this research. Semantic technologies incorporate knowledge representation and intelligent software agents to integrate heterogeneous systems across organizations. A recent and relevant application of semantic web in the context of eBusiness is the Semantic eBusiness Singh et al. 2005), which is described next.

2.2.2.2. Semantic eBusiness

Singh et al. (2005) define Semantic eBusiness as “ an approach to managing knowledge for coordination of eBusiness processes through the systematic application of Semantic Web Technologies”. Semantic eBusiness leverages Semantic Web technologies

and concepts to support the transparent flow of semantically enriched information and knowledge and enable collaborative eBusiness processes within and across organizational boundaries. In addition, Semantic Web aids intelligent agents to organize, store, retrieve, search, and match information and knowledge for effective collaboration among Semantic eBusiness participants.

Semantic Web requires of trusted and secure environments. Semantic Web consists of three semantic layers namely:

1. Semantic eBusiness layer, which includes semantic business process descriptions, semantic business rules, and business process reasoning;
2. Semantic Web Technology layer, which includes semantic workflow descriptions, product ontologies, and semantic service description; and
3. Information Technology layer, which includes Web Services architecture, network architecture, network communications, computational processes, and hardware resources.

The Semantic eBusiness vision provides organizations the means to design collaborative and integrative, inter- and intra-organizational eBusiness processes, and systems founded upon the seamless exchange of knowledge among trusted business partners. Therefore, Semantic eBusiness lays the ground for developing secure semantic eBusiness processes.

2.2.2.3. Ontology

SSeBP design theory requires knowledge to be represented in a way that can be interpreted by software and shared using automated reasoning mechanisms to reach useful inferences. Ontology-based representation of eBusiness processes lends specificity to representation of relevant knowledge domains and enables knowledge exchange.

Even though the word ontology comes from Philosophy, where it means a “systematic explanation of being”, research about ontology has become a very pervasive phenomenon in the computer science field (Guarino, 1998; Sugumaran and Storey, 2002; Wand and Weber, 2002). According to Guarino (1998), ontology has been studied in the field of knowledge engineering (Gruber, 1993; Gaines, 1997; Gómez-Pérez, 1997) knowledge representation (Guarino, 1995; Artale et al., 1996; Sowa, 1998), qualitative modeling (Gotts et al., 1996; Borgo et al., 1997; Casati and Varzi, 1997), language engineering (Lang, 1991; Bateman, 1995), database design (Burg, 1997; Van de Riet et al., 1998), information modeling (Ashenurst, 1996; Weber, 1997), information integration (Wiederhold, 1996; Bergamaschi et al., 1998; Mena et al., 1998), information retrieval and extraction (Guarino, 1997; Benjamins and Fensel, 1998; McGuinness, 1998), agent-based systems design, enterprise integration (Uschold et al., 1998; Gruninger and Fox, 1995), standardization of product knowledge (Boley and Guarino, 1996; Barley et al. 1997; Guarino et al., 1997), electronic commerce (Lehmann, 1995), and geographic information systems (Casati et al., 1998). In general terms, ontologies provide a shared and common understanding of specific domains that can be communicated between disparate application systems, and therein provide a means to

integrate the knowledge used by online processes employed by organizations (Klein et al., 2001). Ontology describes the semantics of the constructs that are common to the online processes, including descriptions of the data semantics that are common descriptors of the domain context. Ontology documents can be created using standardized content languages like BPEL, RDF, OWL, and DAML to generate standardized representations of the *process knowledge* (Sivashanmugam et al., 2004; Thomas et al., 2006).

Ontologies are domain specific; therefore, to craft useful ontologies, it is important to identify the purposes of them. Noy and McGuinness (2002) identified the following as the major purposes of ontologies:

1. Enable and shared understanding of structure of information among people and agents,
2. Enable information reuse in applications,
3. Make the assumptions underlying an IS implementation explicit and well-understood,
4. Specify the knowledge embodied in an ontology at an appropriate level of granularity (universe, bounded universe, domain, operational), and
5. Apply the ontological structures at different stages of IS development: analysis, conceptualization, and design (Kishore et al., 2004).

Jasper and Uschold (1999) identify that ontologies can be classified into: a) ontology for knowledge reuse; b) ontology as specification; c) ontology as a provider of common access of heterogeneous information; and d) ontology as a search mechanism. In this research, we develop ontologies for the *SSeBP* design theory that are aimed to

knowledge reuse, share, and representation and to provide a common vocabulary and secure way to integrate knowledge resources across inter-organizational eBusiness process.

Selecting the language for the implementation of the ontology is one of the most crucial tasks in the ontology development process. Several ontology languages have been developed. In fact, at least 11 different languages can be identified from literature: KIF, Ontolingua, LOOM, OCML, FLogic, SHOE, XOL, RDF(S), OIL, DAML+OIL, and OWL (Gomez-Perez et al., 2004). The reader is referred to Gomez-Perez et al. (2004) for a comprehensive explanation of each ontology language. For this research, we select *SHIQ* Descriptions logics, which is equivalent to DAML+OIL, presented by Li and Horrocks (2004) to develop the SSeBP ontologies.

2.2.2.4. Description Logic

Description logics are logical formalisms for knowledge-representation (Li and Horrocks, 2004; Gomez-Perez et al., 2004). A description logic is divided into two parts: 1) T-BOX, which contains intentional knowledge in the form of a terminology and is built through declarations that describe general properties of concepts; and 2) A-Box, which contains extensional knowledge, which is specified by the individual of the discourse domain (Baader et al., 2003; Gomez-Perez et al., 2004). Description Logics provide a formal linear syntax to express the description of top-level concepts in a problem domain, their relationships and the constraints on the concepts and the

relationships that are imposed by pragmatic considerations in the domain of interest. Description logics provide the language for building composite term descriptions from primitive concepts. The terms denote several sorts of things including *primitive* and *derived concepts*, similar to classes or templates for categorizing individual instances; and *roles* which are binary relationships between *concepts*. In addition to the subsumption hierarchy of primitive and derived concepts, generalizations and specialization hierarchies of relationships can be described to express specialized relationships between derived concepts that are specializations of more general relationships between primitive concepts. The basic description logics language is the *AL* (*Attributive Language*) which provides a minimal set of concept descriptions including atomic concept, atomic concept negation (\neg), concept intersection ($C \sqcap D$), universal value restrictions ($\forall R.C$), and limited existential value restriction ($\exists R.C$). We refer the interested reader to Baader et. al. (2003) for a full explanation of description logics notations, theoretical foundations and applications.

It is important to highlight that the basic DL language does not fulfill the requirements of the present investigation because it is necessary to be able to reason with descriptions, which include, for example, cardinality restrictions on roles, and data types (integers, strings, etc.). The DL SHIQ is used, because it consists of the basic description logics language plus the negation of arbitrary concepts, (qualified) cardinality restrictions, role hierarchies, inverse roles, transitive roles, and data types (a restricted form of DL concrete domains). A detailed discussion of these and other DL constructors can be found in Baader et al. (2003). In this study, we adopt the *SHIQ* Descriptions

logics presented by Li and Horrocks (2004). Li and Horrocks argue that *SHIQ*'s expressive power made it to be equivalent to DAML+OIL. In addition, the Web Ontology Language (OWL) is based on the SH family of description logics which supports Boolean connectives, including intersection, union and complements, restrictions on properties transitive relationships and relationship hierarchies. The increased expressive power of the language is manifested in a range of additional constructors, including:

- $\exists R.C$ (full existential value restriction)
- $\neg C$ (atomic negation of arbitrary concept)
- $\leq n R$ (at-most cardinality restriction)
- $\geq n R$ (at-least cardinality restriction)
- $= n R$ (exact cardinality restriction)
- $\leq n R.C$ (qualified at-most cardinality restriction) \equiv
- $\geq n R.C$ (qualified at-least cardinality restriction)
- $= n R.C$ (qualified exact cardinality restriction)
- $\leq n R$ (concrete domain max restriction)
- $\geq n R$ (concrete domain min restriction)
- $= n R$ (concrete domain exact restriction)

Description logic derives its descriptive power from the ability to enhance the expressiveness of the atomic descriptions by building complex descriptions of concepts using concept constructors. These *terminological axioms* make statements about how concepts or roles are related to each other. This develops a set of terminologies, comprise of definitions, which are specific axioms which define the inclusions (\subseteq) or the equivalence (\equiv). Here, if R is a relationship between two concepts in the problem domain, then R^{-} denotes the inverse of the relationship R . Given the above concepts and relationships in the problem domain, we can begin to define the relationships between the concepts in the domain.

Standardized by the World Wide Web Consortium, OWL is the leading approach to semantic Web ontologies using description logic as its fundamental knowledge representation mechanism. Ontological analysis results in ontology descriptions that are presented formally through description logics for theoretical soundness; and in machine readable format using the Web Ontology Language (OWL) and OWL-DL (OWL-Description Logics) to provide practicality for the model. In addition, software reasoners, such as Racer, support concept consistency checking, T-Box reasoning and A-Box reasoning on models developed using SHIQ description logics translated into OWL-DL. These provide the basis for development of a knowledge base of machine interpretable knowledge representation, in OWL-DL format, that can be used for developing computational ontologies for knowledge integration in inter-organizational eBusiness process.

In this research, for the meta-design, we define the terminology for the secure semantic eBusiness process domain using the aforementioned terminological axioms. We develop DL-based semantic knowledge representation for activity resource coordination in semantic eBusiness processes. These provide the basis for developing machine-interpretable knowledge representation and computational ontologies in OWL-DL format to support knowledge integration in collaborative inter-organizational eBusiness processes. DL-based knowledge representation provides the formalism to express structured knowledge in a format amenable for normative reasoning by intelligent software agents.

2.2.2.5. Functional View of Knowledge

As it was mentioned earlier, in this research, we are concerned with information and knowledge resources of an organization. Organizational and process knowledge is central to business activities of human and software agents. It is important for eBusiness to explicitly recognize knowledge, and the processes and technologies for knowledge management. Newell (1982) provides a functional view of knowledge as “whatever can be ascribed to an agent, such that its behavior can be computed according to the principle of rationality”. This view forms a basis for functional knowledge management using agents, human and software when using explicit, declarative knowledge that is represented using standards-based knowledge representation languages that can be processed using reasoning mechanisms to reach useful inferences.

While all knowledge cannot be explicated and be effectively represented and reasoned with using decidable and complete computational techniques; it is useful to focus on explicit, declarative KR using computationally feasible KR languages to build effective and useful knowledge-based systems. We focus on three specific types of knowledge in this research:

- i. *Component knowledge* including descriptions of skills, technologies, resources, consumer and product knowledge, is amenable to knowledge exchange (Hamel, 1991; Tallman, et al., 2004).
- ii. *Process knowledge* is typically embedded in the process models of workflow management systems or exists as coordination knowledge among human agents to coordinate complex processes (van der Aalst and Kumar, 2003).

- iii. *Security Knowledge* relates to access control mechanisms used to permit or deny access to knowledge resources in distributed systems (Sandhu 1996; Oh and Park 2003).

2.2.2.6. Intelligent Agents

The *SSeBP* design theory must allow multiple organizations to cooperate in an automated, secured, and coordinated manner to accomplish shared goals of the extended-enterprise. An intelligent agent is “a computer system situated in some environment and that is capable of flexible autonomous action in this environment in order to meet its design objectives” (Jennings and Wooldridge, 1998). The agent paradigm can support a range of decision-making activity, including information retrieval, generation of alternatives, preference order ranking of options and alternatives, and supporting analysis of the alternative-goal relationships. The specific autonomous behavior expected of intelligent agents depends on the concrete application domain and the expected role and impact of intelligent agents on the potential solution for a particular problem for which the agents are designed to provide cognitive support. Criteria for application of agent technology require that the application domain should show natural distributivity with autonomous entities that are geographically distributed and work with distributed data; require flexible interaction without a priori assignment of tasks to actors; and be embedded in a dynamic environment (Muller, 1997). Papazoglou (2001) defines intelligent agents as action-oriented abstractions in electronic systems, entrusted to carry out various generic and specific goal-oriented actions on behalf of users. Papazoglou (2001) discuss the use of intelligent agents in eCommerce. Intelligent agents are able to

organize, store, retrieve, search, and match information and knowledge for effective collaboration among Semantic eCommerce participants.

Agents have been conceived to be a key technology to alleviate the problems related to communications in distributed environments (Liang and Huang, 2006) and recently agent technologies have been applied in the context of supply chains (Nissen and Sengupta, 2006). Sikora and Shaw (1998) develop and validate a multi-agent framework for the coordination and integration of heterogeneous information systems. Their work illustrates how agents can be used to represent organizational functions. Nissen and Sengunta (2006) study the application of agent technologies in supply chain. In particular, they successfully demonstrate how agents can be used to automate and facilitate procurement activities and decisions in the area of maintenance, repairs, and operations (MRO). Liang and Huang (2006) develop a multi-agent-based demand forecast systems where agents share information and forecasting knowledge to control inventory and minimize the total cost of supply chain. Furthermore, intelligent agents have been shown to support the processing of complex information and help reduce the cognitive load of decision-makers in the context of eMarketplace. Singh et al. (2005) propose a multiple-agent enabled infomediary-based eMarketplace that incorporates intelligence in the discovery of buyers and suppliers and in the facilitation of transactional roles. Kishore et al. (2006) investigate the characteristics of the multi-agent-based integrative business information systems (MIBIS) universe based on the literatures in both the integrative business information systems (IBIS) and multi-agent systems domains. They propose eight minimal ontological foundation constructs for the MIBIS

universe of discourse, including *goal*, *role*, *interaction*, *task*, *information*, *knowledge*, *resource*, and *agent*.

Intelligent agents can be used for knowledge management to support Semantic eBusiness Process activities. The agent abstraction is created by extending an object with additional features for encapsulation and exchange of knowledge between agents to allow agents to deliver knowledge to users and support decision-making activity (Shoham, 1993). Agents work on a distributed platform and enable the transfer of knowledge by exposing their public methods as Web services using Simple Object Access Protocol (SOAP) (W3C) and XML. In this respect, the interactions among the agents are modeled as collaborative interactions, where the agents in the multi-agent community work together to provide decision support and knowledge-based explanations of the decision problem domain to the user. A fundamental implication is that knowledge must be available in formats that allow for processing by software agents.

2.2.2.7. Secure Information Systems Design Methods

Baskerville (1988) states that “the best approach to the development of security analysis and design methodology, would essentially be to nest it as a component part of an existing, established, successful overall information systems analysis and design methodology” (p. 88). Holistic information systems methodology that includes security aspects in all of its stages is still needed (Baskerville, 1988).

Chung and Nixon (1995) developed a process oriented approach that allows developers to represent security requirements as non-functional requirements. Lee et al. (2005) proposed an integrated software lifecycle process with Security Engineering (SE). Apvrille and Pourzandi (2005) proposed a methodology to produce secure applications by extending the general project life cycle methodology and inserting security concerns at each phase. Mouratidis et al. (2005) extended the TROPOS development methodology incorporating security concepts such as security constraints, secure entities, and secure dependencies. Unified Modeling Language (UML) is de facto standard for modeling information systems (Satzinger and Jackson, 2005) and has successfully been used in process modeling (Glassey, 2008). Specifically, use case, sequence, collaboration and activities diagrams have been recognized as relevant for process modeling (Glassey, 2008). However, the UML approach does not specifically address security aspects during the analysis and design phases of information systems or business processes. Jürjens (2001) extend UML to include modeling of security requirements (UMLsec). While UMLsec allows modeling access control mechanisms and aspects of information confidentiality, this work primarily focuses on the design phase. Mc Dermott and Fox (1999) proposed the use of abuse cases that capture and analyze security requirements. An abuse case is an extension of object oriented use case technique and specifies interactions between system and actors where the results of the interaction are harmful (Mc Dermott and Fox, 1999). An abuse case provides a mechanism to model systems security threats in the requirements analysis phase of the SDLC. Sohr et al. (2005) explain that several classes of authorization constraints can be represented and specified

using UML and the Object Constraint Language (OCL). Sohr et al. (2005), using the UML Specification Environment (USE), demonstrate how authorization policies such as role based access control (RBAC) policies can be modeled using UML/OCL. Dhillon and Backhouse (2001) analyze IS security research using a conceptual framework of four paradigms: functionalist, interpretive, radical humanist, and radical structuralist paradigm. They find that while most IS security research focuses on formalized rule structures in designing security, IS researchers are moving away from the security technical viewpoint towards a socio-organizational perspective. This movement may lead to more holistic IS security research where organizational security aspects are incorporated in the design and development of secure information systems.

Recently Siponen et al. (2006) propose a meta-notation framework to represent and analyze information systems security requirements. They extend the UML-Use Case; to incorporate security requirements into the design phase. They use field study and action research to validate their proposed framework. Table 3 shows the meta-notation for the Enriched-Use Case.

Use case: Booking.
Version: 1.0
Functional Summary: A booking clerk books journeys for customers.
Frequency: Several times a day
Usability requirements: Any database query and booking must be able to complete in less than 30 seconds
Actor/ security subject : A clerk.
Security classification of the subject : confidential
Security objects and access types to security objects : Object: customer file (the clerk must be able to read, update and delete the customer information); Object: booking database (the clerk must be able to read, update and delete the customer information on the database)
Security policy/Specific security restrictions : The clerk is only allowed to access security objects classified as confidential with the booking department.
Preconditions: Booking and customer databases exist. The identity of the booking clerk/ security subject has been validated.
Exceptions: If information on a certain journey is not available, an appropriate error message is produced.

Table 3. Enriched- Use Case (Adopted from Siponen et al., 2006)

Note: Security semantics are illustrated in italics and boldface.

Enriched-Use Case incorporates security constraints, security subjects, and security actors into the design of information systems. However, it fails to capture the security requirements and dynamics of a business process.

Attempts to incorporate security as a functional requirement in the early stages of requirement specification and analysis are worthwhile. Current research identifies security requirements in the requirement specification stage but fail to show how these requirements can be incorporated in the design of secure eBusiness processes.

Table 4 summarizes the theoretical foundations from IS domain kernel theories and their integration in the SSeBP design theory.

Kernel Theory	Description	Application in SSeBP
Semantic Web (Berners-Lee, et al., 2001)	The Semantic Web vision comprises: Knowledge Representation: structured collections of information and inference rules linked into a single system for automated reasoning; Ontologies: to discover common meanings for entity representations and ways to interpret ontology; and Intelligent Agents: that collect content from diverse sources and exchange data enriched with semantics. (Berners-Lee, et. al., 2001).	A Semantic approach to eBusiness processes affords ontological descriptions of the ‘context’ for the roles involved. This approach can be used to describe the roles, permissions, resources and security requirements by creating a standardized vocabulary that describes access control and security for distributed information and knowledge sharing.
Semantic eBusiness (Singh et al., 2005)	Semantic eBusiness is “an approach to managing knowledge for coordination of eBusiness processes through the systematic application of Semantic Web technologies”. Semantic eBusiness supports the transparent flow of semantic information and knowledge to enable collaborative eBusiness processes within and across organizational boundaries.	Application of Semantic Web technologies provides organizations the means to design collaborative and integrative, inter- and intra-organizational business processes, and systems founded upon the seamless exchange of knowledge among trusted business partners.

Kernel Theory	Description	Application in SSeBP
<p>Description Logics (DL) based Knowledge Representation (Baader, 2003; Horrocks et al., 2003; Singh and Salam, 2006)</p>	<p>Description Logics model a problem domain using constructs that describe domain specific objects and their relationships.</p> <p>Description Logics provide formalism for theoretical soundness and it forms the basis for the development of machine interpretable knowledge representation in the OWL-DL format.</p> <p>The Web Ontology Language (OWL) is a W3C standard knowledge representation language for the Semantic Web.</p>	<p>Ontological descriptions are formally represented using DL for theoretical soundness; and in machine-readable and implementable format using OWL and OWL-DL.</p> <p>OWL documents capture domain ontologies and rules for knowledge sharing among agents.</p> <p>OWL has robust theoretical foundations in DL and provides the standards-based foundation for semantic knowledge representation and management.</p>

Kernel Theory	Description	Application in SSeBP
<p>Ontology (Guarino, 1995; Wand and Weber, 2002; Sugumaran and Storey, 2002; Kishore et al., 2006; Ram and Park, 2004)</p> <p>Functional view knowledge (Newell, 1982; Lorange, 1996)</p>	<p>Computational ontologies for IS contain the common syntax and semantics used to model and represent the IS artifacts.</p> <p>This helps increase the quality of analysis and reduce the cost of conceptual analysis, while allowing for knowledge reuse.</p> <p>Knowledge is “whatever can be ascribed to an [software] agent, such that its behavior can be computed according to the principle of rationality”.</p> <p>Semantic Inter-operability mechanisms allow integration of knowledge developed using different vocabularies through Ontologies.</p>	<p>Ontology describes the semantics of constructs common to the eBusiness processes, including data semantic descriptors of the domain.</p> <p>Ontologies capture domain knowledge for knowledge-based systems.</p> <p>Ontologies are an effective means to facilitate collaboration and communication among agents.</p> <p>Ontology that describe access control and security constructs allow local and global entities to share and describe various security requirements in a common semantics for distributed knowledge and information exchange</p> <p>OWL documents capture domain ontologies and knowledge representation for knowledge sharing among agents.</p>
<p>Intelligent Agents to model enterprise functions. (Singh, et al., 2005; Sikora and Shaw, 1998)</p>	<p>Enterprise systems can be modeled as multiple agents and coordination mechanisms and interdependencies in control structures and knowledge exchange required to model agent functions in an enterprise.</p>	<p>Activities are fundamental to multi-agent systems and organizations since both perform activities to accomplish their individual and organization/system goals.</p> <p>Ontologies can be the object of communication between software agents for a common vocabulary, with standard interpretation of problem-domain constructs</p>

Kernel Theory	Description	Application in SSeBP
Secure Information Systems Design Methods (Baskerville, 1988; Siponen et al. 2006; Mouratidis et al. 2005)	Secure information systems design methods must be theoretically grounded and must consider security requirements from the outset and through all their stages.	SSeBP allows for security constraints that incorporate access control mechanisms to be incorporated in the conceptualization of eBusiness processes.

Table 4. Kernel Theories from the IS Knowledge Domain extended and applied in SSeBP.

CHAPTER III

DESIGN OF SECURE SEMANTIC E-BUSINESS PROCESSES DESIGN THEORY

Walls et al. (1992) state that a design theory includes the design product or artifact and design process to produce it. In developing a design theory, kernel theories are applied to develop the theoretical basis for the design theory's meta-requirements and meta-design. Markus et al. (2002) refer to design process as principles that guide artifact development. In the next sections, the meta-requirements, meta-design, and design process of the *SSeBP* design theory are described.

3.1. Meta-Requirements for a Secure Semantic eBusiness Processes Design Theory

A set of meta-requirements is the first component of a design theory. The meta-requirements describe the class of goals to which the theory applies. Since design theory solves a class a problem, the requirements must be stated as abstracted as possible (Walls et al. 1992). Moreover, design theories are prescriptive theories that dictate how things ought to be (Gregor 2006).

Using the relevant extant literature, we specify the meta-requirements for the *SSeBP* design theory as:

1. SSeBP design theory should allow multiple agents to cooperate in a coordinated manner to accomplish goals of an eBusiness process. Agents should represent a business enterprise and fulfill organizational roles by performing business activities.
2. SSeBP design theory must support coordination of dependencies among business activities and information and knowledge resources involved in an eBusiness process.
3. SSeBP design theory should represent access control policies that comply with local, intra-organizational and global, inter-organizational, security requirements for an eBusiness process.
4. SSeBP design theory should decouple and simplify association between agents and resources permissions and incorporates roles, permissions, access, and security of information and knowledge resources from a dynamic eBusiness process perspective.
5. SSeBP design theory must describe eBusiness processes in unambiguous, computer-interpretable knowledge representation, amenable to agent-based reasoning.
6. SSeBP design theory should provide an integrative semantic foundation that facilitates agents reasoning with process and component knowledge in the context of an eBusiness process.

3.2. Meta-Design for a Secure Semantic eBusiness Processes Design Theory

The second component of a design theory is the meta-design intended to meet the meta-requirements (Walls et al., 1992). Kernel theories guide the development of our design artifact to meet these meta-requirements. Analysis of kernel theories reveals that collaborative inter-organizational business processes can be represented using the following atomic concepts: *business enterprise, agent, role, activity, and resource*. Those atomic concepts are consistent with extant research. Similarly, Singh and Salam (2006) propose that essential concepts to model eBusiness Processes include *business enterprise,*

agent, business activity, resource, coordination, information and knowledge. Kishore et al. (2006) propose eight minimal ontological foundation constructs for the Multi-Agent-Based Integrative Business Information (MIBIS) universe of discourse, including *goal, role, interaction, task, information, knowledge, resource, and agent*, based on literature in integrative business information systems and multi-agent systems domains. Here, we propose that business enterprises engaged in collaborative inter-organizational business processes can be represented by *agents*. *Agents* fulfill organizational roles and perform *activities* that consume and produce *resources*. *Activities* require access to resources to perform business activities. *Roles* de-couple the relationships and provide authorization constraints for agents and the individual activities that comprise the business process. Consistent with RBAC, *resources*, in our model, allow activities to be performed on them. Here, we consider only *information* and *knowledge* resources involved in business processes. They are used by agents in a business enterprise to perform their assigned activities in order to accomplish their goals. Dependencies among multiple resources and multiple activities are coordinated using flow, fit, or sharing coordination methods (Adapted from Malone et al. 2003). The design theoretic conceptualization of the SSeBP design theory including constructs and relationships derived from the analysis of the kernel theories and posited to meet the meta-requirements is shown in Figure 3 and conceptualized as:

In an eBusiness process, a Business Enterprise authorizes representation to an actor or Agent to fulfill a Role, which performs Activities that have access permissions to resources.

Resources permit activities performed by Roles fulfilled by Agents that represent Business Enterprises, engaged in an eBusiness Process.

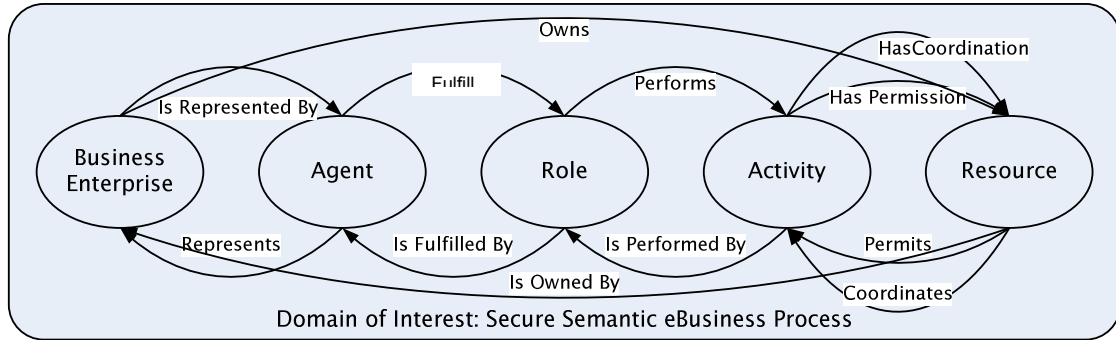


Figure 3. The Secure Semantic eBusiness Process Design Theory (adopted and extended from Singh and Salam, 2006 and Kishore et al., 2006)

It is important to emphasize that the proposed Secure Semantic eBusiness Process Design Theory concepts are consistent with RBAC (Sandhu 1996); coordination mechanism in Malone et al. (2003) and van der Aalst and Kumar (2003); view of business process in Singh and Salam (2006) ,Oh and Park (2003), and Raghu and Vinze (2007); and constructs of a multi-agent systems in Kishore et al. (2006).

DL representation of the SSeBP design theory describes the semantic schema through complex concepts specifications and relation expressions built upon atomic concepts and relations. Constructs are represented as unary predicate *concept constructs* and relationships are the n-ary *relations construct*. These concepts and relationships define KR as terminological axioms for the SSeBP design theory, represented using OWL-D as shown below in Table 5.

Atomic Concepts and Relationships		
Essential atomic concepts in the secure semantic eBusiness process domain include:		Essential atomic relationships in the secure semantic eBusiness process domain include:
<ul style="list-style-type: none"> i. <i>Business Enterprise (BE)</i> ii. <i>Agent (Ag)</i> iii. <i>Role (Rl)</i> iv. <i>Business Activity (Ac)</i> v. <i>Resource (Rs)</i> 		<ul style="list-style-type: none"> i. <i>Represents (≡ IsRepresentedBy[~])</i> ii. <i>Fulfills (≡ IsFulFilledBy[~])</i> iii. <i>Performs (≡ IsPerformedBy[~])</i> iv. <i>Permits (≡ HasPermission[~])</i> v. <i>Coordinates (≡ HasCoordination[~])</i> vi. <i>Owns (≡ IsOwnedBy[~])</i>
Business Enterprise	A Business Enterprise is represented by at least one Agent and owns at least one resource need in the business process.	$BusinessEnterprise \subseteq$ $(\geq 1 \text{ IsRepresentedBy} \cdot Agent) \wedge$ $(\geq 1 \text{ Owns} \cdot Resource) \wedge$ $(\geq 1 \text{ HasClassificationID} \cdot StringData) \wedge$ $(\geq 1 \text{ HasDescription} \cdot StringData) \wedge$ $(\geq 1 \text{ HasAddress} \cdot Address) \wedge$ $(\geq 1 \text{ HasProfile} \cdot Profile)$
Agent	An Agent represents a Business Enterprise and fulfills a Role for the Business Enterprise.	$Agent \subseteq$ $(= 1 \text{ Represents} \cdot BusinessEnterprise) \wedge$ $(\geq 1 \text{ Fulfills} \cdot Role)$
Role	A Role concept is fulfilled by an Agent and performs at least one Business Activity	$Role \subseteq$ $(\geq 1 \text{ IsFullfilledBy} \cdot Agent) \wedge$ $(\geq 1 \text{ Performs} \cdot Activity)$
Business Activity	A Business Activity is performed by a Role, has at least one permission to a Resource, coordinates Resources and has a Begin Time and End Time.	$Business \text{ Activity} \subseteq$ $(\geq 1 \text{ hasLabel} \cdot StringData) \wedge$ $(\geq 1 \text{ isPerformedBy} \cdot Role) \wedge$ $(\geq 1 \text{ hasPermission} \cdot Resource) \wedge$ $(\geq 1 \text{ isCoordinatedBy} \cdot Resource) \wedge$ $(= 1 \text{ hasBeginTime} \cdot DateTimeData) \wedge$ $(= 1 \text{ hasEndTime} \cdot DateTimeData)$
Resource	A Resource is a thing owned by exactly one Business Enterprise and permits Business Activities to perform operations on it and coordinates Business Activities	$Resource \subseteq$ $(= 1 \text{ hasID} \cdot StringData) \wedge$ $(= 1 \text{ IsOwnedBy} \cdot Business \text{ Enterprise}) \wedge$ $(\geq 1 \text{ Permits} \cdot BusinessActivity) \wedge$ $(\geq 1 \text{ Coordinates} \cdot BusinessActivity)$

Table 5. DL Representation of concepts and relationships in the SSeBP model

If a business activity has permissions it is allowed to perform an operation on a resource. *Permits* and *HasPermission* are inverse relationships.

Resource \exists (*Permits*.*BusinessActivity*)
BusinessActivity \exists (*HasPermission*.*Resource*)

Activities depend on resources and require coordination mechanisms to resolve dependencies. A resource is related to an activity by the *Coordinates* relationship.

Resource \exists (*Coordinates*.*BusinessActivity*)
BusinessActivity \exists (*HasCoordination*.*Resource*)

The *Coordinates* relationship is specialized in inheritance hierarchies as *CoordinatesFlow*, *CoordinatesFit*, or *CoordinatesSharing* relationships as shown in Figure 4.

Coordinates \subseteq
CoordinatesFlow
CoordinatesFit
CoordinatesSharing

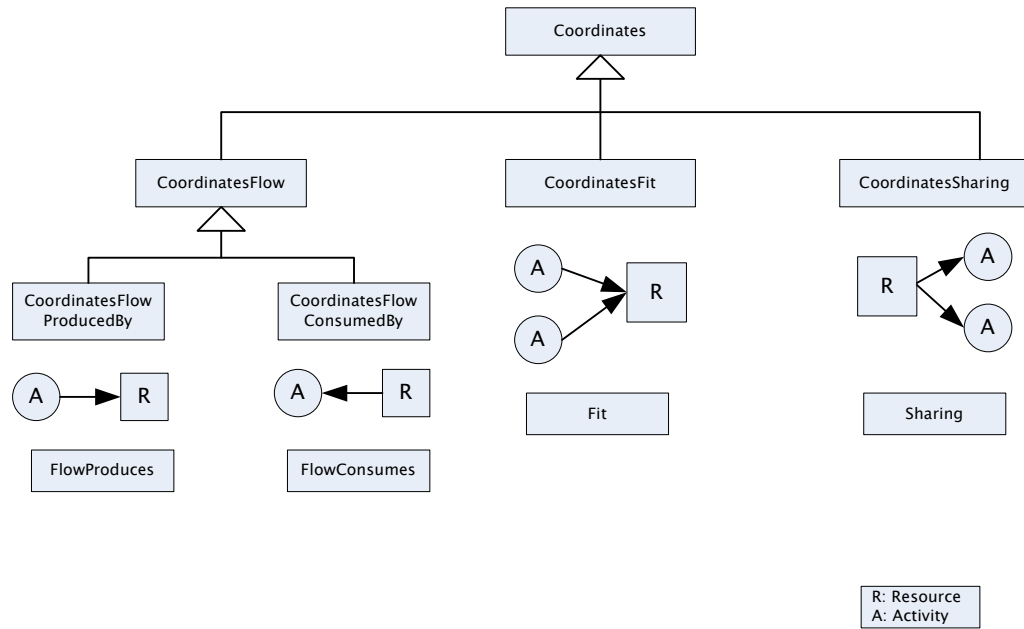


Figure 4. *Coordinates* Relationships between Activities and Resources

This is used to develop a complex description of the relationship between Resources and Business Activities.

Resource \exists
 $(\geq 0 \text{ CoordinatesFlow.BusinessActivity}) \wedge$
 $(\geq 0 \text{ CoordinatesFit.BusinessActivity}) \wedge$
 $(\geq 0 \text{ CoordinatesSharing.BusinessActivity})$

Coordination requirements lead to specific permissions on resources. A *Permits* relationship is specialized as *PermitRead*, *PermitWrite*, *PermitCreate* or *PermitDelete* relationships.

Permits \subseteq
PermitRead
PermitWrite
PermitCreate
PermitDelete

Permits relationships are shown in Figure 5.

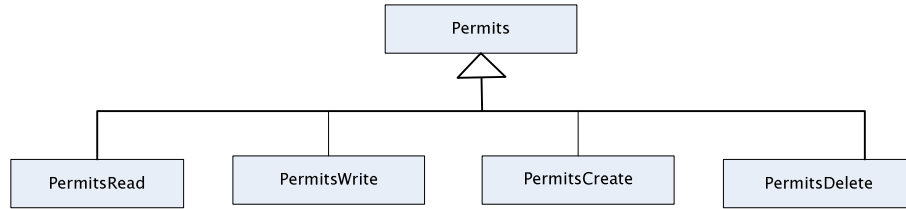


Figure 5. *Permits* Relationships

The inheritance hierarchy of the *Permits* relationship allows more specific relationships between Resources and Business Activities.

Resource \exists
 $(\geq 0 \text{ PermitsRead.BusinessActivity})$
 $(\geq 0 \text{ PermitsWrite.BusinessActivity})$
 $(\geq 0 \text{ PermitsCreate.BusinessActivity})$
 $(\geq 0 \text{ PermitsDelete.BusinessActivity})$

Here we only consider Information and Knowledge as the primary resources pertinent to the problem domain.

Information \subseteq *Resource*
Knowledge \subseteq *Resource*

These definitions comprise terminology, “*TBox*” for the *SSeBP* design theory including primitive concepts and their relationships. An “*ABox*” contains descriptions of individual instances. Specific instance level descriptions, using the *TBox*, provide

illustrative examples for verification, refinement and for implementation of the semantic data models. These form the DL-based KR system used to reason about the problem domain. Terminological axioms comprising definitions and descriptions of problem domain concepts further describe the relationships between concepts and roles. Satisfiability and logical implication in *SHIQ* are ExpTime-complete (Baader, et al., 2003). Tools like Protégé (protege.stanford.edu) and Racer (www.racer-systems.com) verify conformance to DL formalism and modeling requirements and model consistency. Protégé generates OWL-DL for schema and instance level documents for verification and implementation of semantic KR. Reasoning procedures allow inferencing from the model.

3.3.Design Method for a Secure Semantic eBusiness Processes Design Theory

As it was explained earlier, Walls et al. (1992) describe the design method as the procedure(s) for the artifact construction. It has been recognized that an information systems design method includes a process system and a notation system (Siponen et al., 2006; Hirschheim and Klein, 1992). Next, the SSeBP design method and design processes are described.

The design method can focus on any of the information systems analysis and design stage (e.g., requirements analysis, implementation, testing) (Walls et al. 1992; Siponen et al. 2006). In this context, the SSeBP design theory is intended to guide the analysis and design of secure and semantically rich eBusiness processes. Specifically,

SSeBP focuses on security requirements analysis and modeling. Then, we describe the procedure (steps) that must be followed in order to develop an IT artifact that meets the meta-requirements of SSeBP. SSeBP design method is an interactive process that requires the cooperation among information security, information systems, and business analysts and experts from the domain of the eBusiness process.

1. Identify the different business enterprises and business units that are involved in the eBusiness process.
2. Identify the business activities involved in the business process of interest.
Careful analysis of existing Dataflows and Workflows are a good starting point to locate the main activities of a business process. Follow-up interviews and discussions with experts from the domain of the business process are aimed at validating the identified activities and to make sure that relevant activities are not missing. At this stage, it is important to identify both manual and automated activities.
3. Identify the information and knowledge resources involved in the business process of interest. The analysts should not limit to identify data sources from existing IS. Documents and spreadsheets are important information and knowledge resources.
4. Identify the attributes of each information and knowledge resource identified in the previous step. Follow-up interviews and discussions with experts from the domain of the business process are aimed at validating the identified resources.
5. Decide which activities can be automated. Here, activities can be automated by representing resources in a machine-readable format or by assigning activities to be performed by intelligent agents on behalf of the human actors.
6. Identify and analyze the organizational roles and security access control (SAC) policies that pertain to the access of the information and knowledge resources identified in *step 3*. In conjunction with the security analyst, authorization and

authentication, non-repudiation, and segregation of duties security mechanisms must be identified.

7. Based on the identified activities, roles, and the SAC policies, a role-activity-resource-permissions mapping for the business process of interest must be created. The *permission* hierarchy which is specialized in *permitsread*, *permitscreate*, *permitsdelete*, and *permitswrite* must be followed.
8. Identify the dependencies that exist among activities and resources and represent them using the *coordinates* hierarchy which is specialized in *coordinatessharing*, *coordinatesfit*, and *coordinatesflow*.
9. Create the SSeBP model of the business process of interest by using the modeling grammar and modeling concepts of the SSeBP design theory.
10. Review and verify the resulting role-activity-resource-permissions mapping and the SSeBP model and repeat the previous steps as it is needed.

SSeBP design method is similar to the one presented in Crowston and Osborn (2003). Crowston and Osborn (2003) based on the coordination theory develop process model descriptions and process redesign through six steps: *setting process boundaries*, *collecting data*, *identifying actors and resources*, *identifying activities*, *identifying dependencies*, and *verifying a model*. However, SSeBP incorporates the security requirements and constraints which are missing in the Crowston and Osborn approach.

3.3.1. Design Process for a Secure Semantic eBusiness Processes Design Theory

Markus et al. (2002) refer to the design process as a set of principles that effectively guide the artifact development process. Based on the analysis of the theoretical foundations and the meta-design, we identify the following modeling concepts

and grammar (Hadar and Soffer, 2006) as guiding principles for developing secure eBusiness processes.

1. Actors fulfill organizational roles.
2. Organizational Roles are authorized to perform Business Activities.
3. Business Activities are permitted operations, including read, delete, write, create, on Information and Knowledge Resources.
4. Business activities cannot directly produce or consume another business activity.
5. Dependencies do not exist directly between Business Activities.
6. In activity-resource dependency, activities have a sharing, fit, flow dependency with an information resource.

It is important that information modeling methods provide notations to represent security requirements and constraints in the context of eBusiness processes. As depicted in Figure 3, the modeling concepts of the SSeBP design theory include business enterprise, agents, roles, activities, and resources. As a way to standardize the representation of those modeling concepts we adopt the following graphical notations. Table 6 presents the graphical representation adopted to model an SSeBP.



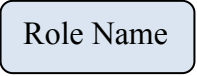
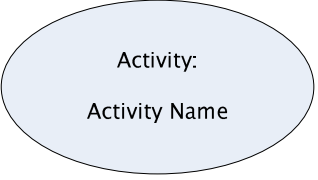
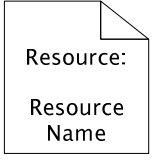
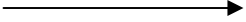
Modeling Concept	Graphical Representation
<i>Business Enterprise</i>	 Business Enterprise
<i>Agent</i>	 Agent
<i>Role</i>	
<i>Activity</i>	
<i>Resource</i>	
<i>Relationship</i> <i>IsRepresentedBy</i> <i>Fulfills</i> <i>Performs</i> <i>HasCoordination</i> <i>HasPermission</i>	 Relationship Name

Table 6. Graphical Representations for an SSeBP

CHAPTER IV

EVALUATION OF THE SECURE SEMANTIC EBUSINESS PROCESS DESIGN THEORY

The main purpose of this chapter is to explain how the proposed design theory is evaluated. Here, we describe the different methods used to assess the efficacy and utility of *SSeBP* design artifacts.

An IS design theory is a prescriptive theory that dictates, by integrating normative and descriptive theories, how to produce a specific type of IT artifact (Walls et al., 1992). While the natural sciences are concerned with how things are, design sciences are concerned with how things “ought” to be, with devising artifacts to attain goals (Simon, 1996). Hence, the utility and efficacy of an IS design theory are established by evaluating its outputs, design artifacts. A design artifact must be evaluated to demonstrate its utility, quality, and efficacy. The goals of the design artifact evaluation are to show that the proposed artifact provides value to the problem domain. By showing that the design artifact fulfills the requirements and constraints of the problem domain, the researcher demonstrates that the design theory is complete and effective.

Hevner et al. (2004) suggest that the nature of the problem, characteristics of the artifact, and available resources dictate the selection of the evaluation method. Hevner et al. (2004) state that any of the evaluation methods available in the knowledge base may be used to rigorously evaluate an IT artifact.

Five different kinds of evaluation methods, namely observational, analytical, experimental, testing, and descriptive have been suggested to evaluate a design artifact.

The observational evaluation method involves the use of case study and field study to evaluate the design artifact. The observational methods allow studying and monitoring the artifact in depth in the real business environment. *The analytical evaluation method* encompasses static analysis, which evaluates the structure of the artifact for static qualities; architecture analysis, which studies the technical fit of the artifact into the IS architecture; optimization, which is used to demonstrate optimal properties of the artifact; and, dynamic analysis, which evaluates the artifact in terms of dynamic qualities. *The experimental evaluation method* involves the use of controlled experiments and simulation to study the artifact qualities and functionality. *The testing evaluation method* consists of functional and structural testing. Functional testing considers the artifact as a “black box” and therefore evaluates its interfaces to identify any failures and/or defects in the operation of the artifact. Structural testing considers the artifact as a “white box” and evaluates the artifact using some metrics in the artifact implementations. The last evaluation method, *the descriptive method* encompasses the use of informed argument and scenarios. The informed argument relies on the application of knowledge base to illustrate and demonstrate the utility of the artifact. The scenarios method consists of using scenarios to demonstrate the artifact’s utility.

Baskerville et al. (2007) suggest that in order to have a comprehensive evaluation approach and to avoid errors during the evaluation processes, a combined evaluation approach that includes “hard methods”, such as experiments, and “soft methods”, such as

case studies, should be used. Consistently with Baskerville et al. (2007) and Hevner et al. (2004), we demonstrate the utility and efficacy of *SSeBP* design theory by evaluating its outputs, *SSeBP* design artifacts. We use a multi-method and rigorous evaluation approach that includes descriptive, observational, and experimental evaluations.

For the descriptive evaluation, we use the *Collaborative Planning Forecasting and Replenishment* (CPFR) approach, which is an emergent standard developed by the industry to deal with demand uncertainty. It seeks to develop collaborative relationships between buyers and sellers through co-managed processes and shared information (www.VICS.org). Its standards provide the templates for collaborative inter-organizational business processes in the value chain. Since CPFR's standards are developed and adopted by a wide array of firms, evaluating the applicability of *SSeBP* design artifacts to CPFR process templates provides a level of generalizability to the *SSeBP* design theory. In addition, CPFR guidelines do not include sharing *process knowledge* across partner organizations and its *technical specifications do not include security knowledge*. We demonstrate the utility of *SSeBP* design theory by showing how to model and enhance CPFR process templates as secure business processes using *SSeBP* design artifacts.

Even though industry standards such as CPFR provide guidelines for business processes, they are not intended to capture nuances of the real world. Therefore, for the *SSeBP*'s observational evaluation, we conduct a detailed case study at a leading apparel business, a Fortune 100 organization and its key customer, a Fortune 50 retailer. We apply *SSeBP* design theory to illustrate its application in mapping core business processes

of the selected organization. We show how *SSeBP* design artifacts resolve semantic conflicts and enable the exchange of component, process and security knowledge in the context of a real organization. We use multiple decision makers in the IT and other functional areas to evaluate the *SSeBP* design artifact's utility.

For the experimental evaluation, we use Situational Awareness (SA) theory (Endsley, 1995) to empirically evaluate the *SSeBP* artifacts against an existing approach. Situational Awareness (SA) theory explains how individuals perceive, comprehend, and predict elements' meaning and status. The objective of the experimental evaluation is to illustrate how *SSeBP* design artifacts generate security awareness at least as well as existing methods. Specifically, we assess the efficacy of *SSeBP* design artifacts in representing access control mechanisms that prevent unauthorized access to information resources, provide non-repudiation mechanisms, and allow for segregation of duties. Thus, an experimental design that demonstrates the utility of *SSeBP* is developed and executed.

The following sections of this chapter present a detailed description and discussion of the results of the descriptive, observational, and experimental evaluation of *SSeBP* design theory.

4.1.Descriptive Evaluation of the Secure Semantic eBusiness Processes Design Theory

To show *SSeBP* design theory's utility, we describe how business processes from the Collaborative Planning, Forecasting, and Replenishment (CPFR) approach can be modeled and enhanced by the application of the *SSeBP* design theory. Since CPFR is an industry standard, adopted by several organizations, evaluating the applicability of our approach with CPFR's process templates provides a level of generalizability to *SSeBP* design theory.

The descriptive evaluation's goal is to illustrate how business processes can be analyzed, mapped and enhanced by using *SSeBP* design artifacts. In addition, we develop and validate description logics (DL)-based semantic knowledge representation for activity resource coordination of CPFR eBusiness processes. By developing such DL, we illustrate the technical feasibility of the *SSeBP* design artifacts. DL-based knowledge representation provides machine-interpretable knowledge representation and computational ontologies in OWL-DL format to support knowledge integration in collaborative inter-organizational eBusiness processes.

4.1.1. Collaborative Planning, Forecasting, and Replenishment (CPFR) Approach

Successful supply chain management involves the coordination of activities performed by multiple independent companies to deliver a product or service to the end customer (Lee and Whang, 1998). Several factors affect the success of supply chains.

Demand uncertainty has always been a topic of interest for the academic and practitioner communities. Swaminathan and Tayur (2003) explain that the Collaborative Planning, Forecasting, and Replenishment (CPFR) is an approach aimed at alleviating the issues related to demand uncertainty. CPFR attempts to create collaborative relationship between buyers and sellers through co-managed processes and shared information (www.VICS.org). CPFR standards provide the templates for collaborative inter-organizational business processes. CPFR aims to make pertinent information available to all members of the supply chain to improve its efficiency. In particular, seamless flow of information across the supply chain helps to coordinate and improve the accuracy of the critical demand forecasting and capacity planning information. According to the Voluntary Inter-industry Commerce Standards Association (VICS), several leading retailers and manufacturers have successfully adopted CPFR and have obtained benefits such as reducing working capital and fixed capital, reducing operation expensive, improved technology ROI, and growing sales (www.VICS.org). Appendix A shows corporations at various positions in the supply chain that have adopted CPFR.

While several organizations have implemented CPFR models to varying degrees of success, several practical impediments remain. CPFR guidelines do not include sharing process knowledge across partner organizations and do not consider how private and proprietary information and knowledge can be systematically and securely shared while maintaining information assurance concerns. *CPFR technical specifications do not include security knowledge*. In other words, the permissions about the kinds of activities agents can perform over resources are missing. Atallah et al. (2005) highlight the need to

secure CPFR data flows through a Secure Multi-Party Computation framework. They explain that the fear that a supply-chain partner may take advantage of private information or that information may leak to a competitor is preventing organization from adopting the CPFR approach. The lack of appropriate access control mechanisms on the information and knowledge exchange among business activities leaves organizations vulnerable to various information assurance threats and prevents them from engaging in collaborative eBusiness process.

CPFR specifies nine primary business processes and data flows needed to enable collaboration among business partners. Table 7 summarizes the main CPFR's business processes and data flows.

Business Process	Data Consumed	Data Produced
Develop Front End Agreement	(None; Manual process)	(None; Manual process)
Create Joint Business Plan	Buyer's Corporate Strategy	Joint Business Plan
Create Sales Forecast	Joint Business Plan POS Data Event Sales Forecast Revisions	Sales Forecast
Identify Sales Forecast Exceptions	Sales Forecast Exception Criteria Metrics Events	Identified Exception Items
Collaborate on Sales Forecast Exceptions	Buyer Secondary Data for Exception Items Identified Exception Items Seller's Secondary Data for Exceptions Items	Sales Forecast Item Revisions
Create Order Forecast	Order Forecast Revisions POS DATA Current Inventory on Hand Sales Forecast Events Product Historical Demand & Shipments Product Availability Data Item Management Profile Data	Order Forecast
Identify Order Forecast Exceptions	Order Forecast Exception Criteria and Values Events	Identified Order Exception Items
Collaborate on Order Forecast Exceptions	Buyer's Secondary Data for Exception Items Identified Exception Items Seller's Secondary Data for Exception Items	Order Forecast Revisions
Generate Order	Order Forecast Item Management Profile	Order

Table 7. CPFR Business Processes and Data Flows (Source: CPFR Technical Specifications, VICS 1999)

From those CPFR business processes, we consider the *Create Order Forecast* and *Generate Order* business processes. These processes are of strategic and tactical importance (Caridi et al., 2005) and require high degree of collaboration and integration. Figure 6 presents the dataflow in the *Create Order Forecast* and *Generate Order* processes. The *Create Order Forecast* dataflow describes the information exchanged in an initial order forecast for products within a planning period. The *Generate Order* dataflow shows the transmission of a “firm” order for products, based on an order forecast and an item management profile (CPFR Technical Specifications, VICS 1999).

More specifically, *Create Order Forecast* and *Generate Order* business processes take place between a buyer and a seller. Sellers and buyers must work together to estimate future orders needs. In other words, they must determine the right products and their quantities that must be ordered for the next planning period. Accurate order forecasts drive sales increases, improve customer service, and support better inventory decisions. The process is triggered at the beginning of each planning period. The buyer organization consolidates its point of sales (POS) data and generates an initial prediction of its sales for the next planning period (sales forecast). Such information, along with the available stock, the promotions and event calendars, including weather, school season, and holidays information, and the historical order shipment data are then retrieved by the seller organization to generate an initial sales forecast. At this point, the buyer and the seller organizations with the assistance of a collaborative information system must compare their initial estimates to reach an agreement. Basically, the collaborative system retrieves information about the buyer inventory strategies, seller order shipment data, and

collaborative policies to determine any differences and/or errors that might exist in the initial sales forecast. Finally, the collaborative system produces the exceptions resolution data that are used to make the corrections or adjustments to the seller and buyer sales forecast.

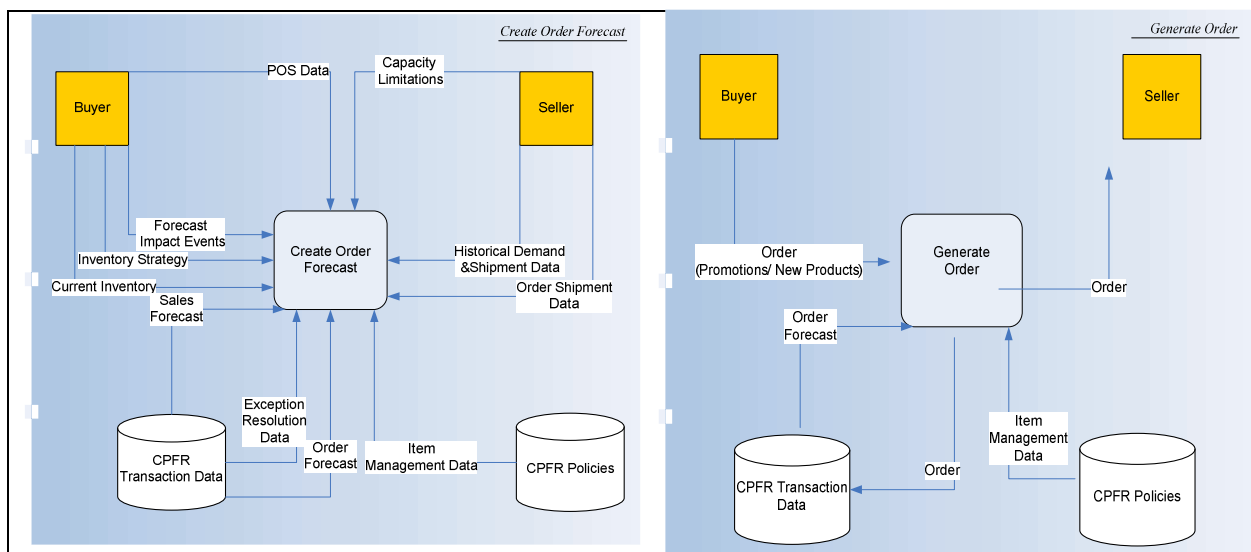


Figure 6. Create Order Forecast and Generate Order Processes Data Flow (Adapted from CPFR Technical Specifications, VICS 1999)

We analyze these business processes using the *SSeBP* meta-design (from Figure

1) and identify the following atomic concepts:

- i) Business Enterprise: Buyer and Seller.
- ii) Business Activities: Communicate POS Data; Communicate Forecast Events; Communicate Inventory Strategy; Communicate Current Inventory; Communicate Order; Communicate Capacity Limitation; Communicate Historical Demand & Shipment; Communicate Order Shipment Data; Create Order Forecast; Generate Actual Order; and Receive Order.

- iii) Resources: POS Data; Forecast Impact Events; Inventory Strategy; Current Inventory; Sales Forecast; Exception Resolution Data; Order Forecast; Capacity Limitation; Historical Demand & Shipment Data; Item Management Data; Order.

By applying the meta-design to the CPFR approach, we create DL formalisms for knowledge representation for such business processes, which form the basis for the development of machine interpretable knowledge representation in the OWL-DL format. All DL knowledge representations have been developed, validated and checked for consistency using Protégé and Racer. Appendixes B1-B4 show the DL for the following business activities and resources: 1) creates order forecast activity, 2) order forecast resource, 3) generates order activity, 4) order resource. Figure 7 shows the results of the DL validation. We did not find any consistency or integrity violations in the DL.

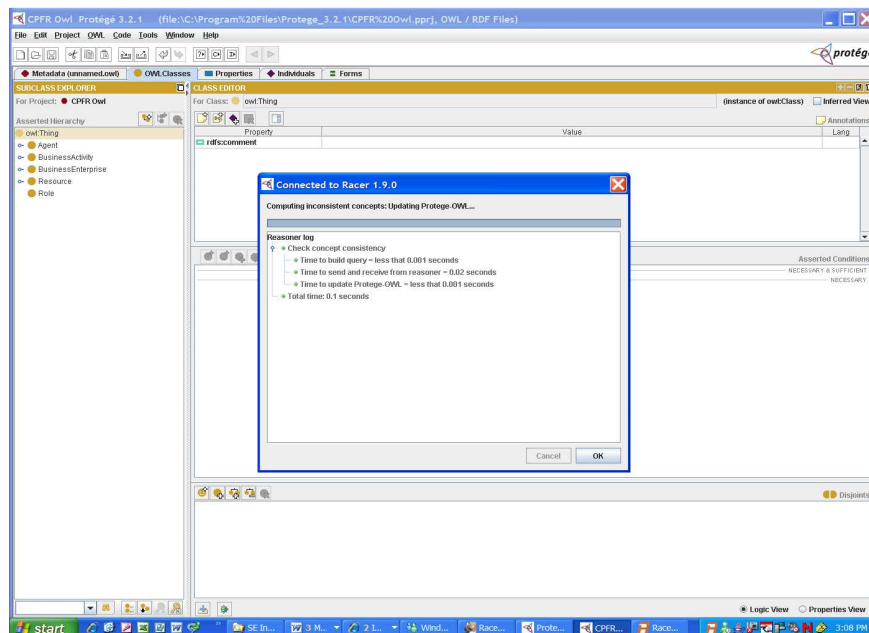


Figure 7. Consistency and Integrity Checks Results

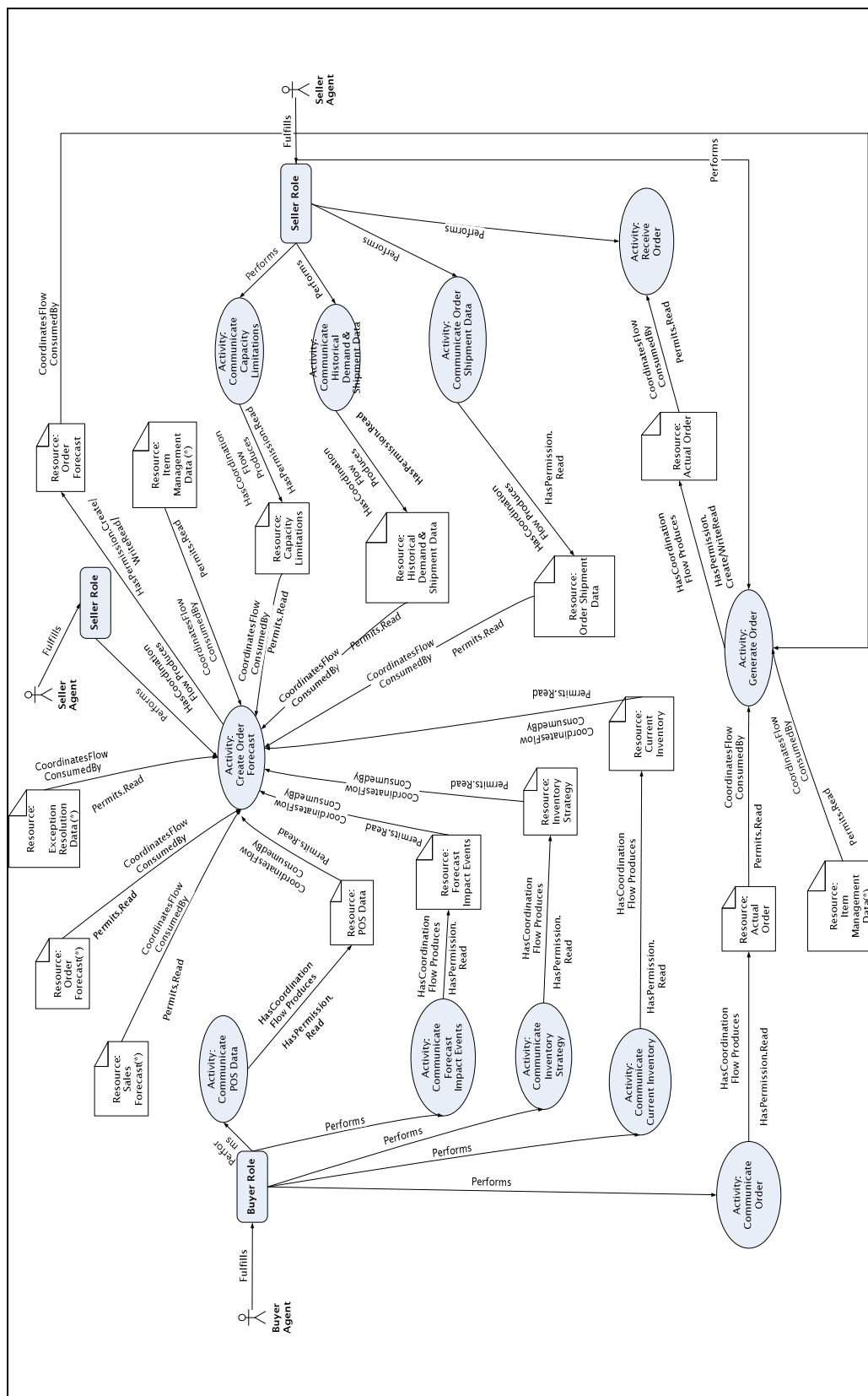
These DL formalisms provide computationally feasible knowledge representation mechanisms for business processes for VICS-CPFR. This forms the basis for the development of machine interpretable knowledge representation in the OWL-DL format. DL is used as the knowledge representation formalism to express structured knowledge in a format amenable for intelligent software agents to reason with it in a normative manner. This illustrates the technical feasibility of instantiations of *SSeBP* design artifacts.

Our design artifact enhances CPFR by incorporating the roles-activities and resource-permissions needed in the business processes. Using RBAC (Sandhu et al., 1996), we show, in Table 8, the role-activity-resource permissions for CPFR's generate order business process.

Agent	Role	Business Activity	Permission Type (Write, Read, Create, Delete)	Resource
Buyer Agent	Buyer Role	Communicate POS Data	Read	POS Data
		Communicate Forecast Events	Read	Forecast Impact Events
		Communicate Inventory Strategy	Read	Inventory Strategy
		Communicate Current Inventory	Read	Current Inventory Data
		Communicate Order	Read	Order
Seller Agent	Seller Role	Communicate Capacity Limitation	Read	Capacity Limitations
		Communicate Historical Demand & Shipment	Read	Historical Demand & Shipment Data
		Communicate Order Shipment Data	Read	Order Shipment Data
		Create Order Forecast	Read	Order Forecast, Sales Forecast, Exception Resolution Data, Item Management Data, POS Data, Forecast Impact Events, Inventory Strategy, Current Inventory, Capacity Limitations, Historical demand & Shipment Data, Order Shipment Data
			Create/Write/Read	Order Forecast
		Generate Actual Order	Read	Item Management Data, Order Forecast Order
			Create/Write/Read	Actual Order
		Receive Order	Read	Actual Order

Table 8. Security analysis for role-activity-resource permissions for the CPFR's generate order business process

The atomic concepts and their relationships in the design artifact are used to map core business processes of CPFR and to incorporate security knowledge in the CPFR models and technical specifications. Figure 8 shows how *SSeBP* design theory's atomic concepts, grammar, and relationships are used to develop the secure semantic activity-resource coordination mapping for the *Create Order Forecast* and *Generate Order* business processes discussed above.



(*) Resources produced in previous business processes)

By applying *SSeBP* design theory to the CPFR *-Create Order Forecast and Generate Order* business processes, we demonstrate how the *SSeBP* meta-requirements, meta-design, and design method, including modeling concepts and grammar, can be used not only to model business processes but to enhance them by incorporating security access control requirements and standard knowledge representation that provide the foundation for the seamless and secure exchange of information and knowledge resources within and across partner organizations in the context of eBusiness processes.

A primary motivation of our design artifact is including security as a functional requirement in the early analysis of the business process. We show how our artifact can be used to analyze and represent granular security requirements for specific CPFR business processes. For instance, based on results of analysis presented in Table 8 and Figure 8, business and system analysts can recognize that the POS Data can only be read by the Communicate POS Data Activity, which can only be performed by the Buyer Role. This implies that if any other business activity tries to modify the POS Data, it would result in a security violation. The Role-Activity Resource permission analysis allows mapping organizational responsibilities into roles, fulfilled by specific agents. In addition, for instance, the seller agent, fulfilling the seller role, is responsible for executing the business activities identified in Table 8. If the Seller Agent, in the Seller role, executes a business activity not identified above, it is a security violation. These analyses, for all agents, roles, activities and resources, can be used to develop security policies for the inter-organization business process.

Although we have not applied our approach to the business processes of organizations that have developed and adopted the CPFR industry standard, demonstrating the applicability of the approach to model processes of an industry standard does provide a level of confidence that the approach presented here can be used by other companies' business processes.

4.2.Observational Evaluation of the Secure Semantic eBusiness Processes Design Theory

The objective of the observational evaluation is to assess the utility and efficacy of *SSeBP* design artifact in the context of a real organization. Yin (2002, pp. 2) states that “case study method allows the investigators to retain the holistic and meaningful characteristics of real-life events”. Case study is used when the researcher wants to address the “how” and “why” type of questions about contemporary events, where the researcher has little or no control over the events. Here, it is important to highlight that case studies play an important role in evaluation research. They can be used to explain, describe, illustrate, explore, and meta-evaluate the phenomenon of interest (Yin, 2002).

We demonstrate the utility of the proposed design theory by applying *SSeBP* design theory to analyze and map core business processes of an organization and their security requirements. The researcher, with the assistance of Supply Chain and IT senior managers from the selected organization, identify core business processes that exhibit the characteristics of the problem domain. We show how the resulting *SSeBP* artifacts lay the foundation to resolve semantic conflicts and enable the exchange of component, process

and security knowledge in the context of a real organization. Finally, we use multiple decision makers in the IT and other functional areas from the chosen organization to assess the *SSeBP* design artifact's utility.

4.2.1. Applying the Secure Semantic eBusiness Processes Design Theory: A Case Study

We analyzed business processes related to the demand forecast and capacity planning business processes for *Organization A* and its primary customer. These processes were selected because of their strategic value. In addition, they require an exchange of information and knowledge resources within and across organizations while a secure and seamless flow of information and knowledge is guaranteed. We conducted open-ended interviews on key stakeholders to have a better understanding about the current business processes and the challenges that *Organization A* faces in securing and integrating them. Specifically, we interviewed senior managers in IT, planning, customer management and operations, and demand analysts. Questions related to the business processes' background, stakeholders' roles and responsibilities were asked. In addition, we reviewed and analyzed different information systems and documentation that pertain to the *Create Order Forecast* and *Generate Order* (COFGO) business processes of *Organization A*.

Organization A is a leader in the apparel industry, with annual revenues of over \$1.2 billion for the fiscal year of 2005. It designs and manufactures clothing that is distributed to warehouses and retailers throughout the world. *Organization A's* demand

is fragmented into a few large customers that account for approximately 65% of its revenues. *Organization A's* demand is highly sensitive to seasonal and fashion volatility, which is common in the apparel industry. *Organization A's* COFGO business processes require information and knowledge resources from multiple business units, including replenishment, forecasting, planning, and procurement, from within *Organization A* and across partner organizations. Further investigation of *Organization A's* COFGO processes reveals the following issues in automating the secure and seamless exchange of information and knowledge resources needed for the business processes.

- *Organization A* and its primary customers are advocates of the CPFR approach. While they implement CPFR models to varying degrees of success, several practical impediments remain. CPFR guidelines do not include sharing process knowledge across partner organizations in a systematic manner, and do not consider how private and proprietary information and knowledge can be systematically and securely shared while maintaining information assurance concerns. Paraphrasing the director of planning and replenishment “Our organization is trying to have a collaborative process, but in reality we are struggling to make it happen”.
- According to *Organization A's* Director of Planning and Replenishment, COFGO business processes are very complex and require integration of information from multiple business units of *Organization A* and its customers. It requires coordinated information exchange across the customer's decision support system for Point of Sales (POS) data, a logistic system and two CPFR systems. Currently, *Organization A's* planning analysts use several spreadsheets to develop an annual demand and

capacity plans for each Stock Keeping Unit (SKU) per week. There are seven product categories with hundreds of SKUs. Ten planning analysts maintain and analyze these spreadsheets and manually feed the forecasting systems. This literally requires using every column available in an Excel spreadsheet.

- Frequent manual data entry interventions are needed to identify and record demand adjustments for every product, due to seasonality and promotions. Bi-weekly meetings between the customer, planning analysts, and replenishment analysts are needed to analyze the differences between the *real* demand, the *expected* demand, and the historical demand forecast from the system. This “collaborative” demand forecasting process results in a final, agreed-upon, weekly demand per SKU. The customer development manager notes: “This process is very inefficient. We have to manually feed the seasonality and special offers indicators for each product into our systems and into the customer systems, and on top of that if any error occurs, *we have to manually do the adjustment and absorb the cost, if any*”.
- Given the extent of manual processes and heterogeneous information systems, it is very difficult to develop and enforce security policies in a systematic manner. Manual and ad-hoc processes are difficult to secure and monitor, and almost impossible to audit. Separation of duty and non-reputation mechanisms has not been implemented at all. A single organizational log-in is used to access the primary customer’s systems with read and write privileges. This is exacerbated by sharing of the authorization credentials with various organizational roles due to the need for information and knowledge. While changes submitted to the customer’s system are subject to approval

by the customer, a systematic method of non-repudiation and segregation of duty in identifying and adjusting exceptions to demand forecast is clearly lacking. As a result, critical information for demand forecasting, is shared verbally in meeting or is not shared at all with customers.

- *Organization A* does not have a single production forecasting system in place. Due to several mergers and acquisitions, production units have their own forecasting systems that range from customized packages to spreadsheets. Demand forecasts are manually input to each system on a weekly basis.
- *Organization A* uses EDI with its primary customers. However, semantic conflicts stemming from new product descriptions, the customer's promotion codes and packaging and bundling for *Organization A's* promotions, occur frequently. The customer development manager explained that *Organization A* distributes customer orders to various warehouses served by the customer's logistics. These three business organizations each use different units of measurements for ordering. A package for a warehouse system could be a pallet of thousands of items, while the package for customers could be a dozen items. *Organization A* has to determine the correct measurement unit for each order by analyzing its final destination. *Organization A* managers use lookup tables for units of measurement for various shipment types and manually translate from one type to another for recording as product moves from one business activity to another. Once conflicts are resolved, revisions are manually entered by customer development officers and approved by directors of planning and

execution. “*Can you imagine the kind of confusions and rework this simple error might produce if we didn’t spend time looking at each order?*”

It is important to highlight that *Organization A* was a leader in the development of the CPFR approach. It has adopted CPFR approach with their main customers, albeit with several modifications. In addition to the standard CPFR’s dataflows depicted on Figure 6, *Organization A* provides information about orders’ adjustments, event calendar, and cancellation to the buyer organizations. An analysis of the COFGO business processes using *SSeBP* meta-design reveals the following atomic concepts:

- i) Business Enterprise: Buyer and Seller.
- ii) Business Activities: Communicate POS Data; Communicate Event Calendar; Communicate Inventory Strategy; Communicate Available Stock; Communicate Sales Forecast; Communicate Exception Resolution Data; Receive Adjustments; Communicate Adjustments; Communicate Historical Demand and Shipment Data; Communicate Order Shipment Data; Communicate CPFR policies; Communicate Item Management Data; Communicate Cancellations; Communicate Order (Promotions// New Products); Communicate Order Forecast; Create Order Forecast; Generate Order; Received Order.
- iii) Resources: POS Data; Event Calendar; Inventory Strategy; Available Stock; Sales Forecast; Exception Resolution Data; Adjustments; Historical Demand and Shipment Data; Order Shipment Data; CPFR policies; Item Management Data; Cancellations; Order (Promotions// New Products); Order Forecast.

Applying the design artifact leads to a design where agents can perform activities that heretofore were manual. Standardized ontologies represent *component*, *process*, and *security knowledge* for streamlining collaborative eBusiness processes, while semantic inter-operability problems are solved in a systematic manner that lends itself to automation. To identify the key organizational roles and functions associated with the

Create and Generate Order Forecast, we interviewed the *Organization A*'s director of planning and replenishment. We gathered information about the roles and permissions that the different actors have in the *Create Order Forecast* and *Generate Order* processes and analyzed them using RBAC (Sandhu et. al, 1996), to develop the role-activity-resource permissions shown in Table 9. Three primary roles, namely planning, replenishment, and demand forecast are shown. It is noteworthy that the buyer organization presents similar roles to those of *Organization A*.

Agent	Role	Business Activity	Permission Type (Write, Read, Create, Delete)	Resource
Buyer Planning Agent	Planning Role	Receive Adjustments	Read	Adjustments
		Communicate POS Data	Read	POS Data
		Communicate Events Calendar	Read	Events Calendar
		Communicate Available Stock	Read	Available Stock
		Communicate Order (Promotions//New products)	Read	Order (Promotions//New products)
Buyer Replenishment Agent	Replenishment Role	Communicate Inventory Strategy	Read	Inventory Strategy
		Communicate Sales Forecast	Read	Sales Forecast
		Communicate Exception Resolution	Read	Exception Resolution Data
Seller Planning Agent	Planning Role	Communicate Adjustment	Read	Adjustment
		Communicate CPFR Policies	Read	CPFR Policies
		Communicate Item Management Data	Read	Item Management Data
		Create Order Forecast	Read	POS Data, Events Calendar, Inventory Strategy, Available Stock, Sales Forecast, Exception Resolution Data, CPFR Policies, Item Management Data, Historical Demand & Shipment Data
			Create/Write/Read	Order Forecast
Seller Forecast Agent	Demand Forecast Role	Communicate Historical Demand & Shipment	Read	Historical Demand & Shipment Data
		Communicate Order Shipment Data	Read	Order Shipment Data

Agent	Role	Business Activity	Permission Type (Write, Read, Create, Delete)	Resource
Seller Replenishment Agent	Replenishment Role	Receive Order	Read	Order
		Communicate Item Management Data	Read	Item Management Data
		Communicate Cancellations	Read	Cancellations
		Generate Actual Order	Read	Order (Promotions and New Products), Order Forecast, Item Management Data, Cancellations
			Create/Write/Read	Order

Table 9. Security Analysis for role-activity-resource permissions for the *Organization A's Create Order Forecast* and *Generate Order* processes

Using the atomics concepts, grammar, and relationships from our artifact, we show how the *Create Order Forecast* and *Generate Order* processes can be mapped to the semantic activity-resource coordination of the design artifact. Figure 9 shows the secure semantic activity-resource coordination for the *Create Order Forecast* business process.

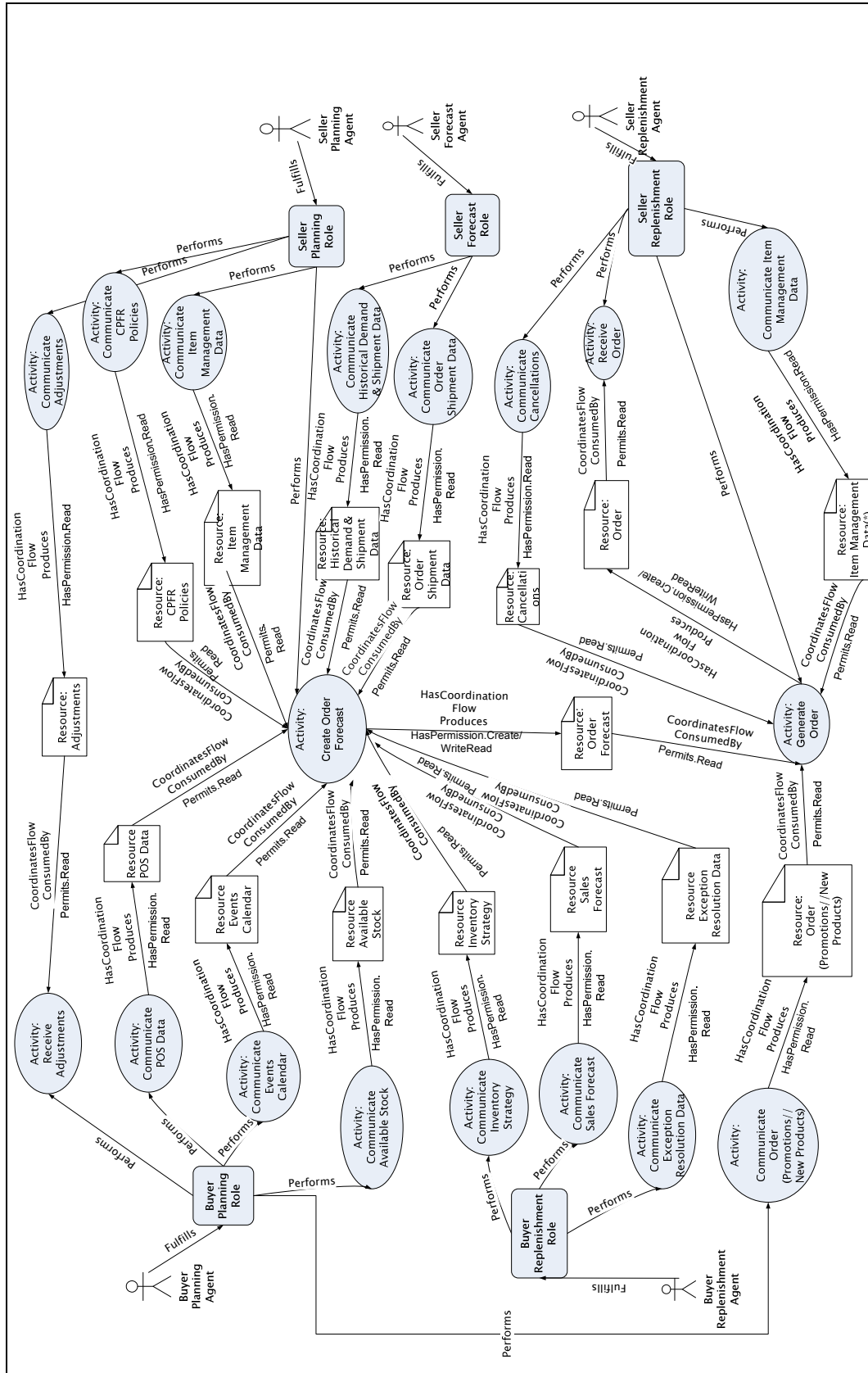


Figure 9. Organization A's Semantic activity-resource coordination For Generate//Create Order Forecast

We show the ontological engineering using DL-based definitions for the activity resource coordination for *Organization A*. It is important to highlight that these demand requirement characteristics are intended to serve as examples and they are not exhaustive. In the create order forecast business process, the buyer business enterprise is represented by a buyer planning agent and by a buyer replenishment agent. The security of the *Organization A*'s Generate Order Forecast and Create Order business process is incorporated through the role-activity-resource permissions mapping.

$$\begin{aligned} \text{PlanningRole} \subseteq & \\ & (=1 \text{ isRepresentedBy . BuyerPlanningAgent}) \wedge \\ & (=1 \text{ Performs. ReceiveAdjustments}) \wedge \\ & (=1 \text{ Performs. CommunicatePOSData}) \wedge \\ & (=1 \text{ Performs. CommunicateEventsCalendar}) \wedge \\ & (=1 \text{ Performs. CommunicateInventoryStrategy}) \wedge \\ & (=1 \text{ Performs. CommunicateAvailableStock}) \wedge \\ & (=1 \text{ Performs. CommunicateOrder_Promotions_New Products}) \wedge \\ & (=1 \text{ Performs. CommunicateOrderForecast}) \end{aligned}$$

$$\begin{aligned} \text{ReplenishmentRole} \subseteq & \\ & (=1 \text{ isRepresentedBy . BuyerReplenishmentAgent}) \wedge \\ & (=1 \text{ Performs. CommunicateSalesForecast}) \wedge \\ & (=1 \text{ Performs. CommunicateExceptionResolution}) \end{aligned}$$

The business activities: *Receive Adjustments*, *Communicate Adjustments*, and *Create Order*, and the resources: *Adjustments* and *Order Forecast*, from Figure 9, are critical to this business process and their DLs are shown in Appendixes B5-B9.

These DL formalisms provide computationally feasible knowledge representation mechanisms for business processes for both VICS-CPFR and *Organization A*'s case study. This forms the basis for the development of machine interpretable knowledge representation in the OWL-DL format. We utilize DL as the knowledge representation formalism to express structured knowledge in a format amenable for intelligent software

agents to reason with it in a normative manner. Understanding the inherent relationships among business processes within and between organizations is a key topic of the information systems field.

All DL knowledge representations presented in this research have been developed, validated and checked for consistency using Protégé and Racer. These tools generate OWL-DL knowledge representations essential to development of semantic collaborative inter-organizational business processes incorporating reasoning and inferencing mechanisms based on DL-formalism. The use of standard semantic models such as W3C's OWL (Web Ontology Language) and OWL-DL transforms this approach into a truly implementable framework without loss of theoretical robustness. These provide the basis for practitioners to initiate further development and evaluation of secure semantic eBusiness processes that are semantically rich, highly coordinated and seamlessly integrated.

By applying the *SSeBP* design theory to COFGO business processes, we provide the foundation to develop semantic wrappers aimed at reducing manual inputs and adjustments. The standard ontology that is used to represent the information related to such adjustments and activities are represented in a machine-readable format. This allows the activity to be automatically performed by seller and buyer agents while managing semantic inter-operability in a secure and coordinated manner.

As the final step of *SSeBP* design theory observational evaluation, the semantic process mappings presented in the previous section were the subject of multiple discussions with managers and analysts at *Organization A*. Such stakeholders are directly

responsible for systems support for demand forecasting, capacity planning and customer development with specific responsibility for the business with the customer organization. In addition, we held follow-up interviews with the CIO of the organization and the director of planning and replenishment. Specifically, the proposed artifact was evaluated with respect to the motivating problems identified before. The results show that the proposed artifact allows for mapping and representing security requirements of business processes leading to segregation of duties and non-repudiation of business activities.

Organization A's CIO recognizes that *SSeBP* design artifacts would help them to develop formal controls to guarantee the integrity and confidentiality of critical data sources in the context of a business process. The *SSeBP* artifacts describe access control and security constructs that allow local and global entities to share and describe various security requirements in common semantics for distributed knowledge and information exchange. Paraphrasing the remarks of *Organization A's* CIO, this helps us understand the delicate balance between accessibility, transparency and security and allows us to put documented security needs on the table in discussions with the customer organizations.

In addition, the *SSeBP* design artifact lays the foundations for semantic conflict resolution and integration of multiple dispersed data and information sources by providing common semantics for distributed knowledge and information exchange. Delineation of a common ontological structure for the information exchanged between the organizations provides a basis to move manual processes back into the systems. Implementing a common ontology of resources for these business activities will allow *Organization A* to move these activities from a time-consuming and error prone manual

process that is currently conducted out of the system to one that requires managerial oversight and approval. In this way, errors can be avoided and significant amounts of time can be saved by managing the semantic conflict resolution by exception rather than as the norm, as is the current practice. *Organization A* currently hosts weekly meetings with the customer where managers sit with individual laptops and resolve issues with semantic conflicts for a variety of ad-hoc issues including new products, promotion codes for the customer organization and packaging issues for *Organization A* and product bundling for promotions. When conflicts are resolved and agreements are reached, the revised information is manually entered by customer development officers and directors of planning and execution. The proposed *SSeBP* design artifacts can be used to develop semantic wrappers to dynamically solve semantic conflicts and feed the subsequent systems. An overall view of the business process and its constituent business activities, along with semantically consistent ontological definitions of the various resources utilized in the business process, assists in common vocabulary for establishing and institutionalizing a standard vocabulary of terms used in the process. This saves valuable time and money, and also reduces the chance of errors in data input, in the affected business process. *Organization A's* director of planning and replenishment said “this kind of approach will help us to integrate multiple dispersed data and information sources, to reduce inaccurate information and errors, and definitively it will assist us in advancing toward having real collaborative processes”.

A primary motivation of *SSeBP* design artifacts is to analyze, express and incorporate access control policies that comply with security requirements for activities and resources involved in business processes within and across organizations. *Organization A's* management expressed that the proposed IT artifact requires them analyze and define the relationships between organizational roles, and the activities that they perform. It assists in analysis of roles and in the identification of issues with segregation of duties within and across the organization in the context of the eBusiness process. The analysis, with the resultant secure activity resource coordination mapping provides everyone, including the customer organization, with a detailed representation of the inter-organizational business process. This includes the activities to be performed, the resources produced and consumed by the activities and their inter-relationships. In addition, it provides an analysis of the organizational roles needed by both organizations. The *SSeBP* design artifact provides an understanding of the resources that are needed by the activities and the human or software agents that will have access to these resources. The mapping provides granular information about the organizational responsibilities associated with a particular role and allows process designers to incorporate a detailed analysis of the security requirements of the business process for partner organizations. This creates the foundations for incorporating security requirements as functional requirements in the early analysis of the business processes, which is critically needed in the development of methods for the design of secure information systems (Siponen et al., 2006).

Based on the findings from the discussion and follow-up interviews, business and IT executives felt that the proposed IT artifact has significant impact on the issues that are considered in the planning of business processes, as well as the systems that support them. They were most interested in the security aspects of the planning processes. In particular, they were interested in incorporating a review of the security requirements and policy needs of business activities. Since *Organization A* has recently undertaken a significant Sarbanes-Oxley compliance effort, the issues of segregation of duty and non-repudiation of business activities were of significant interest. In particular, the systematic management of exceptions and demand forecast adjustments through the mapping presented in this research was perceived as useful for the organization. An additional benefit of the concepts presented in this research as perceived by the *Organization A* was the possibility of dynamic and flexible supply chain configuration for handling ad-hoc requests from the customer organization. Common and shared ontology serve as a means to resolve conflicts and move towards more seamless integration between systems within and across both *Organization A* and the customer organization in a secure manner.

We have shown how *SSeBP* design theory atomic concepts and grammar can be applied to analyze and represent real-world core business processes. Specifically, *SSeBP* design artifacts allow the analysis and design of business processes that require the exchange of information and knowledge resources within and across organizations while a secure and seamless flow of information and knowledge are guaranteed. By using real core business processes, we capture both the information and knowledge, including component, process, and security knowledge related to the business processes and the

richness of the organizational environment. *SSeBP* design artifacts' utility was evaluated and demonstrated by using the inputs from different stakeholders. We illustrate how *SSeBP* design theory provides a holistic framework to integrate *component*, *process*, and *security* knowledge that enables the sharing of information and knowledge resources in a coordinated and secure manner within and across organizations of a value chain. Thus, we have shown using an observational evaluation method that the *SSeBP* design theory prescribes the models (meta-requirements); methods (*development practices*), and mechanism for artifact instantiation (*system solution*) as suggested by Hevner et al. (2004) and Walls et al. (1992).

4.3.Experimental Evaluation of the Secure Semantic eBusiness Process Design Theory

In design science research, experimental evaluations assess the utility of design artifacts, which are the instantiations of the design theories. Evaluating the proposed design theory using an experiment empirically demonstrates the qualities of the artifact (Hevner et al., 2004) and allows for the generalizability of the findings. Walls et al. (1992) suggest an experimental design where the performance of the experimental group using the IT artifact is compared against the performance of the control group not using the IT artifact.

A primary purpose of the *SSeBP* design theory is to incorporate security requirements into the conceptualization of business processes. The experimental evaluation of *SSeBP* design theory assesses how design artifacts developed using *SSeBP*

generates awareness of security constraints in modeling the secure exchange of information resources in coordinated business processes. Situational Awareness (SA) (Endsley, 1995) theory explains how individuals perceive, comprehend, and predict elements' meaning and status. We use Situational Awareness theory as foundation to assess how an individual perceives, comprehends, and predicts security elements in the context of a business process.

UML-Use case, sequence, collaboration and activities diagrams are relevant for process modeling (Glassey, 2008). However, the UML approach does not specifically address security aspects during the analysis and design phases of information systems or business processes. Siponen et al. (2006) propose a meta-notation framework to represent and analyze information systems security requirements. They extend the UML-Use Case to incorporate security requirements into the design phase. Enriched-Use Case incorporates security constraints, security subjects, and security actors into the design of information systems. We empirically evaluate the difference between the security awareness generated by the SSeBP design artifact and the security awareness generated by the Enriched-Use Case (Siponen et al., 2006) and UML-Activity diagram. Specifically, we study how *SSeBP* design artifacts and the Enriched-Use Case (Siponen et al., 2006) and UML-Activity diagrams allow analysts to identify, explain and predict security constraints and violations in a business process.

The following sections describe this empirical evaluation including the research model, research hypotheses, experimental design, data analysis, and results.

4.3.1. Research Model

Business process models are used to increase the awareness and knowledge about business processes and to decouple organizational complexity (Davenport, 1993; Hammer and Champy, 1993). Existing methods for the design of secure information systems still lack a conceptualization of secure business process. We evaluate the utility of *SSeBP* design theory in representing security constraints in the conceptualization of a secure business process. We use situational awareness theory (Endsley, 1995) to empirically evaluate the *SSeBP* design artifacts against the Enriched-Use case (Siponen et al., 2006) and UML-activity diagram. We assess how *SSeBP* design artifacts help in developing a greater level of security awareness.

We argue that when security specifications are incorporated as functional requirements early in the modeling and analysis of business processes, analysts become more aware of security constraints and possible violations resulting into more secure business processes. This, in turn, leads to the incorporation of security policies and constraints in subsequent stages of information systems development, including modeling, analysis, and design.

We expect that *SSeBP* design artifacts lead to greater security awareness, including the perception, comprehension, and prediction of security requirements and constraints in business processes. Figure 10 shows the research model.

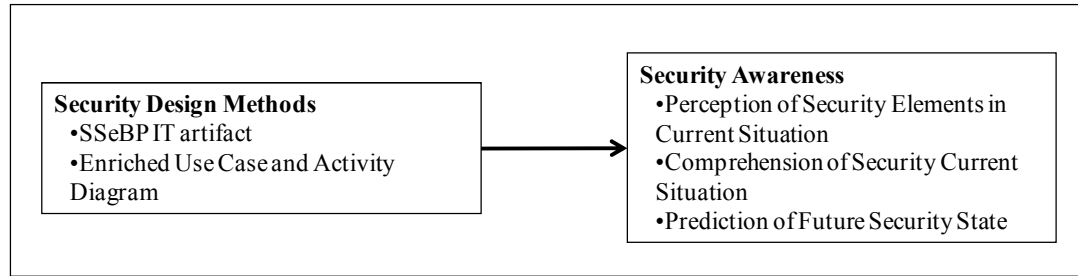


Figure 10. Research Model to Test Security Awareness

4.3.1.1. Research Hypotheses

According to Larkin and Simon (1987, p. 67) “two representations are informationally equivalent if all the information in the one is also inferable from the other, and vice versa”. Even though *SSeBP* and the Enriched-Use Case and UML-Activity diagrams provide two different representations for the same business process, we must ensure that *SSeBP* design artifacts are at least informationally equivalent to Enriched-Use Case and UML-Activity diagrams in capturing the dynamics of business processes. Only then we guarantee that our approach is at least as good as existing approaches and does not create any loss of information about the business process. Therefore, we must first test that the two approaches are *informationally equivalent*. This is tested in hypothesis H1 by comparing the inferences that users make about the business processes represented using *SSeBP* design artifacts and the Enriched-Use Case (Siponen et al. 2006) combined with the UML- activity diagrams.

H1: Business Process Models (BPM) represented by SSeBP and Enriched-UseCase combined with UML activity diagrams are informationally equivalent.

A primary goal of conceptual process modeling of business processes is to provide a better understating about activities, resources, and dependencies present. In particular, a business process model (BPM) developed using *SSeBP* design theory must convey a better security awareness than those developed using Enriched-Use Case and UML-Activity diagram. We hypothesize that:

H2: BPM developed using SSeBP Artifact creates a higher level of security awareness than a Business process model developed using an Enriched Use Case and Activity Diagram.

More specifically:

H2a: BPM developed using SSeBP Artifact creates a more accurate perception of security elements (i.e.: segregation of duties, non-repudiation, and authorization), in a business process than those using the Enriched Use Case and Activity Diagram.

H2b: BPM developed using SSeBP Artifact creates a more accurate comprehension perception of security elements (i.e.: segregation of duties, non-repudiation, and authorization) in a business process than those using the Enriched Use Case and Activity Diagram.

H2c: BPM developed using the SSeBP Artifact creates a more accurate prediction of the future security state of the business process, that those using the Enriched Use Case and Activity Diagram.

4.3.2. Experimental Design

An experimental design consists of four elements: (i) a set of treatments; (ii) a set of experimental units; (iii) rules for assigning treatments to experimental units; and (iv) measurements on the experimental units (Neter et al., 1990).

We empirically compare the utility of two treatments in generating security awareness. A simplified version of a “create order forecast” business process was selected as the scenario for both treatments. We based our selection on the fact that “create order forecast” business process requires that business partners exchange high volume of information in a secure and coordinated manner. With the help of demand and forecast analysts from *Organization A*, we developed the description for the scenario. Appendix D presents the narrative for the “create order forecast” business process. Treatment A consists of Enriched-Use Case and UML-Activity Diagram. We followed Siponen et al. (2006) guidelines to develop the Enriched-Use Case representation, and to develop the UML-Activity diagram, we followed the Object Management Group’s guidelines (OMG, 2003). Figure 11 and 12 show Enriched-Use Case and UML-Activity Diagram respectively. We validated these figures with the help of the CIO and systems analysts from the Organization A.

Use Case:	<i>Create Order Forecast</i>
Scenario:	Create a new Order Forecast
Brief Description:	Determining the right products and quantities that must be ordered for the next planning period
Actors/Security Subjects:	Buyer and Seller
Security Classification of the subject:	All Data Sources are confidential
Security Objects and Access Types to Security Objects:	<p>Object: Buyer Forecast and Inventory Database (the buyer must be able to read and write sales forecast, point of sales (POS) Data, and to read Inventory Strategy)</p> <p>Object: Seller Forecast and Inventory Database (the seller must be able to read sales forecast, POS Data, Available Stock, Events Calendar, Historical Order Shipment Data)</p> <p>Object: Collaborative Planning and Replenishment Database(the collaborative systems must be able to read order shipment, CPFR policies, Inventory Strategy and Item Management Data. The collaborative system must be able to read and write the seller and buyer adjustment forecast and the order forecast)</p>
Security Policy/Specific Security Restrictions	Buyer and Seller are only allowed to access security objects classified as confidential with the planning and replenishment department
Preconditions:	All the Data Sources exists
Flow of Events:	<p>Actor:</p> <ol style="list-style-type: none"> 1. The buyer generates and consolidates its point of sales (POS Data) 2. The buyer generates the initial Sales forecast 3. The seller retrieves the buyer's POS data, available stock, events calendars, and historical order shipment data. 4. The seller generates an initial Sales forecast 5. The buyer sends its inventory strategy 6. The seller sends the order shipment data and retrieve CFPR policies and Item Management Data 7. The collaborative system generates the exceptions resolution data 8. The collaborative system generates the adjustments to the seller and buyer Sales forecast
Exception Conditions:	If information about any object is not available, an appropriate error message is produced.

Figure 11. Enriched- Use Case for the “create order forecast” business process

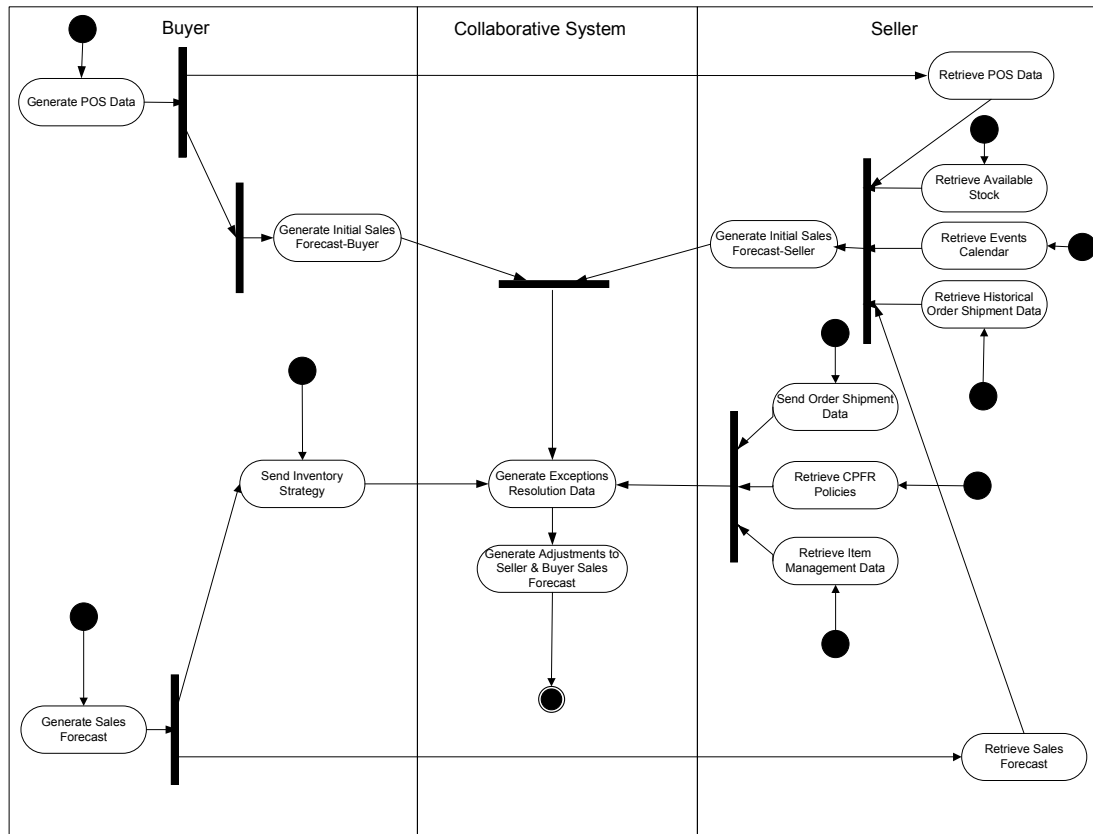


Figure 12. UML- Activity Diagram for the “create order forecast” business process

Treatment B consists of the representation of the “create order forecast” business process using the *SSeBP* design artifacts. We followed *SSeBP* design theory design principles to develop the *SSeBP* Role-Activity-Resource Permissions and the *SSeBP* Secure Activity Resource Coordination diagram for the selected business process, which are depicted in figure 13 and 14 respectively.

Agent	Role	Business Activity	Permission Type	Resource
Buyer Planning Agent	Buyer Planning Role	Generate POS Data	Create/Write/Read	POS Data
		Generate Buyer Initial Sales Forecast	Create/Write/Read	Buyer Initial Forecast Sales
			Read	POS Data, Sales Forecast
Buyer Replenishment Agent	Buyer Replenishment Role	Communicate Sales Forecast	Read	Sales Forecast
		Communicate Inventory Strategy	Read	Inventory Strategy
		Communicate Exceptions Resolution Data	Read	Exceptions Resolution Data
Seller Forecasting Agent	Seller Forecasting Role	Retrieve POS Data	Read	POS Data
		Retrieve Sales Forecast	Read	Sales Forecast
		Generate Seller Initial Sales Forecast	Create/Write/Read	Seller Initial Sales Forecast
			Read	POS Data, Sales Forecast, Available Stock, Events Calendar, Historical Demand Shipment Data
Seller Planning Agent	Seller Planning Role	Retrieve Available Stock	Read	Available Stock
		Retrieve Events Calendar	Read	Events Calendar
		Communicate Historical Demand & Shipment Data	Read	Historical Demand & Shipment Data
		Communicate Order Shipment	Read	Order Shipment

Agent	Role	Business Activity	Permission Type	Resource
		Communicate CPFR Policies	Read	CPFR Policies
		Communicate Item Management Data	Read	Item Management Data
		Generate Exceptions Order Forecast	Read	Inventory Strategy, Buyer Initial Sales Forecast, Seller Initial Sales Forecast, Order Shipment, CPFR Policies, Item Management Data
			Create/Write/Read	Exceptions Resolution Data
		Communicate Exceptions Resolution Data	Read	Exceptions Resolution Data

Figure 13. SSeBP Role-Activity-Resource Permissions for the “create order forecast” business process

Experimental designs with repeated measures have several benefits (Keren, 1993; Brooks, 1980). First, they have high statistical power due to the fact that there will be a positive correlation between treatments. Second, under repeated measures designs, subjects act as their own control and the confounding effects due to different subjects' background are minimized. Finally, repeated-measures designs require fewer subjects as compared to a between-subject design to achieve the same statistical power level.

Despite the benefits of repeated-measures designs, a shortcoming of this type of experimental design is the existence of a carryover or learning effect (Greenwald, 1976), where the former treatment effects are confounded with the results of the first treatment. To address the potential negative consequence of the carryover effect, we follow a counter-balanced repeated-measures experimental design. The effect of the counterbalancing is to spread the unwanted variance arising from the treatment by practice or sequence interaction among the different treatments (Laitenberger et al. 2001).

An experimental design with repeated measures is used to assess the utility of both treatments in generating security awareness. Specifically, we follow a crossover experimental design with two treatments. Under this experimental design, one group receives the treatment sequence $A \rightarrow B$ and another group receives the sequence $B \rightarrow A$. This type of experimental design is equivalent to the 2x2 Latin Square arrangement with two treatments and two periods (Williams, 1949). As a result, the treatments effects are not confounded by the effect of sequences (Kuehl, 2000).

Specifically, in this dissertation, subjects in each group are presented with a detailed scenario describing the “create order forecast” business process. The first group of subjects is given a representation using an Enriched Use-Case description following Siponen et al. (2006) and a UML-activity diagram, (Treatment A). Next, subjects are asked to identify elements of security in the models presented to them including the authorization constraints and security policies. Then, the subjects in the same group are presented with *SSeBP* design artifacts conceptualization (Treatment B) in a table and diagram format of the same business process, followed with a set of questions aimed at identifying elements of security in the models presented to them. For the second group the sequence of the treatment (Treatment B → Treatment A) is swapped to minimize the carryover or learning effect (Laitenberger et al. 2001). Table 10 presents the experimental design.

Group 1	Enriched Use Case and Activity Diagram (Treatment A)	<i>Observation</i>	SSeBP Design Artifacts (Treatment B)	<i>Observation</i>
Group 2	SSeBP Design Artifacts (Treatment B)	<i>Observation</i>	Enriched Use Case and Activity Diagram (Treatment A)	<i>Observation</i>

Table 10. Experimental Design

4.3.2.1. Sampling Strategy

Previous studies aimed at studying conceptual models approaches (Bolloju and Leung, 2006), software inspections (Porter et al., 1994) and systems modeling tools (Jeyaraj and Sauter, 2007; Danesh and Kock, 2005; Agarwal and Sinha, 2003) have successfully used IS students as subjects. This selection is supported by the fact that IS students would become information systems and/or business analysts responsible for the analysis and design of information systems. Therefore, such students resemble the characteristics of information systems and business analysts' population.

For this study, the experimental units are human subjects and the sample consists of undergraduate and graduate students enrolled in business process information technology, information systems analysis and design, and advanced information systems courses.

Participation in the study was totally voluntary; however, the instructors awarded credits for students who participated in the study. Even though there was not a time limit for completing the questions of the experiment, the subjects were expected to complete the questions in not less than 30 minutes. We used a 30 minute cut-off to determine whether or not the subjects answered the questions conscientiously. We set this cut-off time based on the numbers of questions of the instrument and on the average time it took subjects to complete the experiment during the pilot study. A total of 154 students participated in the study and 84 (54.54%) usable answers were obtained. The average time to complete the experiment was 46 minutes, and the minimum and maximum times were 30 min. and 110 min. respectively.

4.3.2.2. Sample Size

An analysis of the relevant literature was conducted to identify the appropriate sample size to test the differences between *SSeBP* design artifact and the Enriched Use Case (Siponen et. al, 2006) combined with the UML-Activity Diagram. Table 11 lists relevant studies with their sample size.

Reference	Sample Size	Subject Types	Experimental Design
Jeyaraj and Sauter (2007)	117	Students	Repeated Measurement- Two treatments
Porter et al. (1994)	48	Students	Repeated Measurement- Two treatments
Laitenberger et al. (2001)	60	Professional Software developers	Replicated Quasi-Experiment Two Treatments
Laitenberger et al. (2000)	18	Practitioners- Programmers	Repeated Measurement- Two treatments
Miller et al. (1998)	50	Students	Repeated Measurement- Two treatments
Agarwal and Sinha (2003)	39	Students	Single Measurement- Four Treatments

Table 11. Sample Sizes Used in Literature

Based on the above analysis, a sample size of at least 18 subjects seems to be appropriate to obtain a significant power of the statistical test. In addition, Kuehl (2000) suggests that the required number of subjects to obtain a power level $(1-\beta)$ of .95 at an α level of 0.01 to be at least 36 subjects and to obtain a power level of .80 at an α level of 0.01 to be at least 24. Based on the extant literature, for this study, we consider that a sample size of at least 50 subjects, students enrolled in information systems related courses, to be appropriate.

4.3.2.3. Research Procedure

Before conducting the study, we obtained approval from the Institutional Review Board (IRB), Office of Research Compliance (ORC) at the University of North Carolina at Greensboro. Copies of the IRB acceptance document and the project description are included in Appendix C.

Subjects completed a questionnaire about their demographics and experience using systems analysis and design methods; UML modeling techniques; business process modeling; and analyzing information security requirements.

The stimulus material in the experiment consists of a “create order forecast” business process represented as Enriched-Use case combined with UML-Activity diagram and *SSeBP* design artifacts. We developed multiple-choice and yes/no type questions to assess the level of security awareness generated by each artifact. The use of these types of questions reduces subjects’ cognitive burden and facilitate the gathering,

verification, and coding of the responses. Appendix D shows the instrument used for this study.

Specifically, to test the level security perception, the first level of situational awareness, subjects answered five questions aimed at identifying elements of security in the models presented to them including the authorization constraints and security policies. The following is an example question to assess security perception:

Who has permission to perform the Communicate Inventory Strategy activity?

- a) Buyer Planning Analyst*
- b) Buyer Replenishment Analyst*
- c) Seller Planning Analyst*
- d) Seller Forecasting Analyst*
- e) All*
- f) None*
- g) It cannot be determined from the information given*
- h) I do not know*

To test the level of security comprehension, second stage of situational awareness, subjects answered five questions aimed at identifying the reasons of security violations. Since comprehension involves some type of explanation power, we use a “why/because” type questions. The following is an example of the questions to assess security perception:

Why? Because

- a) The Buyer Replenishment Analyst has permission to Read the Inventory Strategy information*

- b) The Seller Planning Analyst has permission to Read the Inventory Strategy information*
- c) All analysts have permission to Read the Inventory Strategy information*
- d) Nobody has permission over the Inventory Strategy Information*
- e) It cannot be determined from the information given*
- f) I do not know*

To test security prediction, subjects were presented with five questions about access control violation scenarios and were asked to predict how the business process conceptualization would prevent the threat from propagating through the business process. To assess security prediction, we asked “what would happen if” type of questions. The following is an example of the questions to assess security perception:

What would happen if the Replenishment analyst from the buyer organization does not have permission to read the Inventory Strategy information?

- a) The Communicate Order Shipment activity would not be performed*
- b) The Generate Exceptions Order Forecast activity would not be performed*
- c) The execution of the remaining activities would not be affected*
- d) The Generate Buyer Initial Sales forecast activity would not be performed*
- e) It cannot be determined from the information given*
- f) I do not know*

Finally, to test the level of business process coordination and the information equivalence of the two approaches, using five questions subjects were asked to identify elements of workflows such as predecessors and successors activities needed to complete

the business process. The following is an example of the questions to assess security perception:

Can the activity Generate Exceptions Order Forecast be executed before retrieving CPFR Policies? Yes ____ No ____

In addition, using six questions, the subjects were asked about their perceptions on the utility and efficacy of the *SSeBP* design artifacts and the Enriched-Use Case combined with the UML-Activity diagram. These six questions are assessed using a Likert-scale from 1 to 5, where 1 is equal to “strongly disagree” and 5 is equal to “strongly agree”.

Since we are using an experiment with counter-balanced repeated-measures approach, we ensured that all subjects were exposed to both treatments. To achieve this, subjects were randomly assigned to two groups. Using a different treatment sequence, each group received both treatments. Then after each treatment, subjects were asked the same questions related to security perception, security comprehension, security prediction, and business process coordination. Color coded questionnaires were used to avoid confusion.

It is important to highlight that although feedback helps subjects understand their performance, subjects did not receive any kind of feedback to alleviate the problems related to the learning effect (Basili et al. 1998, Laitenberger et al, 2000). In addition, given the effect that time constrains could have over the subject’s performance (Benbasat and Dexter, 1986; McDaniel, 1990; Payne et al., 1980), we did not impose any time limit to finishing the experiment.

The experiment was conducted between November 2007 and February 2008 and it was run at the University of North Carolina at Greensboro and at North Carolina State University. A total of 154 responses were obtained.

4.3.3. Data Analysis

In this section, we provide a detailed analysis of the data collected from the experiment. Sample demographics and descriptive statistics are summarized. Results from the carryover effect test using the procedure suggested by Grizzle (1965) are presented. Finally, based on the research model, the research hypotheses are tested using paired t-tests. All of the statistical procedures in this study were conducted using SAS version 9.1 running in a Windows environment.

4.3.3.1. Data Preparation

An important step for hypothesis testing is to make sure that the data are in the appropriate form. In this particular case, we use several Microsoft Excel spreadsheets to load and clean the data obtained from the experiment. After the data were loaded into MS Excel, using an answer key the data were then recoded to either correct-value of one, or incorrect-value of zero. Only a few missing values were found and were treated as wrong answers. After a thorough review of the data, inconsistent responses were dropped from the final data set.

4.3.3.2. Sample Demographics

The sample of 84 responses was analyzed based on gender, age, education level, and primary occupation. Tables 12 to 14 provide demographic information about the sample.

	Frequency	Percent
Female	35	41.67%
Male	49	58.33%

Table 12. Gender Distribution

	Frequency	Percent
Less than 18 years	0	0%
18-25 years	51	60.71%
26-35 years	25	29.76%
36-55 years	7	8.33%
More than 55	1	1.19%

Table 13. Age Distribution

	Frequency	Percent
High School	0	0%
Some Years of college	44	52.38%
Bachelors Degree	29	34.52%
Masters Degree	10	11.90%
Doctorate Degree	1	1.19%

Table 14. Educational Level Distribution

Table 14 shows that there is an even representation of undergraduate and graduate students in the sample.

	Frequency	Percent
Full time Employee	18	21.43%
Part Time Employee	17	20.24%
Self-Employed	4	4.76%
Full Time Student	45	53.57%

Table 15. Primary Occupation Distribution

Table 15 shows that an even representation of full time students and professionals exists in the sample. In addition, the sample was analyzed to determine the subjects'

level of experience using System Development Methodologies (SDM), Use Case Diagram and Activity Diagrams.

	Frequency	Percent
No experience in SDM	28	33.33%
College experience in SDM	49	58.33%
Industrial experience in SDM	7	8.33%

Table 16. Level of Experience using System Development Methodologies (SDM)

UML Technique	In School		At Work	
Activity Diagrams	Frequency	Percent	Frequency	Percent
None	25	29.76%	69	82.14%
Less than 6 months	42	50%	11	13.10%
More than 6 months and less than 1 years	12	14.29%	1	1.19%
More than 1 year and less than 2 years	4	4.76%	1	1.19%
More than 2 years	1	1.19%	2	2.38%

Table 17. Level of Experience using UML- Activity Diagrams

UML Technique	In School		At Work	
Use Case	Frequency	Percent	Frequency	Percent
None	56	66.67%	83	98.81%
Less than 6 months	19	22.62%	0	0%
More than 6 months and less than 1 years	7	8.33%	0	0%
More than 1 year and less than 2 years	1	1.19%	0	0%
More than 2 years	1	1.19%	1	1.19%

Table 18. Level of Experience using UML- Use Case

Tables 17 and 18 show that about 30% of the subjects did not have experience using UML-activity diagrams and that 67 % of subjects did not have experience using UML-Use Case. These sample's characteristics were expected; therefore, we included an explanation of how to read UML diagrams in the experiment.

4.3.3.3. Descriptive Statistics

The descriptive statistics for each treatment are broken down into security perception, security comprehension, security prediction, and business process coordination items. Tables 19 and 20 present the minimum (Min), maximum (Max), Mean, Standard Deviation, Skewness, and Kurtosis for each treatment.

	Min	Max	Mean	Std. Dev.	Skewness	Kurtosis
Security Perception	0	5	1.607	0.905	0.769	1.605
Security Comprehension	0	4	1.083	1.1323	0.802	-0.187
Security Prediction	0	4	1.488	1.124	0.238	-0.970
Business Process Coordination	0	4	1.535	1.155	0.126	-1.115

Table 19. Descriptive Statistics for the Enriched-Use Case combined with UML-Activity Diagram

	Min	Max	Mean	Std. Dev.	Skewness	Kurtosis
Security Perception	0	5	4.095	1.001	-1.448	2.9712
Security Comprehension	1	5	3.654	1.023	-0.568	0.016
Security Prediction	0	5	2.547	1.206	-0.240	-0.200
Business Process Coordination	0	4	2.5	1.207	-0.126	-1.263

Table 20. Descriptive Statistics for the SSeBP Design artifacts

A common rule-of-thumb for normality test is to compute the Skewness and Kurtosis values for the sample. Based on the Skewness and Kurtosis values, several cut-off points are suggested for normality test. For instance, the most stringent criterion is to use a range of -1 to +1 for Skewness and Kurtosis. In addition, some authors suggest a range of -2 to +2. And some more moderate authors suggest a range of -3 to +3 (Boneau, 1960; Cohen, 1969). Based on those cut-off points for normality test, it seems appropriate to conclude that the collected data for both treatments fall within the normally distribution range.

In addition, we use six questions with a five point Likert-scale to compare the subjects' perceptions about the utility of the two treatments. We are interested in determining if *SSeBP* design artifacts are perceived to be superior to the Enriched-Use Case and UML-Activity diagrams. Interestingly, *SSeBP* design artifacts are perceived to be better than the Enriched-Use Case and UML-Activity diagrams in representing security aspects of a business process. Table 21 summarizes the results for the subjects' perceptions about the two methods.

Question	<i>SSeBP's Mean</i>	<i>Enriched USeCase & UML-Activity Diagram's mean</i>
Question 1: <i>These diagrams help me to identify the security aspects of a business process</i>	3.59	2.40
Question 2: <i>These diagrams help me to understand the security aspects of a business process</i>	3.52	2.36
Question 3: <i>These diagrams help me to determine what would happen with the business process when security aspects are violated</i>	3.38	2.45
Question 4: <i>The security aspects depicted in the diagrams are easy to understand</i>	3.44	2.38
Question 5: <i>Representations of processes using this approach are clear</i>	3.64	2.67
Question 6: <i>Representations of processes using this approach provide useful security information</i>	3.46	2.34

Table 21. Results for the subjects' perceptions about the two methods

Note: 1= Strongly Disagree; 5 =Strongly Agree

4.3.3.4. Carryover Effect

Carryover, residual, or learning effect is defined as the effect of the treatment from the previous time period on the response at the current time period. It occurs when the effect of a treatment given in the first time period persists into the second period and distorts the effect of the second treatment. Only if the preliminary test for carryover is not significant, the data from both periods are analyzed in the usual manner (Grizzle, 1965). Following Grizzle's procedure to test for carryover effect, we conducted an ordinary least squares (OSL) analysis of variance test with a standard α -level of 0.05 to determine whether there is a carryover effect for the different stages of the security awareness and business process coordination.

For the security perception, we failed to detect a carryover effect (p-value= 0.0614) for the different sequence of treatments. As a result, the order in which the treatments are applied (i.e.: Enriched-Use Case combined with UML-Activity Diagrams → SSeBP artifacts vs. SSeBP artifacts → Enriched-Use Case combined with UML-Activity Diagram) does not have an effect over the observed results for the security perception.

For the security comprehension, we failed to detect a carryover effect (p-value= 0.1100) for the different sequence of treatments. In other words, the order in which the treatments are applied does not have an effect over the observed results for the security comprehension.

For the security prediction, we failed to detect a carryover effect (p-value= 0.1068) for the different sequence of treatments. It means that the order in which the treatments are applied does not have an effect over the observed results for the security prediction.

For the business process coordination, we failed to detect a carryover effect (p-value= 0.4124) for the different sequence of treatments. In other words, the order in which the treatments are applied does not have an effect over the observed results for the business process coordination items.

Given that a carryover effect was not detected for any of the stages of the security awareness and business process coordination, the data from both periods can be analyzed in the usual manner (Grizzle, 1965).

4.3.3.5. Hypotheses Testing

To test our hypotheses, we need to determine whether the mean of one group is statistically significant greater than the mean of another group. A paired t-test is suitable to test mean differences between two groups for repeated measures (Westgard and Hunt, 1973). In addition, t-test statistic is robust against violations of normality and homogeneity of data (Aron and Aron, 1994; Shapiro and Wilk, 1968). We test our hypotheses using a paired t-test. Since there are not previous studies that compare *SSeBP* design artifacts and the Enriched-Use Case combined with UML-Activity diagrams, the effect size for this kind of experiment has not been established; therefore, the a priori

power analysis cannot be determined. In this case, literature recommends a power level of at least 0.8 as a threshold value (Cohen, 1988). Studies with power levels higher than 0.8 have a high probability of rejecting the null hypotheses if they were false (Cohen, 1988). In addition, it is an accepted practice to set an α level of 0.05 to test hypotheses (Fisher, 1948). We adopt a power level of 0.80 and an α level of 0.05.

H1: Business Process Models (BPM) represented by SSeBP and Enriched-Use Case combined with UML activity diagrams are informationally equivalent.

For *H1*, we empirically compared the mean of the business process coordination's questions of each treatment. Using a paired t-test. The data support *H1* with a p-value ≤ 0.001 and an observed power of 0.999.

H2: BPM developed using the SSeBP Artifact creates a higher level of security awareness than a Business process model developed using an Enriched Use Case and Activity Diagram.

For *H2*, we empirically compared the mean of the 15 security awareness questions for each treatment. Using a paired t-test, the data support *H2* with a p-value ≤ 0.001 and an observed power of 0.999.

H2a: BPM developed using the SSeBP Artifact creates a more accurate perception of security elements (i.e.: segregation of duties, non-repudiation, and authorization), in a business process than those using the Enriched Use Case and Activity Diagram.

For *H2a*, we empirically compared the mean of the 5 security perception questions for each treatment. Using a paired t-test, the data support *H2a* with a $p\text{-value} \leq 0.001$ and an observed power of 0.999.

H2b: BPM developed using the SSeBP Artifact creates a more accurate comprehension perception of security elements (i.e.: segregation of duties, non-repudiation, and authorization) in a business process than those using the Enriched Use Case and Activity Diagram.

For *H2b*, we empirically compared the mean of the 5 security comprehension questions for each treatment. Using a paired t-test, the data support *H2b* with a $p\text{-value} \leq 0.001$ and an observed power of 0.999.

H2c: BPM developed using the SSeBP Artifact creates a more accurate prediction of the future security state of the business process, than those using the Enriched Use Case and Activity Diagram.

For *H2c*, we empirically compared the mean of the 5 security prediction questions for each treatment. Using a paired t-test, the data support *H2c* with a $p\text{-value} \leq 0.001$ and an observed power of 0.999. Table 22 summarizes the hypotheses testing results.

<i>Hypothesis</i>	<i>p-value; Observed power</i>	<i>Supported//Not Supported</i>
<i>H1: Business Process Models (BPM) represented by SSeBP and Enriched-Use Case combined with UML activity diagrams are informationally equivalent</i>	p-value \leq 0.001; observed power =0.999	<i>Supported</i>
<i>H2: BPM developed using the SSeBP Artifact creates a higher level of security awareness than a Business process model developed using an Enriched Use Case and Activity Diagram</i>	p-value \leq 0.001; observed power=0.999	<i>Supported</i>
<i>H2a: BPM developed using the SSeBP Artifact creates a more accurate perception of security elements (i.e.: segregation of duties, non-repudiation, and authorization), in a business process than those using the Enriched Use Case and Activity Diagram.</i>	p-value \leq 0.001; observed value=0.999	<i>Supported</i>
<i>H2b: BPM developed using the SSeBP Artifact creates a more accurate comprehension perception of security elements (i.e.: segregation of duties, non-repudiation, and authorization) in a business process than those using the Enriched Use Case and Activity Diagram</i>	p-value \leq 0.001; observed power=0.999	<i>Supported</i>
<i>H2c: BPM developed using the SSeBP Artifact creates a more accurate prediction of the future security state of the business process, that those using the Enriched Use Case and Activity Diagram</i>	p-value \leq 0.001; observed power=0.999	<i>Supported</i>

Table 22. Test of hypotheses summary

4.3.3.6. Discussion of Findings

Business process modeling methods are intended to support the capture, representation, organization, and storage of knowledge on the state of an organization. The use of formal process modeling methods provides standardized semantics and representation and forms a bridge between process analysis and design and process implementation (Glassey, 2008). By showing that *SSeBP* design artifacts are informationally equivalent to Enriched-Use Case and UML-Activity Diagrams, we can affirm that not only business process represented using *SSeBP* design theory convey at least the same level of information than those business process represented using UML-models, but also that *SSeBP* design artifacts provide the semantics and grammar to analyze and represent the dynamics of business process.

In addition, the results from hypothesis H1 allows us to infer that *SSeBP* design artifacts accurately depict the coordination of activities and data flows needed to complete a specific business process. This demonstrates how *SSeBP* design artifacts fulfill the second *SSeBP* meta-requirement, which states that *SSeBP must support coordination of dependencies among business activities and information and knowledge resources involved in an eBusiness process*.

Hypotheses H2, H2a, H2b, and H2c all were supported by the data. In other words, business process models developed using *SSeBP* design theory generates a greater level of security awareness than those developed using Enriched-Use case and UML-Activity diagrams. A direct implication of this is that when security requirements are incorporated as functional requirements in the analysis of business processes, individuals

become more aware of security constraints and possible violations. This implies that business processes conceptualizations represented using *SSeBP* design artifacts generate greater awareness of security policies and constraints than those represented using Enriched-Use Case and UML Activity diagrams. Using the *SSeBP* design artifacts conceptualization of a business process, analysts would be able to better explain the current state of security of a business process. If any security violations occur, analysts would be able to explain the nature of them, in terms of segregation of duties, non-repudiation and authorization. In addition, analysts can use this understanding to predict the future security state of the business process in the event of a security threat.

In particular, the data supported hypothesis H2a. This demonstrates that *SSeBP* design artifacts assist subjects to identify security constraints in a business process. *SSeBP* design artifacts clearly represent who (agents/roles) has access to what (information resources) and under what conditions. In fact, when subjects used the *SSeBP* design artifacts treatment, they were able to correctly answer 82% of the security perception questions in comparison to only 32% when they used the Enriched-Use Case and UML-Activity diagram treatment. In other words, hypotheses H2a indicates that *SSeBP* design artifacts effectively represent access control policies that comply with inter and intra-organizational security requirements. This, in turn, shows that *SSeBP* design artifacts are more useful to subjects to decouple the association between agents and resources permissions and incorporates roles, permissions, access, and security of information and knowledge resources from the business process perspective. According to the situational awareness theory (Endsley, 1995), perception of relevant elements of

environment is needed to comprehend and project their status within the near future. It is worthwhile to point out that although this finding relates to the security perception aspect of the security awareness, it is significant because it forms the basis for the security comprehension and prediction.

Hypothesis H2b was also supported by the data. This indicates that *SSeBP* design artifacts can be used to provide a better understanding of the different security aspects of a business process. Interestingly, when subjects used the *SSeBP* design artifacts treatment they were able to correctly answer 73% of the security comprehension questions in comparison to only 22% when they use the Enriched-Use Case and UML-Activity diagram treatment. *SSeBP* design artifacts can be used to explain why certain activities have particular permissions over an information resource and can be only executed by specific roles fulfilled by specific agents. In addition, *SSeBP* design artifacts assist subjects in understanding which resources are need to complete a specific business activity.

Hypothesis H2c was supported by the data. This shows that *SSeBP* design artifacts allow subjects to make better inferences about future security states of a business process. Specifically, when subjects used the *SSeBP* design artifacts treatment they were able to accurately answer 51% of the security predictions questions in comparison to only 30% when they use the Enriched-Use Case and UML-Activity diagram treatment. Using *SSeBP* design artifacts, subjects were able to infer that when an activity did not have the right permission to read, write, or delete an information resource, the execution of the remaining activities may fail, as result the business process could not be completed. In

addition, the finding from H2c shows how *SSeBP* design artifact can be utilized to perform *what-if* type analyses of security violations. In summary, business process models developed using *SSeBP* design artifacts generate a greater level of security prediction than those models developed using Enriched-Use Case and UML-Diagram.

Finally, the findings from the subjects' perceptions about the utility of the two treatments indicate that *SSeBP* design artifacts are perceived to be superior to Enriched-Use Case and UML-Activity diagrams in representing security aspects of a business process. This is consistent with the findings of hypotheses H2a, H2b, and H2c. Here, subjects not only perceived *SSeBP* design artifacts to be superior, but also they performed better when they used *SSeBP* design artifacts to identify, comprehend, and predict security requirements and constraints of a business process.

SSeBP's experimental evaluation demonstrates that *SSeBP* design artifacts can be used to effectively represent both coordination and security aspects of a business process. *SSeBP* design theory represents a method to effectively incorporate security requirements in the conceptualization of business processes, which in turn leads to a better understanding and awareness of how to incorporate security as a functional requirement in the modeling, analysis, and design of information systems that enable secure business processes within and across organizations.

The utility and efficacy of an IS design theory are established by evaluating its outputs, design artifacts. By showing that the design artifact fulfills the requirements and constraints of the problem domain, the researcher demonstrates that the design theory is complete and effective (Walls et al., 1992; Simon 1969). We evaluate the efficacy and

utility of the *SSeBP* design theory using a rigorous multi-method approach. First, using a descriptive informed argument method, we illustrate *SSeBP* design artifact's utility and application. Specifically, we apply *SSeBP* design artifacts to enhance and map critical business processes from the prevalent industry-developed Collaborative Planning, Forecasting, and Replenishment (CPFR) approach. Second, the *SSeBP* design theory is evaluated using an observational method. We demonstrate how *SSeBP* design theory is used to represent and enhance real core business processes of a business organization. Finally, using situational awareness theory (Endsley, 1995), we empirically demonstrate how *SSeBP* design artifacts generate greater security awareness than Enriched-Use Case (Siponen et al., 2006) and standard UML activity diagram. Table 23 summarizes the results of the *SSeBP* design theory evaluation.

Evaluation Method	Results
<p>Descriptive Evaluation demonstrates <i>SSeBP</i> design theory applicability to represent and enhance core business process from an industry standard</p>	<p><i>SSeBP</i> meta-requirements, meta-design, and design method, including modeling concepts and grammar, can be used to model business processes that require a high degree of collaboration and secure environment</p> <p><i>SSeBP</i> design theory can be used to enhance CPFR business process by incorporating security access control requirements and standard knowledge representation</p> <p>Using the atomic concepts of <i>SSeBP</i> design theory, DL formalisms were generated and validated for knowledge representation for CPFR business process, which forms the basis for the development of machine interpretable knowledge representation in the OWL-DL format</p>
<p>Observational Evaluation demonstrates the utility and efficacy of <i>SSeBP</i> design theory in modeling and enhancing security aspects of core business processes of a large organization</p>	<p><i>SSeBP</i> design theory can be used to represent and enhance core business processes from a large apparel organization. Organization A's Management and demand and planning analysts perceived the following as benefits of <i>SSeBP</i> design artifact:</p> <ul style="list-style-type: none"> • <i>SSeBP</i> approach provides the foundations to integrate heterogeneous IT systems (Organization A's CIO) • The <i>SSeBP</i> design artifacts allows us to have the big picture about the different actors and resources involved in the execution of the business processes (Organization A's Director of Planning) • This approach facilitates the modeling and analysis of organizational functions and responsibilities involved in a eBusiness Process (Organization A Demand Analyst) • These diagrams help us understand the delicate balance between accessibility, transparency and security (Organization A's CIO)

Evaluation Method	Results
<p><i>Experimental Evaluation</i> empirically demonstrates the security awareness generated by <i>SSeBP</i> design artifact against the best known existing approach</p>	<p>We empirically demonstrate that business process models developed using <i>SSeBP</i> design theory are superior in representing business process's dynamics to those model developed Enriched-Use Case and UML-Activity Diagram</p> <p>We empirically validate that business process models developed using <i>SSeBP</i> design artifacts generate a greater level of security awareness than those models developed using Enriched-Use Case and UML-Activity Diagram</p> <p><i>SSeBP</i> design artifacts generate greater level of security perception, comprehension and prediction than Enriched-Use Case and UML-Activity Diagram</p>

Table 23. *SSeBP* Design Theory Evaluation Results

CHAPTER V

CONCLUSION

This chapter summarizes the main aspects of the *SSeBP* design theory and presents the theoretical and practical implications, limitations of the study, and potential future research.

This research is motivated by the need of a theoretically grounded design method that guides the analysis and design of secure and coordinated e-Business processes. Following a design science approach, we attempt to answer the research question: *How can we formulate a design theory to guide the analysis and design of Secure Semantic eBusiness processes?* We answer that question by developing and evaluating a Secure Semantic eBusiness Processes (SSeBP) design theory that provides design principles, including modeling concepts and grammar, for the design and development of secure eBusiness processes.

Based on the perspectives of Walls et al. (1992), Hevner et al. (2004), March and Smith (1995) and Vaishnavi et al. (2006), the theoretical foundations for the development of *SSeBP* design theory are established. Specifically, after a thorough review of the extant literature, kernel theories from the application domain and from the IS knowledge domain are analyzed and applied to formulate the *SSeBP* design theory.

In developing the theoretical foundations for our research, we bring together multiple theoretical foundations in a design artifact that integrates *component knowledge of resources* (Tallman et al, 2004) involved in a process, *process knowledge* (van der Aalst and Kumar, 2003) including process models, and *security knowledge* (Sandhu, 1996) including access control. *SSeBP* design theory's kernel theories are listed in Figure 15.

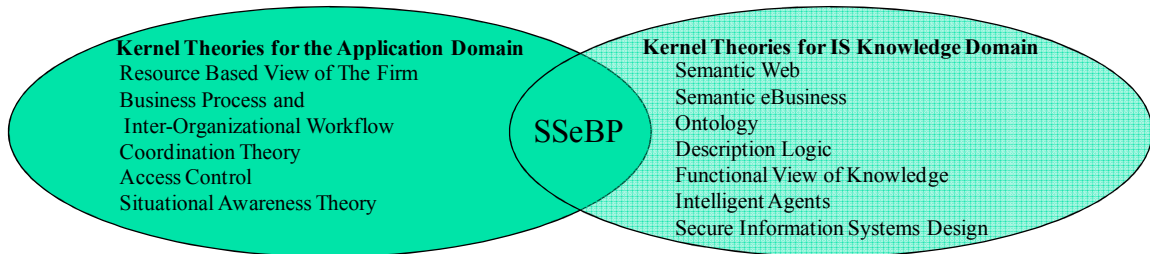


Figure 15. SSeBP Design Theory Kernel Theories

These kernel theories and the characteristics of the problem domain are used to define the *SSeBP* design theory's meta-requirements.

- i. The *SSeBP* design theory should allow multiple agents to cooperate in a coordinated manner to accomplish goals of an eBusiness process
- ii. The *SSeBP* design theory must support coordination of dependencies among business activities and resources

- iii. The *SSeBP* design theory should represent access control policies and security requirements for an eBusiness process
- iv. The *SSeBP* design theory should decouple and simplify association between agents and permissions to resources
- v. The *SSeBP* design theory must describe eBusiness processes in unambiguous, computer-interpretable knowledge representation
- vi. The *SSeBP* design theory should provide an integrative semantic foundation that facilitates agents reasoning with process and component knowledge in the context of an eBusiness process

We develop a meta-design, which includes the constructs and relationships derived from the analysis of the kernel theories and posited to meet the meta-requirements. *SSeBP* design theory meta-design's atomic-concepts consist of *business enterprise*, *agent*, *role*, *activity*, and *resource*. Specifically, *SSeBP* meta-design is conceptualized as: in an eBusiness process, a Business Enterprise authorizes representation to an actor or Agent to fulfill a Role, which performs Activities that have access permissions to resources. Resources permit activities performed by Roles fulfilled by Agents that represent Business Enterprises, engaged in an eBusiness Process.

Description Logics (DL) provide formalism for theoretical soundness and it forms the basis for the development of machine interpretable knowledge representation. We develop and validate DL representation for the *SSeBP* atomic-concepts and their relationships.

A design theory requires a design artifact and a design process. *SSeBP* design theory's design process provides the guiding principles and procedures (steps) that must be followed in order to develop *SSeBP* design artifacts that satisfy the *SSeBP* design theory's meta-requirements.

The utility and efficacy of an IS design theory are established by evaluating its design artifacts. A design artifact must be evaluated to demonstrate its utility, quality, and efficacy. We assess the efficacy and utility of *SSeBP* design theory using a rigorous multi-method approach which includes descriptive, observational, and experimental evaluations. The descriptive evaluation results show that *SSeBP* design theory can be used to represent and enhance core e-business processes of an industry standard. *SSeBP* allows for incorporating security policies and constraints in the analysis and design of e-business processes. The observational evaluation demonstrates that *SSeBP* design theory can be applied to represent and enhance real core business processes. The experimental evaluation shows that *SSeBP* design artifacts do not incur in any loss of information. The findings from the *SSeBP* design theory's empirical evaluation clearly demonstrate that business models developed using *SSeBP* design artifacts generate greater security awareness than those models developed using Enriched-Use Case and UML-diagrams.

We follow Hevner et al. guidelines (2004) to summarize the main aspects of the *SSeBP* design theory in Table 24.

Guideline	SSeBP Description
Design as an Artifact	<p>We developed the constructs, the models, methods and instantiation for the <i>SSeBP</i> design theory. The <i>SSeBP</i> design theory defines the atomic concepts (i.e.: business enterprise, agent, role, activity, resource) and the relationship that exists among them.</p>
Problem Relevance	<p>This research attempts to answer the research question:</p> <p><i>How can we formulate a design theory to guide the analysis and design of Secure Semantic eBusiness processes?</i></p> <p>This is a relevant research question due to the following facts:</p> <ul style="list-style-type: none"> i. Collaborating organizations must exchange information and knowledge resources in a coordinated and secure manner to efficiently conduct inter-organizational eBusiness processes. ii. Seamless knowledge exchange within and across organizations involved in secure business processes is critically needed. iii. Organizations engaged in collaborative inter-organizational processes continue to be plagued with semantic conflict issues and a lack of integration in heterogeneous systems. iv. The lack of process visibility across organizations mitigates the development of trust between the partner organizations. This is confounded by the lack of security knowledge regarding authorized access to resources. v. Extant literature does not <i>explicitly</i> consider or systematically represent <i>component knowledge</i> of resources such as description of skills and product knowledge; <i>process knowledge</i> including process workflow models; and <i>security knowledge</i> of authorized access for activities to resources within and across organizations. vi. Information systems methodology that includes security aspects in all stages is still needed (Baskerville, 1988). Siponen et al. (2006) argued that that existing SIS design methods fail to satisfy secure systems design requirements.

Guideline	SSeBP Description
Design Evaluation	<p>The utility and application of <i>SSeBP</i> was demonstrated using multiple evaluation methods from the IS knowledge base.</p> <ul style="list-style-type: none"> i. It was demonstrated how the Collaborative Planning, Forecasting, and Replenishment (CPFR) approach can be mapped and enhanced by applying <i>SSeBP</i> design theory. ii. <i>SSeBP</i> design theory was validated by mapping real core business processes of a large apparel organization. By using real core business processes, we capture both the information and knowledge, including component, process, and security knowledge related to the business processes and the richness of the organizational environment. iii. <i>SSeBP</i> design theory was empirically validated using situational awareness theory (Endsley, 1995). <i>SSeBP</i> design artifacts were empirically evaluated against the Enriched-Use Case (Siponen et al., 2006) and UML- activity diagram.

Guideline	SSeBP Description
Research Contribution	<ul style="list-style-type: none"> i. <i>SSeBP</i> design theory provides practitioners with the meta-design and the design process, including the system features and systems principles, to guide the crafting of secure eBusiness processes that are semantically rich, highly coordinated and seamlessly integrated. ii. <i>SSeBP</i> design theory presents a novel and holistic approach that contributes to the IS knowledge base by filling an existing research gap in the area of design of information systems to support secure and coordinated eBusiness processes. iii. <i>SSeBP</i> is an IS design and action theory (Gregor, 2006) that allows IS researchers to understand the design principles needed to model secure semantic eBusiness process. iv. <i>SSeBP</i> provides design process and modeling concepts and grammar to guide the analysis and design of secure and semantically rich business processes. v. <i>SSeBP</i> offers eBusiness process conceptualizations that allow analysts to better explain the current and future security state of an eBusiness process. vi. <i>SSeBP</i> allows management to analyze and define the relationships between organizational roles and the activities that they perform. This leads to assurance of segregation of duty in the context of eBusiness processes. vii. <i>SSeBP</i> enables information and knowledge resources to be represented in a standard and unambiguous machine readable format. Common ontologies provide the foundation for semantic conflict resolution and seamless flow of information and knowledge among heterogeneous systems involved in an eBusiness process.

Table 24. A Design Science approach for SSeBP

5.1.Implications

Information Systems design science research must contribute to the IS knowledge base and provide an effective solution for relevant business problems.

5.1.1. Theoretical Implications

Theoretical implications of this research include the development and validation of a design theory (*SSeBP*). Current academic and practitioner literature in business process modeling does not address security requirements in the early stages. In addition, secure information systems design methods and business process modeling techniques are theoretically underdeveloped (Siponen et al. 2006; Soffer and Wand, 2007). There is still a need for information systems methodologies that include security requirements in all stages of development (Baskerville 1988, Apvrille and Pourzandi, 2005, Siponen et al. 2006). *SSeBP* design theory presents a theoretical grounded and novel approach that contributes to the IS knowledge base by filling an existing research gap in the area of design of information systems that support secure and coordinated business processes. *SSeBP* design theory provides a security information systems methodology that incorporates security requirements and constraints into the analysis and design phases and considers security aspects as functional requirements.

SSeBP design theory provides a sound framework that allows IS researchers to decompose the complexity of business processes into atomic-concepts and their relationships. *SSeBP* design theory provides an explicit and systematic way to represent

component knowledge of resources such as description of skills and product knowledge; *process knowledge* including process workflow models; and *security knowledge* of authorized access for activities to resources within and across organizations.

We demonstrate, using a rigorous multi-evaluation approach, how *SSeBP* utilizes emerging technologies to solve semantic conflict issues, to prevent unauthorized access to resources, to foster knowledge exchange, and to integrate heterogeneous systems. This evaluation provides researchers with rich information and important guidelines that can be used to evaluate resulting IT artifacts.

Theory for design and action prescribes “*how to do something*”. This type of theory provides a description of the method or structure or both for the construction of an artifact (Gregor, 2006). *SSeBP* design theory is an IS design and action theory (Gregor, 2006) that allows IS researchers to understand the design principles needed to model secure semantic eBusiness processes. Specifically, *SSeBP* design theory prescribes the atomic concepts and the design-method needed to analyze and design secure semantic e-Business processes. As Simon (1996, p.132) states, “solving a problem simply means representing it so as to make the solution transparent”.

5.1.2. Practical Implications

SSeBP design theory integrates streams of research in design science paradigm, eBusiness Process, authorization and Role-Based Access Control, ontology, coordination theory, and Description Logics (DL) and Semantic Web technologies. A business process

provides the context and global perspective to information and knowledge sharing within and across organizational boundaries. *SSeBP* design theory can be used to describe the roles, permissions, resources and security requirements by creating a standardized vocabulary that describes access control and security for distributed information and knowledge sharing. It provides practitioners with the meta-design and relevant examples that can be used to develop semantically rich models of business processes. These models can be verified through DL formalisms and can be converted to standardized machine-interpretable knowledge representation. *SSeBP* provides an integrative mechanism for detailed analysis of business processes including the business enterprises and their agents involved, the roles they fulfill, the activities they perform and coordination mechanism and access control policies with respect to access and sharing of knowledge resources of organizations in a value chain.

Organizations and practitioners would benefit from *SSeBP* in several ways. *SSeBP* design theory can help practitioners to analyze and enhance collaborative industry standards. We showed how the security of CPFR business processes can be enhanced by incorporating roles and permissions over resources and activities. *SSeBP* design artifact uses RBAC that allows for non-repudiation, auditing, and separation of duties mechanism much needed in collaborative business processes. Furthermore, *SSeBP* design theory provides the foundations for integrating heterogeneous data sources. *SSeBP* design artifacts can be used to develop semantic wrappers to dynamically feed CPFR data and information to ERP systems. Finally, a key success factor for CPFR is to integrate CPFR processes into existing business processes. In this context, *SSeBP* design theory provides

the atomic concepts, their relationships, and coordination mechanisms that can be used to analyze, map, and integrate existing business processes with CPFR's processes. We strongly believe that the proposed IT artifact has the potential to benefit not only organizations that are planning to adopt CPFR, but also organizations that have adopted it.

SSeBP design theory provides organizations with a design process, which establishes a set of principles and procedures to analyze and design secure eBusiness process. This facilitates the management of analysis and development activities and will result in more secure eBusiness processes. Moreover, management and analysts can utilize *SSeBP* design artifacts to have the whole picture about the different actors and resources involved in the execution of a specific business processes. In *SSeBP* design theory, roles specify organizational functions responsible for particular activities, which allow management to analyze and define the relationships between organizational roles and the activities that they perform. This leads to assurance of segregation of duty in the context of eBusiness processes. This, in turn, helps management with the modeling and analysis of organizational functions and responsibilities involved in an eBusiness Process. This allows for the inclusion of non-repudiation mechanisms into the analysis and design of eBusiness processes. Non-repudiation mechanisms lay the foundations for auditing, which is needed for compliance with regulations such as Sarbanes-Oxley (SOX) and Health Insurance Portability and Accountability Act (HIPAA).

SSeBP design artifacts allow analysts to identify and understand security requirements and constraints involved in a business process. *SSeBP* design theory enables the inclusion of security specifications as functional requirements early in the modeling and analysis of business processes; as a result analysts become more aware of security constraints and possible violations resulting in more secure eBusiness processes. This is very important in the design of inter-organizational business processes, where the lack of security knowledge regarding authorized access to resources hinders the development of trust between the partner organizations.

SSeBP design theory can assist security analysts in developing technical and formal security controls needed for a secure eBusiness Process. Specifically, *SSeBP* design artifacts provide audit trail and segregation of duty mechanisms that can be used to develop technical and formal controls to ensure non-repudiation and authorized access to resources. In addition, *SSeBP* design artifacts enable information systems stakeholders to have a common understating of the security requirements and constraints involved in a specific eBusiness process. *SSeBP* design artifacts can be used to document existing and future eBusiness process. A common representation that is expressive and easy to understand by the stakeholders of the business process is a key factor for good requirements communication. Finally, *SSeBP* design artifacts can be used as a means of planning for eBusiness process security. Here, the security prediction generated by *SSeBP* design artifacts can be utilized by security analysts to predict the future security state of the business process in the event of a security threat. *SSeBP* design theory can be

proactively used to develop security mechanisms that would prevent security threats from happening or escalate.

The *SSeBP* design theory enables information and knowledge resources to be represented in a standard and unambiguous machine readable format. Common ontologies provide the foundation for semantic conflict resolution and seamless flow of information and knowledge among heterogeneous systems involved in an eBusiness process. A desirable outcome of enforcing the relationships between agents, business activities and resources is accountability of resource utilization and non-repudiation of business activities. When agents are allowed to fulfill organizational roles by performing business activities, their function is monitored for exceptions and logged for validation of authorization requirements. Roles specify organizational functions responsible for specific activities and provide mechanisms for non-repudiation and auditing.

5.2.Limitations

Although we diligently followed the design science guidelines proposed by Hevner et al. (2004), March and Smith (1995), Walls et al. (1992) and Vaishnavi et al. (2006) in this study, our research has some limitations.

We base our observational and descriptive evaluations on the CPFR industry standard and apply the design artifact to a relevant case of a complex business problem of a large organization. While CPFR models are used by numerous organizations, one must be careful in drawing generalizations to other industry standards. Single cases and

analysis of industry standards have been used in research similar to ours. For example, Sikora and Shaw (1998) show the application of a multi-agent framework for coordination using a single case that illustrates a manufacturing problem in a printed circuit-boards facility. Walls et al. (1995) provide a single example to explain the information system design theory for Vigilant Executive Information Systems (VIS). Nissen and Sengupta (2006) evaluate the application of agent technology to an e-Procurement task. Soffer and Wand (2007) present a generic process model and demonstrate its utility by application to the Supply Chain Operations Reference-model (SCOR).

The CPFR model and the case study used in this research show a dyadic supply chain. Therefore, to increase the validity of *SSeBP* design artifacts, more complex relationships need to be analyzed. It is important to mention that this practice is a common one, given the difficulties that represent to model multi-echelon supply chains. For instance, Nissen and Sengupta (2006) show how intelligent agents can enhance supply chain performance. They conduct experiments to demonstrate that agents are capable of interacting in a marketplace with one buyer and one supplier. We evaluated our artifact using a multi-method approach, which includes observational, descriptive, and experimental. However, in order to increase the generalizability of the *SSeBP* design theory, we recommend further evaluations through simulations.

Limitations of the experimental evaluation are related to the selected subjects and selected scenario. First, since subjects were information systems students, we must be careful in drawing generalizations from the findings to information systems professionals

in general. However, extant literature recognizes that IS students resemble the characteristics of information systems and business analysts' population (Bolloju and Leung, 2006; Porter et al., 1994; Jeyaraj and Sauter, 2007; Danesh and Kock, 2005; Agarwal and Sinha, 2003). Second, we used a simplified version of a "create order forecast" business process as the stimulus for the experimental evaluation. Even though this business process exhibits the characteristics of our problem domain, it represents a dyadic relationship between buyer and seller organizations. We recognize that real core business processes are usually more complex and larger in size. A danger of designing tasks for experiments is to select tasks that are either too complex or too easy for the subjects (Jarvenpaa et al., 1985). We carefully selected and validated the scenario for the experiment and considered that given the amount of time needed to complete the experiment and expertise of the subjects, the selected scenario was appropriate.

We developed and validated DLs for the atomic concepts represented in the secure activity-resource coordination diagrams. The DL formalisms serve as examples to illustrate the development of the formalisms for concepts and relationships needed to represent component, process, and security knowledge. While this serves the central theme of this research, the DL formalisms presented are not exhaustive. Future research would benefit the practitioner and researcher community by developing complete system knowledge representation DL formalisms that can form the basis for cross domain industry ontologies. Organizations and research groups, such as DERI (www.deri.org), are involved in such efforts. However, these efforts focus on EDI-type component descriptions and do not incorporate process and security knowledge to provide a

complete view of transparent information flows in secure and coordinated business processes.

Despite these limitations, the approach presented in this dissertation is well grounded in kernel theories and it has been evaluated using a rigorous multi-methods approach.

5.3.Future Research

Quality research must also generate a new set of inquiries. Here, *SSeBP* design theory provides three lines of inquiries for IS research. First, the atomic concepts of *SSeBP* design theory include business enterprise, agents, roles, business activities, and resources. Research aimed at extending these atomic concepts to analyze and design information systems in general is needed. For instance, are those atomic concepts universal? Can accounting information systems be analyzed and designed using those atomic concepts? Are there any alternative sets of atomic concepts? Second, *SSeBP* design theory identifies a set of meta-requirements for designing secure and coordinated business processes. Here, new research aimed at establishing the completeness of those requirements is needed. Are those *SSeBP* meta-requirements a complete set? Are there any alternative sets of meta-requirements? Third, *SSeBP* design theory's evaluation demonstrates that *SSeBP* design artifacts can be used to analyze and represent business processes in the context of apparel and retailing organizations; however, future research in different contexts is needed. Are *SSeBP* design artifacts effective in other business

context? For instance, the proposed design theory might be applied to enhance the security and interoperability of business processes in the areas of e-supply chain, e-healthcare, and e-government.

Another future research area includes qualitative studies aimed at factors that might affect the adoption of the type of IT artifact developed by applying *SSeBP* design theory. Here, research that answers the following questions is needed: What kind of enabler and inhibitor factors may affect the adoption of *SSeBP* design artifacts? What kind of organizations will benefit the most from the adoption of *SSeBP* design artifacts? Moreover, since the *SSeBP* design method natural path is to evolve into an IS methodology, an important area of research is about incorporating *SSeBP* design method into the IS curriculum. Is the *SSeBP* design method effective and easy to use? Can *SSeBP* design process be integrated into existing security information systems design methods?

Experimental designs that include multiple tasks, different business processes, with different levels of complexity can be used to evaluate *SSeBP* design theory further. Here, the effect of tasks characteristics in the security awareness generated using the *SSeBP design* artifacts can be assessed. Does the complexity of the task play a role on the efficacy of the *SSeBP* artifact in creating security awareness? This type of experimental design increases the external validity of the experimental evaluation and helps to overcome the negative effects of learning effect.

Cognitive fit theory (Vessey, 1991) states that problem solving is the outcome of the relationship between the external problem representation and the problem solving task. Agarwal et al. (1999) suggest that problem representation is a determinant of

performance, from the perspective of problem solving as well as comprehension. In the context of *SSeBP* design theory, cognitive fit theory can be used to design an experiment that compares the performance obtained by subjects using *SSeBP* design artifacts against the performance obtained by subjects using existing security information systems methods in identifying business process security requirements and constraints.

REFERENCES

- Agarwal, R., De, P., and Sinha, A. (July/August 1999) "Comprehending Object and Process Models: An Empirical Study," *IEEE Transactions on Software Engineering*, (25:4), pp. 541-556.
- Alter, S. (2006) "Work Systems and IT Artifacts – Does the Definition Matter?," *Communications of the Association for Information Systems* (17), pp. 299-313.
- Anand, K.S. and H. Mendelson (1997) "Information and Organization for Horizontal Multi-market Coordination," *Management Science*, 43(12), pp. 1609-1627.
- Apvrille, A., and M. Pourzandi (2005) "Secure Software Development by Example," *IEEE Security and Privacy*, pp. 10-17.
- Aron, A. and E. Aron, *Statistics for Psychology*. First ed., Prentice Hall, 1994.
- Ashenhurst, R. L. (1996) "Ontological Aspects of Information Modelling," *Minds and Machines*, (6), pp. 287-394.
- Atallah, M., Blanton, M., Deshpande, V., Frikken, K., Li, J., and Schwarz, L. (2006) "Secure Collaborative Planning, Forecasting, and Replenishment (SCPFR)," In *Proceedings of Multi-Echelon Inventory Conference*.
- Baader, F., Calvanese, D., McGuinness, D., Nardi, D., and Patel-Schneider, P.F., eds. *The Description Logic Handbook: Theory, Implementation and Applications*. Cambridge: Cambridge University Press, 2003.
- Badaracco, J. L. (1991) *The Knowledge Link*, Boston, MA; Harvard Business School Press.
- Barley, M., Clark, P., Williamson, K., and Woods, S. (1997) "The Neutral Representation Project," In *Proceedings of AAAI Spring Symposium on Ontological Engineering*. Stanford University, CA, AAAI Press: pp.1-8.

- Barney, J. (1991) "Firm Resources and Sustained Competitive Advantage," *Journal of Management*, 17(1), pp. 99-120.
- Basili, V., Shull, F., Lanubile, F. (1998) "Using Experiments to build body of Knowledge," Technical Report, University of Maryland, CS-TR-3983.
- Baskerville, R. *Designing Information Systems Security*, John Wiley & Sons, New York, 1988.
- Baskerville, R., Pries-Heje, J., and Venable, J. (2007) "Soft Design Research: Extending the Boundaries of Evaluation in Design Research," *In Proceedings of the 2nd DESRIST Conference, May 13-15 2007, Pasadena, CA, pp. 19-38.*
- Basu, A., and A., Kumar (2002) "Research Commentary: Workflow and Management Issues in e-Business," *Information Systems Research*, 13(1), pp. 1-14.
- Bateman, J. A. (1995)"On the Relationship Between Ontology Construction and Natural Language: A Socio-Semiotic View," *International Journal of Human-Computer Studies*, (43), pp. 929-944.
- Benbasat, I. A.Dexter (1986) "An Investigation of the Effectiveness of Color and Graphical Information Presentation under Varying Time Constraints ," *MIS Quarterly*, (10:1), pp. 59-83.
- Benbasat, I. and Zmud, R. (2003), "The Identity Crisis within the IS Discipline: Defining and
- Benjamin, R., I., De Long, D. W., and Scott Morton, M.C. (1990) "Electronic Data Interchange: How Much Competitive Advantage?," *Long Range Planning (UK)*, 23(1), pp 28-40.
- Benjamins, V. R. and Fensel, D.. The Ontological Engineering Initiative (KA) 2. In N. Guarino (ed.) *Formal Ontology in Information Systems*. IOS Press. 1998.
- Bergamaschi, S., Castano, S., De Capitani di Vimercati, S., Montanari, S., and Vincini, M.. An Intelligent Approach to Information Integration. In N. Guarino (ed.) *Formal Ontology in Information Systems*. IOS Press. 1998.
- Berners-Lee, T., Hendler, J. and Lassila, O. (May 2001) "The Semantic Web," *Scientific American*, pp.34-43.

- Bhatti, R. et al. (2004) "XML-Based Specification for Web Services Document Security," *IEEE Computer Society*, pp.41-49.
- Boley, H. and Guarino, N. (1996) Proceedings of the Workshop on Product Knowledge Sharing for Integrated Enterprises. In M. Wolf and U. Reimer (eds.), Proceedings of the First International Conference on Practical Aspects of Knowledge Management. Schweizer Informatiker Gesellschaft, Basel, Switzerland.
- Bolloju, N. and S.K. Leung (2006) "Assisting Novice Analysts in Developing Quality Conceptual Models with UML," *Communications of the ACM* (49:7), pp. 108-112.
- Boneau, C.A. (1962) "A Comparison of the Power of the U and t Test," *Psychological Review*, (69), pp. 246-256.
- Borgo, S., Guarino, N., and Masolo, C. (1997) "An Ontological Theory of Physical Objects," In Proceedings of Qualitative Reasoning 11th International Workshop. Cortona, Italy, IAN-CNR, Pavia. pp. 223-231.
- Brooks, R. "Studying Programmer Behavior Experimentally: The Problems of Proper Methodology", *Communication of ACM*, (23: 4), pp. 207-213, Apr. 1980.
- Burg, J. F. M. Linguistic Instruments in Requirements Engineering. IOS Press. 1997.
- Caridi, M., Cigolini, R., De Marco, D. (2005) "Improving Supply-Chain Collaboration by Linking Intelligent Agents to CPFR," *International Journal of Production Research*, 43(20), pp. 4191-4218.
- Carpenter, B., and P. Janson. (2004) "Abstract Interdomain Security Assertions: A Basis for Extra-Grid Virtual Organizations," *IBM Systems Journal*, 43(4), pp. 689-701.
- Casati, R. and A., Varzi. Spatial Entities. In O. Stock (ed.) Spatial and Temporal Reasoning. Kluwer, Dordrecht. 1997.
- Casati, R., Smith, B., and Varzi, A.. Ontological Tools for Geographic Representation. In N. Guarino (ed.) *Formal Ontology in Information Systems*. IOS Press. 1998.
- Choobinedh, J., Dhillon, G., Grimalia, M., and Rees, J. (2008) "Management Information Security: Challenges and Research Direction," *Communication of the Association for Information Systems*, 20, pp. 958-971.

Chung, L., and B., Nixon (1995) "Dealing with Non-Functional Requirements: Three Experimental Studies of a Process-Oriented Approach," *in the Proceedings of the 17th International Conference on Software Engineering*, Seattle- USA.

Cohen, J. *Statistical Power Analysis for the Behavioral Sciences*, second ed. Lawrence Erlbaum Associate Publishers, 1988.

Cohen, J. *Statistical Power Analysis for the Behavioral Sciences*. New York: Academic Press, 1969.

Communicating the discipline's Core Properties", *MIS Quarterly*, (27:2), pp.183-194

Crowston, K. and Osborn, C. (2003) "The Interdisciplinary Study of Coordination," in Malone, T. W., Crowston, K., and Herman, G. A., editors, *Organizing business knowledge: the MIT process handbook*, MIT Press, Cambridge, Massachusetts.

Daft, R. *Organization Theory and Design*. New York: West. 1983.

Davenport, T. "Process Innovation: Reengineering Work through Information Technology", Harvard Business School Press, 1993.

Davenport, T.H., Short, E.J. (1990), "The new industrial engineering: information technology and business process redesign", *Sloan Management Review*, pp.11-27.

Dhillon, G. and J., Backhouse (2001) "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal*, (11), pp. 127-153.

Dyer, J., (2000) *Collaborative advantage: winning through extended enterprise supplier networks* Oxford University Press, New York.

Endsley, M.R. (1995) "Toward a theory of Situational Awareness in dynamic systems," *Human Factors* (37:1), pp 32-64

Fisher, R (1948) "Combining Independent Tests of Significance," *The American Statistician*, 2(5).

Gaines, B. (1997) "Editorial: Using Explicit Ontologies in Knowledge-based System Development," *International Journal of Human-Computer Systems*, (46) pp. 181.

- Glassey, O. "A Case Study on Process Modeling - Three questions and Three Techniques," *Decision Support Systems*, (44:4), pp. 842-853.
- Gomez-Perez, A., Fernandez-Lopez, M., and Corcho, O. (2004) *Ontological Engineering*. Springer, London.
- Gordon, L., Loeb, M., Lucyshyn, W., and Richardson, R. (2006) Eleventh Annual CSI/FBI Computer Crime and Security Survey, Computer Security Institute.
- Gotts, N. M., Gooday, J. M., and Cohn, A. G. (1996) "A Connection Based Approach to Commonsense Topological Description and Reasoning," *The Monist: An International Journal of General Philosophical Inquiry*, (79:1).
- Grant, R. (1996), "Toward a Knowledge-base Theory of the Firm," *Strategic Management Journal*, 17, pp. 109-122.
- Greenwald, A. "Within-Subjects Designs: To Use or Not to Use?" *Psychological Bull.*, (83:2), Sept. 1976.
- Gregor, S. (2006) "The Nature of Theory in Information Systems," *MIS Quarterly*, 30(3), pp. 611-642.
- Grizzle, J. "The Two-Period Chance-Over Design and Its Use in Clinical Trials," *Biometrics*, (1:21) , pp. 314-320, 1965.
- Gruber, T. R. (1993) "A translation approach to portable ontology specifications," *Knowledge Acquisition*, (5), pp. 199-220.
- Gruninger, M. and Fox, M. S.. *The Logic of Enterprise Modelling*. In J. Brown and D. O' Sullivan (eds.), *Reengineering the Enterprise*. Chapman and Hall. 1995.
- Guarino, N. (1995) "Formal Ontology, Conceptual Analysis and Knowledge Representation," *International Journal of Human and Computer Studies*, 43(5/6), pp. 625-640.
- Guarino, N. (1998) "Some Ontological Principles for Designing Upper Level Lexical Resources," In A. Rubio, N. Gallardo, R. Castro, A. Tejada (eds.), *Proceedings of First International Conference on Language Resources and Evaluation. ELRA - European Language Resources Association*, Granada, Spain, pp. 527-534.

- Guarino, N., Borgo, S., and Masolo, C. (1997) "Logical Modelling of Product Knowledge: Towards a Logical Semantics for STEP," In Proceedings of European Conference on Product Data Technology (PDT Days 97). Sophia Antipolis, France, QMS, Berkshire, UK, pp. 183-190.
- Guarino, N..(1997) Semantic Matching: Formal Ontological Distinctions for Information Organization, Extraction, and Integration. In M. T. Pazienza (ed.) *Information Extraction: A Multidisciplinary Approach to an Emerging Information Technology*. Springer Verlag: 139-170.
- Hadar, I. and P., Soffer (August 2006) "Variations in Conceptual Modeling: Classification and Ontological Analysis," *Journal of the Association for Information Systems*, (7:8), , pp. 568-592.
- Hamel, G. (1991) "Competition for Competence and Inter-Partner Learning with International Strategic Alliances," *Strategic Management Journal*, 12, pp. 83-103.
- Hammer, M. & Champy, J.M. *Reengineering the Corporation: A Manifesto for Business Revolution*, Nicholas Brealey Publishing, Allen and Urwin, London, 1993.
- Hevner, A., March, S.T., Park, J., and Ram, S. (March 2004) "Design Science Research in Information Systems," *MIS Quarterly*, 28(1), pp. 75-105.
- Hirschheim, R. and Klein, H .(1992) "A Research Agenda for Future Information Systems Development Methodologies," In W.W. Cotterman and J.A. Senn (eds): *Challenges and Strategies for Research in Systems Development*, pp. 113-129.
- Holsapple, C., and Singh, M. (Jul/Sep 2000) "Toward a Unified View of Electronic Commerce, Electronic Business, and Collaborative Commerce: A Knowledge Management Approach," *Knowledge and Process Management*, 7(3), pg. 159.
- Hult, G., Ketchen, D., and Slater, S. (2004) "Information Processing, Knowledge Development, and Strategic Supply Chain Performance," *Academy of Management Journal*, 47(2), pp. 241-253.
- Jarvenpaa, S., Dickson, G., and DeSanctis, G. (1985) "Methodological Issues in Experimental IS Research: Experiences and Recommendations," *MIS Quarterly*, 9 (2), pp. 141-156.

- Jasper, R. and M.,Uschold (1999) "A Framework for Understanding and Classifying Ontology Applications," *Proceedings of the IJCAI-99 Workshop on Ontologies and Problem-Solving Mehtods*, Stockholm, Sweden.
- Jennings, N.R. and M. Wooldridge *Agent Technology: Foundations, Applications, and Markets*, Springer, London. 1998.
- Jensen M. C., and W., Meckling (1976) "Theory of the Firm: Managerial Behaviour, Agency Costs and Capital Structure," *Journal of Financial Economics*, 3, pp.305-360.
- Jeyaraj, A. and V. L., Sauter (2007) "An Empirical Investigation of the Effectiveness of Systems Modeling and Verification Tools," *Communications of ACM* (50:6), pp. 62-67.
- Joshi, et al. (2001) "Security model for Web-based Applications," *Communication of the ACM* 44(2), pp. 38-44
- Jürjens, J. (2001) "Towards Development of Secure Systems Using UMLsec," in *H. Hussmann, editor, Fundamental Approaches to Software Engineering, 4th International Conference, Proceedings,LNCS*, , pp. 187-200, Springer.
- Keren, G. *A Handbook for Data Analysis in the Behavioural Sciences -Methodological Issues*, chapter 19: Between- or Within- Subjects Design: A Methodological Dilemma. Lawrence Erlbaum, Associates, 1993.
- Khatri, V., Vessey, I., Ramesh, V., Clay, P., and Park, S. (2006) "Understanding Conceptual Schemas: Exploring the Role of Application and IS Domain Knowledge," *Information Systems Research*, 17(1), pp.81-99.
- Kishore, R., Zhang, H., and Ramesh, R. (2006) "Enterprise integration using the agent paradigm: foundations of multi-agent-based integrative business information systems", *Decision Support Systems*, 42(1), pp. 48-78.
- Klein, M., Fensel, D., van Harmelen, F., and Horrocks, I. (2001) "The Relation Between Ontologies and XML Schemas," *Electronic Transactions on Artificial Intelligence (ETAI), Linköping Electronic Articles in Computer and Information Science*, 6(4).
- Kuehl, R. *Design of Experiments: Statistical Principles of Research and Design and Analysis*, second ed., Pacific Grove: Duxbury Press, 2000.

- Laitenberger, O, Atkinson, C., Schlich, and El Emam, K. (2000) "An Experimental Comparison of Reading Techniques for Defect Detection in UML Design Documents," *The Journal of Systems and Software*, (53), pp. 183-204
- Laitenberger, O., El Emam, K., and Harbich, T. (2001) "An Internally Replicated Quasi-Experiment Comparison of Checklist and Perspective-Based Reading of Code Documents," *IEEE Transactions on Software Engineering*, (27:5).
- Lang, E. The LILOG Ontology from a Linguistic Point of View. In O. Herzog and C. R. Rollinger (eds.), *Text Understanding in LILOG*. Springer-Verlag, Berlin. 1991.
- Larkin J.H. and H.A., Simon (1987) "Why a Diagram Is (Sometimes) Worth Ten Thousand Words," *Cognitive Science*, (11), pp. 65-99
- Lee, H., and S., Whang *Information Sharing in a Supply Chain* Research Paper Series, Graduate School of Business, Stanford University. 1998.
- Lee, J., Upadhyaya, S., Rao, H.R., and Sharman, R. (2005) "Secure Knowledge Management and the Semantic Web," *Communications of ACM*, 48(12), pp. 48-54.
- Lee, Y., Lee, J., and Lee, Z. (2002) "Integrating Software Lifecycle Process Standards with Security Engineering," *Computer and Security*, (21:4), pp. 345-355.
- Lehmann, F. (1995) "Machine-Negotiated, Ontology-Based EDI (Electronic Data Interchange)," In *Proceedings of CIKM-94 Workshop on Electronic Commerce*, Springer Verlag.
- Li, L. and I., Horrocks (2004) "A Software Framework for Matchmaking Based on Semantic Web Technology," *International Journal of Electronic Commerce*, 8(4), pp. 39-60.
- Liang, W. Y. and C.C., Huang (2006) "Agent-Based Demand Forecast in Multi-Echelon Supply Chain," *Decision Support Systems*, 42, pp. 390-407.
- Loebecke, C., van Fenema, P. and Powell, P. (1999) "Co-Opetition and Knowledge Transfer," *Database for Advances in Information Systems*, 30(2), pp. 14-25.
- Lorange, P. (1996) "Strategy at the Leading Edge –Interactive Strategy- Alliances and Partnership," *Long Range Planning*, 29(4), pp. 581-584.

- Luftman, J. , Kempaiah, R., and Nash, E. (2006) "Key issues for IT executives 2005," *MIS Quarterly Executive*, (5:22), pp. 27-45.
- Malone, T. and K. Crowston (1994) "The Interdisciplinary Study of Coordination," *ACM Computing Surveys*, 26(1), pp. 87-119.
- Malone, T. W., Crowston, K., and Herman, G. A. (2003) editors, *Organizing business knowledge: the MIT process handbook*, MIT Press, Cambridge, Massachusetts.
- Malone, T. W., Crowston, K., Lee, J., Pentland, B., Dellarocas, C.; Wyner, G., Quimby, J., Osborn, C. S., Bernstein, A., Herman, G., Klein, M., O'Donnell, E. (1999) "Tools for Inventing Organizations: Toward a Handbook of Organizational Processes" *Management Science*, 45(3), pp. 425-444.
- Malone, T. W., Yates, J., and Benjamin, R. I. (1987) "Electronic Markets and Electronic Hierarchies," *Communications of the ACM*, 30(6), pp. 484-497.
- March, S., Hevner, A., Ram, S. (2000) "Research Commentary An Agenda for Information Technology Research in Heterogeneous and Distributed Environments," *Information Systems Research*, 11(4), pp. 327-341.
- March, S.T., and Smith, G. (December 1995) "Design and Natural Science Research on Information Technology," *Decision Support Systems*, 15(4), pp. 251-266.
- Markus, M.L., Majchrzak, A., and Gasser, L. (September 2002) "A Design Theory for Systems that Support Emergent Knowledge Processes," *MIS Quarterly*, 26(3), pp. 179-212.
- Mata, F., Fuerst, W. L., and Barney, J.B. (1995) "Information Technology and Sustained Competitive Advantage: A Resource-Based Analysis," *MIS Quarterly*, (19: 4), pp. 487-505.
- Mc Dermott, J., Fox, C. (December 1999) "Using Abuse Care Models for Security Requirements Analysis," in *Proceedings of the 15th Annual Computer Security Applications Conference*.
- McDaniel, L. (1990) "The Effects of Time Pressure and Audit Program Structure on Audit Performance ," *Journal of Accounting Research*, (28: 2), pp. 267-285.

- McGaughey, S. (2002) "Strategic Interventions in Intellectual Asset Flows," *Academy of Management Review*, 27(2), pp. 248-274.
- McGuinness, D.. Ontological Issues for Knowledge-Enhanced Search. In N. Guarino (ed.) *Formal Ontology in Information Systems*. IOS Press. 1998.
- McIlraith, S., Son, T.C. and Zeng, H., (March/April 2001) "Semantic Web Services," *IEEE Intelligent Systems*, pp. 46-53.
- Mena, E., Kashyap, V., Illarramendi, A., and Sheth, A.. Domain Specific Ontologies for Semantic Information Brokering on the Global Information Infrastructure. In N. Guarino (ed.) *Formal Ontology in Information Systems*. IOS Press. 1998.
- Miller, J. Wood, M., and Roper, M. (1998) "Further Experiences with Scenarios and Checklists," *Empirical Software Engineering*, (3:1), pp. 37-64.
- Mouratidis, H., Giorgini, P., and Manson, G. (2005) "When Security Meets Software Engineering: A Case of Modelling Secure Information Systems," *Information Systems* (30), pp. 609-629.
- Muller, H.J. (1997) "Towards agent systems engineering," *Data and Knowledge Engineering*, 23, pp. 217-245.
- Mylopoulos, J. (1992) "Conceptual Modeling and Telos", Chapter 2 in P. Loucopoulos and R. Zicari (Ed.), *Conceptual Modeling, Databases, and CASE*. UK: Wiley, pp. 49-68.
- Neter J, Wasserman W, and Kutner MH. *Applied Statistical Models: Regression, Analysis of Variance, and Experimental Design*. 3rd ed. Boston, Mass: Irwin; 1990.
- Newell, A. (1982) "The Knowledge Level," *Artificial Intelligence*, 18, pp. 87-127.
- Nissen, M. and K., Sengupta (2006) "Incorporating Software Agents into Supply Chains: Experimental Investigation with a Procurement Task," *MIS Quarterly*, 30, pp. 145-166.
- Noy, N. F. and D. L. McGuinness (2002) *Ontology Development 101: A Guide to Creating Your First Ontology*. Stanford University, Stanford, CA, Stanford Medical Informatics Report SMI-2002-0880.

- Oh, S. and Park, S. (2003) "Task-role-based Access Control Model," *Information Systems* 28(6), pp. 533-562.
- Papazoglou, M. P. (April 2001) "Agent Oriented Technology in Support of e-business: Enabling the Development of Intelligent Business Agents for Adaptive, Reusable Software," *Communications of the ACM*, 44(4), pp. 71-77.
- Park, J. S., Sandhu, R., and Ahn, G. (February 2001) "Role-Based Access Control on the web", *ACM Transactions on Information and Systems Security*, 4(1), pp. 37-71.
- Payne, J.W., Laughhunn D. J., and Crum, R. (1980) "Translation of Gambles and Aspiration Level Effects in Risky Choice Behavior," *Management Science* (26:10), pp. 1039-1060.
- Porter, A. A., Votta, L. G., and Basili, V. R. (1994) "Comparing detection methods for software requirement inspections: A replicated experiment," *IEEE Transactions on Software Engineering* 21, pp. 563-575.
- Porter, M.E., Millar, V.E. (July/August 1985) "How Information Gives You Competitive Advantage", *Harvard Business Review*, 63(4).
- Raghu, T.S. and A., Vinze (2007) "A Business Process Context for Knowledge Management," *Decision Support System*,
- Rai, A., Patnayakuni, R., and Patnayakuni, N. (2006) "Firm Performance Impacts of Digitally Enabled Supply Chain Integration Capabilities," *MIS Quarterly*, 30(2), pp. 225-246.
- Ram, S. and J. Park (2004) "Semantic Conflict Resolution Ontology (SCROL): An Ontology for Detecting and Resolving Data and Schema Level Conflicts", *IEEE Transactions on Knowledge and Data Engineering*, 16(2), pp. 189-202.
- Sandhu, R.S., Coyne, E.J., Feinstein, H.L., and Youman, C.E. (February 1996) "Role-Based Access Control Models," *IEEE Computer*, 29(2), pp. 38-47.
- Satzinger, J., and R., Jackson (2003) "Making the Transition from OO Analysis to OO Design with the Unified Process," *Communication of the Association for Information Systems*, (12), pp. 659-683.

Sawhney, M., and D., Parikh (January 2001) "Where Value lies in a Networked World," *Harvard Business Review*, pp. 79-86.

Schwarz, L. *The State of Practice in Supply-Chain Management Perspective in Applications of Supply Chain Management and E-Commerce Research in Industry*, E. Akcali, J. Geunes, .M. Pardalos, H.E. Romeijn, and Z.J. Shen (editors), Kluwer, Academic Publishers, Dordrecht, The Netherlands. 2004.

Segars, A.H., and Chatterjee, D. (2003). "An Overview of Contemporary Practices and Trends," in: *Transformation of the Enterprise through eBusiness*, Society for Information Management.

Shapiro, S. and M. Wilk, (1968) "A Comparative Study of Various Tests of Normality," *Journal of the American Statistical Association*, pp. 1343-1372.

Shoham, Y. (1993) "Agent Oriented Programming," *Journal of Artificial Intelligence*, 60(1), pp. 51-92.

Sikora, R., and M.J., Shaw (1998) "A Multi-Agent Framework for the Coordination and Integration of Information Systems," *Management Science*, 44(11), pp. S65-S78.

Simon. H.A. *The Sciences of the Artificial*, MIT Press, Cambridge, MA, 1996..

Simonin, B. L. (1999) "Ambiguity and the process of knowledge transfer in strategic alliances", *Strategic Management Journal*, 20, pp. 595-623.

Singh, R. and Salam, A.F. (2006) "Semantic Information Assurance for Secure Distributed Knowledge Management: A Business Process Perspective" *IEEE Transactions on Systems, Man and Cybernetics*. 36(3), pp. 472-486.

Singh, R., Iyer, L.S., and Salam, A.F. (2005) "Semantic eBusiness," *International Journal of Semantic Web and Information Systems*, 1(1), pp. 19-35.

Singh, R., Iyer, L.S., and Salam, A.F. (2005) "The Semantic eBusiness Vision," *Communications of the ACM*, 48(12), pp. 38-41.

Siponen, M., Baskerville, R., and Heikka, J. (2006) "A Design Theory for Secure Information Systems Design Methods," *Journal of the Association for Information Systems* (7:8), pp. 568-592.

- Sivashanmugam, K., Miller, J. A., Seth, A. P. and Verma, K. (2004) "Framework for Semantic Web Process Composition," *International Journal of Electronic Commerce*, 9(2), pp. 71-106.
- Soffer, P. and Y., Wand (2007) "Goal-Driven Multi-Process Analysis," *Journal of the Association for Information Systems* (8:3), pp.175-203.
- Sohr, K., Ahn, G., and Migge, L. (2005) "Articulating and Enforcing Authorisation Policies with UML and OCL," *Software Engineering for Secure System- Building Trustworthy Applications (SESS'05)*, 2005, St. Luis, MO, USA.
- Sugumaran, V., and Storey, V. C. (2002) "Ontologies for Conceptual Modeling: Their Creation, Use, and Management," *Data and Knowledge Engineering*, 42(3), pp. 251-271.
- Swaminathan, J., and S., Tayur (2003) "Models for Supply Chains in E-Business," *Management Science*, 49(10), pp. 1387-1406.
- Tallman, S., Jenkins, M., Henry, N., Pinch, S. (2004) "Knowledge, Clusters and Competitive Advantage," *Academy of Management Review*, 29(2), pp. 258-271.
- The National Institute of Standards and Technology (NIST), 2004 available at <http://csrc.nist.gov/rbac>. Accessed on November 2006.
- Thomas, M., Redmond, R. T., Yoon, V., and Singh, R. (2006) "A Semantic Approach to Monitoring Business Process Performance", *Communications of the ACM*, 48(12) pp. 55-59.
- Uschold, M., King, M., Moralee, S., and Zorgios, Y. (1998) "The Enterprise Ontology," *The Knowledge Engineering Review*.
- Vaishnavi, V. and B., Kuechler "Design Research in Information Systems," <http://www.isworld.org/Researchdesign/drIsIsworld.htm>, Accessed December, 2006.
- Van de Riet, R., Burg, H., and Dehne, F.. Linguistic Issues in Information Systems Design. In N. Guarino (ed.) *Formal Ontology in Information Systems*. IOS Press. 1998

- van der Aalst, W.M.P. and Kumar, A. (2003) "XML Based Schema Definition for Support of Inter-Organizational Workflow," *Information Systems Research*, 14(1), pp.23-46.
- van Wyk, K. and G., McGraw (2005) "Bridging the Gap Between Software Development and Information Security," *IEEE Security & Privacy*, Sept-Oct 2005, pp. 75-79.
- Vessey, Iris (1991) "Cognitive Fit: A Theory-Based Analysis of the Graphs Versus Tables Literature," *Decision Sciences*, (22:2), pp. 219-240.
- VICS, 1999, CPFR Technical Specifications, available at http://www.vics.org/standards/cpfr_roadmap_case_studies/13_5_CPFR_specification_s.pdf. Accessed on November, 2006.
- VICS, 2004, Voluntary Inter-industry Commerce Standards Association (VICS) - Collaborative Planning, Forecasting and Replenishment (CPFR®), available at http://www.vics.org/committees/cpfr/CPFR_Overview_US-A4.pdf. Accessed on November, 2006.
- Walls, J.G., Widmeyer, G.R., and El Sawy, O. A. (1992) "Building an Information System Design Theory for Vigilant EIS," *Information Systems Research*, 3(1), pp. 36-59.
- Wand, Y. and R., Weber (2002) "Research Commentary: Information Systems and Conceptual Modeling—A Research Agenda," *Information Systems Research*, 13(4), pp. 363-376.
- Weber, R.. Ontological Foundations of Information Systems. Coopers and Lybrand. 1997
- Wernerfelt, B.(1984) "A Resource-Based View of the Firm," *Strategic Management Journal* 5(2) pp. 171-180.
- Westgard, J.O., and M.R., Hunt (1973) "Use and Interpretation of Common Statistical Tests in Method Comparison Studies," *Clinical Chemistry*, 19, pp. 49-57.
- WfMC, Workflow Management Coalition, www.wfmc.org, 1996.
- WfMC, Workflow Standard-Interoperability Wf-XML Binding. Workflow Management Coalition, 1999, Document WFMC-TC-1023.

Wiederhold, G. (ed.). *Intelligent Integration of Information*. Kluwer Academic Publishers, Boston, MA. 1996.

Williams, E. J. (1949) "Experimental designs balanced for the estimation of residual effects of treatments," *Australian Journal of Scientific Research*, A(2), pp. 149-168.

Yin, R. K. (2002) *Case Study Research, Design and Methods*, 3rd ed. Newbury Park, Sage Publications.

APPENDICES

Appendix A-CPFR Partnerships

List of Buyers and Suppliers Participating in CPFR Partnerships		
Buyer Organizations		
10 Internal Affiliates	4 Retailers	850 n-Tier Partners
Ace Hardware	Albertson's	Best Buy
Canadian Tire	CVS	Dansk
Dealers	Delhaize le Lion	Distributors
Do It Best	Eckerd	Federated Department Stores
H.E. Butt	Home Depot	J.C. Penny
Jusco	Londis	Marshall Field's
Match Supermarket	McDonald's US/ McDonald's France	Mijer
Mervyn's	Radio Shack	RiteAid
Royal Ahold	RONA	Safeway/Safeway UK
Safe	Sainsbury	SAKS
Sears Roebuck	Somerfield	Sports Authority
Staples	Superdrug	Target
Tesco	Tru Value	Walgreens
Wal-Mart	Wickes Furniture	Woolworth UK
Supplier Organizations		
12 Suppliers	20+ Suppliers	Ashley Furniture
Ball Sports	Black & Decker	Broyhill
Channel	Chapin	Colgate-Palmolive
Compaq	Eastman Chemicals	ECPG3
Eli Lilly	Feather Fruit Growers' Cooperative	FujiFilm
GE Appliances	General Mills	Genovs
Georgia Pacific	Harley-Davidson	Hasbro
Heineken	Henkel	Herlitz
Hewlett-Packard	HYKo	Inland Paperboard & Packaging
International Paper	John Deere	Johnson & Johnson
Kao	Kimberly Clark	Kraft
Lever-Fabrege	Levi Strauss	Liquid Nails
Liz Claiborne	Manco	Mars
Master Lock	Meriat	Mitsubishi Motor
Nestle UK	New Balance	Panasonic
Philips Consumer	Pillowtex	Polo Ralph Lauren

List of Buyers and Suppliers Participating in CPFR Partnerships		
Proctor & Gamble	Reynolds Metal	Sara Lee
Schering-Plough	Solo Cup	Unilever Argentina
Vandemoortele of Belgium	Warner-Lambert	Woodstream
Source: Schwarz, L. (2004)		

Appendix B-Description Logics

Appendix B-1. Seller agent creates order forecast activity to coordinate order forecast

$\text{CreateOrderForecast} \sqsubseteq (\text{BusinessActivity}) \wedge$
 $(= 1 \text{ IsPerformedby. SellerRole}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. POSData}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. ForecastImpactEvents}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. InventoryStrategy}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. CurrentInventory}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. SalesForecast}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. OrderForecast}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. ExceptionResolutionData}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. ItemManagementData}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. CapacityLimitations}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. HistoricalDemandShipment}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. OrderShipmentData}) \wedge$
 $(= 1 \text{ HasCoordinationFlowProduces. OrderForecast}) \wedge$
 $(= 1 \text{ HasPermissionRead. POSData}) \wedge$
 $(= 1 \text{ HasPermissionRead. ForecastImpactEvents}) \wedge$
 $(= 1 \text{ HasPermissionRead. InventoryStrategy}) \wedge$
 $(= 1 \text{ HasPermissionRead. CurrentInventory}) \wedge$
 $(= 1 \text{ HasPermissionRead. SalesForecast}) \wedge$
 $(= 1 \text{ HasPermissionRead. OrderForecast}) \wedge$
 $(= 1 \text{ HasPermissionRead. ExceptionResolutionData}) \wedge$
 $(= 1 \text{ HasPermissionRead. ItemManagementData}) \wedge$
 $(= 1 \text{ HasPermissionRead. CapacityLimitations}) \wedge$
 $(= 1 \text{ HasPermissionRead. HistoricalDemandShipment}) \wedge$
 $(= 1 \text{ HasPermissionRead. OrderShipmentData}) \wedge$
 $(= 1 \text{ HasPermissionRead. OrderForecast}) \wedge$
 $(= 1 \text{ HasPermissionWrite. OrderForecast}) \wedge$
 $(= 1 \text{ HasPermissionCreate. OrderForecast})$

Appendix B-2. Sellers create their order forecast using standardized ontology for specifying the resource

$\text{OrderForecast} \sqsubseteq (\text{Resource}) \wedge$
 $(= 1 \text{ IsOwnedBy. Seller}) \wedge$
 $(= 1 \text{ hasID .8}) \wedge$
 $(= 1 \text{ CoordinatesFlowProducedBy. CreateOrderForecast}) \wedge$
 $(= 1 \text{ CoordinatesFlowConsumedBy . GenerateOrder}) \wedge$
 $(= 1 \text{ Permits .CreateOrderForecast}) \wedge$
 $(= 1 \text{ Permits . GenerateOrder}) \wedge$
 $(= 1 \text{ hasCharacteristics. ForecastType}) \wedge$
 $(= 1 \text{ hasCharacteristics. GenerationDate}) \wedge$
 $(= 1 \text{ hasCharacteristics. StartDate}) \wedge$
 $(= 1 \text{ hasCharacteristics. EndDate}) \wedge$

$(=1 \text{ hasCharacteristics.ProductID}) \wedge$
 $(=1 \text{ hasCharacteristics.Quantity}) \wedge$
 $(=1 \text{ hasCharacteristics.ChangeRestrictionIndicator})$

Appendix B-3. The seller agent generates order activity to coordinate order

$\text{GenerateOrder} \subseteq (\text{BusinessActivity}) \wedge$
 $(=1 \text{ IsPerformedby.SellerRole}) \wedge$
 $(=1 \text{ HasCoordinationFlowConsumes.Order}) \wedge$
 $(=1 \text{ HasCoordinationFlowConsumes.ItemManagementData}) \wedge$
 $(=1 \text{ HasCoordinationFlowConsumes.OrderForecast}) \wedge$
 $(=1 \text{ HasCoordinationFlowProduces.Order}) \wedge$
 $(=1 \text{ HasPermissionRead.Order}) \wedge$
 $(=1 \text{ HasPermissionRead.ItemManagementData}) \wedge$
 $(=1 \text{ HasPermissionRead.OrderForecast}) \wedge$
 $(=1 \text{ HasPermissionRead.Order}) \wedge$
 $(=1 \text{ HasPermissionWrite.Order}) \wedge$
 $(=1 \text{ HasPermissionCreate.Order})$

Appendix B-4. Sellers communicate their order data using standardized ontology for specifying the resource

$\text{Order} \subseteq (\text{Resource}) \wedge$
 $(=1 \text{ IsOwnedBy.Buyer}) \wedge$
 $(=1 \text{ hasID.9}) \wedge$
 $(=1 \text{ CoordinatesFlowProducedBy.CommunicateOrder}) \wedge$
 $(=1 \text{ CoordinatesFlowConsumedBy.GenerateOrder}) \wedge$
 $(=1 \text{ Permits.CommunicateOrder}) \wedge$
 $(=1 \text{ Permits.GenerateOrder})$

Appendix B-5. Seller planning agent communicates adjustments to coordinate the Create Order Forecast activity

$\text{CommunicateAdjustments} \subseteq (\text{BusinessActivity}) \wedge$
 $(=1 \text{ IsPerformedby.SellerPlanningRole}) \wedge$
 $(=1 \text{ HasCoordinationFlowProduces.Adjustments}) \wedge$
 $(=1 \text{ HasPermissionRead.Adjustments}) \wedge$
 $(=1 \text{ HasPermissionWrite.Adjustments})$

Appendix B-6. Buyers receive adjustments using standardized ontology for specifying the resource

$\text{Adjustments} \subseteq (\text{Resource}) \wedge$
 $(=1 \text{ IsOwnedBy.Buyer}) \wedge$
 $(=1 \text{ hasID.7}) \wedge$
 $(=1 \text{ CoordinatesFlowProducedBy.CommunicateAdjustments}) \wedge$
 $(=1 \text{ CoordinatesFlowConsumedBy.ReceiveAdjustments}) \wedge$
 $(=1 \text{ Permits.CommunicateAdjustments}) \wedge$

$(= 1 \text{ Permits. ReceiveAdjustments}) \wedge$
 $(\geq 1 \text{ hasCharacteristics. ProductID}) \wedge$
 $(\geq 1 \text{ hasCharacteristics. RightQuantity}) \wedge$
 $(\geq 1 \text{ hasCharacteristics. Date})$

Appendix B-7. The buyer planning agent receives adjustments to coordinate the Create Order Forecast activity

$\text{ReceiveAdjustments} \sqsubseteq (\text{BusinessActivity}) \wedge$
 $(= 1 \text{ IsPerformedby. BuyerPlanningRole}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumedBy. Adjustments}) \wedge$
 $(= 1 \text{ HasPermissionRead. Adjustments})$

Appendix B-8. Activity Creates Order Forecast, which is performed by the seller forecast agent

$\text{CreateOrderForecast} \sqsubseteq (\text{BusinessActivity}) \wedge$
 $(= 1 \text{ IsPerformedby. SellerForecastRole}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. POSData}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. EventsCalendar}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. InventoryStrategy}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. AvailableStock}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. SalesForecast}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. OrderForecast}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. ExceptionResolutionData}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. ItemManagementData}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. HistoricalDemandShipment}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. OrderShipmentData}) \wedge$
 $(= 1 \text{ HasCoordinationFlowConsumes. CPFRPolicies}) \wedge$
 $(= 1 \text{ HasCoordinationFlowProduces. OrderForecast}) \wedge$
 $(= 1 \text{ HasCoordinationRead. POSData}) \wedge$
 $(= 1 \text{ HasCoordinationRead. EventsCalendar}) \wedge$
 $(= 1 \text{ HasCoordinationRead. InventoryStrategy}) \wedge$
 $(= 1 \text{ HasCoordinationRead. AvailableStock}) \wedge$
 $(= 1 \text{ HasCoordinationRead. SalesForecast}) \wedge$
 $(= 1 \text{ HasCoordinationRead. OrderForecast}) \wedge$
 $(= 1 \text{ HasCoordinationRead. ExceptionResolutionData}) \wedge$
 $(= 1 \text{ HasCoordinationRead. ItemManagementData}) \wedge$
 $(= 1 \text{ HasCoordinationRead. HistoricalDemandShipment}) \wedge$
 $(= 1 \text{ HasCoordinationRead. OrderShipmentData}) \wedge$
 $(= 1 \text{ HasCoordinationRead. CPFRPolicies}) \wedge$
 $(= 1 \text{ HasPermissionWrite. OrderForecast}) \wedge$
 $(= 1 \text{ HasPermissionCreate. OrderForecast})$

Appendix B-9. Sellers create their order forecast using standardized ontology for specifying the resource

$\text{OrderForecast} \sqsubseteq (\text{Resource}) \wedge$

(= 1 *IsOwnedBy*. *Seller*) ∧
 (= 1 *hasID* .12) ∧
 (=1 *CoordinatesFlowProducedBy*.*CreateOrderForecast*) ∧
 (= 1 *CoordinatesFlowConsumedBy* . *GenerateOrder*) ∧
 (=1 *Permits* .*CreateOrderForecast*) ∧
 (= 1 *Permits* . *GenerateOrder*) ∧
 (=1 *hasCharacteristics*. *ForecastType*) ∧
 (=1 *hasCharacteristics*. *GenerationDate*) ∧
 (=1 *hasCharacteristics*. *StartDate*) ∧
 (=1 *hasCharacteristics*. *EndDate*) ∧
 (>=1 *hasCharacteristics*. *ProductID*) ∧
 (>=1 *hasCharacteristics*.*Quantity*) ∧
 (>=1 *hasCharacteristics*.*MinQuantity*) ∧
 (>=1 *hasCharacteristics*.*MaxQuantity*) ∧
 (>=1 *hasCharacteristics*.*ChangeRestrictionIndicator*)

Appendix C- Institutional Review Board Office (IRB) of Research Compliance (ORC) at the University of North Carolina at Greensboro acceptance Document and Project Description



THE UNIVERSITY of NORTH CAROLINA
GREENSBORO

Office of Research Compliance

2718 Beverly Cooper Moore and Irene Mitchell Moore
Humanities and Research Administration Building
PO Box 26170, Greensboro, NC 27402-6170
336.256.1482 Phone 336.256.1482 Fax
www.uncg.edu/orc/

October 3, 2007

Dr. Lakshmi Iyer
Information Systems and Operations Management
482 Bryan Building
Refer to: IRB No.078078

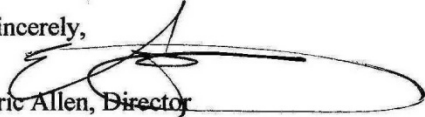
Dear Dr. Iyer,

As required by University policy a member of the UNCG IRB has given your research protocol entitled "A Design Theory for Secure Semantic eBusiness Processes" (IRB No. 078078) an exempt review as permitted under UNCG's Federal Wide Assurance (FWA 00000216). Your minimal risk protocol has been deemed exempt under section B2 of 45 CFR 46.101.

You should be aware that any changes in your protocol must be approved by the IRB prior to being implemented. Likewise, any problems, complaints or injuries that arise during the course of your project which involves human participants must be reported promptly to the Office of Research Compliance. The approved informed consent form is attached. This version must be used when obtaining informed consent as outlined in this protocol but the stamp does not need to appear on the form.

This research protocol is valid for five years unless changes are made which remove the exempt status. You will receive a continuing review form prior to the fifth anniversary to keep this protocol active. Conversely you are responsible for notifying the ORC when your study is completed and all work is published. Thank you for your cooperation on this matter and best wishes on your project.

Sincerely,


Eric Allen, Director
Office of Research Compliance
Cc:

THE UNIVERSITY OF NORTH CAROLINA AT GREENSBORO
CONSENT TO ACT AS A HUMAN PARTICIPANT: LONG FORM

Project Title: A Design Theory for Secure Semantic eBusiness Processes

Project Director: Fergle D'Aubeterre and Dr. Lakshmi S. Iyer

Participant's Name: _____

DESCRIPTION AND EXPLANATION OF PROCEDURES:

Purpose and Procedure: This survey is conducted as part of a research study by Fergle D'Aubeterre and Dr. Lakshmi S. Iyer in the ISOM Department at The University of North Carolina at Greensboro. It will take about 30 minutes to complete the survey. The purpose of this study is to evaluate a new information system analysis and design methodology that is intended to guide the analysis and design of secure business processes. We expect that the empirical results will demonstrate the utility of the method in generating greater awareness of security policies and constraints for business and systems analysts.

- This survey does not identify you through any personal identification and only collects data about you as it pertains to demographic information.
- Your answers will be kept strictly confidential and will not be released in any form that can be identified with you individually.
- Results of the survey may be published in aggregate form only, without identifying any individual. Data will be kept until the results are disseminated in aggregate form. The estimated time is 4 years from the time data collection is complete.
- Paper copies will be in lockable file cabinets and data files in a password protected computer. Both of these will be in Fergle D'Aubeterre's lockable office. Paper copies will be shredded after the study is complete and data files will be deleted from the computer used to store and analyze data.
- This survey has been approved by IRB at UNCG.
- It is important that you answer the questions honestly and accurately.
- Questions regarding the research itself will be answered by Fergle D'Aubeterre via email: fjdaubet@uncg.edu.

RISKS AND DISCOMFORTS:

There are no known risks associated with this project.

POTENTIAL BENEFITS:

This research will make important contributions to research in understanding business process security requirements and modeling techniques. This research also helps us develop and offer better content for students in relevant courses offered by the Department and the School.

COMPENSATION/TREATMENT FOR INJURY:

Since no risks are foreseen, there will be no compensation for any injuries.

CONSENT:

By signing this consent form, you agree that you understand the procedures and any risks and benefits involved in this research. You are free to refuse to participate or to withdraw your consent to participate in this research at any time without penalty or prejudice; your participation is entirely voluntary. Your privacy will be protected because you will not be identified by name as a participant in this project.

The University of North Carolina at Greensboro Institutional Review Board, which insures that research involving people follows federal regulations, has approved the research and this consent form. Questions regarding your rights as a participant in this project can be answered by calling Mr. Eric A. G. (336) 256-1482. Questions regarding the research itself will be answered by Fergle D'Aubeterre

APPROVED IRB

CONSENT FORM

(fjdaubet@uncg.edu) or [Dr. Iyer\(Isiyer@uncg.edu\)](mailto:Dr.Iyer@uncg.edu). Any new information that develops during the project will be provided to you if the information might affect your willingness to continue participation in the project.

By signing this form, you are agreeing to participate in the project described to you by Fergle D'Aubeterre.

Participant's Signature*

Date

APPROVED IRB

OCT 04 2007

CONSENT FORM

Appendix D- Experiment Material

Questions and Scenario for SSeBP Design Theory Experimental Evaluation

Note: Two types of instruments were used for the study. The difference between the instruments is that the order in which Part III and IV are presented.

Part I

Subject's Characteristics

1. Gender: ☐ Male ☐ Female
2. Age in years (check one):
☐ Less than 18 years ☐ 18-25 ☐ 26-35
☐ 36-55 ☐ More than 55 years

If you are **UNDER** 18 years of age, Please do **NOT** complete this survey.

3. Currently, what is your highest level of education? (Check one):
☐ High School ☐ Some years of college ☐ Bachelors Degree;
Major: _____
☐ Masters Degree; Degree _____ ☐ Doctorate Degree;
Degree _____
4. Please choose the option that **best** describes your current occupation status (check one):
☐ Full time Employee; Number of years of experience _____; Job
Title: _____
☐ Part time Employee; Number of years of experience _____; Job
Title: _____
☐ Self-employed; Number of years of experience _____; Job
Title: _____
☐ Full time College Student ☐ Other: _____
5. Please specify your Experience using System Development Methodologies (SDM)
☐ No experience in SDM ☐ College experience in SDM ☐ Industrial
experience in SDM

6. Please specify your level of experience using the following Unified Modeling
Language (UML) techniques

UML Technique	In School	At Work
Sequence Diagrams	Years _____ Months _____	Years _____ Months _____
Activity Diagrams	Years _____ Months _____	Years _____ Months _____

Use Case Diagrams	Years_____ Months_____	Years_____ Months_____
Class Diagrams	Years_____ Months_____	Years_____ Months_____
State Transition Diagrams	Years_____ Months_____	Years_____ Months_____
Other:_____	Years_____ Months_____	Years_____ Months_____

7. Please specify your level of experience using the following business process modeling techniques:

Business Process Modeling Technique	In School	At Work
Business Process Modeling Notation (BPMN)	Years_____ Months_____	Years_____ Months_____
Event-Driven Process Chains (EPC)	Years_____ Months_____	Years_____ Months_____
Role Activities Diagrams	Years_____ Months_____	Years_____ Months_____
Process Description Capture Method (IDEF3)	Years_____ Months_____	Years_____ Months_____
Other:_____	Years_____ Months_____	Years_____ Months_____

8. Please specify your level of experience using any of the following:

	In School	At Work
Gathering Information Security Requirements	Years_____ Months_____	Years_____ Months_____
Analyzing Information Security Requirements	Years_____ Months_____	Years_____ Months_____
Modeling Information Security Requirements	Years_____ Months_____	Years_____ Months_____
Other:_____	Years_____ Months_____	Years_____ Months_____

Part II: Please read the description about the “Create Order Forecast Business Process”

Scenario I: “Create Order Forecast Business Process”

The “create order forecast” business process takes place between a retailer (i.e.: buyer) and a manufacturer (i.e.: seller) organization. Here, retailers and manufacturers must work together to estimate future orders needs. In other words, they must determine the right products and their quantities that must be ordered for the next planning period. Accurate order forecasts drive sales increases, improve customer service, and support better inventory decisions.

The process is triggered at the beginning of each planning period. Here, the retailer (buyer) organization consolidates its point of sales (POS) data and generates an initial prediction of its sales for the next planning period (sales forecast). Such information, along with the available stock, the promotions and event calendars (i.e.: weather, school season, holidays, etc.), and the historical order shipment data is then retrieved by the manufacturer (seller) organization to generate an initial sales forecast.

At this point, the buyer and the seller organization with the assistance of a collaborative information system must compare their initial estimates to reach an agreement. Basically, the collaborative system retrieves information about the buyer inventory strategies, seller order shipment data, and collaborative policies (i.e.: CPFR policies), to determine any differences and/or errors that might exist in the initial sales forecast. Finally, the collaborative system produces the exceptions resolution data that is used to make the corrections or adjustments to the seller and buyer sales forecast.

1. Please specify your level of experience in **School** about the business process described before:
 - a) None
 - b) Less than 6 months
 - c) More than 6 months and less than 1 years
 - d) More than 1 year and less than 2 years
 - e) More than 2 years
2. Please specify your level of experience at **Work** about the business process described before:
 - a) None
 - b) Less than 6 months

- c) More than 6 months and less than 1 years
- d) More than 1 year and less than 2 years
- e) More than 2 years

Part III

The following Enriched Use Case and Activity Diagrams correspond to the business process of “create order forecast” describe in scenario I, part II.

Figure 1. Enriched Use Case

Use Case:	<i>Create Order Forecast</i>
Scenario:	Create a new Order Forecast
Brief Description:	Determining the right products and quantities that must be ordered for the next planning period
Actors/Security Subjects:	Buyer and Seller
Security Classification of the subject:	All Data Sources are confidential
Security Objects and Access Types to Security Objects:	<p>Object: Buyer Forecast and Inventory Database (the buyer must be able to read and write sales forecast, point of sales (POS) Data, and to read Inventory Strategy)</p> <p>Object: Seller Forecast and Inventory Database (the seller must be able to read sales forecast, POS Data, Available Stock, Events Calendar, Historical Order Shipment Data)</p> <p>Object: Collaborative Planning and Replenishment Database(the collaborative systems must be able to read order shipment, CPFR policies, Inventory Strategy and Item Management Data. The collaborative system must be able to read and write the seller and buyer adjustment forecast and the order forecast)</p>
Security Policy/Specific Security Restrictions	Buyer and Seller are only allowed to access security objects classified as confidential with the planning and replenishment department
Preconditions:	All the Data Sources exists
Flow of Events:	Actor:

	<ul style="list-style-type: none"> 9. The buyer generates and consolidates its point of sales (POS Data) 10. The buyer generates the initial Sales forecast 11. The seller retrieves the buyer's POS data, available stock, events calendars, and historical order shipment data. 12. The seller generates an initial Sales forecast 13. The buyer sends its inventory strategy 14. The seller sends the order shipment data and retrieve CFPR policies and Item Management Data 15. The collaborative system generates the exceptions resolution data 16. The collaborative system generates the adjustments to the seller and buyer Sales forecast
Exception Conditions:	If information about any object is not available, an appropriate error message is produced.

How to Read an Activity Diagram

Figure 2 shows an example of an Activity Diagram. Here, the process begins when *Actor 1* executes *Activity 1*, which is needed to complete *Activity 2*, which is executed by *Actor 2*. Then in order for *Actor 2* to execute *Activity 4*, both *Activity 3* and *Activity 2* must be completed first. Notice that, the process ends after *Activity 4* is completed.

Figure 2. Activity Diagram

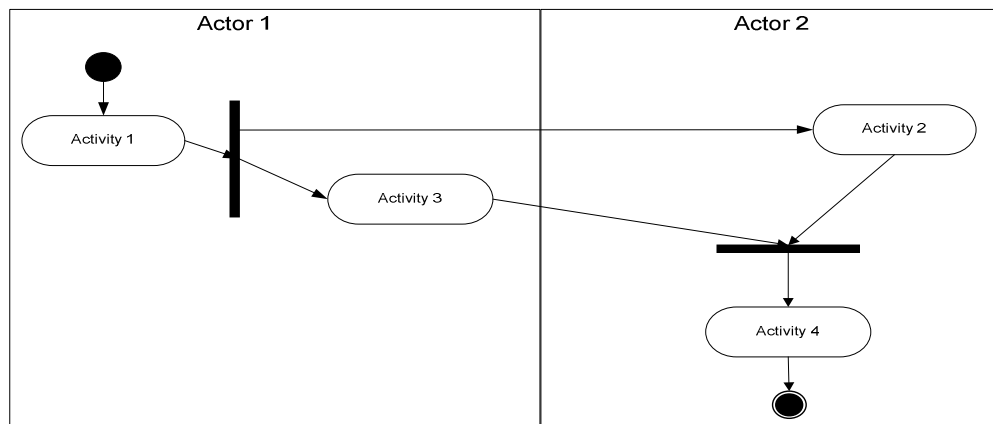
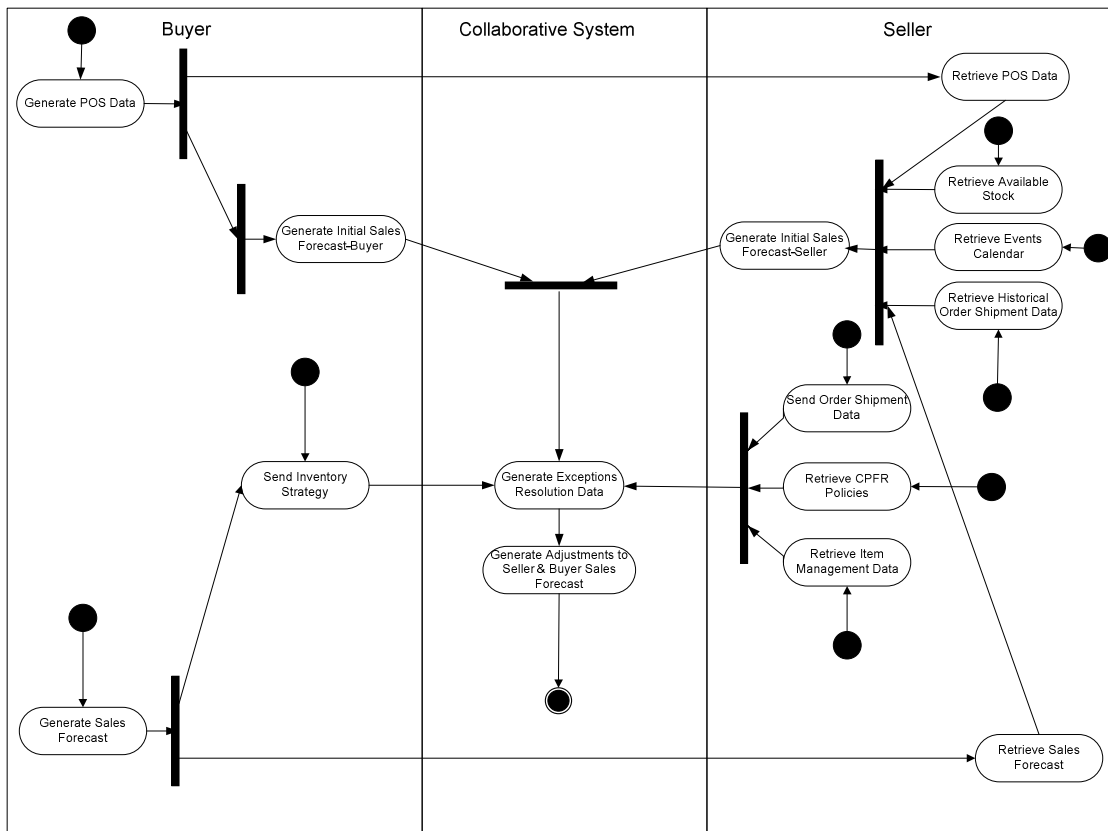


Figure 3. Activity Diagram



Please answer the following questions based on the description and diagrams provided above (Figure 1-Page 4 and Figure 3-Page 5).

1. Can the *Forecasting* analyst from the seller organization perform the *Retrieve Events Calendar* activity? Yes___ No___
2. Why? Because
 - a) Only the Buyer Planning analyst has permission to Read the *Events Calendar* information
 - b) Only the Seller Forecasting analyst has permission to Read the *Events Calendar* information
 - c) Only the Seller Planning analyst has permission to Read the *Events Calendar* information
 - d) All analysts have permission to Create/Write/ Read the Events Calendar information
 - e) It cannot be determined from the information given
 - f) I do not know
3. What would happen if the *Forecasting* analyst from the seller organization cannot perform the *Retrieve Events Calendar* activity?
 - a) The Generate Exceptions activity would not be performed
 - b) The execution of the remaining activities would not be affected
 - c) The Generate Seller Initial Sales forecast activity would not be performed
 - d) The Communicate Inventory Strategy activity would not be performed
 - e) It cannot be determined from the information given
 - f) I do not know
4. Who has permission to perform the *Communicate Inventory Strategy* activity?

i) Buyer Planning Analyst	l) Seller Forecasting Analyst
j) Buyer Replenishment Analyst	m) All
k) Seller Planning Analyst	n) None

- o) It cannot be determined from the information given
- p) I do not know
5. Why? Because
- g) The Buyer Replenishment Analyst has permission to Read the *Inventory Strategy* information
- h) The Seller Planning Analyst has permission to Read the *Inventory Strategy* information
- i) All analysts have permission to Read the *Inventory Strategy* information
- j) Nobody has permission over the *Inventory Strategy* Information
- k) It cannot be determined from the information given
- l) I do not know
6. What would happen if the Replenishment analyst from the buyer organization does not have permission to read the *Inventory Strategy* information?
- g) The Communicate Order Shipment activity would not be performed
- h) The Generate Exceptions Order Forecast activity would not be performed
- i) The execution of the remaining activities would not be affected
- j) The Generate Buyer Initial Sales forecast activity would not be performed
- k) It cannot be determined from the information given
- l) I do not know
7. Who has permission to perform the *Generate Exceptions Order Forecast* activity?
- a) Buyer Planning Analyst
- b) Buyer Replenishment Analyst
- c) Seller Planning Analyst
- d) Seller Forecasting Analyst
- e) All
- f) None
- g) It cannot be determined from the information given
- h) I do not know
8. Why? Because

- a) The Buyer Planning Analyst has permission to Read the *Inventory Strategy* information
 - b) The Seller Planning Analyst has permission to Create/Write/ Read the *Exceptions Resolution* information
 - c) All analysts have permission to Create/Write/ Read the *Exceptions Resolution* information
 - d) Nobody has permission over the *Exceptions Resolution* information
 - e) It cannot be determined from the information given
 - f) I do not know
9. What would happen if the Replenishment analyst from the buyer organization does not have permission to perform the *Generate Exceptions Order Forecast*?
- a) The Generate Exceptions activity would not be performed
 - b) The execution of the remaining activities would not be affected
 - c) The Generate Buyer Initial Sales forecast activity would not be performed
 - d) It cannot be determined from the information given
 - e) I do not know
10. What kind of permission has the *Generate POS data* activity on the *POS Data*?
- a) Delete
 - b) Write
 - c) Create
 - d) Write/Delete
 - e) Create/Write/Read
 - f) It cannot be determined from the information given
 - g) I do not know
11. Why? Because
- a) *Generate POS data* activity has permissions to Read *POS data*

- b) *Generate POS* data activity has permissions to Create/Write/Read *POS* data
 - c) *Generate POS* data activity does not has permissions over *POS* data
 - d) It cannot be determined from the information given
 - e) I do not know
12. What would happen if *Generate POS Data* activity does not have the right permission over *POS Data*?
- a) The execution of the remaining activities would not be affected
 - b) The communicate sales forecast activity would not be performed
 - c) The Communicate Order Shipment activity would not be performed
 - d) The *Generate POS Data* activity would not be performed
 - e) It cannot be determined from the information given
 - f) I do not know
13. Can the *CPFR Policies* information be *Deleted* by the *Generate POS Data* activity?
Yes___ No___
14. Why? Because
- a) The *Generate POS Data* Activity has permission to Delete the *CPFR Policies* information
 - b) The *Generate POS Data* Activity has only permission to Create/Write/Read the *POS Data*
 - c) The Buyer Planning analyst has permission to Create/Write/Read the *CPFR Policies* information
 - d) Nobody has permission over the *CPFR Policies* information
 - e) It cannot be determined from the information given
 - f) I do not know
15. What would happen if the *Communicate CPFR Policies* activity cannot be performed by the Planning Analyst from the seller organization?
- a) The execution of the remaining activities would not be affected

- b) The Generate Buyer Initial Sales forecast activity would not be performed
- c) The Generate POS Data activity would not be performed
- d) The Generate Exceptions Order Forecast activity would not be performed
- e) It cannot be determined from the information given
- f) I do not know

16. Can the activity *Generate Exceptions Order Forecast* be executed before retrieving POS Data? Yes___ No___
17. Can the activity *Generate Exceptions Order Forecast* be executed before retrieving CPFR Policies? Yes___ No___
18. Can the activity *Generate Initial Sales forecast for the Buyer organization* be executed before *communicating the sales forecast activity*? Yes___ No___
19. Can the activity *Generate Exceptions Order Forecast* be executed before *generating the Order Shipment information*? Yes___ No___
20. Can the activity *Retrieve POS Data* be executed after the *retrieve initial sales forecast activity for the Seller organization*? Yes___ No___

Based on your experience, circle your level of agreement with each statement using the following scale:

1= **2** **3** **4** **5**
 Strongly Somewhat Neutral Somewhat Strongly
 Disagree Disagree Agree Agree

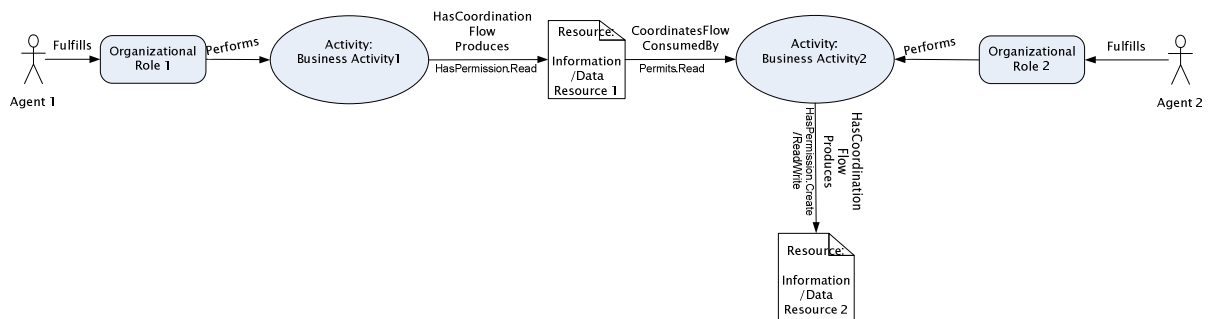
	1 Strongly Disagree	2	3	4	5 Strongly Agree
21. These diagrams help me to identify the security aspects of a business process	1	2	3	4	5
22. These diagrams help me to understand the security aspects of a business process	1	2	3	4	5
23. These diagrams help me to determine what would happen with the business process when security aspects are violated	1	2	3	4	5
24. The security aspects depicted in the diagrams are easy to understand	1	2	3	4	5

25. Representations of processes using this approach are clear	1	2	3	4	5
26. Representations of processes using this approach provide useful security information	1	2	3	4	5

Part IV

Figure 4 shows an example of the modeling concepts and grammar used to design a Secure Activity Resource Coordination Diagram. Here, in order to produce the *information/data resource 2*, *Organizational Role2*, which is only fulfilled by *Agent 2*, must perform *Business Activity 2*, which uses or consumes the *Information/Data Resource 1* that is produced or generated by the *Business Activity1*. In addition, *Business Activity1* is performed only by the *Organizational Role1*, which is only fulfilled by *Agent 1*. Each activity has permission over specific resources and resources permits activities to be performed on them. Permissions type includes *create, read, write* and *delete*. For instance, *Business Activity 1* has *read* permission over the *information/data resource 1*. *Business Activity 2* has *create/read/write* permissions over the *information/data resource 2*. Notice, that one activity cannot interact with another activity, and that activities are performed by specific organizational roles.

Figure 4. Secure Activity Resource Coordination Modeling Concepts and Grammar



How to Read a Role-Activity-Resource Permissions Table

Figure5 shows an example of the Agent- Role-Activity-Resource Permissions Table used to represent the security policies and constraints related to specific activities and information

resources involved in a business process. Here *Agent1* fulfills *Role1* which in turn performs *Business Activity 1*. *Business Activity 1* has permission to create, write, and read the *Data/Information Resource 1*.

Figure 5. shows an example of the Role-Activity-Resource Permissions Table

Agent	Role	Business Activity	Permission Type	Resource
Agent 1	Role1	Business Activity 1	Create/Write/Read	Data/Information Resource 1

The following Secure Activity Resource Coordination Diagram (figure 6) and Role-Activity-Resource Permissions Table (figure 7) correspond to the business process of “create order forecast”.

Note: Agents are similar to Actors. For instance, analysts, students are actors; therefore, they are also agents.

[illegible]

Figure 7. Role-Activity-Resource Permissions Table

Agent	Role	Business Activity	Permission Type	Resource
Buyer Planning Agent	Buyer Planning Role	Generate POS Data	Create/Write/Read	POS Data
		Generate Buyer Initial Sales Forecast	Create/Write/Read	Buyer Initial Forecast Sales
			Read	POS Data, Sales Forecast
Buyer Replenishment Agent	Buyer Replenishment Role	Communicate Sales Forecast	Read	Sales Forecast
		Communicate Inventory Strategy	Read	Inventory Strategy
		Communicate Exceptions Resolution Data	Read	Exceptions Resolution Data
Seller Forecasting Agent	Seller Forecasting Role	Retrieve POS Data	Read	POS Data
		Retrieve Sales Forecast	Read	Sales Forecast
		Generate Seller Initial Sales Forecast	Create/Write/Read	Seller Initial Sales Forecast
			Read	POS Data, Sales Forecast, Available Stock, Events Calendar, Historical Demand Shipment

Agent	Role	Business Activity	Permission Type	Resource
				Data
Seller Planning Agent	Seller Planning Role	Retrieve Available Stock	Read	Available Stock
		Retrieve Events Calendar	Read	Events Calendar
		Communicate Historical Demand & Shipment Data	Read	Historical Demand & Shipment Data
		Communicate Order Shipment	Read	Order Shipment
		Communicate CPFR Policies	Read	CPFR Policies
		Communicate Item Management Data	Read	Item Management Data
		Generate Exceptions Order Forecast	Read	Inventory Strategy, Buyer Initial Sales Forecast, Seller Initial Sales Forecast, Order Shipment, CPFR Policies, Item Management

Agent	Role	Business Activity	Permission Type	Resource
				Data
			Create/Write/Read	Exceptions Resolution Data
		Communicate Exceptions Resolution Data	Read	Exceptions Resolution Data

Please answer the following questions based on the description and diagrams provided above (Figure 6-Page 10 and Figure 7-Page 11).

1. Can the *Forecasting* analyst from the seller organization perform the *Retrieve Events Calendar* activity? Yes ___ No ___
2. Why? Because
 - a) Only the Buyer Planning analyst has permission to Read the *Events Calendar* information
 - b) Only the Seller Forecasting analyst has permission to Read the *Events Calendar* information
 - c) Only the Seller Planning analyst has permission to Read the *Events Calendar* information
 - d) All analysts have permission to Create/Write/ Read the Events Calendar information
 - e) It cannot be determined from the information given
 - f) I do not know
3. What would happen if the *Forecasting* analyst from the seller organization cannot perform the *Retrieve Events Calendar* activity?
 - a) The Generate Exceptions activity would not be performed
 - b) The execution of the remaining activities would not be affected
 - c) The Generate Seller Initial Sales forecast activity would not be performed
 - d) The Communicate Inventory Strategy activity would not be performed

- e) It cannot be determined from the information given
 - f) I do not know
4. Who has permission to perform the *Communicate Inventory Strategy* activity?
- a) Buyer Planning Analyst
 - b) Buyer Replenishment Analyst
 - c) Seller Planning Analyst
 - d) Seller Forecasting Analyst
 - e) All
 - f) None
 - g) It cannot be determined from the information given
 - h) I do not know
5. Why? Because
- a) The Buyer Replenishment Analyst has permission to Read the Inventory Strategy information
 - b) The Seller Planning Analyst has permission to Read the *Inventory Strategy* information
 - c) All analysts have permission to Read the *Inventory Strategy* information
 - d) Nobody has permission over the *Inventory Strategy* Information
 - e) It cannot be determined from the information given
 - f) I do not know
6. What would happen if the Replenishment analyst from the buyer organization does not have permission to read the *Inventory Strategy* information?
- a) The Communicate Order Shipment activity would not be performed
 - b) The Generate Exceptions Order Forecast activity would not be performed
 - c) The execution of the remaining activities would not be affected
 - d) The Generate Buyer Initial Sales forecast activity would not be performed
 - e) It cannot be determined from the information given
 - f) I do not know
7. Who has permission to perform the *Generate Exceptions Order Forecast* activity?

- a) Buyer Planning Analyst
- b) Buyer Replenishment Analyst
- c) Seller Planning Analyst
- d) Seller Forecasting Analyst
- e) All
- f) None
- g) It cannot be determined from the information given
- h) I do not know

8. Why? Because
- a) The Buyer Planning Analyst has permission to Read the *Inventory Strategy* information
 - b) The Seller Planning Analyst has permission to Create/Write/ Read the *Exceptions Resolution* information
 - c) All analysts has permission to Create/Write/ Read the *Exceptions Resolution* information
 - d) Nobody have permission over the *Exceptions Resolution* information
 - e) It cannot be determined from the information given
 - f) I do not know
9. What would happen if the Replenishment analyst from the buyer organization does not have permission to perform the *Generate Exceptions Order Forecast*?
- a) The Generate Exceptions activity would not be performed
 - b) The execution of the remaining activities would not be affected
 - c) The Generate Buyer Initial Sales forecast activity would not be performed
 - d) It cannot be determined from the information given
 - e) I do not know
10. What kind of permission has the *Generate POS data* activity on the *POS Data*?
- a) Delete
 - b) Write
 - c) Create
 - d) Write/Delete
 - e) Create/Write/Read
 - f) It cannot be determined from the information given
 - g) I do not know
11. Why? Because

- a) *Generate POS* data activity has permissions to Read *POS* data
 - b) *Generate POS* data activity has permissions to Create/Write/Read *POS* data
 - c) *Generate POS* data activity does not has permissions over *POS* data
 - d) It cannot be determined from the information given
 - e) I do not know
12. What would happen if *Generate POS Data* activity does not have the right permission over *POS Data*?
- a) The execution of the remaining activities would not be affected
 - b) The communicate sales forecast activity would not be performed
 - c) The Communicate Order Shipment activity would not be performed
 - d) The *Generate POS Data* activity would not be performed
 - e) It cannot be determined from the information given
 - f) I do not know
13. Can the *CPFR Policies* information be *Deleted* by the *Generate POS Data* activity?
Yes___ No___
14. Why? Because
- a) The *Generate POS Data* Activity has permission to Delete the *CPFR Policies* information
 - b) The *Generate POS Data* Activity has only permission to Create/Write/Read the *POS Data*
 - c) The Buyer Planning analyst has permission to Create/Write/Read the *CPFR Policies* information
 - d) Nobody has permission over the *CPFR Policies* information
 - e) It cannot be determined from the information given
 - f) I do not know

15. What would happen if the *Communicate CPFR Policies activity* cannot be performed by the Planning Analyst from the seller organization?
 - a) The execution of the remaining activities would not be affected
 - b) The *Generate Buyer Initial Sales forecast activity* would not be performed
 - c) The *Generate POS Data activity* would not be performed
 - d) The *Generate Exceptions Order Forecast activity* would not be performed
 - e) It cannot be determined from the information given
 - f) I do not know
16. Can the activity *Generate Exceptions Order Forecast* be executed before retrieving POS Data? Yes___ No___
17. Can the activity *Generate Exceptions Order Forecast* be executed before retrieving CPFR Policies? Yes___ No___
18. Can the activity *Generate Initial Sales forecast for the Buyer organization* be executed before *communicating the sales forecast activity*? Yes___ No___
19. Can the activity *Generate Exceptions Order Forecast* be executed before *generating the Order Shipment information*? Yes___ No___
20. Can the activity *Retrieve POS Data* be executed after the *retrieve initial sales forecast activity for the Seller organization*? Yes___ No___

Based on your experience, circle your level of agreement with each statement using the following scale:

1=	2	3	4	5
Strongly	Somewhat	Neutral	Somewhat	Strongly

Disagree

Disagree

Agree

Agree

	1			5	
	Strongly			Strongly	
	Disagree			Agree	
21. <i>These diagrams help me to identify the security aspects of a business process</i>	1	2	3	4	5
22. <i>These diagrams help me to understand the security aspects of a business process</i>	1	2	3	4	5
23. <i>These diagrams help me to determine what would happen with the business process when security aspects are violated</i>	1	2	3	4	5
24. <i>The security aspects depicted in the diagrams are easy to understand</i>	1	2	3	4	5
25. <i>Representations of processes using this approach are clear</i>	1	2	3	4	5
26. <i>Representations of processes using this approach provide useful security information</i>	1	2	3	4	5