Secure activity resource coordination: empirical evidence of enhanced security awareness in designing secure business processes

By: Fergle D'Aubeterre, Rahul Singh and Lakshmi Iyer

D'Auberterre, F., Singh, Rahul, & Iyer, L. (2008). Secure activity resource coordination: empirical evidence of enhanced security awareness in designing secure business processes. *European Journal of Information Systems*, 17 (5), 528-543.

Abstract:
Systems development methodologies incorporate security requirements as an afterthought in the non-functional requirements of systems. The lack of appropriate access control on information exchange among business activities can leave organizations vulnerable to information assurance threats. The gap between systems development and systems security leads to software development efforts that lack an understanding of security risks. We address the research question: how can we incorporate security as a functional requirement in the analysis and modeling of business processes? This study extends the Semantic approach to Secure Collaborative Inter-Organizational eBusiness Processes in D'Aubeterre et al. (2008). In this study, we develop the secure activity resource coordination (SARC) artifact for a real-world business process. We show how SARC can be used to create business process models characterized by the secure exchange of information within and across organizational boundaries. We present an empirical evaluation of the SARC artifact against the Enriched-Use Case (Siponen et al., 2006) and standard UML-Activity Diagram to demonstrate the utility of the proposed design method.
Keywords: secure business process; role-based access control; activity–resource coordination; security awareness; secure systems design

Article:

Introduction

Requirements specification is the most consequential phase of systems development and forms the basis for subsequent systems analysis and design (Agarwal et al., 1999). Software engineering methodologies typically incorporate security as an afterthought in the non-functional requirements of systems (Baskerville, 1988; Mouratidis et al., 2005). In summarizing existing information systems security (ISS) development approaches, Siponen (2005a, b) identifies the need for development of theoretically and empirically grounded ISS methods. Siponen et al. (2006) argue that existing secure information systems (SIS) design fails to satisfy secure systems design requirements. As a result, security is not fully integrated in all systems development phases (Lee et al., 2002; Apvrille & Pourzandi, 2005). The gap between systems development and systems security leads to software development efforts that lack an understanding of security risks (Backhouse & Dhillon, 1996; van Wyk & McGraw, 2005). IS methodology that includes security as a functional requirement in all stages of systems development is needed (Baskerville, 1988). Although Siponen et al. (2006) develop Enriched-Use Case descriptions that incorporate security policies and restrictions, Enriched-Use Case descriptions do not capture the security requirements for information exchange from a business process perspective. This research is motivated by the belief that security requirements must be considered as an integral part of the design of systems that enable secure business processes.

Organizations achieve their business goals by enacting business processes. Business processes provide the context for exchange of information resources within and across organizational boundaries (Raghu & Vinze, 2007). A business process view provides an end-to-end perspective to understand the access requirements and

exchange of information resources among business activities (Singh & Salam, 2006). The lack of appropriate security controls on information exchanged among business activities in a business process can leave organizations vulnerable to information assurance threats (D'Aubeterre et al., 2008). Research on secure access to information in distributed systems lacks an integrative business process perspective on secure information and knowledge sharing (Oh & Park, 2003). In this research, we address the research question: *how can we incorporate security as a functional requirement in the analysis and modeling of business processes*?

We use a design science approach (Hevner et al., 2004) to develop the modeling concepts and grammar for secure activity resource coordination (SARC) in business process and demonstrate its utility in generating greater awareness of security requirements for secure business processes. D'Aubeterre et al. (2008) propose a Semantic approach to Secure Collaborative Inter-Organizational eBusiness Processes (SSCIOBP) and demonstrate the utility of the artifact for secure information exchange in an organization using a case study. However, they do not provide empirical evidence to show that their approach can be used to effectively represent both coordination and security requirements in the analysis of a business process. In the following section, we develop the modeling concepts and grammar for the SARC artifact based on SSCIOBP (D'Aubeterre et al., 2008) and Singh & Salam (2006) to represent a secure business process. We illustrate the application of the SARC artifacts to a real business process that requires secure exchange of information resources within and across organizational boundaries. Situational awareness (SA) theory (Endsley, 1995) is used to empirically evaluate the utility of SARC in generating greater awareness of security requirements in the analysis of business processes. We present a detailed experimental design to compare the security awareness generated by SARC artifacts and Enriched-Use Cases (Siponen et al., 2006) and standard UML-Activity Diagrams. Our results show that SARC artifacts help analysts develop greater security awareness in requirement specifications, modeling, and analysis of business processes while maintaining informational equivalence (Larkin & Simon, 1987) with the best-known existing methods. We assert that when security requirements are incorporated as functional requirements in the analysis of business processes, analysts have greater security awareness in their analysis of the requirements of secure business processes.

SARC design artifacts provide analysts the meta-design, including design principles, modeling concepts and grammar, to guide the analysis and design of secure eBusiness processes. SARC includes security as a functional requirement in the early analysis and modeling of business processes. Security awareness generated by SARC artifacts helps analysts incorporate technical and formal security controls needed for secure business processes design. SARC design artifacts provide mechanisms to analyze non-repudiation and authorized access to resources that are useful in developing controls that ensure segregation of duty and maintain the integrity of information resources involved in business processes. In addition, SARC representations enable IS stakeholders with a common understanding of security requirements and constraints involved in a specific business process, which is a key factor for good requirements communication. As a result, analysts have greater awareness of security requirements in the design of systems that enable secure eBusiness processes. This is very important in the design of inter-organizational business processes, where the lack of security knowledge regarding access to resources hinders the development of trust between the partner organizations.

Theoretical foundations

Design science research addresses classes of relevant and unsolved problems, or solves problems in a more effective and efficient manner (Hevner et al., 2004). Owing to the novelty of many design-research problems, an optimal solution may not always be possible leaving a satisficing (Simon, 1996) solution acceptable (Hevner et al., 2004). Design theory is a prescriptive theory that integrates normative and descriptive kernel theories into design paths to produce the design artifact (Walls et al., 1992). The following sections present a review of the literature in secure systems design and develop the modeling concepts and grammar in SARC. We also illustrate the application of SARC to a complex inter-organizational business process.

SIS design

Knowledge resources must be shared to be useful for business processes (Oh & Park, 2003; Raghu & Vinze, 2007). However, organizations are selective about the nature of knowledge resources shared (Loebecke et al.,

1999). 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. Dhillon & Backhouse (2001) analyze IS security research and 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 toward 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 SIS. Holistic IS methodology that includes security aspects in all of its stages is still needed (Baskerville, 1988) to provide appropriate security controls on information exchange in business processes.

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 IS analysis and design methodology' (p. 88). 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 (Siponen et al., 2006), but fails to show how these requirements can be incorporated in the design of secure business processes. We introduce security constraints that incorporate access control mechanisms in the early conceptualization of business processes to model the secure exchange of information resources in coordinated business processes.

An organization may incur significant costs without appropriate and timely authorization access to information resources when performing business activities. Local security and access control (SAC) policies are not designed for distributed resource sharing, while global SAC policies do not consider impediments to access and control of locally owned resources (Sandhu et al., 1996). Centralized SAC mechanisms fail to capture the distributed nature of systems support required for eBusiness processes in an extended enterprise. There is paucity in the research on security of distributed eBusiness processes that provide a holistic, business process perspective to secure information and knowledge sharing (Oh & Park, 2003). This research provides guidance on how to fill this gap through secure eBusiness process using role-based access control (RBAC) mechanisms.

The National Institute of Standards and Technology adopted RBAC as a National standard in 2004 (csrc.nist.gov/rbac/). RBAC uses roles as a layer of abstraction to decouple the association between users and permission to resources (Sandhu et al., 1996). Access control policies specify user permissions to resources through relationships between users, roles and permissions where organizational role hierarchies reflect organizational hierarchies of responsibility. Roles describe the computational and organizational authority and responsibilities of users assigned to a role. Roles separate the responsibilities of individuals in the organization with respect to their duties and thereby capture the separation of duty needed to preserve segregation of duty principles. They provide non-repudiation mechanisms through auditable activities for users who fulfill these roles. The security literature is rich in mechanisms and extensions of RBAC (Sandhu et al., 1996); however, RBAC does not incorporate information exchange in the context of the business process. Basu & Kumar (2002) note that current workflow systems that enable business processes must allow the representation of rules and policies and ensure that security policies are not breached. We use RBAC as the access control mechanism for the SARC conceptualization in secure business processes.

Recently Siponen et al. (2006) proposed a meta-notation framework to represent and analyze ISS requirements. They extend UML Use Case descriptions to incorporate security requirements into the design phase. They use field study and action research to validate their proposed framework. Enriched-Use Case incorporates security constraints, security subjects, and security actors into the design of IS. However, Enriched-Use Cases do not consider the security requirements and dynamics of access control in a business process. This research identifies security requirements in the requirement specification stage, but does not show the translation of these requirements in the design of secure eBusiness processes. Attempts to incorporate security as a functional requirement in the early stages of requirement specification and analysis have utility in the design of secure business processes.

SARC conceptualization of business processes

Business processes require coordination mechanisms to manage the inter-dependencies of their constituent activities (Malone, 1987). Coordination theory explains activity coordination in business processes. Actors, activities, and resources are identified, and processes are decomposed into activities so that dependencies among activities and resources can be identified and analyzed. Crowston & Osborn (2003) show how coordination theory can be used to develop process descriptions and process redesign through identification and analysis involving *setting process boundaries, collecting data, identifying actors and resources, identifying activities, identifying dependencies, and verifying a model*. We use a simplified view of *activity–resource dependency* where activity dependencies exist as a sharing, flow or fit dependency with another activity through a resource (Singh & Salam, 2006). In this research, we are concerned with information resources only. *Dependencies do not exist directly between activities*. While an activity may consume or produce a resource, it cannot produce or consume another activity (Malone et al., 2003; van der Aalst & Kumar, 2003).

An organization's business processes comprise value activities that create customer value (Porter, 1985). Access control policies define permissions for activities' access to resources. We view security as a functional requirement in the analysis and modeling of the activities in a business process. This view allows us to focus on secure interdependencies and coordination requirements of activities and resources. The SARC conceptualization used in this paper is consistent with RBAC (Sandhu et al., 1996), coordination theory (Malone et al., 2003), and the view of business process in Singh & Salam (2006), Oh & Park (2003), Raghu & Vinze (2007), and the view of Secure Collaborative Inter-Organizational eBusiness Processes in D'Aubeterre et al. (2008).

The following rules, based on SSCIOBP (D'Aubeterre et al., 2008), represent the modeling concepts and grammar for SARC secure business processes:

1. Actors fulfill organizational roles.

2. Organizational roles are authorized to perform business activities.

3. Business activities are permitted to read, write, delete, or create information resources.

4. Dependencies do not exist directly between business activities. Business activities cannot directly produce or consume another business activity.

5. Business activities have a sharing, fit or flow coordination dependency with an information resource.

These rules are represented in the schematic shown in Figure 1.

An illustrative application of SARC

A design artifact must be evaluated to demonstrate its utility, quality, and efficacy. Hevner et al. (2004) state that evaluation methods available in the knowledge base may be used to rigorously evaluate a design artifact. They suggest that the nature of the problem, characteristics of the artifact, and available resources should drive the selection of the evaluation method. The goal of evaluation is to establish that the design artifact fulfills the requirements and constraints of the problem domain and therefore it is complete and effective. We want to establish the utility of SARC in generating security awareness for analysts as they develop the security requirements of complex business processes.

SARC was applied to SupplyCo's (a fortune 100 organization in the apparel industry – name altered to preserve anonymity) create order forecast business process to illustrate its application in modeling and analyzing access control and coordination aspects of core business processes of organizations (D'Aubeterre et al., 2008). Key organizational roles and functions in the Create Order Forecast business process were identified through multi-

ple interviews with SupplyCo's management to develop the role–activity–resource permissions shown in Table 1 (D'Aubeterre et al., 2008).

We applied SARC modeling concepts and grammar to develop the SARC representation, Figure 2, for the create order forecast business process.

These SARC representations were discussed with the main stakeholders directly responsible for systems support for demand forecasting, capacity planning, and customer development at *SupplyCo*. These indicated the utility of the approach to secure the demand forecasting business process for the *SupplyCo*. Specifically, SARC business process representations are useful for analyzing and modeling security and coordination aspects of business processes to an organization (D'Aubeterre et al., 2008). However, D'Aubeterre et al. (2008) do not examine the utility of SARC artifacts in generating security awareness in business and systems analysts, leading to development of models of secure business processes. Baskerville et al. (2007) suggest a combination of 'hard methods,' such as experiments, and 'soft methods,' such as case studies, be used for a comprehensive evaluation and to avoid errors during the evaluation processes. The following section presents a rigorous experimental evaluation of the utility of SARC artifacts in generating security awareness in the analysis of business processes.

Experimental evaluation

Evaluating design artifacts using an experiment empirically demonstrate the qualities of the artifact (Hevner et al., 2004) and provides a basis for the generalizability of 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. Our experimental evaluation assesses how business process models developed using SARC generates higher awareness of security constraints in modeling the secure exchange of information resources in coordinated business processes.

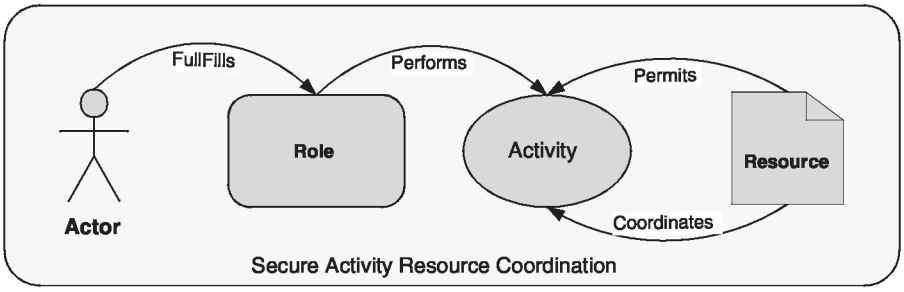

Figure 1 Secure activity resource coordination.

Research model

We use SA theory (Endsley, 1995) to measure business and systems analysts' awareness of security policies and constraints generated by using the SARC conceptualization of a secure business process. 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) defines SA as the ability to perceive the status, attributes, and dynamics of relevant elements in the environment. SA includes the ability to project the future actions of the elements in the environment within temporal constraints of the problem domain achieved through knowledge and comprehension of the situation. We extend SA theory to define security awareness, which assesses the comprehension of security policies and constraints in the analysis of security requirements for business processes. Specifically, we assess the security awareness generated by the SARC conceptualization of a secure business process against existing best-known methods: Enriched-Use Cases (Siponen et al., 2006) to capture the security requirements, and UML-Activity Diagrams to capture the dynamic coordination of activities in a business process. Figure 3 presents the research model for the experimental evaluation of SARC.

Table 1 RBAC for role–activity–resource permissions for create order forecast business process (adopted from D'Aubeterre *et al.*, 2008)

Actor	*Role*	*Business activity*	*Permission type (write, read, create, delete)*	*Resource*
Buyer planning actor	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 actor	Replenishment role	Communicate inventory strategy	Read	Inventory strategy
		Communicate sales forecast	Read	Sales forecast
		Communicate exception resolution	Read	Exception resolution data
Seller planning actor	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 and shipment data
			Create/write/read	Order forecast
Seller forecast actor	Demand forecast role	Communicate historical demand and shipment	Read	Historical demand and shipment data
		Communicate order shipment data	Read	Order shipment data
Seller replenishment actor	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

Hypotheses

According to Larkin & 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.' SARC and Enriched-Use Case and UMLActivity Diagrams provide two different representations for the same business process. It is important to demonstrate that SARC design artifacts are at least informationally equivalent to Enriched-Use Case and UML-Activity Diagrams in capturing the dynamics of business processes. We test that the two approaches are informationally equivalent (Larkin & Simon, 1987) by comparing the inferences that analysts make about the business process represented using the two approaches. This demonstrates that SARC does not create information loss in representing business processes and establishes a pareto efficient basis for further testing the utility of SARC. Thus, our first hypothesis is as follows:

H1 *A business process model developed using SARC artifacts is informationally equivalent to a business process model developed using Enriched-Use Case and standard UMLActivity Diagrams.*

Business processes represented using the SARC artifact must generate greater awareness of the security requirements of the business processes. We hypothesize that:

H2 *A business process model developed using SARC artifacts creates a higher level of security awareness than a business process model developed using Enriched-Use Cases and standard UML -Activity Diagrams.*

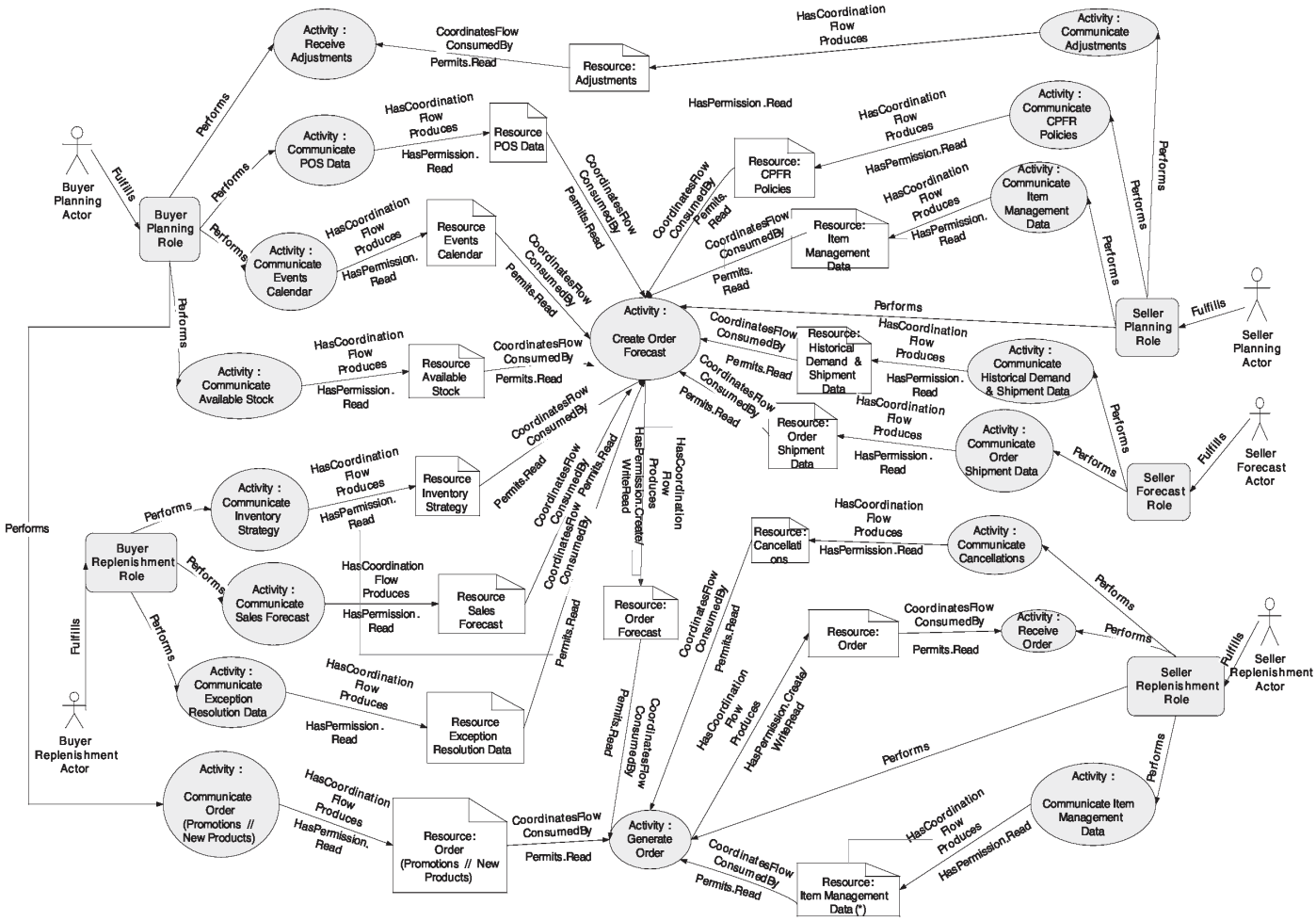

Figure 2 *SARC Diagram* for the *Generate Create Order Forecast* business process (adopted from D'Aubeterre *et al.*, 2008).

Individuals' characteristics influence the perception and interpretation of reality. Individuals' characteristics, such as professional experience and organizational roles, influence the selection and use of modeling tools (Hadar & Soffer, 2006). Allen & March (2006) explain that user's characteristics influence the interaction between comfort level with reading Entity Relationship diagrams and treatment predictions. We test the effect of previous knowledge about business process analysis on individuals' security awareness. Specifically, we test if users with experience in business process analysis develop a higher level of security awareness using SARC that those without experience. This is tested in H3 as follows:

H3 *A business process model developed using SARC artifacts creates a higher level of security awareness than a business process model developed using Enriched-Use Cases and standard UML -Activity Diagrams for users with experience in business process analysis.*

Experimental design

We use an experimental design with repeated measures and a counter-balanced design to evaluate the utility of SARC. Repeated measures designs have high statistical power due to the positive correlation between treatments (Keren, 1993). Under repeated measures designs, subjects act as their own control and the confounding effects due to different subjects' background are minimized. Repeated-measures designs require fewer subjects compared to between-subject designs with similar statistical power level (Brooks, 1980). However, repeated-measured designs are prone to a carry-over or learning effect (Greenwald, 1976), where

subsequent treatment effects are confounded with previous ones. We address this using a counter-balanced repeated-measures design to spread unwanted variance arising due practice or sequence interactions among different treatments (Laitenberger et al., 2001). Table 2 presents our experimental design.

We empirically compare the utility of the two treatments in generating security awareness. The create order forecast business process model developed with the help of demand and forecast analysts from SupplyCo (Table 1 and Figure 2) was simplified for readability and used as the scenario for both treatments. This business process requires the secure and coordinated exchange of information and knowledge across business partners. Appendix A shows the Enriched-Use Case and Activity Diagram (Treatment 1) and SARC (Treatment 2) used for the experiment. Subjects were randomly assigned to two groups and given treatments using the experimental design presented in Table 2.

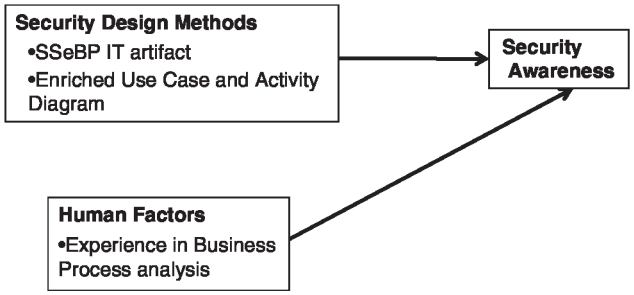

Figure 3 Research model to test security awareness generated by process modeling methods.

Data collection

Our sample comprised business students enrolled in IS analysis and design courses. Previous studies of conceptual modeling approaches (Bolloju & Leung, 2006), software inspections (Porter et al., 1994), and systems modeling tools (Agarwal & Sinha, 2003; Danesh & Kock, 2005; Jeyaraj & Sauter, 2007) have used IS students as subjects. This selection is supported by the fact that IS students would become systems analysts or business analysts responsible for the analysis and design of IS in organizations. Therefore, IS students capture the characteristics of the IS and business analysts' population. For this study, the subjects were undergraduate and graduate IS students enrolled in business process information technology, IS analysis and design, and advanced IS courses.

Table 2 Experimental design

Group 1	Enriched-Use Case and Activity Diagram (Treatment 1)	*Observation*	Secure activity resource coordination (SARC) (Treatment 2)	*Observation*
Group 2	Secure activity resource coordination (SARC) (Treatment 2)	*Observation*	Enriched-Use Case and Activity Diagram (Treatment 1)	*Observation*

Participation in the study was voluntary. We conducted a pilot study using doctoral students in IS. The pilot study revealed that it took at least 30 min to complete the study for doctoral students. In addition, some questions were edited for readability and clarity. While there was no time limit for completing the questions of the experiment, the subjects were not expected to complete the questions in less than 30 min. We used a 30 min cut-off to determine whether or not the subjects answered the questions conscientiously. Subjects completed a questionnaire on demographics and their experience using systems analysis and design methods, UML modeling techniques, business process modeling, and analyzing information security requirements. The stimulus material in the experiment comprised the create order forecast business process represented as Enriched-Use Case combined with UML-Activity Diagram and SARC 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.

Subjects answered 15 questions aimed at identifying elements of security in the business models presented to them including authorization constraints, security policies, and security violations. The following is an example question to assess security awareness:

Who has permission to perform the Communicate Inventory Strategy activity?

1. Buyer Planning Analyst
2. Buyer Replenishment Analyst
3. Seller Planning Analyst
4. Seller Forecasting Analyst
5. All
6. None
7. It cannot be determined from the information given
8. I do not know

To test the level of business process coordination and the information equivalence of the two approaches, we used five questions where subjects were asked to identify elements of workflows such as predecessor and successor activities needed to complete the business process. The following is an example of questions used to assess business process coordination:

> Can the activity Generate Exceptions Order Forecast be executed before retrieving CPFR Policies? Yes___ No___

All subjects were exposed to both treatments in keeping with the principles of the counter-balanced repeated-measures experimental design. Subjects were randomly assigned to one of two groups. Each group received both treatments in different order. Subjects were asked the same questions related to security awareness and business process coordination. Subjects in our study did not receive any kind of feedback on their performance. This alleviates problems related to the learning effect (Basili et al., 1998, Laitenberger et al., 2001). In addition, given the effect that time constrains could have over the subject's performance (Payne et al., 1980; Benbasat & Dexter, 1986; McDaniel, 1990), we did not impose any time limit to finishing the experiment. Data we collected were coded as correct or incorrect using an answer key using MS Excel. The few missing values in the raw data were treated as wrong answers. The experiment was conducted in Fall 2007 and Spring 2008 in two public universities. A total of 84 usable responses were obtained from a possible 154 respondents. All statistical analysis in this study was conducted using SAS version 9.1 running in a Windows environment.

Data analysis

The sample of 84 responses was analyzed based on gender, age, education level, and primary occupation. Tables 3–5 provide demographic information about the sample.

Table 5 shows that there is an even representation of undergraduate and graduate students in our sample. Table 6 shows that our sample comprised an even representation of full time students and professionals. In addition, the sample was analyzed to determine the subjects' level of experience using System Development Methodologies (SDM). Table 7 shows the distribution of the level of experience using SDM.

Table 3 Gender distribution

	Frequency	Percent
Female	35	41.67
Male	49	58.33

Table 4 Age 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 years	1	1.19

Table 5 Educational level distribution

	Frequency	Percent
High school	0	0
Some years of college	44	52.38
Bachelor's degree	29	34.52
Master's degree	10	11.90
Doctorate degree	1	1.19

Table 6 Primary occupation distribution

	Frequency	Percen
Full-time employee	18	21.43
Part-time employee	17	20.24
Self-employed	4	4.76
Full-time student	45	53.57

Table 7 Level of experience using system development methodologies (SDM)

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

The carry-over effect, also known as residual or learning effect, is the effect of the treatment from the previous time period on the response from the current time period. It occurs when the effect of a treatment given in the first time period persists in the second period and distorts the effect of the second treatment. If the preliminary test for carry-over is not significant, the data from both periods can be analyzed in the usual manner (Grizzle, 1965). We followed Grizzle's (1965) procedure to test for carry-over effect and conducted an ordinary least squares analysis of variance test with a standard α level of 0.05 to determine the carry-over effect for security awareness and business process coordination. For security awareness, we failed to detect a carry-over effect (P-value = 0.0508) for the different sequences of treatment. This shows that the order in which the treatments are applied does not have an effect on the observed results for the security awareness items. In other words, the sequence of the various treatments (i.e., Enriched-Use Case → SARC; SARC → Enriched-Use Case) did not influence the results of the study. For business process coordination questions, we failed to detect a carry-over effect (P-value = 0.4124) for the different sequence of treatments. This shows that the order of application of treatments does not have an effect over the observed results for the business process coordination items.

Hypotheses testing

To test our hypotheses, we need to determine whether the difference in means between the groups is significantly different. A paired t-test is suitable to test mean differences between two groups for repeated measures (Westgard & Hunt, 1973). In addition, t-test statistic is robust against violations of normality and homogeneity of data (Aron & Aron, 1994). We test our hypotheses using a paired t-test. Since there are no previous studies that compare SARC 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 that use power levels higher than 0.8 have a high probability of rejecting the null hypotheses if they are false (Cohen, 1988). It is an accepted practice to set an α level of 0.05 to test the hypotheses (Fisher, 1948). We adopt a power level of 0.80 and an α level of 0.05 to test our hypotheses.

H1 *A business process model developed using SARC artifacts is informationally equivalent to a business process model developed using Enriched-Use Case and standard UMLActivity Diagrams.*

For H1, we empirically compared the mean of the business process coordination's questions for each treatment. Using a paired t-test, H1 was supported with a P-value ≤ 0.001 and an observed power of 0.999.

H2 *A business process model developed using SARC artifacts creates a higher level of security awareness than a business process model developed using Enriched-Use Cases and standard UML-Activity Diagrams.*

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

H3 *A business process model developed using SARC artifacts creates a higher level of security awareness than a business process model developed using Enriched-Use Cases and standard UML-Activity Diagrams for users with experience in business process analysis*.

For H3, we empirically compared the mean of the 15 security awareness questions for each treatment for subjects with experience using SDM. Using a paired t-test, the data supported H3 with a P-value ≤ 0.001 and an observed power of 0.999. This demonstrates that subjects in our sample with experience in business process analysis demonstrated greater security awareness using the SARC artifact than with the Enriched-Use Case and UML-Activity Diagram. Table 8 summarizes the hypotheses testing results.

Discussion

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). However, existing business process modeling methods lack detailed access control mechanisms on information exchange among business activities in a business process. This can leave organizations vulnerable to information assurance threats. The SARC artifacts presented here provide the modeling semantics and grammar to analyze and represent a secure business process.

Table 8 Hypotheses test summary

Hypothesis	*P-value; Observed power*	*Supported/not supported*
H1: *Business process models developed using SARC artifacts are informationally equivalent to business process model developed using Enriched-Use Case and standard UML-Activity Diagrams*	*P*-value $\leqslant 0.001$; observed power $= 0.999$	*Supported*
H2: *Business process models developed using SARC artifacts creates a higher level of security awareness than a business process model developed using Enriched-Use Case and Activity Diagram*	*P*-value $\leqslant 0.001$; observed power $= 0.999$	*Supported*
H3: *Business process models developed using SARC artifacts create a higher level of security awareness than a business process model developed using an Enriched-Use Case and Activity Diagram in users with experience in business process analysis*	*P*-value $\leqslant 0.001$; observed power $= 0.999$	*Supported*

H1 demonstrates that SARC design artifacts are informationally equivalent to Enriched-Use Case and UML-Activity Diagrams. Thus, we affirm that a business process represented using SARC conveys at least the same level of information as a business process represented using UML models. This establishes that there is no information loss by using SARC over extant methods.

H2 affirms that business process models developed using SARC generates a greater level of security awareness than those developed using Enriched-Use Case and UML-Activity Diagrams. This implies that when security requirements are incorporated as functional requirements in the analysis of business processes, individuals

become more aware of security requirements and constraints. Moreover, the SARC design artifacts provide the management and analysts a snapshot of the different actors, roles, and resources involved in the execution of a specific business processes. In the design artifacts, roles specify organizational functions responsible for particular activities that allow management to analyze and define the relationships between organizational roles and activities 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 that allows for the inclusion of non-repudiation mechanisms into the analysis and design of eBusiness processes. Non-repudiation mechanisms lay the foundations for auditing, needed for compliance with regulations such as Sarbanes–Oxley and Health Insurance Portability and Accountability Act.

Finally, H3 empirically establishes that business process models developed using SARC generate a greater level of security awareness than those developed using Enriched-Use Case and UML-Activity Diagrams in subjects that have experience in business process analysis. This finding is compelling, as it points out to the deficiencies in the modeling methods we compared to in capturing security requirements of 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.

Conclusions

In this study, we developed the modeling concepts and grammar for the SARC artifact to represent a secure business process. SARC can be used by business analysts to analyze and model secure business processes. SARC integrates streams of research in design science, eBusiness process, authorization and RBAC, coordination theory, and SIS methods. A business process provides the context for information and knowledge sharing within and across organizational boundaries. SARC provides practitioners with the meta-design and relevant examples that can be used to design secure business processes.

Even though we follow a counter-balanced experimental design to minimize the carry-over effects, it is still possible that the learning effect might affect the results. To overcome this negative effect, as part of our future research, we plan to apply a more robust experimental design. In our future work, we are interested in testing the effect of tasks characteristics in the security awareness generated using the SARC artifact. For example, does complexity of the task play a role on the efficacy of the SARC artifact in creating security awareness? In addition, we are interested in studying the discriminatory efficacy of the SARC artifact in helping users identify specific information assurance characteristics such as non-repudiation and segregation of duties.

SARC’s experimental evaluation demonstrates that SARC design artifacts can be used to represent a method to effectively incorporate security requirements in the conceptualization of business processes, which in turn leads to a better understating and awareness of how to incorporate security as a functional requirement in the modeling, analysis, and design of IS that enable secure business processes within and across organizations.

Appendix A

The following Enriched-Use Case and Activity Diagrams correspond to the business process of 'create order forecast' (see Tables A1 and A2 and Figures A1 and A2).

Table A1 Enriched use case (adopted from Siponen *et al.*, 2006)

Use Case:	*Create Order Forecast*
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:	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) 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) 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)
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: The buyer generates and consolidates its point of sales (POS data) The buyer generates the initial sales forecast The seller retrieves the buyer's POS data, available stock, events calendars, and historical order shipment data The seller generates an initial sales forecast The buyer sends its inventory strategy The seller sends the order shipment data and retrieve CFPR policies and item management data The collaborative system generates the exceptions resolution data 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

Table A2 Role–activity–resource permissions table

Actor	*Role*	*Business activity*	*Permission type*	*Resource*
Buyer planning actor	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 actor	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 actor	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 actor	Seller planning role	Retrieve available stock	Read	Available stock
		Retrieve events calendar	Read	Events calendar

Table A2 Continued

Actor	*Role*	*Business activity*	*Permission type*	*Resource*
		Communicate historical demand and shipment data	Read	Historical demand and shipment data
		Communicate order shipment	Read	Order shipment
		Communicate CPFR policies	Read	CPFR policies
		Communicate item management data	Read	Item management data
		Generate new 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

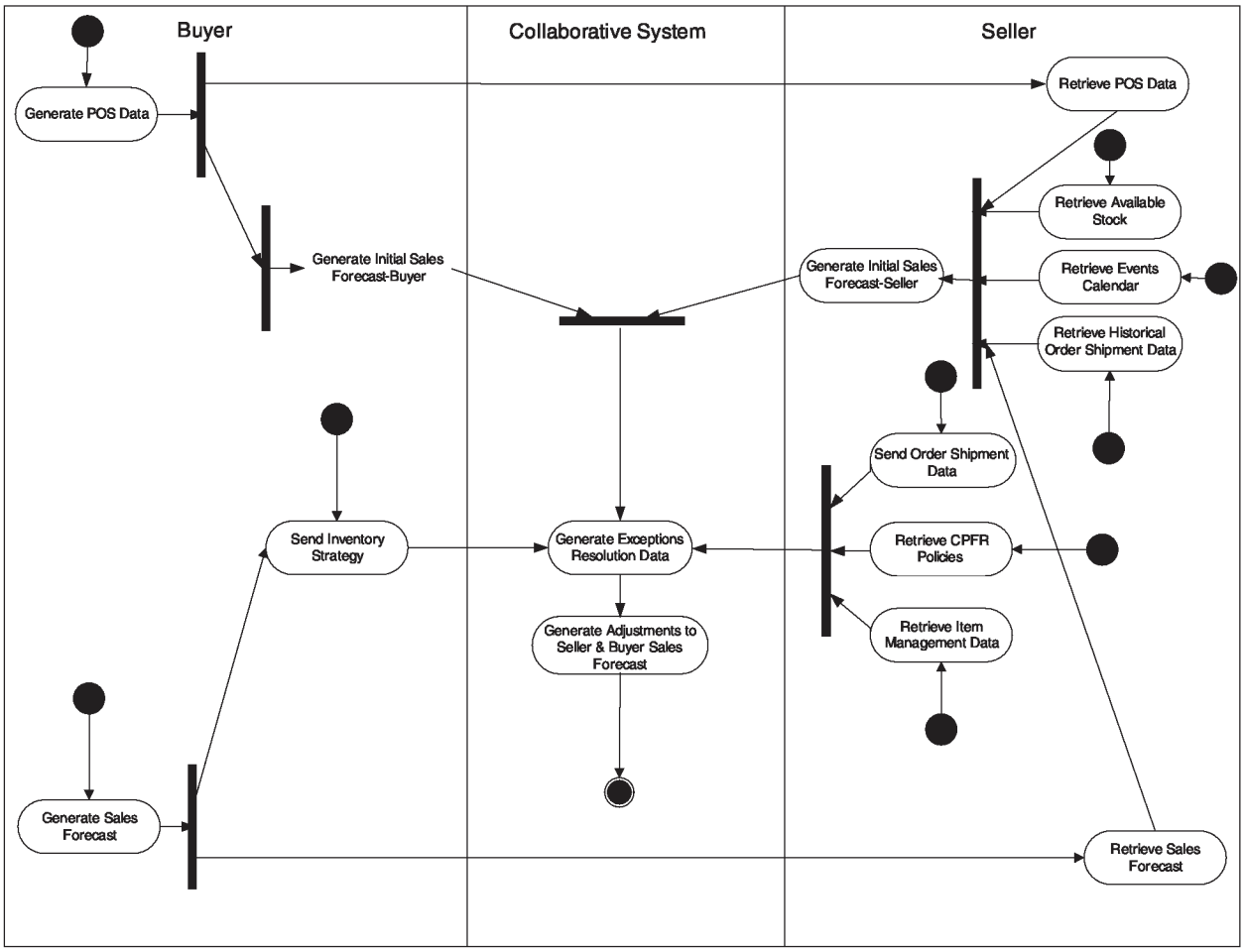

Figure A1 Activity Diagram.

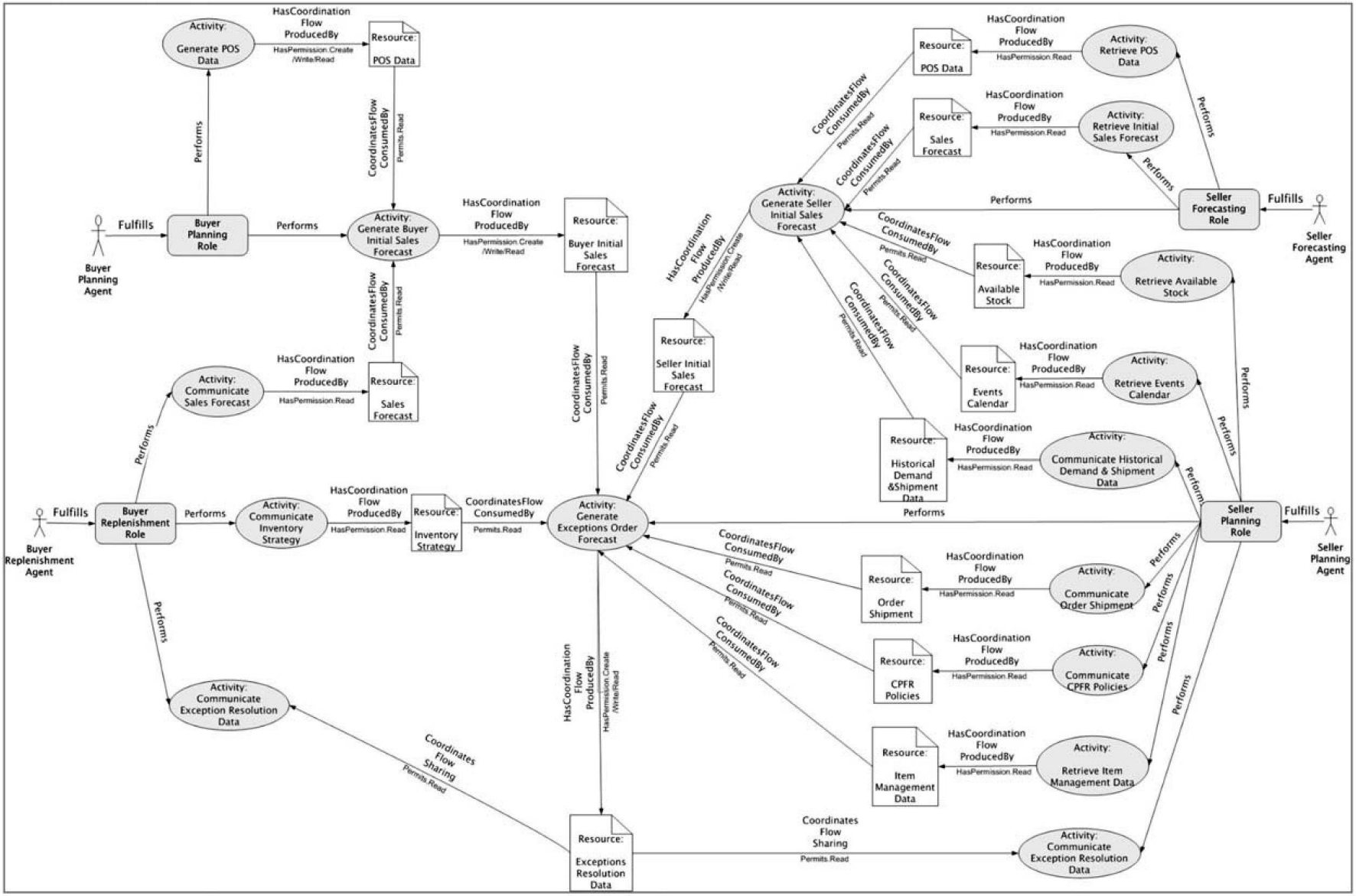

Figure A2 Secure activity resource coordination diagram.

References

AGARWAL R, DE P and SINHAA (1999) Comprehending object and process models: an empirical study. IEEE Transactions on Software Engineering 25(4), 541–556.

AGARWAL R and SINHA AP (2003) Object-oriented modeling with UML: a study of developers' perceptions. Communications of the ACM (CACM) 46(9), 248–256.

ALLEN G and MARCH S (2006) The effects of state-based data representation on user performance in query formulation tasks. MIS Quarterly 30(2), 269–290.

APVRILLE A and POURZANDI M (2005) Secure software development by example. IEEE Security and Privacy 3(4), 10–17.

ARON A and ARON E (1994) Statistics for Psychology, 1 st edn, Prentice-Hall, New Jersey.

BACKHOUSE J and DHILLON G (1996) Structures of responsibility and security of information systems. European Journal of Information Systems 5(1), 2.

BASILI V, SHULL F and LANUBILE F (1998) Using experiments to build body of knowledge. Technical Report, University of Maryland, CS-TR-3983.

BASKERVILLE R (1988) Designing Information Systems Security. John Wiley & Sons, New York.

BASKERVILLE R, PRIES-HEJE J and VENABLE J (2007) Soft design research: extending the boundaries of evaluation in design research. Proceedings of the 2nd DESRIST Conference, 13–15 May 2007, Pasadena, CA, pp 19–38.

BASU A and KUMAR A (2002) Research commentary: workflow and management issues in e-business. Information Systems Research 13(1), 1–14.

BENBASAT I and DEXTER AS (1986) An experimental investigation of the effectiveness of graphical and color enhanced information presentation under varying time constraints. MIS Quarterly 10(1), 59–83.

BOLLOJU N and LEUNG SK (2006) Assisting novice analysts in developing quality conceptual models with UML. Communications of the ACM 49(7), 108–112.

BROOKS R (1980) Studying programmer behavior experimentally: the problems of proper methodology. Communications of ACM 23(4), 207–213.

COHEN J (1988) Statistical Power Analysis for the Behavioral Sciences, 2nd edn, Lawrence Erlbaum Associate Publishers, New Jersey.

CROWSTON K and OSBORN C (2003) The interdisciplinary study of coordination. In Organizing Business Knowledge: The MIT Process Handbook (MALONE TW, CROWSTON K and HERMAN GA, Eds), MIT Press, Cambridge, MA.

DANESH A and KOCK N (2005) An experimental study of process representation approaches and their impact on perceived modeling quality and redesign success. Business Process Management Journal 11(6), 724–735.

D'AUBETERRE F, SINGH R and IYER LS (2008) A semantic approach to secure collaborative inter-organizational eBusiness processes (SSCIOBP). Journal of the Association for Information Systems 9(3/4), 233–269.

DHILLON G and BACKHOUSE J (2001) Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal 11(2), 127–153.

ENDSLEY MR (1995) Toward a theory of situational awareness in dynamic systems. Human Factors 37(1), 32–64.

FISHER R (1948) Combining independent tests of significance. The American Statistician 2(5), 30–31.

GLASSEY O (2008) A case study on process modeling – three questions and three techniques. Decision Support Systems 44(4), 842–853.

GREENWALD A (1976) Within-subjects designs: to use or not to use? Psychological Bulletin 83(2), 314–320.

GRIZZLE JE (1965) The two-period change over design and its use in clinical trials. Biometrics 21, 461–480.

HADAR I and SOFFER P (2006) Variations in conceptual modeling: classification and ontological analysis. Journal of the Association for Information Systems 7(8), 568–592.

HEVNER A, MARCH ST, PARK J and RAM S (2004) Design science research in information systems. MIS Quarterly 28(1), 75–105.

JEYARAJ A and SAUTER VL (2007) An empirical investigation of the effectiveness of systems modeling and verification tools. Communications of ACM 50(6), 62–67.

KEREN G (1993) A Handbook for Data Analysis in the Behavioural Sciences – Methodological Issues, Chapter 19: Between- or Within-Subjects Design: A Methodological Dilemma, Lawrence Erlbaum Associates, New Jersey, Hove & London.
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), 387–421.
LARKIN JH and SIMON HA (1987) Why a diagram is (sometimes) worth ten thousand words. Cognitive Science 11(1), 65–99.
LEE Y, LEE J and LEE Z (2002) Integrating software lifecycle process standards with security engineering. Computer and Security 21(4), 345–355.
LOEBECKE C, VAN FENEMA P and POWELL P (1999) Co-opetition and knowledge transfer. Database for Advances in Information Systems 30(2), 14–25.
MALONE TW (1987) Modeling coordination in organizations and markets. Management Science 33, 1317–1332.
MALONE TW, CROWSTON K and HERMAN GA (Eds) (2003) Organizing Business Knowledge: The MIT Process Handbook. MIT Press, Cambridge, MA. MCDANIEL LS (1990) The effects of time pressure and audit program structure on audit performance. Journal of Accounting Research 28(2), 267–285.
MOURATIDIS H, GIORGINI P and MANSON G (2005) When security meets software engineering: a case of modelling secure information systems. Information Systems 30(8), 609–629.
OH S and PARK S (2003) Task-role-based access control model. Information Systems 28(6), 533–562.
PAYNE JW, LAUGHHUNN DJ and CRUM R (1980) Translation of gambles and aspiration level effects in risky choice behavior. Management Science 26(10), 1039–1060.
PORTER ME and MILLAR VE (1985) How information gives you Competitive Advantage. Harvard Business Review 63(4), 140–160.
PORTER AA, VOTTA LG and BASILI VR (1994) Comparing detection methods for software requirement inspections: a replicated experiment. IEEE Transactions on Software Engineering 21, 563–575.
RAGHU TS and VINZE A (2007) A business process context for knowledge management. Decision Support System 43(3), 1062–1079.
RAGHU TS and VINZE A (2007) A business process context for knowledge management. Decision Support System 43(3), 1062–1079.
SANDHU RS, COYNE EJ, FEINSTEIN HL and YOUMAN CE (1996) Role-based access control models. IEEE Computer 29(2), 38–47.
SIMON HA (1996) The Sciences of the Artificial, 3rd edn, MIT Press, Cambridge, MA.
SINGH R and SALAM AF (2006) Semantic information assurance for secure distributed knowledge management: a business process perspective. IEEE Transactions on Systems, Man and Cybernetics 36(3), 472–486.
SIPONEN MT (2005a) An analysis of the traditional IS security approaches: implications for research and practice. European Journal of Information Systems 14(3), 303–315.
SIPONEN MT (2005b) Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. Information and Organization 15, 339–375.
SIPONEN MT, BASKERVILLE R and HEIKKA J (2006) A design theory for secure information systems design methods. Journal of the Association for Information Systems 7(8), 568–592.
VAN DER AALST WMP and KUMAR A (2003) XML based schema definition for support of inter-organizational workflow. Information Systems Research 14(1), 23–46.
VAN WYK K and MCGRAW G (2005) Bridging the gap between software development and information security. IEEE Security & Privacy 3(5), 75–79.
WALLS JG, WIDMEYER GR and EL SAWY OA (1992) Building an information system design theory for vigilant EIS. Information Systems Research 1(3), 36–59.
WESTGARD JO and HUNT MR (1973) Use and interpretation of common statistical tests in method comparison studies. Clinical Chemistry 19, 49–57.