Risk Analysis in Critical Infrastructure Systems based on the Astrolabe Methodology

Ebrahim Bagheri and Ali A. Ghorbani
Faculty of Computer Science, University of New Brunswick,
Fredericton, NB, Canada
{e.bagheri, ghorbani}@unb.ca

Abstract

Critical infrastructure systems are complex networks of adaptive socio-technical systems that provide the most fundamental requirements of the society. Their importance in the smooth conduct of the society has made their role more and more prominent. A failure in any of these important components of today's industrial society can well affect the lives of millions of people. For this reason it is required that proper risk analysis and management models be devised so that the vulnerabilities, threats, and risks of/to critical infrastructure systems are exhaustively understood and revealed. In this paper, we show how the Astrolabe risk analysis methodology can be exploited to perform a comprehensive risk analysis process on any critical infrastructure system. The strength of the Astrolabe risk analysis methodology is that it focuses on the deviation of a system from its original goals. It also incorporates information from multiple sources through the notion of perspectives.

1 Introduction

A system can be described by its goals and objectives, and the set of scenarios that it carries out to support the operationalization of its ends. In other words, goals are intentional and scenarios (a collection of related and mostly ordered actions) are operational aspects of a system. Studies show that very few systems actually achieve their intended goals to the extent of their initial desire [3]. 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 the 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 initial goals.

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 [2]. 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 need also be analyzed.

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 [5]. This is usually the result of a mere focus on the correct execution of the current scenario and not focusing on its origins.

In this paper we intend to show the applicability of the Astrolabe methodology [1] for identifying any possible vulnerability and/or risk that threatens the proper being of an infrastructure system. The Astrolabe methodology identifies system risks through an iterative process and by performing five major tasks, namely: identifying system goals and objectives, codifying and relating the available evidence of system activity with its goals, exploring system goals and activities for possible threats and risks that they may cause or be threatened to, analyzing and organizing the identified risks in a unified framework to facilitate decision making, and validating the risk analysis process.

The organization of the paper is as follows. In the next section, the Astrolabe metamodel is briefly introduced, then the outlines of the sample infrastructure system that is going to be used as a running example throughout the paper is explained. Section 4 elaborates on the phases of the Astrolabe methodology and gives some details on how Astrolabe can be applied to infrastructure systems. The paper is then concluded in Section 5.
2 Astrolabe Metamodel

The conceptual metamodel of Astrolabe is at the core of all notions used in this methodology. In this risk analysis procedure major system role players are selected (from the dominant coalition which is introduced in [1]) 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, respectively. 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 threats, we can see how a threat can be further detailed. A threat can have various causes, consequences, and appropriate mitigation plans or strategies attached to it. 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.

From among the concepts in Astrolabe, the risk analysis process focuses more on the following concepts which 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.)\(^1\).

- **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 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.

3 A Running Example

As a running example throughout the paper, we employ a subset of a mobile communication infrastructure (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 example 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 Risk Analysis Methodology

The Astrolabe methodology consists of seven phases. Each of these phases have several corresponding steps. Risk analysts can follow these phases in order to reach a unified understanding of the vulnerabilities, threats or risks that threaten a system in general (specifically infrastructure systems). It should be noted that risk identification in Astrolabe is an iterative process. For a comprehensive result, risk analysts should frequently re-visit each of the phases and align any inconsistencies or add any new information. We introduce the Astrolabe’s phases in the following and explain how the running example can be analyzed in each of the different phases.

4.1 Phase 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, and intention. This is important for various reasons: 1. Creating a

\(^1\)Our definition of perspective is close to that of ‘viewpoint’ in [4].
shared understanding between system stakeholders and administrators, and the risk analysis team. 2. Avoiding the waste of resources during the risk analysis procedure by focusing on the defined specifications. 3. Eliciting risks related to structural and social aspects of a system, that may not have been identified if system boundaries were not defined.

Two approaches can be undertaken for defining the boundaries of a risk analysis process: normalist, or realist. 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 Phase 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 2: Perspective Identification

Cyert points out that most often system goals are defined by a negotiation process among a related set: the dominant coalition. 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.

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. 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 explanation purposes.

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. 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. (See Figure 1).

b. Identify Evidences: 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 1, 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:** A system may be performing a task to reach a goal but 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. 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 1, 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.

### 4.3 Phase 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, Astrolab e uses a set of guide words commonly used in methods such as HAZOP 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\}. Figure 2 shows the result of the application of guide words to the initial goal-evidence graph of the telecom engineer perspective.

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.

#### 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, let's 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 2, 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 2, 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:

\[
\sum_j \beta(Con_j, H_i) > 0, \quad (1)
\]

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 would be undertaken 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 for its operation, 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’.

In Astrolabe, each mitigation strategy is annotated with three parameters: Cost ($\gamma$), Time ($\delta$), and Effectiveness ($\zeta$). Based on these parameters the suitability of a mitigation strategy is defined as $f(\gamma, \delta, \zeta)$; where $\gamma$ shows the cost of performing the mitigation strategy, $\delta$ specifies the time needed to execute the mitigation strategy, and $\zeta$ depicts the effectiveness of the anticipated results of the mitigation strategy. Hence, the $i^{th}$ mitigation strategy is the most suitable choice if:

$$\forall j \in \mathcal{J} \rightarrow f(\gamma_i, \delta_i, \zeta_i) = \text{Max}(f(\gamma_j, \delta_j, \zeta_j)),$$

where $j$ is the number of mitigation strategies proposed for a specific cause. In Figure 2, 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. In this step, the analysts should investigate the stability of the goals and evidences that each perspective has introduced.

**Definition** Goal Stability $\vartheta(\text{Goal}_i, P_j)$ 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 $\text{Goal}_i$ by $P_j$. $\varrho_{i,j}$ is the sum of the threats imposed on $\text{Goal}_i$, and $\sigma_{i,j}$ is the inverse number of supporting evidences ($E$) attached to $\text{Goal}_i$ (Table 1 introduces the notations used in Eq. 3-7).

$$\varrho_{i,j} = T_o(i, j) = \sum_{k \in |\text{obs}|} (Pr_o(k, j) \times \sum_{n \in |\text{con}|} S_o(n)),$$

$$\sigma_{i,j} = \frac{1}{|E(i, j)|},$$
Volatile Zone

Definition to be volatile and hence need closer consideration. or evidences that are located within this zone are considered volatility zone more attention and elaboration. To identify such cases, we supporting it. Certainly, such a goal or evidence requires high threat impact value and very few evidences or goals that the goal or evidence has a high importance value, a of the stability factor. A lengthier stability vector means is required to be focused on the related goal or evidence.

= \sum_{k=1}^{m} \sum_{j=1}^{l} n_{evid_i} \cdot \text{Sum of the obstacle consequence severity of the } k^{\text{th}} \text{ obstacle}
= \sum_{k=1}^{m} \sum_{j=1}^{l} n_{hind_i} \cdot \text{Number of hindrances attached to the } k^{\text{th}} \text{ evidence of goal } i
= \rho_{i,j} \cdot \sigma_{i,j} \cdot \varrho

\theta(i, j) = (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 × n diagrams need to be drawn.

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 the related goal or evidence. This is because of the factors that are present in the makeup of the stability factor. A lengthier 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 \( \mathbb{R}^3 \) (Ψ \( \subseteq \mathbb{R}^3 \)) where for every stability vector \( \theta(i, j) = (\rho_{i,j}, \varrho_{i,j}, \sigma_{i,j}) \in \Psi \):

In this definition, \( \Psi_{\rho}, \Psi_{\varrho}, \) and \( \Psi_{\sigma} \) 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 the current situation.

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 (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 view point of the other perspectives. Since in the next phase, the results of the analyses from all perspectives are going to be consolidated into one unified representation, 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 \( P_j \) 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 3. Initial Cross Perspective Consistency Checking for Three Perspectives

Figure 3, 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 annotations of each perspective have been normalized within the context of that perspective (so that comparisons can be made). After that, each perspective has been asked to annotate what he thinks the other perspectives have rated the common concepts. 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 $\psi$ are considered as inconsistent. In these cases, the source perspective needs to go back and revisit its asserted information.

Founded on Chebyshev’s theorem [7], we define $\psi$ 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, $\psi$ 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.

4.4 Phase 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. 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 values assigned to the 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 annotation values of all perspectives have been added to the integratedView set. Figure 4 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 4, in contrast with the annotation values of each perspective, the integrated view consists of annotation vectors. 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 analysis.

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. 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 also calculated. Similar to the analysis performed in Section 4.3.5, the number of values that their difference value is more than $\phi$ is computed for each perspective ($\xi$).

$$\phi = \text{difference values} + \text{STD}(\text{difference values}).$$

(8)

Based on this analysis, $\xi_i$ 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 $\xi$ are considered to be inconsistent. In such a 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 is performed on the four perspectives of our example. 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, $\text{difference values}$ is 0.1609 and $\text{STD}(\text{difference values})$ is 0.1155; therefore $\phi$ 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 replace annotation vectors with the average of each vector’s values.

### 4.5 Phase 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 is 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 4, ‘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.

**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 Astro-labe, three main question words are used, namely: ‘Why’, ‘How’, and ‘How Else’. We do not elaborate on all of the steps in this phase since it is very much similar to the procedure undertaken in methods such as HAZOP or fault trees [6]. The ‘Identify System Resources, Capabilities and Actors’ step is only mentioned here since it is unique to Astro-labe.**

#### 4.5.1 Identify System Resources, Capabilities and Actors

Resources are the essential requirements or outputs of a system, whereas capabilities are the functional tasks that are
<table>
<thead>
<tr>
<th>Evaluated Criteria</th>
<th>T. CEO</th>
<th>Sr. T. Advisor</th>
<th>T. Engineer</th>
<th>M. Expert</th>
<th>Mean (τ)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide Correct &amp; On-Time Billing Information</td>
<td>0.3</td>
<td>-0.17</td>
<td>-</td>
<td>0.2</td>
<td>-0.27</td>
</tr>
<tr>
<td>Gateway Devices and Connections Operation</td>
<td>0.9</td>
<td>+0.125</td>
<td>0.5</td>
<td>0.2</td>
<td>-0.275</td>
</tr>
<tr>
<td>Inter-Region Safe Connection</td>
<td>0.5</td>
<td>+0.025</td>
<td>0.2</td>
<td>0.2</td>
<td>-0.075</td>
</tr>
<tr>
<td>Mobile Network Maintenance</td>
<td>0.4</td>
<td>-0.025</td>
<td>0.2</td>
<td>0.2</td>
<td>-0.225</td>
</tr>
<tr>
<td>Metadata Handling</td>
<td>0.8</td>
<td>+0.15</td>
<td>0.4</td>
<td>0.6</td>
<td>-0.25</td>
</tr>
<tr>
<td>Wireless Technology Research and Development</td>
<td>0.5</td>
<td>+0.05</td>
<td>0.4</td>
<td>0.3</td>
<td>-0.05</td>
</tr>
<tr>
<td>Cater Data Services for Cell-Phone Users</td>
<td>0.7</td>
<td>+0.15</td>
<td>0.4</td>
<td>0.5</td>
<td>+0.15</td>
</tr>
<tr>
<td>High Network Coverage and Acceptable QoS</td>
<td>0.7</td>
<td>+0.1</td>
<td>0.4</td>
<td>0.1</td>
<td>-0.2</td>
</tr>
<tr>
<td>Provisioning New Services in the Coming Year</td>
<td>0.3</td>
<td>-0.15</td>
<td>0.4</td>
<td>0.3</td>
<td>-0.05</td>
</tr>
<tr>
<td>Second Layer Switch/Link Connectivity</td>
<td>0.5</td>
<td>-0.033</td>
<td>-</td>
<td>0.5</td>
<td>-0.033</td>
</tr>
<tr>
<td>Intra-Region Connectivity &amp; Proper Operation</td>
<td>0.7</td>
<td>+0.05</td>
<td>0.5</td>
<td>0.6</td>
<td>+0.15</td>
</tr>
<tr>
<td>Regular Inspection</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0.1</td>
<td>-0.3</td>
</tr>
<tr>
<td>First Layer Device Connection</td>
<td>0.5</td>
<td>+0.05</td>
<td>0.2</td>
<td>0.2</td>
<td>-0.25</td>
</tr>
</tbody>
</table>

Figure 5. A Sample Process Refinement for the ‘Regular Inspection’ Evidence

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 or non-functional goals should be found. These actors may be either human or non-human entities. The ID-FAD system is an instance of an actor in Figure 5, which is in charge of performing the ‘monitoring through intelligent dataflow anomaly detector’ evidence.

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.

4.6 Phase 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 ($\Upsilon_\phi$) is the magnitude of $\vartheta_\phi(P_1)$; where $P_1$ represents the integrated view, and $\phi$ stands for any arbitrary goal or evidence. The difference between $\vartheta_\phi'$ and $\vartheta_\phi$ is that in $\vartheta_\phi'$, $\sigma^{-1}$ is used instead of $\sigma$.

$$\Upsilon_\phi = \sqrt[3]{\sigma^{-1}(\phi, P_1)^2 + \omega(\phi, P_1)^2 + \rho(\phi, P_1)^2}.$$  

Definition Resource/Capability/Actor Severity ($\Omega_\phi$) is the magnitude of a 2-Tuple $(\omega(\phi, P_1), \rho(\phi, P_1))$, where
Table 4. Ranking System Goals based on $\Upsilon_{\phi}$

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

$o(\phi, P_1)$ denotes the number of times that $\phi$ has been seen, and $\varrho(\phi, P_1)$ represents the threat impact of $\phi$.

$$\Omega_{\phi} = \sqrt{o(\phi, P_1)^2 + \varrho(\phi, P_1)^2}.$$

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

```plaintext
Foreach Goal $\phi_g$ do
  Calculate $\Upsilon_{\phi_g}$
  Rank-order goals $\phi$ based on $\Upsilon_{\phi_g}$ in descending order
Foreach Goal $\phi_g$ in $\phi$ do {
  Foreach Evidence $\phi_e$ attached to $\phi_g$ do
    Calculate $\Upsilon_{\phi_e}$
    Rank-order evidences $\phi_e$ attached to $\phi_g$ based on $\Upsilon_{\phi_e}$ in descending order
    Foreach $\phi_{r/c/a}$ attached to $\phi_e$ do
      Calculate $\Omega_{\phi_{r/c/a}}$
      Rank-order $r/c/a$ separately for $\phi_e$ based on $\Omega_{\phi_{r/c/a}}$ in descending order
  } /* 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 Table 4. 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.

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 4, it is more rational to focus more on strengthening the operations related to the ‘Cater Data Services for Cell-Phone Users’, rather than focusing on ‘Provisioning New Services in the Coming Year’. Similar tables to Table 4 can be drawn for the evidences, capabilities, resources, and actors. These tables will assist risk analysts identify the parts of the system that need the highest attention.

5 Conclusions

In this paper, we have introduced the application of the Astrolabe risk analysis methodology for identifying possible threats to an infrastructure system. The proposed methodology focuses on identifying risk from infrastructure systems 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.

6 Acknowledgements

The authors graciously acknowledge the funding from the Atlantic Canada Opportunity Agency (ACOA) through the Atlantic Innovation Fund (AIF) and through grant RGPIN 227441 from the National Science and Engineering Research Council of Canada (NSERC) to Dr. Ghorbani.

References