Applying Game Theory and Computer Simulation to Fault Tree Analysis

Catherine J. Watkins and Eric M. Greenberg

ABSTRACT

Fault tree analysis is a useful probability theory-based tool for evaluating a system's risk and reliability. Typically, fault trees are populated with basic event failure probabilities from a variety of quantitative and qualitative sources. This article presents a new methodology that combines simulation with game theory to populate a fault tree with strictly quantitative probability estimates for basic events in the fault tree. This new method is applied to an example ship self-defense scenario, and the probability of effectiveness against a group of small attack boats is calculated. The resulting fault tree is used to model a war gaming situation in which the players must choose optimal strategies and weapons. This articles describes a means for generating a fault tree in which the top event probability is optimized with the assignment of basic events probabilities in accordance with game theory.

INTRODUCTION

Fault tree analysis (FTA) is an analytic methodology commonly used to assess risk and reliability. FTA is a failure-based approach that begins with an undesired event (top or top-level event) and, through a systematic backward-step process, identifies the basic causes or combination of basic events that lead to the top-level event. The fault tree is a logical illustration of the events and their relationships that provide the necessary and sufficient means for the undesired event to occur. It computes the probability that the undesired event will occur and provides insight on the importance of the basic events modeled within the tree. Fault trees facilitate investigative methods to increase system reliability, reduce opportunities for system failure, and identify the most important contributors to system effectiveness, ultimately in an attempt to minimize risk.

The probability of each basic event is determined from one of three primary sources, two of which are quantitative in nature. Data on the availability of the system's components, collected through a data collection program or by using a manufacturer's specification, are the first and preferred source. If this source of data is not available or is not appropriate for the basic events, the event probabilities may be derived from the second source: modeling and simulation techniques. The third data source, input by subject-matter experts (SMEs), is qualitative. This article explores a quantitative methodology based on game theory as a replacement for the third source of data. Note that the inputs to this study's methodology are the same modeling and simulation results used to inform the second data source. Hence, the goal is to produce a fault tree consisting of data derived from purely quantitative sources.

FTA began in 1961 when H. A. Watson of Bell Telephone Laboratories began looking for ways to quantify the reliability and safety of the Minuteman missile

launch control systems as a part of a contract with the U.S. Air Force.[1] Since its application to the Minuteman system, the use of FTA has become widespread for analyzing the safety and reliability of complex dynamic systems such as nuclear reactors, processing plants, and power systems.[2–4] For systems in which failure probabilities follow well-known distributions, calculating basic event probabilities is straightforward. However, in more complex systems, such as dynamic fault trees, in which failures must occur in a specified sequence, Monte Carlo simulation methods have been applied.[5,6] The idea of applying fault tree methodology to human-based security systems is a relatively new concept.

The concept of game theory is often brought up during the discussion of war games; in fact, sometimes the terms are used so closely in context they appear to be synonymous. However, war gaming and game theory are distinct concepts. War gaming is the simulation of a conflict situation, whereas game theory is a mathematical theory that can aid in identifying an optimal strategy or course of action when certain conditions within the conflict are met. Hence, game theory is a tool that can aid the decision-making process in a war game. In 1957, Walter Deemer and Clayton Thomas suggested that the new concepts of game theory may be used in place of traditional analytical war gaming to solve generalized tactical problems of limited scope.[7] By the late 1950s, both Air Force Col O. G. Haywood and U.S. Navy CAPT R. P. Beebe had written papers supporting the use of game theory as a decision-making aid in war games.[8–10] The game theoretic study of the two-person game fit naturally with war gaming scenarios during the Cold War, where the bipolar world was split into the United States versus the Soviet Union. Since the dissolution of the Soviet Union, the generalization that the current global state of affairs can be modeled as a two-person zero- or nonzero-sum game became impossible.[11] However, on the small-scale, single-engagement level, the two-person game assumption still holds and the results from game theory still serve as a valuable decision-making tool for selecting an optimal strategy. This article will explore how the game theoretic concept developed in post-World War II war gaming can be applied in conjunction with the reliability and risk assessment tool of fault trees for small-scale engagements of a limited scope.

This article considers an engagement scenario in which a Blue (friendly) ship is forced to defend itself against an attack by small Red (adversarial) boats. In this scenario, each side has the option to make one of two tactical decisions. Blue has the choice to select one of two different weapon types, while Red must select between two different engagement tactics. The goal in applying game theory to this scenario is to answer the following question: if both sides follow the best possible strategy during an engagement and also assume the rival will do the same, what is the optimized and best possible Blue system effectiveness for the scenario? For this scenario, system effectiveness is defined as the probability that the Blue ship succeeds in neutralizing all Red boats in a force-on-force engagement before the Blue force is neutralized by Red. Because the tactical actions will greatly affect system performance, it is necessary to determine the optimal frequency for each side to use a particular tactic.

The analytic process used in this study models each combination of tactics using Surface Warfare Simulation (SuWSim), a Johns Hopkins University Applied Physics Laboratory (APL)-developed surface warfare modeling tool. The outputs of the simulation are analyzed using game theory to determine the optimal strategies for each side. The identified optimal decision strategy is then used to populate the basic event probabilities within the fault tree that would have traditionally been gathered from qualitative sources. Finally, a probability of effectiveness (P_E) is computed using the simulation-derived basic event probabilities for the set of basic events.

FAULT TREE ANALYSIS

FTA is an analytic method by which an undesired state of a system (typically critical to reliability or safety) is studied in the context of its environment and operation.[12] Fault trees determine, in a logical manner, basic events by which the specified undesired state, known as the top (or top-level) event, can occur. The fault tree itself is a graphical depiction consisting of branches of sequential and parallel fault mechanisms. The logical combination of these mechanisms and basic events results in system failure at the top level. Examples of lower-level fault events are component hardware failures, human errors, or failure in a force-on-force engagement. Building a fault tree begins with specifying the top event and stepping downward, stopping at the level of interest at which meaningful data can be obtained and initiating failure events can inform overall risk assessment. It is important to note that a fault tree does not model all possible system failures or possible root causes of system failures. The fault tree is restricted and tailored to the system

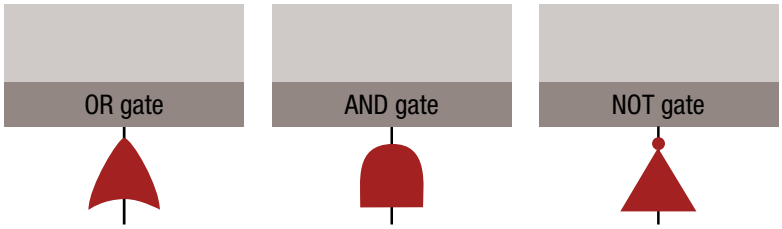

Figure 1. The three most common gates within a fault tree are the OR, AND, and NOT gates.

components and failure mechanisms that contribute to the specified top event. Hence, a fault tree model graphically depicts the logical relationships among basic fault events that lead to the undesired outcome specified as the top event.

Gates show the logical relationships between initiating or basic failure events in a fault tree. Gates serve to permit or inhibit the flow of fault logic up from lower levels of the fault tree toward the top failure event. Each gate shows the relationship among a set of input events required for the occurrence of the output, a higher-level failure event. The logical relationships among the lower-level failure events are inputs to the gate, and a probability of a higher-level event is computed using Boolean algebra.[13] The numerical value computed at the top level of the fault tree is known as the probability of failure, P_F. The complement of P_F is known as probability of effectiveness, P_E, and is computed as $P_E = 1 - P_F$.

Figure 1 illustrates the three most common types of logic gates present in a fault tree: the OR gate, the AND gate, and the NOT gate. The analyst supplies probabilities only for the basic events; all probabilities associated with gates are computed via Boolean algebra. Equations 1–3 determine the mathematical relationships between basic event probabilities for OR, AND, and NOT gates. An OR gate identifies single paths to failure: if any of the inputs are true, the output is true. In set theoretic terms, this is equivalent to the union of the input event sets, which is described algebraically in Eq. 1. An AND gate represents system redundancies: all inputs must be true for the output to be true. This is equivalent to the intersection of the input event sets, which is given by Eq. 2. A NOT gate simply computes the probability of the basic event not occurring by taking its additive inverse (Eq. 3). Basic events are represented by purple and green circles within the fault tree diagram.

$$P(A \text{ or } B) = P(A) + P(B) - P(A) * P(B) \quad (1)$$

$$P(A \text{ and } B) = P(A) * P(B) \quad (2)$$

$$P(\text{Not } A) = 1 - P(A) \quad (3)$$

SuWSim

SuWSim is an agent-based event-driven simulation APL developed in MATLAB to analyze the effectiveness of various naval systems and engagement doctrines.[14] The simulation is Monte Carlo capable and can evaluate the error for a specified confidence level of key metrics. It can model engagements between friendly, hostile, and neutral forces and can include both surface and air platforms. Tactical actions of each of the forces are modeled

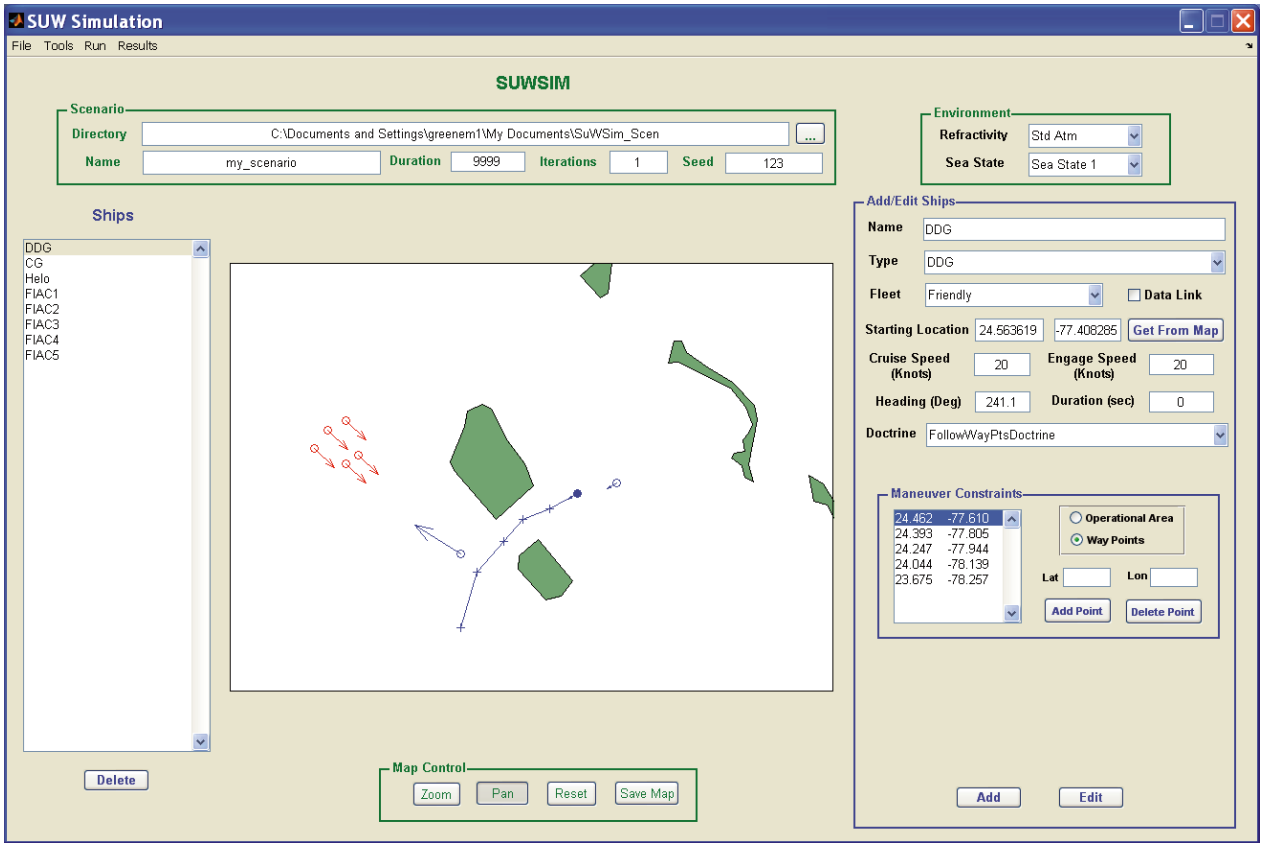

Figure 2. SuWSim graphical user interface.

dynamically based on each platform's view of the battlespace and in accordance with doctrines provided by warfighters. Platforms (ships and aircraft) in SuWSim can have multiple systems on board, including sensors that can detect other platforms and weapons used for engagement. Both current and future warfare systems can be modeled in the simulation. SuWSim can model command and control doctrines based on a defined rule set consisting of maneuver tactics with operational constraints and waypoints, firing tactics with target prioritization, and force coordination tactics.[15] Simulation events are handled by SuWSim's event-driven kernel, which is responsible for keeping track of the timing and order of events. SuWSim also has a graphical user interface to facilitate scenario generation (shown in Fig. 2). Output results can be visualized using SIMDIS (shown in Fig. 3), which is a Naval Research Laboratory-developed visualization tool.[16]

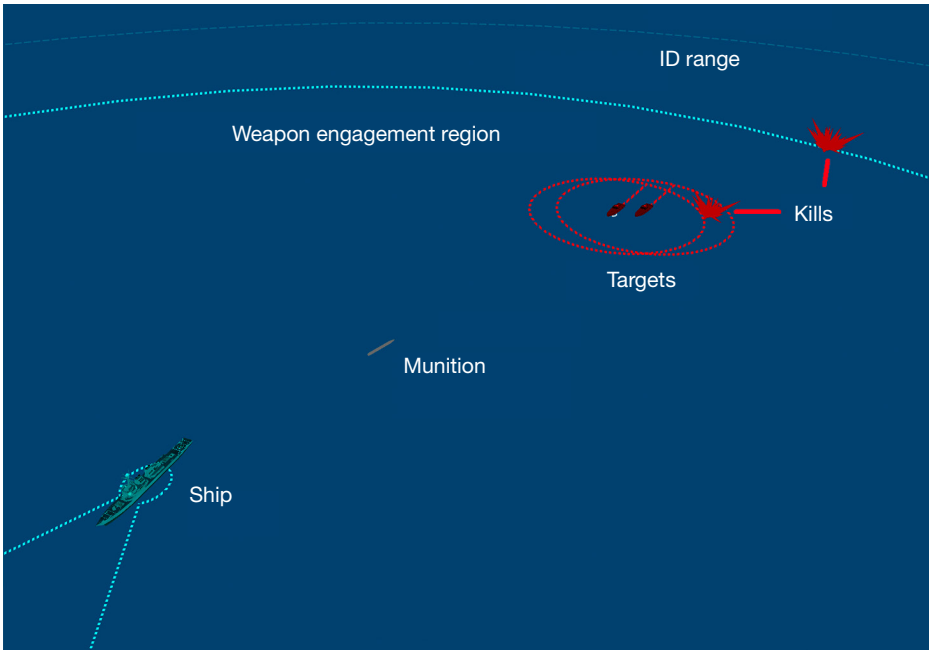

Figure 3. SIMDIS visualization of a SuWSim scenario.

WEAPONS EFFECTIVENESS

In this study, notional probability of hit and probability of kill (P_HP_K) data are used to determine the effectiveness of weapon systems. P_HP_K data indicate the likelihood that a weapon system will hit and catastrophically damage its target at a given range. This study considers two potential notional weapon systems for the Blue ship to use on its single weapon mount. The first weapon system has a low P_HP_K for long ranges, but its effectiveness increases considerably at short ranges. This makes it an ideal defense against a suicide small boat attack but a poor defense against a long-range standoff attack. The second weapon system has constant P_HP_K at all ranges up to 1000 meters. The effec-

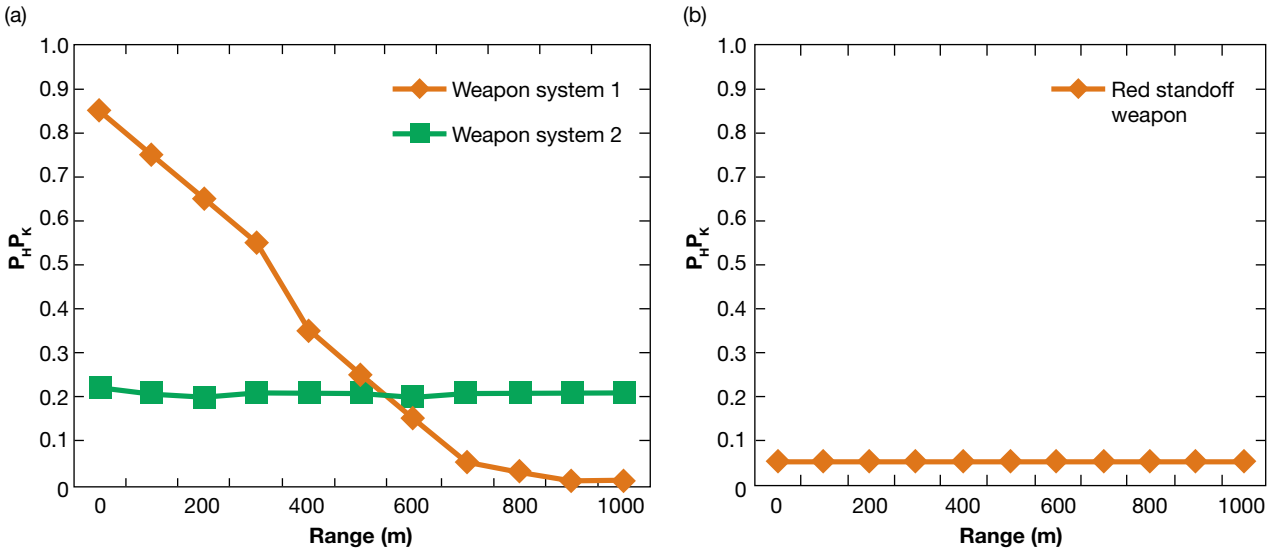

Figure 4. Notional P_HP_K data for Blue (a) and Red (b) weapons. Note that it is assumed for the Red suicide tactic that P_HP_K is 1 at impact and 0 elsewhere.

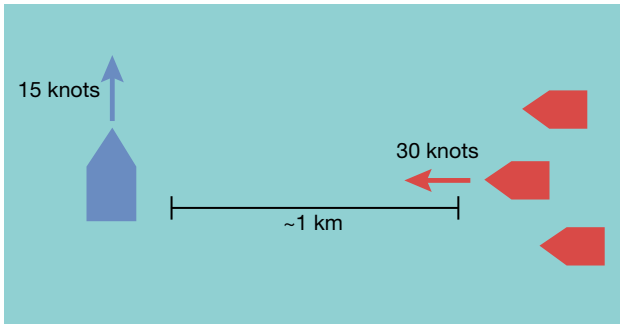

Figure 5. A moving Blue boat detects three incoming adversary boats at approximately 1 km away.

tiveness of the second weapon is relatively low against both Red boat tactics, although at the longest ranges it is higher than that of the first weapon system. Because the Blue ship cannot distinguish between a suicide small boat and a small boat with standoff capabilities until Red makes clear which tactic it is employing, Blue must choose a weapon system before knowing the type of boat it will engage.

Like the Blue ship, the Red boats may be equipped with either of two different weapon systems: a standoff weapon system with $P_H P_K$ values shown in Fig. 4 or explosives to be used in a suicide attack and detonated on contact. As with Blue, it is assumed that Red will be able to use either weapon system but not both.

Table 1. The four cases of the scenario given the respective combinations of decisions made by each side

Case No.	Weapon 1	Weapon 2	Suicide Tactic	Standoff Tactic
1	■		■	
2		■		■
3	■			■
4		■	■	

ENGAGEMENT SCENARIO

In the example scenario, a Blue ship cruising at a constant speed of 15 knots detects a single group of three small boats slightly more than 1 km away. The small boats are approaching at 30 knots and maintain a constant relative bearing of 90°. The small boats follow a direct path toward the Blue ship regardless of their engagement tactic, as depicted in Fig. 5. The Blue ship defends against this attack using its onboard gun system.

In this scenario, the Blue ship much choose between two different weapon systems to engage the Red boats (the scenario assumes that only one system can be used in a single engagement). Similarly, the three identical Red boats in the scenario may be either suicide boats laden with explosives that will detonate on impact with the Blue ship or small attack boats equipped with a standoff weapon system that can engage the Blue ship at

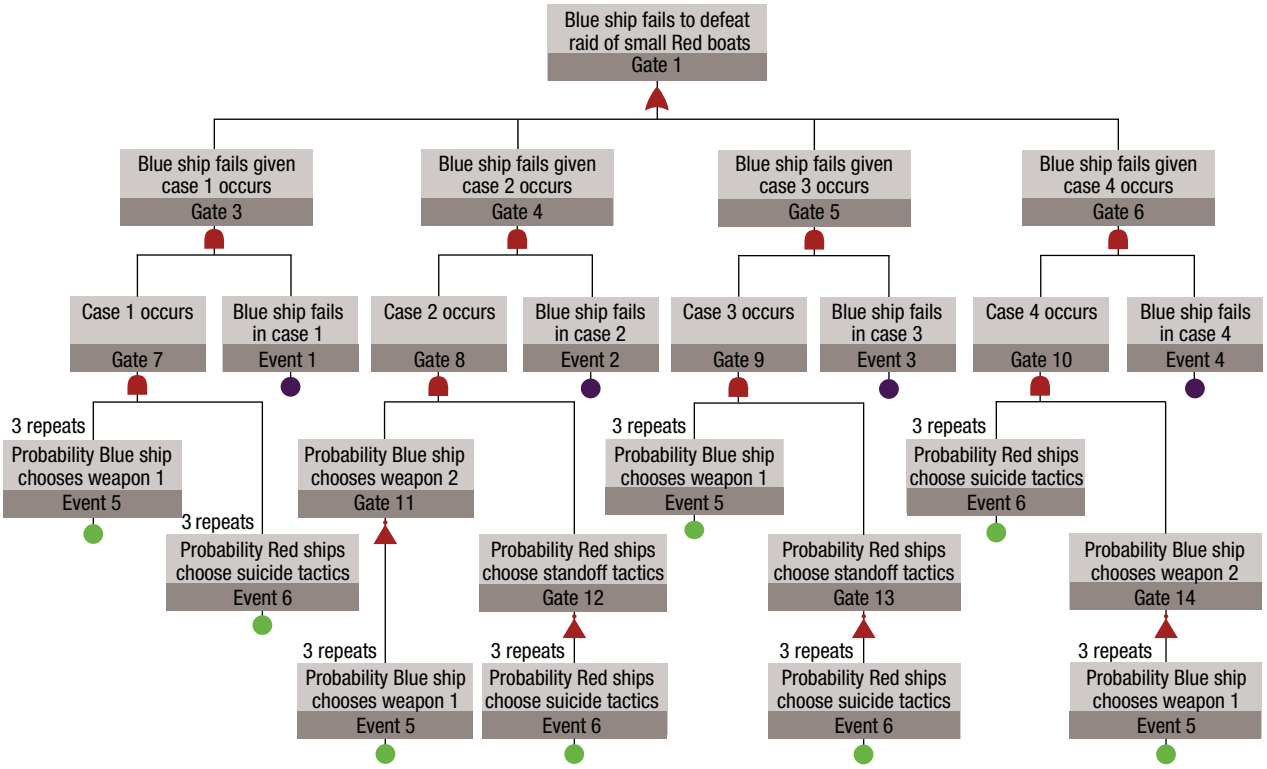

Figure 6. Fault tree describing the four possible cases in which the Blue ship may fail in defense against a raid of Red surface vessels.

Table 2. PRA results from SuWSim simulation for the four possible combinations of Red and Blue tactics

	Suicide Tactic	Standoff Tactic
Weapon system 1	0.81	0.06
Weapon system 2	0.42	0.49

Table 3. Single equilibrium solution representing optimal strategies for Blue ship (in blue) and Red boats (in red)

	Weapon System 1	Weapon System 2	Suicide Tactic	Standoff Tactic
Equilibrium solution	0.08	0.92	0.53	0.47

maximum effective range. These options yield four different cases consisting of each pair of Blue and Red tactics, as outlined in Table 1. The fault tree representing this scenario and its decision points is shown in Fig. 6.

In this tree, gate 1 represents the overall probability that the Blue ship fails to defeat all three Red boats in the raid. Gates 3–6 represent the conditional probabilities that the Blue ship fails in each of the four cases (given that each of the cases occurs). Gates 7–10 depict the probability that each of the four cases occurs based on game theory, which is a direct product from the optimal strategy given by events 5 and 6. In these gates, the optimal strategy replaces the SME input for choice of tactic. Last, events 1–4 represent the probability of raid annihilation (PRA) failure that is determined by the output of a Monte Carlo simulation using SuWSim. PRA represents the probability that the Blue ship catastrophically kills all three small Red boats in the scenario, which is the required criterion for a Blue win. Table 2 shows the PRA, based on the notional $P_H P_K$ data, computed by SuWSim for each of the four cases outlined above. These PRA values, which represent Blue successes, are then inverted into failure events and populate events 1–4 in the fault tree.

One way to determine the probability for event 5, that Blue chooses weapon system 1, in the fault tree is to ask a representative from the Blue force how he or she may act in the given situation or how likely he or she is to make a certain decision over another. Similarly, a SME in threat tactics might be consulted to determine the probability for event 6, that Red may choose suicide tactics over standoff weapons. Although these SME opinions can serve as inputs to a fault tree, they are not derived from data. The actions and responses are subjective and can differ significantly among individuals. It would be better to observe representative drills and collect and use data to best characterize likely actions, but this is often infeasible because of cost or schedule constraints. Game theory can be used to replace qualitative assessments of SMEs with a more quantitative analysis.

GAME THEORY

Game theory techniques can be used to determine optimal strategies that can be converted to inputs for the basic decision-making events within the fault tree. The resulting probability of failure (P_F) for the top event of the fault tree is the complement to the optimized effectiveness based on the computed optimal strategy. Instead of determining P_E based on likely decisions by Blue and Red identified by either SMEs or analysis of historical data of prior decisions made (or historical likelihoods of occurrence observed), the fault tree calculates a P_E that balances risk and reward for large numbers of similarly executed engagements with the same four possible cases of Blue and Red decisions.

This surface engagement scenario is an example of a two-person zero-sum game, in which each player's loss is equal to the other player's gain. The PRA results from Table 2 for each combination of tactics serves as the payoff or success matrix for this game.[17] Given the

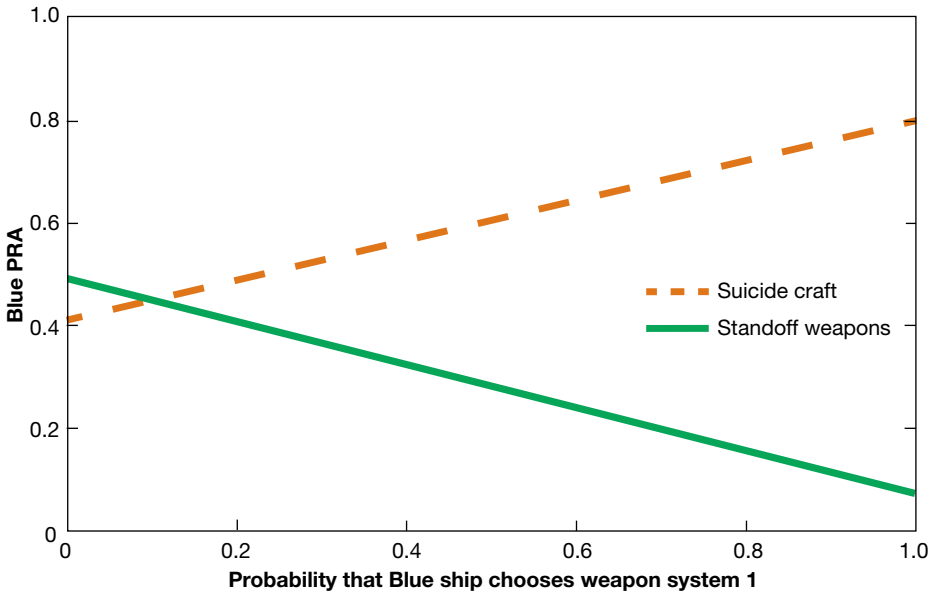

Figure 7. Possible PRA outcomes for the Blue ship by Red tactics as a function of probability of the Blue ship selecting weapon system 1.

choices for each side (outlined previously), there is no obvious best tactic for either team because the best tactic is dependent on the choices made by the rival. For Blue, weapon system 1 provides the best performance if Red selects the suicide tactic, but weapon system 2 is better if Red selects the standoff tactic. Red also faces a similar conundrum when selecting which tactic to use. This suggests that the optimal strategy for each side will be a mixed strategy: players should select a course of action randomly with a specified probability. Because a combined mixed strategy is best for both teams, the next step is to solve for the optimal strategy. The optimal strategy can be computed manually using linear programming or by using software such as the open-source software tool Gambit.[18] The PRA values in Table 2 serve as the inputs when solving for the optimal strategy. Table 3 shows the computed optimal mixed strategy.

The optimal strategy for the Blue ship is to choose the first weapon option only 8% of the time and to choose the second option the remaining 92%. It is in the Red boats' best interest to choose the suicide tactic 53% of the time and the standoff tactic for the other 47% of cases. This Blue–Red ratio of tactical choices is known as the Nash equilibrium of the game. In 1950, John Nash proved that, for every game with a finite number of players in which each player can choose from a finite set of pure strategies, there exists at least one Nash equilibrium.[19] The Nash equilibrium solution represents either a pure strategy (the same decision is made every time the game is played) or a mixed strategy that optimizes the expected payoff for both players.[20] Table 3 represents the latter.

The optimal strategy is to minimize the potential loss against the opponent's best counterstrategy. Figure 7 illustrates how the process determines the optimal mixing strategy. The orange and green lines represent the PRA based on the two possible Red attack strategies. The *x* axis represents the weighting that the Blue ship chooses the first weapon system, and the end points of the lines are points from the payoff matrix. The best strategy for the Blue ship occurs when the worst possible outcome (solid lines) is maximized and is also where Red cannot reduce performance by switching strategies. This occurs at the intersection of the two lines, when x = 0.08, and corresponds to the weapon system 1 being chosen by the Blue ship 8% of the time.

DISCUSSION

Blue's weapon system 1 achieves a PRA of 81% against suicide boats but only a PRA of 6% against a standoff attack. Blue's weapon system 2 achieves a PRA of 42% against suicide boats, but it can achieve a PRA

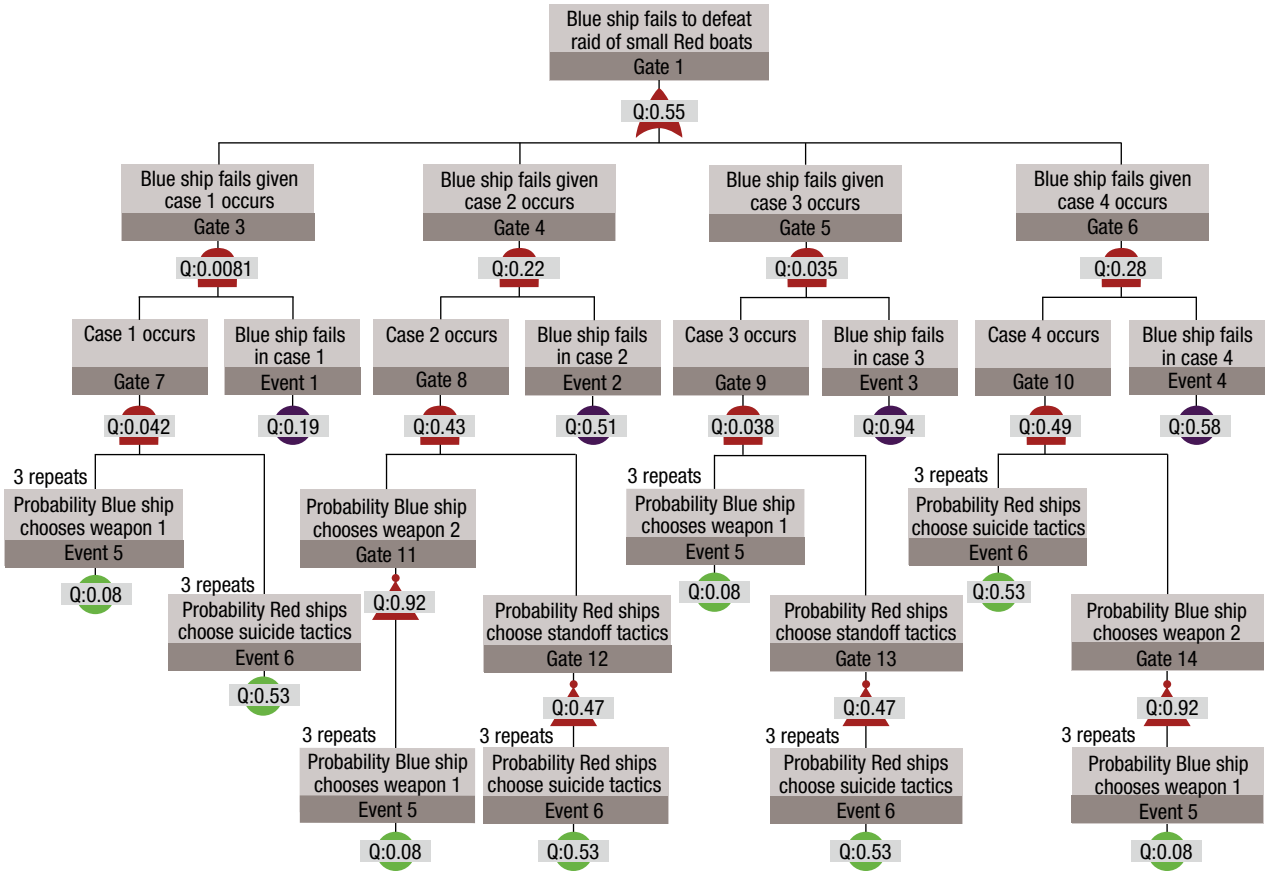

Figure 8. Fault tree containing optimized strategy and simulated PRA outcomes rounded to two significant digits.

of 49% against a standoff attack. If Blue knew *a priori* which tactic Red would use, it would be simple for Blue to determine which weapon system to use. Blue would choose weapon system 1 against suicide boats because it is much more effective against this type of threat. Against a raid using standoff weapons, Blue would choose weapon system 2, which has a somewhat higher PRA in this situation. Therefore, Blue benefits from choosing weapon system 1 at least some of the time. Choosing weapon system 1 is a risky decision because this weapon's effectiveness against a standoff attack is very low. However, making this decision at least some of the time will increase Blue's overall P_E. To optimize the strategy, the Blue ship should opt to use weapon system 1 only 8% of the time, and the remaining 92% of the time it should select the second weapon system. This may seem somewhat counterintuitive given that the optimal strategy computed for the Red boats is to choose the suicide tactic 53% of the time and the standoff tactic the other 47% of the time. Although weapon system 1 produces the highest PRA for the Blue ship when suicide boats attack, it also produces the most risk because it has a very low PRA when Red employs standoff weapons. Hence, the frequency with which to use weapon system 1 is small in the optimal strategy.

The strategy probabilities computed using game theory and the PRA results from SuWSim are then input into the fault tree as shown in Fig. 8. The probabilities in gate 1, gates 3–6, and gates 7–10 are computed using Boolean algebra. Gate 1, which represents the probability of Blue failure against the Red attack, is 0.55. Thus, the P_E is 0.45. Gates 7–10 indicate the probabilities that each of the four cases occur given that the optimal strategy is employed. P_E is driven by the values for events 2 and 4, since more than 90% of the time one of their associated cases will occur.

The intermediate levels of the tree, represented by gates 7–10, inform the reader how often the different cases may occur when each side uses the strategy provided by game theory methods. This knowledge can inform future tactical decisions regarding how to most efficiently improve P_E for the scenario. In the scenario analyzed, we predicted that cases 2 and 4 would occur more frequently than cases 1 and 3 according to the optimal strategy. It should be noted that changes to the PRA payoff matrix caused by changes in $P_H P_K$ data will affect the optimal strategy probabilities that could limit the overall improvement in P_E. To increase its P_E, the Blue ship might consider ways to increase performance of weapon system 2 because this is the weapon system that game theory suggests using most often. Alternatively, if Blue could mitigate the risk of Red using the standoff tactic against weapon 1 (case 3) by improving its performance in this situation, Blue could use this weapon more often to take advantage of its superior performance against the suicide tactic. Consequently, this method presents an interesting opportunity to explore ways to increase P_E by investigating different combinations of strategic options for both sides.

CONCLUSION

Traditionally, fault trees have been used to calculate the P_E for the best- and worst-case scenarios. The difference between these two probabilities of effectiveness indicates system sensitivity. However, by combining modeling and simulation with game theory, it is possible to generate a set of data to populate a fault tree, providing insights into the expected system performance as players make strategic decisions. This method produces a P_E under the assertion that both sides are making strategic decisions. It represents a maximum system P_E that can be achieved when the system is acted on by intelligent and knowledgeable agents on both sides. It is purely quantitative and computes a P_E that is not based on subjective inputs. By replacing subject-matter expertise with game theoretic results, a purely data-driven P_E can be produced. The results of the simulation and game theory can be used to inform military systems how to optimally act in the scenario to maximize the expected value of success, or the P_E. However, this P_E is fundamentally based on the assumption that both sides will act according to principles of game theory.

This method ultimately provides a novel way of populating basic event probabilities in a fault tree by using the principles of game theory. It provides a unique method of computing the P_E that is motivated by choosing the strategy to maximize overall system performance under the assumption that the adversary is actively attempting to minimize it. Furthermore, this method provides the player with critical information regarding how often a tactical decision should be made as well as how often the rival may make its tactical decisions.

REFERENCES

[1]Watson, H. A., *Launch Control Safety Study*, Vol. 1, Bell Telephone Laboratories, Murray Hill, NJ, section VII (1961).

[2]Lee, W. S., "Fault Tree Analysis, Methods, and Applications—A Review," *IEEE Trans. Rel.* **R-34**(3), 194–203 (1985).

[3]Kelly, B. E., "The Propagation of Faults in Process Plants: 1. Modeling of Fault Propagation," *Rel. Eng.* **16**(1), 3–28 (1986).

[4]Volkanovski, A., "Application of the Fault Tree Analysis of Power System Reliability," *Rel. Eng. Syst. Saf.* **94**(6), 1116–1127 (2009).

[5]Durga Rao, K., "Dynamic Fault Tree Analysis Using Monte Carlo Simulation in Probabilistic Safety Assessment," *Rel. Eng. Syst. Saf.* **94**(5), 872–883 (2009).

[6]Alirexa, E., "FPGA-Based Monte Carlo Simulation for Fault Tree Analysis," *Microelectr. Rel.* **44**(6), 1017–1028 (2004).

[7]Thomas, C. J., and Deemer, W. L., "The Role of Operational Gaining in Operations Research," *Oper. Res.* **5**(1), 1–27 (1957).

[8]Haywood, O. G. Jr., "Military Decision and the Mathematical Theory of Games," *Air Univ. Q. Rev.* **4**(1), 17–30 (Summer 1950).

[9]Haywood, O. G. Jr., "Military Decision and Game Theory," *Oper. Res.* **2**(4), 365–385 (1954).

[10]McHugh, F. J., *The United States Naval War College Fundamentals of War Gaming*, 3rd Ed., Department of the Navy, Naval War College (Mar 1966).

[11]Bracken, P., and Schubik, M., "War Gaming in the Information Age," *Naval War College Rev.* **54**(2), 47–60 (Spring 2001).
[12]Stamatelatos, M., and Vesely, W., *Fault Tree Handbook with Aerospace Applications*, Vol. 1.1, NASA Office of Safety and Mission Assurance, Washington, DC (2002).
[13]Myhre, J., *Fault Tree Analysis*, Mathematical Analysis Research Corporation, Claremont, CA (2011).
[14]Greenberg, E. M., and Griggs, D. R., "Engagement Tactics against Asymmetric Small Boat Attacks," in *Proc. 2007 National Fire Control Symp.*, San Diego, CA (2007).
[15]Bankman, I. N., Chrysostomou, A. K., Fry, R. L., Greenberg, E. M., Hegde, C. L., et al., "JHU/APL Fast Attack Craft/Fast in-Shore Attack Craft (FAC/FIAC) Initiative," AMD-13-071FY13, Final Report, JHU/APL, Laurel, MD (Oct 2013).
[16]U.S. Naval Research Laboratory, *SIMDIS* (version 9.5.0), U.S. Naval Research Laboratory, Washington, DC, https://simdis.nrl.navy.mil/Viewpage.aspx?ID=c4ea43ae-7a82-4653-bcd1-4a6f2df848c4.
[17]Waner, S., and Costenoble, S. R., "Game Theory," *Finite Mathematics*, Brooks/Cole, Belmont, CA, pp. 267–284 (2004).
[18]McKelvey, R. D., McLennan, A. M., and Turocy, T. L., *Gambit: Software Tools for Game Theory* (version 14), University of East Anglia, California Institute of Technology, National Science Foundation, http://gambit.sourceforge.net/.
[19]Nash, J. F., "Equilibrium Points in N-person Games," *Proc. Natl. Acad. Sci.* **36**(1), 48–49 (1950).
[20]Von Neumann, J., and Morgenstern, O., *Theory of Games and Economic Behavior*, Princeton University Press, Princeton, NJ (1953).

THE AUTHORS

Catherine J. Watkins is a security systems analyst in the Force Project Sector at APL and a member of the Associate Professional Staff. **Eric M. Greenberg** is the lead developer for SuWSim and a member of the Senior Professional Staff in APL's National Security Analysis Department. For further information on the work reported here, please contact Catherine Watkins. Her e-mail address is catherine.watkins@jhuapl.edu.