2010

Goal Approach to Risk Scenario Identification in Systems Development

Cesar Ariel Pinto
Old Dominion University

Andreas Tolk
Old Dominion University

Rafael Landaeta
Old Dominion University

Original Publication Citation

Pinto, C. A., Tolk, A., & Landaeta, R. (2010). Goal approach to risk scenario identification in systems development. *31st Annual National Conference of the American Society for Engineering Management 2010, ASEM 2010; Fayetteville, AR; United States; 13 - 16 October 2010* (pp. 361-366). American Society for Engineering Management.

GOAL APPROACH TO RISK SCENARIO IDENTIFICATION IN SYSTEMS DEVELOPMENT

C. Ariel Pinto, Old Dominion University
Andreas Tolk, Old Dominion University
Rafael Landaeta, Old Dominion University

Abstract
The scope of this paper is the exploration of fundamental issues in identifying risk scenarios during systems development. Systems development refers to a series of processes which span conceptualization, designing the architecture, obtaining the elements, and eventually integrating all these elements into the fully developed final system. For truly sustainable and green systems, indentifying risk scenarios early and continuously over the system development processes is vital. This paper contains various descriptions of risk from the project (i.e. programmatic) and technical perspectives, an exploration of the generally accepted risk management process, and how these relate to systems development through system goals. The paper shows the importance of goal and anti-goal analyses in the early identification of risk scenarios towards the development of truly sustainable systems. This result is critical for engineering managers and systems engineers who want to make risk management an integral part of the systems development process.

Key Words
Risk, uncertainty, complexity, systems approach, systems development, anti-goal, requirements engineering

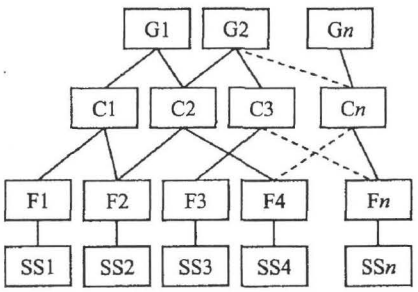
Introduction

"Regardless of whether it is acknowledged, the process of system identification followed by risk estimation is what is truly occurring in risk assessments."

- (Hatfield and Hipel, 2002, 11).

"A *system* can be broadly defined as an integrated set of elements that accomplish a defined objective" (INCOSE, 2004, 10). Most technical and organizational systems are created through a process known as systems development. *Systems development* refers to a series of process with the objective of bringing a system into being. This series of processes is often associated with the profession of systems engineering, engineering management, and project management. In practice of developing a system, there are several established models to choose from, some of which are ad-hoc, iterative, prototyping, exploratory, and reuse, as described in Blanchard and Fabrycky (2006). Industries and some agencies also adopt their own acceptable way for developing systems, as embodied in their respective standards such as MIL-STD-499B, EIA/IS 632, IEEE 1220, EIA 632, ISO/IEC 15288, and others. Nonetheless, systems development starts with goals that need to be satisfied. Based on these goals, necessary capabilities are identified. Functionalities are then identified to support the capabilities. Finally, sub-systems or components are identified which will enable the performance of the functionalities. This hierarchy can be represented as a tree (Exhibit 1) which allows the traceability from the sub-system level up to the goal level.

Exhibit 1. Traceability of goals and sub-systems



The branches connecting the various levels in Exhibit 1 illustrate how sub-systems (SS's) can be associated with particular functionalities (F's). The functionalities, in turn support capabilities (C's) which, in turn enables the attainment of the goals (G's).

Risk & Systems Development

In the context of systems development, risk can be described as "a measure of the uncertainty of attaining a goal, objective, or requirement pertaining to technical performance, cost, and schedule" (INCOSE, 2004, 63). Furthermore, the management of these risks, "in the context of Systems Engineering, is the recognition, assessment, and control of uncertainties that may result in schedule delays, cost overruns, performance problems, adverse environmental impacts, or other undesired consequences" (INCOSE, 2004, 61). In essence, the primary objective of managing risks when developing a system "is to ensure the delivery of a

system and its associated processes that meet the customer's need on time and within budget" in a way that address "uncertainties both in products and processes, as well as their interrelationships" (INCOSE, 2004, 61).

Scenario Identification

In the realm of risk management (to include risk assessment, analysis, and mitigation), the default preliminary step is the identification of risk scenarios. This step essentially determines what later on will be the focus of the rest of the risk management processes. "Risk identification is the process of recognizing potential risks and their root causes" (INCOSE, 2004, 62) and is essential in setting priorities for more detailed risk assessment.

Risk scenarios must be expressed in a clear way to enable analysis and defensible management. Garvey (2008) suggests the "condition-if-then construct" to express risk scenarios (p. 33). In essence, this construct allows the undesirable consequence be stated conditioned on a contributing event or root cause. As an example, consider the undesirable consequence *tunnel is flooded* to be symbolized by A, and a known contributing event *water main in the tunnel breaks* symbolized by B. This risk scenario can be expressed using the condition-if-then construct as:

A|B = *tunnel is flooded* conditioned on *water main in the tunnel breaks*

Risk scenarios expressed in this way facilitates the use of statistics and probabilities, i.e. estimating P(A|B) where P can be interpreted as either the chance of occurrence or degree of belief. Furthermore, this construct also facilitates the search for other contributing events or causes, e.g. A|C, A|D, etc which is a significant aspect of the entire risk management process.

Nonetheless, identifying risk scenarios, particularly the unknown unknowns is not a trivial process, as shown by Parsons (2007) particularly for large and complex systems such as those in NASA's space exploration. This challenge applies to both identifying the root undesirable event A as well as the contributing events B, C, etc. Yet, a complete set of risk scenarios is an ideal characteristic of an effective risk management process (Kaplan 1997).

Lately, there has been an emphasis on expanding the traditional realm of risk scenarios to include those that would usually be seen as remote, unrelated or are out of system bounds. Primarily, these has been the result of the observable but not-well-understood transference of risks across systems boundaries traditionally drawn by convention or convenience, i.e. projects compared to programs as emphasized by Alali and Pinto (2009).

Furthermore, it has always been a challenge to assimilate the temporal domain of risk in the development of systems. As pointed out by Hofstetter et al. (2002) and more recently by Haimes (2009), actions meant to manage risks can create both further risks as well as synergistic effects in the future – similar to a pebble dropped in the pond that creates ripples. These ripple-effects, especially in the context of environmental risks have proven to be a challenge from both the risk management as well as systems analysis perspective, as discussed by Hatfield and Hipel (2002).

From a systems analysis perspective, the two commonly held approaches to risk scenarios identification are bottom-up and top-down approaches. Bottom-up approach to risk identification is drawn from the systems analysis approach of the same name and relies on knowledge of what are elements of the systems and how these elements are expected to work together. This approach is most commonly evident in reliability analysis and is embodied in tools or techniques such as FMEA (Failure Mode and Effect Analysis), fault trees, and alike. On the other hand, top-down approach to risk identification is drawn from the systems analysis approach of the same name and relies on knowledge of the objectives of the systems.

In practice, these two approaches of top-down and bottom-up applied together create synergy which provides risk analysts a more efficient identification of risk scenarios. The bottom-up approach, which relies heavily on empirical and historical data of previously known risks, coupled with knowledge of cause-and-effects leads to a detailed set of risks with causes and effects. These risks are also termed as faults or failures in reliability analysis. The top-down approach, which relies on what is known or perceived to be objectives of the systems coupled with a process of logical elimination or exclusion provides general set of risks. The focus of this article, anti-goal approach, has stronger affinity to the top-down approach to risk identification.

The distinction between these two approaches of identifying risk scenarios become more apparent in systems development for several reasons:

- The system being developed is not yet existing, as such, all risk scenarios, are in essence synthesized and results of informed conjecture,

- Usability of bottom-up approach to identifying risk events is limited and is dependent on the uniqueness of the system being developed and its comparability to existing systems
- The mapping of systems development process with systems life cycle results to decision in the systems development process predicated to the perceived goals
- The large number of possible risk scenarios coupled with the uncertainty in the potential consequences makes discerning the more important risk scenarios more challenging

It is evident that risk identification in the context of systems development is very much related to but not exactly the same in the traditional sense. The entire nature of systems development being primarily system-goal-driven, as shown in Exhibit 1 places more emphasis on the top-down approach to risk identification.

Anti-goals

The notion of anti-goal originates from the notion that security-related goals in systems development require special analysis to assure reliability and dependability. Van Lamsweerde et al. (2003) provides an early discussion of how system goals, models of these goals, and resulting anti-models and anti-goals may provide a better way to draw security-related systems requirements.

The basic steps in identifying anti-goals are (adapted from Van Lamsweerde et al. 2003, 52-53):
1. Enumerate known goals of system being developed (e.g. provide secure data exchange)
2. Generate most general or root anti-goals by negation of known goals (e.g. data exchange is not secure)
3. Refine anti-goals to level of specificity required by the current system development stage.
4. Identify who and what will enable these anti-goals to occur (e.g. who will benefit from insecure data exchange and what they need to do to accomplish this)
5. Refine the details of the anti-goals until these details can be mapped to the technical requirements of the system being developed.

The concept of anti-goal was also mentioned by Barton et al. (2004, p. 10), not from systems development perspective but from the more general system-thinking perspective as a way to look "180 degrees around in the opposite direction" of system goal. Since then, the notion of anti-goal has been extended to safety-critical systems (e.g. in Habli et al. 2007), and has appeared in discussions on human psychology (e.g. Norling, 2004 and Carver, 2006).

In identifying system adversaries and their capabilities that will enable these anti-goals to occur, a threat graph can be created that will show attack – points for the anti goal. A goal is reached when at least one possible combination of necessary capabilities is functioning. It is notable that while a system proponent supports goals that make the system run, a system adversary will support anti-goals that make a system fail.

Extension of anti-goals

As pointed out in the earlier section, there is the more general challenge of identifying risk scenarios (including but not limited to security-related risks) beyond the traditional realms brought about by the evolution of currently existing systems and systems yet to be developed. This is further complicated by the nature of risk scenarios transcending established systems boundaries and being influenced by non-technical factors such as culture, policies, and regulations.

Even though the original intent of using anti-goals is toward more efficient elicitation of security-related requirements, the underlying concepts may hold great potential in addressing the difficulties of identifying risk scenarios in systems development. This article proposes the extension and modification of some underlying concepts of anti-goals in order to affect the following:
- provide a convergence between the practice of risk scenario identification and goal analysis in systems development
- facilitate risk scenario identification in systems development
- develop goal-oriented risk management approach suitable for goal-oriented systems development
- provide risk manager a mindset to expand the realm of traditional risk identification process
- provide a venue to integrate non-technical factors in risk identification, e.g. culture, policies, regulation, conventions, etc.

Initially, working descriptions of terms are laid out. These are adaptation of terms presented by Van Lamsweerde et al. (2003) and supplemented by concepts from works of Kaplan (1997), Hofstetter et al. (2002), Garvey (2008), Haimes (2009), and Alali and Pinto (2009).

Goal is a hierarchical description of a system's desired events
Anti-goal is a statement that expresses the logical negation of a goal

The goal is termed to be hierarchical due to the possibility for any goal to be described is varying degree of details, specificity, or refinement. This implies that anti-goals are also hierarchical similar to goals. Extending and modifying the condition-if-then construct described earlier such that:

A: goal
A': anti-goal
B: contributing event

Then, A'|B is a risk scenario relating the anti-goal (or equivalently, undesirable event) with a contributing event B. Having anti-goal A' traceable to the goal A allows the system developer to use the condition-if-then construct and still have the traceability required in any systems development endeavor. Looking back at Exhibit 1 which illustrates the role of capabilities (C's) in attaining the goals, consider the roles of C1 and C2 in attaining G1. This branch of the larger tree is shown in Exhibit 2.

Exhibit 2. Traceability for G1

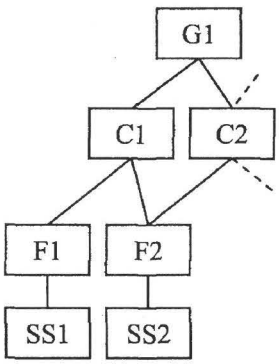


Exhibit 2 suggests both C1 and C2 are needed and are enough to attain G1. That is, C1 and C2 will be, by design, both necessary and sufficient to attain G1. As a direct corollary, failure of either C1 or C2 (or both) will cause G1 to not be attained. In essence, it can be deduced that:

G1: goal
G1': anti-goal
C1': compliment of C1 (i.e. failure to deliver C1)
C2': compliment of C2 (i.e. failure to deliver C2)

If events C1' or C2' or (C1' and C2') are collectively referred to as Ca, then

P(G1'|C1' or C2' or (C1' and C2')) = 1.

$$P(G1'|Ca) = 1 \quad (1)$$

However, Equation (1) only shows that C1' or C2' or (C1' and C2' are sufficient causes for G1', but does not imply necessity. This means that there are possibly other potential causes of G1' not represented by the collection of events Ca. If all these other unspecified causes are collectively expressed as Ca', then

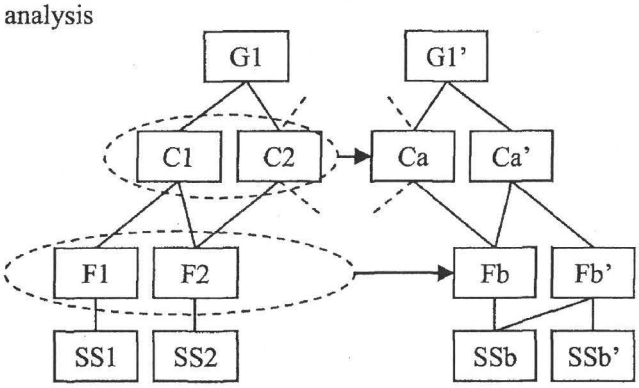
$$P(G1'|Ca') = 1 \quad (2)$$

By total probability theorem, Equation (1) and (2) can be used to express nut just the risk scenarios but also the unconditional probability of G1 not being attained, i.e. P(G1') as shown in Equation (3).

$$P(G1') = P(G1'|Ca)P(Ca) + P(G1'|Ca')P(Ca') \quad (3)$$

What has been shown for the two top-most level in Exhibit 2 can also be applied to other levels, e.g. C1 and functions F2 and F2, etc. Exhibit 3 illustrates the mirror-image that anti-goal analysis may provide for Exhibit 2.

Exhibit 3. Risk scenario tree produced from anti-goal analysis



In essence, Equation (3) expresses the unconditional probability of G1 not being attained. This is illustrated in Exhibit 3 as the mirror image G1'. Goal-oriented systems development process, such as that illustrated in Exhibit 2, provides important information for identifying some risk scenarios, and can be expressed as conditional probabilities such as in Equation (1). Nonetheless, Equation (2) also highlights that there are more risk scenarios that may not be readily identifiable. These two sets of risk scenarios are illustrated in Exhibit 3 as Ca and Ca'. At the lowest level of the risk scenario tree are sub-systems which may be logical suspect to accomplish risk scenarios corresponding to functionality level.

Conclusion, Analysis and Recommendations

It has been shown that the concept of anti-goal holds potential beyond its original intent of facilitating elicitation of security-related requirements is systems development. Coupled with concepts from the risk

management practice, the extension of the concept of anti-goals presents potential areas for further investigation, such as:

- Formally defining goals, capabilities and functions supporting goals – including possible alternative combinations thereof – to pertain not only to proponents but also to adversaries may allow use of game-theories in developing high-assurance systems
- The traceability of the role of sub-systems to failures in functionalities, capabilities, and anti-goal may enable threat and vulnerability analysis to be conducted in parallel to systems development
- The ability to represent risk scenarios as conditional and unconditional probabilities may be coupled with evidence-based analysis (e.g. use of Bayesian analysis) to allow quantitative risk assessment to be performed concurrent with systems development. Conditionality can represent both correlations as well as causation relationships.
- Interdependencies among sub-systems can be described both in the functionality space as well as in risk space
- Use of knowledge management to discover both known and unknown unknowns may lead to more accurate risk assessment.

References

Alali, Baqer and C. Ariel Pinto "Project, Systems, and Risk Management Processes & Interaction," Proceedings of the PICMET '09 Portland International Center for Management of Engineering and Technology, Portland, Oregon, USA (August 2-6) 2009.

Barton, John, Merrelyn Emery, Robert Louis Flood, John W. Selsky, Eric Wolstenholm, "A Maturing of Systems Thinking: Evidence from Three Perspectives," Systemic Practice and Action Research, 17:1 (2004) pp. 3-36.

Blanchard, B.S. & Fabrycky, W.J, Systems Engineering and Analysis, 4th ed., Upper Saddle River, NJ: Prentice-Hall. (2006).

Carver, Charles S., "Approach, Avoidance, and the Self-Regulation of Affect and Action," Motivation and Emotion, Springer Netherlands, 30:2, June (2006).

Garvey, Paul R. *Analytical Methods for Risk Management: A Systems Engineering Perspective* CRC Press (2008).

Habli, Ibrahim Weihang Wu, Katrina Attwood, Tim Kelly, Extending Argumentation to Goal-Oriented Requirements Engineering (Book Series Lecture Notes in Computer Science) (2007).

Haimes, Yacov. Y. "On the Complex Definition of Risk: A Systems-Based Approach." Risk Analysis, 29:12 (2009) pp. 1647-1654.

Hatfield, Adam J. and Keith W. Hipel "Risk and Systems Theory," Risk Analysis, 22:6 (2002) pp. 1043-1057.

Hofstetter, Patrick, Jane C. Bare, James K. Hammitt, Patricia A. Murphy, and Glenn E. Rice, "Tools for Comparative Analysis of Alternatives: Competing or Complementary Perspectives?," Risk Analysis, 22:5 (2002) pp. 833-851.

INCOSE, Systems Engineering Handbook, INCOSE-TP-2003-016-02, Version 2a, 1 June (2004).

Kaplan, Stan "The Words of Risk Analysis," Risk Analysis, 17:4 (1997) pp. 407-417.

Norling, Emma, "Folk Psychology for Human Modelling: Extending the BDI Paradigm," Proceedings of the International Conference on Autonomous Agents and Multiagent Systems, vol1 (2004) pp. 202 - 209

Parsons, Vickie. S. "Searching for "Unknown Unknowns" Engineering Management Journal, 19:1 (2007) pp. 43-46.

Van Lamsweerde, Axel, Simon Brohez, Renaud De Landtsheer, and David Janssens, "From System Goals to Intruder Anti-Goals: Attack Generation and Resolution for Security Requirements Engineering," Proceedings of the 2nd International Workshop on Requirements Engineering for High Assurance Systems (2003) pp. 48-56.

Acknowledgement

The authors would like to acknowledge the support of Old Dominion University (ODU) Office of Research through its 2010 Multidisciplinary Seed Grant, ODU's Department of Engineering Management and Systems Engineering, the National Centers for System of Systems Engineering, and the Emergent Risk Initiative at ODU, and ODU's Batten College of Engineering and Technology through the dean's faculty development grant.

About the Authors

C. Ariel Pinto is an Associate Professor in the Department of Engineering Management and Systems Engineering at Old Dominion University. His research is in the areas of risk management in engineered systems, project risk management, risk valuation and communication, and analysis of extreme-and-rare events. He received his Ph.D. in Systems Engineering from the University of Virginia, and Master and Bachelor degrees in Industrial Engineering from the University of the Philippines.

Andreas Tolk is Associate Professor for Engineering Management and Systems Engineering at Old Dominion University, Norfolk, Virginia. He is also a Senior Research Scientist at the Virginia Modeling

Analysis and Simulation Center (VMASC). He holds a M.S. in Computer Science (1988) and a Ph.D. in Computer Science and Applied Operations Research (1995), both from the University of the Federal Armed Forces of Germany in Munich. He is a member of ASEM, ACM SIGSIM, SCS, SISO, MORS, and NDIA.

Rafael Landaeta is Associate Tenured Professor in the department of Engineering Management and Systems Engineering. He holds a M.S. in Engineering Management and a Ph.D. in Industrial Engineering from the University of Central Florida. He received a B.S. in Mechanical Engineering from UNITEC, Venezuela. He has performed applied research for the U.S. Department of Homeland Security, the U.S. Army Program Executive Office Soldier, The U.S. Army Core of Engineers, Siemens-Westinghouse Power Generation, Walt Disney World-Information Technology, NASA-Kennedy Space Center, The National Centers for Systems of Systems Engineering, The Institute of Simulation and Training, and the Industrialized Housing Partnership of the U.S. Department of Energy.