Assessing Risks and Opportunities in Enterprise Architecture using an extended ADT Approach

Sergio Sousa[*], **Diana Marosin**[†‡], **Khaled Gaaloul**[†] and **Nicolas Mayer**[†]
[*] *P&T Luxembourg, Luxembourg*
[†] *CRP Henri Tudor, Luxembourg*
[‡] *Radboud University Nijmegen, the Netherlands*
Contact: sergio.sousa@ept.lu, {diana.marosin, khaled.gaaloul, nicolas.mayer}@tudor.lu

***Abstract*—At every step in creating an enterprise design, architects encounter risks and opportunities. In most cases, risk assessment and treatment is done using the company's internal methodology or based on some best-practices known by the architect. We propose a method that can combine both qualitative and quantitative risk analysis and also incorporate risk mitigation solutions. In IT security, attack-defence trees (ADT) were used successfully to represent attacks and countermeasures. The goal of this paper is to leverage the ADT approach in order to assess risks and opportunities in enterprise architecture. To that end, we elaborate a framework to identify the best ways to mitigate risks and increase an enterprise's profitability based on architectural principles. This framework will be validated with a practical case study from the insurance sector.**

***Keywords*-Enterprise architecture, risk management, opportunities assessment, profits, ADT**

I. Introduction

Nowadays, more and more organizations make use of enterprise architectures to direct the development of the enterprise as a whole and its IT portfolio in particular. The core process of enterprise architecture consists of creating, applying, and maintaining the architecture for its intended purpose. By maintenance of architecture we understand both monitoring business and technologies and updating the enterprise architecture when relevant changes occur [1].

One of the many challenges an enterprise architect faces are risks that occur at every phase of development. Among other responsibilities of the architect we mention: determining impacts of alternative architectures, selecting frameworks and tools, assessing maturity of the process, managing quality of the enterprise architecture [2], defining the scope and risk of projects based on the needs and wishes of the stakeholders and operational risk management [3]. In The Open Group Architecture Framework (TOGAF) [4] each of the nine identified phases of the construction of an enterprise architecture has specific associated risks, therefore the need to identify and analyse risks, evaluate, respectively treat them. Also, at each step of a project opportunities can be encountered, therefore there is the need to act retroactively in order to benefit from them.

The Business Motivation Model (BMM) specification [5] suggests SWOT (Strength, Weakness, Opportunity, Threat) as an example of an approach for making assessments. In practice, enterprises can substitute different approaches, categorizing potential impacts as "risks"[1] and "potential reward"[2], therefore conducting a risk/benefit analysis.

Most of risk management methodologies are internal procedures for a company, like for example the ones found in the guidelines of the Washington State Department of Transportation [6], that "provide information on how project risk management fits into the overall project management process" and "provide guidance on how to pro-actively respond to risks". The main risk analysis is divided into a qualitative and quantitative approach: on the one hand, qualitative risk analysis assesses the impact and likelihood (high, medium, low) of the identified risks and develops prioritized lists of these risks for further analysis or direct mitigation. On the other hand, in quantitative analysis a numerical estimation of the probability that a project will meet its cost and time objectives is made. Quantitative analysis is based on a simultaneous evaluation of the impacts of all identified and quantified risks.

In parallel, in order to assess the risk associated with a given IT infrastructure, the IT security community developed the so called Attack-Defence-Trees (ADT) [7], [8], [9]. This method gives us a simple framework to assess how vulnerable our system is and which countermeasures need to be implemented in order to keep the (negative) impact, after suffering from an attack, under an acceptable threshold. A research into using defence trees in mixed qualitative and quantitative analysis for evaluation of security investments has already been made [10].

By exploring the capacities of ADTs this paper aims at giving a systematic, intuitive and well-defined risk analysis framework for enterprise architecture; thereby extending the scope of ADTs from IT security to risk management at the enterprise level.

[1]A "risk" is a category of Impact Value that indicates the impact and probability of loss [5].

[2]A "potential reward" is a category of Potential Impact that indicates the probability of gain [5].

We present the background of our research in section II. Further, we introduce the running example in section III. We use this example for the rest of the paper, enriching it iteratively. In section IV we introduce our risk management methodology and its extensions step-by-step. We present related work in section V. Conclusions and future research are presented in section VI.

II. Background

A. Enterprise architecture principles

Enterprise Architecture (EA) is generally considered to provide a good steering instrument to analyse the current state of the enterprise (As-is), identify and describe alternative future states (To-be), and guard the cohesion and alignment between the different aspects of an enterprise such as business processes and their ICT (Information and Communications Technology) support [11]. Architecture is a consistent whole of principles, methods and models that are used in the design and realization of organizational structure, business processes, information systems, and infrastructure [12].

Enterprise principles define the cornerstone of EA. There seems to be no universal agreement on the types of drivers that exist to motivate architecture principles [13]. Nevertheless, much inspiration can be found in various existing models and approaches. The BMM [14] provides important concepts to express motivation. The model was initially created to provide the motivations behind business rules, but can also be used to find the motivation for architecture principles. This idea was brought to enterprise architecture by Engelsman et al. [15] who state that architecture principles are based on an assessment of stakeholder concerns. An assessment represents the outcome of the analysis of some concern, revealing the strengths, weaknesses, and opportunities that may trigger a change to the enterprise architecture. In addition, the EA framework (TOGAF) provides principles such as enterprise principles, IT principles, enterprise mission and plans, enterprise strategic initiatives, external constraints, current systems and technology, and computer industry trends [16].

B. Attack-Defence-Trees

Attack trees are a well-known methodology for assessing the security of complex systems. An attack tree is a rooted tree representing an attack scenario. The root of an attack tree depicts the main goal of an attacker, and the other nodes constitute refinements of this goal into sub-goals. Two kinds of refinements are possible: conjunctive and disjunctive. The non-refined nodes, i.e., leafs of an attack tree, represent the so called basic actions which are used to build complex attacks.

Attack Defence Trees (ADT) are attack trees extended with defence nodes [8]. An ADT is a rooted tree representing an attack defence scenario, involving 1) actions of an attacker trying to compromise a system and 2) counteractions of a defender trying to protect the system. ADTs can also be seen as a game between an attacker and a defender. The player linked to the root node is called "proponent" and the other player is referred as the "opponent" [7].

A quantitative analysis of an attack defence scenario represented by ADTs is done with the help of attributes. An *attribute* expresses a particular property of an attack defence scenario, e.g., the minimal cost of an attack or the expected impact of a defensive measure. In [8] an evaluation method based on node attributes has been defined. The computation is performed in a bottom-up approach, the impact of each leaf node is approximated by experts or based on past experiences (i.e., brainstorming session). The non-leaf nodes are computed based on the attributes of their child nodes using two different functions, for disjunctively refined nodes, respectively for conjunctively refined nodes. Such an attribute domain has been defined as a structure $(\mathcal{V}, \nabla, \Delta)$ where $\mathcal{V}$ is a set of attribute values and $\nabla, \Delta : \mathcal{V} \times \mathcal{V} \rightarrow \mathcal{V}$ are the functions used to compute the attribute value of a disjunctive node and conjunctive node, given as input the attributes of its child nodes.

C. Synthesis

We believe that architecture principles present relevant inputs to build risks and opportunities assessment using ADT methodology in EA. Having a good steering instrument such as EA is very important to make conscious decisions about a future path design related to risk management and goal achievement. To that end, EA principles offer different means such as objectives and motivations to compute opportunities and risks using ADT where probabilities and impacts can be quantified. In the following sections, we present a motivation example comforting the aforementioned statement and explaining the benefit of an extended ADT in EA's profitability (e.g., cost reduction, data consistency).

III. Running example

In this section we briefly present the *ArchiSurance* case study. This case is inspired by a paper on the economic functions of insurance intermediaries [17], and is the running case used to illustrate the ArchiMate language specifications [18].

ArchiSurance is the result of a recent merger of three previously independent insurance companies: *Home and Away*, specializing in home owner's insurance and travel insurance, *PRO-FIT*, specializing in auto insurance and *LegallyYours*, specializing in legal expense insurance. The company now consists of three divisions with the same names and headquarters as their independent predecessors.

The merger has resulted in a number of integration and alignment challenges for the new company's business processes and information systems. These challenges appear

in the *ArchiSurance* baseline business, application, data and technology architecture.

The board's main driver (i.e., goal) is to increase its "Profit". Drivers motivate the development of specific business goals. Sub-goals such as "cost reduction" can be partitioned into the "reduction of maintenance costs" and the "reduction of personnel costs".

Architectural principles are defined as normative properties of all systems in a given context, or the way in which the goals are realized. TOGAF defines a principles catalogue to provide an overview of principles and a guide for good practices. The relations between goals and principles can be modelled as described in Figure 1. The company needs "single data source" in order to fulfil "data consistency", and commit either to "single data source" or "common use application" to ensure "reduction of maintenance costs".

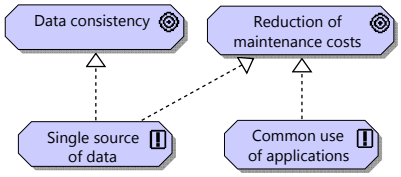

Figure 1: "ArchiSurance" - architectural principles [18]

IV. Framework

Inspired by ADTs, we introduce our approach for planning and risk/opportunity assessments step by step. We differentiate ourselves from the ADT approach by the fact that in our framework, a tree represents a plan, not an attack. We introduce opportunity nodes, not just threats, and an exclusive disjunctive relation between them. Also, we adopt an iterative approach, on three abstraction levels. We enrich the example introduced in previous section. We present how, by executing actions strictly linked to architectural principles, a company can achieve a strategic goal.

A. *Using Trees to Assess Expected Enterprise Performances*

A plan of an enterprise architecture includes the stakeholders (strategic) goals and the means to achieve them: each goal is depicted in sub-goals or atomic planning phases, the architectural principles the company should follow in order to achieve the goals and the atomic actions that need to be taken. A plan can be represented as a tree. A root node represents a strategic goal of the stakeholders. The children nodes represent architectural principles or sub-goals. Each child of the tree can be refined as follows:

- A **conjunctively** refined node is satisfied if all its children are fulfilled.
- A **disjunctively** refined node is satisfied if at least one of its children is fulfilled.
- An **exclusive disjunctively** refined node is satisfied if only one of its children is fulfilled.

Note that an exclusive refinement of a node represent a decision, since choosing one options automatically contradicts the other. A non-refined node of the tree is called a leaf. A leaf node represents one atomic phase of the planning. It can be an atomic action or it can be a whole phase of the project. The scope of this paper is to focus on atomic actions.

Graphical representation: Nodes of the tree are represented with circles. In order to distinguish between refined nodes, we connect the edges pointing from the children of a conjunctively refined node with an arc, and the edges pointing from the children of a exclusive disjunctively refined node with a crossed-arc. The disjunctive nodes remain unconnected (see Figure 2).

B. *Evaluation of a Planning Tree*

In section II we have introduced the foundations of ADTs. The bottom-up evaluation method has proven its efficiency and has been adapted to ADTs and defence trees in [10], [9]. Our aim is to enrich this method and apply the bottom-up evaluation to planning trees.

The main difference between attack trees and planning trees is the presence of a third type of refinement: the exclusive disjunction. Therefore, the attribute domain of a planning tree is defined as a structure $(\mathcal{V}, f_\wedge, f_\vee, f_{\underline{\vee}})$, where $\mathcal{V}$ is the set of possible attribute values, $f_\wedge : \mathcal{V} \times \mathcal{V} \to \mathcal{V}, f_\vee : \mathcal{V} \times \mathcal{V} \to \mathcal{V}$ and $f_{\underline{\vee}} : \mathcal{V} \times \mathcal{V} \to \mathcal{V}$ are the functions used to compute the attribute values associated with a node based on the attributes of its refined nodes (children), that are found respectively in a conjunctive, disjunctive, exclusive-disjunctive relation . Similar to attack trees, the attribute values of the leaf nodes, need at first to be approximated or computed by experts in the domain.

Definition 1. (Benefit) The set of possible benefits $\mathcal{B} \subseteq \mathbb{R}$ of an atomic planning phase represents the set of revenues that can be generated in case of a successful execution of a task. If an action leads to a monetary loss, we represent this as a negative benefit. In order to evaluate the maximal benefit that can be reached given a specific planning tree and the benefits associated with its atomic phases, we need to define a metric $(\mathcal{B}, (f_\wedge, f_\vee, f_{\underline{\vee}}))$.

Let $b_N \in \mathcal{B}$ be the benefit associated to a node N with c child nodes, and let $\mathcal{B}_C = \{b_1, ..., b_c\}$ denote the benefits associated to the child nodes of N. Depending on the nature of N (conjunctive, disjunctive, exclusive disjunctive), we compute the benefit b_N with one of the following functions:

$$f_\wedge(\mathcal{B}_C) = \sum_{b_i \in \mathcal{B}_C} b_i \qquad f_\vee(\mathcal{B}_C) = \sum_{b_i \in \mathcal{B}_C} b_i$$

$$f_{\underline{\vee}}(\mathcal{B}_C) = \max_{b_i \in \mathcal{B}_C} b_i$$

ArchiSurance example:
Considering the example introduced in section III, the

resulting planning tree for achieving the goal "Profit" is represented in Figure 2. We mark the nodes that represent actions, and their value is evaluated a-priori in grey.

Afterwards, using the formulas presented in Definition 1 we compute the overall expected benefit of the project. Only action nodes/atomic planning phases have associated benefits (grey nodes); architecture principles represent the rationalization of *why* a certain action is performed, in order to support the realisation of goals.

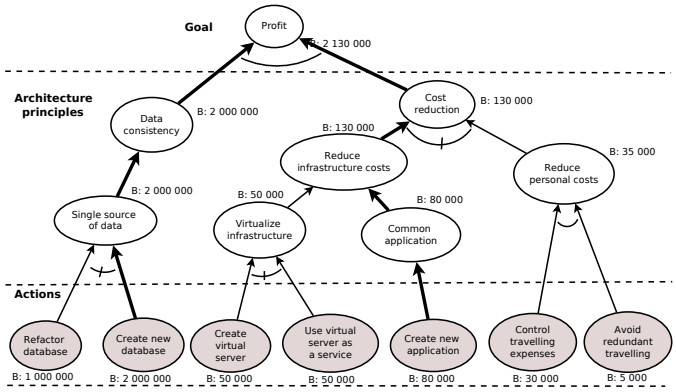

Figure 2: "ArchiSurance" - plan for achieving the goal "Profit" and computed overall benefit

Note that this method does not only provide an overall value for the expected benefits of the project, it also gives a decision process and suggests the choices to be performed in order to maximize the achievement of goals (bolded lines in Figure 2).

We assume that no uncertain event can make our plans fail. In case of an *and*-node all the children need to be completed to satisfy parent goals. The benefit of such an *and*-node is the same as the sum of the benefits of all its children.

In case of an *or*-node not all the refined nodes need to be satisfied, but all can be completed. In the best case all the benefits will be acquired and the value of the parent will be the sum of all refined children's benefits.

The *xor*-node has the particularity that a choice needs to be performed in order to achieve the highest possible benefit (only one of the refined nodes can be executed). In this case we perform the action associated with the child node that brings the highest benefit and thus a *xor*-node will be associated with the maximum benefit among its children's benefits.

C. Actions-Threats-Opportunities

It is often the case that a plan is impossible to follow *ad-literam*, given the changes that constantly occur from the environment: technology can change, costs can increase, employees can quit, etc.. At each stage in the execution of a plan, we can encounter such changes, which can be translated in either risks (i.e., financial crises) or new opportunities (e.g., new investments, increase of actions value) for the company. Therefore, we introduce the following extensions to the plan, in order to accommodate these characteristics.

Definition 2. (ATO tree) An ATO (Actions-Threats-Opportunities) tree is a rooted tree representing a planning scenario during an enterprise change, in the presence of environmental threats and the probability of occurrence of opportunities.

Each node of the ATO tree may have one or more children of the following types:
- an **opportunity node** represents the unexpected event to achieve a benefit in a atomic phase of the project
- a **threat node** represents the likelihood to encounter a risk in a certain atomic phase of the project

We limit our discussion to threats and opportunities of the leaf nodes. The mechanism can easily be extended to sub-trees and planning phases, not just atomic actions.

Each atomic action can have multiple threats or opportunities associated to it, represented by an *or*-relation. Each of the associated threats or opportunities can occur independently of one another, although these concepts can be further refined and analysed. For simplicity, in this paper we consider atomic threats and opportunities.

Graphical representation: Opportunities are represented as hexagons, whereas threats are represented as rectangles (see Figure 3).

D. Evaluation of the ATO Trees

The evaluation of ATO trees is done in two steps. First a planning tree is designed and evaluated. In a second step specialists and stakeholders analyse the leaf-nodes of the planning tree and determine if there are possible threats or opportunities on each node. This second analysis aims at adding the existing threats and opportunities to the planning tree and approximating the impact of these with respect to the chosen metric. In this section we will discuss how the overall impact of risks and opportunities can be computed given the resulted ATO tree.

*1) **Evaluation of the Total Risks/Opportunities of the Project**:* In addition to a planning tree, which works on an abstraction layer where we suppose that all actions will be successfully performed: *action-level* (A-Level), the ATOs provide a level of abstraction where threats and opportunities may occur and impact the project: the *threat-opportunity-level* (TO-Level). A summary of all abstraction levels can be seen in Figure 5. In section IV-B, we argued that in order to evaluate a planning tree (A-Level) we need to define an attribute domain $(\mathcal{V}, f_\wedge, f_\vee, f_{\underline{\vee}})$.

Furthermore, we need to take into consideration how to assign an overall value representing the threats of an action at the A-Level based on the threats/opportunities

from the TO-Level. We introduce an additional function $f_E^N : \mathcal{V} \times \mathcal{V} \to \mathcal{V}$, where E stands for event and represents a threat or an opportunity and N represents an action node of the planning sub-tree. This function can be a simple addition of all the threats, although it can represent a more complex process, depending on the chosen metric and on the overall needs. Therefore, the attribute domain for ADTs is $(\mathcal{V}, f_\wedge, f_\vee, f_\trianglelefteq, f_E^N)$.

Definition 3. (Probable losses) A probable loss $(p, l) \in (\mathcal{P}, \mathcal{L})$, with $\mathcal{P}$ being a set of probabilities and $\mathcal{L}$ a set of losses, is the probability p of a threat to occur and causing a loss l.

It is usually difficult to define accurately the probability of an event occurrence, therefore we adopt a qualitative approach instead of a quantitative one and define the set $\mathcal{P} = \{L(Low), M(Medium), H(High)\}$. Furthermore, we define losses as being the monetary impact on the expected benefit of an action. Since the impact of a loss results in a reduction of the benefit, we define $\mathcal{L} \subseteq \mathbb{R}^-$.

In order to use this definition of probable losses as a metric we define the attribute domain $((\mathcal{P}, \mathcal{L}), f_\wedge, f_\vee, f_\trianglelefteq, f_E^N)$.

Let $(p_N, l_N) \in (\mathcal{P}, \mathcal{L})$ be the probable loss of a node N with c child nodes, and let $(\mathcal{P}_C, \mathcal{L}_C) = \{(p_1, l_1), ..., (p_c, l_c)\}$ denote the probable losses associated to the child nodes of N. Furthermore, let $\mathcal{B}_C = \{b_1, ..., b_c\}$ be the benefit associated to the refined nodes of N. Depending on the nature of the node N, we compute its value with one of the following functions:

$$f_\wedge(\mathcal{P}_C, \mathcal{L}_C) = (\max_{p_i \in \mathcal{P}_C} p_i, \sum_{l_i \in \mathcal{L}_C} l_i)$$
$$f_\vee(\mathcal{P}_C, \mathcal{L}_C) = (\max_{p_i \in \mathcal{P}_C} p_i, \sum_{l_i \in \mathcal{L}_C} l_i)$$
$$f_\trianglelefteq(\mathcal{P}_C, \mathcal{L}_C) = (p_i, l_i) \in (\mathcal{P}_C, \mathcal{L}_C) | b_i = \max_{b_j \in \mathcal{B}_C} (b_j)$$
$$f_E^N(\mathcal{P}_C, \mathcal{L}_C) = (\max_{p_i \in \mathcal{P}_C} p_i, \sum_{l_i \in \mathcal{L}_C} l_i)$$

Note that we define the probability P as being the maximum probability of any threat occurring in a given node and the loss L as being the maximum loss that can occur.

Definition 4. (Probability of an opportunity) An opportunity is an unpredictable event that can have a positive impact on the benefit of a project if an action is taken. It is, therefore, very important to detect such opportunities early in the project in order to be able to implement actions to fructify them.

Let $\mathcal{P} = \{L, M, H\}$ represent the set of probabilities with which an opportunity may occur, where $L/M/H$ represent respectively a low, medium and high probability. Let $p_N \in \mathcal{P}$ be the probability of an opportunity appearing at node N with c child nodes and let $\mathcal{P}_C = \{p_1, ..., p_c\}$ denote the probabilities associated to the child nodes of N. Furthermore, let $\mathcal{B}_C = \{b_1, ..., b_c\}$ be the benefit associated to the child nodes of N. Depending on the nature of the node N, we compute its value p_N with one of the following functions:

$$f_\wedge(\mathcal{P}_C) = \max_{p_i \in \mathcal{P}_C} p_i \qquad f_\vee(\mathcal{P}_C) = \max_{p_i \in \mathcal{P}_C} p_i$$
$$f_\trianglelefteq(\mathcal{P}_C) = p_i \in \mathcal{P}_C | b_i = \max_{b_j \in \mathcal{B}_C} (b_j) \qquad f_E^N(\mathcal{P}_C) = \max_{p_i \in \mathcal{P}_C} p_i$$

We do not associate any benefit with an opportunity, as opposed to threats. This is due the fact that the existence of an opportunity does not generate a benefit *per-se*, instead, an action taking advantage of that opportunity will generate a benefit. In the case of threats it is exactly the opposite: if a threat occurs, a negative effect on the benefit will occur and this can only be avoided by performing a countermeasure action.

*2) **Using ATO Trees to Avoid High Risk Situations**:* After performing a first analysis of the project the stakeholders might decide that they do not wish to invest in projects with a certain risk level (combination between probability of risk and risk impact). In this section we provide an algorithm that after starting with an evaluated ATO tree can compute an alternative tree meeting the requirements of the stakeholders, if such a tree exists.

Algorithm 1:
Let C be the criterion of rejection that the stakeholders defined. Note that criteria of rejection can incorporate financial losses, company's vision and history, reputations, etc.. For every risk-node in the tree, verify if the condition is met and if so delete that node and its parent action to which it is associated. After all rejected nodes are deleted, check if any node of the tree is unachievable due to the pruning: if it is the case prune those nodes too. Repeat this last step until no more unachievable nodes are present. Algorithm 1 shows the details of the procedure.

After defining a risk rejection criterion as mentioned above, each risk being above this threshold is considered (and not formally avoided or mitigated). It generally happens that a company will take an important risk because of money, strategy, context, etc., but a)now, they know this risk exists and b)the management decides to retain the risk with full knowledge of the facts. Our framework provides a decision making support tool; we do not intend to fully automate the process and remove the human decision factor. This discussion is, whatsoever, outside of the scope of this paper.

ArchiSurance example:
Let us consider that the action of "developing a new application" has associated a medium risk that "main developer quits". Also, let us consider that all improvements to the

database have as a result "un-used servers", that the company can further use in order to obtain a profit. Therefore, in the plan we mark this opportunity with a high probability of occurrence.

In Figure 3 we represent the plan, with two abstraction layers (actions and threat/opportunities layers). We compute the over all risk of the project using a bottom-up approach.

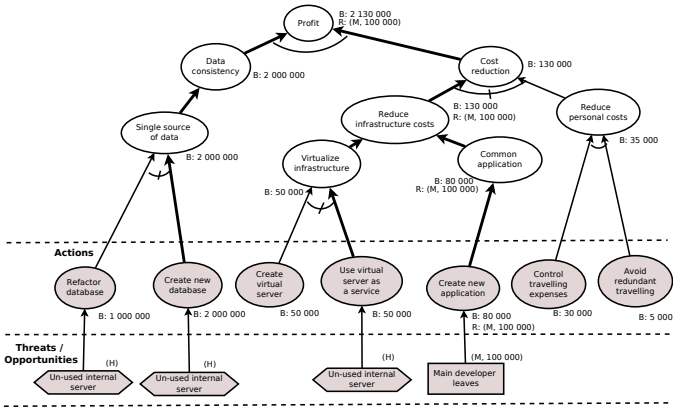

Figure 3: "ArchiSurance" - project risk evaluation

Furthermore, let us suppose that the stakeholders of this project decided that they are not willing to take any action that would involve a risk with a medium probability or more. After applying Algorithm 1 we achieve the result presented in Figure 4 (mitigation of the highest risk of the project).

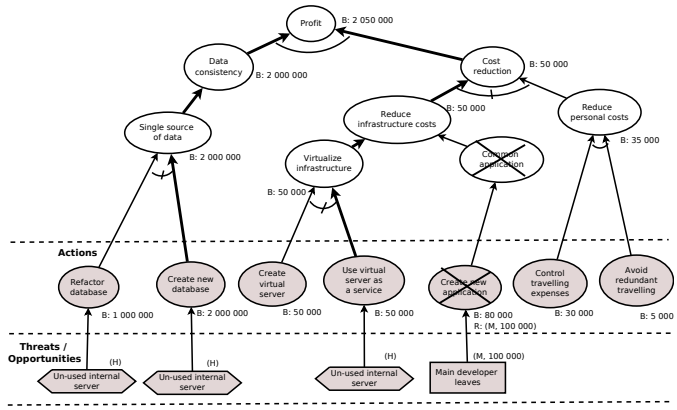

Figure 4: "ArchiSurance" - mitigation of a highly probable risk

E. Extended-ATOs

As seen in the previous section, at this step we are able to evaluate the total risks of a project, as well as identifying and if necessary avoid risk sources. Even if there are cases where risk is acceptable/unavoidable, we present a methodology in order to construct countermeasures with the scope of minimizing the expected losses.

We also identified opportunities but in order to benefit from these opportunities actions need to be taken. This section aims to expend the previous model to accommodate actions taken to increase the advantages of opportunities and to perform countermeasures against threats. We further extend the metrics to directly evaluate the impact of these actions on the expected benefits and losses.

Algorithm 1 Computed Tree Compliant With A Criterion

$C \leftarrow$ rejection criterion from the stakeholders
$Parent(n) \leftarrow$ the parent of node n
$Children(n) \leftarrow$ the children of the node n
$Root(Tree) \leftarrow$ the root node of Tree

//Marks the actions that fulfil the rejection
//criterion of the stakeholders for deletion.
function MARKUNDESIREDTHREATS(C, ATO)
  for all $t \in ATO$ s.t. t is a threat **do**
    if t fulfils C **then**
      mark $Parent(t)$ & $Children(Parent(t))$
    end if
  end for
end function

//Returns a tree without any risk that fulfils the
//rejection criterion given, if such a tree exists
function COMPUTECOMPLIANTTREE(C, ATO)
  MarkUndesiredThreats(C, ATO)
  $verifNeeded \leftarrow true$
  while $verifNeeded$ & !Root(ATO) marked **do**
    $verifNeeded \leftarrow false$
    for all $n \in ATO$ **do**
      if n (exclusive) disjunctive **then**
        //A (exclusive) disjunctive node can not be
        //fulfilled if all its children can't
        if $\forall c \in Children(n), c$ is marked **then**
          mark n
          $verifNeeded \leftarrow true$
        end if
      else if (n is conjunctive) **then**
        //A conjunctive node needs all its children
        //to be fulfilled in order to be fulfilled
        if $\exists c \in Children(n)$ s.t. c is marked **then**
          mark n
          mark all children of n recursively
          $verifNeeded \leftarrow true$
        end if
      end if
    end for
  end while
  drop all marked nodes from ATO
  return ATO
end function

Definition 5. (eATO tree) An eATO (extended Actions-Threats-Opportunities) tree is an ATO where threats can have one or more countermeasures and opportunities can have one or more actions associated to them.

Each threat and opportunity node can have one or more action nodes as children. The graphical representation of these action nodes is the same as normal nodes of the tree (circles).

F. Evaluation of Extended-ATOs

In addition to the two abstraction layers already introduced in the previous sections, ATOs add one extra layer, the countermeasure-layer (C-Level). The starting point for the evaluation of an eATO is a simple ATO where the leaf-nodes of the A-Level and the threats/opportunities already have their attributes evaluated.

At this point, if one wishes to extend the previously conducted analysis, we raise the question how to mitigate the existing risks and how to take advantage of the occurring opportunities.

Each action that results from this analysis is added to its respective risk/opportunity and the resulting residual risk/benefit is approximated and added as an attribute of the nodes.

*1) **Using eATO Trees to Evaluate Total Risk/Opportunity After Mitigation**:* In order to evaluate an extended ATO tree, we define an attribute domain of the form $(\mathcal{V}, f_\wedge, f_\vee, f_\veebar, f_E^N, f_N^E)$ where $f_N^E : \mathcal{V} \times \mathcal{V} \to \mathcal{V}$ is the function that handles the transition of the C-Level to the TO-Level. This function permits us to compute the residual risk/benefit associated to a given threat/opportunity, after given the fact that the countermeasures/actions will be in place at the moment these events will occur.

Definition 6. (Probable losses after mitigation) A probable loss after mitigation is a pair $(p, l) \in (\mathcal{P}, \mathcal{L})$, with $\mathcal{P}$ being a set of probabilities and $\mathcal{L}$ a set of losses, is the probability p of a threat to occur knowing a countermeasure has been applied against it and l is the loss generated by the occurrence of that threat. We define $\mathcal{P}$ as $\mathcal{P} = \{L, M, H\}$, where L, M and H represent a qualitative approximation of the probability of the threat occurring (low, medium, high) and $L \subseteq \mathbb{R}^-$ represents the set of monetary losses that can be generated by the occurrence of a threat. In other words, the probable loss after mitigation is the residual probable loss after a countermeasure was put in place.

The extended attribute domain of this metric has the form $((\mathcal{P}, \mathcal{L}), f_\wedge, f_\vee, f_\veebar, f_E^N, f_N^E)$. Let $(p_N, l_N) \in (\mathcal{P}, \mathcal{L})$ be the probable loss of a node N with c child nodes and $(\mathcal{P}_C, \mathcal{L}_C) = \{(p_1, l_1), ..., (p_c, l_c\}$ the probable losses associated to these nodes. Furthermore, let $B_C = \{b_1, ..., b_c\}$ be the benefit associated to the child nodes of N. Depending on the nature of the node N, we compute its value with one of the following functions:

$$f_\wedge(\mathcal{P}_C, \mathcal{L}_C) = (\max_{p_i \in \mathcal{P}_C} p_i, \sum_{l_i \in \mathcal{L}_C} l_i)$$

$$f_\vee(\mathcal{P}_C, \mathcal{L}_C) = (\max_{p_i \in \mathcal{P}_C} p_i, \sum_{l_i \in \mathcal{L}_C} l_i)$$

$$f_\veebar(\mathcal{P}_C, \mathcal{L}_C) = (p_i, l_i) \in (\mathcal{P}_C, \mathcal{L}_C) | b_i = \max_{b_j \in \mathcal{B}_C} (b_j)$$

$$f_E^N(\mathcal{P}_C, \mathcal{L}_C) = (\max_{p_i \in \mathcal{P}_C} p_i, \sum_{l_i \in \mathcal{L}_C} l_i)$$

$$f_N^E(\mathcal{P}_C, \mathcal{L}_C) = (\min_{p_i \in \mathcal{P}_C} p_i, \max_{1 \le j \le c} (l_j + b_j) | p_j = \min_{p_i \in \mathcal{P}_C} p_i)$$

We suppose that the main goal of the analysis is to reduce as much as possible the probability of occurrence of a threat. Furthermore, among the possible countermeasure, the goal is to choose the one that maximize the overall benefit. Note that the benefit is negatively influenced by the loss introduced by the threat and the cost of implementing a countermeasure. The goal is to reduce the impact of a threat at a minimal cost.

Definition 7. (Probable benefit) We define a probable benefit as a pair $(p, o) \in (\mathcal{P}, \mathcal{O})$, where $\mathcal{P} = \{L, M, H\}$, being the set of probabilities L/M/H of an opportunity occurring, and $\mathcal{O} \subseteq \mathbb{R}^+$ being the revenue that might be generated if an action is implemented in order to fructify the opportunity. The revenue highly depends on the actions taken to benefit from an opportunity, therefore it is important to analyse and act accordingly.

We define the attribute domain $((\mathcal{P}, \mathcal{O}), f_\wedge, f_\vee, f_\veebar, f_E^N, f_N^E)$. Let $(p_N, o_N) \in (\mathcal{P}, \mathcal{O})$ be the probable benefit associated to a node N with c child nodes and let $(\mathcal{P}_C, \mathcal{O}_C) = \{(p_1, o_1), ..., (p_c, o_c)\}$ denote the probable benefits associated to the refined nodes of N. Furthermore, let $\mathcal{B}_C = \{b_1, ..., b_n\}$ be the benefits associated to the refined nodes of N. Depending on the nature of the node N, we compute its value (p_N, o_n) with one of the following functions:

$$f_\wedge(\mathcal{P}_C, \mathcal{O}_C) = (\max_{p_i \in \mathcal{P}_C} p_i, \sum_{o_j \in \mathcal{O}_C} o_j)$$

$$f_\vee(\mathcal{P}_C, \mathcal{O}_C) = (\max_{p_i \in \mathcal{P}_C} p_i, \sum_{o_j \in \mathcal{O}_C} o_j))$$

$$f_\veebar(\mathcal{P}_C, \mathcal{O}_C) = (p_i, o_i) \in (\mathcal{P}_C, \mathcal{O}_C) | b_i = \max_{b_j \in \mathcal{B}_C} (b_j)$$

$$f_E^N(\mathcal{P}_C, \mathcal{O}_C) = (\max_{p_i \in \mathcal{P}_C} p_i, \sum_{o_j \in \mathcal{O}_C} o_j)$$

$$f_N^E(\mathcal{P}_C, \mathcal{O}_C) = (\max_{p_i \in \mathcal{P}_C} p_i, \max_{1 \le j \le c} (o_j + b_j) | p_j = \min_{p_i \in \mathcal{P}_C} p_i)$$

We define the probability $\mathcal{P}$ as being the maximum probability of any opportunity occurring in a given node and the benefit $\mathcal{O}$ as being the maximum benefit that can be achieved if all opportunities occur.

Definition 8. (Benefits II) Until this point, benefits have been computed on the planning tree level. This is not enough when talking about risks mitigation and opportunities.

The taken actions impact the benefit of an enterprise directly. For instance, if one needs to create a back-up server to avoid the failure of one server, this impacts the business even though the failure did not occur yet. Only by deciding to implement a countermeasure the company pays a cost (negative benefit/a loss). In order to take this into consideration we modify the A-Level attribute domain to a C-Level attribute domain.

Let $\mathcal{B} \subseteq \mathbb{R}$ be the set of benefits that can be associated with a node N. If a positive benefit is associated to a countermeasure, it means that implementing this countermeasure will generate an additional revenue, whereas a negative benefit means that implementing the countermeasure has a cost.

Let $b_N \in \mathcal{B}$ be the benefit associated with a node N and let $b_{N^*} \in \mathcal{B}$ be the benefit originally associated with a node before taking into consideration the countermeasures.

Let $\mathcal{B}_C = \{b_1, ..., b_c\}$ represent the set of benefits associated to the c children of N. If N is a threat, let $b_{ct} \in \mathcal{B}$ represent the benefit associated with a selected countermeasure of N.

We define the attribute domain $(\mathcal{B}, f_\wedge, f_\vee, f_\veebar, f_E^N, f_N^E)$. Depending on the nature of the refined nodes, we use the following functions for evaluating the benefit:

$$f_\wedge(\mathcal{B}_C) = \sum_{b_i \in \mathcal{B}_C} b_i \qquad f_\vee(\mathcal{B}_C) = \sum_{b_i \in \mathcal{B}_C} b_i$$

$$f_\veebar(\mathcal{B}_C) = \max_{b_i \in \mathcal{B}_C} b_i \qquad f_E^N(\mathcal{B}_C) = b_{N^*} + \sum_{b_i \in \mathcal{B}_C} b_i$$

$$f_N^E(\mathcal{B}_C) = b_{ct}$$

*2) **Using eATO Trees to Avoid High Risk Situations and Bad Investments**:* Knowing which threats and opportunities exist and what actions can be taken to mitigate risks or take advantages from the opportunities is not enough. Sometimes stakeholders might not wish to invest in countermeasure against risks that only have a small probability of occurring or on opportunities that require a high investment in order to be able to take advantages of them. In this section we present how to compute a new eATO tree that complies to the risks/opportunities and actions that the stakeholders are willing to take.

Algorithm 2:
Let C be the criterion of rejection of an action, opportunity or threat. In order to compute a tree which does not contain unacceptable risks and investments, we start by checking the C-Level nodes. If any of these fulfil the rejection criterion, they will be deleted. Afterwards, we check that no TO-Level nodes fulfil any rejection criterion and delete the ones that are unacceptable. The rest of algorithm consists, as in Algorithm 1, of checking which A-Level nodes can not be achieved and removing them. Compared to Algorithm 1 the main change consists in the function "MarkUndesiredThreats" which need to be replaced by the function "MarkUndesiredNodes" described in Algorithm 1.

Algorithm 2 Computed eATO Tree Compliant With A Criterion

```
function MarkUndesiredNodes(C, ATO)
    //If a C-Level node is unacceptable we
    //mark it for deletion
    for all c ∈ ATO s.t. c is C-Level do
        if c fulfils C then
            mark c
        end if
    end for

    //If an opportunity is not taken
    //mark it for deletion
    for all o ∈ ATO s.t. o is an opportunity do
        if Children(o) is empty then
            mark o
        end if
    end for

    //If a threat is not acceptable mark the
    //action that is origin of that and all
    //its children
    for all t ∈ ATO s.t. t is a threat do
        if t fulfils C then
            mark Parent(t)
            mark Children(Parent(t))
        end if
    end for
end function
```

ArchiSurance example:
In Figure 5 we present the newly computed benefit of the company, after the actions on the C-Level are performed. Let us consider that an opportunity to remain with an "un-used internal server" could bring a consistent income, either by selling the remaining server or using it as a back-up and not invest in a new system. Also, applying a countermeasure on a risk can overall reduce its risk level (countermeasures can be set suck that both probability of occurrence is reduced, as well as the impact).

V. Related work

Today, risk management is mainly performed in a domain-specific manner. Different methods and approaches exist in the different risk-aware domains, e.g., information security, environment, project management, finance. Due to the huge number of references, it is not possible to provide an exhaustive list in this paper. The main issue is that no interoperability between these approaches is possible, thus

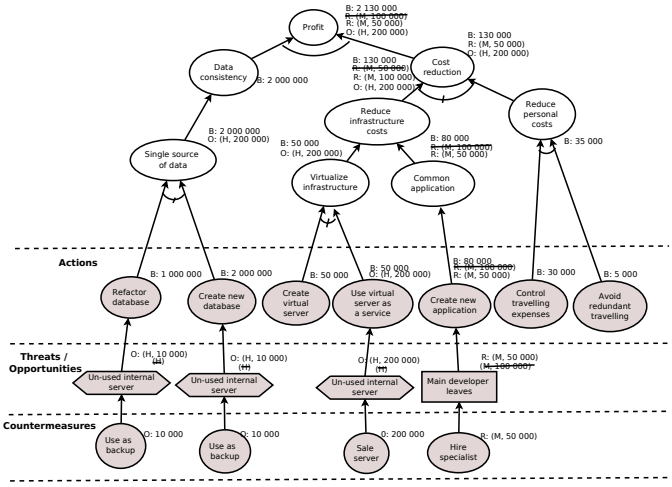

Figure 5: "ArchiSurance" - overall benefit after risks mitigation and profiting on opportunities

it is difficult to compare risk from different domains ("is the information security risk A more or less important than the environmental risk B?") or to be able to define cross-domain impact of risk ("considering the impact of a fire at the information security, environment and financial level, what is its global impact level for the enterprise?").

Integration of the different risk management processes at an enterprise level is a promising and still open research topic. Our framework aims at dealing with risk in different domains. The main initiative in this way is the ISO 31000 series of standards [19], [20] defining the baseline for integrated risk management. At this level, guidance on risk identification and analysis is still informal and very few modelling and computing capabilities are offered. As stated in [21], the introduction of model-based approaches as support of risk management, such as ADTs, is motivated first by an efficiency improvement of the risk management process, and second by the enhancement of the product resulting from the performed process. Moreover, risk management methods usually provide list of common risks to consider, but do not provide capabilities to identify new risks or analyse them in depth, as it is supported through ADTs. Regarding goal-oriented modelling frameworks, many of them provide risk management capabilities, mainly for dealing with information security risks: KAOS and its security extension [21], Misuse cases [22], Malactivity diagrams [23], BPMN [24] and Secure Tropos [25].

Asnar et al. [26] presented a modelling and reasoning framework that considers risk at organizational level. The framework has extended the Tropos goal modelling framework to analyse, evaluate, and select risk among the alternatives that are able to fulfil the stakeholders' goals [27]. The framework describes a 3-layers model which inspired our approach, however its consideration remains organisational while ignoring additional enterprises requirements. In this paper, we positioned our 3-layers model with enterprise principles regarding objectives and motivations for achieving profits.

The Open Group Architecture Framework (TOGAF) is a standardized method for enterprise architecture [16]. Architecture principles play a central role in TOGAF. Even though a template for architecture principles is given, with a number of examples, no crisp definition of the concept is given. Furthermore, no practical way of formulating and using principles is provided either [13]. Moreover, the ArchiMate language for describing enterprise architectures in TOGAF [28] does not contain constructs to represent architecture principles and their motivations. The initial results of our work identified concrete principles dealing with risk mitigation and profitability in EA.

VI. Conclusions and Future Research

In this paper we have extended and combined two methodologies (attack-defence-trees from IT security and goal-oriented modelling) in order to provide an aid in decision making. We made a first step between enterprise architecture principles, aligned with stakeholders goals and risk management. We consider as starting point a case study and present step-by-step how a goal (maximize profitability) of the stakeholders is supported by principles. In addition, we show how these principles support both actions and decisions. We show how ADTs can be adapted in order to offer support for such decisions, in addition to their security applicability. We have also toggled risk assessment, in particular evaluation, and risk treatment, in particular mitigation and avoidance.

We believe that a step in future research can be represented by adopting this framework to the whole project lifecycle: evaluate current situation based on planned situation and perform changes to steer the correct execution of the plan. Also, reverse engineering the trees could give important inputs on how a company arrived to its current state; give information on what were the underlining assumptions of a decision. Note that each action performed is costly by itself. We believe that a game-theoretic approach could be used in order to evaluate the trade-off between investments and benefits.

We consider this paper as a primer for future related work. The are two main questions that were not explicitly elaborated in this paper: inputs and priorities. We need to investigate inputs related to quantitative values and compare it to qualitative analysis. We need also to prioritize our risk mitigation while considering organisation's strategy, context and risk appetite. In other words, we need to find the suitable equation to manage risk while ensuring the stability and the proper functioning of an organisation. Moreover, additional experimentations will assess if, and in which context, the use of ADTs and the related benefits are relevant with regards to the time spent to build the ADTs.

Finally, we plan to extend the used metrics. For this, we would conduct a survey in industry in order to gain more information on procedures, principles and decisions and apply the framework on more (real) case studies.

REFERENCES

[1] M. Op 't Land, H. Proper, M. Waage, J. Cloo, and C. Steghuis, *Enterprise Architecture – Creating Value by Informed Governance*, ser. The EE Series. Springer, 2008.

[2] J. L. G. Dietz, A. Albani, and J. Barjis, Eds., *Advances in EE I, 4th International Workshop CIAO! and 4th International Workshop EOMAS, held at CAiSE 2008, Montpellier, France, June 16-17, 2008. Proc.*, ser. LNBIP, vol. 10. Springer, 2008.

[3] R. Wieringa, P. v. Eck, C. Steghuis, and H. Proper, *Competences of IT Architects*. The Hague, Netherlands: Academic Service – SDU, 2008. [Online]. Available: http://www.sdu.nl/catalogus/9789012580878

[4] The Open Group, *TOGAF Version 9*. Van Haren Publishing, Zaltbommel, The Netherlands, 2009.

[5] Object Management Group, "Business Motivation Model (BMM) Specification," Needham, Massachusetts, Tech. Rep. dtc/06–08–03, August 2006.

[6] Washington State Department of Transportation, "Project Risk Management Guidance for WSDOT Projects," Tech. Rep., July 2010.

[7] B. Kordy, S. Mauw, M. Melissen, and P. Schweitzer, "Attack-defense trees and two-player binary zero-sum extensive form games are equivalent," in *Proc. of the First international conference on Decision and game theory for security*, ser. GameSec'10. Springer, 2010, pp. 245–256.

[8] S. Mauw and M. Oostdijk, "Foundations of attack trees," in *International Conference on Information Security and Cryptology ICISC 2005. LNCS 3935*. Springer, 2005, pp. 186–198.

[9] S. Bistarelli, M. Dall'Aglio, and P. Peretti, "Strategic games on defense trees," in *Proc. of the 4th international conference on Formal aspects in security and trust*, ser. FAST'06. Springer, 2007, pp. 1–15.

[10] S. Bistarelli, F. Fioravanti, and P. Peretti, "Defense trees for economic evaluation of security investments," in *ARES*, 2006, pp. 416–423.

[11] M. M. Lankhorst, *Enterprise Architecture at Work - Modelling, Communication and Analysis (4. ed.)*, ser. The EE Series. Springer, 2013.

[12] H. Jonkers, M. Lankhorst, R. v. Buuren, S. Hoppenbrouwers, M. Bonsangue, and L. Van der Torre, "Concepts for Modeling Enterprise Architectures," *International Journal of Cooperative Information Systems*, vol. 13, no. 3, pp. 257–288, 2004.

[13] D. Greefhorst and H. Proper, *Architecture Principles – The Cornerstones of Enterprise Architecture*, ser. The EE Series. Springer, 2011.

[14] A. Osterwalder and Y. Pigneur, *Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers*. Amsterdam, The Netherlands: Self Published, 2009.

[15] W. Engelsman, H. Jonkers, and D. Quartel, "ArchiMate Extention for Modeling and Managing Motivation, Principles and Requirements in TOGAF," The Open Group, White paper, August 2010.

[16] *The Open Group – TOGAF Version 9*. Van Haren Publishing, Zaltbommel, The Netherlands, 2009.

[17] J. Cummins and N. Doherty, "The economics of insurance intermediaries," *The Journal of Risk and Insurance*, vol. 73, no. 3, pp. 359–396, 2006.

[18] H. Jonkers, I. Band, and D. Quartel, "The ArchiSurance Case Study," The Open Group, White Paper, Spring 2012.

[19] ISO 31000, *Risk management Principles and guidelines*. Geneva: International Organization for Standardization, 2009.

[20] ISO 31010, *Risk management Risk assessment techniques*. Geneva: International Organization for Standardization, 2009.

[21] N. Mayer, "Model-based management of information system security risk," Ph.D. dissertation, University of Namur, 2009.

[22] R. Matulevicius, N. Mayer, and P. Heymans, "Alignment of misuse cases with security risk management," in *Proceedings of the 4th Symposium on Requirements Engineering for Information Security (SREIS'08), in conjunction with the 3rd International Conference of Availability, Reliability and Security (ARES'08)*. IEEE Computer Society, 2008, p. 13971404.

[23] M. J. M. Chowdhury, R. Matulevicius, G. Sindre, and P. Karpati, "Aligning mal-activity diagrams and security risk management for security requirements definitions," in *Requirements Engineering: Foundation for Software Quality*, ser. LNCS, B. Regnell and D. Damian, Eds. Springer, Jan. 2012, no. 7195, pp. 132–139.

[24] O. Altuhhova and R. Matuleviius, "Security risk management using business process modelling notations." [Online]. Available: http://comserv.cs.ut.ee/forms/ati_report/downloader.php?file=2d9492b162c11041043eb586b08b45d5524ad9fe

[25] R. Matulevicius, N. Mayer, H. Mouratidis, E. Dubois, P. Heymans, and N. Genon, "Adapting secure tropos for security risk management during early phases of the information systems development," in *Proceedings of the 20th International Conference on Advanced Information Systems Engineering (CAiSE '08)*. Springer, 2008, pp. 541–555.

[26] Y. Asnar and P. Giorgini, "Modelling risk and identifying countermeasure in organizations." Samos Island, Greece, 30/08/2006 2006.

[27] P. Bresciani, A. Perini, P. Giorgini, F. Giunchiglia, and J. Mylopoulos, "Tropos: An agent-oriented software development methodology," *Autonomous Agents and Multi-Agent Systems*, vol. 8, no. 3, pp. 203–236, May 2004. [Online]. Available: http://dx.doi.org/10.1023/B:AGNT.0000018806.20944.ef

[28] H. Jonkers, H. Proper, and M. Turner, "TOGAF and ArchiMate: A Future Together," The Open Group, White Paper W192, November 2009.