Astrolabe: A Collaborative Multi-Perspective Goal-Oriented Risk Analysis Methodology

EBRAHIM BAGHERI AND ALI A. GHORBANI {e.bagheri,ghorbani}@unb.ca

Faculty of Computer Science, University of New Brunswick, Fredericton, NB, Canada

> Have a definite, clear practical ideal; an end,
> the necessary means to achieve your end,
> and adjust all your means to that end.
> *Aristotle*

Abstract. The intention of this paper is to introduce a risk analysis methodology, called Astrolabe. Astrolabe is based on the key idea of mining system risks from their origins and sources in order to both align the current standpoint of the system with its intentions and identify any vulnerabilities or hazards threatening its being. Astrolabe adopts concepts from organizational theory and software requirement analysis. The aim of Astrolabe is to guide risk analysis through its phases so that a near complete investigation of system risks is performed. The concepts driving the Astrolabe methodology have been defined in a metamodel that has been introduced in this paper.

Keywords: Risk Analysis, Goal-Oriented Modeling, Risk Lifecycle

1. Introduction

Risks are the likelihood and the degree of severity of unplanned or undesirable states. Analogous to its nature, the definition of risk is very much dependant on context and contextual factors. What might not be considered as risk in one context may be identified as a major risk in another. Even in the same context, different points of view may rank the severity or likelihood (in cases where these factors are qualitatively analyzed) of a risk with dissimilar values which results in more ambiguity. However, what is currently the common understanding and is being mostly shared between various contexts in the study of risk is the fact that analyzing risk requires methods to identify the sources of the events that drive a system or an organization towards the states that expose it to risk. Therefore, besides the direct events that lead to unsafe conditions, the courses of action guiding these events and even more importantly the intentions of these actions need to be identified and well understood.

The common sense behind tracking the sources of risk back to its origins (intentional causes) is that without the proper adjustment of these roots, it would be rather impossible to change the outcomes. In other words, the probable formation of the branches of a behavior tree in a system is dependant upon the arrangement of its roots. It is undeniable that local changes made to the branches of this tree can have quick and even spontaneous effects, but they do not have long-term durability. However, The fact that these solutions do not have long-term effect should not cause of an underestimate of their efficiency under certain circumstances.

From a systems engineering perspective, the roots of the behavior of a system[1] belie in the goals that it pursues. Parson argues that goal attainment is an indispensable aspect of any system [(Parsons, 1971)]. Lets consider two very different systems each formed based on communal and associational relationships [(Curry, 2002)]. A system developed for a communal relationship focuses more on mere member gratification. An example of this system may be the formation of a student association that organizes student activities. In a system of associational relationships the membership of the participants is no longer because of the importance or pleasure of a relationship and is more or less attained so that the results of this relationship can indirectly help the participants create other systems based on communal relationships. For instance, employment in a job, is a type of associational relationship that is accepted by a person so that he/she can establish his/her own family (a system of communal relationships). There are fundamental differences between the nature of the systems developed from these types of relationship, but one common factor exists in both of them and that is goal attainment. Even in a student association that has been established for a very informal cause, the inability to cater these requirements may result in the discontinuity of the relationship. Therefore, goal attainment has primacy over all of the activities of any type of system.

Goals are often the result of the strategy selection process through which a system identifies its direction and decision making criteria [(Scott, 1992)]. To achieve its goals, a system devises plans to undertake a series of actions. The implementation of the course of these actions situates the system under various states and conditions among which unsafe states may also be found. The existence of these states depends on the degree of willingness of the system to take risks. If the risk is outweighed by the benefits perceived by the system, then that specific action may be performed. Based on this description, system goals cater related criteria and metrics for action generation and selection. This means that goals are the driving force of system behavior. Hence, the behavior of a system can be justified by its goals. Goals can also be used to appraise current system performance. The appraisal can be based on the gap between the desired system derived from its initial set of goals and its current standing [(Scott, 1990)]. The iterative process of re-appraisal can be employed to adjust a system so that it functions towards its initially planned ends.

In this paper, we intend to formalize the notion of goals for analyzing the risks that threaten a system. Goals in our approach are tied to system operations that provide the means for answering questions such as ‘which goals expose severe hazards to the system’, ‘how can a currently running operation be justified or adjusted based on system intentions’, and etc. To achieve this purpose, we look into organizational theory for the roots of goal definition.

1.1. Conceptual Background

A system can be described by its goals and objectives, and the set of scenarios that it carries out to support the operationalization of these ends. In other words, goals are intentional and scenarios (a collection of related and mostly ordered actions) are operational aspects of a system [(Rolland et al., 1999)]. Studies show that very few systems actually achieve their intended goals to the extent of their initial desire [(Gross, 1969)]. This may be due to several factors. It may be either because the scenarios that have been supporting the attainment of system goals are not in full alignment with these goals, or it may be due to the incomplete or incorrect undertaking of these scenarios. Empirical evidences from the current behavior of a system can help identify the gap between system goals and the present practice. The existence of such a gap is not a rare incident in many systems. Even in political systems, the leaders initially acknowledge the goals of their party, but over time, as they acquire power, become rather conservative and hesitant to change in order to attain the current situation and in consequence sacrifice the initial goals [(Scott, 1992)].

A system can also be caught in a situation where the rapid change of its context has led to the requirement of goal amendment. The need for a quick adjustment can result in a condition where the goals of a system are no longer well defined. This situation can be described with the garbage can theory [(Cohen et al., 1972)]. This theory describes a condition where a system offers a set of solutions and is looking for a suitable problem to match these solutions. Therefore, the risks associated with this state should be also analyzed.

Systems that need to incorporate the role of human resources into their structure also face a different kind of risk. Motivational theory formalizes the reason behind the involvement of any human resource into a system through inducements and contributions [(Simon, 1979)]. Inducements are desired aspects of participation. Inducements of working for a company are a suitable salary along with social welfare and insurance options. Contributions on the other hand, have negative utility from the human resource perspective, but are the requirements for participation. Constant traveling for a salesperson is a type of contribution that he/she has to make in that position. In cases where the contributions and inducements of a position in a system contradict each other, risks may arise for the system, since the human resource may not adhere to the requirements of the contribution (This fact has also been addressed as orthogonal goals of organizations and individuals in related literature).

Other sources for risk may also exist in systems that have human interference. Merton describes a common incident where people unpurposefully replace means for ends in a system [(Merton, 1957)]. This is usually the result of a mere focus on the correct execution of the current scenario and not focusing on its origins. Therefore, even in cases where the scenario is contradicting its own initial causes, it would be still practiced. Other than this problem, the different interpretations and granularity of goals among the involved parties is another source of risk. For example, the goals defined at the administrative level are not comprehensible for others lower down [(Gross, 1969)]. The vice versa is also true where the scenarios performed by actual workers are not well understood and fully attached to system goals by system administrators. The following sub-section clearly defines the types of problems and issues that are intended to be addressed by the Astrolabe methodology and discusses the reasons behind the proposed approach [(Bagheri and Ghorbani, 2007)].

1.2. Design Challenges

The Astrolabe methodology has an iterative procedure through which it intends to undertake five major tasks:

1. Identify system goals and objectives
2. Codify and relate the available evidence of system activity with its goals
3. Explore system goals and activities for possible threats, vulnerabilities, and risks that they may cause or be threatened to
4. Analyze and organize the identified risks in a unified framework to facilitate decision making
5. Validate the risk analysis process

In order to design a methodology that addresses these issues, many concerns need to be initially addressed. We classify these issues and explain each of them in the following lines:

- The knowledge about the objectives and intentions of a system is rarely well documented, and even in cases where sufficient documentation exist, their interpretation is prone to bias and personal judgement [(Kavakli and Loucopoulos, 2006)]. This is because in many cases the people who originally developed these documents are no longer accessible. Besides this fact, the documents related to system goals and objectives are usually out-dated, since the objectives of a system may rapidly change and often no track of the changes are formally kept. Therefore, the process of system goal and activity revelation needs to be complemented by other methods such as round table interviews with the involved parties of the target system (system actors).
- System actors are mostly concerned with the domain of their own capability and expertise; therefore, a concentrated interview with a system actor is more likely to be focused on the specific area of the actor's responsibility (sub-optimized view) [(Zuckerman et al., 1983)]. In effect, this may lead to a very fine-grained understanding of a single aspect of the system, and the under-estimate of the importance of the others. Even more, a focused attention to specific parts of a system may result in negligence towards the social and political aspects of the system structure. For these reasons, the process of system structure and information elicitation should encompass most of the key actors of the system which requires a very careful selection.

- The actor's perception and understanding of the objectives and activities of a system are often fragmented, and situation dependant. Furthermore, these information are not well classified in the mental model of the actors; hence, a systematic methodology for obtaining and eliciting these information from the actors is required. This methodology should be as close as possible to the mental model of system actors both in terms of terminology and procedure. Incremental information elicitation procedures have shown to be among the most viable. This is due to the fact that the actors are incrementally acquainted with the procedure, and will consequently re-evaluate their statements in the previous phases based on their enhanced understanding of the procedure.

- Since an individual actor's information about a system does not depict a complete picture of that system, the knowledge and experience of various system actors should be exploited. The difficulty of this task is that a simple aggregation of the single depictions of each actor does not accumulate to a correct overall understanding of the system. There may be many conflicting or at least non-conforming opinions, and facts among the expressions of the different actors. To overcome this dilemma a proper knowledge composition procedure should be used through which the conflicts can be resolved, new knowledge be acquired and complementing information be incorporated into a whole.

- A methodology for analyzing risk should provide means for validating the reliability, consistency, completeness, traceability and unambiguity of its products. Since these factors are very much dependant on how the methodology has been employed in different contexts, their formalization should focus on using parameters that are common in the structure of the framework regardless of the time, context and actors of the target system that is being analyzed. In an iterative procedure, the evaluation of a risk analysis methodology would allow proper changes to be made both on the undertaken procedure and the studied system.

2. The Overall Process

The Astrolabe methodology is intended to support the process of identifying the risks that threaten a system and provide the means to trace the roots of these risks. It intends to provide means for analyzing the sources of risk so that proper mitigation strategies can be selected. The methodology does not impose any restrictions on the type of systems that can be analyzed; therefore, systems ranging from technical to social can be analyzed using this methodology. Moreover, it can be used concurrently with system design methodologies to assist risk identification throughout the design process. This means that the methodology not only can be used for existing functional systems, but can also be used for the systems that are currently being designed.

In the following, we will briefly introduce the different phases of the Astrolabe methodology, namely: *Boundary Identification, Perspective Identification and System Analysis, Preliminary Hazard Identification, Perspective Integration, Process Refinement, Risk Analysis, and Quality Measurement and Validation*, then we will

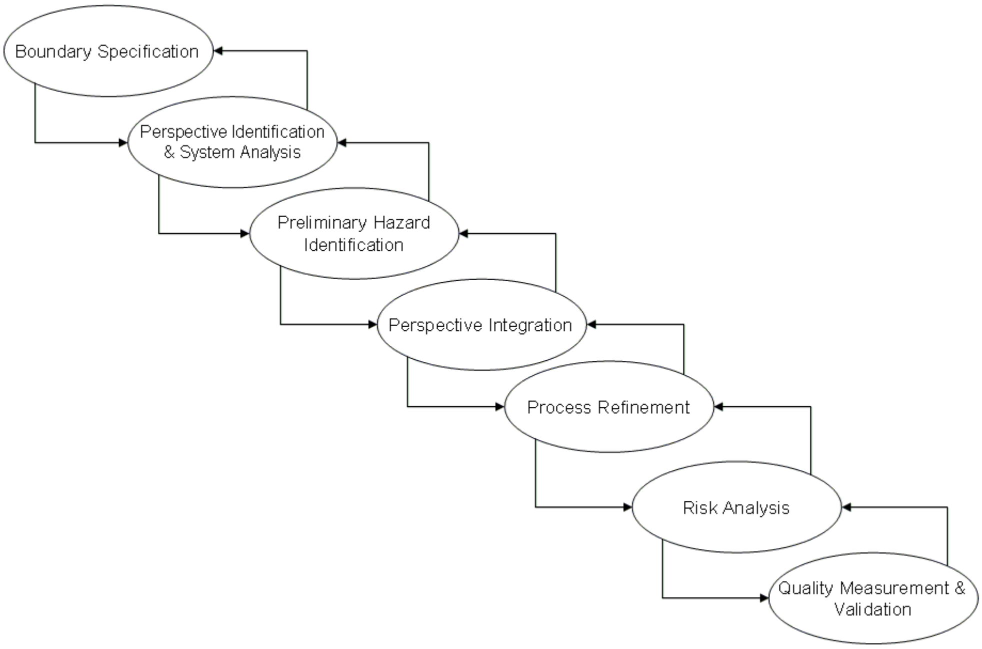
Boundary Specification
Perspective Identification & System Analysis
Preliminary Hazard Identification
Perspective Integration
Process Refinement
Risk Analysis
Quality Measurement & Validation

Figure 1. The Iterative Nature of Astrolabe

define the most important notions that are going to be widely used in the explanation of the methodology phases throughout the paper.

2.1. Analysis Phases

As it can be seen in Figure 1, the Astrolabe methodology has an iterative nature in which all of its phases can be re-visited at any time, if there is a need for change. That is, once the steps in any of the phases have been performed, there may be a need to go back to the previous phases and refine some of the information. For example, if a certain sub-system has been identified to be at a great risk in the risk analysis phase, more attention may need to be given to the refinement of the goals and evidences related to it in the process refinement phase.

The Astrolabe methodology has seven major phases. This does not mean that the completion of these phases ends its lifecycle. As it is inherent in the nature of risk, analyzing and managing risk is a non-stop activity which requires constant revisits and refinements. Within our proposed methodology, after the completion of each iteration, regular examination of the deliverables and products of each phase is required, so that any change in system goals and activities can be captured and suitable risk identification and analysis activities can be performed. The major phases of the Astrolabe methodology are:

I. *Boundary Specification:* The functional and intentional spaces of a system usually span multiple domains; therefore, risk analysts should initially specify which one of the aspects of the system attracts their attention the most and is going to be the target of investigation. Boundary specification should also consist of the identification of the sub-systems of a larger system that are of interest. As an example, in the telecommunication infrastructure, risk analysts should firstly identify which one of the sub-systems of the telecommunication infrastructure they aim to analyze (e.g. mobile network, data network, PSTN network, and so on), and secondly, specify which aspect of this system is of more interest to them (e.g. technical, human resource, marketing, and etc.).

II. *Perspective Identification and System Analysis:* In this phase, risk analysts decide on the parties that are going to be involved in the information elicitation process. For instance, they may decide that only two perspectives one from the CEO and one from the marketing representative suffices their needs and requirements. Based on the information that they acquire with the help of each available perspective, they can identify the set of goals and evidences of system purpose and activity. Note that the set of these goals and evidences may be different from one perspective to the other.

III. *Preliminary Hazard Identification:* Threats, and vulnerabilities of a system can be identified by a close consideration of the goals and evidences that have been identified up to the current point. For example, the representative of a perspective can look at the set of goals and evidences that he/she has identified and think of the risks that threaten their operation. This hazard identification process does not produce a complete list of all system hazards, since neither each perspective is complete nor the elaboration has been extensive enough yet.

IV. *Perspective Integration:* Having identified a set of goals and evidences in each perspective, the risk analysts should consolidate all these information into a unique representation. Within this unique representation conflicts between the statements of the different perspectives should be resolved. Another fact that should also be considered is that different perspectives may be employing different terminology and differing qualitative expressions but be actually referencing the same issue. This phase intends to integrate all of the information that has been gathered from the perspectives, so that further analysis can be performed on this collective set.

V. *Process Refinement:* The concentration of each perspective on the issues more relevant to its position may cause the lack of elaboration on other matters and concerns. This deficiency can be overcome by refining the aggregate information gathered from all of the perspectives. In this way, each perspective will become aware of the goals or evidences that he/she may have missed by viewing the information provided by other perspectives. An instance of such a case may happen when the marketing perspective is so deeply concerned about advertising goals and evidences that he/she forgets to mention other more important goals; however, he/she will become aware of this fact by looking into the information that the other perspectives have provided. In this phase, goal and evidence refinements are made when a common agreement between all perspectives has been reached.

VI. *Risk Analysis:* Identification of risk in Astrolabe does not occur in a single phase and crosscuts all of the phases. The risks that are identified throughout all phases are analyzed in this phase. This analysis includes ranking goals, evidences, capabilities, and resources based on the degree of the threats that they pose. Based on this ranking, risk analysts will be able to concentrate on devising proper risk mitigation strategies.

VII. *Quality Measurement and Validation:* The quality of a risk analysis process is very much subject to the expectations and needs of risk analysts and system administrators; however, in any case, the integrity and correctness of the risk analysis process needs to be validated and the quality of the deliverables be assessed. In Astrolabe, the quality of the products, deliverables, and the analysis process is evaluated based on five metrics. These metrics are namely *reliability, consistency, completeness, traceability and unambiguity*, which will be introduced in the other parts of the paper.

2.2. Key Concepts

The risk analysis process in Astrolabe is based on five key concepts (See Figure 2). It aims to fully identify instances of these concepts for any target system. These information can then collectively describe a system and its status. These key concepts are:

- *Perspective,* is the mental and conceptional standpoint of the representative of a group of related individuals through which they examine the universe of discourse (e.g. the target system being examined.)[2].

- *Goal,* is the conceptualization of the ideal state of affair for a system. Any system may pursue multiple goals.

- *Evidence,* is an activity currently practiced in the universe of discourse for the attainment of one or more goals.

- *Obstacle,* is a goal or evidence, may be from the outside of the universe of discourse, that obstructs the attainment of a goal.

- *Hindrance*, relatively similar to an obstacle, is an evidence, from within or outside the universe of discourse that interrupts the normal operation of another evidence.

The concepts introduced in this section will be widely used throughout the paper, and will be also referenced in the metamodel proposed in Section 5.

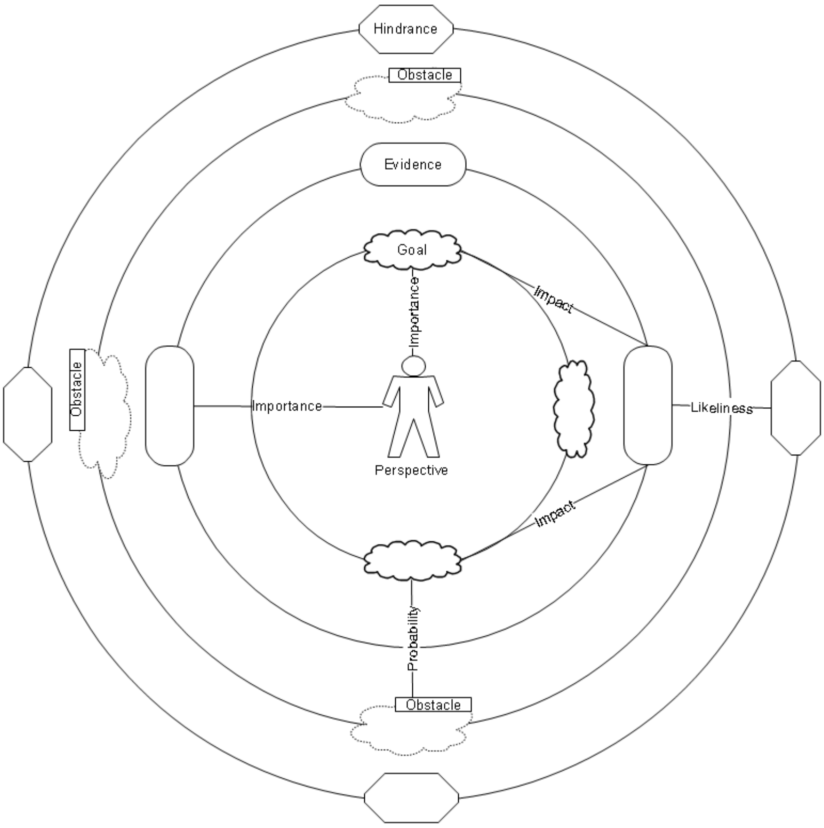

Figure 2. The Key Concepts in Astrolabe

3. Case Study

As a running example throughout the paper, we employ a subset of a mobile telecommunication service provider (GSM mobile network). This network is currently maintaining a connection with the Public Switched Telephone Network (PSTN). It is also providing its customers suitable data services. The stakeholders of this system intend to perform a risk analysis investigation, to both understand the current status of their system, and also any potential source of failure that may threaten the future of their system and business. In the various phases of the Astrolabe methodology, we will regularly visit this case study and incrementally extract the required information about this system and its sub-systems. These information will be used to develop the related models within Astrolabe in each phase.

4. The Astrolabe Methodology

In this section, we will introduce the Astrolabe methodology in detail. It is important to note that the methodology consists of seven major phases each of which can have one or more steps themselves.

4.1. Boundary Specification

Boundary specification is concerned with the identification of the limits of the risk analysis process from different perspectives such as time frame, target system, intention, and etc. This is important for various reasons:

- Creating a shared understanding between system stakeholders and administrators, and the risk analysis team. Since in many cases the risk analysis team is chosen from outside the system[3], boundaries of risk analysis should be properly specified.
- Avoiding the waste of resources during the risk analysis procedure by focusing on the defined specifications. In cases where no formal specification exists, efforts and resources may be exhausted on rather irrelevant tasks.
- Eliciting risks related to structural and social aspects of a system, that may not have been identified if system boundaries were not defined. For instance, the identification of a bottleneck in the borders of system communication with the outside world is only feasible if system borders are clearly identified.

Two approaches can be undertaken for defining the boundaries of a risk analysis process: *normalist*, or *realist* [(Scott, 1992)]. In a normalist approach, system stakeholders do not have a clear understanding of their needs; therefore, risk analysts should choose and advocate a boundary that most closely serves the requirements of the stakeholders and also their analytical principles. On the other hand, in an idealistic approach the participants (ranging from stakeholders to risk analysts) reach a common understanding of analysis requirements and an agreement on the desired boundaries. For systems that are currently being designed, an initial hypothetical boundary model should be devised. The model can evolve throughout the process if need be.

4.2. Perspective Identification and System Analysis

This phase is responsible for defining the perspectives that need to be present in the risk analysis procedure, and then from the identified perspectives, initially determine the high-level goals and evidences of the target system.

4.2.1. Step 1: Perspective Identification Cyert points out that most often system goals are defined by a negotiation process among a related set: the *dominant* *coalition* [(Cyert and March, 1963)]. The dominant coalition is a set of system participants that have an influential role in the decision making process of the target system. In many cases, the dominant coalition does not have a real representation within the universe of discourse, but its influence is felt. There are many factors that affect the makeup of the dominant coalition. Ownership is the most socially and legally defensible source of decision making in a system. This authority is usually delegated to system administrators. Besides ownership, the effect of labor can also be significant. The weight of labor power has direct relation with four factors: uncertainty, immediacy, non-substitutivity, and pervasiveness of the job it pursues. The higher the degree of each of these factors is for a specific labor position, the more influence it would have on the direction of the system. For instance, a technician working with a very vital and critical device for the system has a higher degree of command as compared with the others.

In Astrolabe, we adopt the notion of dominant coalition to select the set of perspectives that should be considered in the process. For each system, a representative of a group of members of the dominant coalition will be selected to act as a separate perspective. Therefore, each perspective will stand for the beliefs of its members by conveying their perception of the target system. It is important that the perspectives are carefully selected from the dominant coalition, so that all viewpoints are covered. For the running example, we identify four perspectives: Telecom CEO, Senior Telecom Advisor, Telecom Engineer, and Marketing Expert. This selection does not mean that these four perspectives are sufficient for the analysis of any mobile telecommunication service provider system, and have only been selected for this specific case study.

4.2.2. Step 2: System Analysis In this step, a set of initial goals and evidences should be identified by each perspective. Therefore, for each of the perspectives, the following tasks needs to be performed:

a. *Identify Goals*: The representatives of each perspective should be asked to list as many goals and objectives of the target system that they can think of. They should also assign an importance factor to each of the goals from their own understanding of the relative significance and value of the goal. The range of the importance value can be determined by the risk analysis team. In this paper, we permit a range of values within $(0, 1]$, where the higher the value is, the more important the goal will be. It should be noted that the assignment of value zero is not permitted, since goals with a zero importance degree are actually not considered as system goals.

   As an example, the senior telecom advisor perspective has initially identified four goals: interoperability with the PSTN network, cater data services for cell phone users, and high network coverage and acceptable QoS, and provisioning new services in the coming year. This perspective has assigned $\{0.8, 0.6, 0.8, 0.4\}$ as the importance values of these goals. The interpretation of these values is that the first and third goals are the most important, while the last goal does

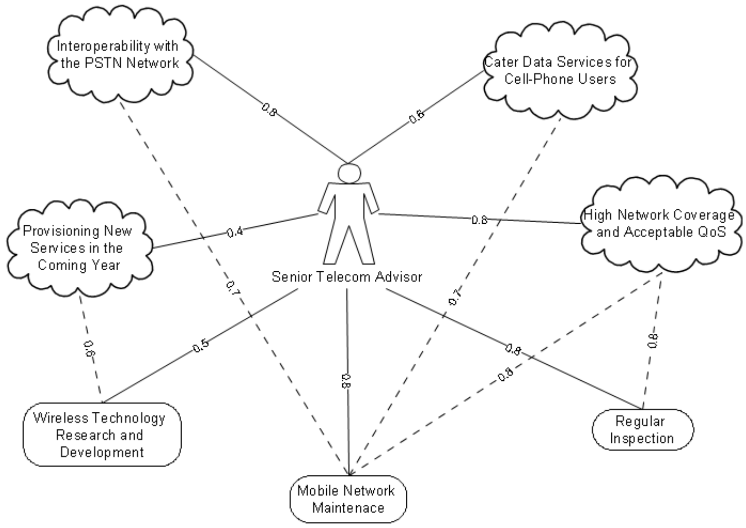
Interoperability with the PSTN Network
Cater Data Services for Cell-Phone Users
Provisioning New Services in the Coming Year
High Network Coverage and Acceptable QoS
Senior Telecom Advisor
Wireless Technology Research and Development
Regular Inspection
Mobile Network Maintenace
0.8
0.6
0.4
0.8
0.7
0.7
0.6
0.5
0.8
0.8
0.8
0.8

Figure 3. The Initial Perception of the Senior Telecom Advisor Only Consisting of Goals and Evidences

not possess that much of a priority and significance from the point of view of the senior telecom advisor (See Figure 3).

b. *Identify Evidences*: Each system desires to perform a set of actions to satisfy its goals. In many cases, there is a slight deviation from the desired state of execution when the action is being performed. For this reason, Astrolabe focuses on evidences derived from the actual process that is currently being practiced and not the desired form of that action, so that risks are identified for a realistic situation and not an idealistic case.

To gather evidences from a system, each perspective is asked to list and describe all of the actions that it thinks that the system is currently performing. Similar to goals, evidences should also be assigned importance values. The importance values assigned to each evidence will reveal the value of that evidence within the universe of discourse. As it can be seen in Figure 3, the senior telecom advisor has listed three evidences namely regular inspection, mobile network maintenance, and wireless technology research and development as system evidences. It has also assigned the following importance values to the evidences, respectively: $\{0.8, 0.8, 0.5\}$.

c. *Inter-relate Goals and Evidences*: Typically the actions that a system performs are much easier to identify than its abstract goals. The reason for this is that actions are frequently seen or performed without reviewing the goals attached to them. Hence, while a system may be performing a task to reach a goal, it may not be consciously aware of the goal at all points of time. For this reason, identified evidences should be connected to the stated goals by each perspective. Performing this task would allow each perspective to re-visit its goals and evidences, and identify any missing goal or evidence. As an example, suppose that the senior telecom advisor had initially missed the high network coverage and acceptable QoS goal. Later, it identifies the regular inspection task. At the point that it needs to inter-relate goals and evidences, it finds out that there are no supporting goals for the regular inspection evidence. Here, the perspective can go back and add the suitable goal. The vice-versa can also be performed when there are no supporting evidences for a goal.

Besides relating goals and evidences, a perspective should also specify the degree of contribution of an evidence in attaining a goal. This value is named evidence impact. In Figure 3, the senior telecom advisor thinks that the 'wireless technology research and development' evidence has a direct effect on the 'provisioning new services in the coming year' goal and its impact is 0.6.

At the end of this phase, the following set of deliverables should be developed:

i. A list of perspectives participating in the process

ii. An initial set of weighted goals and evidences related to each perspective

iii. A graph depicting the relationship between the goals and evidences for each perspective

4.3. Preliminary Hazard Identification

This phase is responsible for deriving the hazards that may threaten the target system from the set of goals and evidences that have been specified by each perspective.

4.3.1. Step 1: Hazard Identification using Guide Words Risks are the result of a threat or vulnerability posed from/to a system goal or evidence. To identify these hazards, Astrolabe uses a set of guide words commonly used in methods such as HAZOP [(Redmill et al., 1999)] to simply deviate the description of a goal or evidence from its actual status. Through the application of these guide words, the analysts can identify any probable source of threat. A list of commonly used guide words includes but is not limited to {No, Less, More, Part Of, As Well As, Reverse, Other Than}.

Guide words can be selected according to the nature of the universe of discourse. These guide words will be applied to all of the goals, and evidences of each perspectives. If the caused deviation is identified as a probable risk, it will be considered for further analysis. Figure 4 shows the result of this process applied to the initial goal-evidence graph of the telecom engineer perspective.

For example, the application of the 'Part of' guide word on the 'suitable connection to the data network' goal suggests the 'unacceptable connection' obstacle.

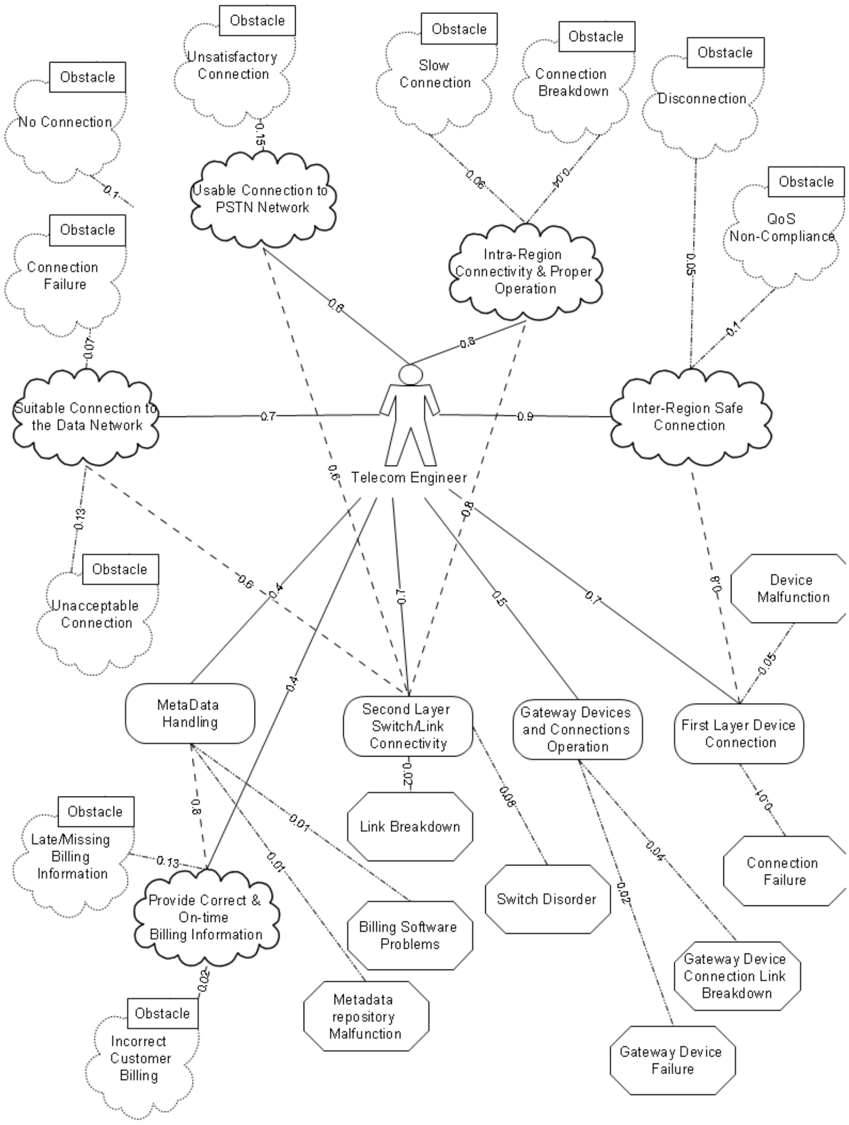
Obstacle
No Connection
0.1
Obstacle
Unsatisfactory Connection
0.15
Usable Connection to PSTN Network
Obstacle
Slow Connection
Obstacle
Connection Breakdown
0.06
0.04
Obstacle
Disconnection
Obstacle
QoS Non-Compliance
0.05
0.1
Intra-Region Connectivity & Proper Operation
Obstacle
Connection Failure
0.07
0.6
0.8
Suitable Connection to the Data Network
0.7
Telecom Engineer
0.9
Inter-Region Safe Connection
0.13
Obstacle
Unacceptable Connection
0.6
0.6
0.4
0.8
0.7
0.5
0.7
0.8
Device Malfunction
0.05
0.4
MetaData Handling
Second Layer Switch/Link Connectivity
Gateway Devices and Connections Operation
First Layer Device Connection
0.02
0.08
0.01
Link Breakdown
0.8
0.01
0.01
0.04
Connection Failure
Obstacle
Late/Missing Billing Information
0.13
Provide Correct & On-time Billing Information
Switch Disorder
0.02
Billing Software Problems
Gateway Device Connection Link Breakdown
0.02
Obstacle
Incorrect Customer Billing
Metadata repository Malfunction
Gateway Device Failure

Figure 4. The Telecom Engineer Perspective after the Application of Guide Words

Since the experience of the telecom engineer shows that this is a rational result, it is added to the graph as an obstacle. Similar to this process, guide words are also applied to evidences and probable hindrances are identified and added to the graph. For any of these obstacles, or hindrances the analysis team should look for actual previous facts as to how probable their occurrence is. A possible way to do this may be to count the number of times that these events have been previously observed. In cases were such information does not exist, the perspective should provide an estimated value itself. The telecom engineer perspective, for instance, has stated that with the probability of 13%, the 'suitable connection to the data network' goal will face an 'unacceptable condition' obstacle.

4.3.2. Step 2: Hazard Elaboration Once the obstacles and hindrances that threaten the target system are identified through the application of guide words on goals and evidences, the details of these hazards needs to be more deeply elaborated. In this step, the analysts should identify the set of possible causes of an obstacle or hindrance. They should also clearly depict what consequences these threats pose on the universe of discourse. Going back to our running example, lets consider the obstacles that may impede the proper attainment of the 'high network coverage and acceptable QoS' goal in the senior telecom advisor perspective. As it can be seen in Figure 5, this goal faces two obstacles: 'mobile network breakdown', and 'inefficient network design'. The perspective has also specified that the probability of any of these perspectives are 5%, and 1%, respectively. Through more elaboration, the perspective has come up with different reasons for why these obstacles may take place. For instance, 'mobile network breakdown' may be a result of 'network overload', 'power outage', and/or 'device failure'. The consequence of this obstacle has also been identified which is 'customer dissatisfaction'.

After identifying the causes of a hazard (H_i), the perspective should specify the conditional cause probability, $\alpha(C_j, H_i)$, for each of the identified causes(C_j).

Definition Conditional Cause Probability $\alpha(C_j, H_i)$ is the conditional probability of C_j given H_i, which is equal to $P(C_j|H_i)$. Note that the values of any $\alpha(C_j, H_i)$ may not be mutually exclusive; therefore, a hazard may be set off by one or more causes.

In Figure 5, the conditional cause probability of 'network overload' for 'mobile network breakdown' is 0.4, which means that if a 'mobile network breakdown' obstacle occurs, it has been caused by a 'network overload' with the probability of 0.4. Moreover, the perspective should also specify what the conditional consequence probability for each of the consequences (Con_j) of a hazard is.

Definition Conditional Consequence Probability $\beta(Con_j, H_i)$ is the conditional probability of Con_j given H_i, which is equal to $P(Con_j|H_i)$. For any hazard (H_i), the following equation should always hold:

$$\sum_j \beta(Con_j, H_i) > 0 \tag{1}$$

More specifically $\beta(Con_j, H_i)$ depicts the probability of the occurrence of a consequence, if a particular hazard happens. For this reason, the sum of all $\beta(Con_j, H_i)$ values for a given hazard (H_i) cannot be zero. This is due to the fact that a hazard with no effect is in reality not a hazard. From the senior telecom perspective, the 'inefficient network design' obstacle has two consequences: 'inefficient capacity for new customers' and 'increased failure in network'. The conditional consequence probability for these two consequences are 0.7 and 0.5, respectively. These values show that if the network design is inefficient then with a probability of 70% and 50% these two consequences will occur.

Further into analysis, each perspective has to identify a set of mitigation strategies or plans that they would undertake if a hazard takes place. These mitigation strategies are attached to the related causes of each hazard. This means that if the system feels that one of the causes of a hazard is too dangerous, one of the proposed mitigation strategies attached to that cause should be selected and performed. The senior telecom advisor perspective has proposed two mitigation strategies to overcome the 'inefficient network design' obstacle, for cases where 'change in population distribution' is perceived to be the major reason that may eventually cause this hazard to happen. These mitigation strategies are 1. 'plan and anticipate population distribution', and 2. 'expand network capacity evenly'.

The main concern with the mitigation strategies is making an appropriate choice for a selection criteria. The selection criteria is very much dependant on the context of the universe of discourse and the major concerns of the system; therefore, a unique selection criteria cannot be proposed that suits all application areas. In Astrolabe, each mitigation strategy is annotated with three parameters: Cost (γ), Time (δ), and Effectiveness (ζ). Based on these parameters the suitability of a mitigation strategy is defined as $f(\gamma, \delta, \zeta)$; where γ shows the cost of performing the mitigation strategy, δ specifies the time needed to execute the mitigation strategy, and ζ depicts the effectiveness of the anticipated results of the mitigation strategy. Hence, the i^{th} mitigation strategy is the most suitable choice if:

$$\forall j \in \jmath \longrightarrow f(\gamma_i, \delta_i, \zeta_i) = Max(f(\gamma_j, \delta_j, \zeta_j)) \tag{2}$$

where $\jmath$ is the number of mitigation strategies proposed for a specific cause. In Figure 5, the senior telecom advisor perspective has assigned values based on two base factors (a for cost, and b for time). It has also given a value between $[0, 1]$ for the effectiveness of the mitigation strategy. For example, it has assigned $3a$, $4b$, and 0.4 to the 'install backup routes' mitigation strategy which is attached to the 'network overload' cause.

4.3.3. Step 3: Volatility Analysis In Astrolabe, goals are the central point of focus, since their attainment is considered to be the most important reason of the existence of the system. Until this step, each perspective has expressed its understanding of the system goals, evidences, and the hazards (obstacles and hindrances) that threaten the operation of the system. It has also specified the probable causes of the hazards, their consequences and the possible set of mitigation strategies and

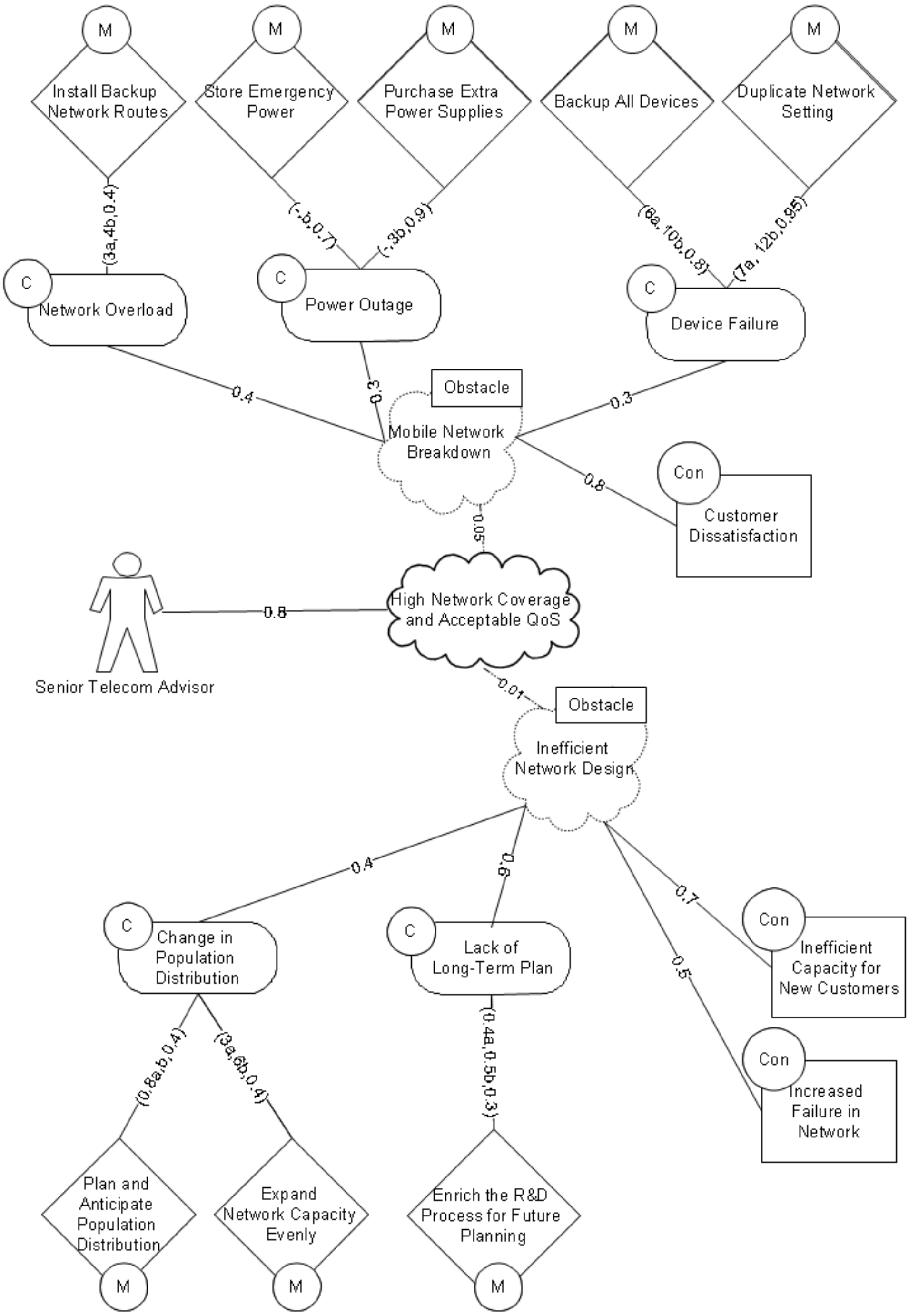
M
Install Backup Network Routes
M
Store Emergency Power
M
Purchase Extra Power Supplies
M
Backup All Devices
M
Duplicate Network Setting
(3a,4b,0.4)
(-,b,0.7)
(-,3b,0.9)
(6a, 10b,0.8)
(7a, 12b,0.95)
C
Network Overload
C
Power Outage
C
Device Failure
0.4
0.3
Obstacle
0.3
Mobile Network Breakdown
0.8
Con
Customer Dissatisfaction
0.05
High Network Coverage and Acceptable QoS
0.8
Senior Telecom Advisor
0.01
Obstacle
Inefficient Network Design
0.4
0.8
0.7
0.5
C
Change in Population Distribution
C
Lack of Long-Term Plan
Con
Inefficient Capacity for New Customers
Con
Increased Failure in Network
(0.8a,b,0.4)
(3a,6b,0.4)
(0.4a,0.5b,0.3)
Plan and Anticipate Population Distribution
M
Expand Network Capacity Evenly
M
Enrich the R&D Process for Future Planning
M

Figure 5. The Result of a Sample Hazard Elaboration Process on the 'High Network Coverage and Acceptable QoS' Goal of the Senior Telecom Advisor Perspective

Table 1. Notations

Symbol	Description
$I_e(l_i)$	Importance of the l^{th} evidence attached to goal i
$\|obs_i\|$	Number of obstacles attached to goal i
$\|evid_i\|$	Number of evidences attached to goal i
$Pr_o(k,j)$	Probability of the occurrence of obstacle k from the j^{th} perspective
$\sum_{n\in\|con_k\|} S_o(n)$	Sum of the obstacle consequence severity of the k^{th} obstacle
$\|hind_{l_i}\|$	Number of hindrances attached to the l^{th} evidence of goal i
$Pr_h(m,j)$	Probability of occurrence of the m^{th} hindrance from the j^{th} perspective
$\|con_k\|$	Number of consequences of obstacle k
$S_h(m,j)$	Hindrance consequence severity of the m^{th} hindrance from the j^{th} perspective
$\|E(i,j)\|$	Number of evidences attached to goal i from the j^{th} perspective

plans. In this step, the analysts should investigate the stability of the goals and evidences that each perspective has introduced.

Definition Goal Stability $\vartheta(Goal_i, P_j)$ is defined for perspective P_j based on three factors: goal importance $(\rho_{i,j})$, threat impact $(\varrho_{i,j})$, and supportive evidences $(\sigma_{i,j})$. $\rho_{i,j}$ is the importance value assigned to $Goal_i$ by P_j. $\varrho_{i,j}$ is the sum of the threats imposed on $Goal_i$, and $\sigma_{i,j}$ is the inverse number of supporting evidences attached to $Goal_i$. (The employed notations have been introduced in Table 1.)

$$\varrho_{i,j} = T_o(i,j) + \sum_{l_i \in |evid_i|} (I_e(l_i) \times T_e(l_i,j)), \tag{3}$$

$$T_o(i,j) = \sum_{k \in |obs_i|} (Pr_o(k,j) \times \sum_{n \in |con_k|} S_o(n)), \tag{4}$$

$$T_e(l_i,j) = \sum_{m \in |hind_{l_i}|} (Pr_h(m,j) \times S_h(m,j)), \tag{5}$$

$$\sigma_{i,j} = \frac{1}{|\ E(i,j)\ |}, \tag{6}$$

$$\vartheta(Goal_i, P_j) = \overrightarrow{(\rho_{i,j}, \varrho_{i,j}, \sigma_{i,j})}. \tag{7}$$

As an example, we calculate the stability of the ‘high network coverage and acceptable QoS’ goal (i) from the senior telecom advisor perspective (j) shown in Figure 5. Since there are no evidences attached to goal i in that figure, we do not consider the effect of evidences in the calculation of $\varrho_{i,j}$; therefore,

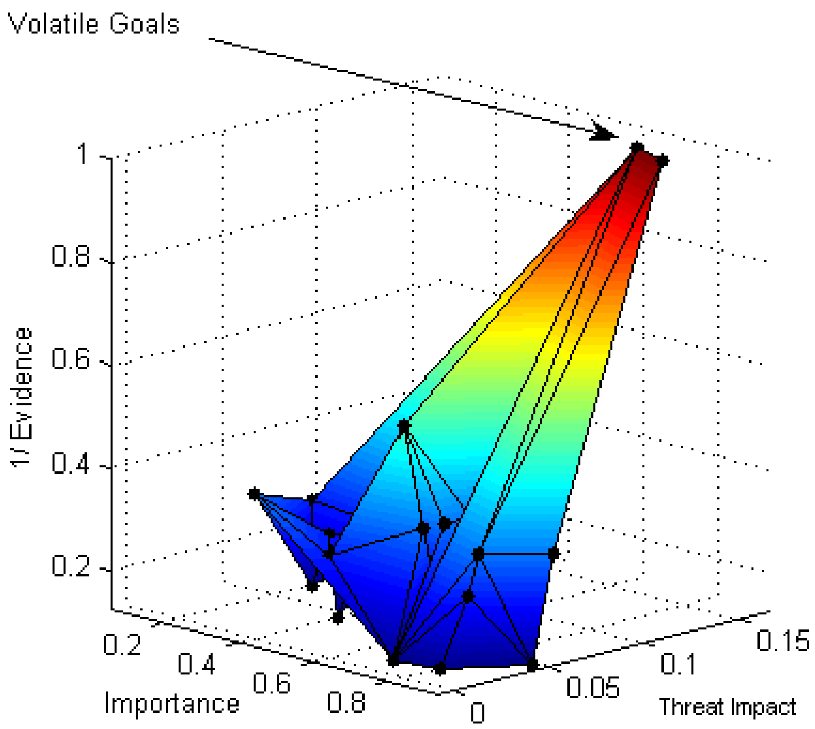

Figure 6. A Sample Goal Stability Diagram for a Single Perspective

$$\varrho_{i,j} = (0.05 \times 0.8) + (0.01 \times (0.7 + 0.5)) = 0.052$$
$$\rho_{i,j} = 0.8$$

and if we assume that there are five evidences attached to this goal (not shown in the figure), we will have:

$$\sigma_{i,j} = 0.2$$
$$\vartheta(i,j) = \overrightarrow{(0.052, 0.8, 0.2)}$$

The stability of an evidence is calculated similarly to that of a goal; with the slight difference of focusing on each evidence rather than the goals. For each perspective, the goal and evidence stability vectors of all the goals and evidences need to be calculated separately. Based on these data, the stability vectors of the goals and evidences are plotted on two different three dimensional diagrams (one for the goals and one for the evidences). If there are n perspectives present in the analysis, $2 \times n$ diagrams need to be drawn. Figure 6 shows a sample goal stability diagram. The black dots show the end of each goal stability vector.

In the goal and evidence stability diagrams, the longer the vector related to a goal or evidence is, the more attention is required to be focused on that goal or evidence.

This is because of the factors that are present in the makeup of the stability factor. A longer stability vector means that the goal or evidence has a high importance value, a high threat impact value and very few evidences or goals supporting it. Certainly, such a goal or evidence requires more attention and elaboration. To identify such cases, we define a *volatility zone* in the stability diagrams. The goals or evidences that are located within this zone are considered to be volatile and hence need closer consideration.

Definition Volatile Zone (Ψ) is a subspace of $\Re^3$ ($\Psi \subseteq \Re^3$) where for every stability vector $\vartheta(i,j) = (\rho_{i,j}, \varrho_{i,j}, \sigma_{i,j}) \in \Psi$:

$$\rho_{i,j} > \Psi_\rho, \tag{8}$$

$$\varrho_{i,j} > \Psi_\varrho, \tag{9}$$

$$\sigma_{i,j} > \Psi_\sigma. \tag{10}$$

In this definition, Ψ_ρ, Ψ_ϱ, and Ψ_σ specify the lower boundaries of the volatile zone. The values of these parameters are very much dependant on the degree of elaboration that the risk analysts intend to undertake. In any case, the more vacant the volatile zone is, the more stable the current setting of the system is. Other than the current instability of the target system, insufficient amount of detail and incomplete revelation of goals, evidences, obstacles, and hindrances in the risk analysis process may be the reason behind a populated volatile zone. To overcome this situation the following tasks can be performed:

- The analysts can gather more information from the universe of discourse, and ask each perspective to elaborate more on the details of the information that they have provided thus far. The result of the volatility analysis can also be given to each perspective, so that they know which goal, and/or evidence requires more attention. The perspectives may add or remove different information to/from their previous model. They may also adjust the significance of the annotation values (e.g. increase the importance value of a goal, or decrease the severity of a consequence of an obstacle).

- In the systems that are currently in their design process, each perspective may be persuaded to change the goals and evidences that it initially thought were essential for the system, after observing the results of the volatility analysis. It is important to note that the change of goals and evidences is only feasible for the systems that are currently under design. This is because the systems that are currently running cannot simply decide to change their operational scenarios and objectives without actual implementation.

These tasks can be iteratively repeated, until the best possible result from the volatility analysis is reached.

Table 2. Deviation of the Anticipated Values from the Actual Values in Figure 7

Source Perspective	Evaluated Perspective	Dev. in Interoperability Goal	Dev. in Cater Data Services Goal
Senior Telecom Advisor	Telecom Engineer	0.6770	0.3651
	Marketing Expert	1.6429	-
Telecom Engineer	Senior Telecom Advisor	0.3604	1.4048
	Marketing Expert	1.2664	-
Marketing Expert	Senior Telecom Advisor	0.6823	-
	Telecom Engineer	0.921	-

4.3.4. Step 4: Annotation Value Validity Checking Each perspective may loose its consistency in giving the annotation values during the analysis process. For this reason, these values should be cross-checked to make sure that inconsistencies have not occurred. To perform the cross-check evaluation two lists need to be created. The first list should contain all of the evidences present in a single perspective based on their importance values in decremental order. The most important evidences from the viewpoint of this perspective will be placed higher in the list. A second list decrementally rank-orders the same evidences based on their average impact on system goals ($\overline{goal\_importance \times evidence\_impact}$). The result of both lists should be similar, since the idea behind them is conceptually the same. Both of the lists are showing the significance of an evidence: the first list based on the directly assigned values, and the second one through inference. If the order of evidences in these two lists is incompatible with each other, then the information provided by that perspective should be thoroughly revised.

4.3.5. Step 5: Initial Cross-perspective Consistency Evaluation Until this point in the methodology, each perspective has only been focused on its own information, regardless of the viewpoint of the other perspectives. Since in the next phase, the results of the analyses from each perspective are going to be consolidated into one unified representation for all perspectives, it is strictly required that the analysts make sure that all the perspectives have a clear and common understanding of the target system. Therefore, the following procedure needs to be performed:

```
Foreach Perspective $P_i$ do {
  Normalize annotation values
  Selectall Perspectives like $P_j$ with at least one similar G/E
  Annotate all common G/E instances by $P_i$ for $P_j$
  Calculate the deviation of the given value from the actual value
} /* G/E stands for Goal/Evidence */
```

Figure 7, and Table 2 show the result of this process which has been performed on the common goals of the three perspectives of our example. The values of the

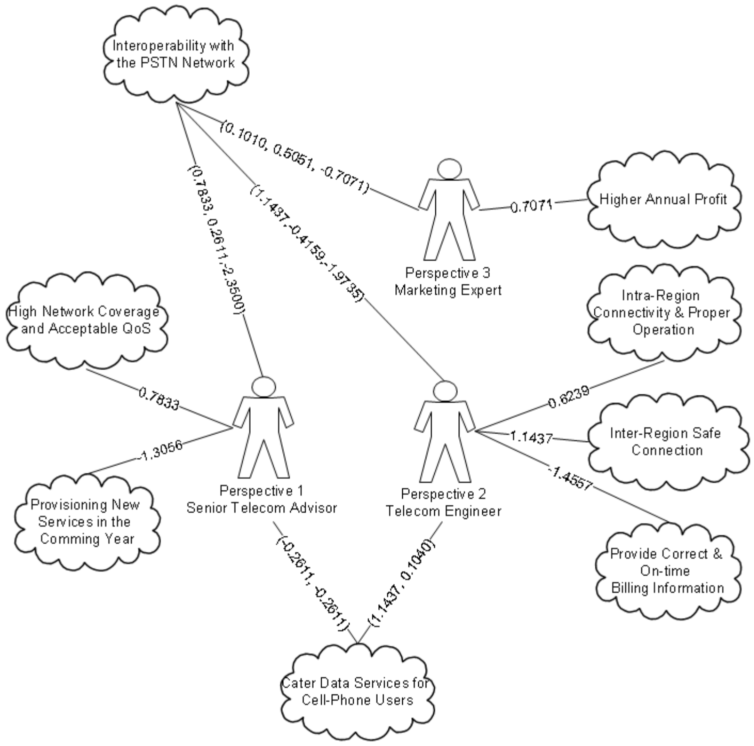
Interoperability with the PSTN Network
(0.1010, 0.5051, -0.7071)
(0.7833, 0.2611,-2.3500)
(1.1437,-0.4159,-1.9735)
Perspective 3
Marketing Expert
0.7071
Higher Annual Profit
High Network Coverage and Acceptable QoS
Intra-Region Connectivity & Proper Operation
0.7833
-1.3056
0.6239
1.1437
Inter-Region Safe Connection
-1.4557
Provisioning New Services in the Comming Year
Perspective 1
Senior Telecom Advisor
Perspective 2
Telecom Engineer
Provide Correct & On-time Billing Information
(-0.2611, -0.2611)
(1.1437, 0.1040)
Cater Data Services for Cell-Phone Users

Figure 7. Initial Cross Perspective Consistency Checking for Three Perspectives

annotations of each perspective have been normalized within the context of that perspective (so that comparisons can be made). In Astrolabe, the normalization of a set of values is performed by first subtracting the set mean from each variable and then dividing the result by the standard deviation of the set. After normalization, each perspective is asked to annotate what he thinks the other perspectives have rated the goals that they have in common. Based on this, the difference between the anticipated value and the actual value is calculated which shows the degree of conceptual misalignment of the perspectives. From the calculated values, those values that are more than ψ are considered as inconsistent. In these cases, the source perspective needs to go back and revisit its asserted information.

Founded on Chebyshev's theorem [(Walpole, 1983)], we define ψ as sum of the average misalignment values (e.g. values shown in Table 2) and their standard deviation. For the values in Table 2, their mean value is 0.9935, and their standard deviation is 0.4801; therefore, ψ will be 1.4736. Using this value, it can be inferred that the senior telecom advisor perspective is misaligned with the marketing expert perspective ($1.6429 > 1.4736$) on the 'interoperability with the PSTN network' goal, so it needs to revise its information.

At the end of this phase, the following deliverables should be produced separately for each perspective:

i. An enhanced list of annotated goals and evidences

ii. For each goal and evidence its related obstacles, and hindrances should be identified.

iii. For all threats (obstacles and hindrances), their causes, consequence and mitigation plans and strategies should be identified.

iv. Two separate stability diagrams for system goals and evidences should be drawn.

4.4. Perspective Integration

The information gathered in the previous phases are centered around each perceptive. Therefore, each set of information can only reveal that perspective's conception of the system, which is not sufficient for a complete analysis. To create a unified representation, all of the information in each perspective should be integrated into a single cohesive view.

4.4.1. Step 1: Information Integration To consolidate all of the information in different perspectives into a unified perspective, the following procedure should be followed:

```
Set integratedView = ∅
Foreach Perspective $P_i$ do {
  Foreach Item as Concept in $P_i$ do
    If (no Conceptually_Similar Item in integratedView)
      Insert Item into integratedView
  } Insert Normalized Annotations from $P_i$ into integratedView
}
```

The above procedure reads as follows. The final information model which is the result of this process will be accumulated in the *integratedView* set, which is initially empty. To start, one of the perspectives is randomly selected. For any item such as a goal, evidence, hindrance, obstacle, cause, mitigation plan, or consequence (concept) in that perspective, a check is performed to see if other perspectives have already inserted that concept into the *integratedView* set or not. This check not only should search for grammatical and dictation similarities, but should also be aware of conceptually similar concepts that have been expressed using different wordings by different perspectives. Once all the concepts present in the perspective have been either added to or found in the *integratedView* set, the related annotation

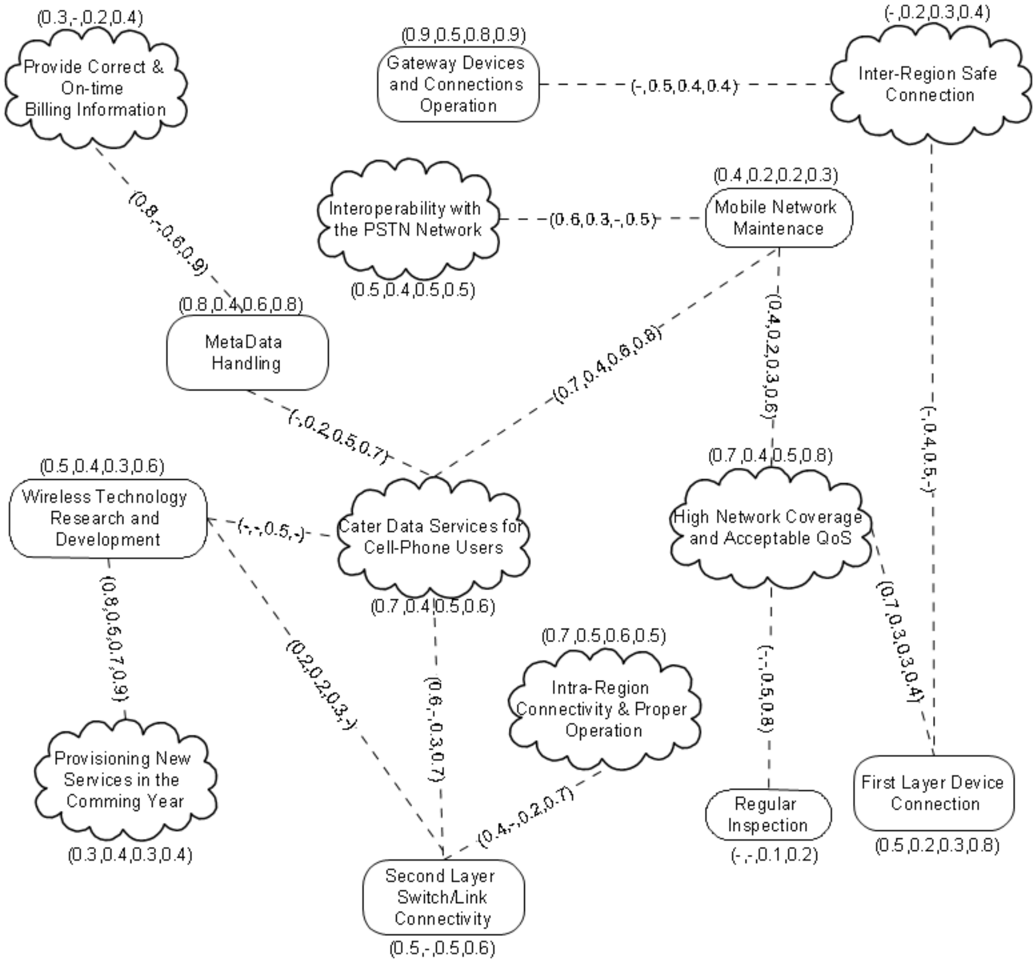

Figure 8. The Partial Integration of Information from Multiple Perspectives. Annotation Values that did not Have Any Match in the Corresponding Perspective have been Shown by a - Mark.

values assigned to each concept (or to multiple concepts such as the evidence impact factor on a goal) should be normalized within the context of that perspective and then added to the *integratedView* set. This process should continue until all of the concepts and annotatoion values of all perspectives have been added to the *integratedView* set. Figure 8 depicts a partial view of the result of this process performed on the information gathered from the four perspectives in our running example.

As it can be seen in Figure 8, in contrast with the annotation values of each perspective, the integrated view consists of annotation vectors. This is because the annotation values of all the perspectives have been normalized and positioned in the corresponding place. For example a vector like $[-, 0.1, 0.2, -]$ shows that the first and last perspectives do not consider the related concept in their information, while the second and third perspectives assign 0.1 and 0.2 to it. It should also be noted that the length of each annotation vector is equal to the number of perspectives involved in the study.

The collective view of information allows the perspectives to get a new insight into the system and allows them to get familiar with the point of view of the other perspectives. This insight may also lead them to change some of their initially assigned annotation values.

4.4.2. Step 2: Final Cross Perspective Consistency Evaluation Before finalizing and accepting the integration, the information provided by each perspective needs to be verified. The major difference between the process in this step with the one explained in Section 4.3.5 is that the latter only considers the annotation values that are common between two perspectives for its analysis; while in this stage the analysis evaluates all of the information provided by the perspectives as a whole.

To perform the analysis, a table needs to be drawn. The rows of the table list all of the reasons why an annotation value may have been provided (e.g. importance to a goal or evidence, impact factor of an evidence for a goal, etc.). The columns of the table depict all of the participating perspectives and the values that they have assigned to each row. In each row, and for all the perspectives, the difference of the value assigned by a perspective from the average value of that row is calculated ($difference\_values$). Similar to the analysis performed in Section 4.3.5, in each perspective the number of values that their difference value is more than φ is counted (ξ_i).

$$\varphi = \overline{difference\_values} + STD(difference\_values) \tag{11}$$

Based on this analysis, ξ_i will show the number of cases where the opinion of perspective i is really different with that of the others. Here, the perspectives with a large number for ξ are considered to be inconsistent. In this case, the analysts should either allow this perspective to adjust itself, or abandon that perspective from the analysis.

Table 3 shows the results of this analysis that has been performed on the four perspectives of our case study. The analysis shows that marketing expert perspective is the most inconsistent perspective among the others ($\xi_4 = 5$), and requires a thorough re-visit. In this example, $\overline{difference\_values}$ is 0.1609 and $STD(difference\_values)$ is 00.1155; therefore φ is equal to 0.2764.

The completion of this phase produces a unified perspective and understanding of the universe of discourse that includes system goals, evidences, obstacles, hindrances, threat causes, consequences, and mitigation plans along with related annotation vectors. Analysts can now replace annotation vectors with the average of each vector's values.

Table 3. Analyzing the Degree of Cross Perspective Consistency

	T. CEO		Sr. T. Advisor		T. Engineer		M. Expert		Mean (τ)
Evaluated Criteria	*val*	$val - \tau$	*val*	$val - \tau$	*val*	$val - \tau$	*val*	$val - \tau$	
Provide Correct & On-Time Billing Information	0.3	-0.17	-	-	0.2	-0.27	0.9	+0.43	0.47
Gateway Devices and Connections Operation	0.9	+0.125	0.5	-0.275	0.8	+0.025	0.9	+0.125	0.775
Inter-Region Safe Connection	-	-	0.2	-0.1	0.3	0	0.4	+0.1	0.3
Interoperability with the PSTN Network	0.5	+0.025	0.4	-0.075	0.5	+0.025	0.5	+0.025	0.475
Mobile Network Maintenance	0.4	-0.025	0.2	-0.225	0.2	-0.225	0.9	+0.375	0.425
Metadata Handling	0.8	+0.15	0.4	-0.25	0.6	-0.5	0.8	+0.15	0.65
Wireless Technology Research and Development	0.5	+0.05	0.4	-0.05	0.3	-0.15	0.6	+0.15	0.45
Cater Data Services for Cell-Phone Users	0.7	+0.15	0.4	+0.15	0.5	-0.05	0.6	+0.05	0.55
High Network Coverage and Acceptable QoS	0.7	+0.1	0.4	-0.2	0.5	-0.1	0.8	+0.2	0.6
Provisioning New Services in the Coming Year	0.3	-0.15	0.4	-0.05	0.3	-0.15	0.8	+0.35	0.45
Second Layer Switch/Link Connectivity	0.5	-0.033	-	-	0.5	-0.033	0.6	+0.067	0.533
Intra-Region Connectivity & Proper Operation	0.7	+0.05	0.5	-0.15	0.6	-0.05	0.8	+0.15	0.65
Regular Inspection	-	-	-	-	0.1	-0.3	0.7	+0.3	0.4
First Layer Device Connection	0.5	+0.05	0.2	-0.25	0.3	-0.15	0.8	+0.35	0.45
ξ_i	0		0		1		5		-

4.5. *Process Refinement*

It is possible that the unified information about the target system need more refinement. Refinement may be required since the information that has been provided by each perspective can be rather coarse grained. The participating perspectives are in many cases unfamiliar with how goals and evidences can be generalized or instantiated. For example in Figure 8, 'wireless technology research and development' has been identified as an instance of the target system's evidences. It is clear that this evidence is too coarse grained and needs to be further operationalized.

From this phase forward, unlike the previous phases, activities are mostly performed by the analysts while they are benefiting from the help of the participating perspectives.

4.5.1. Step 1: Goal Refinement and Evidence Operationalization Refinement and operationalization of goals and evidences can be carried out using appropriate question words. Question words can accompany any goal and/or evidence to clarify their intention or model of performance. In Astrolabe, three main question words are used, namely: 'Why', 'How', and 'How Else'. These question words are explained in more detail in the following lines with the help of Figure 9.

- 'Why' is mainly used for clarifying the intention and purpose of an action. It can help the abstraction of a goal or evidence. Consider the 'constant signal quality assessment' evidence. To find out what has been the roots of this evidence a why question can be asked: *Why perform 'constant signal quality assessment'?*.

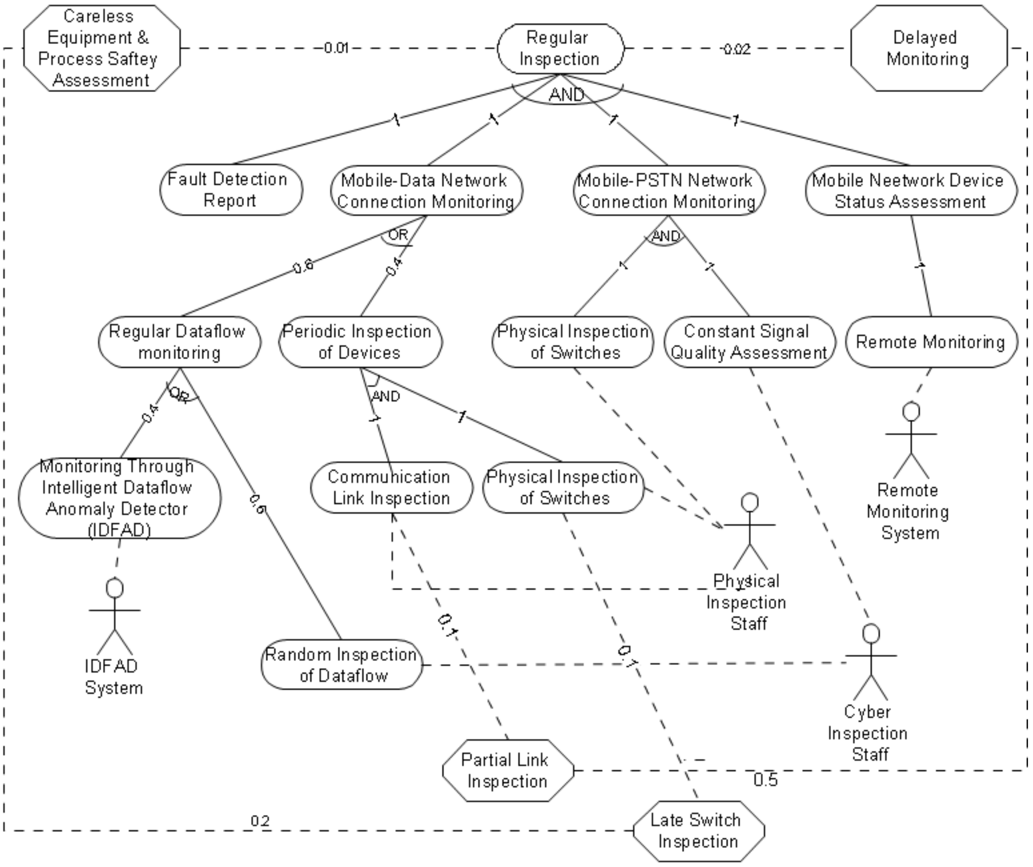
Careless Equipment & Process Saftey Assessment
0.01
Regular Inspection
0.02
Delayed Monitoring
AND
1
1
1
1
Fault Detection Report
Mobile-Data Network Connection Monitoring
Mobile-PSTN Network Connection Monitoring
Mobile Neetwork Device Status Assessment
OR
0.6
0.4
AND
1
1
1
Regular Dataflow monitoring
Periodic Inspection of Devices
Physical Inspection of Switches
Constant Signal Quality Assessment
Remote Monitoring
OR
0.4
0.6
AND
1
1
Monitoring Through Intelligent Dataflow Anomaly Detector (IDFAD)
Communication Link Inspection
Physical Inspection of Switches
Remote Monitoring System
Physical Inspection Staff
IDFAD System
Random Inspection of Dataflow
0.1
0.1
Cyber Inspection Staff
Partial Link Inspection
0.5
0.2
Late Switch Inspection

Figure 9. A Sample Process Refinement for the 'Regular Inspection' Evidence. The Structure is Similar to a Typical Fault Tree [(Haimes, 2004)].

The answer to this question is: *To monitor mobile-PSTN network connection* which leads us to the 'mobile-PSTN network connection monitoring' evidence.

- 'How' questions provide analysts with the chance of operationalizing goals and evidences. For example, the 'periodic inspection of devices' evidence can be broken into two finer grained evidences by asking: *How can* 'periodic inspection of devices' *be performed*? 'communication link inspection' and 'physical inspection of switches' are the two answers to this question.

- The answers of 'How' questions are mainly focused on only one solution. Although these solutions may have multiple parts (e.g. the previous example), all of their parts should be performed together, or in other words they are connected to each other with an 'And' connector. Other than this kind of connection, a goal or evidence may be achievable through different solutions or paths. To find these solutions 'How Else' questions need to be asked. The answers to these questions have an 'Or' connection with each other. The operationalization of the 'regular dataflow monitoring' is an example of such a case.

There is always the chance that the identification of goals is driven towards *Utopian* and/or *Unstated* goals [(Gross, 1969)]. Utopian goals are the goals that are ranked as highly important but no real world evidence is supporting their actual attainment. Unstated goals on the other hand, are the goals that are under-estimated by their importance value, but are highly involved in the operation of system evidences. Risk analysts should be aware of such cases, and elaborate more when they are encountered.

4.5.2. Step 2: Linking Goals and Evidences Through the application of the question words on the previous information, new goals and/or evidences may be detected. For all the newly detected concepts proper annotation values need to be provided. It is important to notice that while new annotation values are assigned to these concepts, the importance value of the child goals and/or evidences cannot be higher than that of its parent. For instance in Figure 9, the overall importance value of the 'fault detection report' evidence cannot be higher than the importance value of the 'regular inspection' evidence.

4.5.3. Step 3: Detecting Obstacles and Hindrances The process of identifying obstacles and hindrances for the newly detected goals and evidences is similar to what has been previously introduced in Section 4.2.2; however, it should be noted that the obstacles or hindrances that are specified in this step have either been previously identified within a higher level threat in the previous phases, or are a new threat that have not been discovered before. In the first case, the analysts should specify what degree of overlap these threats have with the higher level threats identified in the previous phases. This is required for computing the threat impact factor of each goal and/or evidence. If this degree is not specified, the threat impact from the same source may be calculated multiple times. In Figure 9, it has been shown that the 'late switch inspection' hindrance has overlap with 'careless equipment & process safety assessment'; which is a higher level hindrance (the degree of overlap is 0.2).

4.5.4. Step 4: Identify System Resources, Capabilities and Actors Resources are the essential requirements or outputs of a system, whereas capabilities are the functional tasks that are performed by a system. The major focus of risk analysis is on identifying the most vulnerable or hazardous resources and/or capabilities of the target system. For this reason, it is required that through the analysis process, the set of resources and capabilities that are available within the target system or universe of discourse that may affect the target system are identified. Astrolabe, employs the nouns and verbs of the concept (goals, evidences, obstacles, and hindrances) descriptions for detecting system resources and capabilities. To identify system resources, all of the descriptions of the concepts are searched for nouns. The same procedure takes place for the identification of system capabilities; where verbs are sought for.

As an example, consider the following description of an evidence: 'provide correct and on-time billing information'. The noun in this evidence is 'billing information' and the verb is 'provide information'; therefore, 'billing information' and 'provide information' are considered as possible candidates for system resources, and capabilities, respectively.

The identification of system actors is also very important since it provides the analysts with information such as the most vulnerable and/or hazardous actors. To specify system actors, the party in charge of performing all last layer evidences should be found. These actors may be either human or non-human entities. The IDFAD system is an instance of an actor in Figure 9, which is in charge of performing the 'monitoring through intelligent dataflow anomaly detector' evidence.

The completion of this phase should provide the analysts with the following information:

i. Complete understanding of system goals, evidences, hindrances, and obstacles with proper annotations in a unified way

ii. List of all system resources, capabilities and actors

4.6. Risk Analysis

The process of analyzing risk in Astrolabe revolves around identifying the goals, evidences, resources, capabilities, and actors of the target system that need close consideration, and are reckoned to be more vulnerable or hazardous compared with the others. The identification of these concepts is a relative and fuzzy procedure; therefore, the overall *significance/severity* of each concept is only determined relative to the status of the others.

Definition Goal/Evidence Significance (Υ_ϕ) is the magnitude of $\vartheta'(\phi, P_1)$; where P_1 represents the integrated view, and ϕ denotes any arbitrary goal or evidence. The difference between ϑ' and ϑ is that in ϑ', σ^{-1} is used instead of σ.

$$\Upsilon_\phi = \sqrt[2]{\sigma^{-1}(\phi, P_1)^2 + \varrho(\phi, P_1)^2 + \rho(\phi, P_1)^2} \tag{12}$$

Definition Resource/Capability/Actor Severity (Ω_ϕ) is the magnitude of a 2-Tuple $(o(\phi, P_1), \varrho(\phi, P_1))$, where $o(\phi, P_1)$ denotes the number of times that ϕ has been seen, and $\varrho(\phi, P_1)$ represents the threat impact of ϕ.

$$\Omega_\phi = \sqrt[2]{o(\phi, P_1)^2 + \varrho(\phi, P_1)^2} \tag{13}$$

To rank-order all concepts of the target system, the following procedure needs to be undertaken:

Table 4. Ranking System Goals based on Υ_{ϕ}

Rank	Goal	Importance	Number of Evidences	Threat Impact	Significance
1	Cater Data Services for Cell-Phone Users	0.55	4	0.3	4.04876
2	High Network Coverage and Acceptable QoS	0.6	3	0.35	3.07936
3	Inter-Region Safe Connection	0.35	2	0.281	2.04974
4	Intra-Region Connectivity & Proper Operation	0.7	1	0.24	1.24402
5	Interoperability with the PSTN Network	0.5	1	0.215	1.13851
6	Provide Correct & On-time Billing Information	0.3	1	0.128	1.05184
7	Provisioning New Services in the Coming Year	0.2	1	0.09	0.018

```
1.  **Foreach** Goal $\phi_g$ **do**
2.    **Calculate** $\Upsilon_{\phi_g}$
3.  **Rank-order** goals $\phi$ based on $\Upsilon_{\phi_g}$ in descending order
4.  **Foreach** Goal $\phi_g$ in $\phi$ **do** {
5.    **Foreach** Evidence $\phi_e$ attached to $\phi_g$ **do**
6.      **Calculate** $\Upsilon_{\phi_e}$
7.    **Rank-order** evidences $\phi_e$ for $\phi_g$ based on $\Upsilon_{\phi_e}$ in descending order
8.    **Foreach** $\phi_{r/c/a}$ attached to $\phi_e$ **do**
9.      **Calculate** $\Omega_{\phi_{r/c/a}}$
10.   **Rank-order** r/c/a seperately for $\phi_e$ based on $\Omega_{\phi_{r/c/a}}$ in descending order
11. }
12. /* r/c/a stands for resource/capability/actor */
```

The compilation of the results of this process in our running example has been partially shown in Tables 4 to 6. As it can be seen, the 'Cater Data Services for Cell-Phone Users' goal with a significance rate of 4.04876 needs the highest attention. From within the evidences that are attached to this goal, the 'Second Layer Switch/Link Connectivity' evidence seems to be the most critical evidence among the others. The resources, capabilities and actors that are involved in the operation of the 'Regular Inspection' evidence have also been rank-ordered. The order shows that 'Physical Inspection of Switches ', 'Network Backbone Switch ', and 'Physical Inspection Staff' are the most vulnerable or hazardous capability, resource, and actor of the 'Regular Inspection' evidence, respectively. From another viewpoint, it can be seen that the 'Provisioning New Services in the Coming Year' goal is really not of that much of importance to the target system, and moreover, it does not possess a really high degree of significance. If the analysis is performed correctly, this fact should also be visible in the degree of significance of the evidences related to this goal. From Table 5 it can be seen that the evidence related to this goal has one of the lowest significance values (2.05973), which is in accordance with what had been inferred from Table 4.

Based on the rankings provided in this phase, risk analysts can identify the most vulnerable or hazardous aspects of the target system, and select an appropriate mitigation strategy. It is recommended that the mitigation plans that are attached to the obstacles, or hindrances of the concepts that are higher up in the rankings be selected, since they are likely to be more effective. For example, based on the information in Table 6, it is more rational to focus on strengthening the operation of the 'Network Backbone Switch' ($\Omega_\phi = 12.004$), rather than focusing on 'Network Dataflow Information' ($\Omega_\phi = 3.0006$).

4.7. Quality Measurement and Validation

For evaluating the quality of the results obtained from the risk analysis methodology, quality assurance metrics need to be developed. In a methodology, following a specific number of steps does not guarantee the validity of the results. This may be due to various reasons, such as a misunderstanding of the intentions of the methodology, mistake in some of the calculations, use of incorrect sources of information, or even insufficient amount of elaboration. In this phase of Astrolabe, the obtained results from the previous six steps of the methodology are validated using five metrics, namely reliability, consistency, completeness, traceability and unambiguity. In the following, we introduce these metrics and show how they can be applied to the obtained results.

4.7.1. Reliability In a collection of related concepts to a goal in the first layer, if the average standard deviation of the normalized values assigned by each perspective remains close together, it can be inferred that the risk analysis procedure has been reliably pursued and therefore, the results are reliable. Consider the goals in Figure 10. There are three first layer goals in the information of this figure: G_1, G_2, and G_3. To calculate the average standard deviation of the annotation values for each goal, the *a, b,* and *c* zones on the graph need to be considered for goals G_2, G_1, and G_3, respectively. The average standard deviation of zones *a, b,* and *c* are 0.0904, 0.1237, and 0.1414. These values show that the average standard deviation for all three goals are relatively similar, and therefore, the results can be considered reliable. It is also possible to define a closeness threshold for reliability. We do not intend to address that issue in this paper.

4.7.2. Completeness In order to understand if the currently acquired information are complete enough for the risk analysis process, the notion of information enthalpy is developed.

Definition Information Enthalpy (ω) is defined as the magnitude of a five dimensional vector ($\omega_{g-g}, \omega_{e-e}, \omega_{g-e}, \omega_{g-o}, \omega_{e-h}$) where

$$\omega_{g-g} = \frac{|goalrefinement|}{|goal|},$$

$$\omega_{e-e} = \frac{|evidenceoperationalization|}{|evidence|},$$
$$\omega_{g-e} = \frac{|goal-evidence\_relation|}{|goal|},$$
$$\omega_{g-o} = \frac{|goal-obstacle\_relation|}{|goal|},$$
$$\omega_{e-h} = \frac{|goal-hindrance\_relation|}{|evidence|}.$$

$|x|$ denotes count of x.

Let's suppose that the information in zone d have not yet been added. The information enthalpy factor for the current situation would be (using hypothetical values for ω_{e-h}, and ω_{g-o} which are not shown in the figure): $\omega = \overrightarrow{(6/9, 5/9, 10/9, 8/9, 7/9)} = 1.8390$.

To evaluate that the degree of completeness and suitability of further refinements, the information enthalpy value is calculated for both before (ω_i) and after (ω_{i+1}) the refinements. If $\omega_{i+1} > \omega_{i+1}$ the changes are accepted, else the current information are considered complete enough for the analysis. Now consider adding the information in the d zone to the current information. The new information enthalpy value will be: $\omega = \overrightarrow{(8/11, 6/11, 12/11, 8/11, 7/11)} = 1.7174$. This shows that the information enthalpy has been reduced by adding the new set of information; therefore, the previous setting is believed to be relatively complete and hence the information added in zone d can be ignored.

4.7.3. Consistency Consistency is used to specify if each perspective has been correctly relating the goals, evidences and their descendants together. For this purpose, we define the notion of obedient goals. An obedient goal is a goal which has at least one connection with the evidences that are the children of the higher layer evidence that is connected to their parent goal. For example, $G_{2,1,1}$ is an obedient goal, since it is connected to $E_{3,2}$ which is the child of E_3. E_3 is in turn connected to the parent of $G_{2,1,1}$, $G_{2,1}$. In cases where information have been properly classified or in other words are consistent, the children of a goal should relate to the children of the parent evidences related to that goal; therefore, we define consistency as the overall ratio of the total number of obedient goals to the total number of available goals. This value is in the best case equal to one. It should also be noted that the first layer goals are omitted from the calculation of the consistency value. In Figure 10, the consistency value is 0.6667, because there are four obedient goals among six.

Table 5. Evidences Related to each Goal are Ranked Separately based on their Υ_ϕ value

Goal	**(Rank) Evidence**	**Importance**	**Number of Goals**	**Threat Impact**	**Significance**
Cater Data Services for Cell-Phone Users					
	(1) Second Layer Switch/Link Connectivity	0.7	3	0.37	3.10272
	(2) Mobile Network Maintenance	0.3	3	0.15	3.01869
	(3) Metadata Handling	0.65	2	0.08	2.10449
	(4) Wireless Technology research and Development	0.45	2	0.2	2.05973
High Network Coverage and Acceptable QoS					
	(1) Mobile Network Maintenance	0.3	3	0.15	3.01869
	(2) First Layer Device Connection	0.4	2	0.25	2.02113
	(3) Regular Inspection	0.15	1	0.075	1.01396
Inter-Region Safe Connection					
	(1) First Layer Device Connection	0.4	2	0.25	2.02113
	(2) Gateway Devices and Connections Operation	0.6	1	0.215	1.18584
Intra-Region Connectivity & Proper Operation					
	(1) Second Layer Switch/Link Connectivity	0.7	3	0.37	3.10272
Interoperability with the PSTN Network					
	(1) Mobile Network Maintenance	0.3	3	0.15	3.01869
Provide Correct & On-time Billing Information					
	(1) Metadata Handling	0.65	2	0.08	2.10449
Provisioning New Services in the Coming Year					
	(1) Wireless Technology Research and Development	0.45	2	0.2	2.05973

Table 6. Resources, Capabalities, and Actors Can be Rank-ordered based on their Ω_ϕ Value

Evidence Name	**Capability**	**Occurrence Rate**	**Threat Impact**	**Severity**
Regular Inspection				
	(1) Physical Inspection of Switches	5	0.7	5.0487
	(2) Random Inspection of Dataflow	4	0.064	4.0005
	(3) Monitoring Through Intelligent Dataflow Anomaly Detector	3	0.061	3.0006
	(4) Communication Link Inspection	3	0.04	3.0002
	(5) Constant Signal Quality Assessment	2	0.05	2.0006
	(6) Remote Monitoring	1	0.055	1.0015

Evidence Name	**Resource**	**Occurrence Rate**	**Threat Impact**	**Severity**
Regular Inspection				
	(1) Network Backbone Switch	12	0.31	12.004
	(2) Backbone Connection Link	10	0.28	10.0039
	(3) Network Dataflow Information	3	0.061	3.0006

Evidence Name	**Actor**	**Occurrence Rate**	**Threat Impact**	**Severity**
Regular Inspection				
	(1) Physical Inspection Staff	8	0.74	8.0341
	(2) Cyber Inspection Staff	6	0.114	6.001
	(3) Intelligent Dataflow Anomaly Detector	3	0.061	3.0006
	(4) Remote Monitoring Software	1	0.055	1.0015

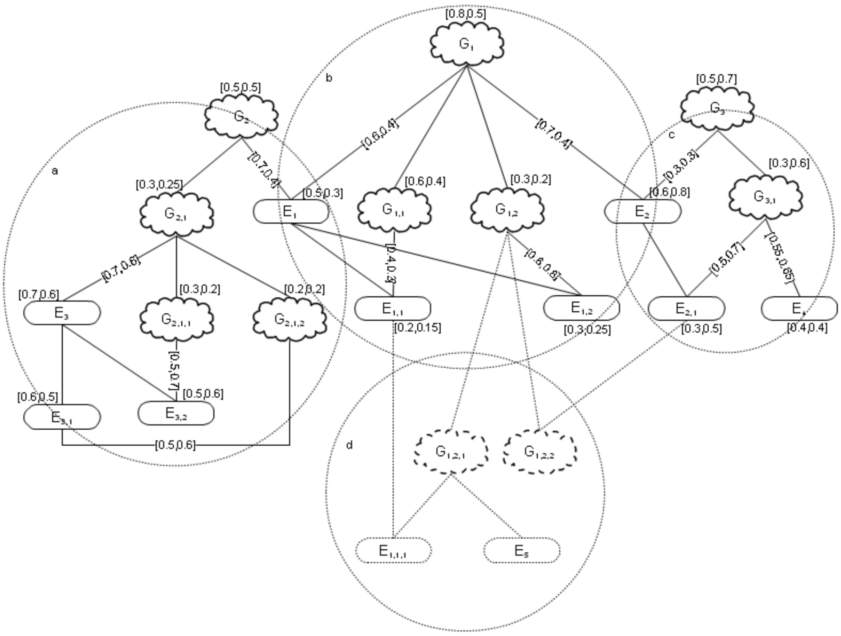

Figure 10. A Sample Graph Depicting the Relationships Between the Goals and Evidences of a Target System

4.7.4. Traceability This metric shows how well system goals have been supported by real world evidences in the extracted information. The more evidences are identified for a given goal, the better the operationalization of a goal can be traced and understood. As the building block of the traceability metric, we define the branching factor ($\aleph_i$). For a given tree that represents the connections of the goals and evidences in the collected information, $\aleph_i$ denotes the average number of evidences connected to a goal in layer i. Based upon this definition, traceability is defined as:

$$sum_{i \in |layers|}(\frac{1}{2^{i-1}})(\aleph_i) \tag{14}$$

The tracability factor should at least be equal to:

$$\sum_{i \in |layers|}(\frac{1}{2^{i-1}})(\frac{|evidence\_in\_layer_i|}{|goals\_in\_layer_i|}) \tag{15}$$

For Figure 10, the traceability metric is equal to 3.9475 ($2.67 + 0.5 \times 2 + 0.25 \times 0.86 + 0.125 \times 0.5$) which is higher than the required minimum (2.5025).

4.7.5. Unambiguity Unambiguity reveals the lack of common understanding between the viewpoint of the involved perspectives about the target system. It is desired that only one interpretation be derived for each concept of the target system. The average standard deviation of the annotation values assigned to all of the concepts in the information across all perspectives shows how convergent or divergent the various perspectives have been. If the average standard deviation is too high, this means that the obtained results are rather ambiguous since a common understanding has not been reached between the participating perspectives. For the example, the value of the unambiguity metric is 0.1156. Similar to the reliability metric, a threshold can be defined by the analysts to specify what degree of ambiguity is permitted.

At the end of this phase, risk analysts become relatively aware of the validity of the results of their risk analysis procedure. Based on this understanding, they should either satisfy themselves with what has been achieved so far, or refer back to previous phases of the methodology and refine the acquired information. As we have shown in Figure 1, Astrolabe and risk analysis in general, are iterative in nature; therefore, the results of a single iteration do not necessarily guarantee a complete and consistent identification of all system risks. The regular update of the results of the risk analysis procedure is required for an accurate monitoring of system status.

5. The Metamodel

The conceptual metamodel of Astrolabe is at the core of all notions used in the methodology. This metamodel can be seen in Figure 11. In the risk analysis procedure proposed in this paper, major system role players are selected (from the dominant coalition) to express their belief about the current system goals and evidences of its activities. Each perspective identifies a set of goals and evidences and shows how important these goals and evidences are for the success of the target system. They also specify the degree of impact that each evidence may have on system goals. These goals and evidences are further refined and operationalized with the help of the risk analysts. Possible obstacles and/or hindrances that may disturb the attainment of system goals and/or evidences are also thoroughly investigated. For each obstacle, and hindrance, the perspectives assign a probability of occurrence value that shows how likely it is that this specific threat occurs.

If we suppose that both obstacles and hindrances are conceptually similar and classify them as threat, we can see how a threat can be further detailed. A threat can have various causes, consequences, and appropriate mitigation plans or strategies. For a cause of a threat, the conditional probability that this threat is actually a cause given that the threat has actually occurred, is required from each perspective. The severity of the consequences, and the time, cost, and effectiveness of the mitigation plans or strategies need also be specified for decision making purposes. The scale of these values can be defined in any range, but as an example the range has been selected from the values between $(0, 1]$ in this paper.

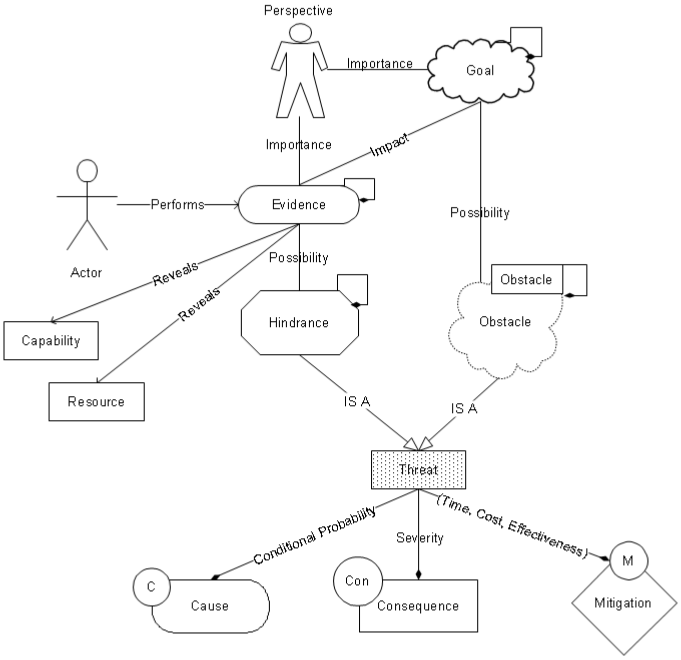

Figure 11. The Conceptual Metamodel of Astrolabe

Furthermore, the capabilities, resources and the involved role players (actors) of the target system, or the universe of discourse that affect the target system can be identified by analyzing the specifications of the derived evidences. All evidences can be studied to find any sign of system capabilities, resources and possible actors. Based on the other gathered information, the degree of vulnerability or hazardousness of these concepts can be estimated. The Astrolabe metamodel consists of twelve concepts and requires ten different types of annotation values between its concepts.

6. Related Work

Research in the area of goal oriented risk analysis/management has been very limited. To the extent of the authors' knowledge, there have only been three previous attempts to identify risk from system goals. In one attempt, Turner and Hunsucker have extensively discussed that risks can be identified from top organizational goals and objectives [(Turner and Hunsucker, 1999)]. They propose five steps for building an integrated risk consequence scorecard which is used for risk analysis. In these steps, top organizational goals, and objectives are identified, and refined, risk measures are determined, risk consequence scales are developed and are all integrated into the risk consequence scorecard which then allows a comprehensive risk analysis procedure.

Asnar and Giorgini have also focused on the notion of determining risk from organizational goals [(Asnar and Giorgini, 2006)]. In their approach, they build upon the Tropos methodology [(Bresciani et al., 2004)], for deriving and identifying organizational goals. Their model consists of three layers namely goal layer, event layer, and treatment layer. Close to this work is [(Mayer et al., 2005)], which builds on the i* framework [(Yu and Mylopoulos, 1994)]. There are similarities between what we propose in Astrolabe and these models; however, unlike the others, Astrolabe is a methodology that benefits from a multi-phase lifecycle. In Astrolabe, risk analysis can be performed by following the steps in the methodology phases. Benefiting from a multi-perspective approach is unique to the Astrolabe methodology. These three proposals do not address the quality of the obtained risk analysis results; whereas in Astrolabe, five different quality measurement metrics have been proposed.

Besides the area of risk management, Astrolabe has roots in methods commonly used in goal-oriented requirement engineering. Analogous to what we have defined as goals and evidences, Rolland et al. propose the notion of requirement chunk [(Rolland et al., 1999)]. A requirement chunk is a pair $< G, SC >$ where G is a goal and SC a scenario supporting that goal. They believe that goal discovery and scenario authoring are complementary activities in software requirement engineering. The difference between scenarios in requirement engineering and evidences in Astrolabe, is that scenarios are desired set of actions of the to-be system, but evidences are the actual behavior of a currently running system.

The notion of obstacle defined in Astrolabe is similar to the work presented in [(van Lamsweerde and Letier, 2000)]. Although the ideas in that work can be migrated to Astrolabe, but there is a major restriction facing risk analysis methods, and that is risk analysis models try to identify the risks that currently exist and threaten a running system, whereas these models mostly focus on the obstacles that may later threaten the software design process and the software goals.

AGORA is another software requirement analysis methodology that introduces the notion of multiple perspectives for identifying system goals [(Kaiya et al., 2002)]. The difference between the integration of perspectives in Astrolabe and AGORA is that AGORA requires each perspective to also annotate the goal graphs of the other perspectives. We do not pursue this in Astrolabe, since we believe that if the perspectives were aware of the concepts and annotation values of the other perspectives they would have incorporated them into their own information model. In Astrolabe, perspectives are only required to annotate the common concepts of their information with other perspectives.

7. Conclusions

In this paper, we have introduced the Astrolabe risk analysis methodology. The proposed methodology focuses on identifying risk from system goals. In reality, goals are supported by system activities; therefore, the risk analysis methodology focuses on the relationship between system goals and evidences. To identify risks, threats to/from each system goal and/or evidence is analyzed and properly classified. This classification of threats allows the analysts to take proper mitigation strategies based on their available resources and interests.

The most outstanding features of Astrolabe are: 1. Identifying risk from its system origins, 2. Tracing risk causes in both bottom-up (threats to system goals) and top-down approaches (goals to threats), 2. Incorporating multiple perspectives on system intention and structure for risk analysis, 3. Quality measurement metrics for process validation purposes, and 4. An iterative model for risk management with clearly enumerated phases, steps and deliverables. As future work, we are interested in studying the application of fuzzy variables in annotation value collection from the involved perspectives.

Notes

1. We consider an organization as a kind of system that can evolve. With this definition our definition of a system can encompass a wide range of entities from fully static to completely evolving.
2. Our definition of perspective is close to that of 'viewpoint' in [(Nuseibeh et al., 1994)].
3. This practice is encouraged due to the fact that many of the risks easily perceived by outsiders is often transparent to insiders.

References

Asnar, Y. and Giorgini, P. (2006). Modelling risk and identifying countermeasure in organizations. In *1st International Workshop on Critical Information Infrastructures Security.*

Bagheri, E. and Ghorbani, A. A. (2007). Risk analysis in critical infrastructure systems based on the astrolabe methodology. *In ACM/IEEE Communication Networks and Services Research Conference (CNSR 2007).*

Bresciani, P., Giorgini, P., Giunchiglia, F., Mylopoulos, J., and Perini, A. (2004). Tropos: An agent-oriented software development methodology. *Journal of Autonomous Agents and Multi-Agent Systems*, 8(3):203–236.

Cohen, M., March, J., and Olsen, J. (1972). A garbage can theory of organizational choice. *Administrative science quarterly.*

Curry, J. a. (2002). *Sociology for the Twenty-First Century.* Prentice-Hall, 3rd edition.

Cyert, R. M. and March, J. G. (1963). *A Behavioral Theory of the Firm.* Prentice-Hall, Englewood Cliffs, NJ.

Gross, E. (1969). The definition of organizational goals. *British Journal of Sociology*, 20(3):277–294.

Haimes, Y. Y. (2004). *Risk Modeling, Assessment, and Management.* Wiley, second edition.

Kaiya, H., Horai, H., and Saeki, M. (2002). Agora: Attributed goal-oriented requirements analysis method. *RE '02: Proceedings of the IEEE International Symposium on Requirements Engineering*, 00:13.

Kavakli, E. and Loucopoulos, P. (2006). Experiences with goal-oriented modeling of organizational change. *IEEE Transaction on Systems, Man and Cybernetics Part C*, 36(2):221–235.

Mayer, N., Rifaut, A., and Dubois, E. (2005). Towards a risk-based security requirements engineering framework. In *11th International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ05).*

Merton, R. (1957). *Social Theory and Social Structure.* Free Press, New York.

Nuseibeh, B., Kramer, J., and Finkelstein, A. (1994). A framework for expressing the relationships between multiple views in requirements specification. *IEEE Trans. Soft. Eng.*, 20(10):760–773.

Parsons, T. (1971). *The System of Modern Societies.* Prentice-Hall, Englewood Cliffs, NJ.

Redmill, F., Chudleigh, M., and Catmur, J. (1999). *System Safety : HAZOP and Software HAZOP.* John Wiley & Sons.

Rolland, C., Grosz, G., and Kla, R. (1999). Experience with goal-scenario coupling in requirements engineering. In *RE '99: Proceedings of the 4th IEEE International Symposium on Requirements Engineering*, page 74, Washington, DC, USA. IEEE Computer Society.

Scott, W. R. (1990). Technology and structure: An organization-level perspective. In Goodman, P. S. and Sproull, L. S., editors, *Technology and Organizations.* Josey-Bass, San Francisco.

Scott, W. R. (1992). *Organizations: Rational, Natural, and Open Systems.* Prentice-Hall, Englewood Cliffs, NJ.

Simon, H. A. (1979). Rational decision making in business organizations. *American Economic Review*, 69(4):493–513. available at http://ideas.repec.org/a/aea/aecrev/v69y1979i4p493-513.html.

Turner, J. V. and Hunsucker, J. L. (1999). Effective risk management: a goal based approach. *International journal of technology management*, 17(4):438–458.

van Lamsweerde, A. and Letier, E. (2000). Handling obstacles in goal-oriented requirements engineering. *IEEE Transactions on Software Engineering*, 26(10):978–1005.

Walpole, R. E. (1983). *Elementary Statistical Concepts.* Macmillan, New York, 2nd edition.

Yu, E. and Mylopoulos, J. (1994). Understanding why in software process modelling, analysis, and design. In *Proceedings of 16th International Conference on Software Engineering*, pages 159–168.

Zuckerman, M., Kernis, M. H., Guarnera, S. M., Murphy, J. F., and Rappoport, L. (1983). The egocentric bias: Seeing oneself as cause and target of others behavior. *Journal of Personality*, 51(4):621–630.