Risk as Dependability Metrics for the Evaluation of Business Solutions: A Model-driven Approach

Yudistira Asnar
University of Trento
yudis@dit.unitn.it

Rocco Moretti
University of Bologna
moretti@cs.unibo.it

Maurizio Sebastianis
Think3 Inc.
sebastianis@think3.com

Nicola Zannone*
University of Toronto
zannone@cs.toronto.edu

Abstract

The analysis of business solutions is one of critical issues in industry. Risk is one of the most preeminent and accepted metrics for the evaluation of business solutions. Not surprisingly, many research efforts have been devoted to develop risk management frameworks. Among them, Tropos Goal-Risk offers a formal framework for assessing and treating risks on the basis of the likelihood and severity of failures. In this paper, we extend the Tropos Goal-Risk to assess and treat risks by considering the interdependency among actors within an organization. To make the discussion more concrete, we apply the proposed framework for analysis of the risks within manufacturing organizations.

1 Introduction

The definition of metrics for evaluating business solutions is challenging in industry. This is, for instance, the case for Think3 Inc.,[1] a company that supplies product development solutions, consulting services, and customer care to assist Small and Medium Enterprises' (SMEs) in the optimization of their product development processes. Specifically, Think3 has to provide business solutions consistently with the business strategy (e.g., product-oriented, order-oriented) chosen by the client. A strong demand from the clients is, in particular, the provision of solutions that guarantee the availability, reliability, and security of their procedures and IT systems. Service disruptions might be caused by malicious events (e.g., attacks), which are launched by attackers, or non-malicious events (e.g., accidents, errors, etc.), which are resulted from normal behaviors of users and IT systems within the organization. Ideally, Think3 should provide all safeguards necessary to protect their clients from both malicious and non-malicious events. However, this approach is very expensive and not applicable in practice.

In the last years, risk has been emerged as a metrics for prioritizing events. Risk, defined as the combination of the likelihood of an event and its consequences [11], depicts the criticality of an event in disrupting the system. Typically, analysts assess the risk of those events towards the system and allocate the resources for safeguards according to their criticality. Many frameworks have been proposed for risk management (e.g., [2, 4, 7, 8]), but most of them overlook to analyze the organizational setting where the system operates. An organization involves several actors in its operations. In such setting, actors can depend on others actors for fulfilling their goals. For instance, in manufacturing SMEs the production planning division is usually appointed to define the most suitable solution for the product. To achieve this goal, that division needs to consider the feedback from different sources, such as manufacturing, customer care, and marketing divisions. Accordingly, the production planning division depends on all those divisions for the feedback necessary to come up with the most suitable solution. A failure in fulfilling the assigned duty will affect the goal of the production planning. Thereby, the last needs to ensure that each division provides the necessary feedback. An appointed division may argue that it has accomplished the assigned duties taking low risks, but the adopted process may be still too risky from the perspective of the production planning. As a consequence, this division can adopt additional safeguards to mitigate risks. These issues demand the use of risk assessment frameworks able to identify, model, and evaluate risks also on the basis of the relationships among the actors within the organization.

This paper builds on the Tropos Goal-Risk (GR) framework [1], a formal framework that allows for tool-supported risk assessment and treatment selection. This framework extends the Tropos Goal Model [10] by adopting the idea of the three layers analysis introduced by Feather et al. [9] in their Defect Detection and Prevention (DDP) framework. These three layers are used to reason about uncertain events that obstruct business goals and to evaluate the effectiveness of treatments in mitigating such events.

The GR framework was initially developed for assessing

*This work was done when the author was at the University of Trento.
[1] Official web site of the company: http://www.think3.com

the risks of single actors during early requirement analysis. In this paper, we have extended it to assess and treat risks by considering also the interdependency among the actors within an organization. Through this extension analysts can assess the risk perceived by each actor, taking into account the organizational environment where the actor acts. Based on such analysis, we have provided a method to assist analysts in determining the treatments to be introduced in order to make risks to be acceptable by all actors.

An important objective for this work is also the evaluation of the expressiveness of the modeling language and the validation of the formal framework against industrial case studies. To this intent, we have applied the framework to analyze an intra-manufacturing integration model. In the TOCAI.IT project,[2] we have collaborated with Think3 for the elicitation of the core requirements of manufacturing SMEs [13]. Specifically, we applied Tropos [3] for the elicitation of such requirements on the basis of Think3's clients. Starting from that work, we have identified the risks affecting intra-manufacturing SMEs and the treatments that are usually adopted in industrial practices.

The paper is organized as follows. Next we present an intra-manufacturing integration model and the risk that can affect it. We then introduce the notion of risk and the risk management process (§3). Next, we give an overview of the GR framework (§4) and of the reasoning process behind it (§5). Then, we apply the GR framework to the intra-manufacturing integration model (§6). Finally, we discuss related work (§7) and conclude the paper (§8).

2 Intra-manufacturing SMEs

An intra-enterprise integration model is characterized by different divisions within the same organization (or of several organizations with strong synergies) collaborating for reaching common objectives or for executing specific processes. In the manufacturing domain, the objective is, in particular, the realization of a specific product. In the model presented in [13], we have mainly focused on activities concerning production planning, testing and correction of the products, achievement of a global efficiency, and reduction of costs and time-to-market. Such activities were reputed to be particularly significant by Think3.

Manufacturing SMEs can be partitioned into two main categories: *product-oriented companies* and *order-oriented companies*. The first category of companies is mainly involved in the production of a fixed set of products with a cost-quality trade-off. One of the client in this category is INTERPUMP,[3] a company operating in the hydraulic sector and producing high pressure piston pumps. The second category concerns the production of a variable set of products depending on the specific requirements given by customers. Such customers are willing to support higher costs because of the flexibility that they require. One of the client in this category is AROL,[4] a company producing closure systems.

As regards product-oriented companies like INTERPUMP, risk analysis has to deeply investigate aspects concerning how to "produce the product right", while for order-oriented ones like AROL the analysis considers the issues of producing the "right product". From a software engineering viewpoint, such concerns are similar with the concepts of *verification* and *validation* of a product, respectively. The former considers the compliance of the final product with its requirements, whereas the latter focuses on the acceptance of the final product by the client. In a product-oriented company, the acceptance process of the products by clients is not feasible due to the large set of products and clients to be considered. Similarly, it does not make sense for an order-oriented company to evaluate the compliance with the requirements of a product without considering its acceptance by a specific client.

Since our goal is to perform risk analysis on the core requirements for SMEs, the model presented in this paper is essentially a generalization of an organizational model for both product- and order-oriented companies. Such a model presents how the divisions in the same enterprise collaborate together achieving the objectives of enterprise and managing the level of risks in the enterprise.

3 Risk Management

The concept of risk is well known and several attempts to define it can be found in literature. In this work, we adopts the one proposed by ISO/IEC that defines risk as the "*combination of the probability of an event and its consequence*" [11]. Risk Management is the continuous process for systematically identifying, analyzing, treating, and monitoring risk throughout life cycle of a product or a service [12]. Risk Management comprises a number of coordinated activities to achieve this purpose, namely risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring (see Fig. 1[5]).

Risk assessment consists of risk analysis (identification and estimation) and risk evaluation. Starting from the identification of the business objectives of an organization, analysts identify the events that can obstruct such objectives. Analysts also define the description of the events (e.g., the impacts over the objectives or assets), and estimate their likelihood and severity over objectives and assets. Risk evaluation compares the result of risk estimation with defined risk criteria (e.g., costs, benefits, priorities, acceptable

[2] FIRB-TOCAI.IT RBNE05BFRK – http://www.dis.uniroma1.it/~tocai/

[3] Official web site of the company: http://www.interpumpgroup.it/

[4] Official web site of the company: http://www.arol.it/

[5] The figure is built based on ISO Guide-73:2002 [11] as baseline, and several adjustments following ISO 16805:2006 [12] and COSO-ERM [6].

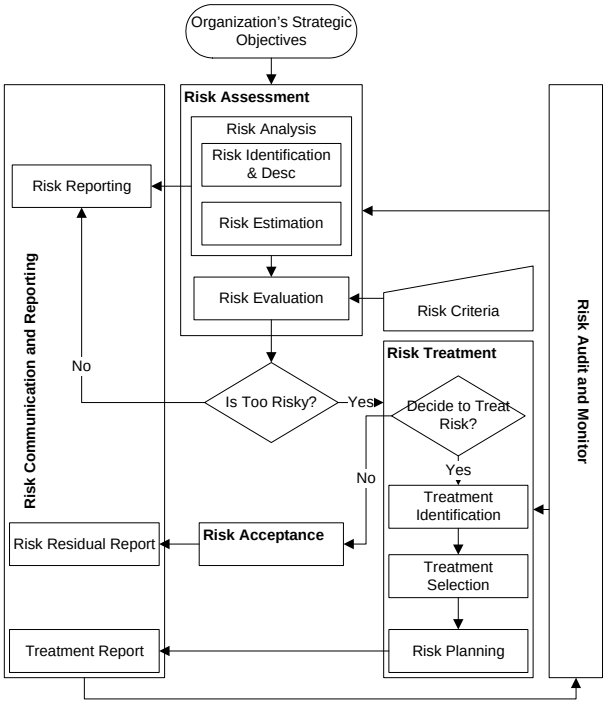

Figure 1. Risk Management Process

loss). In case the risk level is too high (i.e., it is beyond the risk tolerance that an actor can sustain), analysts perform risk treatment for identifying the treatments necessary to mitigate risks by reducing their likelihood or severity. Often the selected treatments are not sufficient to mitigate risks due, for instance, to a limited budget. Therefore, stakeholders may decide to accept risks. Risk acceptance thus intends to relax the level of acceptable loss by an actor. All these processes are reported for the purpose of communication among actors across the organization as well as for monitoring and auditing purposes.

In this paper, we mainly focus on the first two activities: risk assessment and treatment. In the following sections, we show how the identified concepts can be captured in the GR framework and the risk assessment and treatment process.

4 Tropos Goal-Risk Modeling Framework

4.1 Modeling Language

The Tropos Goal-Risk (GR) framework [1] consists of three conceptual layers – strategy, event, and treatment (see Fig. 2 in the Production Planning's viewpoint) – to assess the risk of uncertain events over organizations' strategies and to evaluate the effectiveness of treatments.

Strategy layer (previously called goal layer [1]) analyzes strategic interests of the stakeholders;

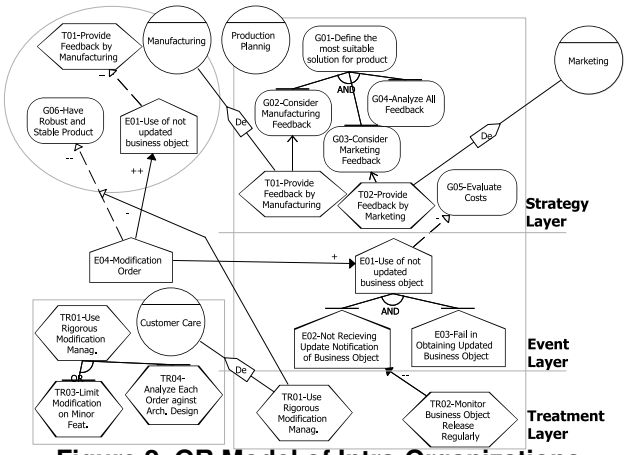

Figure 2. GR Model of Intra-Organizations

Event layer analyzes uncertain events along their impacts to the strategy layer;

Treatment layer analyzes treatments to be adopted in order to mitigate risks.

In this work, we have enhanced the GR framework by extending the conceptual model to assess the risk in a multi-actors setting. Accordingly, the (new) GR framework employs the concept of actor and dependency between actors besides the concepts of goal, task, and event. *Actors* (depicted as circles) are active entities that have strategic goals and perform tasks to achieve them. *Goals* (depicted as ovals) represent the objectives that actors intend to achieve. *Tasks* (depicted as hexagons) are courses of actions used to achieve goals or treat events. In the last case, tasks are also called *treatments*. Goals and tasks are characterized by attributes SAT and DEN, which represent the evidence of goals or tasks to be satisfied and denied, respectively. Their values are spanned in three qualitative values: *(F)ull*, *(P)artial*, and *(N)one*, with intended meaning $F \geq P \geq N$. Suppose that an actor A intends to achieve goal G, we denote the evidence of G in A's viewpoint as $Sat(A, G)$ and $Den(A, G)$. Goals and tasks are also characterized by attribute cost (denoted by $Cost(A, G)$ and $Cost(A, T)$, resp.), which represents the efforts (e.g., money, time) necessary to achieve a goal or execute a task. Finally, goals are also characterized by attribute utility (denoted by $Utility(A, G)$), which represents the utility-value generated by the fulfillment of goal G for actor A. Its values are in the range $[0 \dots 100]$. Suppose $Utility(A, G_{01}) = 80$, $Utility(A, G_{05}) = 40$, and $Utility(B, G_{06}) = 80$, we may conclude that actor A considers G_{01} as important (i.e., utility) as actor B does for G_{06}, and A considers G_{05} to be 50% less important than G_{01}. In this context, the *loss* introduced by risk, is represented as the reduction of utility (in terms of percentage). Accordingly, the *risk tolerance* of an actor is represented as the total loss accepted by an actor.

Events (depicted as pentagon) are used to represent uncertain circumstances that can affect goals or tasks in the strategy layer. Events are characterized by attribute Likelihood (denoted by $\lambda(E)$), which represents how likely an event occurs. Its values are defined as follow: *(L)ikely*, *(O)ccasional*, *(R)are*, and *(U)nlikely*, with the intended meaning $L > O > R > U$. The severity of events is captured by *impact* relations, which are explained below. Different from the previous two constructs (i.e., goal and task), events can be outside of actors' boundaries. Therefore, we distinguish between *global events* ($\mathcal{E}_G$), which are independent from actors, and *local events* ($\mathcal{E}_L$), which are events related to particular actors. In Fig. 2, event E_{04} is global, whereas event E_{01} occurs within a single actor. For instance, E_{01} can be less likely in the production planning than in the manufacturing since most updates are made by the production planning.

A GR model is a tuple of $\langle \mathcal{N}, \mathcal{I}, \mathcal{R}, \mathcal{D} \rangle$ where

- $\mathcal{N}$ is a set of nodes which is the union of *global events* $\mathcal{E}_G$ and pairs of the form (a, o), where
  - $a \in \mathcal{A}$, where $\mathcal{A}$ is the set of *actors* participating in the system;
  - $o \in \mathcal{O}$, where $\mathcal{O}$ is a set of objects that comprise *goals* $\mathcal{G}$, *tasks* $\mathcal{T}$, and *local events* $\mathcal{E}_L$.
- $\mathcal{I} \subseteq \big((\mathcal{A} \times \mathcal{E}_{\mathcal{L}}) \cup \mathcal{E}_{\mathcal{G}}\big) \times \big(\mathcal{A} \times (\mathcal{G} \cup \mathcal{T})\big)$ is the set of *impact* relations,[6] which are used to represent the severity of events ($\mathcal{E}_L$ and $\mathcal{E}_G$) on the strategy layer. Impact relations are distinguished into four types: $++$, $+$ to model opportunities (i.e., events with positive impacts), and $--$, $-$ to model risks (i.e., events with negative impacts). Impact relations introduce new evidence – DEN for negative relations and SAT for positive relations – to goals and tasks in the strategy layer depending on the likelihood of events and the type of impact relations as defined in [1].
- $\mathcal{R}$ is the set of relationship among GR constructs. They relate *source* nodes with a *target* node and are partitioned into
  - $\texttt{Dec} \subseteq 2^{\mathcal{N}} \times \mathcal{N}$ is the set of *decomposition* relations. There are two types of decomposition relation: AND and OR decomposition. AND decomposition is used to refine goals, tasks, or events into more refined structures. In Fig. 2, goal G_{01} is AND decomposed into goals G_{02}, G_{03}, and G_{04}. OR decomposition is used to model the alternatives to achieve a goal, to execute a task, or for the occurrence of an event. For instance, the treatment TR_{01} has two alternatives of execution (OR-decomposition), either TR_{03} or TR_{04}. Notice that source nodes must have the same type of target node. Moreover, decomposition relations are *intra-actor*, that is, the target and source nodes must be in the rationale of the same actor.[7]
  - $\texttt{Means-end} \subseteq (\mathcal{A} \times \mathcal{T}) \times (\mathcal{A} \times \mathcal{G})$ is the set of *means-end* relations, which identify the tasks used to satisfy goals. Means-end relations are intra-actor relations.
  - $\texttt{Contr} \subseteq \mathcal{N} \times \mathcal{N}$ is the set of *contribution* relations, which denote the side-effects of goals/tasks to the other goals/tasks/events. Contribution relations can be of 4 types: $++$, $+$, $--$, and $-$. Intuitively, the type represents the influence of a source node on the target node. Contribution relations can be either intra-actor or inter-actor since the fulfillment of an actor's goal can affect positively/negatively the fulfillment of goals (or the execution of the task) of another actor. These relations are also used to model the effect of treatments on the likelihood of events. For instance, the production planning division can adopt treatment TR_{02} to reduce the likelihood of event E_{02}.
  - $\texttt{Alleviate} \subseteq (\mathcal{A} \times \mathcal{T}) \times \mathcal{I}^{-}$ is the set of *alleviation* relations, which denote the mitigation of the (negative) impact of events due to the adoption of some treatment. Alleviation relations are distinguished into: $-$ and $--$.

  The formal semantics of these relations have been presented in [1]. Besides alleviation relations that affect the target impact relations, all other relations propagate evidence from source nodes to the target node.
- $\mathcal{D} \subseteq \mathcal{A} \times (\mathcal{G} \cup \mathcal{T}) \times \mathcal{A}$ is the set of *dependency* relations, which denote that an actor (the *depender*) depends on another actor (the *dependee*) for the fulfillment of a goal/execution of a task (the *dependum*). Intuitively, dependency relations bound the evidence of the depender to the evidence of the dependee about the dependum. For instance, the production planning depends on the manufacturing for the execution of T_{01}. Accordingly, the production planning has the same evidence of executing T_{01} that the manufacturing has.

4.2 Risk Assessment and Risk Treatment

In the previous section, we proposed a conceptual modeling technique for risk identification, description, estimation, and treatment identification. Here, we present a method that intends to assist analysts during risk assessment and risk treatment processes (Fig. 3).

[6] Impact relations have not been considered together with the other types of relations since they can act as target nodes of alleviation relations.

[7] If a target node is a global event, then all source events should be also global events.

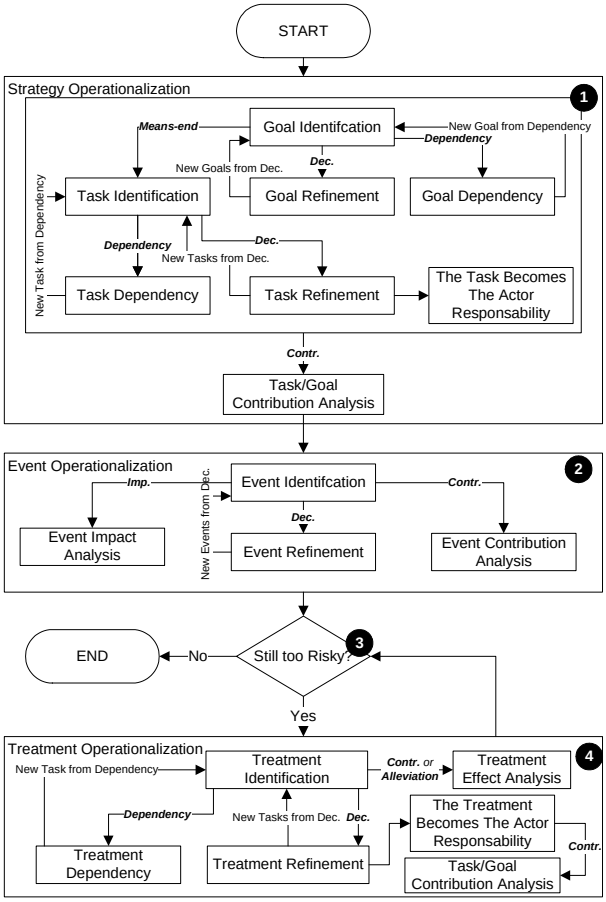

Figure 3. Assessment and Treatment Process

1. *Goal Operationalization* aims to analyze actors' goals and the tasks used to achieve them. First, goals are identified. Actors may not be able to fully achieve their goals by themselves, so they can either appoint other actors to fulfill them entirely or decompose them and assign part of them to other actors. Thus, goals are used as input for goal refinement or goal dependency. The tasks providing means for achieving goals are also identified in this phase. They are analyzed in a manner similar to that for goals. The first step of goal operationalization ends when all goals have been dealt with to the satisfaction of the actors who want them. Next step consists in analyzing the side-effects of a goal/task over other goals/tasks using contribution analysis
2. *Event Operationalization* aims to analyze events and their impact on the strategy layer. First, the events relevant for the application domain are identified and depicted in the event layer. These are then analyzed through refinement and contribution analysis. Finally, their impact over the strategy layer is described and their likelihood estimated. The framework allows analysts to model events with multi-impacts. This permits to do trade-off analysis when an event acts as a risk for some goals and as an opportunity for other goals. The event operationalization terminates when all events cannot be refined further and the likelihood of leaf-events is assessable;
3. *Risk Reasoning* calculates the risk level perceived by each actor in the organization. This process is explained in detail in Section 5;
4. *Treatment Operationalization* intends to refine the GR model in case the risk-level is higher than the risk acceptance defined by actors. First, treatments are identified along with the effect that their adoption leads to the mitigation of the risks. Analysts need to ensure that treatments do not introduce any unacceptable negative influences over the strategy layer. To this end, contribution analysis is used to model the influences of treatments on the strategy layer.

5 Reasoning Process

To verify if requirements are satisfied (i.e., the risk level is acceptable for every actor), we have developed algorithms to reason about risk on a GR model. The risk reasoning algorithms calculate the risk for every actor within an organization and evaluate whether or not the risk is acceptable for each actor. In case risks are higher than those accepted by actors, analysts can introduce treatments to mitigate such risks. The reasoner verifies whether the adopted treatments are sufficient to reduce the risk under a given threshold obstructing actors' objectives.

Before presenting the algorithms, let us briefly discuss about likelihood. Different from our previous works [1], we require the likelihood of events instead of their evidence values. The main reason for this change was that our industrial partners found more intuitive and practical to provide values in term of likelihood. To exploit our previous work, we have thus defined a mapping to translate likelihood into evidence values (Fig. 4).[8] Looking at such a mapping, one may argue that we have chosen a 4-value scale instead of a more "natural" 5-value scale. This choice was driven by the observation that our industrial partners often select the middle value. Conversely, having a 4-value scale enforce them to make a decision on the values.

The Risk Reasoning Process (Alg. 1) requires in input:

- a GR model $\langle \mathcal{N}, \mathcal{I}, \mathcal{R}, \mathcal{D} \rangle$;
- the *evidence values* – SAT and DEN – of tasks and goals;
- the *costs* of leaf nodes;
- the *utility* values of root goals;

[8] Likelihood values are converted into non-conflicted evidence (illustrated in bold in Fig. 4). These are evidence for which at least one of SAT or DEN is $None$.

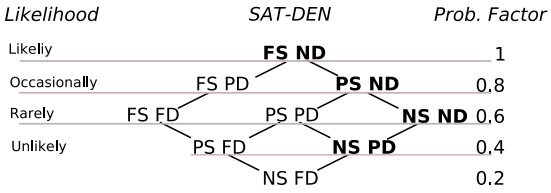

Figure 4. Evidence Mapping

Algorithm 1 Risk Reasoning

Require: $\langle \mathcal{N}, \mathcal{I}, \mathcal{R}, \mathcal{D} \rangle$, likelihoods, utilities, costs, risk_tolerance evidence_array

1: ev_evidence_array $\leftarrow convert\_likelihood(likelihoods)$
2: initial $\leftarrow$evidence_array $\uplus$ ev_evidence_array{concatenate evidence values of tasks-goals and events}
3: i $\leftarrow$0
4: **repeat**
5: **while** $old \neq current$ **do**
6: old $\leftarrow$current
7: **for all** $N_j \in \mathcal{N}$ **do**
8: current$_j$ $\leftarrow Update\_Label(N_j, \langle \mathcal{N}, \mathcal{I}, \mathcal{R}, \mathcal{D} \rangle, old, initial)$
9: **end for**
10: **end while**
11: **if** i=0 **then**
12: $\langle \mathcal{N}, \mathcal{I}', \mathcal{R}, \mathcal{D} \rangle \leftarrow Apply\_Alleviation(\langle \mathcal{N}, \mathcal{I}, \mathcal{R}, \mathcal{D} \rangle, current)$
13: $\mathcal{I} \leftarrow \mathcal{I}'$
14: current $\leftarrow$**nil**
15: **end if**
16: $i++$
17: **until** i=2
18: **if** $isAcceptable(\langle \mathcal{N}, \mathcal{I}, \mathcal{R}, \mathcal{D} \rangle, current, utilities, risk\_tolerance)$ **then**
19: **return** $\langle current, calculate\_costs(evidence\_array, costs) \rangle$
20: **else**
21: **return nil**
22: **end if**

- the *likelihood* of local and global events;
- the *risk tolerance* for each actor.

The algorithm starts converting likelihood of events into the corresponding values of evidence (line 1). It then runs through two loops. Specifically, *Risk Reasoning* calculates SAT and DEN evidence of nodes by invoking procedure *Update Label* that calculates the labels (i.e., the evidence values) of nodes on the basis of all relations among them (e.g., impact, decomposition, contribution, means-end, and dependency) following the idea of Giorgini et al. [10]. If a node has several incoming relations then the final labels of the node are defined as the maximum values. This procedure terminates when evidence values have reached the fix point (i.e., $old = current$).

During the first iteration, the procedure *Apply Alleviation* is executed to implement the influence of treatments on reducing the severity of events over the strategy layer (line 12). In other word, this procedure rewrites negative impact relations into the less severe ones. Then, *Update Label* is executed again to calculate the new values of evidence. Finally, procedure *isAcceptable* verifies that for every actor the expectancy utility loss (EUL) complies with its risk tolerance (line 18), where EUL is the ratio of the total utility-loss to the total utility (of root goals). If the risk level (i.e., EUL) is acceptable, the algorithm returns the final evidence values and the total cost of tasks (used to achieve the goals) and treatments (used to secure the goals) (line 19).

Event	product	order
engineering change request	R	L
modification order	U	L
production error	R	O
test failure and/or quality check failure	U	R
not respected deadline for the delivery of product	R	O
spare parts not found in the warehouse	R	O
(Production Planning, use of not updated business object)	U	O
(Marketing, use of not updated business object)	O	R
(Sales, use of not updated business object)	O	U
(Quality Assurance, use of not updated business object)	R	R
(Manufacturing, use of not updated business object)	U	R

Table 1. Likelihood wrt Business Strategies

6 Evaluation

We have applied the GR framework to analyze intra-manufacturing organizations. Specifically, we have assessed the risks affecting intra-manufacturing organizations when they employ different business strategies and identified the measures to be adopted in order to mitigate such risks with respect to the selected strategy. In this section, we report a summary of our experience.

In the TOCAI.IT project, we have elicited the requirements characterizing intra-manufacturing organizations and modeled them in Tropos [13]. Starting from such models, Think3 has identified the events that typically affect the business operations of manufacturing organizations and their impact on actors' goals (Fig. 5). However, such events can have a different likelihood depending on the strategy adopted by a certain organization. Table 1 reports the likelihood of events with respect to product- and order-oriented strategies. With the support of Think3, we have also identified the practices that are often adopted to mitigate the likelihood and impact of such events in industry (Fig. 5). Finally, Think3 has provided us with values concerning the utility of actors' goals and the cost of treatments.[9]

The results of the analysis are shown in Table 2. For each actor we report the total utility (TU) and risk tolerance (RT). We have calculated the expected utility loss when no treatments are in place (EUL_i) and when the treatments necessary to mitigate risks have been employed (EUL_f). We also have reported the cost of selected treatments.

It is worth noting that the order-oriented strategy is usually more risky than the product-oriented strategy. There are, however, some exceptions (e.g., the CEO and the Mar-

[9]Numbers have been obfuscated to maintain the confidentiality of Think3's client, but readers can still grasp the idea behind the framework.

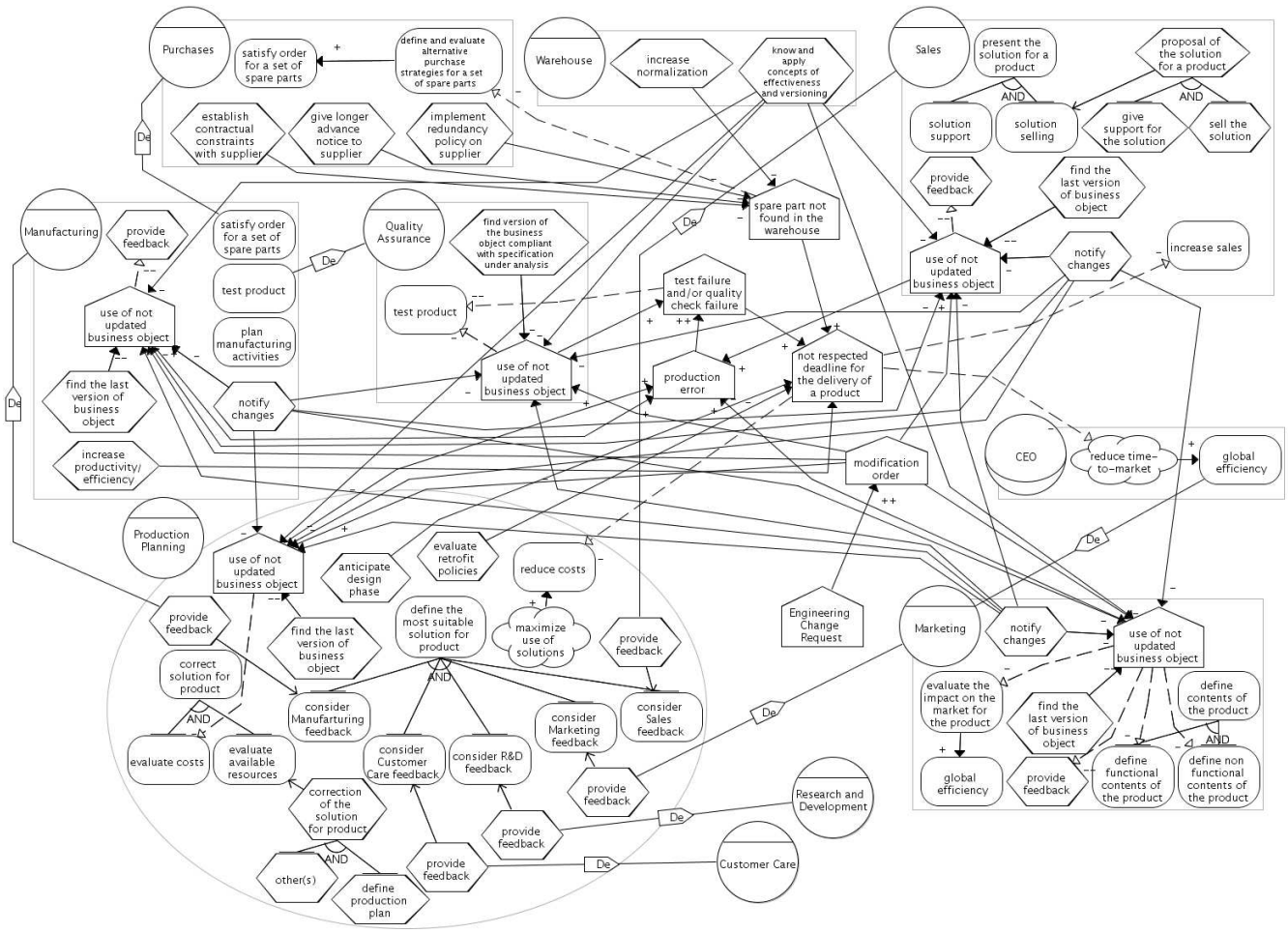

Figure 5. Intra-Manufacturing Organization Model including Events and Risk Treatments

Actor	TU	RT	Product			Order		
			EUL_i	EUL_f	Cost	EUL_i	EUL_f	Cost
Production Planning	230	0.05	0.148	0	110	0.2	0	150
Manufacturing	210	0.05	0.119	0	50	0.139	0	50
Sales	160	0.05	0.113	0	50	0.123	0	50
CEO	80	0.04	0.2	0	0	0.2	0	0
Purchases	50	0.10	0.129	0	40	0.2	0	40
Marketing	160	0.05	0.2	0	60	0.2	0	60
Warehouse	—	—	—	—	0	—	—	120

Table 2. EUL and total costs of treatments

keting). This mainly happens because of the dependency among events. Though the use of not updated business objects is more unlikely in Marketing in order-oriented companies than in product-oriented ones, in the former modification orders are more frequent and, consequently, the versioning of business objects is more critical.

In both strategies, we notice that it is more convenient (in terms of cost) for a company to enforce each division to notify changes rather than to employ systems for searching the last version of business objects. Indeed, the last solution is not always accepted by stakeholders. This is, for instance, the case of some Think3's clients. In their organization, each division has its own IT system so that it is necessary a network architecture to ensure interoperability among those systems. However, these architectures are usually very expensive and clients prefer to adopt a different solution.

The last finding, we mention concerns the lack of needed spare parts in the warehouse. One again, order-oriented companies are more sensitive by this event. Thereby, such companies have to adopt additional treatments to mitigate this event, for instance, by increasing normalization for stocks in the warehouse (see Table 2).

7 Related Works

Many approaches have been proposed for identifying products and systems enabling to support the coordination and cooperation in the intra-enterprise integration model for SMEs. For instance, Lindsey et al. [14] have studied the relationship between the organizational strategy and the effect of IT. Their work points out that a responsive infrastruc-

ture enabling to adapt and accept changes is essential to the strategic effectiveness of IT. According to McFarlan [15], IT may influence the competition by introducing barriers to the entrance of new competitors, changing the relationship between customers and suppliers, enlarging the basis of potential suppliers or strengthening the existent relationships, or even by creating new businesses. Finally, Pooley and Wilcox [16] have analyzed the application of IT for supporting the coordination of geographically-distributed teams. The development of such distributed environments can support decision making processes by means of the exchange of ideas and discussion.

In the risk analysis domain, there are several models that attempt to quantify uncertain events with likelihood and severity. Probabilistic Risk Analysis (PRA) [2] is widely used to assess risks quantitatively, while FMECA [8] proposes qualitative values (i.e., frequent, reasonable probable, occasional, remote, and extremely unlikely). Events are prioritized using the notion of "loss expectancy" which is defined on the basis the likelihood of events and their severity. This priority represents the criticality of an event. When resources are limited, analysts can decided to adopt countermeasures for mitigating events on the basis of their priority. Butler and Fishbeck recognized that many factors (e.g., reliable, available, safe, etc.) can be critical for a system and each of them has its own risks [4]. Based on this intuition, they proposed Multi-Attribute Risk Assessment to the improve the risk analysis process by considering multi-attributes. In fact, it simultaneously considers many factors like reliability, availability, safety and confidentiality by enabling analysts to find the right trade-off among these factors. The capability of choosing cost-effective countermeasures to deal with existing security threats using Multi-Attribute Risk Assessment is presented in [5]. Finally, the CORAS methodology [7] combines UML and Unified Process to support a model-based risk assessment. In particular, it proposes an integrated system development and risk management process for security critical systems.

8 Concluding Remarks

In this paper, we have enhanced the GR framework in order to assess and treat risk in organizational settings. This framework can be applied in different contexts. Here it has been used to assess risk affecting intra-manufacturing organizations and identify the treatments necessary to mitigate such risks with respect to different business strategy.

The GR framework with all new features presented in this paper is supported by the S&D Tropos Tool.[10] This tool is an Eclipse plugin developed to analyze security and dependability requirements of socio-technical systems. The tool provides requirements engineers with a graphical interface that allows them to draw GR diagrams. It also supports the automatic transformation of GR graphical models into formal specifications (expressed as SAT formulas) that allow for tool supported risk assessment.

[10] Available on the web at `http://sesa.dit.unitn.it/sistar_tool/`.

Acknowledgments This work has been partially funded by the EU-SERENITY project, by the FIRB TOCAI.IT project, by the PRIN-MENSA project, and by the Canada's NSERC Hyperion project.

References

[1] Y. Asnar and P. Giorgini. Modelling Risk and Identifying Countermeasures in Organizations. In *Proc. of CRITIS '06*, *LNCS 4347*, pages 55–66. Springer, 2006.

[2] T. Bedford and R. Cooke. *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge University Press, 2001.

[3] P. Bresciani, A. Perini, P. Giorgini, F. Giunchiglia, and J. Mylopoulos. Tropos: An Agent-Oriented Software Development Methodology. *JAAMAS*, 8(3):203–236, 2004.

[4] S. Butler and P. Fischbeck. Multi-Attribute Risk Assessment. Technical Report CMU-CS-01-169, Carnegie Mellon University, 2001.

[5] S. A. Butler. Security Attribute Evaluation Method: a Cost-Benefit Approach. In *Proc. ICSE'02*, pages 232–240. ACM Press, 2002.

[6] COSO. *Enterprise Risk Management - Integrated Framework*, 2004.

[7] F. den Braber, T. Dimitrakos, B. A. Gran, M. S. Lund, K. Stølen, and J. Ø. Aagedal. The CORAS Methodology: Model-Based Risk Assessment using UML and UP. In *UML and the Unified Process*, pages 332–357. Idea Group, 2003.

[8] DoD. Military Standard, Procedures for Performing a Failure Mode, Effects, and Critical Analysis. MIL-STD-1629A, 1980.

[9] M. S. Feather, S. L. Cornford, K. A. Hicks, and K. R. Johnson. Applications of Tool Support for Risk-Informed Requirements Reasoning. *CSSE*, 20(1), 2005.

[10] P. Giorgini, J. Mylopoulos, and R. Sebastiani. Goal-Oriented Requirements Analysis and Reasoning in the Tropos Methodology. *EAAI*, 18(2):159–171, 2005.

[11] ISO/IEC. Risk management-vocabulary-guidelines for use in standards. ISO/IEC Guide 73, 2002.

[12] ISO/IEC. Systems and software engineering – life cycle processes – risk management. ISO/IEC 16085, 2006.

[13] N. Kiyavitskaya, R. Moretti, M. Sebastianis, and N. Zannone. Project Report on the Initial Analysis of (Early) Requirements of Domain 1. TOCAI Deliverable D2.1, 2007.

[14] D. Lindsey, P. Cheney, G. M. Kasper, and B. Ives. TELCOT: An application of information technology for competitive advantage in the cotton industry. *MIS Quarterly*, 14(4):347–357, 1990.

[15] W. E. McFarlan. Information technology changes the way you compete. *Harvard Business Rev.*, 62(3):98–103, 1984.

[16] R. Pooley and P. Wilcox. Distributing decision making using Java simulation across the World Wide Web. *Journal of the Operational Research Society*, 51(4):395–404, 2000.