The Emerald Research Register for this journal is available at
www.emeraldinsight.com/researchregister

The current issue and full text archive of this journal is available at
www.emeraldinsight.com/1463-7154.htm

Modelling the regulative role of business processes with use and misuse cases

Gil Regev
School of Computer and Communication Sciences, Ecole Polytechnique Fédérale de Lausanne, Lausanne, Switzerland
Ian F. Alexander
Scenario Plus Ltd, London, UK, and
Alain Wegmann
School of Computer and Communication Sciences, Ecole Polytechnique Fédérale de Lausanne, Lausanne, Switzerland

Abstract

Purpose – The purpose of this paper is to provide a framework for understanding value-added and abuse prevention activities in business processes.

Design/methodology/approach – The paper considers business processes as a regulation mechanism that an organization uses to survive and flourish in its environment. It proposes a theoretical framework based on the concept of homeostasis, the maintenance of identity in a changing world. In this framework the paper classifies business processes into three levels (strategic, operational, regulative) and analyse the relationships between these three levels. Based on this framework, the paper extends the "Use and Misuse Cases" technique to support modelling of value-added and abuse prevention activities.

Findings – The main finding is the importance of considering business processes as regulation mechanisms. Traditionally, business processes are analysed through the goals they are designed to achieve. This paper analyses what the organization aims at maintaining. This makes it possible to explicitly model the potential abuses (threats) to business processes and their associated corrective measures (regulative processes).

Practical implications – Use of this framework enables process designers to explicitly model abuse prevention activities, even though they are traditionally considered as not participating in customer value creation. This should lead to better-fitting business processes.

Originality/value – The framework is useful because it provides a theoretical justification for the value creation and abuse prevention activities that can be found in business processes. The three levels that we use to analyse business processes (strategic, operational and regulative) constitute an innovation in business process modelling where only two levels (strategic and operational) have been considered thus far. Few, if any, business process theoretical frameworks provide this kind of rationale for abuse prevention activities.

Keywords Organizational processes, Modelling, Systems theory

Paper type Research paper

Introduction

An organization's business processes are sets of activities that create value for a customer (Hammer and Champy, 1993). However, not all business activities directly participate in this creation of value. As stated by Hammer and Champy, business

Business Process Management Journal
Vol. 11 No. 6, 2005
pp. 695-708

1463-7154
DOI 10.1108/14637150510630864

processes also contain activities designed to prevent abuse; many business processes contain too much abuse prevention, whose cost may surpass the cost of abuse.

Thus, to define a complete business process, an organization needs to understand what value it wants to provide to its customers, what potential abuses it may face, and what actions it can take to protect itself.

Standard process modelling techniques model the activities in a process, without differentiating between those that create value and those that prevent abuse. Moreover, they do not model potential abuse explicitly. As a result, these modelling techniques do not include the rationale for abuse prevention. This missing rationale may result in either inflexibility during redesign or ignoring essential abuse prevention activities.

In this paper, we present an innovative theoretical framework based on general systems thinking (GST) and cybernetics. The framework explains business processes as a mechanism through which an organization regulates its relationships with its stakeholders. This framework provides the necessary background for modelling business processes with a technique that models value creation and abuse prevention activities with use cases, and potential abuses with misuse cases. This technique is inherited from requirements engineering (RE). It helps in the design or redesign of business processes by making value creation, abuses and countermeasures explicit.

The larger context of this work is the modelling of the rationale of business processes, the so-called "why question". Several goal-directed techniques have been defined in RE as solutions to this question (Yu and Mylopoulos, 1994; Anton, 1997; van Lamsweerde, 2001). Related techniques exist in the systems sciences movement (Checkland and Scholes, 1990; Forrester, 1971) and in information systems (Coakes *et al.*, 2000; Liu *et al.*, 2002). Our background in GST and RE leads us to propose a lightweight, graphical technique that throws light on value creation, abuse and counter-abuse measures. It is useful in the early stages of a project and for discussion with non-technical stakeholders; it is not designed for detailed business process description. However, it provides a rationale for value creation and abuse prevention activities which can be revisited to reassess the adequacy of the business process model.

This paper is structured in the following way. In the second section, we briefly explain the role of business processes in the regulation of the relationships between an organization and its stakeholders. We then explain our theoretical framework for understanding business processes and for modelling them with use and misuse cases. In the third section, we explain the concepts of use and misuse cases and show how they can be used to model business processes with the help of the theoretical framework. In the fourth section, we apply the modelling technique to a simplified case study of a private bank facing money laundering. In the fifth section, we review relevant related work. Finally, we conclude and outline potential future work.

The regulative role of business processes

The traditional view of business processes as sets of activities designed to achieve a well-defined goal (Hammer and Champy, 1993) can be enriched by considering businesses as open systems that regulate relationships with their environment (Checkland and Scholes, 1990; Regev, 2003). From this viewpoint, inherited from GST (Weinberg and Weinberg, 1988) and cybernetics (Ashby, 1956), a business has relationships with stakeholders in its environment. These relationships are necessary

for the business to maintain its identity as distinct from other businesses. Maintaining a separate identity defines a business' success and survival. For example, Compaq lost its separate identity when it merged with HP due to its declining success, whereas Dell has managed to maintain a separate identity.

Relationships with stakeholders are necessary for a business but are also potentially harmful. Having relationships with customers, for example, is obviously necessary, but customers who demand too much of the business can contribute to its demise. This is true of all other relationships that the business maintains with stakeholders such as employees, suppliers, and investors.

To understand how the identity of a business is kept more or less stable in such a complicated environment, it is useful to introduce the concept of homeostasis drawn from the field of physiology.

The principles of homeostasis, first enunciated by the physiologist Walter B. Cannon (Weinberg and Weinberg, 1988) provide a set of heuristics that explain how the identity of a system is kept stable in an unstable environment. These principles, restated in business process vocabulary are:

- in a business subjected continually to disturbing conditions, stability is in itself evidence that one or more processes are in place to maintain this stability;
- if the business remains stable it is because any tendency towards change automatically results in increased effectiveness of processes that resist change;
- to keep a business stable, a number of cooperating processes may be brought into action at the same time or successively; and
- when a process can change an inherently stable state, it is reasonable to look for automatic control of this process or for processes that have an opposite effect, in order to avoid overcompensation.

We call norm the state of a given relationship that the business attempts to maintain unchanged (Vickers, 1968, 1987; Liu *et al.*, 2002). The number of norms that a business maintains is very large. Examples of such norms are the stability of a business' name, its reputation, its revenues, its profits, its number of employees, etc. The norms maintained by the business define its identity. A norm is stable but not necessarily static. It may change over time as the business adapts to its environment, for example, when the revenues grow as the business adapts to a growing market. A steady growth or decline is also a kind of norm, for example, a steady revenue growth.

Norms very often depend on each other (Weinberg and Weinberg, 1988). For example, the norm represented by employee benefits is usually dependent on the norm represented by its profits. High profits usually translate into high employee benefits. When profits decline it is difficult to cut employee benefits because the lifestyles of the employees themselves depend on the norms that their benefits represent. Employees are likely to take action (as suggested by the homeostatic principles) if their benefits are reduced. Thus, at any given time, the norm gives a reference point from which to judge the current state of affairs (Vickers, 1987, p. 14).

We call strategic level, the level where the norms to which the business's relationships need to adhere to are defined and modified as a result of changes within the business and in its environment. Norms can be defined proactively as in planning or in retrospect when the business settles in them without prior planning

(Mintzberg *et al.*, 1998). Maintaining and modifying these norms implies continuous effort, as suggested by the principles of homeostasis. In RE these efforts are represented by the concept of maintenance goal (Regev and Wegmann, 2002). The principles of homeostasis show that we should expect successful businesses to have processes in place that set unconditional barriers to change in their norms, processes that detect such change, and processes that act conditionally when such change is detected.

In our theoretical framework we, therefore, distinguish between operational processes, which unconditionally maintain a relationship with a stakeholder in a given norm, and the regulative processes, which are applied conditionally when an operational process fails to maintain the relationship within the norm. In a bank, for example, processes defined for taking customer orders and fulfilling them maintain the customer relationship within a prescribed norm. Detecting money-laundering activities, however, may require the processing of several financial transactions. The pattern may not be detectable by the execution of order taking and order fulfillment processes. Separate processes for identifying money laundering patterns, and addressing them, are needed.

Our framework thus contains the three levels summarized below:

(1) the strategic level contains the relationships with stakeholders, the norms with which these relationships need to comply;

(2) the operational level contains the unconditional processes that the business has developed to maintain its relationships with stakeholders within the norms, i.e. to unconditionally regulate the relationship; and

(3) the regulative level contains the processes that are applied when operational processes fail to maintain a relationship within a given norm when a threat is presented, i.e. to conditionally regulate the relationship.

This framework enables us to reflect on processes that apparently do not provide value to a customer but are necessary for the survival and success of the business in the face of threats to its norms. These threats can originate within the business or from its environment.

Notice that the addition of a regulative level is a novelty in itself, as most frameworks only distinguish between the strategic and operational levels. In the next section, we explain the use and misuse case technique, and show how our framework can enhance this technique in order to use it to supply a rationale for value-added and abuse prevention processes.

Modelling business processes with use and misuse cases

Use cases were proposed by Jacobson *et al.* (1992). The idea was to capture brief narratives describing possible uses of the system under design as distinct cases; these could then supposedly be implemented in the design one at a time. Each narrative would be named as a use case and diagrammed as a white elliptical bubble. The role principally involved with the use case (the "actor") would be diagrammed as a stick-man, linked to the bubble as in Figure 1.

Cockburn (2001) extended Jacobson's use case concept by identifying the use case's name as a functional goal, and by documenting a suggested structure for use cases, to include a primary or main success scenario, as well as exception (he called them

"extension") scenarios to handle undesired events. He made it clear that use cases documented system behaviour desired by people (or possibly other intelligent agents) playing specific system roles. The unified modelling language (OMG, 2003) documents functional requirements with use cases.

The name "use case" was clearly intended by Jacobson to apply only to uses of a system, but scenario modelling has long been applied much more widely, e.g. for military planning and film storyboarding (Alexander, 2002d), so there is really no a priori reason why use case-type scenarios should not be applied to business process modelling. Some practitioners find the use case approach convenient for thinking about business processes as well as system behaviour, and document processes as scenarios using use case notation for their context diagrams (Robertson and Robertson, 1999).

In use case modelling, processes are modelled primarily as scenarios (sequences of activities); these are not visible in the diagram, which only names the goal of each process.

Sindre and Opdahl (2000, 2001) further extended the modelling range by introducing the idea of the misuse case to document negative security scenarios. They inverted the colours of the use case to indicate the undesired intentions of a hostile agent (Figure 2). The behaviour of a hostile agent results in a loss to the business or its stakeholders (Sindre and Opdahl, 2001).

A misuse case documents conscious and active opposition in the form of a goal that a hostile agent intends to achieve, but which the organization perceives as detrimental to some of its goals. This is a stronger sort of problem than an "Obstacle" (van Lamsweerde and Letier, 2000) which suggests passively getting in the way of a desired goal. In particular, an obstacle does not react by creatively devising counter-measures when it is surmounted. A hostile agent and its misuse cases imply a dynamic and intelligent pattern of threats, not just the threatening goals actually named.

This opens the way to a game-playing or MiniMax view of process modelling. Both the organization and its opponents (such as criminals and business rivals) act intelligently to discover and play their best move, which is – as in games like chess and go – whatever best counters their opponent's best move. In our previous work, we proposed two new relationships, threatens and mitigates, to model the resulting zigzagging arms race between the players (Alexander, 2002b, c). A misuse case is

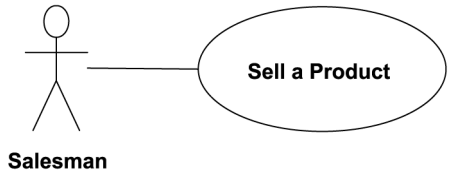

Figure 1.
Use case diagram

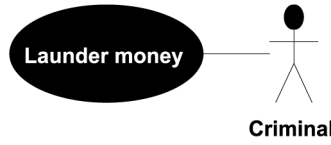

Figure 2.
Sindre and Opdahl misuse case

relevant only if it threatens the goal of a use case in the same model. Analysis may reveal one or more candidate counter-measures to the threat, and these may be documented as lower-level use cases that mitigate the threat posed by the misuse case.

The use cases are the responsibility of the roles shown on the left, as in Figure 3; the misuse case is owned by the negative role on the right. Higher-level use cases are shown furthest left; successively lower-level use cases are shown further towards the right. Relationships between use cases are shown as arrows; four types of relationship are visible in the diagram, namely includes, has exception, threatens, and mitigates.

Normally, one role has the primary responsibility for a given use case – sales is responsible for selling – though other secondary roles may also be involved. Roles may be filled by either human or machine agents, as long as these have sufficient intelligence for the tasks involved.

The models in this paper are based on use/misuse case models constructed with Scenario Plus, a free toolkit for use with the requirements tool DOORS (Scenario Plus, 2003; DOORS, 2003). The toolkit provides a rich set of options for the modeller, including model creation, editing, linking, checking, metrics, and export. The resulting technique is suitable for a wide range of purposes, most obviously security threat mitigation, but also reasoning in design space for trade-off and conflict analysis as we have shown in a previous work (Alexander, 2002a).

To use this technique for business process modelling, we propose to model the strategic level norms, the operational processes, and the regulative processes of the business with use cases, and the threats the business believes it faces as misuse cases. The legitimate stakeholders are modelled as actors, and the rest as hostile agents. Figure 3 shows a use case establish reputation being threatened by a misuse case launder money, which in turn is mitigated by the use case check money laundering. This has an exception, a regulative use case alert authorities, which corrects for a possible deviation from the norm of not allowing money-laundering activities. We extend Sindre and Opdahl's technique by delimiting the business's actors and use cases with a rectangle and by adding a stereotype to the use cases to show the level (strategic, operational, regulative) at which we classify them.

Notice that the hostile agent is only hostile from the point of view of the business or even of an individual process. The "hostile agent" may be a bona-fide customer of the

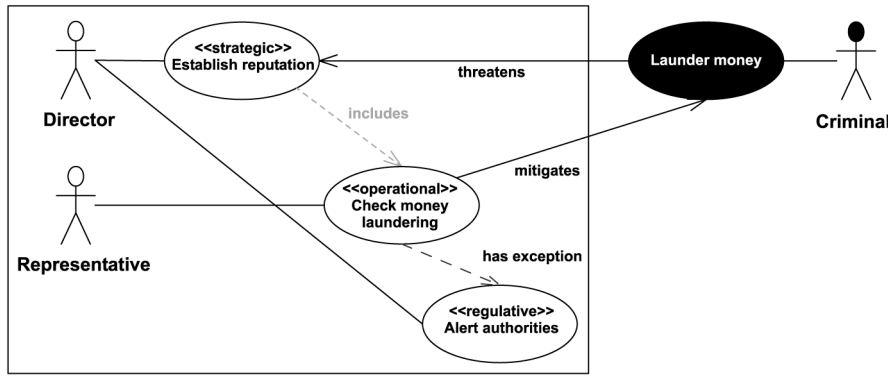

Figure 3.
Documenting threat and mitigation with use and misuse cases

organization who performs actions without understanding their implications, or a customer who sometimes has behaviour that the organization dislikes.

The case of the private bank

In this section we show how the use/misuse case approach, coupled with our theoretical framework, can be used to model business processes. We use the simplified example of a private bank that needs to address money-laundering issues. This example is inspired by a reengineering project conducted at a Swiss portfolio management company.

The service offered by private banks can easily be used as a tool for laundering money earned illicitly. Taking measures to protect against money laundering is not directly part of the service a private bank provides to its clients. However, accepting money-laundering activities sets the bank outside of the norm established by countries and international organizations, such as the Task Force on Money Laundering (FATF, 2003) recommendations. These recommendations strongly encourage financial institutions to monitor for money laundering and take regulative action when such activity is detected. Below, we show how our use/misuse case approach can be used to model the processes of a private bank subject to the FATF recommendations. Because of space constraints we only consider a small subset of these that we call the country recommendations.

We consider that the country recommendations specify that client identity be verified when client accounts are opened, that transaction amounts exceeding a certain threshold be considered as suspect, that the origin of funds be verified, and that transaction records be kept for a period of five years. This gives us a pattern of threats from criminals who try to invest money anonymously, under false identity, who want to invest illegal funds, and who invest large sums of money in one transaction.

Figure 4 shows the strategic level for the private bank. At this level we consider the following use cases for the bank, maintain business, establish good reputation and comply with country regulations. The relevant actors are the bank's director and the bank's client. The hostile agents are the criminal and the country authority. The bank maintains its identity by doing business with clients. As part of this identity, the bank establishes the good reputation needed for customers to trust it with managing their portfolios. This reputation, a norm, is threatened by people, "criminals", who want to launder money earned illegally. Country authorities may also tarnish this reputation, i.e. create deviations from the norm, by launching probes into the bank's activities if they suspect that it is used for money laundering. These two threats are represented as

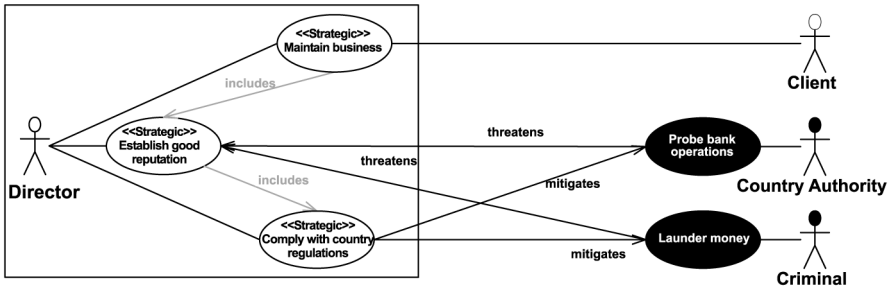

Figure 4.
Strategic level use and misuse cases for the private bank

the misuse cases launder money and probe bank operations. The use case comply with country regulations mitigates both of these threats. Notice that the country authority is represented as a hostile agent whereas it could appear elsewhere as a cooperating actor, illustrating the complexity of relationships with stakeholders.

Figure 5 adds operational level use cases. The use case enrol new clients represent a process that maintains the bank's revenue stream and hence its identity; it is, therefore, included by the use case maintain business. The use case provides ROI to clients both helps the bank to establish its good reputation and maintains its revenue stream (the bank is paid commission relative to the return on investment it provides to its clients). This use case is, therefore, included by both of the strategic use cases.

In this model, the bank's customer representative is responsible for enrolling new clients. The account manager for a given client's account is responsible for providing the return on investment to clients. However, clients can also place orders themselves, by contacting the bank's customer representative. By providing these services, the bank becomes vulnerable to money laundering threats and needs to regulate access to these services to prevent their abuse.

The model in Figure 5 shows that the verify client identity use case mitigates the threat from the misuse cases invest under false identity and invest anonymously. Indeed, merely asking for the identity of a client may deter those who want to launder money anonymously. Verifying that the identity provided by the client is genuine may

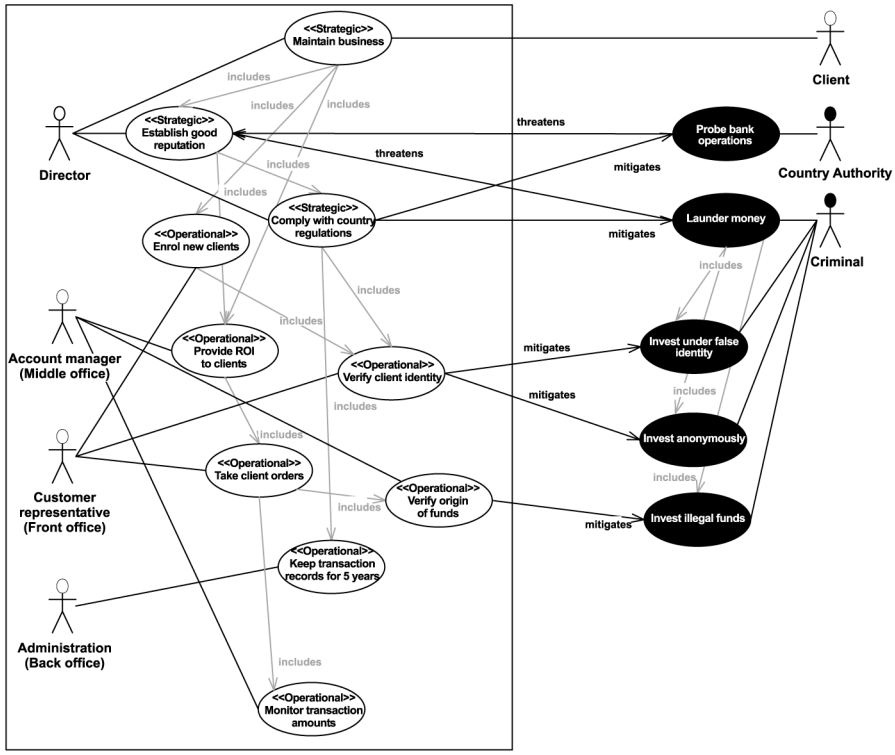

Figure 5.
Operational level use and misuse cases for the private bank

deter those who want to launder money using a false identity. Similarly, the use case verify origin of funds mitigates the threat from those who want to invest illegally obtained funds irrespective of their identity.

Figure 5 shows two more use cases recommended by the country recommendations. These are Keep transaction records for five years and monitor transaction amounts. These use cases in themselves do not mitigate any threat. However, they serve as the needed norm for the regulative use cases reject suspicious clients, reject if transaction amount above threshold, and alert authorities in case of suspicion shown in Figure 6. These are invoked only when the norm of dealing with trustworthy clients who perform normal transaction is violated. They are then considered as mitigating the threat from money laundering.

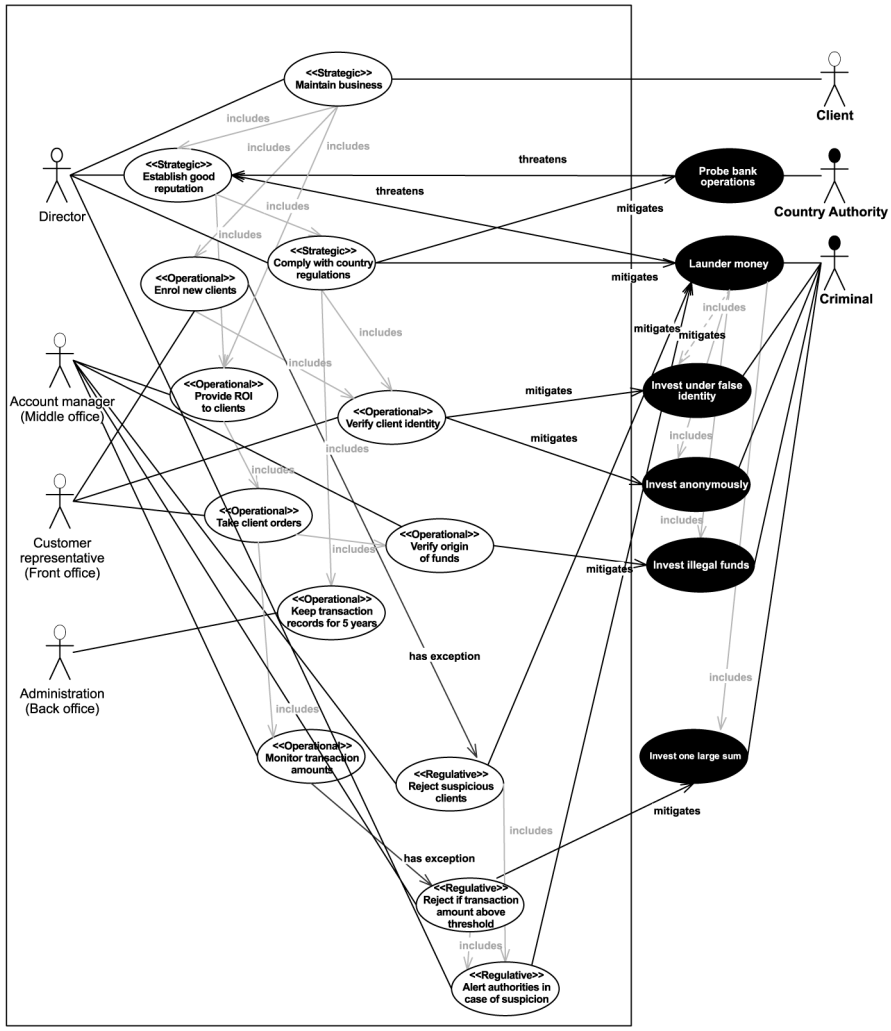

Figure 6.
The complete use and misuse cases for the private bank

In this section we have shown how a use/misuse case model can provide a valuable rationale for the processes of a private bank based on the relationships the bank wants to establish with its stakeholders and threats to these relationships. This rationale is either inclusion in a higher-level process or mitigation of an explicit threat. This enables process engineers to identify and document when a given process is needed. When conditions change, e.g. when money-laundering patterns mutate, relevant processes can be revisited, modified, or removed. Notice, though, that some processes are performed for several reasons and need to be maintained even when some documented threats that they mitigate are considered not to exist any more. For example, get client identity and keep transaction records for five years are necessary for mitigating other threats, such as queries by tax authorities, and should probably be kept regardless of the threat from money laundering.

Related work

The number of candidate techniques for redesigning business processes is large. These techniques originate in many disciplines. In this section we will mention some of the most prominent, and briefly discuss the way our technique differs from them.

Use case-related techniques

Use case diagrams can be used to provide rough models of business processes but they do not include the rationale for these processes. An emerging ITU standard, use case maps (ITU, 2002) offers a graphical notation for a more detailed description of behaviour with the aim of specifying so-called functional requirements, but like use case diagrams these do not include the rationale for the processes they describe.

Sindre and Opdahl proposed and applied the misuse case technique to develop security requirements for IT systems. The theoretical background we propose in this paper makes this technique suitable for business process redesign.

Business process modelling

Many business process modelling methods exist; for example, Workflow, ARIS, IDEF0, IDEF3, Petri Nets, UML activity diagrams and sequence diagrams, etc. All of those include a graphical representation, a diagram, of the activities that compose a process. However, none of the methods we know includes the rationale for the activities that compose a process. Some rationale is hidden in messages received from the environment, as can be done in UML activity diagrams, but this is rather implicit.

Systems thinking-based techniques

Soft system methodology (SSM) (Checkland and Scholes, 1990) and system dynamics (SD) (Forrester, 1971; Senge *et al.*, 1999) are two methods that have evolved from the systems sciences movement. SSM uses activity diagrams called Rich Pictures and SD uses SD diagrams. Both rich pictures and SD can be used to model business processes. SD as presented in Senge *et al.* (1999) uses the concept of constraint but does not make it clear from where the constraint comes from. Furthermore, a constraint is a weaker form of a threat. SSM includes measure and control activities in its rich pictures, which could be compared to the regulative processes in our framework. However, it is not made clear, in the SSM literature, why these activities are necessary, e.g. for threat mitigation.

Goal-oriented requirements engineering techniques

Many goal-oriented techniques have been developed in the field of RE. The most prominent being KAOS (Dardenne *et al.*, 1993; van Lamsweerde and Letier, 2000), GBRAM (Anton, 1997), i* (Yu and Mylopoulos, 1994), GRL (ITU, 2001), etc. Some of them, in particular i* have been applied for business process reengineering. GRL is an evolution of i* and is used for specifying non-functional requirements as part of the user requirements notation of which UCM is the functional part.

KAOS and GBRAM specify the concepts of constraints and obstacles that prevent the achievement of goals. As we argued in this paper, these represent weaker forms of the threats that we consider in our technique. Furthermore, these techniques do not include a graphical notation that can be used to reason about the models with stakeholders.

i* and GRL do provide a graphical notation where networks of dependencies between actors who depend on each others to achieve goals are specified. These dependencies are only positive dependencies. Threats such as the ones we represent cannot be conveniently and explicitly represented.

Business-oriented techniques

BPR techniques (Hammer and Champy, 1993; Kueng and Kawalek, 1997) specify that abuse-prevention activities should be kept to a minimum. However, they do not provide a framework for designing abuse prevention activities except by specifying that their cost (mainly financial) should not outweigh the protection they offer.

Balanced scorecards (BSC) (Kaplan and Norton, 1996) is a technique that models a business in four dimensions – financial, internal business processes, learning and growth, and customer. The internal business processes is the dimension where existing processes are analysed and new ones are invented. BSC subscribes to a theory similar to the one underlying BPR. Business processes are developed from the point of view of the value they provide to customers and the financial returns that they bring to the business. No threat-prevention activities are explored.

In the field of organizational semiotics (Liu *et al.*, 2002) business processes are thought of as norms of behaviour of an organization. These norms are extracted from descriptions of the organization's current processes. The meaning of the norms for different people within the organization is analysed. Use cases are derived from these norms (Shishkov *et al.*, 2002). The rationale for these norms and the way they are maintained is not explicitly represented.

Conclusions

In this paper we described a theoretical framework for understanding business processes and a modelling technique that can be used for process redesign. The theoretical framework is based on a proven theory from another field, homeostasis (from biology). Homeostasis shows that deviation from a norm is a powerful catalyst for action and, therefore, for business process definition.

The framework is useful because it provides a theoretical justification for the value creation and abuse prevention activities that can be found in business processes. The three levels that we use to analyse business processes (strategic, operational and regulative) constitute an innovation in business process modelling where only two levels (strategic and operational) have been considered thus far. Explicitly modelling

the potential abuses (threats) to business processes and their associated corrective measures (regulative processes) becomes possible during process redesign. We believe that few if any business process theoretical frameworks provide this kind of rationale for abuse prevention activities.

The modelling technique is an extension of the use/misuse case technique, developed in RE. Its purpose is to provide an overall understanding of the business processes and their rationale. It is not intended to provide a detailed description of business processes. Initial experience with this technique was gained by describing trade-offs for a railway design workshop (Alexander, 2002a). The workshop was able to advance rapidly from a previously stuck position once all participants understood the nature of the conflicting pressures on the design.

Rationale in the form of threats can be thought of as a business' belief about itself and its environment. Such beliefs can bring about the feared threats, as the business partly constructs its environment in its image. Also, a focus on threats can result in paralysis, but can also create opportunities for learning and constructively modifying business processes.

Hence, future work could include:

- Research into the way threats are interpreted by organizations and the effects of these interpretations on the business and its environment.
- Threat-oriented extensions to detailed business process design techniques, such as IDEF, UCM.
- Extension of use/misuse case diagrams with argumentation artefacts to help select the right amount of regulative processes to avoid antagonising stakeholders. Such artefacts could be borrowed from goal-oriented methods such as GRL, from problem-solving methods such as IBIS (Conklin *et al.*, 2001), or from design rationale methods such as QOC (MacLean *et al.*, 1989).

References

Alexander, I. (2002a), "Initial industrial experience of misuse cases in trade-off analysis", *Proceedings of the IEEE Joint International Requirements Engineering Conference (RE'02)*, Essen, 9-13 September, pp. 61-8.

Alexander, I. (2002b), "Towards automatic traceability in industrial practice", *Proceedings of the First International Workshop on Traceability*, Edinburgh, 28 September, in conjunction with the 17th IEEE International Conference on Automated Software Engineering, pp. 26-31.

Alexander, I. (2002c), "Modelling the interplay of conflicting goals with use and misuse cases", *Proceedings of the Eighth International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ'02)*, Essen, 9-10 September, pp. 145-52.

Alexander, I. (2002d), "On abstraction in scenarios", *Requirements Engineering*, Vol. 6 No. 4, pp. 252-5, Viewpoints Article.

Anton, A.I. (1997), "Goal identification and refinement in the specification of software-based information systems", PhD dissertation, Georgia Institute of Technology, Atlanta, GA.

Ashby, W.R. (1956), *An Introduction to Cybernetics*, Chapman Hall, London.

Checkland, P. and Scholes, J. (1990), *Soft System Methodology in Action*, Wiley, Chichester, UK.

Coakes, E., Willis, D. and Lloyd-Jones, R. (2000), *The New SocioTech: Graffiti on the Long Wall*, Springer, London.

Cockburn, A. (2001), *Writing Effective Use Cases*, Addison-Wesley, Reading, MA.

Conklin, J., Selvin, A., Buckingham Shum, S. and Sierhuis, M. (2001), "Facilitated hypertext for collective sensemaking: 15 years of from gIBIS", *Proceedings ACM Conference on Hypertext and Hypermedia*, Århus.

Dardenne, A., van Lamsweerde, A. and Fickas, S. (1993), "Goal directed requirements acquisition", *Science of Computer Programming*, Vol. 20 Nos 1/2, pp. 3-50.

DOORS (2003) available at: www.telelogic.com

FATF, Financial Action Task Force on Money Laundering (2003), "The forty recommendations", available at: www.fatf-gafi.org/40Recs_en.htm (accessed 20 June 2003).

Forrester, J. (1971), *World Dynamics*, 2nd ed., Wright-Allen, Cambridge, MA.

Hammer, M. and Champy, J. (1993), *Reengineering the Corporation: A Manifesto for Business Revolution*, Nicholas Brealey, London.

ITU – Telecommunication Standardization Sector (2001), *Draft Specification of the Goal-oriented Requirement Language (Z.151)*, September.

ITU – Telecommunication Standardization Sector (2002), *Draft Specification of the Use Case Map Notation (Z.152)*, February.

Jacobson, I., Christerson, M., Jonsson, P. and Övergaard, G. (1992), *Object-oriented Software Engineering: A Use Case Driven Approach*, Addison-Wesley, Reading, MA.

Kaplan, R.S. and Norton, D.P. (1996), *The Balanced Scorecard: Translating Strategy into Action*, Harvard Business School, Boston, MA.

Kueng, P. and Kawalek, P. (1997), "Goal-based business process models: creation and evaluation", *Business Process Management Journal*, Vol. 3 No. 1, pp. 17-38.

Liu, K., Clarke, R.J., Anderson, P.B. and Stamper, R.K. (2002), *Coordination and Communication Using Signs: Studies in Organizational Semiotics*, Kluwer, Dordrecht.

MacLean, A., Young, R.M. and Moran, T. (1989), "Design rationale: the argument behind the artifact", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: Wings for the Mind*, pp. 247-52.

Mintzberg, H., Ahlstrand, B. and Lampel, J. (1998), *Strategy Safary – The Complete Guide through the Wilds of Strategic Management*, Prentice-Hall, London.

OMG (2003), *Unified Modeling Language (UML)*, specification version 1.5, March.

Regev, G. (2003), "A systemic paradigm for early IT system requirements based on regulation principles: the lightswitch approach", PhD thesis, Ecole Polytechnique Fédérale de Lausanne (EPFL), Lausanne.

Regev, G. and Wegmann, A. (2002), "Regulation based linking of strategic goals and business processes", paper presented at Third BPMDS Workshop on Goal-oriented Business Process Modeling, The 16th British HCI Group Annual Conference, London, 2-6 September.

Robertson, S. and Robertson, J. (1999), *Mastering the Requirements Process*, Addison-Wesley, Reading MA.

Scenario Plus (2003), available at: www.scenarioplus.org.uk

Senge, P., Roberts, C., Ross, R., Smith, B., Roth, G. and Kleiner, A. (1999), *The Dance of Change*, Nicholas Brealey, London.

Shishkov, B., Xie, Z., Liu, K. and Dietz, J.L.G. (2002), "Using norm analysis to derive use cases from business processes", *Proceedings of the Fifth Workshop on Organizational Semiotics OS 2002*, Delft, 14-15 June, pp. 187-95.

Sindre, G. and Opdahl, A.L. (2000), "Eliciting security requirements by misuse cases", *Proceedings of the 37th International Conference on Technology of Object-oriented Languages and Systems*, Sydney, 20-23 November, pp. 120-31.

Sindre, G. and Opdahl, A.L. (2001), "Templates for Misuse Case Description", *Proceedings of the Seventh International Workshop on Requirements Engineering: Foundation for Software Quality REFSQ'01*, Ben Achour – Salinesi, C., Opdahl, A.L., Pohl, K. and Rossi, M. Essener Informatik Beiträge, Interlaken, 4-5 June.

van Lamsweerde, A. (2001), "Goal-oriented requirements engineering: a guided tour. Invited mini-tutorial paper", *Proceedings of the Fifth IEEE International Symposium on Requirements Engineering, RE'01*, Toronto, 27-31 August, pp. 249-62.

van Lamsweerde, A. and Letier, E. (2000), "Handling obstacles in goal-oriented requirements engineering", *IEEE Transactions on Software Engineering*, Vol. 26 No. 10, pp. 978-1005.

Vickers, S.G. (1968), *Value Systems and Social Process*, Tavistock Publications, London.

Vickers, S.G. (1987), *Policymaking, Communication, and Social Learning*, Transaction Books, New Brunswick, NJ.

Weinberg, G.M. and Weinberg, D. (1988), *General Principles of Systems Design*, Dorset House, New York, NY.

Yu, E. and Mylopoulos, J. (1994), "Using goals, rules and methods to support reasoning in business process reengineering", *Proceedings of the 27th Hawaii International. Conference on System Sciences*, Vol. 4, Maui, Hawaii, 4-7 January, pp. 234-43.

Further reading

Weinberg, G.M. (1975), *An Introduction to General Systems Thinking*, Wiley, New York, NY.