III APPLICATIONS IN SECURITY AND PRIVACY

7 Improving Risk-Based Security Analysis with *i**

Eric Dubois, Nicolas Mayer, and André Rifaut

7.1 Introduction

Information systems (ISs) are everywhere. They have a large impact on the everyday lives of organizations as well as on individuals. In the light of ambient, pervasive, and ubiquitous computing, this impact is increasing significantly. At the heart of information systems, security aspects play a vital role and are thus becoming central issues in those systems' effective usage. The importance of security technologies and of their enabling technical platforms has been widely recognized and receives continuous attention (e.g., new encryption algorithms, public key infrastructures, etc.). However, organizations also increasingly consider the management dimension of security. From an anecdotal perspective, one can say that security management issues start with updating an antivirus database, but from a more serious economic perspective, organizations understand that security concerns are the source of important costs, not only in terms of technologies but especially in terms of related management activities. As an example, many organizations (e.g., banks) first introduced public key infrastructures, considered as the most secure technical platform for coping with authentication, confidentiality, integrity, and nonrepudiation security issues. But after a while, many of these organizations abandoned such solutions for lighter weight platforms because of the costs generated. Sources of these costs are mainly related to associated management activities and interoperability issues, and also to indirect costs, due to the difficulty of usage by their customers. To summarize, many security solutions and infrastructures exist and can be deployed, but the key problem is to know if their associated direct and indirect costs should be adopted. In practice, these costs have to be compared with the consequences of not using these secure solutions and infrastructures to measure the total impact cost of a security problem on the business.

ROI (return on investment) issues related to the cost of security technologies compared to their benefits are thus becoming a vital question in many organizations. As a consequence, the traditional role of IS security officers is evolving more and more from a purely technical profile to a new profile in which a mix of business and technical competencies is

required. These competencies are needed for being able to evaluate the fit that must be established between secure IT infrastructure and the assets to be protected at the business level of an organization. Central to this business/IT alignment problem (Henderson & Venkatraman, 1993) is the risk analysis process, in which the cost of a technical security solution should be balanced against the vulnerabilities of the IS and the costs of the impact on the business related to the exploitation of these vulnerabilities. This need for setting up security risk analysis processes within organizations is further reinforced and broadened at the institutional and/or sector-based levels, with major initiatives such as the Sarbanes–Oxley Act (see American Institute of Certified Public Accountants, 2002), governing the integrity of financial and accounting data or, in the banking industry, the Basel II agreement (Basel Committee on Banking Supervision, 2004), which requires banks to comply with instructions for defining the level of their capital requirements in relation to the maturity of their risk management activities. To answer this need there are several initiatives, ranging from the identification of the management *processes* to be set up in organizations (Rifaut, 2005), to *methods* that provide assistance and guidelines in the production of the deliverables associated with security risk management activities.

In this chapter our focus is on the *method* aspect. More specifically, after a brief introduction to some of the most popular risk management methods and to their fundamentals in section 7.2, we will explain some of their drawbacks and the benefit of complementing them with a more formal framework supporting the production of more rigorous descriptions, associated with a continuous risk analysis activity. This framework is introduced in section 7.3, in which we will also explain the importance of models that can be produced both at the business level (the ''what'') and at the software architectural level (the ''how''). However, as such models are not sufficient to really help in coping with the business/IT alignment issues, we will motivate the benefits of complementing them with a requirements engineering (RE) approach based on the *i** framework (see chapter 2 in this book; see also Yu, 1997) to address the ''why'' question underlying this alignment within the context of a risk-based process. In the rest of the chapter, we will illustrate the overall approach through the handling of a simplified health care case study related to an IS supporting the approval of and reimbursement for physicians' medical procedures. In section 7.4, we will show how the *i** framework complements a classical business process model approach for achieving a better understanding of business assets and of the security goals associated with them. Then, in section 7.5, at the software architectural level, we will see how goals can be systematically refined into traceable security requirements. Finally, in section 7.6, together with the components identified in the detailed software architecture, we will explain how the security requirements are the inputs for a more systematic risk analysis applied to the IS level. To support it, we have enriched the *i** framework with a few additional concepts, and notations for the concepts, that support reasoning over security risks, the associated security solutions (also referred to as controls or countermeasures), and their traceability. Section 7.7 concludes this chapter with a comparison to other uses of the *i**

and other modeling frameworks in security contexts and introduces directions for future work.

7.2 Security Risk Analysis Methods

7.2.1 State of the Art

Today a number of methods are available to security officers in organizations for performing risk analyses of security problems and identifying solutions that are the most adequate in the context of the alignment of the business with an IS solution. Based on the ontology for the security risk management domain elaborated in the work of Mayer (2009), figure 7.1 introduces the main components of a risk-based management approach.

- *Business Assets* are anything that has economic value to the organization and that is central in the realization of its business objectives. The protection of these assets is essential for the survival of the organization.
- Within organizations, business assets management relies heavily on ISs. *IS Assets* (including IT resources) are any components that are part of IS and of their operating

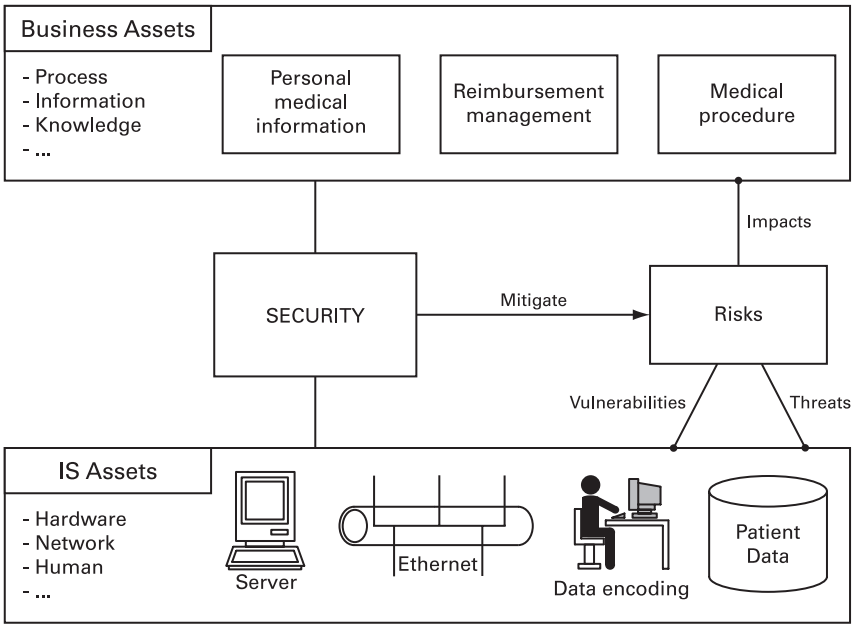

Figure 7.1
Risk-based management approach.

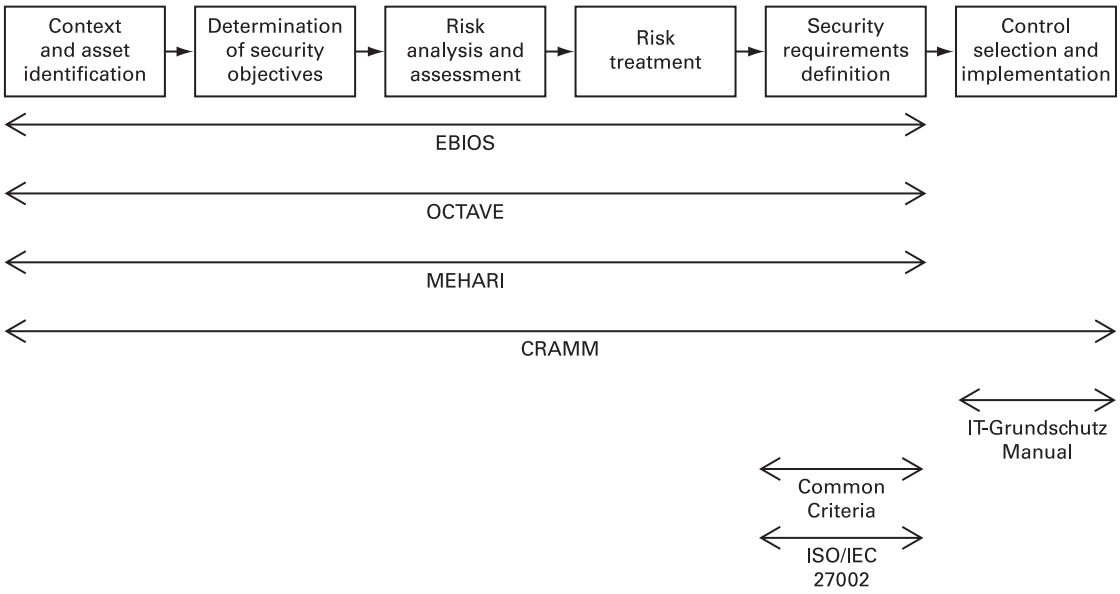

Figure 7.2
Classification of some risk management methods.

environment. In many cases IS assets are direct mirrors of business assets (e.g., the data stored in the database that mirror the medical procedure business information).

- *Security* is the central property expected from the installed IS. It defines different qualities expected from the IS. Besides the pure security aspects (e.g., confidentiality of data), it also encompasses aspects such as reliability, performance, and resilience.
- *Risk Management* is the essential equation to be kept in mind when handling the various security qualities. For each IS asset, one has to ask questions about its *vulnerabilities*, the existence of potential *threats* capable of exploiting these vulnerabilities, and the *impact* of this exploitation on the running of the business. All this risk analysis activity results in the identification of best controls (security countermeasures) to be implemented.

The risk management process is composed of the activities presented in figure 7.2. The process begins with a study of the organization's *context* and the identification of its *assets*. In this step, the organization and its environment are described, and an overview of the IS, when already in place, is made. For example, in a medical context (not defined in depth here), patient information is a business asset and the medical database that stores that patient information is an IS asset. Then, based on the level of protection required for the assets, one needs to determine the *security objectives*. Security objectives are often defined in terms of confidentiality, integrity, and availability of the assets. Returning to the medical example, the confidentiality of patient information should be assured. The main step of

the risk management process is *risk analysis*, which elicits the risks that are harming assets and threatening security objectives. This step consists of identifying risks and estimating their level in a qualitative or quantitative manner. We speak about *risk assessment* only after the level of analyzed risks is evaluated against the security needs, which are determined during the second step of the process. For instance, the database supporting the patient information can be the target of a hacker trying to exploit common TCP/IP weaknesses to access the confidential data. This risk has an estimated level high enough for it to be considered. Once risk analysis is performed, decisions about *risk treatment* are taken, such as reducing the risk with controls or transferring the risk to a third party. *Security requirements* on the IS can thus be determined as security solutions to mitigate the risks. For our example, technical controls are chosen to reduce the risk, such as enabling filtering and intrusion detection on the IS network. Requirements are finally instantiated into security *controls* (i.e., system-specific countermeasures) that are implemented within the organization. In our example, a firewall and an intrusion detection system (IDS) are selected and implemented within the IS.

A number of commercial methods are now on the market. Some of the best-known approaches are OCTAVE (Alberts & Dorofee, 2001), IT-Grundschutz Manual (BSI, 2004), CRAMM (Insight Consulting, 2003), ISO/IEC 27002 (ISO, 2005a), Common Criteria (Common Criteria, 2006), MEHARI (Club de la Sécurité de l'Information Français, 2004), and EBIOS (Direction Centrale de la Sécurité des Systèmes d'Information, 2004). As shown in figure 7.2, they differ mainly in the weight put on the different risk management activities, some of them being, for example, only best practices and proposing a set of security requirements to implement (ISO, 2005a; Common Criteria, 2006).

7.2.2 Weaknesses of Traditional Methods

Even if existing methods cover the activities of risk management, they have a number of weaknesses that result mainly from a lack of well-defined concepts, detailed analysis, and a rigorous, analytical, and systematic approach. In particular, the following are needed:

- More rigorous documents associated with the activities depicted in figure 7.2. For a long time, IS engineering has been familiar with the problems associated with informal documents and has proposed "models" as a way to achieve more formality and better quality. Proposed models include enterprise/process models, which can be useful for identifying and representing business assets within their organizational context, and MDA (Model Driven Architecture)-based approaches for representing IS resources and software components within the context of logical and physical IS architecture.
- More systematic methods to guide and guarantee business/IT alignment within a security context. This requires being able to reason about the traceability links that need to be established between the business and IS assets. Most of the existing approaches support only a coarse-grained view of these traceability links, whereas a more detailed

and analytical analysis would make possible more precise reasoning. At this level, lessons drawn from the relation between RE and AE (architectural engineering) are helpful for achieving an enhanced traceability framework, in which the links existing between security requirements and IS components are represented.

- Better integration of risk analysis activities all along the IS development life cycle. In many of the existing approaches, risk analysis activities are planned at the end of IS development and even, sometimes, at the time of IS deployment. However, many of the risk analysis activities could be performed at the same time as the IS development stages, with a more beneficial and direct effect in terms of traceability between risk management decisions and the information collected during these stages.

7.3 The Proposed RE and Modeling Framework for Risk Analysis

For improving existing methods, our proposal is to complement them with a framework having three components, with a focus on the early and more productive stages of IS development:

- A modeling component that provides better support in the formalization of information and knowledge created and exchanged during risk management activities, by way of models associated with business and architectural domains.
- An AE component that, together with RE techniques and methods, provides better systematic support in terms of business/IS alignment. The improvement will concern, on the one hand, the alignment of security requirements with business assets, through the adoption of a goal-oriented approach, and on the other hand, the alignment of IS software architecture with security requirements, on the basis of a systematic IS risk-based analysis.
- A risk analysis component that supports the RE activities described above through a risk-driven decision process that is led by a costs/benefits analysis focusing on the ROI issue described in section 7.1.

The contributions made by our approach are shown by additions to figure 7.1, which are shown in boldface type in figure 7.3.

The three components are now further detailed along with our motivations for using the *i** framework in support of them.

7.3.1 The Modeling Component

At the model level, our proposal is not new regarding the benefits of using rigorous notations for achieving better and more precise representation of business (the "what") and architectural (the "how") aspects. In subsection 7.4.1, the benefit of using rigorous notations is illustrated by using classical representations coming from standard notations associated with business processes (BPM) and software architecture (MDA) models.

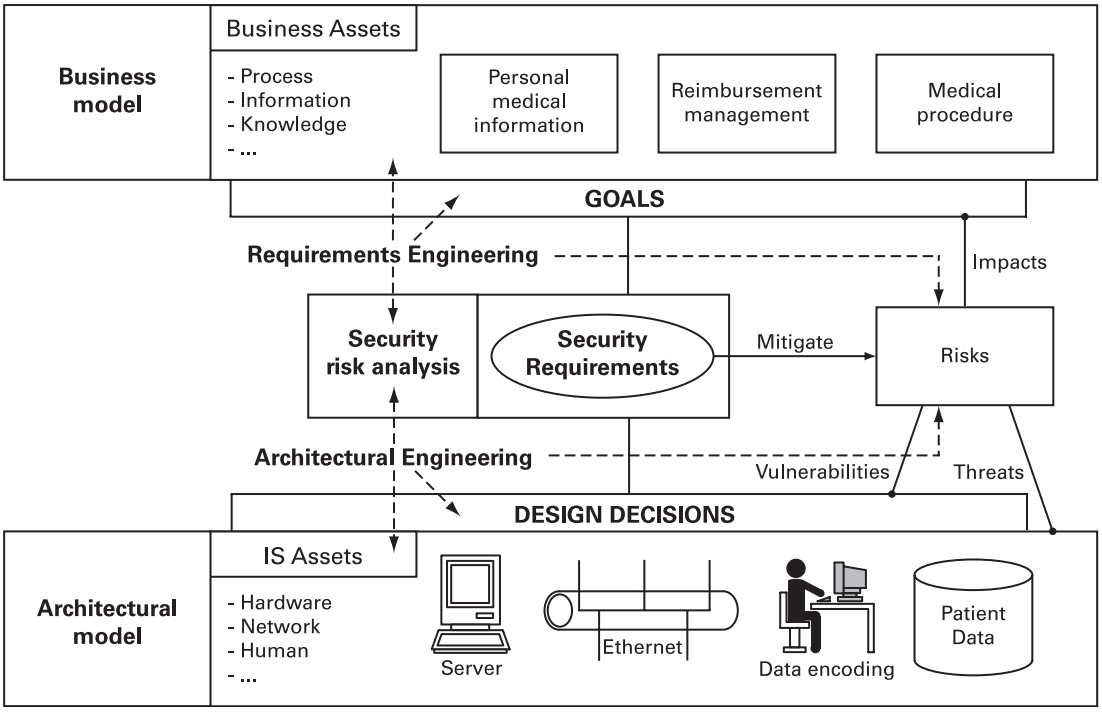

Figure 7.3
A proposal for a rigorous framework for risk management.

But more important is the need for reasoning over business and IS assets, because doing so is critical for risk analysis activities. Even if these assets can be identified in the "what" and "how" diagrams, we propose to use the *i** framework to support reasoning over the "whys" associated with the different assets, and thus to capture the knowledge required for risk analysis.

7.3.2 The AE/RE Component

The alignment of the business with the IS is guaranteed through the use of RE techniques that identify high-level requirements (goals) related to business assets, and low-level requirements that are attached to properties expected from the IS solution.

Due to the impact of nonfunctional aspects on all AE activities, the elicitation of nonfunctional aspects (including security aspects) must be addressed at the earliest stages of the IS engineering process, in particular at the RE activities stage. This need is fulfilled through the use of *i** diagrams.

As defined by the concept of "twin peaks" first described by Nuseibeh (2001), there is an unavoidable intertwining of RE and AE activities: "Analysis of a requirements

specification will lead to a design proposal, and analysis of the design will show the need for further requirements" (Moffett & Nuseibeh, 2003, p. 5). Handling the management of this intertwining aspect is part of the risk analysis component.

7.3.3 The Risk Analysis Component

7.3.3.1 Principles of a Risk-Driven Process

Throughout the development of an IS, a number of design decisions are taken at abstraction levels ranging from the strategic business level up to the detailed architectural level. All these decisions imply some associated risks, most of them having severe impacts on the level of security that the IS will ultimately provide. For example, these impacts may be related to incorrect identification of the business assets in the company, of the security goals and requirements of the IS assets, and so on. Ultimately, incorrect assessments of all or some of these elements result in an inadequate evaluation and/or selection of security measures. For dealing with such problems, our aim is to introduce a systematic risk-driven process:

1. Guaranteeing the quality of the engineering activity within the cost/benefit trade-off. In particular the engineering of nonfunctional aspects interleaved into the RE and AE is very sensitive to the *completeness* of analyses (which is one of the most important quality aspects of engineering activities, besides the correctness and adequacy of the analysis).
2. Dynamically tailoring the decision process to the *abstraction level* (business high-level/detailed IS architecture) of the analyses taking place during the activities, all along the engineering process, concerning the nonfunctional aspect, the RE process, and the AE process.
3. Quickly defining the right *scope* of the concepts already modeled, in order to decide the next activities to select at any time. This is the most important feature when models tend to be large in real case studies and strong relationships exist between different concerns and abstraction levels.

7.3.3.2 A Proposed Risk-Based Decision Process

The proposed method (further detailed in Mayer, Rifaut, & Dubois, 2005) uses a qualitative risk assessment for focusing, at any moment of the iterative security engineering activity, on the most critical parts of the business and of the IS. The risk assessment criteria are based on risks and the costs of mitigating them. In other words, we face a trade-off typical in NFR (nonfunctional requirement) reconciliation (e.g., performance versus memory space constraints). However, this method is extended at each abstraction level of the analysis, as will be seen in the case study. The accuracy of qualitative risk assessments is highly dependent on expert knowledge about the domain, and often on the subjective aspects that are included in order to reflect the viewpoints of all stakeholders.[1] At this stage, we will not enter into details of how to get an objective measure of the confidence in those quali-

tative analyses and how to reconcile different viewpoints. In any case, the accuracy of the qualitative assessment increases during the engineering process. For instance, depending on the specifics of the IS development project, the following aspects can be qualitatively assessed at the different steps of the IS life cycle:

- At the beginning, only a coarse estimation of the value of the business assets can be taken independently of the probability of risks.
- Next, there is a progressive identification of the IS assets that mirror the business assets for which security goals have been established.
- Next, the probability of major attacks on the IS assets can be considered when threats and vulnerabilities have been identified.
- Next, the major costs of selected countermeasures can be taken into account.
- Last, the details of the costs, depending on the IS load, are evaluated.

Keeping the scope of the security engineering process on just the most important qualitative aspects helps to optimize budget resources allocated for the analysis, without weakening the completeness of the risk analysis.[2] Moreover, taking advantage of traceability links, the scope of each iteration of the security engineering process is always defined at the right level of abstraction. Thus, only details meaningful to the scope and abstraction level of each iteration are added.

The whole process depends heavily on the *i** framework, which is very useful for supporting a risk-driven process. Indeed, dependency links, means-end decomposition links, and task-decomposition links can be used to define the right scope of the risk analysis. NFR reconciliation is based on the assessment of goals and softgoals that are based on the method used in Tropos (Castro, Kolp, & Mylopoulos, 2002) and the NFR framework (Chung, Nixon, Yu, & Mylopoulos, 2000).

The next sections illustrate all these principles and guidelines, together with the benefits offered by the support of *i** diagrams.

7.4 Business Process, Business Assets, and Goals

In the rest of the chapter we illustrate our approach through the handling of a simplified case study related to the health care domain.

Case Study Presentation

The context of the case study is the reimbursement for procedures performed by physicians by health insurance companies. In most of the existing national systems, a physician willing to perform specific (and often costly!) medical procedures needs first to get the approval of the health insurance company before executing them. In practice, this means that the physician has to transmit information about the patient and the requested procedure to the health insurance company. Once the physician receives an authorization, then he/she can perform the medical procedure, report on its execution to the health insurance company, and wait for reimbursement from the company.

In a classical approach based on paper-based information exchange, all of this process is subject to time delay, which can have severe consequences for patients in terms of health, as well as for physicians in terms of monetary reimbursement. Thus, the new proposed approach is to adopt electronic means for supporting these exchanges and to develop a new IS for managing them.

Given a context, the first activity of risk management is concerned with a better understanding of the business organization and the importance of its business assets.

7.4.1 Business Process Modeling

To achieve a more precise representation of the business at some abstract level, one can decide to adopt process/enterprise modeling techniques. Different modeling approaches (UML, Object Management Group, 2007b; UEML, Jochem, 2003; BPMN, Object Management Group, 2007a; CIM (from MDA), Object Management Group, 2001) allow for the expression of the different business activities executed in an enterprise, as well as for the representation of the business actors performing these activities; for the expression of information flowing between these activities; and for the nature of the information itself. An example of a business process model associated with our case study is the UML activity diagram depicted in figure 7.4.

The usage of an enterprise/business modeling language helps in achieving a better clarification of the business of the organization, in terms of its processes, actors, and flows of information. These concepts are elements of the ontology associated with the metamodel of the BPM language. However, these elements also provide hints for the identification of business assets, to be elicited during risk analysis management: for example, the availability (nondisruption) of a process or the integrity of some information. However, a number of additional elements cannot be expressed in such languages, such as those concerning who is depending on these assets, what goals are associated with these assets, and so on.

This is why we claim that a more expressive language, such as that provided by the *i** framework, needs to be considered for supporting a better exploration of business assets' properties and therefore achieving a better understanding of their criticality for the business.

7.4.2 Risk-Based Decision Process at the Business Goals Level

According to the first step of the risk-based decision process introduced in subsection 7.4.1, one has to proceed to a coarse estimation of the value of the most critical business assets, without considering the probability of risks associated with threats and vulnerabilities. For those assets, a qualitative analysis is done about the business impact of security risk on the overall economic value proposition.

The concept of *value* is receiving an increasing interest in the scientific community, in which a number of business models (as opposed to business process models) have recently been proposed on top of the original REA proposal (McCarthy, 1982). Some examples are

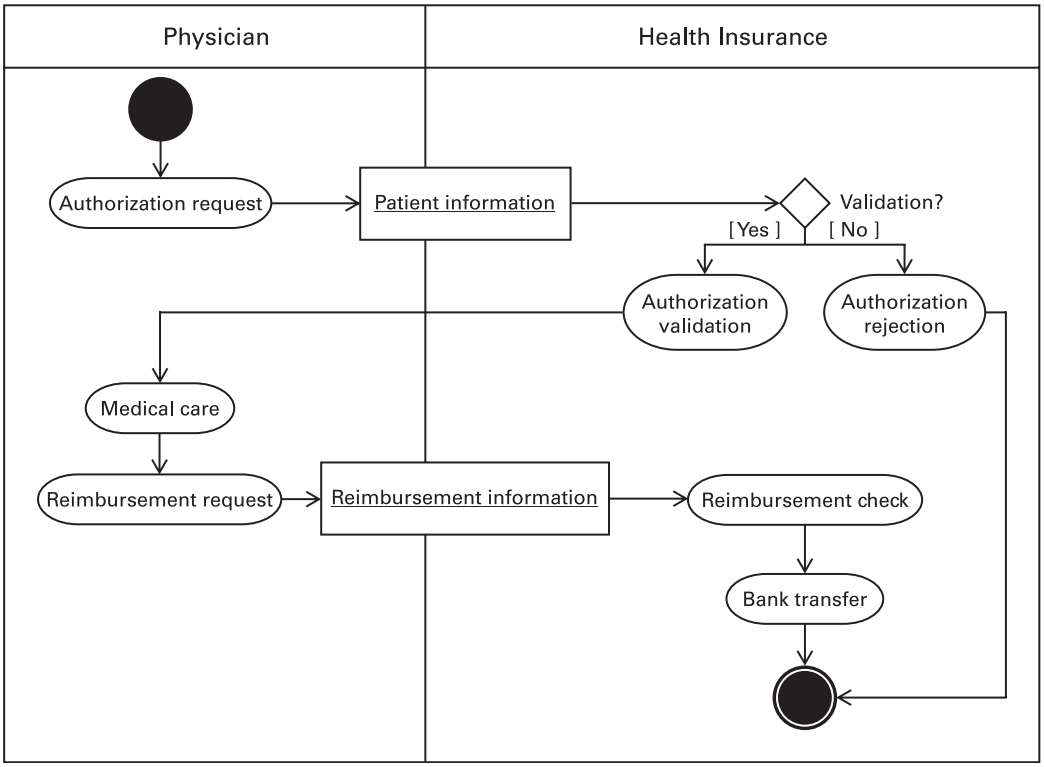

Figure 7.4
UML activity diagram of business process model of medical procedures reimbursement.

BMO (Osterwalder & Pigneur, 2003) and e3-value (Gordijn, Kartseva, Schildwacht, Wieringa, & Akkermans, 2004), which consider economic actors, economic relationships, and value objects exchanged (Schmitt, Grégoire, Ramel, Incoul, Brimont, & Dubois, 2005). Regarding e3-value, there has been some interesting initial work comparing it with the *i** framework (van der Raadt, Gordijn, & Yu, 2005). More specifically, Gordijn, Petit, and Wieringa (2006) emphasize the relation existing between *value propositions* expressed in e3-value and *strategic business goals* expressed in *i**.

In line with these approaches, the *i** Strategic Dependency (SD) diagram produced at this level makes the following explicit:

- The identification of business assets through the *dependencies* that exist among *actors* on information (*i** *resources*), processes (*i** *goals*), and activities—more detailed process steps—(*i** *tasks*). For example, a dependum could be related to information that is relevant for an actor or to the execution of a process that is critical within the value chain of an organization.

- The identification of value propositions associated with business assets. A value proposition is composed of a set of *i* softgoals* to which the correct handling of the business asset contributes. For example, in an organization, one can identify a specific process as being a business asset contributing to goals regarding the reduction of costs and the satisfaction of customers. The identification of softgoals is central in the way of reducing risks at the business level.
- The assessment of risk reduction is based on a qualitative assessment in which the *contribution* links (Chung et al., 2000) linking the business assets to the value proposition are identified. The assessment is composed of two parts. First, the qualitative importance of the contribution is considered (as in Castro et al., 2002; Chung et al., 2000): HELP/+, MAKE/++, HURT/−, BREAK/−− for, respectively, partial positive support, sufficient positive support, partial negative support, and sufficient negative support. Second, the assessment also depends on the qualitative importance of the target of the link.

We are relying on the *i** framework but with a slightly different interpretation than in the usual NFR framework. That approach aims at evaluating different alternative solutions against different softgoals. On the other hand, in our approach we are evaluating the *impact* of a correct handling of the business assets against the value proposition represented as a set of softgoals.

The overall risk-based analysis process sketched above is now instantiated to the case study and to the incremental elaboration of the *i** diagram.

The first stage of iterations of the risk-based process results is shown in figure 7.5. This figure should be considered as the business model produced by the Public Health Authority and is the result of discussions held with the stakeholders and of arbitration.

From this figure, one can read the following:

- The identification of one business asset associated with Patient information and three assets associated with the correct handling of three processes (Medical procedure authorization, Medical care, and Reimbursement). Among these assets, the focus is not on the Medical care goal but on the other two goals, Medical procedure authorization and Reimbursement, which are central in a positive support for the central softgoal Minimize administrative costs associated with an efficient use of the medical care budget.
- In terms of the assessment of the impact of a business asset on the value proposition, one can read that the correct handling of the Medical procedure authorization asset will have a sufficient positive impact in terms of contribution to Efficient medical care management, since there is now an a priori control of medical procedures (preventing, e.g., the execution of multiple similar procedures). It is also positively contributing to the Trust relationship between the Physician and Health Insurance, as well as to Respect for private life. However, it has a negative impact on Minimize administrative costs because there will be new costs associated with the implementation of this new process. Other value proposals and risk

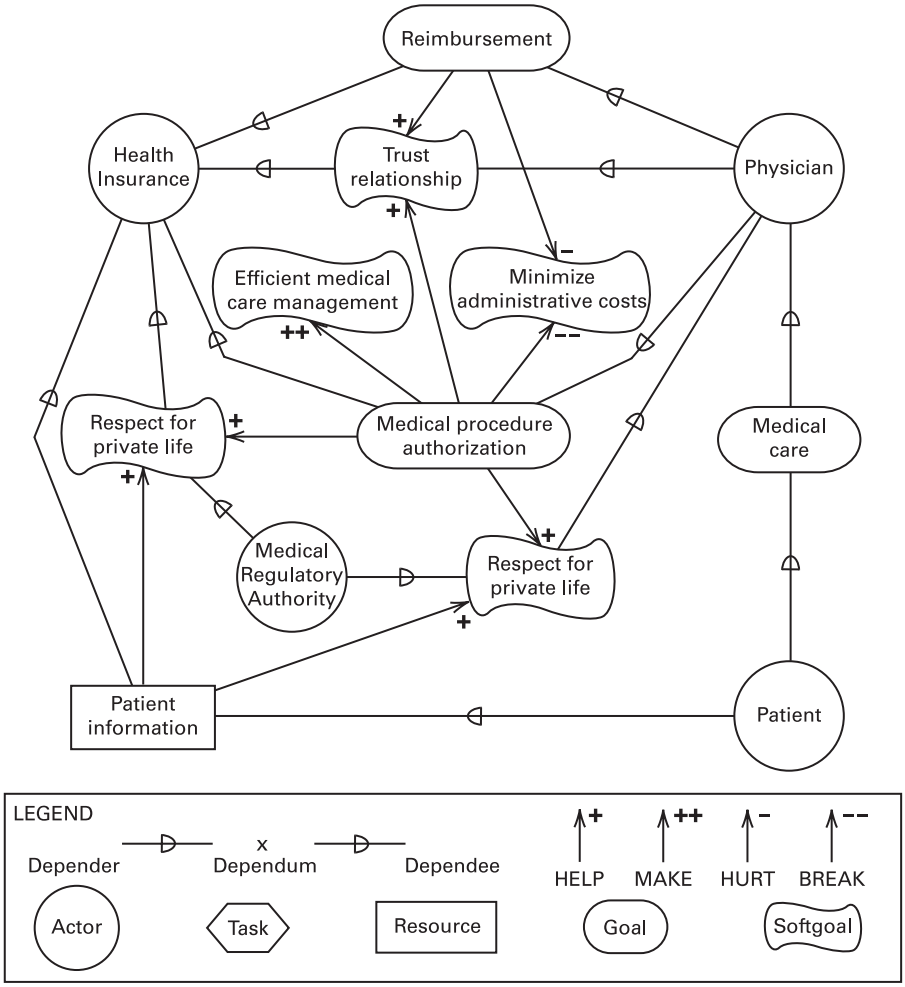

Figure 7.5
*i** SD diagram of the business assets and associated impacts.

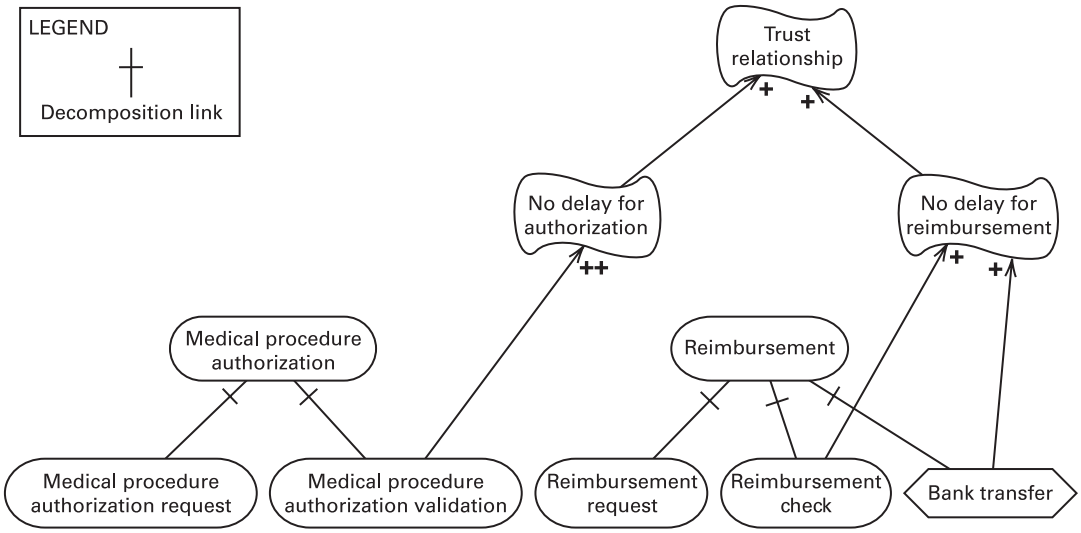

Figure 7.6
Goal decomposition.

assessments associated with Reimbursement and Patient information can be paraphrased in a similar way.

The risk management activity then continues by detailing the analysis of the two most critical goals cited following the first bullet: Medical procedure authorization and Reimbursement. This analysis results in goal decomposition (with decomposition links extended to goals, as in for example, Liu, Yu, & Mylopoulos [2003] and to softgoals, as in Castro et al. [2002]). Medical procedure authorization is decomposed into Medical procedure authorization request and Medical procedure authorization validation, and Reimbursement into Reimbursement request, Reimbursement check, and Bank transfer, as depicted in figure 7.6.

At the same time softgoals can be introduced. They can be associated with a new value proposition or, more often, with the refinement of elements of the original value proposition. For example, in figure 7.5, the Trust relationship to be maintained between the Physician and Health Insurance is improved if there is an efficient handling of critical medical procedure requests and a reduced delay in physician reimbursement.

7.4.3 The *i** SD Diagram and the Derivation of Security Objectives

When the risk-based decision process is completed at the business level, the analysis continues with elaboration of an SD diagram in which a new actor, corresponding to the

system to be put in place, is introduced together with its interface with the actors of its environment. In our case study, as shown in figure 7.7, we have introduced the Medical System in charge of managing the authorization of and reimbursement for medical procedures.

At this stage, similarly to security methods reviewed in section 7.2, we propose to elicit security objectives concerning the business assets identified so far. Different taxonomies of objectives are proposed by those methods. The most classical ones are confidentiality, integrity, and availability:

- Confidentiality: the property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- Integrity: the property of safeguarding the accuracy and completeness of assets
- Availability: the property of being accessible and usable upon demand by an authorized entity

More recent types of security goals are also commonly used, such as accountability or authenticity (ISO, 2004). As already demonstrated by multiple authors (Chung et al., 2000; Liu et al., 2002), security objectives can be easily mapped into *i** softgoals with the benefits of achieving a better structuring and of supporting (possibly formal) reasoning. Here, for modeling security objectives we choose to use the *security constraint* notation introduced in Bresciani, Giorgini, Mouratidis, and Manson (2004) and Mouratidis, Giorgini, and Manson (2003), defined as a constraint that is related to the security of the system.

For each asset, security constraints are identified for securing it. For example, in our case study, we identify the importance of handling the medical procedure authorizations as soon as possible, in order not to delay urgent medical procedures (implying the softgoal No delay for authorization). In terms of security, the result is the introduction of two security constraints dealing with Available medical system and Integrity answer (i.e., the integrity for ensuring the correct answer about the requested medical procedure). Because of lack of space, the complete identification of security objectives is not further detailed, but its completion results in the production of the *i** diagram presented in figure 7.7. The figure includes a number of security dependencies, the associated rationale for them being the following:

- Health Insurance depends on the Medical System for the Integrity of the answer (including non-repudiation). A bad authorization is critical, because it could provoke unauthorized medical procedures.
- Physician depends on the Medical System for its Availability. If the system is unavailable, Physician cannot do his or her job.
- Medical Regulatory Authority depends on the Medical System for Respect for private life, leading to the Confidentiality of medical procedures and patient information.

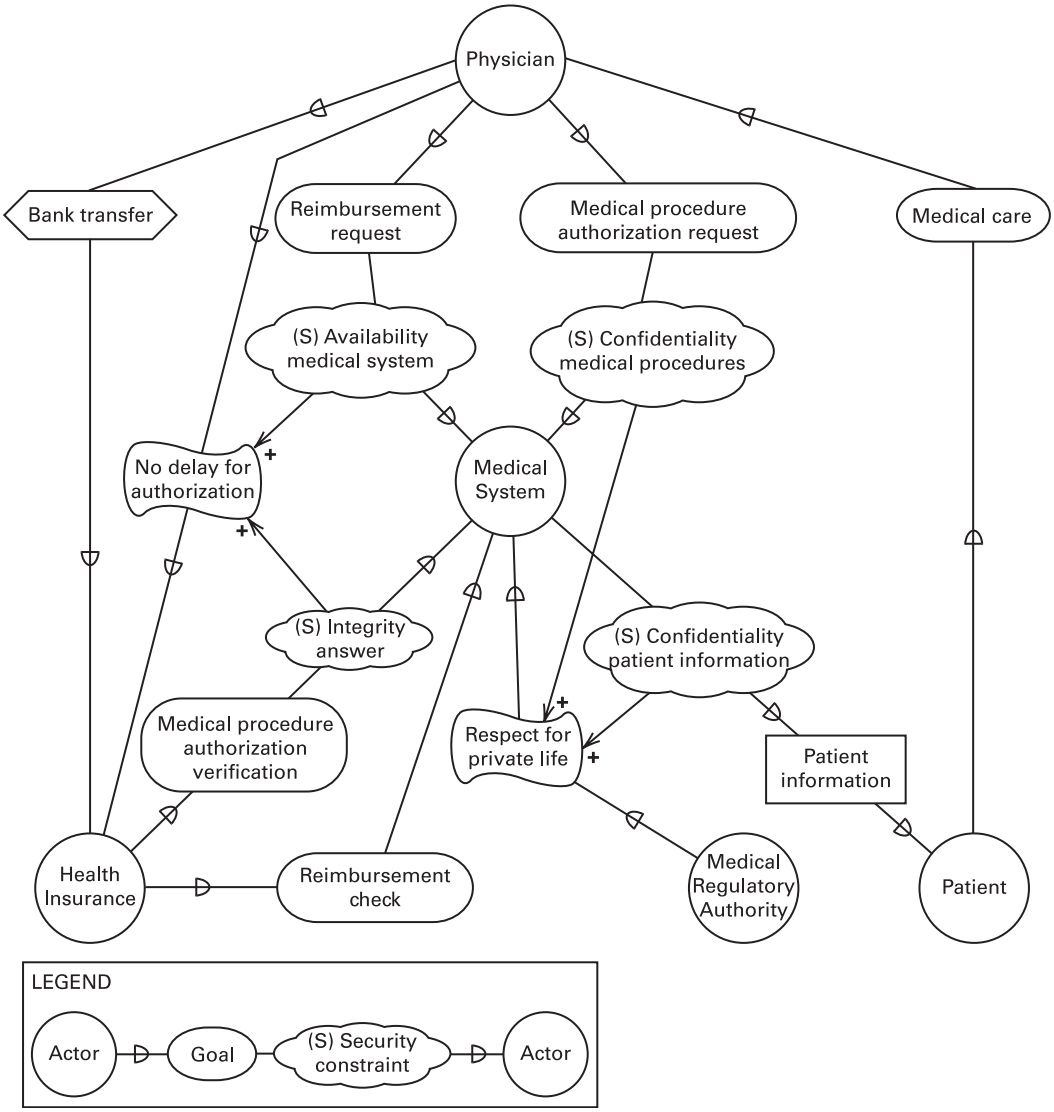

Figure 7.7
*i** SD diagram associated with the identification of security constraints.

It is interesting to note that the dynamics of the qualitative criteria that are assessed may change the ranking of risks to set the focus back to a higher abstraction level. For instance, after adding the aforementioned softgoals, the security risk impact that was revealed may qualitatively lower or raise the significance of the business softgoals introduced during the preliminary analysis. For instance, the qualitative assessment of the business impact of the penalties that could be imposed by the Medical Regulatory Authority (see figure 7.5) when there is noncompliance with its regulations about the confidentiality aspects of medical procedures (implying the security constraint Confidentiality medical procedures) may raise Respect for private life to the top of the assessment ranking.

7.5 High-Level Architectural Design and Identification of Security Requirements

7.5.1 IS High-Level Architectural Model

Progressing along the IS life cycle, the next focus is on the development of the IS architecture. According to software engineering best practices, a high-level architecture (sometimes called ''logical'' architecture or ''platform-independent'' architecture [OMG, 2001]) is first produced. In this architecture the logical modules associated with the management of the data and of the processing activities are represented, as well as the interactions between these modules through operations calls. Two typical diagrams produced according to UML-based methodologies at this level are a class diagram depicting static relations between objects and a sequence diagram associated with the dynamic invocation of operations. Figure 7.8 presents a sequence diagram for the Medical System, restricted to the authorization process in order to keep the diagram short. This expresses the nature of interfaces between the Medical System and its environment (made up of Health Insurance and the Physician), as well as the overall structure of the system in terms of two basic entities: the Authorization management entity deals with the processing of transactions associated with authorizations, and the Medical information entity keeps track of information exchanged about medical procedures for the management of these transactions (reconciliation of reimbursement request against the authorization answer). The Authorization management entity also keeps track of log histories (in case of disputes).

UML diagrams, as well as alternative notations such as ADL (Architectural Description Languages) and the ODP reference and architecture model (Linington, 1995), are useful notations for representing logical IS architectures. However, if they provide sufficient expressiveness for representing the ''how'' of the IS, we need to use additional *i** diagrams for reasoning on the link between the business and the architectural model, on the one hand, and on the elicitation of security requirements, on the other hand.

Figure 7.9 presents a new *i** diagram in which the business and the IS architecture are connected through a Strategic Rationale (SR) diagram.

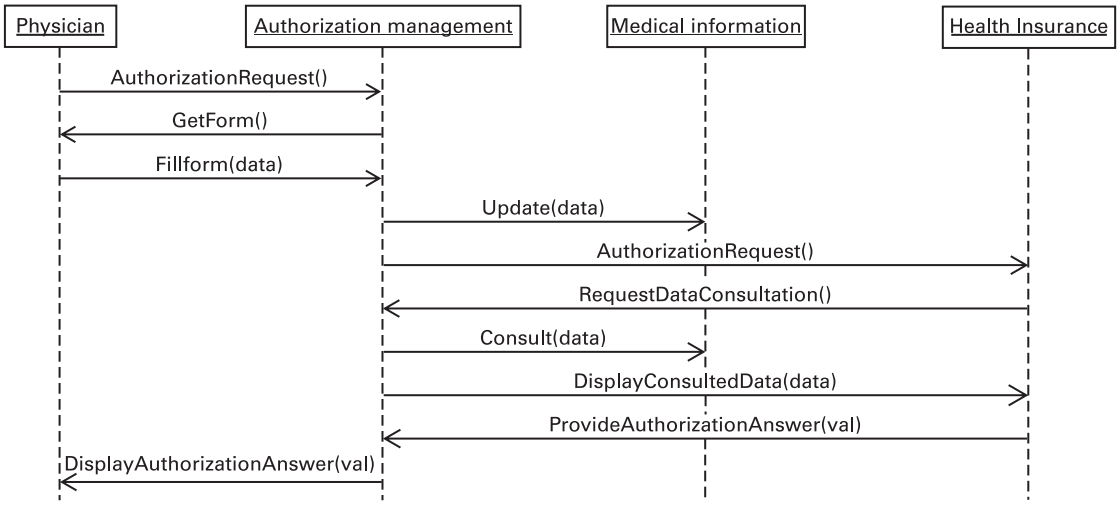

Figure 7.8
The UML sequence diagram associated with authorization part of the IS.

From this diagram, one can read that Authorization management (one of the basic UML entities in figure 7.8) is made up of a number of subtasks, one of which, Display patient data, is a "sensitive" task that directly contributes to Confidentiality patient information. Other dependencies between architectural artifacts and security goals are established at the level of Authorization answer and Authorization management, which contribute, respectively, to the Integrity answer and Confidentiality medical procedures security constraints. All IS artifacts that are related to those security business goals (which themselves are associated with business assets) correspond to IS assets (as opposed to business assets in the system's environment).

7.5.2 Risk-Based Decision Process at the Security Requirements Level

In the previous subsection we identified IS assets, such as get medical procedures, and their relation to security goals (also called security constraints), such as Confidentiality medical procedures. Now we have to translate such security goals expressed at the business model level in terms of equivalent subgoals expressed at the IS level. We will call such goals security requirements.

Security requirements do not need to be invented by the analyst, who can instead rely on a body of knowledge available in most of the methods presented in figure 7.2. For example, a list of security requirements is available in security standards such as ISO/IEC 27002 (ISO, 2005a) or Common Criteria (Common Criteria, 2006). Based on this available

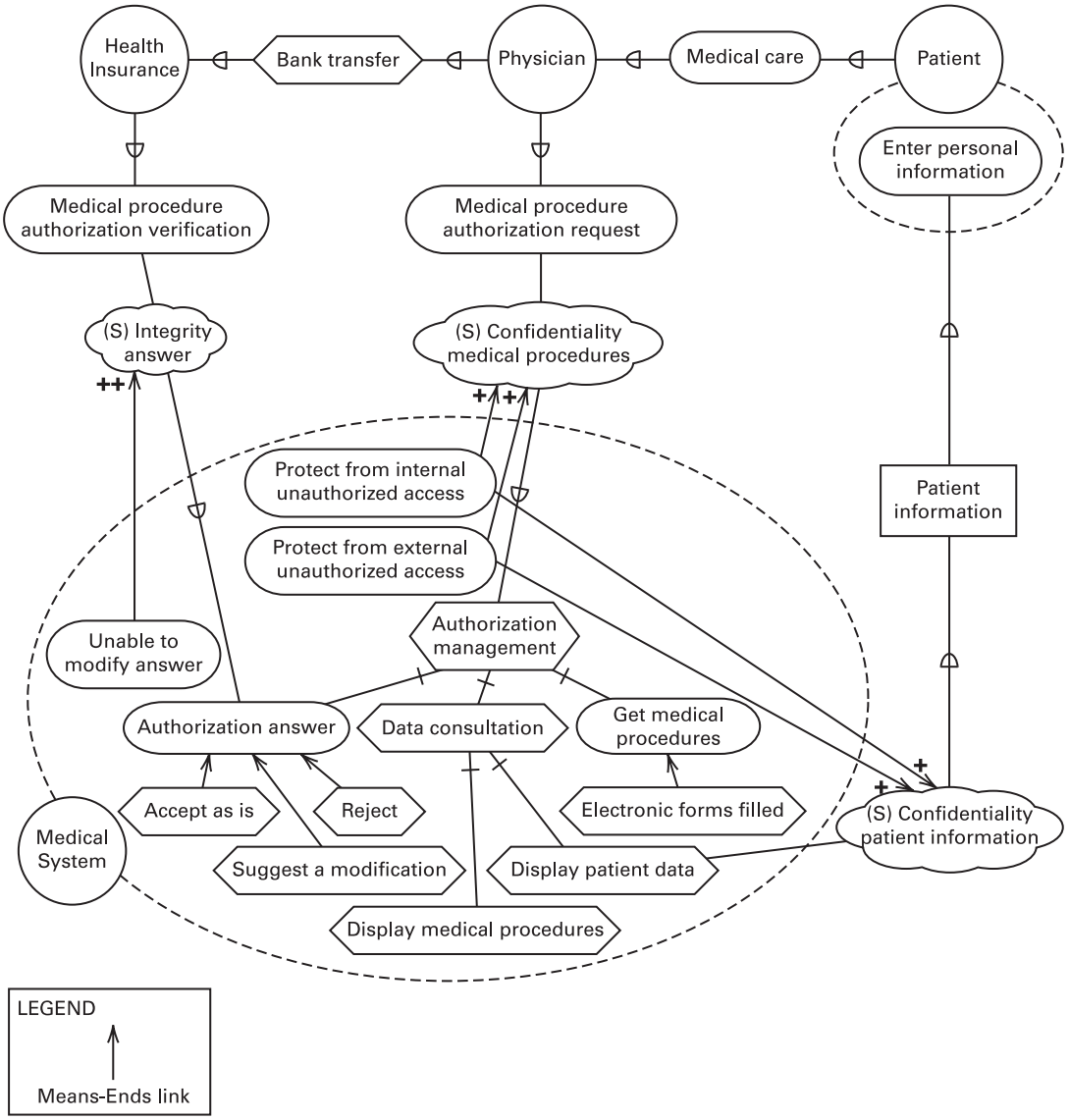

Figure 7.9
*i** SR diagram in which business and IS assets are linked.

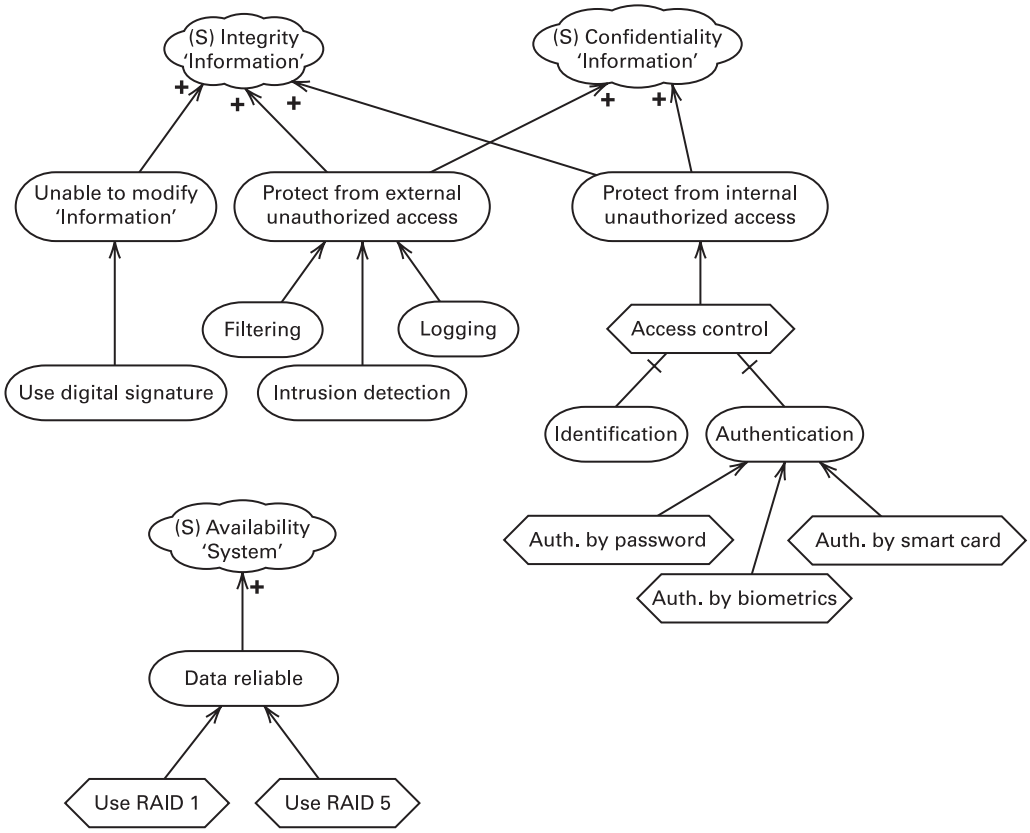

Figure 7.10
Goal tree refining security softgoals.

knowledge, one ongoing part of our research is concerned with the elaboration of security ''patterns'' according to which business security goals are decomposed in terms of finer security requirements. A fragment of the available patterns library is depicted in figure 7.10.

In this figure, it is explained that confidentiality of information is respected if the system is protected, on the one hand, from external unauthorized access and, on the other hand, from internal unauthorized access. These two goals are considered as positive contributions to the confidentiality of information softgoal. They also contribute positively to the softgoal of information integrity. Requirements can themselves be refined in terms of finer requirements and even implementation solutions. In figure 7.10, the requirements for protection from external unauthorized access can be refined in terms of requirements for filtering, intrusion detection, and logging (note that the proposed list of requirements is not exhaustive).

- Filtering: a preventive measure acting on external elements for controlling their access to a system
- Intrusion detection: a detection measure controlling access of external elements to a system
- Logging: a detection measure acting as a log on a system component

The goal tree also illustrates the proposal of implementation solutions for the security requirements. For example, it proposes three different tasks of authentication for implementing the requirement for access control: authentication by password, authentication by biometrics, and authentication by smart card.

From these available patterns the selection of the right requirements needs to follow a new iteration of the risk-based decision process. IS assets have been identified through their link with business security goals. These security goals are related to business assets that themselves have been assessed against different qualitative criteria. Using these links, we can therefore assess the risk associated with the IS assets. For example, in the architecture shown in figure 7.9, we can conclude that the topmost-ranked assessed risks concern the Medical procedures IS asset. This is due to the importance of the confidentiality constraint imposed during the second stage of iterations on the required medical procedures, but also due to the integrity constraint imposed on the authorization data, including the required medical procedures (i.e., the costs incurred in the diagnosis and restoration of corrupted data, which represents an additional IT cost to be considered as part of Minimize administrative costs).

When the main focus of concern is selected, a deeper analysis of the library of requirements patterns and of their contribution to the different security goals ends with the identification of the security requirement Protect from external unauthorized access on which the medical procedures depend. By incrementally assessing other risks (not shown), security engineers incrementally create the diagram of the most important security requirements, as shown in figure 7.9.

7.6 Detailed Secured Architectural Design

In the previous section, we derived the security requirements from a risk analysis based on a joint evaluation of the high-level security goals and of the preliminary design of the IS architecture. The next stage is then to perform an in-depth analysis of risks associated with the proposed detailed architecture, with respect to its conformance to the security requirements. It is at this stage that we will analyze the threats and vulnerabilities associated with the components of the architecture, and identify controls (i.e., the countermeasures that can be used for fulfilling security requirements).

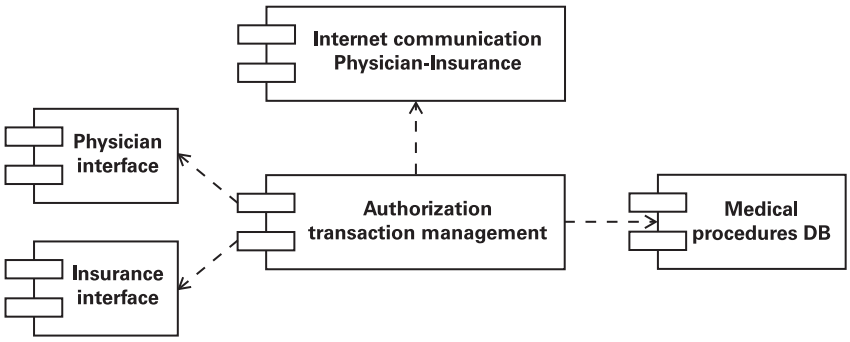

Figure 7.11
UML component diagram of the medical system.

7.6.1 Detailed IS Architectural Model

As in the previous IS development stages, models can also be produced for representing a functional view of the detailed architecture. These models basically represent the physical components of the detailed architecture together with their interrelations. If we decide to use a UML artifact, the component diagram is the usual artifact for representing this detailed architecture.

Figure 7.11 represents the physical architecture of the medical system. It is made up of dedicated interfaces for the Physician and Health insurance actors, a central Authorization transaction management component for authorization processing, and the Medical procedures DB. Finally, the figure also indicates that an Internet-based communication medium is used between actors.

Analogously to previous UML diagrams, this component diagram does not provide us with useful information about security concerns, nor about nonfunctional dependencies aspects. However, the identification of the components is of interest for refining the *i** diagram produced at the high-level architectural step so that dependencies among components can be analyzed. In the context of our case study, such a diagram is depicted in figure 7.12, which refines figure 7.9.

From this diagram we can see that Interface and Communication Phys. Ins. are dependent on each other for inputting and displaying data. The Interface is dependent on Authorization Transaction Management to do the required processing of the data entered, and Authorization Transaction Management depends on Communication Phys. Ins. for communicating the results of its operations. Finally, Authorization Transaction Management is dependent on the Medical Procedures DB for providing persistence of data and operations. Note that, due to lack of place, the Interface actor is not fully detailed.

The benefit of this diagram is that it establishes needed traceability links among the new IS assets identified at the detailed component level, the IS assets identified in the

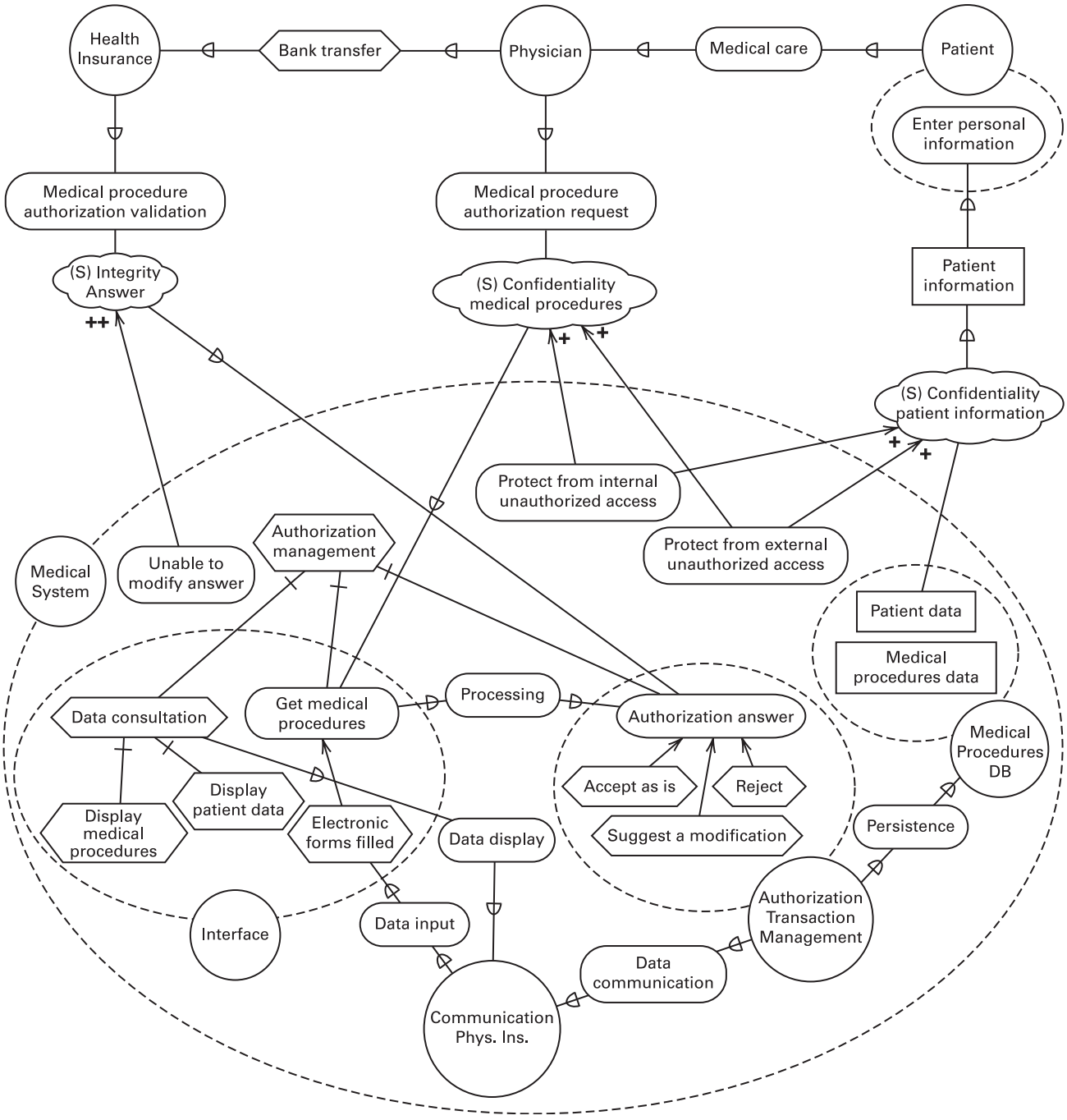

Figure 7.12
*i** SR diagram in which business and IS assets of the detailed architecture are linked.

preliminary architectural design, and the mirror of the IS assets in terms of business assets identified in the business domain.

7.6.2 Risk-Based Decision Process at Security Components Level

At the level of the IS detailed architecture, it is now possible to detail the security risks and give precise scenarios involving specific threats and vulnerabilities and resulting in specific impacts. This is done on the basis of the large body of knowledge that can be found in the most recent security risk methods such as the IT-Grundschutz Manual (BSI, 2004) or EBIOS (Direction Centrale de la Sécurité des Systèmes d'Information, 2004). For the sake of brevity, we will illustrate the approach on a single scenario associated with the Medical Procedures DB (see this component in figure 7.12). One can find a scenario with a high probability and a high impact on the confidentiality of data, in which the threat comes from a hacker who gains access to medical procedures due to a security hole in the database management system. Quantitative data can also be used to refine the qualitative data concerning the probability of the scenarios and the costs of the impacts. Thus, the qualitative criteria can be modified to take into account those quantitative data.[3] In the running example, the topmost-ranked assessed risks concern the actor Medical Procedures DB due to the high probability of the attack and the importance of its impact.

At this stage, the analyst can propose different solutions (countermeasures) for the Medical Procedures DB to be protected: either the firewall alone, or an intrusion detection system (IDS) together with a firewall, or for advanced protection, a logging tool in addition to an IDS and a firewall.

The selection of the adequate countermeasure includes an analysis that goes up to the business abstraction level and may take a couple of iteration cycles. In our example, the final decision is the selection of the second countermeasure (Firewall & IDS). This solution does not fulfill all the finer requirements associated with the Protect from external unauthorized access security requirements (see figure 7.10) because the logging facility is not supported. However, considering the two driving business softgoals involved at this stage, Respect for private life and Minimize administrative costs, the choice to limit Protect from external unauthorized access to Filtering and Intrusion detection is considered by the analyst as the best trade-off. In particular, using the Logging security requirement to complete Protect from external unauthorized access would improve the satisfaction of Respect for private life, but would negatively contribute to Minimize administrative cost.

7.6.3 *i** SR Diagrams Associated with Detailed Architectural Design

In order to support the risk-based reasoning presented in the previous subsection, we propose some *i** notational extensions for representing such reasoning that are inspired from preliminary work reported in Gaunard and Dubois (2003) and fully consolidated in Matu-

levičius et al. (2009). In figure 7.13, part of the scenario described in the previous subsection is reformulated in an *i** diagram that is explained as follows. A hacker can read medical procedures (*threats* are represented by diamonds) by using a Medical Procedures DB security hole (*vulnerabilities* are represented by diamonds with a black corner). The relation between the vulnerability and the threat is modeled by a positive contribution link, showing that the vulnerability provides a sufficient support for the achievement of the threat. A new link, called AFFECT, is used to connect the vulnerability with the corresponding IS asset: the medical procedures database. The *impact* of the threat on the security constraint Confidentiality medical procedures is also expressed with contribution links, showing that the constraint is fully denied with the achievement of the threat. Finally, security countermeasures are selected from the security goal tree (figure 7.10) to mitigate the risk. The mitigation is expressed with a negative contribution link, showing that requirements selected are strong enough to break the risk. The high-level security requirement Protect from external unauthorized access, composed of the Filtering and Intrusion detection security requirements, is therefore a positive contribution to the Confidentiality medical procedures and Confidentiality patient information security constraints.

But during the next steps of the risk analysis, some other risks could be elicited with an unacceptable level. If no sufficient mitigation measures are currently chosen in the architecture, some security requirements could be added, increasing the cost of the architecture; however, this may be necessary, considering the new assessment of the trade-off between the top business softgoals. Risk management is thus used as the tool for managing security and finding the best trade-offs between security and other softgoals.

Due to space restrictions, we cannot elaborate on the complete handling of the case study, but similar reasoning can be applied to the management of other security concerns by applying the same risk-based decision process on the security concerns. Full case studies can be found in the work of Mayer (2009).

7.7 Conclusion

In this chapter, our objective was to introduce the benefits of using the *i** framework in support of the improvement of a risk-based security management approach, performed in the context of a business/IT alignment perspective. Besides a better identification of business assets and IS resources, we have suggested how *i** diagrams can improve reasoning, from the early to the late stages of a secure IS development life cycle. In particular, we have explained how *i** diagrams can be produced and related together, within a traceability framework, linking business assets to security goals (or constraints), security goals to security requirements, security requirements to security vulnerabilities and threats attached to IS components, and, finally, to the identification of system security components acting as countermeasures to the identified risks. All along the production of the *i** diagrams at the different levels of abstraction, we have shown the importance of having a continuous

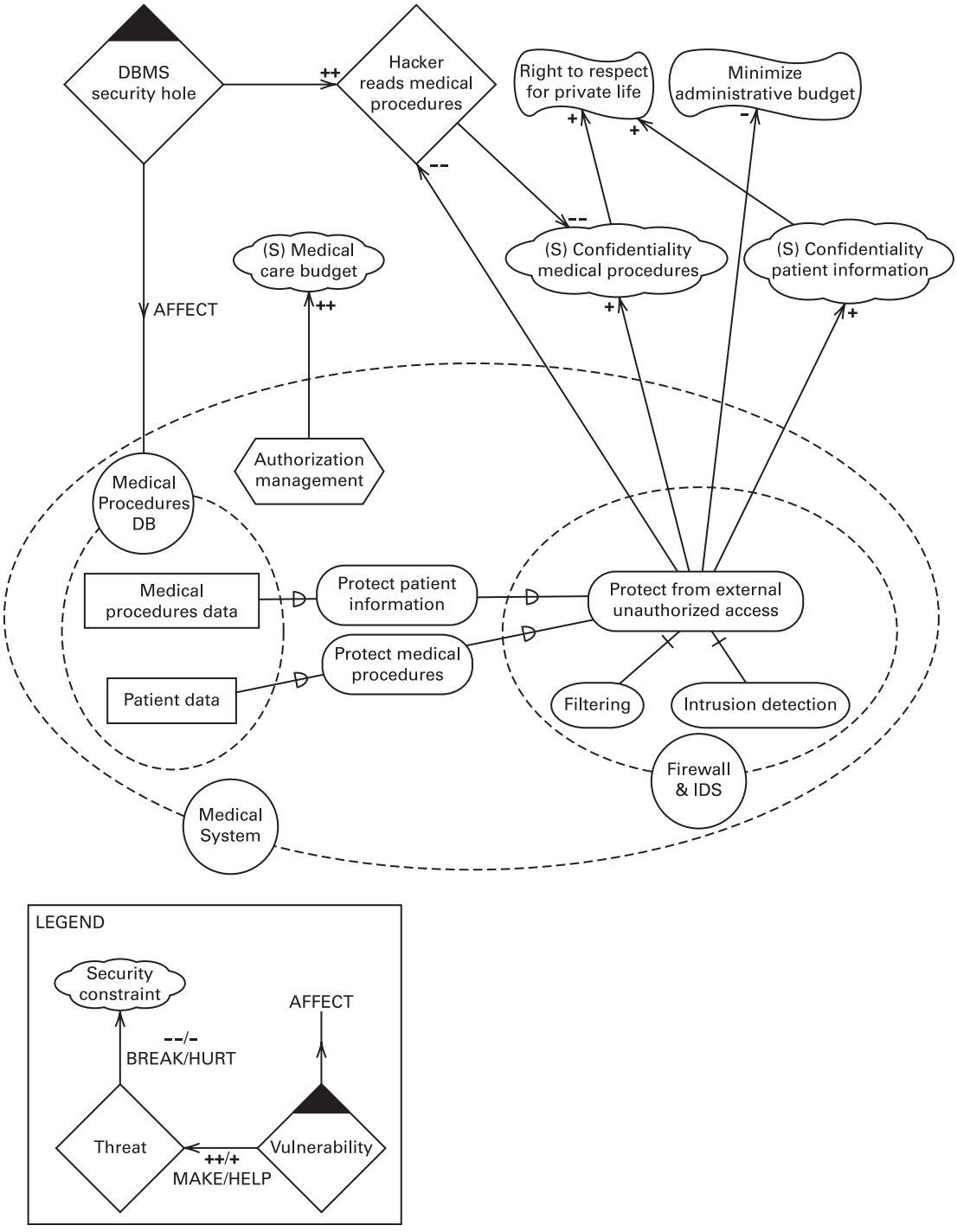

Figure 7.13
Threats and vulnerabilities notations.

risk-driven process that allows recording the rationale behind the decisions taken regarding risk mitigation, using a cost/benefit perspective.

Although the handling of the case study in this chapter seems sometimes to follow a top-down process (from security goals down to security software components), our experience indicates that this is never the case, since the reality shows an inevitable intertwining of the RE and architectural engineering phases. As further explained in Mayer et al. (2005), the analyst cannot identify all the security goals and requirements at the initial stage, and in most cases it is only when additional technical details are considered at the IS solution level that new requirements and new goals can be identified and handled at the RE level.

The use of the *i** framework for security modeling is not new. Liu et al. (2002, 2003) represent attacks as softgoals having negative contributions to security softgoals. Attackers are represented as malicious agents and vulnerabilities are identified as dependency issues. Other security modeling notations not based on the *i** framework are also relevant and pursue the same goal, for example, the work on extensions of use cases, such as misuse cases (Sindre & Opdahl, 2004) and abuse cases (McDermott & Fox, 1999). In these approaches, the focus is more on elicitation of new threats and vulnerabilities exploited by malicious actors.

CORAS (Fredriksen, Kristiansen, Gran, Stølen, Opperud, & Dimitrakos, 2002) is one of the very few approaches in which risk management issues are tackled through a model-based approach that is based on extensions to UML. On the basis of the *i** framework, Mouratidis, Giorgini, and Schumacher (2003) propose a pattern language for the development of secure systems based on the agent-oriented paradigm. This methodology stands on the Tropos approach and is called Secure Tropos (Mouratidis & Giorgini, 2006). It is based on a set of security patterns (Mouratidis, Giorgini, & Schumacher, 2003) and defines the concepts of security constraints and secure capabilities (Mouratidis, Giorgini, & Manson, 2003). Security concepts of criticality and complexity are presented in Bresciani et al. (2004). Our proposed approach is aligned with these works while complementing them with a systematic risk-based analysis that is used in an incremental and iterative manner. This view is largely inspired by the one proposed in traditional security methods such as OCTAVE, CRAMM, or EBIOS (Alberts & Dorofee, 2001; Insight Consulting, 2003; DCSSI, 2004). In line with the content of these approaches, we have introduced an extended *i** framework supporting more detailed reasoning over security risk management issues. This framework includes extensions of the *i** notation for dealing with threat and vulnerability issues. More details can be found in the work of Mayer (2009). At the RE level, another extension that we should consider is the one of trust, and similarly the enhancement to *i** proposed in Yu, Mylopoulos, and Lespérance (1996) and Castro et al. (2002), which defines concepts for modeling trust by the ownership link.

The joint usage of the *i** framework and of the risk-based analysis approach may help in answering a key question regarding the difficulty encountered in private companies in real

cases: producing *i** diagrams that tend to grow large and complex. Our preliminary answer is that the modeling process for creating *i** diagrams has to be adapted, because a necessary trade-off must be made between the large size of the diagrams and the time and budget allocated to the software engineering activities, which are decreasing every year in private companies. We think that a systematic risk analysis activity, performed at the early and late stages of IS development, can help in identifying where *i** diagrams are worth being produced for supporting a complex decision.

From ongoing real experiments, we can conclude that the use of our approach provides a finer-grained support to security risk management than most of the commercial approaches based on informal textual and "box and arrows" documents. Besides the application of the approach in the context of the development of a new system (as illustrated in this chapter), we have also experienced the benefit of using this approach on existing systems and improving documentation of the risk management process and control of risks afterward, which are, for example, main requirements for an ISO/IEC 27001 (ISO, 2005b) certification.

In terms of ongoing research, our concerns are related to the following:

- The development of a tool set supporting the proposed approach of which the kernel will be a repository whose schema will be the IS security risk management metamodel (Mayer, Heymans, & Matulevičius, 2007).
- The investigation of an adequate risk management component, central in the tool set and offering a set of advanced features like those developed by Feather and Cornford (2006) to support the design and development of complex systems.

Acknowledgments

This work was partially supported by the Research National Fund of Luxembourg, in the frame of the ACCES-PME project. Part of the research was performed within the context of the LIASIT (Luxembourg International Advanced Studies in Information Technologies) Institute.

Notes

1. Note that the judgment of business experts, as well as of technical experts, might be more important than the judgment of the users, and could be different from their usual involvement in requirements engineering.
2. Recall that when considering operational risk management (which includes security risk management), security risk analysis is itself a mitigation technique, and it must satisfy the same cost/benefit trade-off as any other risk mitigation.
3. The quantitative data can be used to define a more detailed qualitative scale with more confidence.

References

Alberts, C.J., & Dorofee, A.J. (2001). *Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) Method Implementation Guide Version 2.0*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

American Institute of Certified Public Accountants (AICPA). (2002). *Summary of provisions of the Sarbanes-Oxley Act of 2002*. Retrieved November 2, 2007, from AICIPA—Centre for Audit Quality Web site: http://thecaq.aicpa.org/Resources/Sarbanes+Oxley/Summary+of+the+Provisions+of+the+Sarbanes-Oxley+Act+of+2002.htm.

Basel Committee on Banking Supervision. (2004). *International Convergence of Capital Measurement and Capital Standards. A Revised Framework*. Basel, Switzerland: Bank for International Settlements Press & Communications. http://www.bis.org/publ/bcbs107a.pdf.

Bresciani, P., Giorgini, P., Mouratidis, H., & Manson, G. (2004). Multiagent systems and security requirements analysis. In C. Lucena, A. Garcia, A. Romanovsky, J. Castro, and P. Alencar (eds.), *Advances in Software Engineering for Multi-Agent Systems*. Lecture Notes in Artificial Intelligence 2940. Berlin: Springer.

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2004). *IT-Grundschutz Manual*. Retrieved November 1, 2007, from Federal Office for Information Security (BSI) Web site: http://www.bsi.bund.de/english/gshb/manual/index.htm.

Castro, J., Kolp, M., & Mylopoulos, J. (2002). Towards requirements-driven information systems engineering: The Tropos project. *Information Systems*, *27*(6), 365–389.

Carvallo, J.P. (2005). *Systematic construction of quality models for COTS-based systems*. Ph.D. thesis, Department LSI, Polytechnic University of Catalunya, Spain.

Chung, L., Nixon, B.A., Yu, E., & Mylopoulos, J. (2000). *Non-functional Requirements in Software Engineering*. Norwell, MA: Kluwer Academic.

Club de la Sécurité de l'Information Français (CLUSIF). (2004). *MEHARI Version 3, Concepts and Mechanisms*. Paris: CLUSIF Methods Commission.

Common Criteria. (2006). *Common criteria for information technology security evaluation version 3.1*. Retrieved November 1, 2007, from the Common Criteria Portal Web site: http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2.

Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI). (2004). *EBIOS—Expression of needs and identification of security objectives*. Retrieved November 1, 2007, from Information Systems Security special purpose server: http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html.

Dubois, E., Mayer, N., Rifaut, A., & Rosener, V. (2006). Contributions méthodologiques pour l'amélioration de l'analyse des risques. In T. Ebrahimi, F. Leprévost, and B. Warusfel (eds.), *Enjeux de la Sécurité Multimédia. Série Informatique et Systèmes d'Information*, IC2. (pp. 79–131). Paris: Hermes.

Feather, M.S., & Cornford, S.L. (2006). Relating risk and reliability predictions to design and development choices. In *Proceedings of the Annual Reliability and Maintainability Symposium* [RAMS] (pp. 492–498). Los Alamitos, CA: IEEE Computer Society Press.

Fredriksen, R., Kristiansen, M., Gran, B.A., Stølen, K., Opperud, T.A., & Dimitrakos, T. (2002). The CORAS framework for a model-based risk management process. In *Proceedings of the 21st International Conference on Computer Safety, Reliability and Security* [SAFECOMP'02] (pp. 94–105). London: Springer.

Gaunard, P., & Dubois, E. (2003). Bridging the gap between risk analysis and security policies. In D. Gritzalis, S.D.C. di Vimercati, P. Samarati, and S.K. Katsikas (eds.), *Security and Privacy in the Age of Uncertainty* (pp. 409–412). Berlin: Springer.

Gordijn, J., Kartseva, V., Schildwacht, J., Wieringa, R.J., & Akkermans, J.M. (2004). Developing a domain-specific cross-organizational RE method. In *Proceedings of the 12th IEEE International Conference on Requirements Engineering* [RE'04] (pp. 134–143). Los Alamitos, CA: IEEE Computer Society Press.

Gordijn, J., Petit, M., & Wieringa, R.J. (2006). Understanding business strategies of networked value constellations using goal- and value modeling. In *Proceedings of the 14th IEEE International Conference on Requirements Engineering* [RE'06] (pp. 129–138). Los Alamitos, CA: IEEE Computer Society Press.

Henderson, J.C., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, *32*(1), 4–16.

Insight Consulting. (2003). *CRAMM (CCTA Risk Analysis and Management Method) User Guide Version 5.0*. Walton-on-Thames, UK: Siemens.

International Organisation for Standardisation (ISO). (2004). *Information Technology—Security Techniques—Management of Information and Communications Technology Security. Part 1, Concepts and Models for Information and Communications Technology Security Management*. ISO/IEC 13335-1. Geneva: ISO.

International Organisation for Standardisation (ISO). (2005a). *Information Technology—Security Techniques—Code of Practice for Information Security Management*. ISO/IEC 27002. Geneva: ISO.

International Organisation for Standardisation (ISO). (2005b). *Information Technology—Security Techniques—Information Security Management Systems—Requirements*. ISO/IEC 27001. Geneva: ISO.

Jochem, R. (2003). Common representation through UEML: Requirements and approach. In K. Kosanke, R. Jochem, J.G. Nell, and A. Ortiz Bas (eds.), *Proceedings of the 12th International Conference on Enterprise Integration and Modeling Techniques* [ICEIMT'02] (pp. 371–379). IFIP Conference Proceedings 236. Norwell, MA: Kluwer Academic.

Linington, P. (1995). RM-ODP: The architecture. In K. Raymond and L. Armstrong (eds.), *Open Distributed Processing: Proceedings of the IFIP 3rd International Conference on Open Distributed Systems* (pp. 15–33). London: Chapman & Hall.

Liu, L., Yu, E., & Mylopoulos, J. (2002). Analyzing security requirements as relationships among strategic actors. In *Proceedings of the 2nd Symposium on Requirements Engineering for Information Security* [SREIS'02] (paper 5). http://www.sreis.org/old/2002/index.html.

Liu, L., Yu, E., & Mylopoulos, J. (2003). Security and privacy requirements analysis within a social setting. In *Proceedings of the 11th IEEE International Conference on Requirements Engineering* [RE'03] (pp. 151–161). Los Alamitos, CA: IEEE Computer Society Press.

Matulevičius, R., Mayer, N., Mouratidis, H., Dubois, E., Heymans, P. & Genon, N. (2008). Adapting Secure Tropos for security risk management during the early phases of information systems development. In Z. Bellahsene, and M. Léonard (eds.), *Proceedings of the 20th International Conference on Advanced Information Systems Engineering* [CAiSE'08] (pp. 541–555). Lecture Notes in Computer Science 5074. Berlin: Springer.

Mayer, N. (2009). *Model-based Management of Information System Security Risk*. Ph.D. thesis, University of Namur, Belgium.

Mayer, N., Heymans, P., & Matulevičius, R. (2007). Design of a modelling language for information system security risk management. In C. Rolland, O. Pastor, and J.-L. Cavarero (eds.), *Proceedings of the First International Conference on Research Challenges in Information Science* [RCIS'07] (pp. 121–132). Marrakech, Morocco: École Marocaine des Sciences de l'Ingénieur Press. http://www.farcampus.com/rcis2007/.

Mayer, N., Rifaut, A., & Dubois, E. (2005). Towards a risk-based security requirements engineering framework. In *Proceedings of the 11th International Workshop on Requirements Engineering: Foundations for Software Quality* [REFSQ'05] (pp. 83–97). Los Alamitos, CA: IEEE Computer Society Press.

McCarthy, W.E. (1982). The REA accounting model: A generalized framework for accounting systems in a shared data environment. *The Accounting Review*, *3*, 554–578.

McDermott, J., & Fox, C. (1999). Using abuse case models for security requirements analysis. In *Proceedings of the 15th Annual Computer Security Applications Conference* (pp. 55–66). Los Alamitos, CA: IEEE Computer Society Press.

Moffett, J.D., & Nuseibeh, B.A. (2003). *A framework for security requirements engineering*. Report YCS 368. Retrieved October 22, 2007, from University of York, Department of Computer Science's Web site: http://www.cs.york.ac.uk/ftpdir/reports/.

Mouratidis, H., & Giorgini, P. (2006). Secure Tropos: Dealing effectively with security requirements in the development of multiagent systems. In H. Mouratidis, D. Spears, A. Unruh, and M. Barley (eds.), *Third International Workshop on Safety and Security in Multiagent Systems: Selected Papers*. Berlin: Springer. http://sasemas.org/2006/sasemas2006_proc.pdf.

Mouratidis, H., Giorgini, P., & Manson, G. (2003). An ontology for modelling security: The Tropos approach. In *Knowledge-Based Intelligent Information and Engineering Systems: Proceedings of the 7th International Conference* [KES2003] (part *I*, pp. 1387–1394). Lecture Notes in Computer Science 2773. Berlin: Springer.

Mouratidis, H., Giorgini, P., & Schumacher, M. (2003). Security patterns for agent systems. In *Proceedings of the 8th European Conference on Pattern Languages of Programs* [EuroPLoP'03]. http://hillside.net/europlop/europlop2003/.

Nuseibeh, B.A. (2001). Weaving together requirements and architectures. *IEEE Computer*, *34*(3), 115–117.

Object Management Group (OMG). (2001). *Model Driven Architecture—A Technical Perspective. OMG Document ab|2001-02-04*. Needham, MA: OMG.

Object Management Group (OMG). (2007a). *Business Process Modeling Notation specification (BPMN 1.0)*. Retrieved November 30, 2007, from the OMG BPMN Web site: http://www.bpmn.org/.

Object Management Group (OMG). (2007b). *UML resource page*. Retrieved November 2, 2007, from OMG's Unified Modeling Language Web site: http://www.uml.org.

Osterwalder, A., & Pigneur, Y. (2003). Modeling value propositions in e-business. In N.M. Sadeh, M.J. Dively, R.J. Kauffman, Y. Labrou, O. Shehory, R. Telang, & L.F. Cranor (eds.), *Proceedings of the 5th International Conference on Electronic Commerce* [ICEC'03] (pp. 429–436). New York: ACM Press.

Rifaut, A. (2005). Goal-driven requirements engineering for supporting the ISO 15504 assessment process. In I. Richardson, P. Abrahamsson, and R. Messnarz (eds.), *Proceedings of the 12th European Conference on Software Improvement* [EuroSPI 2005] (pp. 151–162). Lecture Notes in Computer Science 3792. Berlin: Springer.

Schmitt, M., Grégoire, B., & Dubois, E. (2005). A risk based guide to business process design in inter-organizational business collaboration. In K. Cox, E. Dubois, Y. Pigneur, S.J. Bleistein, J. Verner, A.M. Davis, and R. Wieringa (eds.), *Proceedings of the First International Workshop on Requirements Engineering for Business Need and IT Alignment* [REBNITA 2005] (pp. 116–122). http://homepage.mac.com/karlalancox/documents/onlinefinalprocREBNITA2005.pdf.

Schmitt, M., Grégoire, B., Ramel, S., Incoul, C., Brimont, P., & Dubois, E. (2005). If business models could speak! Efficient: A framework for appraisal, design and simulation of electronic business transactions. In P. Bermus and M. Fox (eds.), *Knowledge Sharing in the Integrated Enterprise—Interoperability Strategies for the Enterprise Architect* (pp. 161–171). International Federation for Information Processing, vol. 183. New York: Springer.

Sindre, G., & Opdahl, A.L. (2004). Eliciting security requirements with misuse cases. *Requirements Engineering*, *10*(1), 34–44.

Van derRaadt, B., Gordijn, J., & Yu, E. (2005). Exploring Web services ideas from a business value perspective. In J. Atlee and C. Roland (eds.), *Proceedings of the 13th IEEE International Conference on Requirements Engineering* [RE'05] (pp. 53–62). Los Alamitos, CA: IEEE Computer Society Press.

Yu, E. (1997). Towards modelling and reasoning support for early-phase requirements engineering. In *Proceedings of the 3rd IEEE International Conference on Requirements Engineering* [RE'07] (pp. 226–235). Los Alamitos, CA: IEEE Computer Society Press.

Yu, E., Mylopoulos, J., & Lespérance, Y. (1996). AI models for business process reengineering. *IEEE Expert: Intelligent Systems and Their Applications*, *11*(4), 16–23.