

ARMY RESEARCH LABORATORY



Discrete Time Integrated Analysis Methodology for a Ground Combat System

by Brian G. Ruth

ARL-TR-2017

July 1999

19990823 047

Approved for public release; distribution is unlimited.

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

Army Research Laboratory

Aberdeen Proving Ground, MD 21010-5423

ARL-TR-2017

July 1999

Discrete Time Integrated Analysis Methodology for a Ground Combat System

Brian G. Ruth

Survivability/Lethality Analysis Directorate, ARL

Approved for public release; distribution is unlimited.

Abstract

In this report, a methodology is presented for the integrated analysis of a military weapon system across all classes of battlefield threats addressed by the Survivability/Lethality Analysis Directorate (SLAD) of the U.S. Army Research Laboratory (ARL). The target audience for this report is vulnerability/lethality (V/L) analysts who might participate in such an integrated analysis. The integrated analysis methodology is based on the V/L taxonomy, which provides a framework for the analysis of a military system. Available system capability states are mapped to required mission tasks as described in the military system's Operational Mode Summary/Mission Profile (OMS/MP) and then tracked along a discrete time axis, allowing for both threat sequencing and interthreat synergy on required battlefield performance to be studied and analyzed. Since the discrete time integrated analysis methodology is a mechanism for aggregating survivability measures of performance (MOP) and measures of effectiveness (MOE), the integrated analysis product provides the decision maker with a means to evaluate the overall impact of battlefield threats on potential combat system effectiveness.

Table of Contents

	<u>Page</u>
List of Figures	v
List of Tables	vii
Executive Summary	ix
1. Introduction	1
1.1 Purpose	1
1.2 Background	1
1.2.1 <i>General</i>	1
1.2.1.1 <i>V/L Taxonomy</i>	1
1.2.1.2 <i>Discrete Time V/L Process Structure</i>	4
1.2.2 <i>Threat</i>	6
1.3 Scope	6
2. Theory of Discrete Time V/L Processes	7
2.1 The Generic $O_{1,2}$ Mapping	7
2.2 The Synergistic $O_{1,2}$ Mapping	10
2.3 Threat-Specific Level 2] and Level 3] Metrics	12
2.4 The Integrated $O_{2,3}$ Mapping	14
2.5 The Mission Fitness Mapping	20
2.6 The Discrete Time Analysis Process	24
2.7 Time Series Analysis of the Requirement Vector	30
3. Implementation	32
4. Example Applications	34
4.1 A Simple System With Four Capability Metrics	34
4.2 Ground Combat System for Troop Transport	38
4.2.1 <i>Binary-State Analysis</i>	38
4.2.1.1 <i>No Interthreat Synergy Assumption</i>	55
4.2.1.2 <i>Synergy Between B1 and E Assumption</i>	62
4.2.2 <i>Trinary-State Analysis</i>	62
4.2.3 <i>Binary-State Analysis Results</i>	68
4.2.4 <i>Trinary-State Analysis Results</i>	75
4.2.5 <i>Analysis Constraints Involving Time Discretization</i>	76

	<u>Page</u>
5. Conclusions	79
6. References	81
Appendix A: Fault Trees	83
Appendix B: A Lukasiewicz Trinary Logic	89
Appendix C: Example of a Mission Profile.....	93
Glossary	97
Distribution List	101
Report Documentation Page.....	105

List of Figures

<u>Figure</u>	<u>Page</u>
1. The V/L Taxonomy as Implemented Within the Integrated Analysis Process.....	3
2. The Discrete Time V/L Taxonomy	5
3. Elements of the Generic $O_{1,2}$ Mapping	9
4. The Synergistic $O_{1,2}$ Mapping	11
5. Suggested V/L Taxonomy Levels Where Threat-Specific Metrics Should Be Integrated With Other Threat-Specific Metrics.....	13
6. Elements of the Integrated $O_{2,3}$ Mapping	15
7. Fitness Trees For the Battlefield (a) Mobility, (b) Firepower, and (c) Communication Requirements as Described by Equations (20) and (21)	23
8. Layout of a Typical Discrete Time Axis	25
9. The Integrated Analysis Process Using Predetermined Threat Profiles	28
10. The Integrated Analysis Process Using a Stochastic Threat Profile.....	29
11. Implementation of the Integrated Analysis Process	33
12. Initial Component Functional States Within the Combined Fault/Fitness Tree for a Simple System With Four Capability Metrics	36
13. Component Functional States Within the Combined Fault/Fitness Tree From Figure 12 After 30 min of Mission Time Have Elapsed	37
14. Component Functional States Within the Combined Fault/Fitness Tree From Figure 12 After 60 min of Mission Time Have Elapsed	39
15. The Requirement Vector for the Ground Combat System Example.....	42
16. Fitness Trees for the Requirements (a) R_1 and (b) R_2	44
17. Fault Tree for the Mobility Subsystem DS M_2 : Maximum Speed Reduced to 30% of Full Mobility (Adapted From Comstock [1991] and Kinsler [1989]).....	45

<u>Figure</u>	<u>Page</u>
18. Fault Tree for the Mobility Subsystem DS M_3 : Stop After Time t (From Kinsler [1989])	46
19. Fault Tree for the Mobility Subsystem DS M_4 : Total Immobilization (From Kinsler [1989])	47
20. Fault Tree for the Crew Subsystem DS C_3 : Three Crew Members Incapacitated (From Kinsler [1989])	48
21. Fault Tree for the Catastrophic Loss DS K_1 : K-Kill (From Kinsler [1989])	49
22. Plot of the Range of Available Ground System Capability for Which the Fitness of R_1 and R_2 Is Equal to 1	50
23. Plot of R_1 Fitness Profile No. 9 From Table 4 (Based on Threat Profile No. 9 From Table 3)	59
24. Average Fitness Profile for R_1 Without Interthreat Synergy	60
25. Average Fitness Profile for R_2 Without Interthreat Synergy	61
26. The Synergistic $O_{1,2}$ Mapping Involving Both of the Threat Events B1 and E	63
27. Plot of R_1 Fitness Profile No. 9 From Table 6	65
28. Average Fitness Profile for R_1 Assuming Interthreat Synergy	66
29. Average Fitness Profile for R_1 Using Trinary States (Without Interthreat Synergy)	71
30. Average Fitness Profile for R_1 Using Trinary States (Assuming Interthreat Synergy)	72
31. Plot of R_1 Fitness Profile No. 9 From Table 9 Using Trinary States	73
32. Hypothetical Result Derived From Applying Threat Profile No. 9 (From Table 3) to All Metrics in the Requirement Vector (Assuming Interthreat Synergy and Trinary States)	78
A-1. Example of a Simple Fault Tree	85
A-2. Example of Two Different Boolean Logic Conventions Applied to the Fault Tree in Figure A-1: (a) Positive Logic, (b) Negative Logic	87

List of Tables

<u>Table</u>	<u>Page</u>
1. Degraded Subsystem States for a Generic Ground Combat System (Based on Information From Comstock [1991] and Saucier [in publication])	41
2. The Effect of the Threat Events B1, B2, E, and C on the Binary States (Following the Positive Logic Convention) of the Requirement Metrics R_1 and R_2 (No Interthreat Synergy Is Assumed)	54
3. Ten Different Threat Profiles for the Integrated Analysis of the Ground Combat System	54
4. Fitness Profile of the Ground Combat System Requirement Metric R_1 With No Interthreat Synergy	56
5. Fitness Profile of the Ground Combat System Requirement Metric R_2 With No Interthreat Synergy	57
6. Fitness Profile of the Ground Combat System Requirement Metric R_1 Using a Dynamic Target That Models Synergy Between a Ballistic and an EM Threat Event	64
7. Fitness Profile of the Ground Combat System Requirement Metric R_1 Using Trinary-Logic States and No Interthreat Synergy	69
8. Fitness Profile of the Ground Combat System Requirement Metric R_1 Using Trinary-Logic States and a Dynamic Target That Models Synergy Between a Ballistic and an EM Threat Event	70
B-1. The AND Operation (Using the Lukasiewicz Trinary Logic)	91
B-2. The OR Operation (Using the Lukasiewicz Trinary Logic)	91
B-3. The NOT Operation (Using the Lukasiewicz Trinary Logic)	92
C-1. Example of an "Attack" Mission Profile for a Generic Ground Combat System (CT = 24 hr)	96

INTENTIONALLY LEFT BLANK.

Executive Summary

Currently, the Survivability/Lethality Analysis Directorate (SLAD) of the U.S. Army Research Laboratory (ARL) is developing and refining an integrated vulnerability/lethality (V/L) analysis process for military systems exposed to the full spectrum of battlefield threats, including chemical/biological, nuclear, and environmental (CBN&E) threats; ballistic threats; and electronic warfare (EW) threats. This residual capability analysis is implemented through the use of an analytical process structure, or V/L taxonomy, which was developed for the V/L analysis of military systems exposed to battlefield threats. The V/L taxonomy clearly defines the elements of the V/L analysis process as: (1) generation/formation of the threat event (Level 0]), (2) initial conditions of the threat and the target system (Level 1]), (3) component response within the system (Level 2]), and (4) final remaining subsystem capability levels (Level 3]). Within a dynamic V/L process, which includes all battlefield threat/target interaction/response processes, the state of the system's battlefield capabilities can be determined at any instant in time, based on the states of those critical components that contribute to a specific system capability. Requirements exist for a methodology that provides both multithreat integration of component functional metrics (when appropriate), as well as a wide dispersal of initial threat/target interaction times for various threats within a predetermined window of time (reflecting a particular mission). The discrete time integrated analysis methodology documented in this report is such a methodology.

The discrete time integrated analysis methodology is built upon the following processes:

- an $O_{1,2}$ mapping, which maps one or more specific Level 1] threat/target initial conditions to a Level 2] component functionality metric for all critical components within the military system under analysis, resulting in a Level 2] state vector (interthreat synergy can be considered within this process);
- an integrated $O_{2,3}$ mapping, which maps a Level 2] vector listing the functional states (with respect to specific threats) of all critical components in the system, where allowed state values are 0, 1, or u (undetermined), to an integrated Level 3] capability state vector;

- a new mission fitness mapping, which maps a Level 3] capability vector to a vector of required mission tasks as defined in the system Operational Mode Summary/Mission Profile (OMS/MP); and
- the discrete time process, which assigns the aforementioned processes (in sequence) to each of a sequence of discrete time bins within a mission time frame.

Taken together, these processes define the overall discrete time integrated analysis process.

Implementation of the overall analytical process can be executed by using the following steps:

- (1) formulate the mission requirement vector for the system based on information contained in the OMS/MP and possible additional information from the U.S. Army Training and Doctrine Command (TRADOC) System Manager (TSM);
- (2) formulate a complete set of Level 3] capability metrics;
- (3) construct the fitness trees linking the Level 3] weapon system capabilities to the elements of the mission task requirement vector;
- (4) establish a complete set of Level 2] critical components and construct fault trees to map component damage to the appropriate Level 3] capability states;
- (5) determine which threats to be considered within the analysis produce Level 2] and Level 3] outcomes after interacting with the military system ($O_{1,2}$ or $O_{1,3}$ mapping);
- (6) implement the discrete time analysis structure by setting up time bins within each mission profile to be addressed; and

- (7) determine the nature of the integrated analysis by assembling the relevant threat profile(s).

After carrying out these last requirements, the analyst should be prepared to execute the integrated analysis.

To demonstrate the discrete time integrated analysis methodology, two example analyses are provided:

- (1) a simple system described by a four-element capability state vector, with particular focus on battlefield mobility requirements, and
- (2) a generic armored ground system for transportation of troops within the battlefield, where the system capability vector represents the states of seven on-board subsystems.

In both examples, application of the various processes within the discrete time integrated analysis methodology is illustrated.

In conclusion, the integrated analysis methodology allows for the effects of threat sequencing and interthreat synergy on required battlefield performance to be studied and analyzed. The discrete time analysis process also allows for both permanent component damage and transient component/subsystem dysfunction types of effects to be addressed. Finally, the integrated analysis methodology connects the analysis product to required battlefield performance metrics for a military system, thus providing the decision-maker with a means to evaluate the overall impact of battlefield threats on potential combat system effectiveness.

INTENTIONALLY LEFT BLANK.

1. Introduction

1.1 Purpose. The purpose of this report is to describe and illustrate, by application, a methodology for the integrated analysis of a military weapon system across all classes of battlefield threats addressed by the Survivability/Lethality Analysis Directorate (SLAD) of the U.S. Army Research Laboratory (ARL). In particular, focus is directed to the integrated analysis of a ground combat system. The process of discrete time analysis is applied to the battlefield operation of a ground combat system within a multithreat environment, where operation is limited to an interval of time matching one or more mission time windows. The analytical output of this methodology provides the military weapon system evaluator with a unique perspective on system operation within a multithreat battlefield environment.

1.2 Background.

1.2.1 General.

1.2.1.1 V/L Taxonomy. Currently, SLAD is developing and refining an integrated vulnerability/lethality (V/L) analysis process for military systems exposed to the full spectrum of battlefield threats, including chemical/biological, nuclear, and environmental (CBN&E) threats, ballistic threats, and electronic warfare (EW) threats. This analysis process uses the new and novel approach of integrating residual operational battlefield capabilities of materials, components, personnel, and subsystems into a top-level system assessment. This residual capability analysis is implemented through the use of an analytical process structure, or V/L taxonomy, which was developed for the V/L analysis of military systems exposed to battlefield threats (Deitz 1986; Deitz and Ozolins 1989; Deitz et al. 1990; Klopacic, Starks, and Walbert 1992; Walbert 1994; Ruth 1994; Hughes 1995; zum Brunnen 1995). This V/L Taxonomy, which is really a mathematical framework for V/L analysis developed by the Ballistics and NBC Division (BND),* SLAD/ARL, clearly defines the elements of the V/L analysis process as:

*The part of BND wherein this work was originally done was formerly known as the Vulnerability/Lethality Division of the U.S. Army Ballistic Research Laboratory (BRL), which was deactivated on 30 September 1992 and subsequently became part of ARL on 1 October 1992.

(1) generation/formation of the threat event, (2) interaction between the threat and the target system, (3) component response within the system, and (4) final remaining system capability levels.

Within the context of the V/L taxonomy framework, two critical concepts are defined.

- (1) Vulnerability Level: a set of points, where each point represents a vector containing information on the state of the weapon system under analysis. The number of points in a particular level is a function of the analytical granularity applied to the weapon system.
- (2) Mapping: a function that operates on a point (state vector) in one vulnerability level to generate a point in the next level. The mapping function itself is an algorithm (or set of algorithms) that incorporates the physics or engineering of a real-time and real-space process (such as electromagnetic pulse [EMP] coupling into a cable or chemical-agent penetration into an enclosure). The mapping operator $O_{n,n+1}$ is defined as the noninvertible function that maps a point in Level n] to another point or locus of points in Level $n + 1$].

Within the context of this report, four separate V/L taxonomy levels are considered: (1) Level 1], which is the set of all possible threat and weapon system conditions at the time of initial threat/target interaction; (2) Level 2], which is the set of all possible damaged components or “subsystem responses” resultant from threat/target interactions; (3) Level 3], which is the set of all possible residual capabilities of the target weapon system; and (4) Level 4], which is the set of all possible levels of overall postthreat battlefield utility of the weapon system. These four levels are then connected through the use of mapping operators, as previously described. Figure 1 illustrates the V/L taxonomy.

Recently, the first integrated V/L analysis of a U.S. Army system was completed through the use of the analysis methodology described by the V/L taxonomy (Myers, Ruth, and Kunkel in review). This analysis integrated all threat-specific analyses at Level 3]. Although a truly

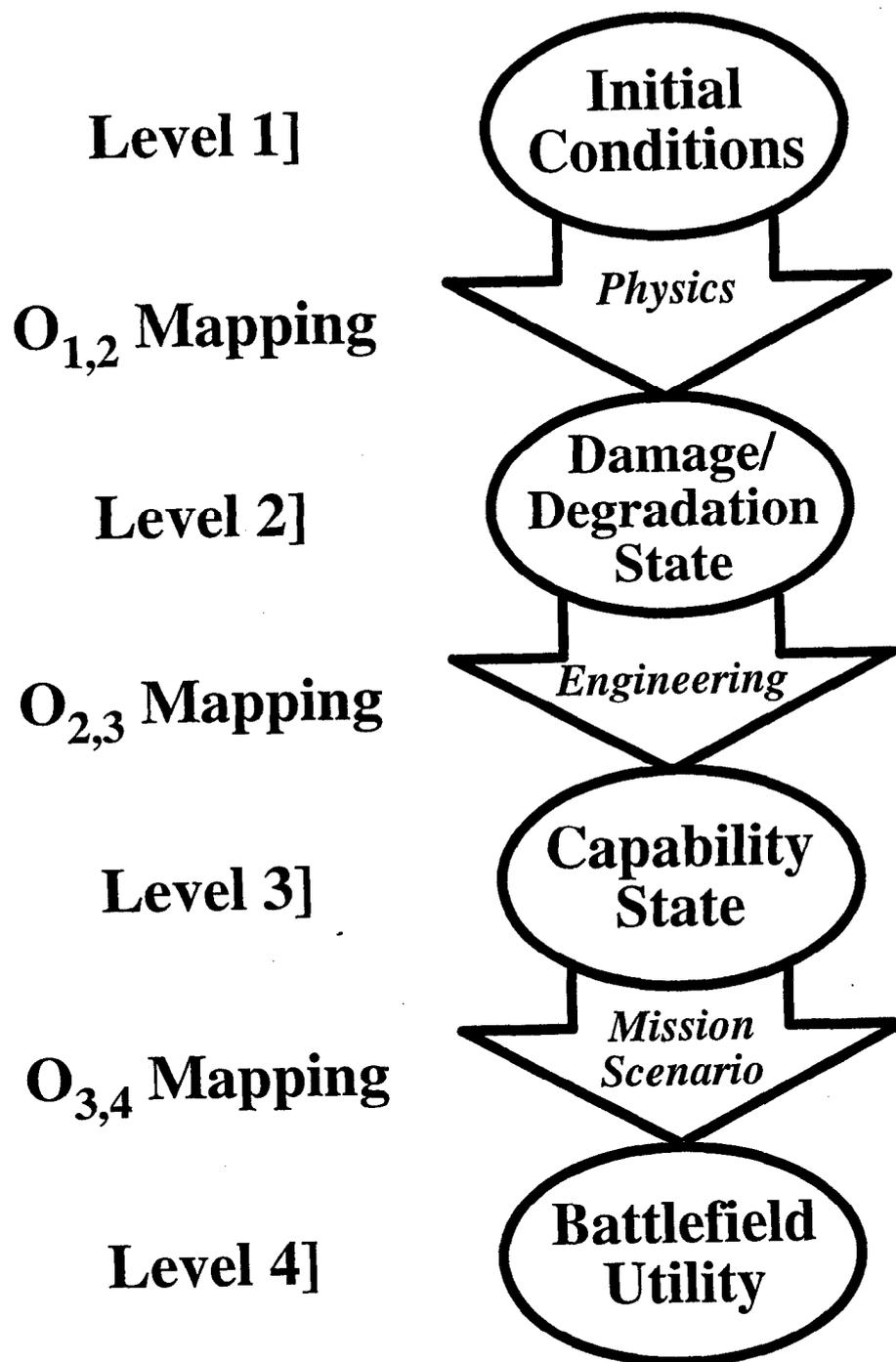


Figure 1. The V/L Taxonomy as Implemented Within the Integrated Analysis Process.

technical integration of threat-specific analyses should occur at Level 2], there are several issues that must first be addressed. One of these issues is the different nature of Level 2] metrics, namely the two classes corresponding to (1) component functionality values, which are evaluated from component damage vectors, and (2) subsystem response values, which are evaluated from subsystem response vectors. A second issue is the often-complex combination (through the $O_{2,3}$ mapping) of these different Level 2] metrics required to produce Level 3] system capability metrics.

1.2.1.2 Discrete Time V/L Process Structure. The state of a dynamical weapon system at a given instant can be envisioned as a “snapshot” in time fully describing the system dynamics (in terms of descriptive parameters) at the sample time. Within a dynamic V/L process, the state of the system’s battlefield capabilities can be determined at any instant in time, based on the states of those critical components that contribute to a specific system capability. Figure 2 illustrates the use of the V/L taxonomy to analyze system-level capabilities as a function of time.

In the real battlefield, dynamical V/L processes are continuous. The continuum that contains all V/L process vectors can be discretized into a set of time-sampled states, where each sampling represents a snapshot in time and the total number of time samplings is limited to a finite number. In this approach, the discretization of continuous time into a set of intervals or time bins (which may be either homogeneous or variable) is driven by two factors: (1) the relative time scales of the system dynamics, including both the threat/target system interaction physics and the postinteraction subsystem component response, and (2) the analytical granularity that a threat-specific model imposes upon the system dynamics. In Figure 2, t_k represents a “snapshot in time” of V/L processes within the k th time bin. The number of possible states that might occur at any sample time varies between the different levels of the V/L taxonomy: for Level 1], the possible states are countably infinite; for Level 2], the number of states is 2^n , where n is the number of critical components within the system (assuming binary component metrics); for Level 3], the number of states is, for a typical ground combat system (Saucier in publication), the product shown in equation (1):

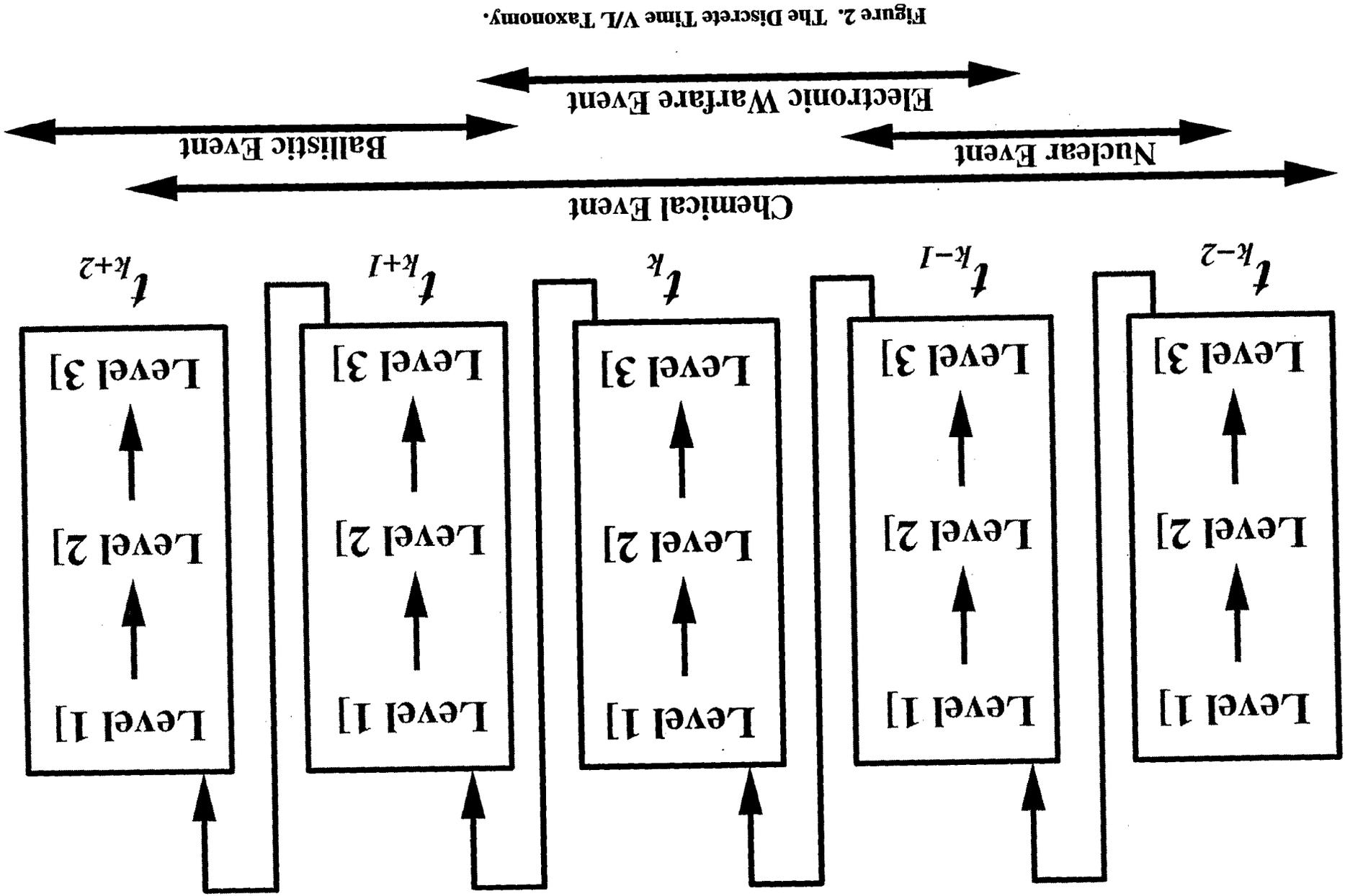


Figure 2. The Discrete Time V/L Taxonomy.

$$S_{\text{Level 3}} = S_{\text{Mobility}} * S_{\text{Firepower}} * S_{\text{Target Acq}} * S_{\text{Communication}} * S_{\text{Crew}} * S_{\text{Scouts}} * S_{\text{Catastrophic Loss}}, \quad (1)$$

where the term S_X = total number of degraded capability states in the X subsystem within the ground combat system.

The previous integrated analysis methodology used to analyze the Bradley Linebacker air defense system (Myers, Ruth, and Kunkel in review; Kunkel and Ruth in publication) used several assumptions that severely limited the scope of the analysis. In this approach, each threat-specific analysis was carried out independently from Level 1] to Level 3] of the V/L taxonomy, with the final “integration” of threat-specific capability metrics at Level 3]. Although this approach produced the correct capability states at Level 3], information was not presented in a manner allowing the analyst or system evaluator to compare different threat effects on a component at Level 2]. In addition, the time bins required for discrete time V/L analysis were set up to reflect an imprecise nonlinear passage of time; successive time bins were labeled “seconds,” “minutes,” “hours,” and “days.” Because of this limitation, it was necessary to assume that all battlefield threats in the analysis commenced interaction with the target system at the same time t_0 in order to compare the dynamical effects of different threats. What is required now is an improved methodology that provides both multithreat integration of component metrics at Level 2] (when appropriate), as well as a wide dispersal of initial threat/target interaction (Level 1]) times for various threats within a predetermined window of time (reflecting a particular mission).

1.2.2 Threat. The methodology presented in this paper addresses the effects of all battlefield threats on a military weapon system, which include ballistic, nuclear, biological, and chemical (NBC), nuclear EMP, nuclear blast/thermal wave, initial nuclear radiation (INR), smoke/obscurants, EW, EMI/EMC (E3), lightning, and information warfare (IW) threats.

1.3 Scope. The scope of the methodology described in this paper is summarized by the following statements.

- The operational performance requirements for the ground combat system must be quantitatively specified in a document such as the Operational Mode Summary/Mission Profile (OMS/MP) for the system under analysis.
- All separate threat-specific system analyses of the ground combat system may be combined into one common structure.
- All battlefield processes are constrained to a discrete time framework, which is adjustable according to the dynamics within the threat scenario driving the analysis.
- Only limited interthreat synergy is considered; most threat/system interactions are considered to be independent from one another.

2. Theory of Discrete Time V/L Processes

In this section, the elements of the improved integrated analysis methodology are described in detail, as well as the steps required to implement the methodology within an analysis.

2.1 The Generic $O_{1,2}$ Mapping. The first step in the integrated analysis process is to set up what happens within a generic time bin at t_k . The first mapping within this time bin (the $O_{1,2}$ mapping) connects one or more specific Level 1] threat/target interaction events to a Level 2] component functionality metric for all critical components within the system under analysis. There are two submappings within the overall $O_{1,2}$ mapping, namely, the interaction mapping and the evaluation mapping.* The interaction mapping models the physical interaction between a threat and the target system, which can result in physically measurable damage to components within the system.† The evaluation mapping then follows the interaction mapping by assigning a

* This two-stage mapping process is based on the similarly named interaction and evaluation modules as implemented within the Modular UNIX-based Vulnerability Estimation Suite (MUVES) (Murray, Moss, and Coates, unpublished).

† In this methodology, transient component dysfunction due to electromagnetic (EM) threats is also included under the rubric of "component damage" even though no physical damage is incurred by the component.

component functionality metric to all critical components within the system based on the damage incurred by a component. Figure 3 illustrates the elements of the generic $O_{1,2}$ mapping.

In the present methodology, there are two classes of Level 2] component damage metrics:

- (1) A fractional remaining functionality (FRF) metric, which follows the positive-logic convention:

Component Function = 0 if component becomes dysfunctional during, and/or after interaction with a threat, or
= 1 if component remains functional during and/or after interaction with a threat.

- (2) A loss of function (LOF) metric, which follows the exact opposite convention (the negative-logic convention):

Component Dysfunction = 0 if component remains functional during and/or after interaction with a threat, or
= 1 if component becomes dysfunctional during and/or after interaction with a threat.

The positive-logic convention for binary metrics assigns a 1 to represent “positive” or residual function, while the negative-logic convention assigns a 1 to represent “negative” function or dysfunction (Kunkel 1995). In the present methodology, the positive-logic convention is followed for functional metrics, unless otherwise noted.

Since the interaction and evaluation submappings within the overall $O_{1,2}$ mapping are threat-specific, the completeness of the submapping processes will likely vary from threat to threat. Because of this, it is necessary to provide mapping paths within the generic $O_{1,2}$ mapping to account for incomplete or unavailable processes. These paths are shown explicitly in Figure 3. If, for a particular threat/target interaction, the interaction mapping is incomplete, then evaluation

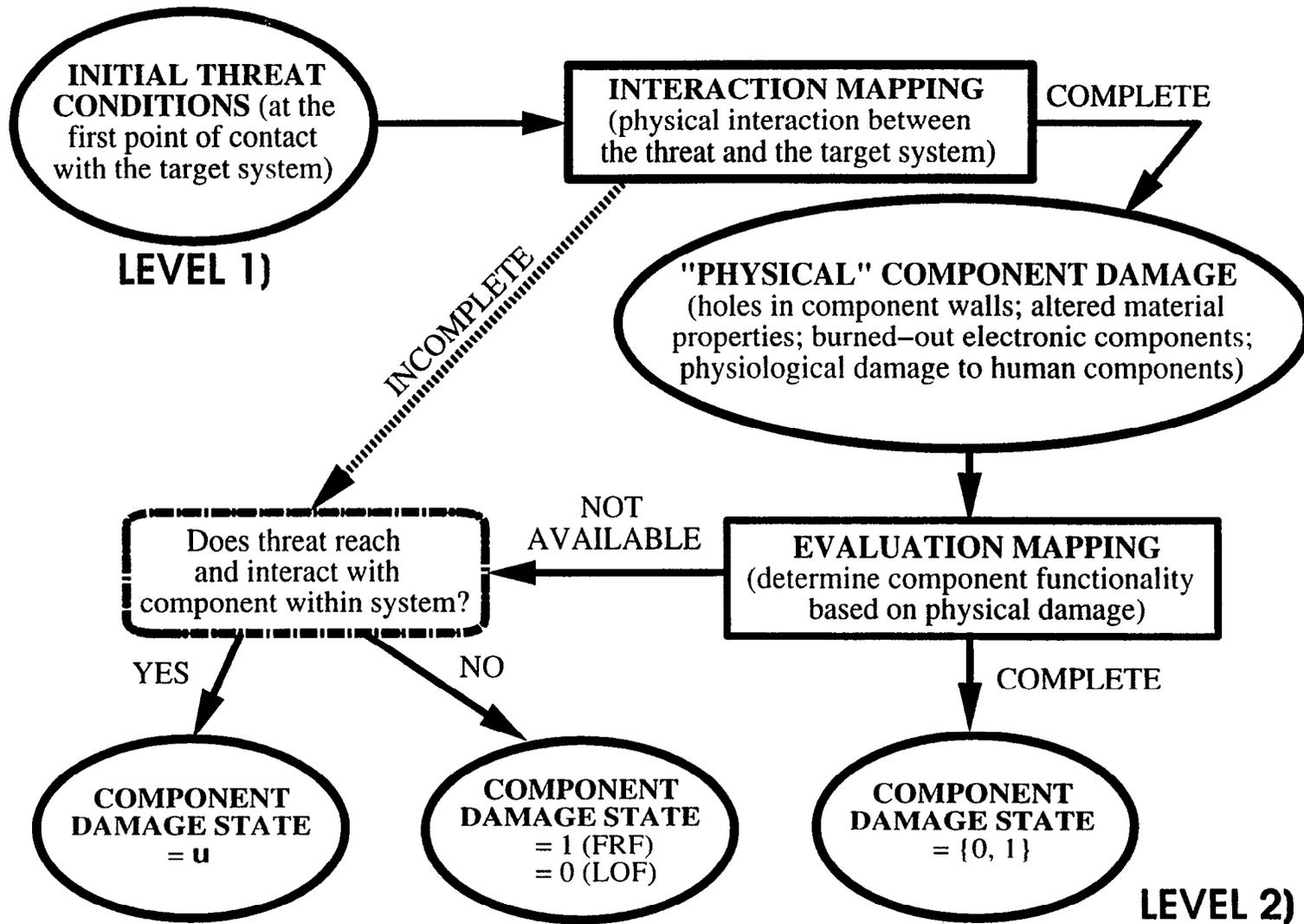


Figure 3. Elements of the Generic O_{1,2} Mapping.

of a component damage state may not be feasible and the mapping path follows the dotted line as shown in Figure 3) to the round-edged box where one must answer the question:

Does the threat reach and interact with a specific component within the system?

This question is also reached in the mapping process when the interaction mapping is complete but the corresponding evaluation mapping is not available. If the answer to the above question is “no,” then the component functionality is unaffected by the threat, and the FRF state is equal to 1. If, on the other hand, the answer is “yes,” then all that is known about the state of the component is that it may be dysfunctional; in this case, the component damage state is “undetermined” and symbolized by a “u.” In the remaining case where both interaction and evaluation mappings are complete, a measurable component damage state is realizable and the value is drawn from the value set $\{0, 1\}$. Note that, at this stage in the V/L analysis process, the undetermined component damage state u is really a third type of functional metric that is part of neither the positive- nor negative-logic conventions.

2.2 The Synergistic $O_{1,2}$ Mapping. The mapping processes described in the previous section assume that separate and independent $O_{1,2}$ mappings are carried out for each specific threat within the analysis, with a resulting set of independent threat-specific component damage metrics. In order to account for possible synergy between two threats, a target description that reflects and “remembers” possible physical damage from a threat (a target description with memory) is required. Figure 4 illustrates the processes within a synergistic $O_{1,2}$ mapping involving two threats that are sequential in time.

The processes commence at time t_k when a threat (designated threat no. 1 in Figure 4) interacts with and possibly damages components within the target. The interaction and evaluation mappings are carried out relative to threat no. 1, and all resultant component damage states are mapped into a component damage state vector encompassing all critical components:

$$c(\text{threat no. 1}) = [c_1(\text{threat no. 1}), c_2(\text{threat no. 1}), c_3(\text{threat no. 1}), \dots, c_n(\text{threat no. 1})], \quad (2)$$

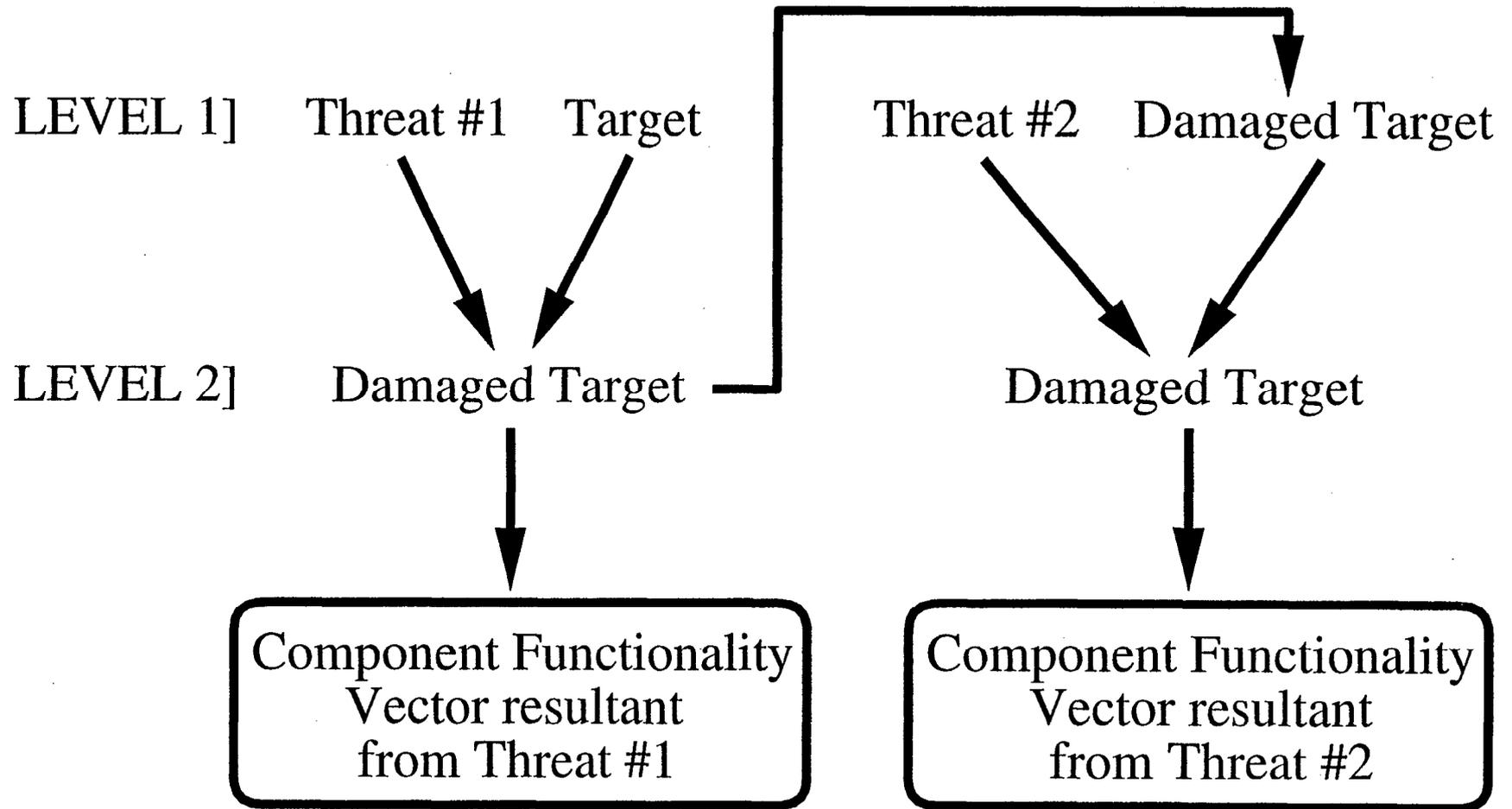


Figure 4. The Synergistic O_{1,2} Mapping.

where $c_1, c_2, c_3, \dots, c_n$ = component functionality metrics for the n critical components in the system. The next process involves the interaction of a second threat (designated threat no. 2 in the Figure 4) with the target at a point in time proceeding the threat no. 1/target interaction time, which is designated t_{k+1} in Figure 4.* But this second threat/target interaction process now involves a possibly modified target description reflecting damage from threat no. 1. The interaction and evaluation mappings are carried out relative to threat no. 2 using this modified target description, with the resultant component functionality vector

$$c(\text{threat no. 2}) = [c_1(\text{threat no. 2}), c_2(\text{threat no. 2}), c_3(\text{threat no. 2}), \dots, c_n(\text{threat no. 2})]. \quad (3)$$

The two vectors $c(\text{threat no. 1})$ and $c(\text{threat no. 2})$ are then added together at time t_{k+1} by using the Boolean AND operation; this operation is described further in section 2.4.

2.3 Threat-Specific Level 2] and Level 3] Metrics. It should be noted at this point that not all threat-specific interactions with a target system produce component damage metrics, nor do all threat-specific analyses follow the $O_{1,2}$ mapping (described in detail in the next section). Certain threat/target interactions involve the flow of a resource between electrical/electronic components, where the flowing resource in question may be either electromagnetic (EM) signals, electrical currents, or digital information packets. The disruption in flow or “corruption” (i.e., additive signal noise or misinformation) of these resources will result in the temporary dysfunction of a component or subsystem of connected components. In some cases, it is not feasible to measure these transient effects at the component level but, rather, at the subsystem platform level through a “hardware-in-the-loop” simulation.

Figure 5 illustrates the suggested V/L taxonomy levels where threat-specific metrics should be integrated with other threat-specific metrics. In general, ballistic, NBC, nuclear blast/thermal, and lightning threats result in component damage and are thus integrated at Level 2]; nuclear

* It is also possible that threat no. 1 may occur during the threat no. 2/target interaction, where the duration of threat no. 1 is much shorter than that of threat no. 2. In this case, the remainder of the threat no. 2/target interaction the threat no. 1/target interaction is considered within the context of the synergistic $O_{1,2}$ mapping. For example, this situation would arise when a ballistic threat event occurred during the infiltration of a chemical agent into a battlefield system; the ballistic threat might not damage any critical components but would still alter the target by puncturing a wall, resulting in increased ingress of the chemical-agent threat.

THREAT	Integrate at Level 2]	Integrate at Level 3]
ballistic	●	
NBC	●	
nuclear EMP	●	
nuclear blast/thermal	●	
INR	●	
smoke/obscurants		●
EMI/EMC (E3)	●	
EOCM		●
Lightning	●	
MOPP IV Compatability		●
Information Warfare (IW)	●	

Figure 5. Suggested V/L Taxonomy Levels Where Threat-Specific Metrics Should Be Integrated With Other Threat-Specific Metrics.

EMP, INR, electromagnetic interference/electromagnetic compatibility (EMI/EMC), and IW threats can result in either component damage or resource interruption/corruption but can still be integrated at Level 2]; finally, smoke/obscurants, electro-optical countermeasures (EOCM), and mission-oriented protective posture level 4 (MOPP IV) compatibility threats will usually affect the function of an entire subsystem platform (such as a target acquisition system or a crew member), and must be integrated at Level 3] since the threat effect directly affects a system capability rather a single component. The actual integration processes involving the threat-specific metrics previously described are explained in the next section.

2.4 The Integrated O_{2,3} Mapping. Once threat-specific Level 2] component damage states have been established for all critical components at time t_k , a mapping to integrated Level 3] system capability states may be executed; this is called the integrated O_{2,3} mapping. Starting with a vector listing the functional states of all critical components in the system, where allowed state values are 0, 1, or u, several logical processes are carried out on the component states in the vector until a resultant capability state vector at time t_k is produced. The processes within the integrated O_{2,3} mapping are diagrammed in Figure 6.

The first process within the O_{2,3} mapping involves the integration of all threat-specific functionality metrics for a specific component into one net component metric. This basically involves finding the “weak link” among all threat-specific metrics for a component. For the positive-logic convention, the weak link can be expressed as the intersection among a set of independent threat-specific component “activation” events:*

$$\text{Comp}(N)_{\text{NET}} = \bigcap_{i=1}^n \text{Comp}(N)_i, \quad (4)$$

where $\text{Comp}(N)_i$ is the functionality of the N th critical component during or after exposure to the i th threat (from a total of n threats), which represents the intersection operation between sets, and

* The threat-specific events are assumed to be independent, in that, there is no physical interaction/coupling between two Level 1] threat events. However, interthreat synergy is still possible, given that two threats are sequential intime and target description is dynamic (see section 2.2).

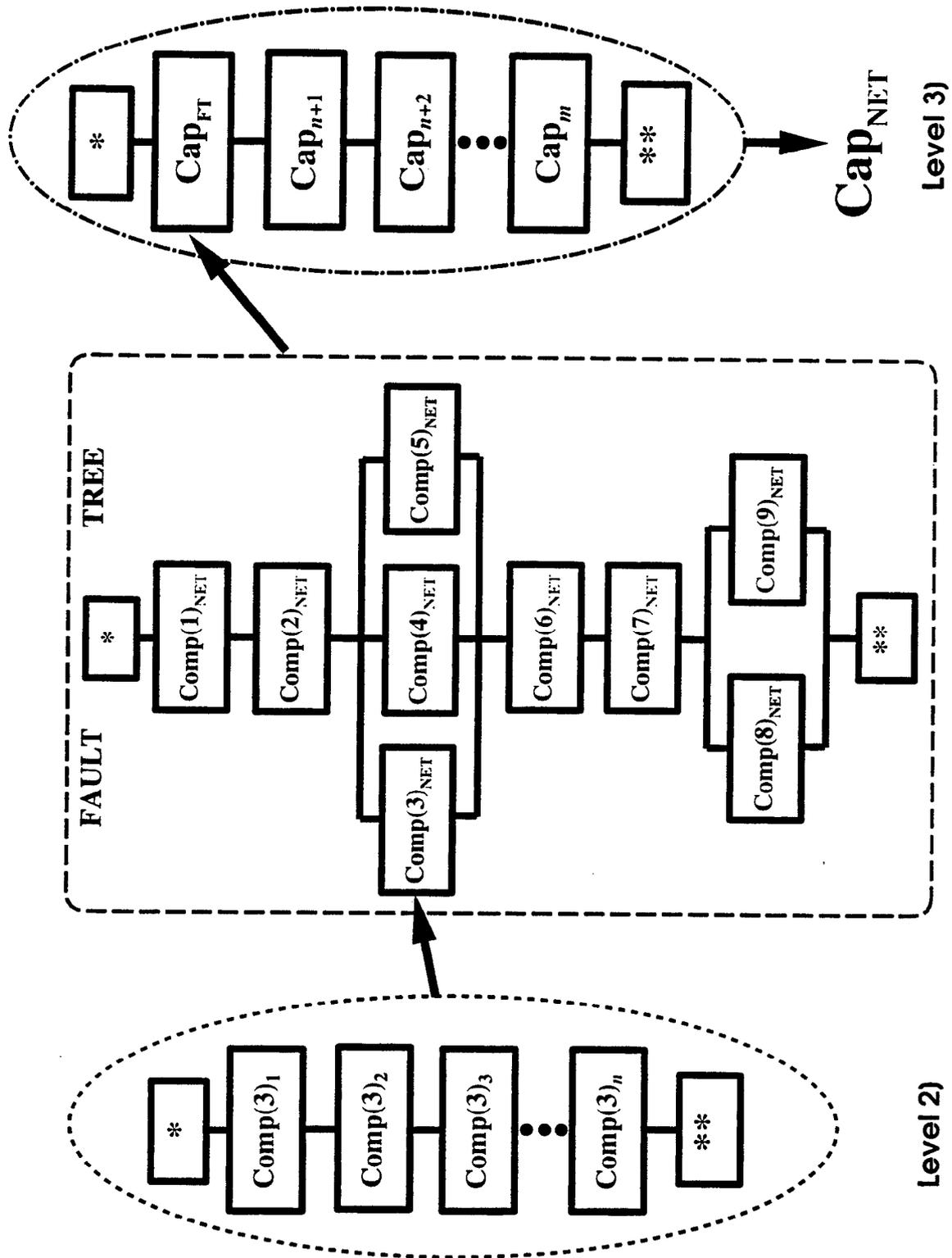


Figure 6. Elements of the Integrated $O_{2,3}$ Mapping.

$\text{Comp}(N)_{\text{NET}}$ is the net component functionality after integration (i.e., the intersection among all threat-specific sets of functional metrics relating to $\text{Comp}(N)$). Evaluation of equation (4) can be carried out through the logical expression

$$\text{Comp}(N)_{\text{NET}} = \text{Comp}(N)_1 \& \text{Comp}(N)_2 \& \text{Comp}(N)_3 \& \dots \& \text{Comp}(N)_n, \quad (5)$$

where the symbol “&” represents the logical AND operation between two metrics. Then $\text{Comp}(N)_{\text{NET}}$ is the *minimum* value among the threat-specific metrics $\text{Comp}(N)_1$, $\text{Comp}(N)_2$, $\text{Comp}(N)_3$, ... $\text{Comp}(N)_n$. Similarly, for the negative-logic convention, the weak link can be expressed as the union among a set of independent threat-specific component “deactivation” events

$$\text{Comp}(N)_{\text{NET}} = \bigcup_{i=1}^n \text{Comp}(N)_i, \quad (6)$$

where the symbol \bigcup represents the union operation between sets; this is evaluated through the logical expression

$$\text{Comp}(N)_{\text{NET}} = \text{Comp}(N)_1 \mid \text{Comp}(N)_2 \mid \text{Comp}(N)_3 \mid \dots \mid \text{Comp}(N)_n, \quad (7)$$

where the symbol “|” represents the logical OR operation between two metrics. In this case, $\text{Comp}(N)_{\text{NET}}$ is the maximum value among the threat-specific metrics $\text{Comp}(N)_1$, $\text{Comp}(N)_2$, $\text{Comp}(N)_3$, ... $\text{Comp}(N)_n$. Thus, in the example shown in Figure 6, $N = 3$ (the third of nine different components within a subsystem/system) and the output of the first process is $\text{Comp}(3)_{\text{NET}}$. If only threat no. 2 causes the component to dysfunction, then:

$$\text{Comp}(3)_{\text{NET}} = [\text{Comp}(3)_1 = 1] \& [\text{Comp}(3)_2 = 0] \& [\text{Comp}(3)_3 = 1] \& \dots \& [\text{Comp}(3)_n = 1] = 0, \quad (8)$$

following the positive-logic convention, and

$$\text{Comp}(3)_{\text{NET}} = [\text{Comp}(3)_1 = 0] \mid [\text{Comp}(3)_2 = 1] \mid [\text{Comp}(3)_3 = 0] \mid \dots \mid [\text{Comp}(3)_n = 0] = 1, \quad (9)$$

following the negative-logic convention. In both cases, threat no. 2 is of principal concern to the analyst since it alone has caused the third critical component in the system to fail (which is reflected in the metric $\text{Comp}(3)_{\text{NET}}$).

The second process within the $O_{2,3}$ mapping involves the evaluation of one or more fault trees, where a fault tree comprises net component functionality states for all critical components in combination with logical operators. In Figure 6, the net functionality state for component no. 3, $\text{Comp}(3)_{\text{NET}}$, is input into a fault tree which executes the logical expressions

$$\begin{aligned} \text{Cap}_{\text{FT}} = & \text{Comp}(1)_{\text{NET}} \& \text{Comp}(2)_{\text{NET}} \& (\text{Comp}(3)_{\text{NET}} \mid \text{Comp}(4)_{\text{NET}} \mid \text{Comp}(5)_{\text{NET}}) \\ & \& \text{Comp}(6)_{\text{NET}} \& \text{Comp}(7)_{\text{NET}} \& (\text{Comp}(8)_{\text{NET}} \mid \text{Comp}(9)_{\text{NET}}), \end{aligned} \quad (10)$$

or

$$\begin{aligned} \text{Cap}_{\text{FT}} = & \text{Comp}(1)_{\text{NET}} \mid \text{Comp}(2)_{\text{NET}} \mid (\text{Comp}(3)_{\text{NET}} \& \text{Comp}(4)_{\text{NET}} \& \text{Comp}(5)_{\text{NET}}) \\ & \text{Comp}(6)_{\text{NET}} \mid \text{Comp}(7)_{\text{NET}} \mid (\text{Comp}(8)_{\text{NET}} \& \text{Comp}(9)_{\text{NET}}), \end{aligned} \quad (11)$$

for positive- and negative-logic conventions, respectively. The terms $\text{Comp}(1)_{\text{NET}}$, $\text{Comp}(2)_{\text{NET}}$, $\text{Comp}(3)_{\text{NET}}$, ..., $\text{Comp}(8)_{\text{NET}}$, $\text{Comp}(9)_{\text{NET}}$ represent the functional states of the first, second, third, ..., eighth, and ninth components in the fault tree, respectively, after all of the battlefield threats within the analysis have been applied to the components. The term Cap_{FT} represents the output of the fault tree and is thus submitted to the next process within the integrated $O_{2,3}$ mapping. For more information on fault trees, see Appendix A.

The third and final process within the $O_{2,3}$ mapping involves the integration of the net component functional state (the fault-tree output) with a set of threat-specific capability states; these latter states are the result of threat-specific analyses that directly map from Level 1] to Level 3]. This so-called " $O_{1,3}$ mapping" is necessary in situations where a threat will act to deactivate or functionally degrade a subsystem of components as a unit, such as hardware-in-the-loop simulations involving EM threats and MOPP IV compatibility effects. As with the first process previously described, this current process involves finding the weak link

among a set of states, which includes Cap_{FT} , as well as the previously mentioned threat-specific capability states resulting from the $O_{1,3}$ mapping. For the positive-logic convention, the weak link can be expressed as the intersection among a set of independent threat-specific capability activation events:

$$Cap_{NET} = Cap_{FT} \cap \left\{ \bigcap_{i=n+1}^m Cap_i \right\}, \quad (12)$$

where Cap_i is the subsystem/system capability during or after exposure to the i th threat following the $O_{1,3}$ mapping convention (from a total of $m - n$ threats, which follow this convention, thus making a total of m threats addressed within the integrated analysis), \cap represents the intersection operation between sets and Cap_{NET} is the net subsystem/system capability after integration. Evaluation of equation (12) can be carried out through the logical expression

$$Cap_{NET} = Cap_{FT} \& Cap_{n+1} \& Cap_{n+2} \& Cap_{n+3} \& \dots \& Cap_m. \quad (13)$$

Similarly, for the negative-logic convention, the weak link can be expressed as the union among a set of independent threat-specific capability “deactivation” events:

$$Cap_{NET} = Cap_{FT} \cup \left\{ \bigcup_{i=n+1}^m Cap_i \right\}, \quad (14)$$

where \cup , again, represents the union operation between sets; this is evaluated through the logical expression

$$Cap_{NET} = Cap_{FT} | Cap_{n+1} | Cap_{n+2} | Cap_{n+3} | \dots | Cap_m. \quad (15)$$

Again, referring back to the example shown in Figure 6, if, instead of threat no. 2 failing component no. 3, threat $n + 2$ causes the capability to deactivate through the $O_{1,3}$ mapping, then:

$$Cap_{NET} = [Cap_{FT} = 1] \& [Cap_{n+1} = 1] \& [Cap_{n+2} = 0] \& [Cap_{n+3} = 1] \& \dots \& [Cap_m = 1] = 0, \quad (16)$$

following the positive-logic convention, and

$$\text{Cap}_{\text{NET}} = [\text{Cap}_{\text{FT}} = 0] \mid [\text{Cap}_{n+1} = 0] \mid [\text{Cap}_{n+2} = 1] \mid [\text{Cap}_{n+3} = 0] \mid \dots \mid [\text{Cap}_m = 0] = 1, \quad (17)$$

following the negative-logic convention. In both cases, the system capability has been lost after analyzing the effects of all of the battlefield threats considered within the integrated analysis.

It is important to note, at this point, that the integrated capability state, Cap_{NET} , in equation (12) reflects the situation where a Level 3] degraded capability state can be reached by following either the standard $O_{1,2}$ and $O_{2,3}$ mappings (where component-level dysfunction is assessed) or the $O_{1,3}$ mapping (where subsystem-level dysfunction is directly assessed). In addition to states such as Cap_{NET} , there may be other Level 3] degraded capability states that are not based on fault trees and thus arise solely from a threat-specific $O_{1,3}$ mapping. An example of such a capability state might be a target acquisition state (where acquisition range is limited by the presence of a smoke/obscurant threat); this degradation to subsystem capability is not traceable to any kind of component-level damage but rather to an attenuated acquisition signal. In general, the $O_{1,3}$ mapping can generate Level 3] capability states that also arise out of fault trees (within the $O_{2,3}$ mapping), as well as other states that are unique to the $O_{1,3}$ mapping.

The integrated $O_{2,3}$ mapping (which is really an integrated $O_{1,3}/O_{2,3}$ mapping combination) within time bin t_k is completed when the aforementioned three processes are executed for all critical components within the weapon system under analysis and a complete Level 3] capability state vector has been determined. Since it has been established within the context of this methodology that some of the threat-specific Level 2] component damage metrics (as well as certain threat-specific Level 3] capability metrics) may be in the undetermined (u) state, the standard Boolean operations on binary states must be extended to address logical operations on the set $\{0, 1, u\}$. This can be done through the application of a trinary system of logical operations developed by Lukasiewicz (Borkowski and Slupecki 1958). For more information on the Lukasiewicz trinary logic, see Appendix B.

2.5 The Mission Fitness Mapping. Once the Level 3] capability state vector has been determined, a final mapping process can be executed in order to evaluate the fitness or battlefield readiness of a weapon system at a point in time. To illustrate this process, consider a simple generic Level 3] capability state vector of the form

$$\vec{C} = \begin{bmatrix} M(\text{Mobility}) \\ F(\text{Firepower}) \\ X(\text{Communication}) \\ C(\text{Personnel}) \end{bmatrix}, \quad (18)$$

where each of the four metrics in this vector represent the state of availability of a battlefield capability in an ground combat system at a point in time. In this simple example, the hypothetical ground combat system can only move/not move, fire/not fire, communicate/not communicate, and maintain functional/dysfunctional personnel. Using these four binary metrics, the operational state of the ground combat system can always be represented by one of $2^4 = 16$ possible binary state vectors. If a third undetermined state is added to extend the set of allowable metric states to $\{0, 1, u\}$, then the cardinality of the Level 3] space is also extended from 16 to $3^4 = 81$ possible state vectors.

Once an allowable set of Level 3] capability state vectors is established, a second set of state vectors is formulated in order to represent the operational functions required of the system in the battlefield. The required mission task vector or requirement vector R is thus defined as a set of metrics representing the various battlefield operations required of the weapon system within a specific type of mission. The elements within a requirement vector are based on the required system operations as specified in a military performance requirements document such as the system's OMS/MP, which is typically included as part of the system's Operational Requirements Document (ORD). To continue the previously stated example, the capability state vector in equation (18) is mapped into the following requirement vector:

$$\begin{bmatrix} M(\text{Mobility}) \\ F(\text{Firepower}) \\ X(\text{Communication}) \\ C(\text{Personnel}) \end{bmatrix} \Rightarrow \begin{bmatrix} R_1 \\ R_2 \\ R_3 \end{bmatrix}, \quad (19)$$

where R_1 , R_2 , and R_3 are the requirement metrics for the system in the battlefield. If the crew capability C is expanded to include the three specific crew members C_{comm} = commander, C_{driver} = driver, and C_{gunner} = gunner, then the three requirements can be defined as

$$R_1 = M \ \& \ C_{\text{driver}} \rightarrow \text{battlefield mobility requirement}, \quad (20a)$$

$$R_2 = F \ \& \ C_{\text{gunner}} \rightarrow \text{battlefield firepower requirement, and} \quad (20b)$$

$$R_3 = X \ \& \ C_{\text{comm}} \rightarrow \text{battlefield communication requirement}, \quad (20c)$$

following the positive-logic convention, and

$$R_1 = M \ | \ C_{\text{driver}} \rightarrow \text{battlefield mobility requirement}, \quad (21a)$$

$$R_2 = F \ | \ C_{\text{gunner}} \rightarrow \text{battlefield firepower requirement, and} \quad (21b)$$

$$R_3 = X \ | \ C_{\text{comm}} \rightarrow \text{battlefield communication requirement}, \quad (21c)$$

following the negative-logic convention. It is fairly straightforward to reason that each of the three requirements in turn requires both a hardware platform capability and a crew member in order to function, where each crew member is trained to perform a specific function (this example assumes no cross-training). Thus, the requirement vector is just a logical extension of the system capability state vector that can be evaluated by using logical expressions similar to those in equations (20) and (21).*

* The requirement vector is not the results of a force-on-force analysis but could serve as an input into such a process.

The logical constructs represented by the previous equations are referred to as fitness trees within the context of this methodology, where a fitness tree maps Level 3] system capability metrics to requirement metrics as specified in the system OMS/MP. The logical operations within a fitness tree can include both the standard AND, OR, and NOT operators as well as conditional logic statements (as is illustrated in section 4.2). Figure 7 illustrates the fitness trees for the logical expressions in equations 20 and 21. Fitness trees are similar to fault trees, except that the latter are utilized within the $O_{2,3}$ mapping, while the former are limited to use within the mission fitness mapping.

It should be noted that the requirement states R_1 , R_2 , and R_3 are different from system capability states in that the former are based on an operational performance standard (OMS/MP), while the latter emerge from system engineering-based design. Thus, the requirement states rate the mission fitness or battlefield readiness of the weapon system to perform required operations based on the Level 3] capability states. To illustrate this concept, let us return to the example of the ground combat system. Assume that a ballistic threat has disabled the mobility hardware platform (M) and a transient EM threat has coupled into the communication hardware/software platform (X); however, further assume that the effects of the EM threat on communication system functionality cannot be presently measured, only estimated. Then, following the positive-logic convention,

$$R_1 = [M = 0] \& [C_{\text{driver}} = 1] = 0, \quad (22a)$$

$$R_2 = [F = 1] \& [C_{\text{gunner}} = 1] = 1, \text{ and} \quad (22b)$$

$$R_3 = [X = u] \& [C_{\text{comm}} = 1] = u, \quad (22c)$$

and, following the negative-logic convention,

$$R_1 = [M = 1] \mid [C_{\text{driver}} = 0] = 1, \quad (23a)$$

$$R_2 = [F = 0] \mid [C_{\text{gunner}} = 0] = 0, \text{ and} \quad (23b)$$

$$R_3 = [X = u] \mid [C_{\text{comm}} = 0] = u. \quad (23c)$$

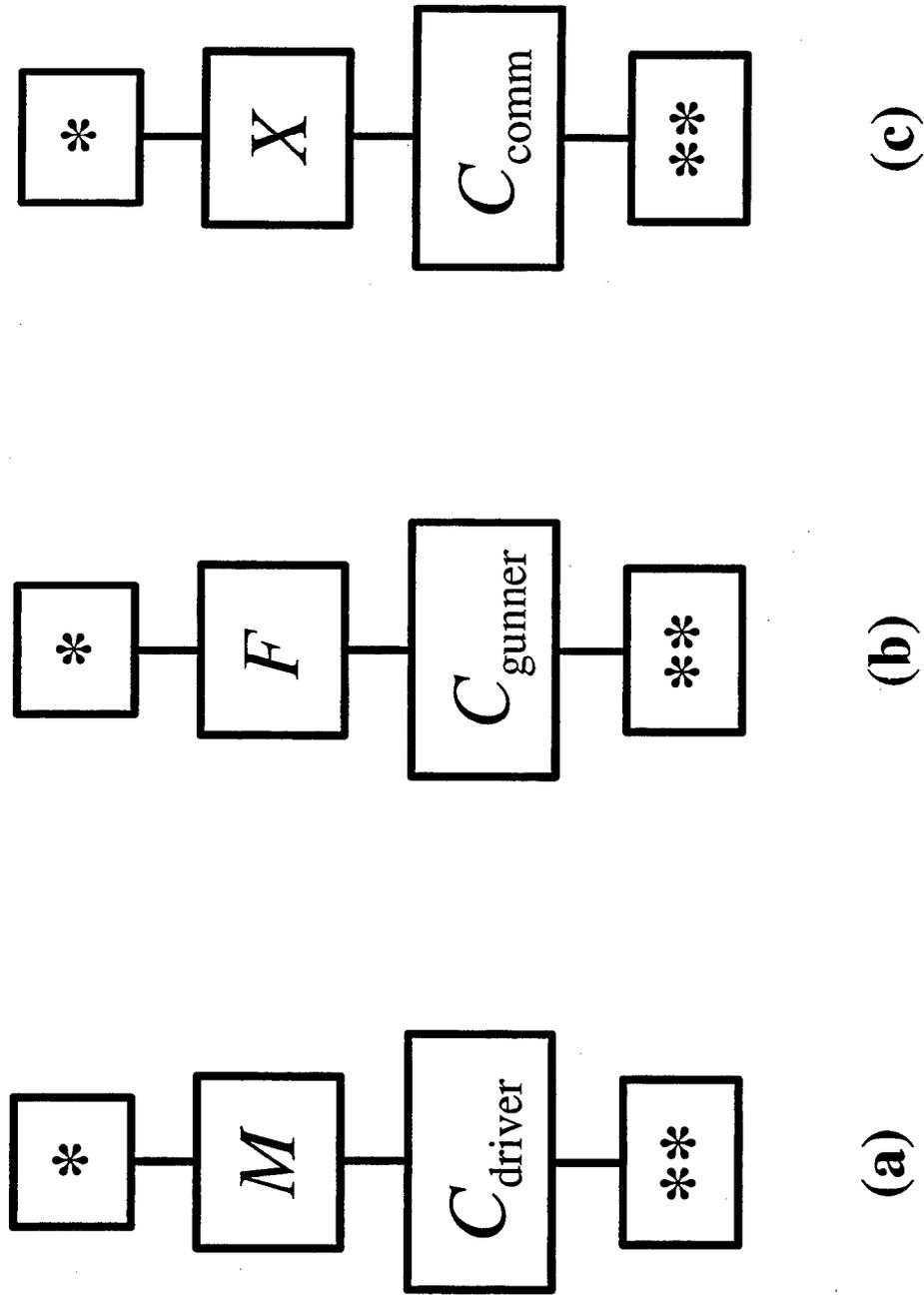


Figure 7. Fitness Trees For the Battlefield (a) Mobility, (b) Firepower, and (c) Communication Requirements as Described by Equations (20) and (21).

Thus, the ground combat system (1) cannot fulfill its battlefield mobility requirement, (2) can fulfill its battlefield firepower requirement, and (3) may fail to fulfill its battlefield communication requirement. The weapon system evaluator might think of these metrics in terms of indicative colors: (1) red (No Go/Fail), (2) green (Go), and (3) yellow (Warning). It is interesting to also note that the u state will emerge regardless of whether the positive- or negative-logic convention is followed.

2.6 The Discrete Time Analysis Process. In section 1.2.1.2, the discrete time V/L process structure was introduced. Once all of the required V/L mapping processes (from Level 1] to the requirement vector) have been executed for a time bin, the resultant system functional information must be placed within the framework of a dynamical system. This is done by executing the V/L mapping processes within each time bin of the discrete time V/L process structure. In this section, the steps involved in setting up the discrete time V/L process structure and running the discrete time analysis are described.

First of all, the discrete time axis must be configured. This basically involves three steps: (1) establish the duration of a discrete time bin, which should be adjustable according to the threat scenario(s) considered within the analysis; (2) establish the length of the time axis to match that of a particular mission profile,* as described in the weapon system's OMS/MP; and (3) discretize the time scale into a sequence of time bins of equal length. Figure 8 shows a typical discrete time axis; if the length of a mission (mission time frame) is equal to T , and there are m time bins within the mission time frame, then the length of a time bin is equal to T/m . In step (1), the length of a time bin should reflect the time scale of the most dynamic threat addressed within the analysis; this is typically some form of EM threat. Unfortunately, the time duration of a pulsed EM threat is typically $\ll 1$ s, and the duty cycle (on/off cycle) of an intermittent EM threat (or other intermittent threat, such as a smoke/obscurant, which affects EM signal transmission/reception by the weapon system) may also be on the order of 1 s or less. To amplify the complexity of this problem, intermittent threats often do not result in any permanent

* A mission profile is a table identifying the tasks, number of occurrences of each task, and task duration associated with a particular mission. For an example, see Appendix C.

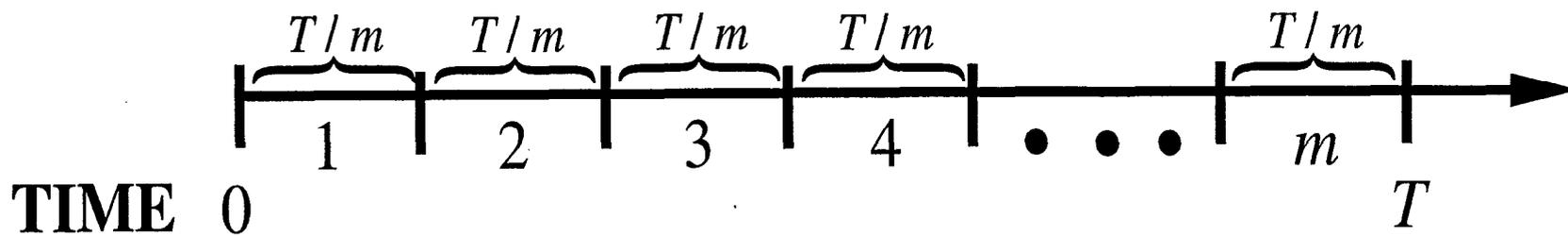


Figure 8. Layout of a Typical Discrete Time Axis.

damage to components, so that component and/or subsystem functionality is restored once the threat is removed.

Because these intermittent threats (and their resultant effects on component and/or subsystem functionality) may vary greatly over a fixed-length time bin, the component/subsystem functional history within the time bin is compressed into a time-averaged state, which can be written as $\langle State \rangle$. This time-averaged state is mathematically defined as

$$\langle State \rangle = \frac{1}{T_2 - T_1} \int_{T_1}^{T_2} State(t) dt, \quad (24)$$

where $State(t)$ = component or subsystem functionality state at time t , T_1 = initial time within a time bin, and T_2 = final time within a time bin. This equation assumes that time is continuous within a time bin. In general, the value of $\langle State \rangle$ will usually lie between 0 and 1, provided that (1) a threat is present and interacting with the target system and (2) the time bin is large compared to the response transient of the component.

As an example, consider an obscurant interacting with an optical sensor during a hardware-in-the-loop simulation. Let us assume that a receiver/data processing subsystem samples the output signal from the sensor once a second (sampling frequency = 1 Hz) and the function of the subsystem is to provide electro-optical lock-on to a target (i.e., a target acquisition capability). Due to the dynamics of the obscurant cloud, the output signal from the sensor will fluctuate up and down on a second-by-second time scale, resulting in a lock/no lock condition which also varies on a second-by-second time scale. Thus, the time-averaged target acquisition capability state (measured directly in the simulation) $\langle State \rangle_{\text{Target Acq}}$ for a time bin will be

$$\langle State \rangle_{\text{Target Acq}} = \frac{\text{Total number of positive lock-on states within the time bin}}{\text{Total number of seconds within the time bin}}. \quad (25)$$

For instance, if the length of a time bin is 60 s (1 min) and there are 45 positive occurrences of target lock-on during that time bin, then $\langle State \rangle_{\text{Target Acq}} = 0.75$ (following the positive-logic convention) or 0.25 (following the negative-logic convention).

After the discrete time axis is configured, the next step is to define the Level 1] threat events, which are assumed to occur within the mission time frame. A threat profile is thus defined as a history of Level 1] threat events as they are assigned to specific time bins within a mission time frame.* Threat profiles may be either predetermined or stochastic (i.e., a probability of threat occurrence is first assigned to each time bin, then multiple-trial Monte Carlo sampling is engaged to generate the profiles).

The final step is to actually run the discrete time analysis. The processes involved in this step are contingent on the nature of the threat profile. If a predetermined threat profile is used, the analysis process (illustrated in Figure 9) applies the given Level 1] threat events for each time bin to generate a requirement state vector. Multiple threat profiles are created by varying the sequencing of threats throughout the mission time frame. If, on the other hand, a stochastic threat profile is used, the analysis process (illustrated in Figure 10) applies Monte Carlo sampling within each time bin to determine whether or not specific Level 1] threat events occur; a requirement state vector is generated for each time bin based on Level 1] threat events. In general, the greater the number of threats addressed within a stochastic threat profile, the more simulation trials are required in order to produce meaningful statistics†. In both the predetermined and stochastic approaches, the histories of the metrics within a requirement state vector (for a single simulation run or trial) are called fitness profiles, in that, they describe the fitness or battlefield readiness of a weapon system to perform a required mission task at any point of time within a mission time frame.

* Since, in a discrete time simulation, a system can only change state by advancing into a proceeding time bin, threat events assigned to a time bin will act to change the system state at the start of the time bin (assuming threat effects are “instantaneous”). If there is a characteristic delay time between threat/target interaction and the manifestation of damage, then the delay count commences at the start of the time bin.

† Unfortunately, the number of required simulation trials can quickly approach an impractical limit as the number of time bins within a mission and number of threat events are increased. For example, if an analysis requires m time bins and n different threat events, then, assuming that a threat event can occur only once with a threat profile, the number of possible threat event sequences is equal to m^n .

Start with OMS/MP's and mission scenario(s) as supplied by TSM.

**Multiple
Pre-Determined
Multi-Threat
Profiles**

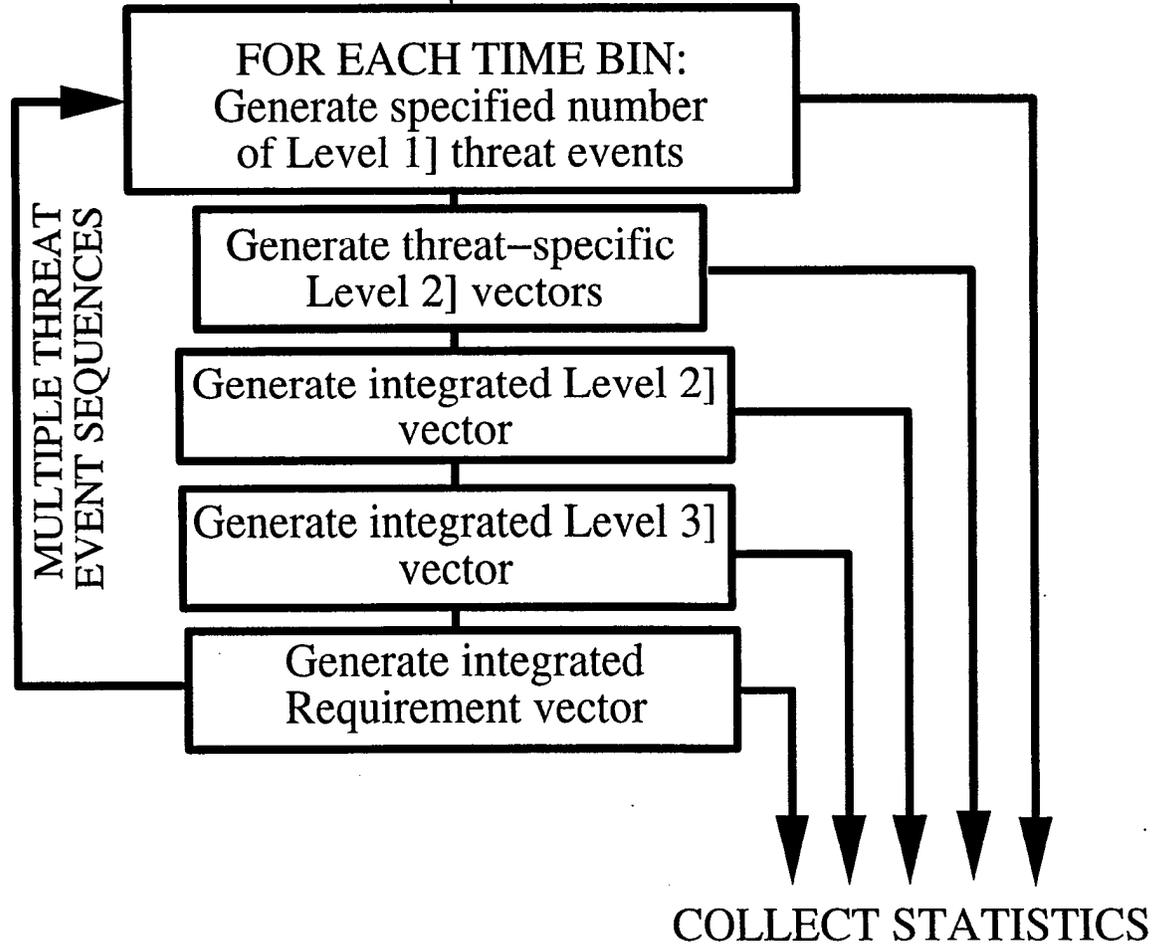


Figure 9. The Integrated Analysis Process Using Predetermined Threat Profiles.

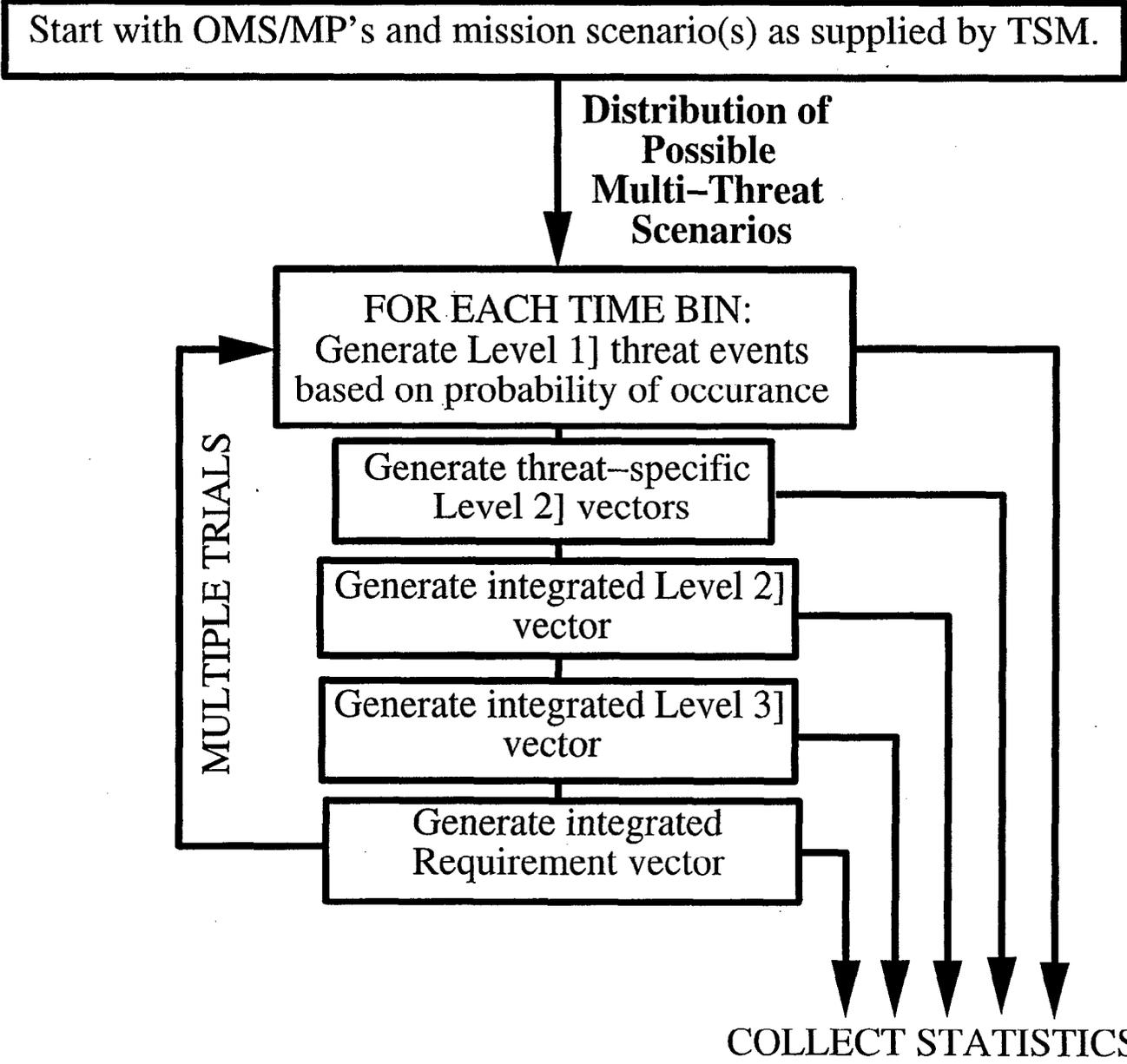


Figure 10. The Integrated Analysis Process Using a Stochastic Threat Profile.

It is worthwhile at this point to distinguish between mission and fitness profiles. A mission profile defines the execution time for all required mission tasks, as well as the number of occurrences of each task within the mission time frame. A fitness profile defines the dynamic available capability state of a military system with respect to fulfilling a specific required mission task across a mission time frame; it makes no indication as to if or when a required mission task should be executed but, rather, whether that task can be executed at all, given a command decision to do so. The only information required from a mission profile to construct relevant fitness profiles is a list of the required mission tasks and the total calendar time defining the mission time frame (for more information on mission profiles, see Appendix C).

2.7 Time Series Analysis of the Requirement Vector. Once the history of the requirement state vector has been established for all of the threat profiles in the analysis, some techniques of time series analysis may be applied to the simulation data. In this section, two data-averaging vectors are introduced to facilitate the time series analysis of the requirement vector.

The first equation represents the time-averaged fitness of a requirement metric for one specific threat profile. For a requirement vector containing n different requirement metrics,

$$\bar{R} = (R_1, R_2, R_3, \dots, R_k, \dots, R_n), \quad (26)$$

and a mission time frame discretizes into m time bins, the time-averaged requirement vector produced by one specific threat profile is

$$\langle \bar{R} \rangle = (\langle R_1 \rangle, \langle R_2 \rangle, \langle R_3 \rangle, \dots, \langle R_k \rangle, \dots, \langle R_n \rangle), \quad (27a)$$

where

$$\langle R_k \rangle = \frac{1}{m} * \sum_{t=1}^m R_k(t) \quad (27b)$$

and $R_k(t)$ is the value of the k th requirement metric at time t . The metric $\langle R_k \rangle$ is basically equal to the total amount of time within a mission time frame where a system is capable of fulfilling the k th requirement divided by the total mission time for one specific threat profile. Thus, the elements of the vector $\langle \bar{R} \rangle$ are the time fractions that a particular requirement metric is available (positive-logic convention) or unavailable (negative-logic convention) to carry out the related operational task.

The second data-averaging vector calculates the average fitness of a requirement metric across all threat profiles for one specific time bin. For the requirement vector expressed in equation (26) and a mission time frame discretized into m time bins, the average fitness profile across L different threat profiles for the k th requirement metric (see equation [26]) is

$$\bar{R}_k = (\bar{R}_k(t_1), \bar{R}_k(t_2), \bar{R}_k(t_3), \dots, \bar{R}_k(t_i), \dots, \bar{R}_k(t_m)) \quad (28a)$$

where

$$\bar{R}_k(t_i) = \frac{1}{L} * \sum_{j=1}^L [R_k(t_i)]_j, \quad (28b)$$

and $[R_k(t_i)]_j$ is the value of the k th requirement in the i th time bin for the j th threat profile. The metric $\bar{R}_k(t_i)$ is basically equal to the number of threat profiles where a system is fit to fulfill the k th requirement within the i th time bin divided by the total number of threat profiles. Thus, the average fitness profile for a particular requirement metric ($\bar{R}_{requirement}$) describes the average availability (or probability of availability for stochastic analyses) of system capabilities needed to fulfill the associated requirement across a mission time frame.

3. Implementation

The actual integrated analysis of a weapon system is conducted through the implementation (Figure 11) of the various processes described in section 2. The first step is to formulate the requirement vector for the system based on information contained in the OMS/MP and possible additional information from the U.S. Army Training and Doctrine Command (TRADOC) System Manager (TSM). Typically, the OMS/MP will contain a list of “system tasks/events” for each specific Mission Profile of concern; these “system tasks/events” are operational battlefield requirements of the weapon system and thus can be interpreted as the elements of the requirement vector. In addition, the TSM may specify certain of these “system tasks/events” as mission critical, meaning that loss of any one of them will result in mission abort.

After the requirement vector is constructed, a complete set of Level 3] capability metrics must be formulated, which then are used to build fitness trees that map these capability metrics to elements of the requirement vector. Following the approach described by Saucier (in publication), the capability state vector for the weapon system is comprised of one state from each of the subsystems contained within the main system, which for an ground combat system will include mobility, firepower, communication, target acquisition, crew, passengers, and catastrophic kill.* It is also important that the states within each subsystem be mutually exclusive and exhaustive (for more information on this concept, see Saucier, [in publication]).

The next step is to construct the fitness trees linking the Level 3] weapon system capabilities to the elements of the requirement vector. As mentioned in section 2.5, the elements of these fitness trees will generally involve the crew subsystem in conjunction with one or more other subsystems. In addition, there may also be conditional statements contained within the fitness tree, where the truth (or falsehood) of a statement determines its logical value. Finally, the construction of these fitness trees should be guided by input from an expert in the operational deployment of the weapon system, such as the TSM.

* Catastrophic kill can be interpreted as a mission-abort condition, since all subsystems within the weapon system will be dysfunctional when catastrophic kill = 1 (negative-logic convention).

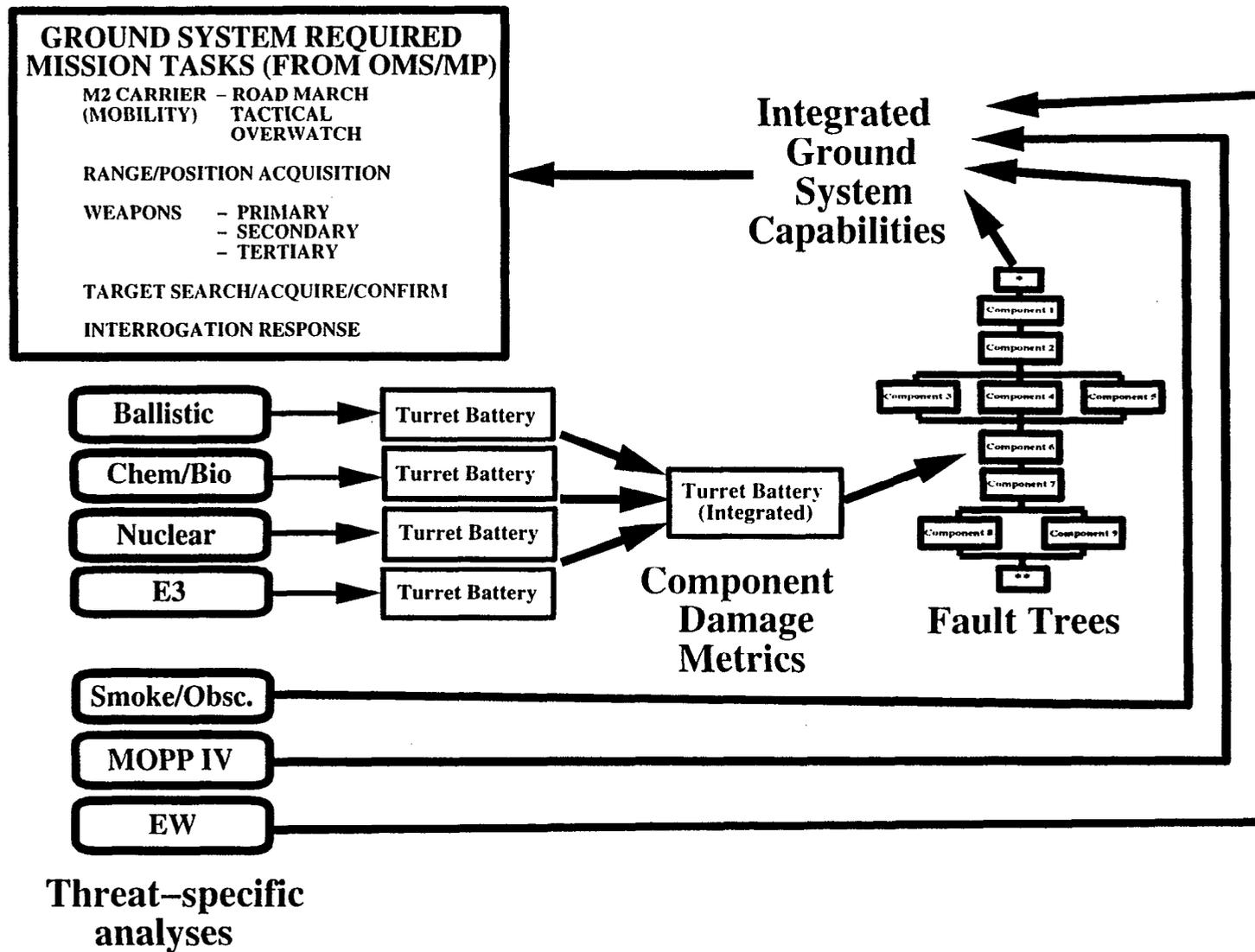


Figure 11. Implementation of the Integrated Analysis Process.

After the mission fitness mapping is constructed (as described in the preceding paragraphs), a complete set of Level 2] component damage metrics must be established and fault trees constructed to map these component damage metrics to the appropriate Level 3] capability states. If the Level 3] metrics are formulated so that they are mutually exclusive and exhaustive, then each Level 2] component damage metric is mapped to one and only one Level 3] state. Identification of the critical components in the weapon system and the fault trees built from the correlated component damage metrics should be guided by an expert in the functional design of the system.

Once the elements of the integrated analysis structure have been set up (Figure 11), there are several last steps that must be carried out before starting the analysis.

- A determination must be made as to which threats to be considered within the analysis produce Level 2] metrics and which produce Level 3] metrics when interacting with the target system (see section 2.3).
- The discrete time analysis structure must be implemented by setting up time bins within each mission profile to be addressed (see section 2.6).
- The analyst must determine the nature of the integrated analysis (deterministic or stochastic), then assemble the relevant threat profile(s) (see section 2.6).

After carrying out these last requirements, the analyst should be prepared to execute the integrated analysis.

4. Example Applications

4.1 A Simple System With Four Capability Metrics. In the first example, a simple system described by the four-element capability state vector in equation (18) is considered, with particular focus on the battlefield mobility requirement as described in equation (20a). This requirement is derived by the application of the mobility hardware capability in conjunction with

a crew member to function as a driver, and may thus be determined by combining the fault trees for the mobility and crew capabilities into one fitness tree representing the battlefield mobility requirement. This effectively combines the $O_{2,3}$ and mission fitness mappings into one process. Figure 12 illustrates the structure of this combined fault/fitness tree and the initial component functional states at the start of a simulated mission time frame (time = 0). The top and middle portions of the tree define the mobility hardware platform, with redundancy in the braking and fuel-supply components; the bottom of the tree defines the required driver capability. It is assumed in this example that each crew member is trained to perform one specific function (commander, gunner, or driver), so that only one crew member may function as the driver of the combat system. Finally, to the right is a block indicating the logical output of the tree, which is the state of the mobile transport requirement. In this example, the positive-logic convention is followed, so that all initial component functional states are equal to 1.

Next, time is assumed to evolve forward and the state of the mobile transport requirement is evaluated after 30 min of mission time have passed (time = 30 min). Figure 13 illustrates the component and MOPP states within the combined fault/fitness tree at this point in time. Two different threats are assumed to have occurred or are occurring during this 30-min period of time. First, a ballistic threat has penetrated the driver's compartment within the ground combat system and subsequently destroyed the hand brake, so that component is now permanently dysfunctional (hand brake = 0). However, the braking function is still maintained due to redundancy in the foot brake. The second threat is assumed to be a high-power microwave (HPM) signal that is applied to the ground combat system for an extended (but finite) period of time; the time = 30 min sampling point (Figure 13) falls within the HPM signal time window. It is further assumed that the HPM signal can couple into the engine compartment of the ground combat system and temporarily disrupt the function of the fuel computer within the transmission subsystem. However, the actual response of the fuel computer to the HPM signal is unknown (due to lack of test data), but threat conditions exist so that a transient current can couple into the computer and possibly disrupt component function, so that transmission = u. The net result of these threat-induced processes is a possible loss of the requirement (mobile transport = u).

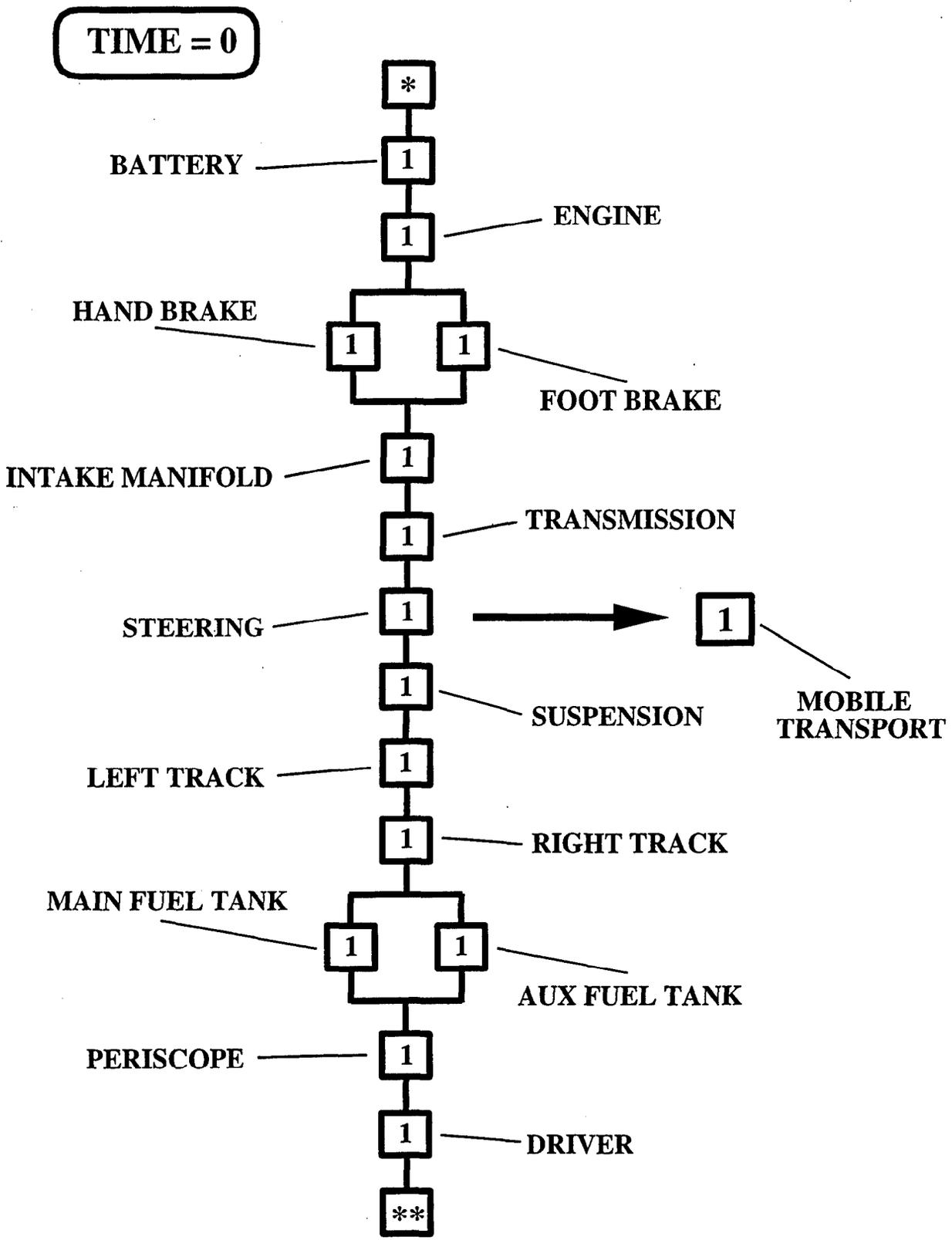


Figure 12. Initial Component Functional States Within the Combined Fault/Fitness Tree for a Simple System With Four Capability Metrics.

TIME = 30 min

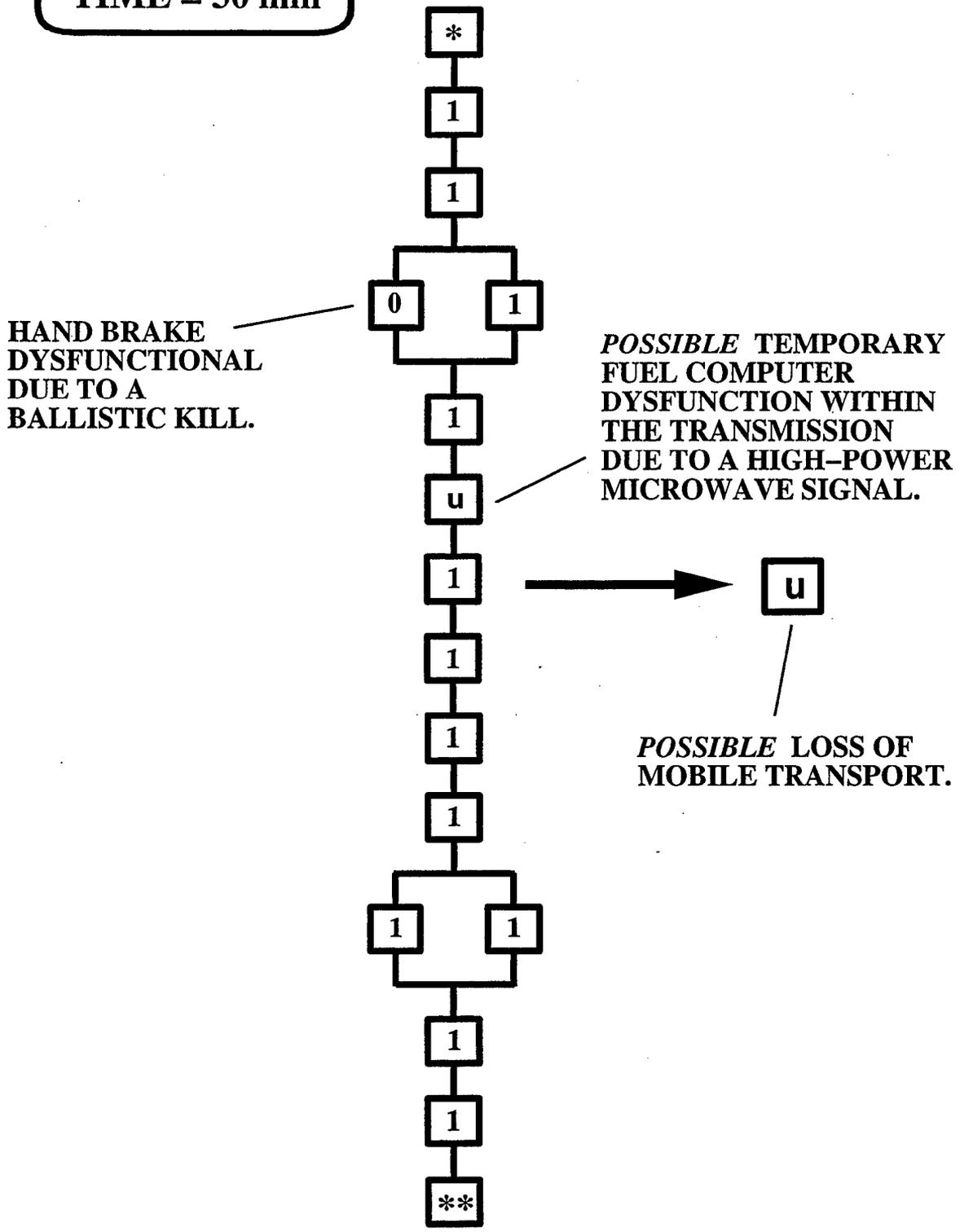


Figure 13. Component Functional States Within the Combined Fault/Fitness Tree From Figure 12 After 60 min of Mission Time Have Elapsed.

The third and final point of time where the system state is sampled is 60 min into the mission (time = 60 min), as illustrated in Figure 14. To start with, it is important to note that the HPM threat has now terminated and the transmission thus reverts back to full functionality.* There is, however, one new threat event that has occurred since the last sample time: a ballistic threat has penetrated the crew compartment of the ground combat system and severely wounded the driver, rendering him incapacitated. Then, the final state of the mobile transport requirement (mobile transport = 0) indicates that there is insufficient available system capability to execute the mobile transport task.

The main point of this first example is to illustrate the manner in which component functional states can change over time due to the ground combat system's local threat environment and thus change the fitness (or battlefield readiness) state of the mobile transport requirement. It is clearly shown in this example that the ability of the system to execute the required mission task changes as a function of component damage states, which themselves are functions of the threat profile. In a more realistic integrated analysis, (1) there are considerably more than four degraded-state (DS) metrics in the Level 3] capability state vector, (2) more sampling times to assess the system state are required, and (3) threat profiles consisting of multiple sequencing combinations of threat events (or multiple trials involving Monte Carlo sampling of threat-event occurrence probabilities per time bin for stochastic analysis) are also required. These issues are addressed in the next example.

4.2 Ground Combat System for Troop Transport.

4.2.1 Binary-State Analysis. In the second example, a generic ground combat system for transportation of troops within the battlefield is considered, where all functional metrics are limited to the binary states {0, 1}. As described by Saucier (in publication), the ground combat system can be represented in an operational sense as a set of seven on-board subsystems. These subsystems are identified as:

* If the HPM threat were strong enough to possibly burn out the fuel computer, assumed in the next example, then the transmission would remain in the undetermined functional state u for the remainder of the mission.

TIME = 60 min

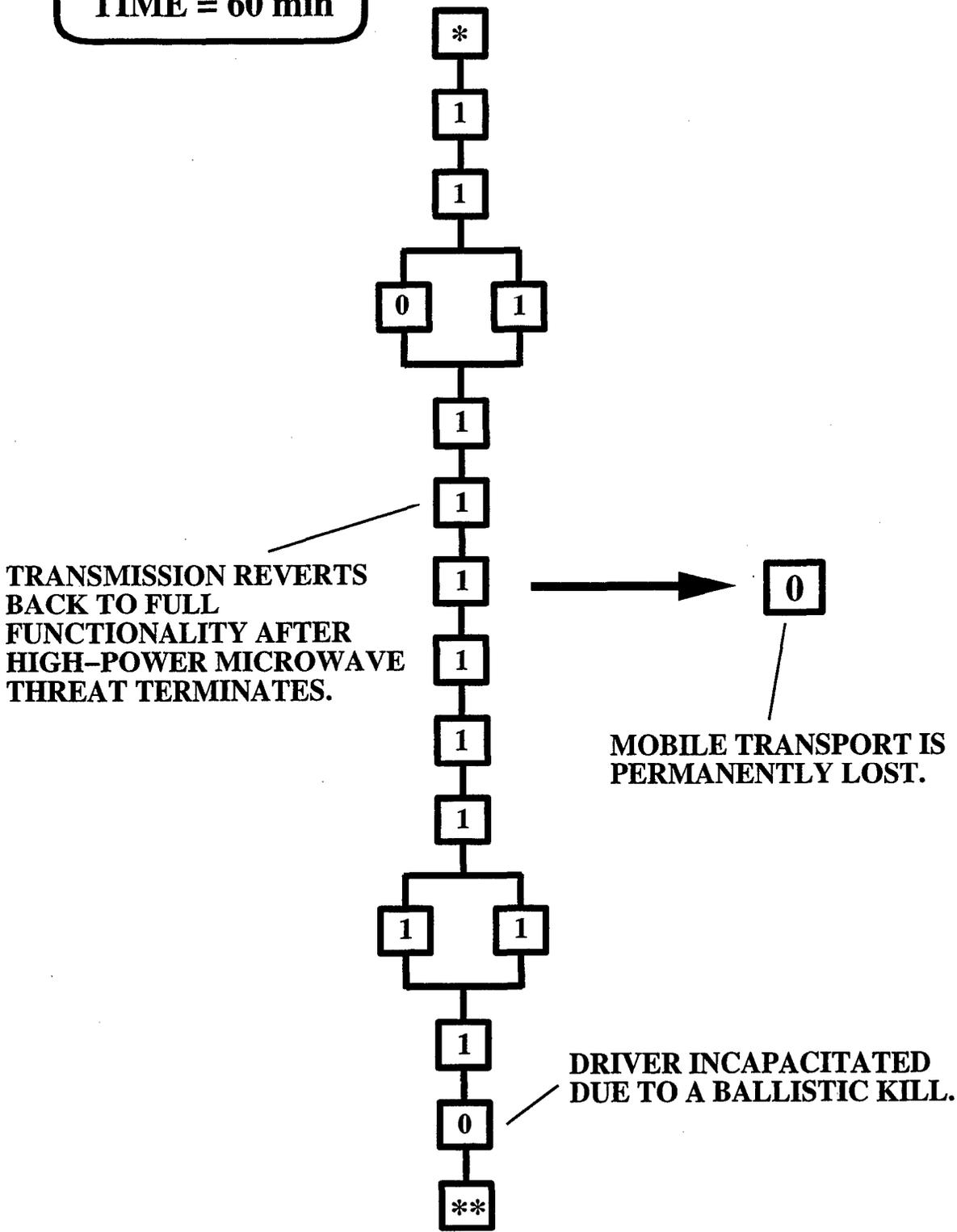


Figure 14. Component Functional States Within the Combined Fault/Fitness Tree From Figure 12 After 60 min of Mission Time Have Elapsed.

- M = mobility,
- F = firepower,
- A = acquisition,
- X = communication,
- C = crew,
- P = passengers, and
- K = catastrophic.

Each of these subsystems is represented by a specific Level 3] capability metric. Following the Degraded-States Vulnerability Methodology (DSVM) (Roach 1993; 1996), each subsystem in the aforementioned set may be in one and only one state at a point in time; these subsystem states are enumerated in Table 1. Each of these subsystem states is evaluated through a fault tree. Finally, the subsystem states are mutually exclusive and exhaustive; for the generic ground combat system described by the subsystem states in Table 1, there are $7 * 21 * 4 * 6 * 4 * 3 * 2 = 84,672$ distinct DS vectors (where a generic DS vector is of the form $[M_m, F_f, A_a, X_x, C_c, P_p, K_k]$, and $m = 0, 1, 2, 3, 4, 5, 6$; $f = 0, 1, 2, 3, \dots, 20$; $a = 0, 1, 2, 3$; $x = 0, 1, 2, 3, 4, 5$; $c = 0, 1, 2, 3$; $p = 0, 1, 2$; and $k = 0, 1$).

Following the methodology described in section 2, each of the ground combat system's DS vectors can be mapped into a distinct requirement vector. Suppose that the requirement vector \bar{R} , as shown in Figure 15, describes the 12 different requirements or operations that the ground combat system can perform in the battlefield. Note that these requirements are basically logical combinations of the different hardware subsystem capabilities with one or more crew members (as in the simple example presented in sections 2.5 and 4.1). Then a process can be designed to map a DS vector into a unique requirement vector:

Table 1. Degraded Subsystem States for a Generic Ground Combat System (Based on Information From Comstock [1991] and Saucier [in publication])

Mobility Subsystem (7 States)		Target Acquisition Subsystem (4 States)	
M ₀	Full Mobility (No Damage)	A ₀	Full Acquisition (No Damage)
M ₁	Maximum Speed Reduced to 80% of Full Mobility	A ₁	Reduced Acquisition Capability
M ₂	Maximum Speed Reduced to 30% of Full Mobility	A ₂	Loss of Acquire on the Move
M ₃	Stop After Time <i>t</i>	A ₃	A ₁ and A ₂
M ₄	Total Immobilization	Communication Subsystem (6 States)	
M ₅	M ₁ & M ₃	X ₀	Full Communication (No Damage)
M ₆	M ₂ & M ₃	X ₁	No External Communication >500 ft
Firepower Subsystem (21 States)		X ₂	No External Communication ≤500 ft
F ₀	Full Firepower (No Damage)	X ₃	No Internal Communication
F ₁	Loss of Main Armament	X ₄	X ₁ and X ₃
F ₂	Unable to Fire on the Move	X ₅	X ₂ and X ₃
F ₃	Increased Time to Fire (Reducing Firing Frequency)	Crew Subsystem (4 States)	
F ₄	Reduced Delivery Accuracy	C ₀	All Crew Functional
F ₅	Loss of Secondary Armament	C ₁	One Crew Member Incapacitated
F ₆	Loss of Tertiary Armament	C ₂	Two Crew Members Incapacitated
F ₇	F ₁ and F ₅	C ₃	Three Crew Members Incapacitated
F ₈	F ₁ and F ₆	Passengers' Subsystem (3 States)	
F ₉	F ₂ and F ₃	P ₀	All Passengers Functional
F ₁₀	F ₂ and F ₄	P ₁	One Passenger Incapacitated
F ₁₁	F ₂ and F ₆	P ₂	Two Passengers Incapacitated
F ₁₂	F ₃ and F ₄	State of Catastrophic Loss (2 States)	
F ₁₃	F ₃ and F ₆	K ₀	No K-Kill
F ₁₄	F ₄ and F ₆	K ₁	K-Kill
F ₁₅	F ₅ and F ₆		
F ₁₆	F ₁ and F ₅ and F ₆		
F ₁₇	F ₂ and F ₃ and F ₄		
F ₁₈	F ₂ and F ₃ and F ₆		
F ₁₉	F ₂ and F ₄ and F ₆		
F ₂₀	F ₂ and F ₃ and F ₄ and F ₆		

$\vec{R} =$

$R_1 =$ Mobile Protected Transport of Infantry –
Road March

$R_2 =$ Mobile Protected Transport of Infantry –
Tactical

$R_3 =$ Mobile Protected Transport of Infantry –
Overwatch

$R_4 =$ Primary Firepower

$R_5 =$ Secondary Firepower

$R_6 =$ Tertiary Firepower

$R_7 =$ Range Acquisition

$R_8 =$ Position Acquisition

$R_9 =$ Search for Target

$R_{10} =$ Target Acquisition

$R_{11} =$ Target Confirmation

$R_{12} =$ Interrogation Response

Figure 15. The Requirement Vector for the Ground Combat System Example.

$$\begin{bmatrix} M_m \\ F_f \\ A_a \\ X_x \\ C_c \\ P_p \\ K_k \end{bmatrix} \Rightarrow \begin{bmatrix} R_1 \\ R_2 \\ R_3 \\ R_4 \\ R_5 \\ \cdot \\ \cdot \\ \cdot \\ R_{12} \end{bmatrix} . \quad (29)$$

Each of the requirement metrics in the right-hand-side vector of equation (29) is based on the combined state of the crew subsystem and one other subsystem within the ground combat system. The requirement state vector for the ground combat system, shown in Figure 15, is assumed to be derived from the operational requirements for the ground combat system as specified in the weapon system's OMS/MP. Each of the 12 elements in the vector can be constructed by logical combinations of the Level 3] DS enumerated in Table 1 together with certain conditional logic statements; both kinds of logical metrics are then combined in fitness trees to yield the elements of the requirement vector. In this example, special focus is directed on two of the battlefield mobility elements of the requirement vector, which specifically are R_1 (mobile protected transport of infantry on a road march) and R_2 (mobile protected transport of infantry in a tactical environment).

Given the seven Mobility subsystem states described in Table 1, R_1 and R_2 can be evaluated by the fitness trees shown in Figures 16(a) and (b), respectively. These are constructed of both Level 3] capability metrics and a conditional logic metric; the fault trees representing these Level 3] metrics are shown in Figures 17–21. In both the fault and fitness trees, the negative-logic convention is followed; however, the outputs of the fitness trees (requirement metrics) are converted into positive-logic metrics through the binary inversion operator, which is symbolically represented at the bottom of the fitness trees in Figures 16(a) and (b). In essence, the fitness trees define the many ways that the mobile transport requirement can be deactivated. In this sense, the conditional logic statements within the fitness trees work the same way as capability metrics, in that they must be true (=1) in order for the fitness tree to evaluate to 1.

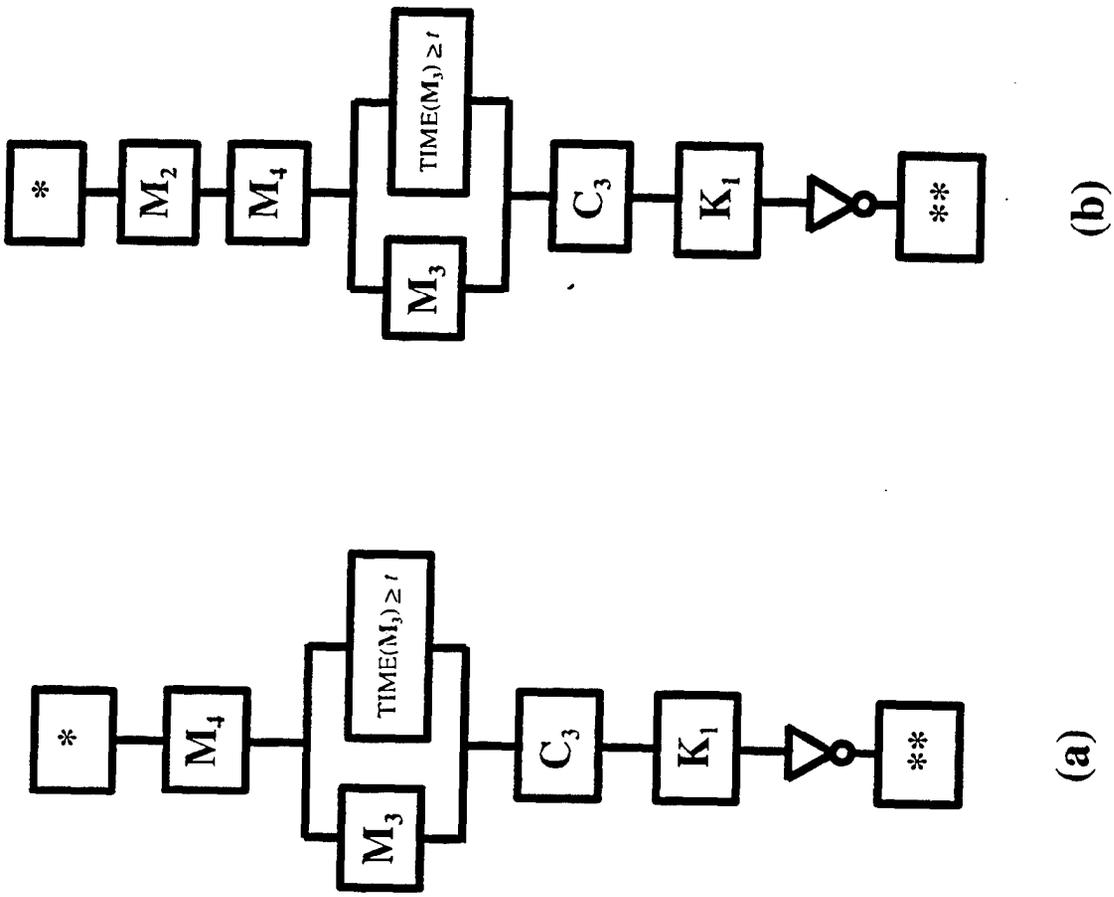


Figure 16. Fitness Tress for the Requirements (a) R_1 and (b) R_2 .

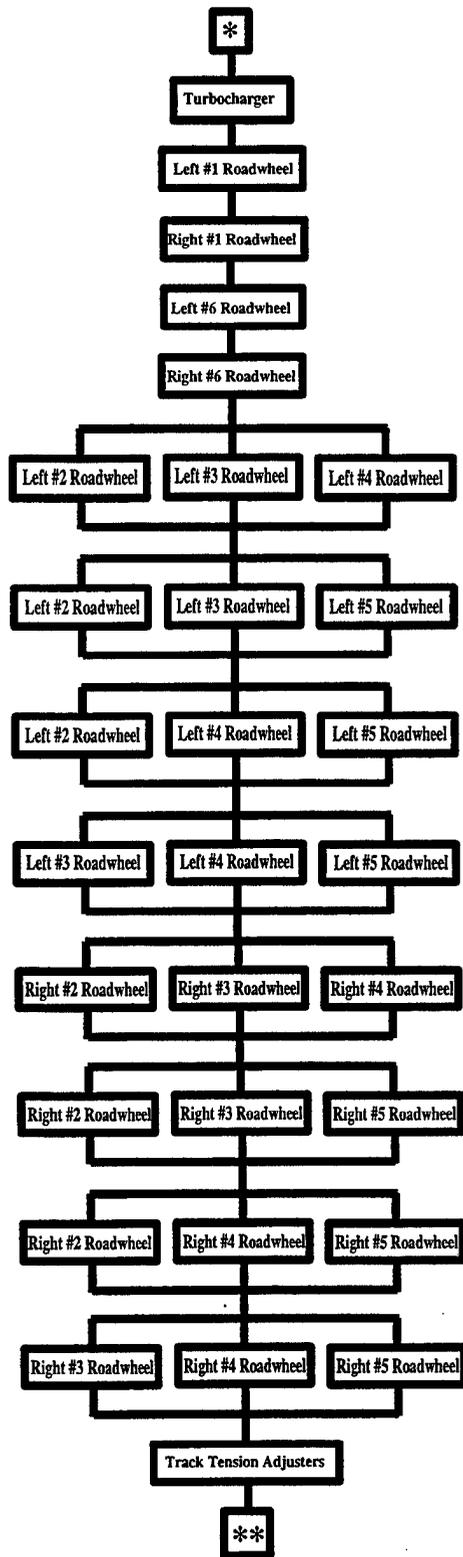


Figure 17. Fault Tree for the Mobility Subsystem DS M_2 : Maximum Speed Reduced to 30% of Full Mobility (Adapted From Comstock [1991] and Kinsler [1989]).

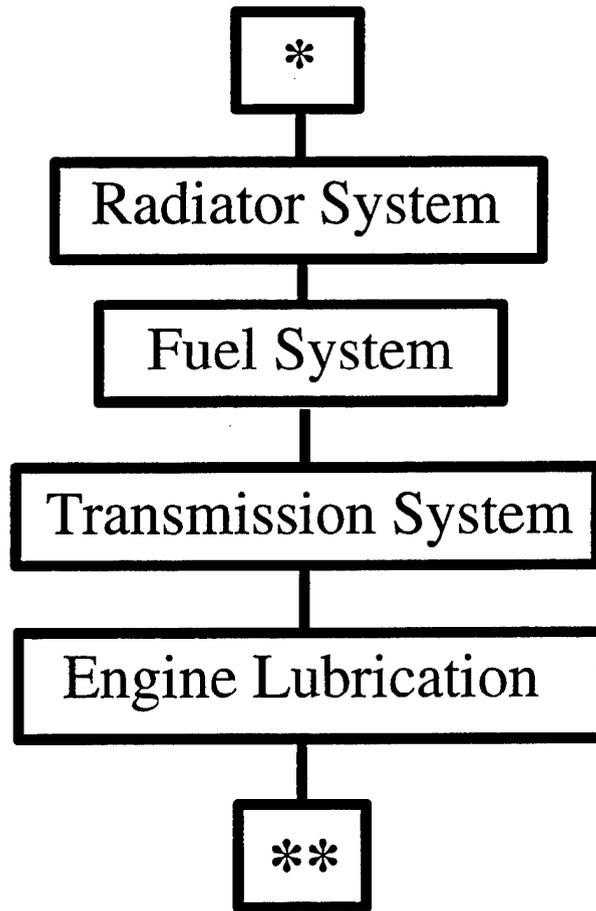


Figure 18. Fault Tree for the Mobility Subsystem DS M_3 : Stop After Time t (From Kinsler [1989]).

For the purposes of this example, any level of functionality (other than total dysfunction) within the mobility subsystem is deemed acceptable to fulfill the mobile protected transport requirement (i.e., $R_1 = 1$ and $R_2 = 1$). This point is illustrated in Figure 22, which indicates the range in capability degradation for which the level of the mobile protected transport requirement is equal to 1. In Figure 22, the plot shows the increasing level of available mobility subsystem capability along the horizontal axis and the corresponding ability of the ground system to fulfill the requirements R_1 and R_2 along the vertical axis. Thus, the requirements may be fulfilled as long as the available capability is at least equal to the minimum threshold level as indicated in Figure 22.

It is important that the reader understand the difference between the two fitness trees shown in Figures 16(a) and (b). The fitness tree for the requirement metric R_1 (Figure 16[a]) represents the logical statement

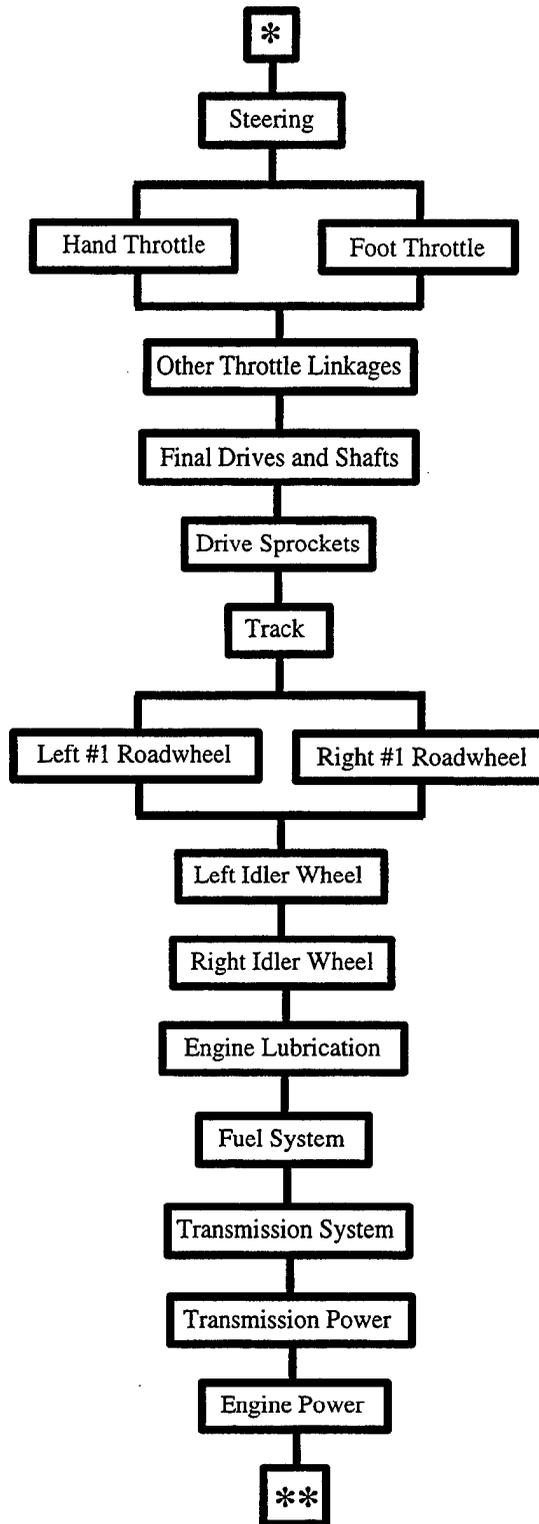


Figure 19. Fault Tree for the Mobility Subsystem DS M_4 : Total Immobilization (From Kinsler [1989]).

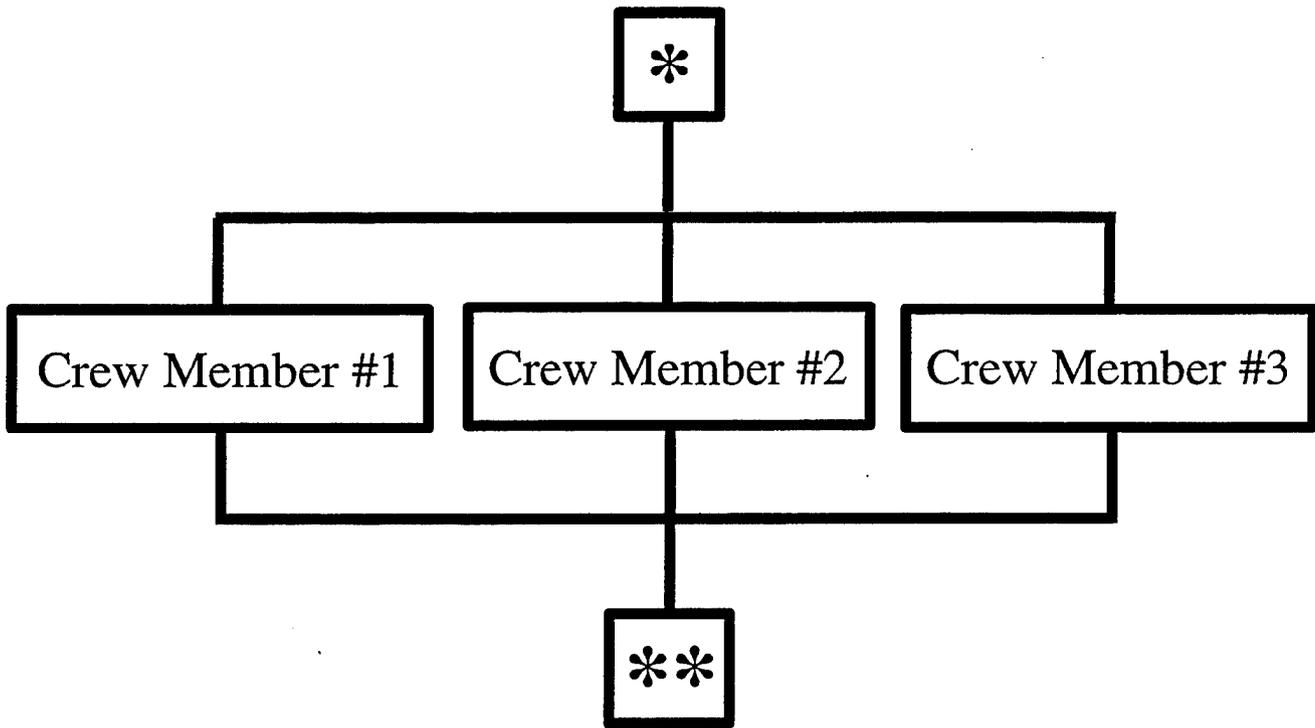


Figure 20. Fault Tree for the Crew Subsystem DS C_3 : Three Crew Members Incapacitated (From Kinsler [1989]).

$$R_1 = M_4 \mid [M_3 \ \& \ \{\text{time}(M_3) \geq t\}] \mid C_3 \mid K_1, \quad (30)$$

which, if false ($R_1 = 0$), means that at least one of the following conditions is true:

- (1) the ground system is totally immobilized (M_4);
- (2) the ground system will cease to move after an amount of time t passes (M_3) and an amount of time t (or more) has indeed passed since the system entered this state ($\text{time}(M_3) \geq t$);
- (3) all three crew members are incapacitated, leaving no one available to drive the ground system (C_3);
- (4) the entire ground system has been destroyed (and is thus totally dysfunctional) due to a catastrophic kill (K_1).

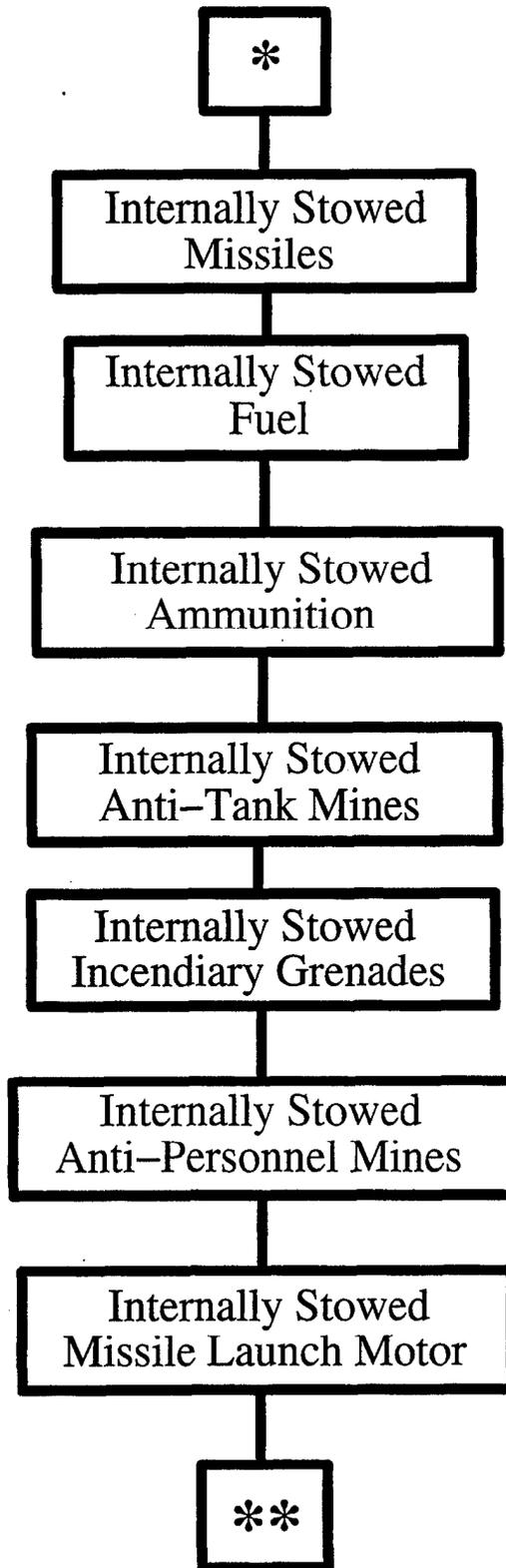


Figure 21. Fault Tree for the Catastrophic Loss DS K_1 : K-Kill (From Kinsler [1989]).

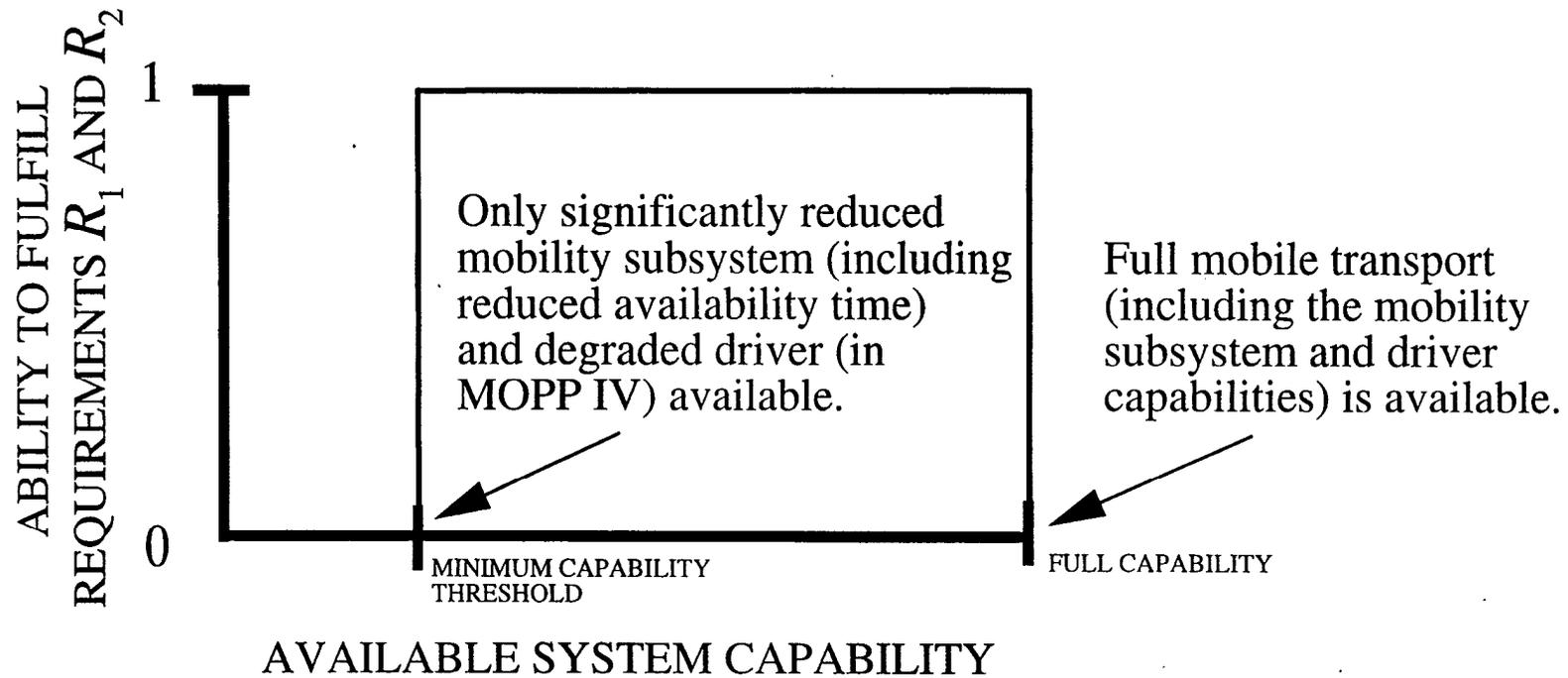


Figure 22. Plot of the Range of Available Ground System Capability for Which the Fitness of R_1 and R_2 Is Equal to 1.

Any one of these conditions is sufficient to deactivate the requirement metric R_1 . Similarly, the fitness tree for the requirement metric R_2 (Figure 16(b)) represents the logical statement

$$R_2 = \overline{M_2 \mid M_4 \mid [M_3 \ \& \ \{\text{time}(M_3) \geq t\}] \mid C_3 \mid K_1}, \quad (31)$$

which, if false, means that, in addition to the conditions described in equation (30), a fifth deactivation condition can exist where the maximum ground combat system speed is 30% of the maximum speed available from an undegraded system (M_2). This assumes that the ground system is unfit to perform the requirement R_2 , which requires it to move troops in a tactical environment, when the maximum speed is reduced by 70%. The fitness tree for R_2 is partially based upon operational judgment and must thus be constructed using input from a qualified expert in the area of ground combat system operations (such as the system TSM). Ten different threat profiles, or 10 different time-ordered sequences of Level 1] threat events, are designed as input conditions. Each of these profiles is predetermined and constructed from four different threat-specific Level 1] events/Level 2] states as follows.

- Ballistic threat event no. 1 (B1): an exploding munition blasts a hole into the ground system armor and damages the turbocharger, resulting in component dysfunction.
- Ballistic threat event no. 2 (B2): a kinetic energy (KE) penetrator punctures through the body armor and then damages the radiator system, resulting in component dysfunction.
- EM threat event (E): an HPM pulse that burns out the fuel computer embedded within the fuel system component, resulting in component dysfunction. Threat E can couple into the interior of the ground system only if ballistic threat B1 has previously occurred to rupture the EM shielding integrity of the ground system armor near the engine compartment.

- Chemical threat event (C): a chemical-agent cloud infiltrates into the ground system through the ventilation ducts and damages the rubber gaskets within the engine power component after 12 hr of exposure, resulting in component dysfunction.

These threat events are constrained to each occur once within the time frame of a 24-hr mission.

Before setting up the different threat profiles for this example, it is useful to examine how each of the aforementioned four Level 1] threat events affects the requirement metrics R_1 and R_2 . In order to do this, component damage states are first input into the relevant fault trees to produce capability metrics, which are then in turn input into the fitness trees shown in Figures 16(a) and (b). In this case, the negative-logic convention is followed. Thus, the following mappings are made for the four Level 1] threat events.

- Event B1 generates the component damage state turbocharger = 1, which is input into the fault tree shown in Figure 17; the fault-tree output is the capability state $M_2 = 1$. Then this capability state is input into the fitness trees in Figures 16(a) and (b) to produce the requirement metrics $R_1 = 1$ and $R_2 = 0$, respectively.
- Event B2 generates the component damage state radiator system = 1, which is input into the fault tree shown in Figure 18; the fault-tree output is the capability state $M_3 = 1$. Then this capability state is input into the fitness trees in Figures 16(a) and (b) to produce the requirement metrics $R_1 = 0$ and $R_2 = 0$, respectively, only after 1 hr of time has elapsed since the occurrence of event B2.
- Event E generates the component damage state fuel system = 1 (given that event B1 has previously occurred), which is input into the fault-tree shown in Figure 19; the fault-tree output is the capability state $M_4 = 1$. Then this capability state is input into the fitness trees in Figures 16(a) and (b) to produce the requirement metrics $R_1 = 0$ and $R_2 = 0$, .
- Event C generates the component damage state engine power = 1, which is input into the fault tree shown in Figure 19; the fault tree output is the capability state

$M_4 = 1$. Then this capability state is input into the fitness trees in Figures 16(a) and (b) to produce the requirement metrics $R_1 = 0$ and $R_2 = 0$, respectively.

Table 2 summarizes these threat-event-specific effects, where each of the four threat events is considered to occur separately, as well as in conjunction. The first four columns in Table 2 list whether a threat event occurs (represented by a 1) or does not occur (represented by a 0) at some arbitrary point in time; note that anywhere from 0 to 4 threat events may occur at this point. The last two columns in Table 2 represent the states of R_1 and R_2 , given that the threat events listed in that table row have occurred. For the purposes of the table, enough time is assumed to have passed so that all threat-induced degradation to system capabilities have manifested (and in turn degraded requirement levels), so that the states of R_1 and R_2 reflect the minimum possible levels of available system capability to meet a requirement, given that a set of threat events has occurred. In this case, since no interthreat synergy is assumed,* the only threat with no effect on both R_1 and R_2 is the EM threat event E, while the ballistic threat event B1 only deactivates requirement metric R_2 .

In order to simplify the dynamics within this example, each of the Level 1] threat events described above is constrained to begin at one of four different points of time, namely, 0, 6, 12, and 18 hours after the mission commences. Note that threat events B1, B2, and E may be modeled as “instantaneous” events, so that the entire event occurs at one of the above five points of time, whereas threat event C will unfold over a window of time measured from the commencement of the event. It is further assumed that any number of different threat events from 0 to 4 can occur at each of the four allowed points of time within the mission time frame (provided that the single occurrence of a threat event constraint described in the previous paragraph is observed). Table 3 describes the 10 threat profiles.

* Synergy between threat events is inherently a dynamical process, where event sequencing is critical (is explained in section 4.2.1.2).

Table 2. The Effect of the Threat Events B1, B2, E, and C on the Binary States (Following the Positive-Logic Convention) of the Requirement Metrics R_1 and R_2 (No Interthreat Synergy Is Assumed)

Level 1] Threat Event				State of Requirement Metric	
B1	B2	E	C	R_1	R_2
0	0	0	0	1	1
0	0	0	1	0	0
0	0	1	0	1	1
0	0	1	1	0	0
0	1	0	0	0	0
0	1	0	1	0	0
0	1	1	0	0	0
0	1	1	1	0	0
1	0	0	0	1	0
1	0	0	1	0	0
1	0	1	0	1	0
1	0	1	1	0	0
1	1	0	0	0	0
1	1	0	1	0	0
1	1	1	0	0	0
1	1	1	1	0	0

Table 3. Ten Different Threat Profiles for the Integrated Analysis of the Ground Combat System

Threat Profile	Mission Time (Within a 24-hr Mission)			
	$t = 0$ hr	$t = 6$ hr	$t = 12$ hr	$t = 18$ hr
1	B2, C, E	—	—	B1
2	C, E	B1	—	B2
3	B1	—	—	B2, C, E
4	C, E	—	B1	B2
5	B1	C	E	B2
6	B1	C	B2	E
7	—	B1, C	E	B2
8	E	B1	C	B2
9	B1	E	C	B2
10	—	—	C	B1, B2, E

Notes: B1 = ballistic threat event 1.
 B2 = ballistic threat event 2.
 C = chemical/biological threat event.
 E = EM threat event.

Once the threat profiles have been configured, 10 different simulations are run where the simulation inputs are specific threat profiles. This is done through the use of the discrete time V/L process structure (as described in section 2), which, for each time bin within the mission time frame, maps one or more Level 1] threat events to Level 2] component damage states, then to Level 3] capability states, and finally to requirement states. To simplify the example, the 24-hr mission time frame is discretized into hour-long time bins, making for a total of 24 time bins. Threat events (and the resultant changes in component/subsystem functional states) are constrained to occur at the transition between time bins. Thus, for example, the ballistic event B2 occurring within the second threat profile (see Table 3) would affect functional states starting with time bin no. 19 (which commences after 18 hr of mission time have elapsed). Thus, a threat event occurring at mission time = n produces a change in component/subsystem functional state starting with the $(n + 1)$ th time bin.

Within the context of this example, two cases are considered based on different modeling assumptions: (1) no synergy between threats is assumed, and (2) synergy between the ballistic threat event B1 and the EM threat event E is assumed. Both cases are examined in turn.

4.2.1.1 No Interthreat Synergy Assumption. In case (1), the assumption is made that all threats act independently to damage components and/or disrupt component/subsystem function, so that there is no resultant interthreat synergy. In this case, each threat encounters a “pristine” target description, so that the target description has no “memory” of damage/dysfunction from previous threat events. Thus, the EM threat event E has no effect on component/subsystem functionality since the signal cannot penetrate through the ground system’s armor without the coupling aperture produced by the ballistic threat event B1.

Now, given the threat profiles described in Table 3, the time histories (or fitness profiles) of the requirement metrics R_1 and R_2 are calculated. Table 4 presents the fitness profile data for R_1 , while Table 5 presents similar data for R_2 . In both profiles, the average values of R_1 and R_2 (i.e., the average fitness values) are tabulated per time bin and per threat profile. The average fitness values per time bin are displayed in the bottom rows of the tables, while the average fitness values per fitness profile are displayed in the last column on the right-hand-side of the tables.

Table 4. Fitness Profile of the Ground Combat System Requirement Metric R_1 With No Interthreat Synergy

Threat Profile No.	Mission Time (hr)																								Avg.	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24		
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.04
2	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0.50
3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0.79
4	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0.50
5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0.75
6	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0.50
7	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0.75
8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0.79
9	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0.79
10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0.79
Avg.	1	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.6	0.6	0.6	0.6	0.6	0.6	0.4	0	0	0	0	0	0	0.62

Table 5. Fitness Profile of the Ground Combat System Requirement Metric R_2 With No Interthreat Synergy

Threat Profile No.	Mission Time (hr)																								Avg.
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.25
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.00
4	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0.50
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.25
8	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.25
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0.75
Avg.	0.5	0.5	0.5	0.5	0.5	0.5	0.2	0.2	0.2	0.2	0.2	0.2	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0	0	0	0	0	0.20

Finally, the box in the lower right corners of Tables 4 and 5 presents the fitness averaged over all time bins for all threat profiles. The average fitness value for a threat profile may be calculated by the ratio

$$\frac{\text{total availability of time required system capabilities}}{\text{total mission time}};$$

in the current example, this is equal to

$$\frac{\text{total number of time bins where fitness} = 1}{24 \text{ time bins}}.$$

Figure 23 presents a plot of fitness profile no. 9 from Table 4 (based on threat profile no. 9 from Table 3; this profile illustrates how one specific threat scenario modifies the fitness state of the requirement metric R_1 . As shown in Figure 23, threat events B1, E, C, and B2 occur throughout the 24-hr mission time frame. Given this threat scenario, the ground system is capable of fulfilling the requirement R_1 up until 1 hr, following the occurrence of threat event B2 (a total of 19 mission hours). This ability to fulfill requirement R_1 is then represented as the fitness of the requirement metric R_1 .

Plots of the average fitness states of R_1 and R_2 as calculated in Tables 4 and 5 are shown in Figures 24 and 25, respectively. In both of these figures, the level of requirement metric fitness is averaged over the set of 10 fitness profiles as described in Tables 4 and 5; this averaging is carried out separately for each time bin within the mission time frame. Thus, in Figure 24, for example, the average fitness level of R_1 from hours 2 through 12 is equal to 0.9; this indicates that, for 9 of the 10 threat scenarios described by the threat profiles in Table 3, the ground system is capable of fulfilling requirement R_1 from hours 2 through 12 of the mission. The “descending staircase” look characteristic of the profiles in Figures 24 and 25 indicates that, as mission time elapses, the ground system is less likely to be able to fulfill the required mission tasks represented by R_1 and R_2 .

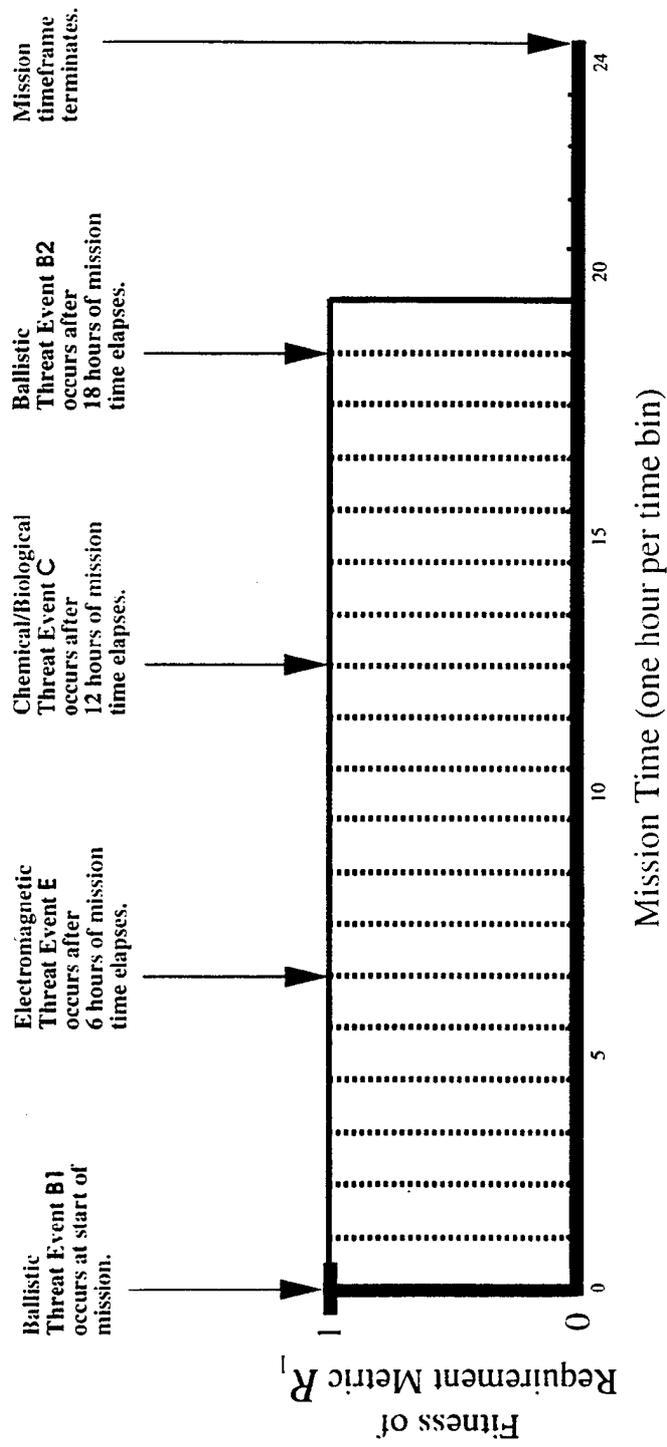


Figure 23. Plot of R_1 Fitness Profile No. 9 From Table 4 (Based on Threat Profile No. 9 From Table 3).

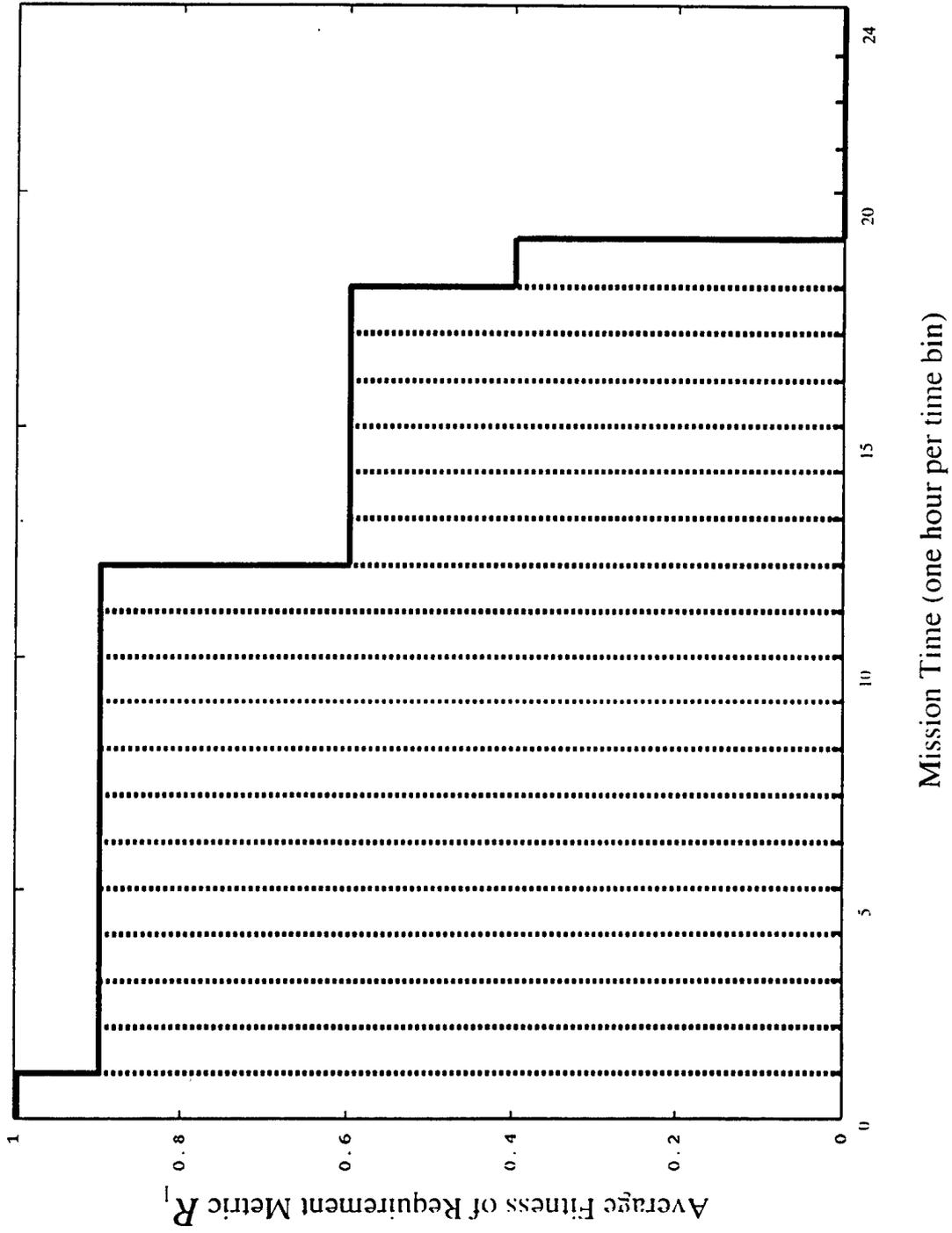


Figure 24. Average Fitness Profile for R_1 Without Interthreat Synergy.

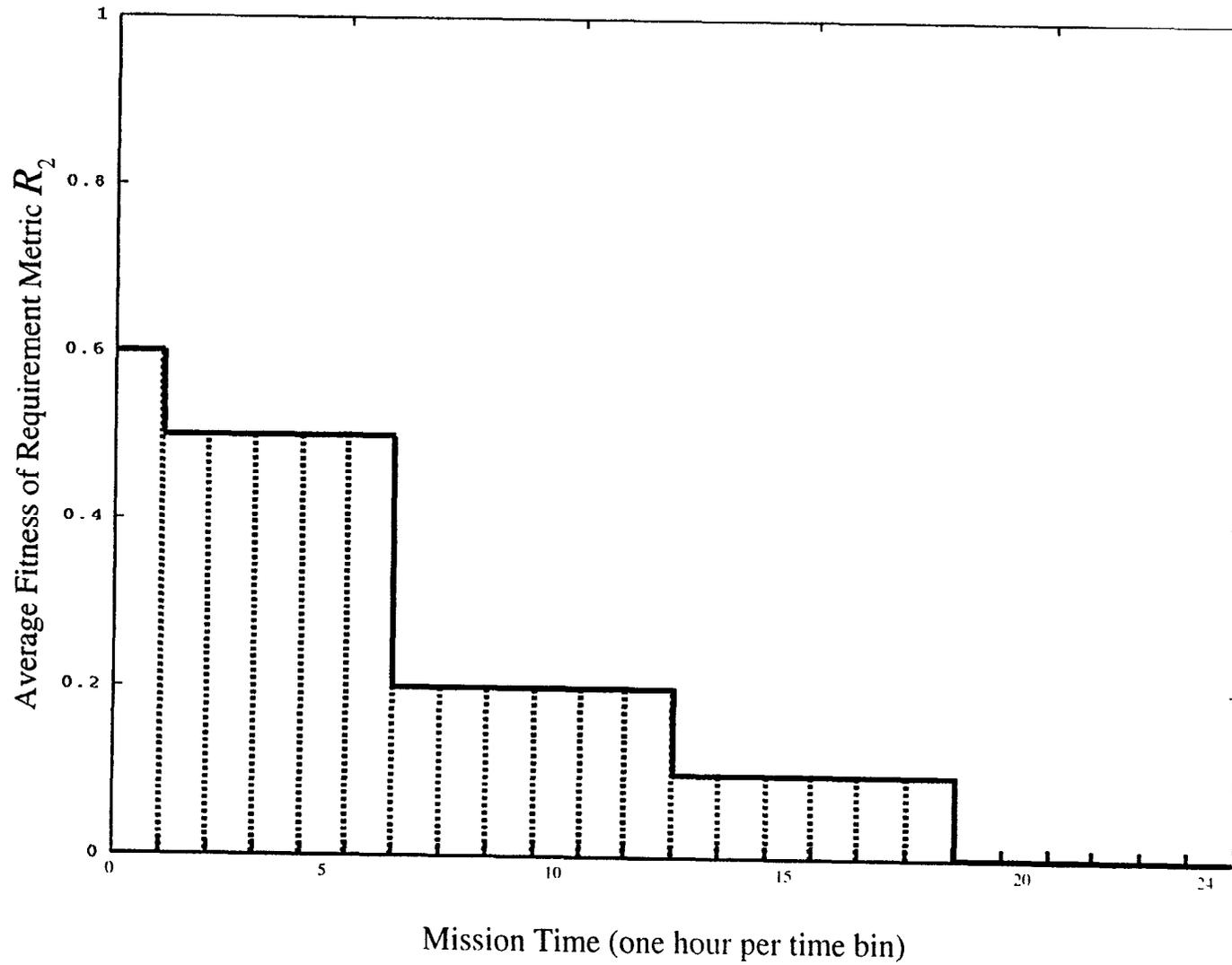


Figure 25. Average Fitness Profile for R_2 Without Interthreat Synergy.

4.2.1.2 Synergy Between B1 and E Assumption. In case (2), the assumption is made that the ballistic threat event B1 and the EM threat event E are correlated through their mutual interaction with the ground combat system. In this case, sequencing of threat events is important, so that event E will result in component damage only when preceded by event B1. As a result, all threat profiles, as shown in Table 3, where B1 follows E, will produce no damage to the fuel computer in the engine compartment, and thus no degradation to the mobility hardware subsystem. In this event, R_1 and R_2 are unaffected. Figure 26 illustrates the synergistic $O_{1,2}$ mapping involving both of the threat events B1 and E.

Again, given the threat profiles described in Table 3, the fitness profile of the requirement metric R_1 is calculated (the metric R_2 is unaffected by B1/E synergy and thus is the same as in the nonsynergy case). Table 6 presents the fitness profile data for R_1 . Figure 27 presents a plot of fitness profile no. 9 from Table 6, while a plot of the average fitness profile of R_1 as calculated in Table 6 is shown in Figure 28. By comparing the plots in Figures 24 and 28, it is seen that the addition of interthreat synergy to a specific threat profile acts to shorten the overall availability time of the system capabilities needed to fulfill the requirement R_1 .

4.2.2 Trinary-State Analysis. Next, the generic ground combat system described in section 4.2.1 is again addressed, except that functional metrics are now extended to the set of trinary states $\{0, u, 1\}$. This means that Level 2], Level 3], and requirement metrics may, in addition to the binary values 0 and 1, assume the value u , indicating an undetermined level of function. This modification requires the following revised assumptions

- EM threat event E possibly burns out the fuel computer in the engine compartment, resulting in ground combat mobility state M_4 . This assumes that test data on the fuel computer response to the HPM threat are unavailable. The effectiveness of threat E is still contingent on the previous occurrence of ballistic threat event B1.
- Chemical threat event C possibly damages the rubber gaskets within the engine power component after 12 hr of exposure, resulting in ground combat system mobility state M_4 .

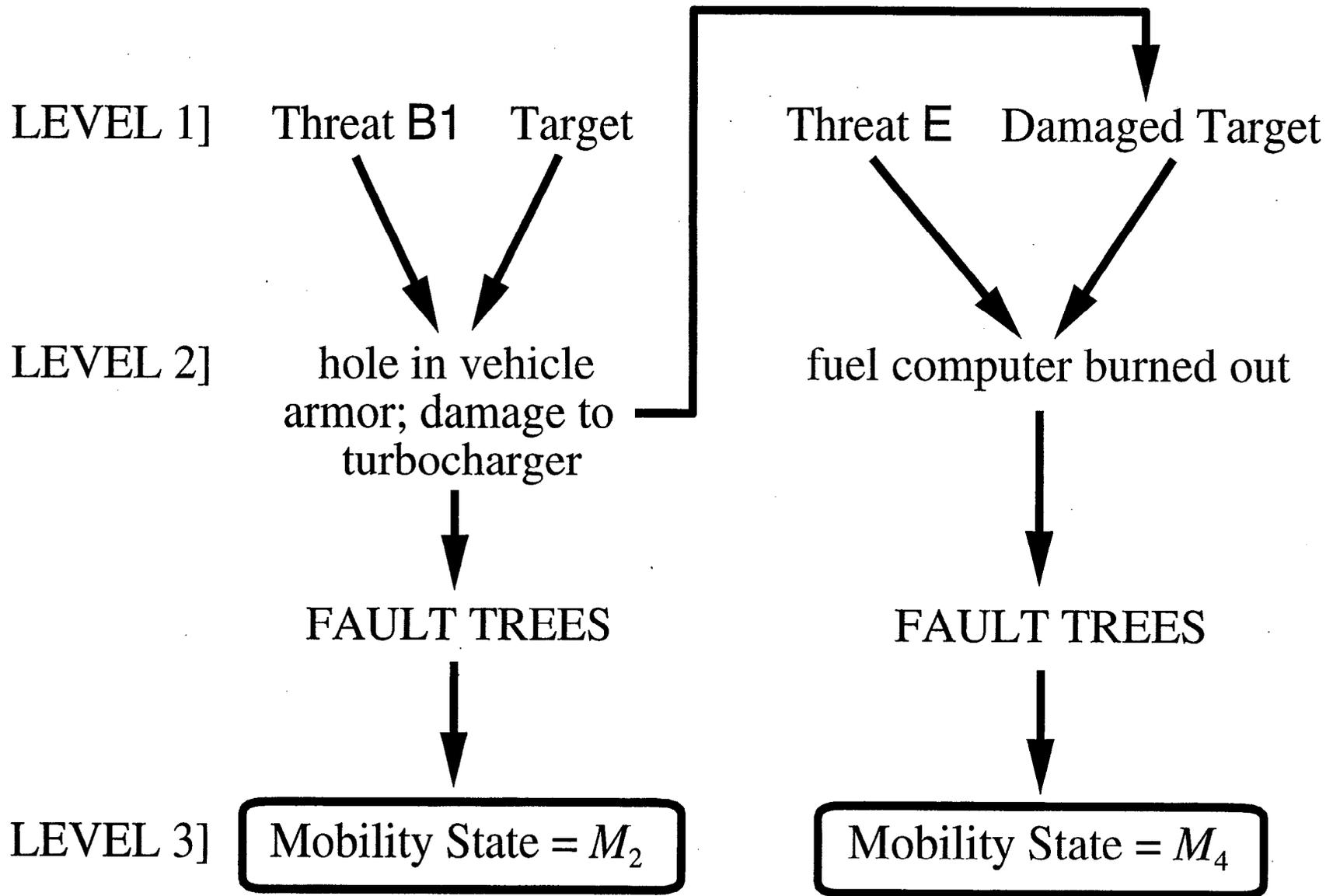


Figure 26. The Synergistic $O_{1,2}$ Mapping Involving Both of the Threat Events B1 and E.

Table 6. Fitness Profile of the Ground Combat System Requirement Metric R_1 Using a Dynamic Target That Models Synergy Between a Ballistic and an EM Threat Event

Threat Profile No.	Mission Time (hr)																								Avg.
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.04
2	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0.50
3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0.75
4	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0.50
5	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0.50
6	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0.54
7	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0.50
8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0.79
9	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.25
10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0.79
Avg.	1	0.9	0.9	0.9	0.9	0.9	0.8	0.8	0.8	0.8	0.8	0.8	0.4	0.3	0.3	0.3	0.3	0.3	0.2	0	0	0	0	0	0.52

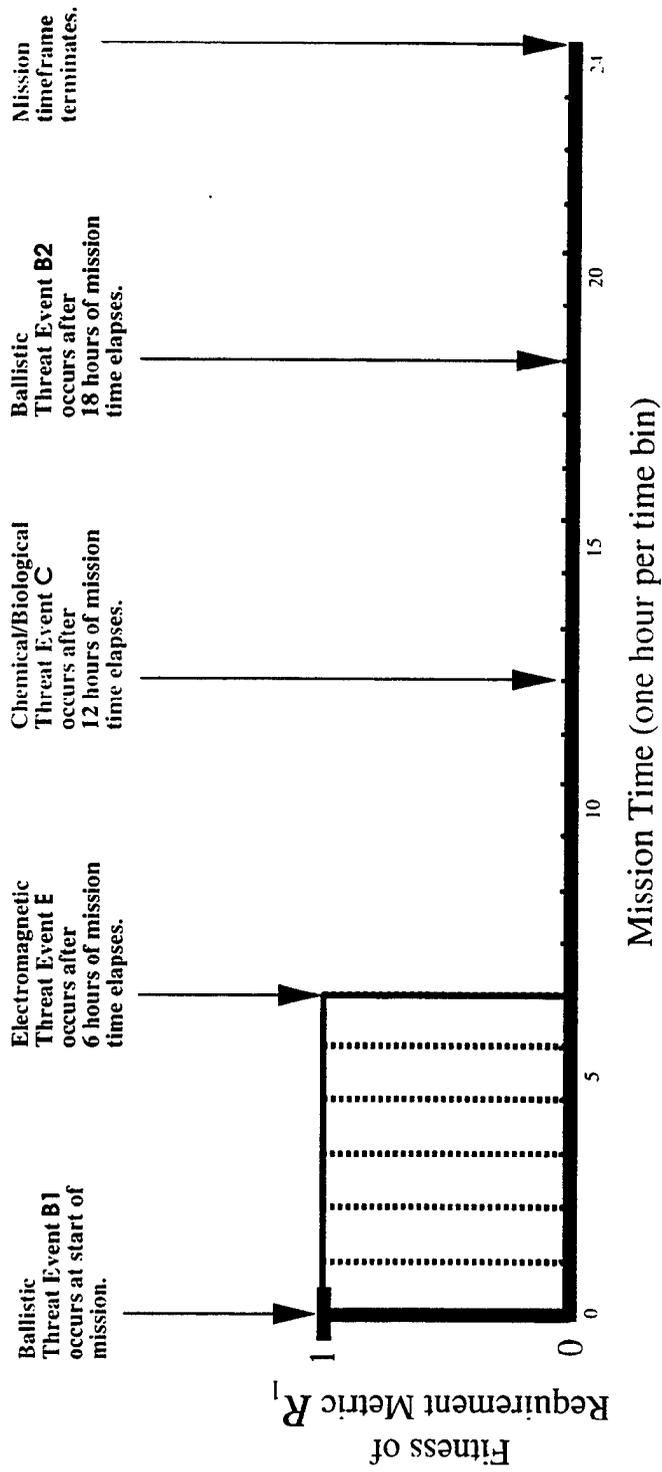


Figure 27. Plot of R_1 Fitness Profile No. 9 From Table 6.

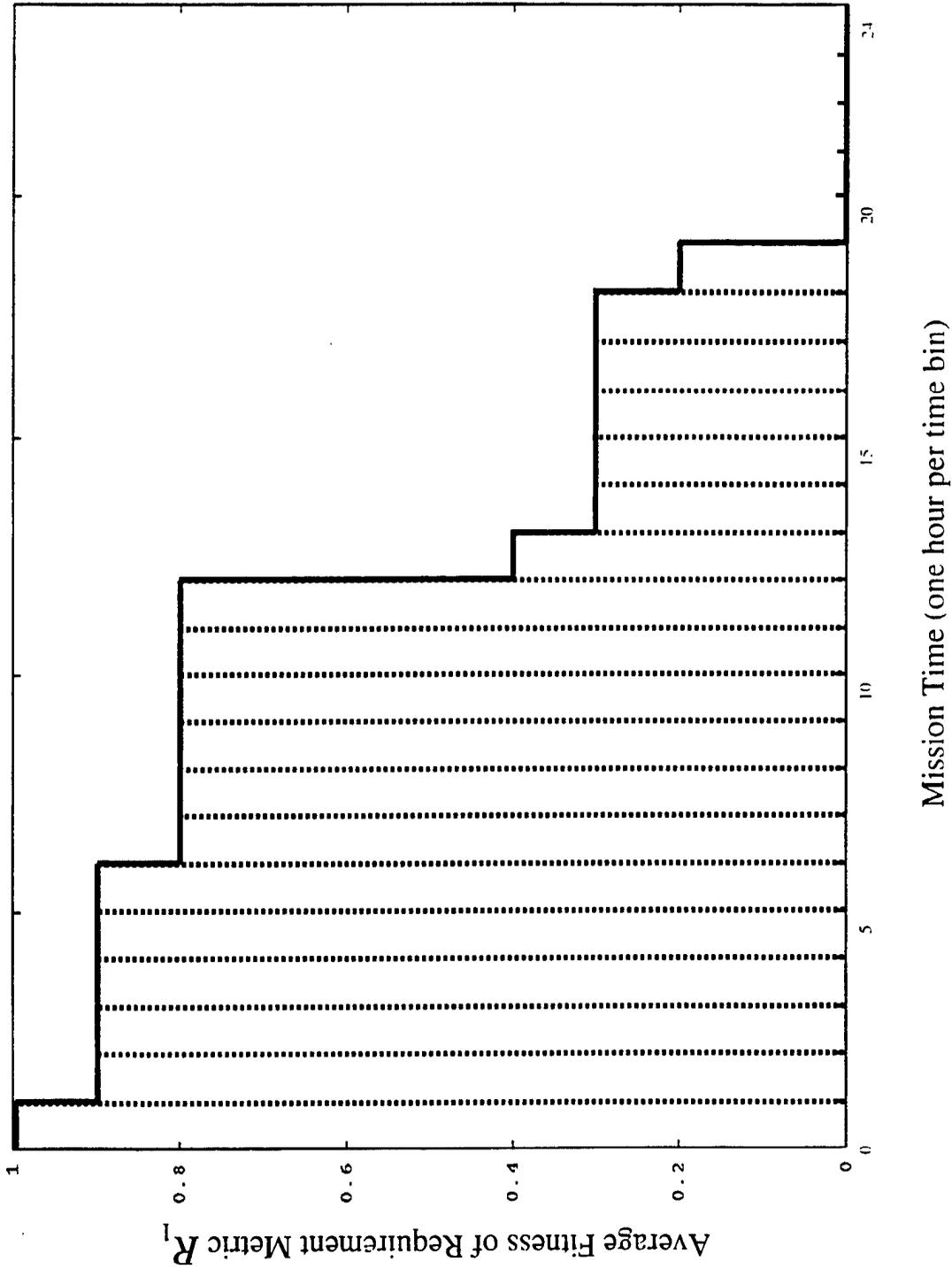


Figure 28. Average Fitness Profile for R_1 Assuming Interthreat Synergy.

This assumes that test data on the gasket response to the chemical-agent threat are unavailable.

All other assumptions are maintained from the example in section 4.2.1

As with the binary-state analysis in section 4.2.1, it is again useful to examine how each of the Level 1] threat events B1, B2, E, and C affects the requirement metrics R_1 and R_2 . As was done for the binary-state analysis in section 4.2.1, component damage states are first input into the relevant fault trees (Figures 17–21) to produce capability metrics, which are then in turn input into the fitness trees (Figures 16[a] and [b]). Again, the negative-logic convention is followed. Due to the use of trinary states, the following mappings are different from the binary state analysis.

- Event E generates the component damage state fuel system = u (given that event B1 has previously occurred), which is input into the fault tree shown in Figure 19; the fault tree output is the capability state $M_4 = u$ (which also implies that $M_0 = u$). Then this capability state is input into the fitness trees in Figures 16(a) and (b) to produce the requirement metrics $R_1 = u$ and $R_2 = u$, respectively.
- Event C generates the component damage state engine power = u, which is input into the fault tree shown in Figure 19; the fault tree output is the capability state $M_4 = u$ (also implying $M_0 = u$). Then this capability state is input into the fitness trees in Figures 16(a) and (b) to produce the requirement metrics $R_1 = u$ and $R_2 = u$, respectively.

As with the previous example, two cases are again considered based on different modeling assumptions: (1) no synergy between threats is assumed and (2) synergy between the ballistic threat event B1 and the EM threat event E is assumed. Given the threat profiles described in Table 3, the fitness profiles of the requirement metric R_1 are calculated for both of the aforementioned cases. The requirement metric R_2 is not re-evaluated here since it is not a function of any undetermined component functional states, and thus remains unchanged from its previously calculated values in section 4.2.1.

Table 7 presents the fitness profile data for R_1 with no interthreat synergy. Table 8 presents the fitness profile data for R_1 with synergy between the threat events B1 and E. In both tables, the bottom row presents the average fitness per time bin, while the right-most column presents the fitness averaged over all time bins for each of the 10 threat profiles. The box in the bottom right corner presents the fitness averaged over all time bins for all threat profiles. In all cases, the averaged metrics are calculated for values of 1, u, and 0. For example, the value set $AVG(1) = 0.6$, $AVG(u) = 0.2$, $AVG(0) = 0.2$ (as read from the bottom row under time bin no. 18 in Table 7) indicates that, within the eighteenth time bin, the ground system is fit to fulfill R_1 in six of the threat scenarios, undetermined in two of the threat scenarios, and unfit in the remaining two threat scenarios. Figures 29 and 30 depict plots of the average fitness profile data as recorded in Tables 7 and 8, respectively.

Finally, Figure 31 presents a plot of fitness profile no. 9 from Table 8. By comparing Figure 31 with similar plots in Figures 23 and 27, it is seen that the latter two plots define the maximum and minimum possible values of R_1 , respectively, which bound the “uncertain” region shown in Figure 31.

4.2.3 Binary State Analysis Results. In order to understand the relevance of the discrete time integrated analysis of the ground combat system using binary states, the reader is again directed to the data in Tables 4, 5, and 6. In each of these tables, the values of the time-averaged requirement metric (as described in section 2.7), which is calculated across all time bins within the mission time frame for each threat profile, are listed in the right-most column. By studying these time-averaged requirement metrics, the following trends can be observed.

- Most of the values in Table 4 range from 0.50 to 0.79 (with one exception equal to 0.04), meaning that the ground combat system is capable of fulfilling requirement R_1 from 50% to 79% of the time through the entire mission. The average amount of time where R_1 can be fulfilled is equal to 62% of the entire mission length. Put another way, the time-averaged mission fitness of R_1 for all threat profiles is equal to 0.62.

Table 7. Fitness Profile of the Ground Combat System Requirement Metric R_1 Using Trinary-Logic States and No Interthreat Synergy

Threat Profile No.	Mission Time (hr)																								Avg.			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	1	u	0	
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.04	0	0.96
2	1	1	1	1	1	1	1	1	1	1	1	1	u	u	u	u	u	u	u	0	0	0	0	0	0	0.50	0.25	0.21
3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0.79	0	0.21
4	1	1	1	1	1	1	1	1	1	1	1	1	u	u	u	u	u	u	u	0	0	0	0	0	0	0.50	0.29	0.21
5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	u	0	0	0	0	0	0	0.75	0.04	0.21
6	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0.54	0	0.46
7	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	u	0	0	0	0	0	0	0.75	0.04	0.21
8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0.79	0	0.21
9	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0.79	0	0.21
10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0.79	0	0.21
Avg.	1	1	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.9	0.7	0.6	0.6	0.6	0.6	0.6	0.4	0	0	0	0	0	0.62	—	—
	u	0	0	0	0	0	0	0	0	0	0	0	0	0.2	0.2	0.2	0.2	0.2	0.2	0.4	0	0	0	0	0	—	0.07	—
	0	0	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.2	0.2	0.2	0.2	0.2	0.2	1.0	1.0	1.0	1.0	1.0	—	—	0.34

Table 8. Fitness Profile of the Ground Combat System Requirement Metric R_1 Using Trinary-Logic States and a Dynamic Target That Models Synergy Between a Ballistic and an EM Threat Event

Threat Profile No.	Mission Time (hr)																								Avg.		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	l	u	
	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.04	0
2	1	1	1	1	1	1	1	1	1	1	1	1	u	u	u	u	u	u	u	0	0	0	0	0	0.50	0.29	0.21
3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	u	0	0	0	0	0	0.75	0.04	0.21
4	1	1	1	1	1	1	1	1	1	1	1	1	u	u	u	u	u	u	u	0	0	0	0	0	0.50	0.29	0.21
5	1	1	1	1	1	1	1	1	1	1	1	1	u	u	u	u	u	u	u	0	0	0	0	0	0.50	0.29	0.21
6	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0.54	0	0.46
7	1	1	1	1	1	1	1	1	1	1	1	1	u	u	u	u	u	u	u	0	0	0	0	0	0.50	0.29	0.21
8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0.79	0	0.21
9	1	1	1	1	1	1	u	u	u	u	u	u	u	u	u	u	u	u	u	0	0	0	0	0	0.25	0.54	0.21
10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0.79	0	0.21
Avg.	1	0.9	0.9	0.9	0.9	0.9	0.8	0.8	0.8	0.8	0.8	0.8	0.4	0.3	0.3	0.3	0.3	0.3	0.2	0	0	0	0	0	0.52	—	—
	u	0	0	0	0	0	0.1	0.1	0.1	0.1	0.1	0.1	0.5	0.5	0.5	0.5	0.5	0.5	0.6	0	0	0	0	—	0.17	—	
	0	0	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.2	0.2	0.2	0.2	0.2	0.2	1.0	1.0	1.0	1.0	1.0	—	—	0.31

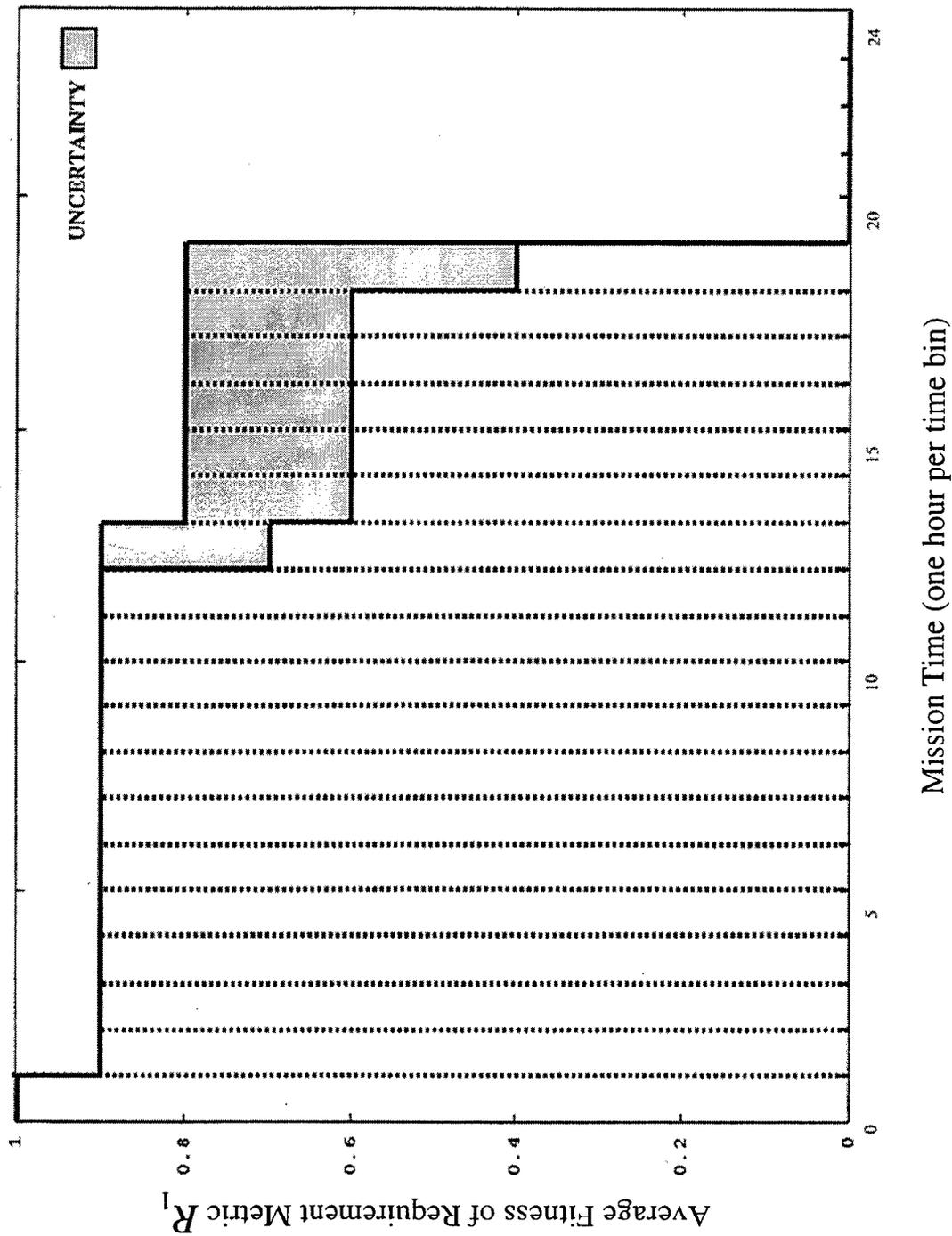


Figure 29. Average Fitness Profile for R_1 Using Trinary States (Without Interthreat Synergy).

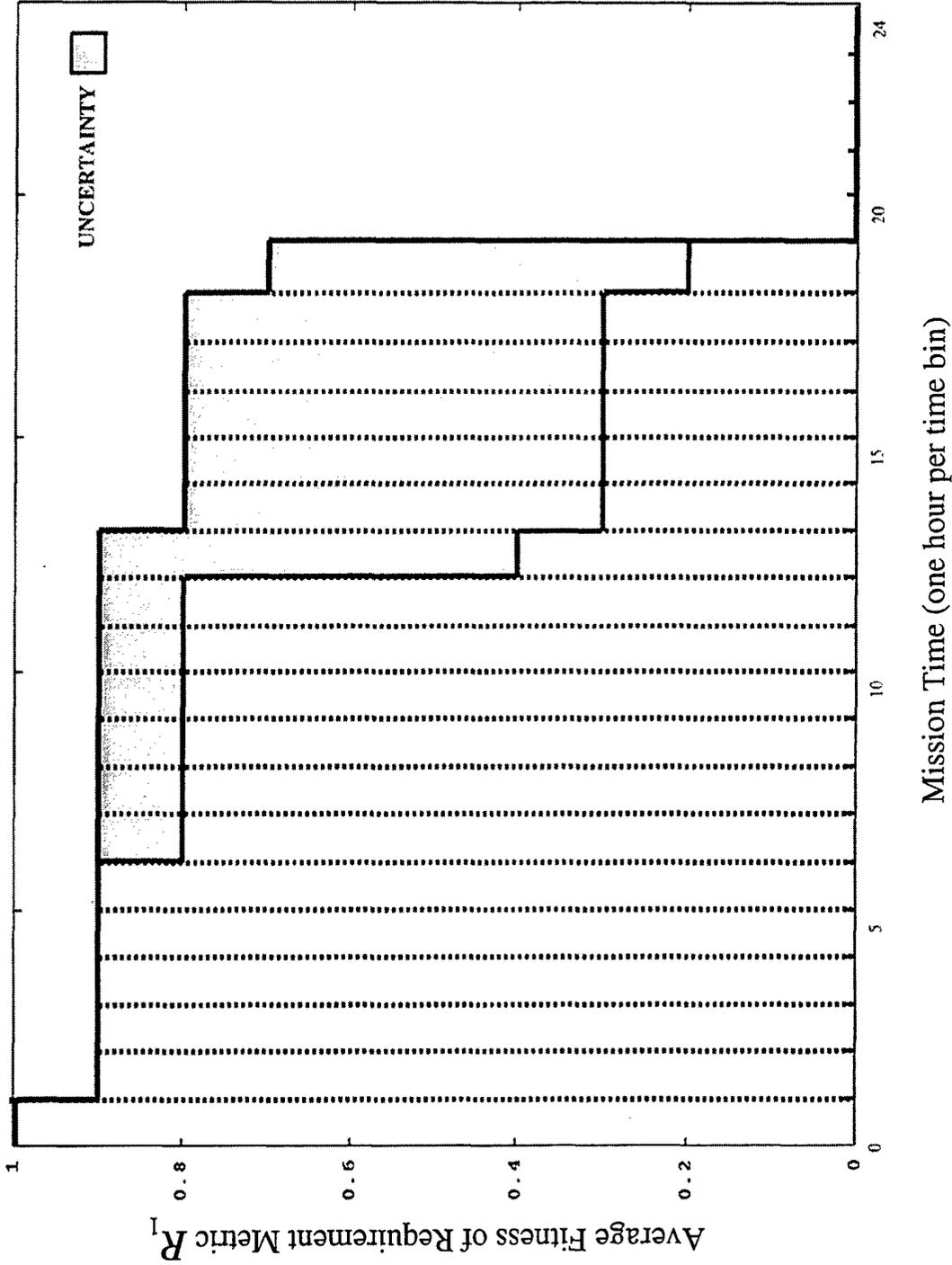


Figure 30. Average Fitness Profile for R_1 Using Trinary States (Assuming Interthreat Synergy).

UNCERTAINTY 

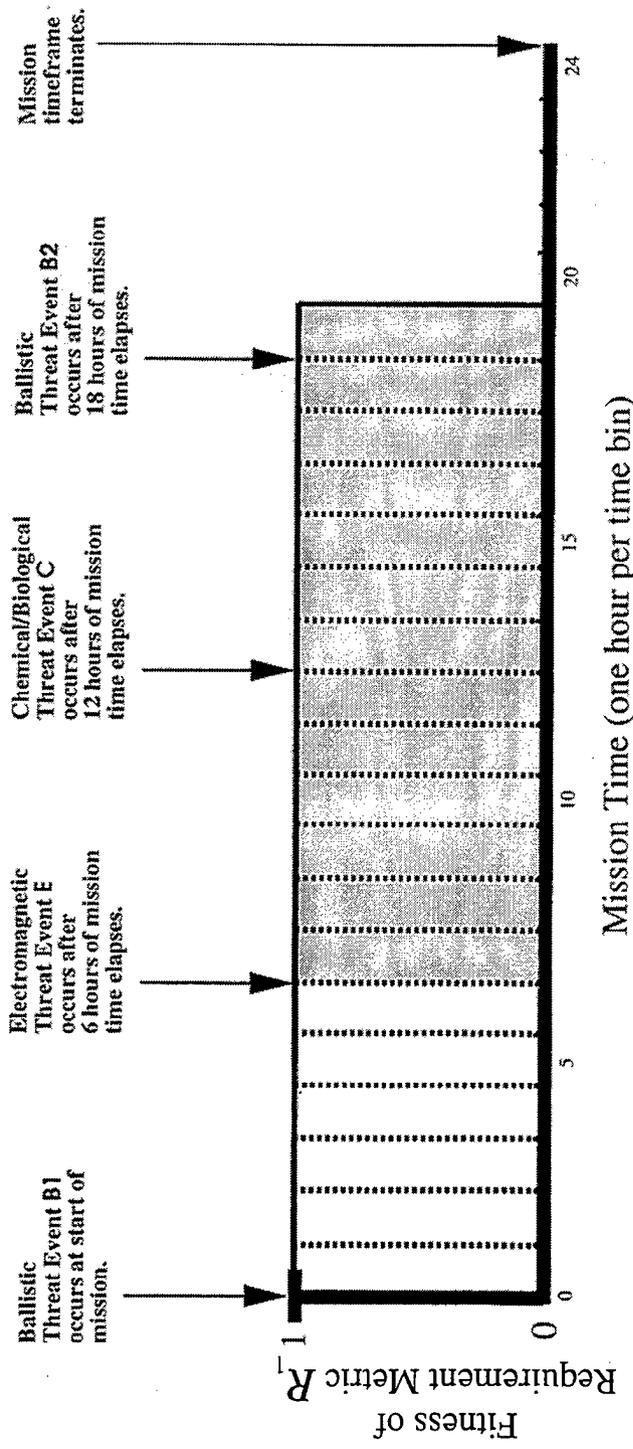


Figure 31. Plot of R_1 Fitness Profile From Table 9 Using Trinary States.

- Half of the values in Table 5 are equal to 0, while the other half range from 0.25 to 0.75, meaning that the ground combat system is incapable of fulfilling requirement R_2 in half of the threat scenarios and capable, for limited periods of time, in the remaining scenarios. The average amount of time that R_2 can be fulfilled is equal to 20% of the entire mission length; the time-averaged mission fitness of R_2 for all threat profiles is equal to 0.20.
- The values in Table 6 closely track those in Table 4, ranging again from 0.50 to 0.79 (with two exceptions this time, equal to 0.04 and 0.25). This means that the inclusion of interthreat synergy effects on the ability of the system to fulfill R_1 only changes a fraction of the threat profiles, with the average amount of time where R_1 can be fulfilled reduced from 62% to 52% of the entire mission length (or the time-averaged mission fitness of R_1 for all threat profiles is reduced from 0.62 to 0.52).

If the degree of synergy between threats is increased, then it is possible that the time-averaged requirement metric for all threat profiles will decrease (it will never increase, since interthreat synergy can only act to either maintain or degrade the survivability of a system).

Next, the profile-averaged requirement metrics per time bin (also described in section 2.7) are displayed in the bottom rows of the tables. Since each row in a table describes a fitness profile relative to a specific threat profile (see section 2.6), the bottom row can be thought of as an average fitness profile, which provides the average likelihood (per time bin) that the system is capable of fulfilling a required mission task. By studying the average fitness profiles in the three tables, the following trends are observed.

- The average fitness profiles in all tables monotonically decrease in steps as time advances, as illustrated in Figures 24, 25, and 28. This is due to the manner in which the different threat events are applied to the ground system as a function of time (see Table 3).

- Synergy acts to add structure to the average fitness profile. For example, when comparing the no-synergy average fitness profile for R_1 (Figure 24) with the B1/E synergy profile (Figure 28), it is seen that the latter figure contains more interim steps in the plot.

In this example, the practical impact of considering interthreat synergy is a slight decrease in the average fitness of R_1 as a function of time.

4.2.4 Trinary-State Analysis Results. The main effect of adding the undetermined functional state u in the trinary-state analysis approach is to create “uncertainty zones” within certain time bins in the 24-hr mission time frame. The extent of these zones is represented by the data in Tables 7 and 8, and can also be observed in the plots of average fitness profiles in Figures 29 and 30 and fitness profile no. 9 (from Table 8) in Figure 31. As is seen in these various plots, an uncertainty zone defines a confidence interval per time bin, which spans values from the lowest to highest possible fitness (either averaged or profile-specific) of the requirement under analysis. For example, the average fitness profile shown in Figure 30 indicates that the ground combat system is capable of fulfilling requirement R_1 :

- under all threat conditions during hour 1 of the mission,
- 90% of the time (given the 10 threat profiles) from hour 2 through hour 6 of the mission,
- between 80% and 90% of the time from hour 7 through hour 12 of the mission,
- between 40% and 90% of the time during hour 13 of the mission,
- between 30% and 80% of the time from hour 14 through hour 18 of the mission,
- between 20% and 70% of the time during hour 19 of the mission, and
- under no conditions from hour 20 to the end of the mission.

As an example of a fitness profile based on a single threat profile, Figure 31 indicates that the ground combat system is:

- definitely capable of fulfilling R_1 during the first 6 hr of the mission,
- possibly incapable of fulfilling R_1 from hour 7 through hour 19 of the mission, and
- definitely incapable of fulfilling R_1 from hour 20 to the end of the mission.

The uncertainty in the aforementioned plots originates from the undetermined responses of the fuel computer to threat event E and the rubber gaskets in the engine to threat event C after 12 hr of exposure; this uncertainty disappears when a decision is enforced as to whether the fuel computer and engine are definitely functional or dysfunctional (as in section 4.2.1). Thus, the integrated analysis process tends to amplify the effect of undetermined Level 2] component metrics at the operational requirement level, especially those component metrics that are functionally affected by multiple threats or those that map into more than one requirement metric.

4.2.5 Analysis Constraints Involving Time Discretization. In this section, the practical impact of analysis constraints involving the level of time discretization is examined. Although the ground combat system example described in this section is studied over a 24-hr window of time, the nature of the threat profiles in Table 3 effectively constrains the analysis to four time bins: (1) time ≥ 0 to time = 6 hr, (2) time > 6 hr to time = 12 hr, (3) time > 12 hr to time = 18 hr, and (4) time > 18 to time = 24 hr. In this case, the total number of possible threat profiles (only 10 of which are tabulated in Table 3) is equal to $4^4 = 256$. Of course, not all of these sequences need be explored. For example, the chemical threat event C has no effect within a 24-hr mission time frame when the event occurs in either time bin no. (3) or (4), as previously described (where time > 12 hr to time = 24 hr).

The problem with using the four large time bins previously described is that the effects of time-dependent system capability states can be lost. Specifically, the reader is directed to the

mobility subsystem degraded state M_3 (stop after time t) described in Table 1. In the ground combat system example in that section, $t = 1$ hr; this metric then defines the sampling frequency (one sample per hour) for updating both requirement metrics R_1 and R_2 so as to obtain meaningful results. Thus, to see the effect of M_3 on the average fitness profiles of R_1 and R_2 , one would need to calculate and average over the fitness profiles resultant from all possible threat profiles distributed across the 24 1-hr time bins within the mission time frame. Given that four different threat events can occur in a time bin, the total number of required profiles is $24^4 = 331,776$. Without an automated computer code to calculate and average these profiles, this level of analysis is somewhat intractable.

An alternate approach to calculating average fitness profiles is to concentrate on a limited number of specific threat profiles that are meaningful to the system evaluator, and then generate the corresponding set of fitness profiles (as was done for the ground combat system in the current example). Figure 32 depicts a hypothetical result derived from applying threat profile no. 9 (from Table 3) to all metrics in the requirement vector as shown in Figure 15, where interthreat synergy and trinary-functional states are assumed. In this hypothetical result, it is seen that:

- requirement metrics R_1 and R_3 are possibly deactivated by the EM threat event E, and then are both definitely deactivated 1 hr following the ballistic threat event B2 (total immobilization due to radiator failure);
- requirement metric R_2 is definitely deactivated by the ballistic threat event B1;
- requirement metrics R_7 , R_8 , R_{10} , R_{11} , and R_{12} are possibly deactivated by threat event E and remain in this uncertain functional state for the remainder of the mission; and
- requirement metrics R_4 , R_5 , R_6 , and R_9 are unaffected by any of the threats and, thus, are executable throughout the mission.

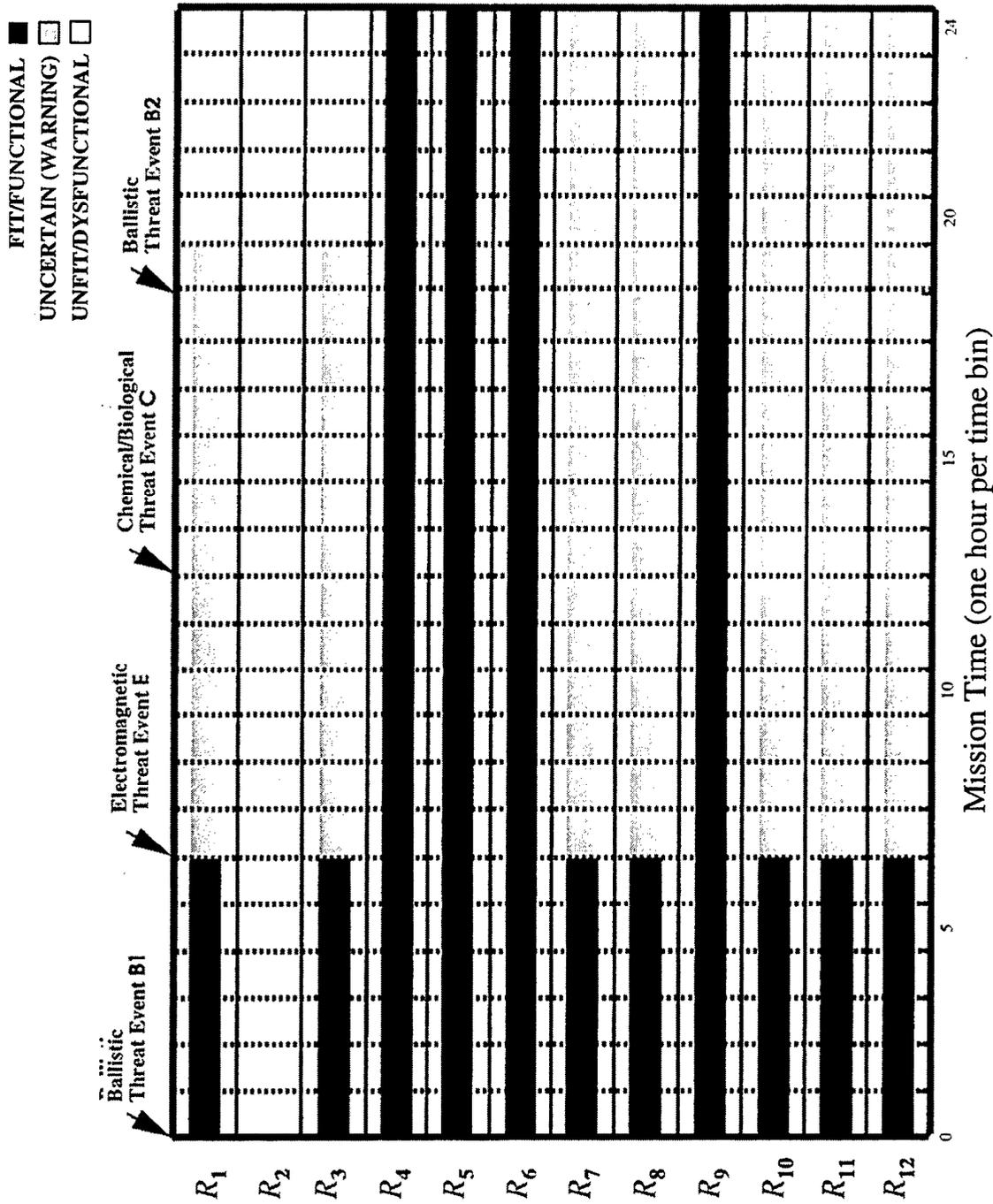


Figure 32. Hypothetical Result Derived From Applying Threat Profile No. 9 (From Table 3) to All Metrics in the Requirement Vector (Assuming Interthreat Synergy and Trinary States).

By restricting the integrated analysis to a limited set of threat profiles, more complex threat sequencing can be explored, as well as greater discretization resolution (more time bins per mission) within a mission time frame.

5. Conclusions

The integrated analysis methodology that has been described and demonstrated within this report allows for all of the battlefield threats within SLAD's analysis domain to be addressed in one framework. This methodology allows for the effects of both threat sequencing and interthreat synergy on required battlefield performance to be studied and analyzed. The discrete time analysis process allows for both permanent component damage and transient component/subsystem dysfunction types of effects to be addressed. Finally, the integrated analysis methodology connects the analysis product to required battlefield performance metrics for the military system as described in the system OMS/MP. Since the discrete time integrated analysis methodology is a mechanism for aggregating survivability measures of performance (MOP) and measures of effectiveness (MOE), the integrated analysis product will provide the decision maker with a means to evaluate the overall impact of battlefield threats on potential combat system effectiveness.

INTENTIONALLY LEFT BLANK.

6. References

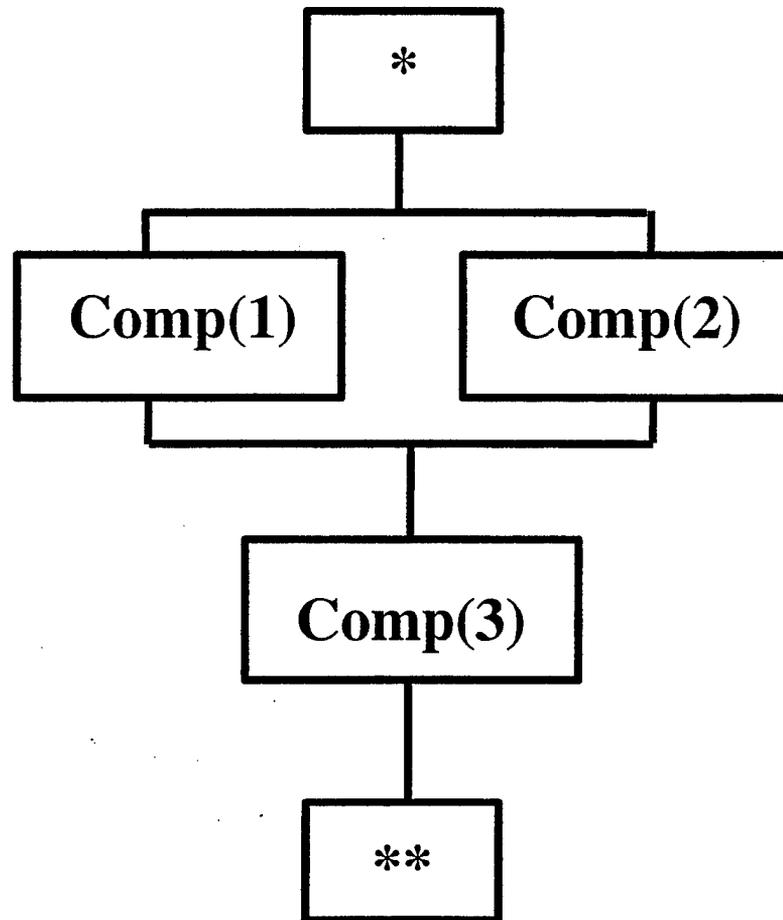
- Borkowski, L., and J. Slupecki. "The Logical Works of Jan Lukasiewicz." *Studia Logica*, vol. 8, pp. 7-56, 1958.
- Comstock, G. R. "The Degraded States Weapons Research Simulation (DSWARS): An Investigation of the Degraded States Vulnerability Methodology in a Combat Simulation." AMSAA-TR-495, U.S. Army Materiel Systems Analysis Activity, February 1991.
- Deitz, P. H. Comments in response to the report of the Board on Army Science and Technology's Committee on Vulnerability. U.S. Army Ballistics Research Laboratory, Aberdeen Proving Ground, MD, July 1986.
- Deitz, P. H., and A. Ozolins. "Computer Simulation of the Abrams Live-Fire Field Testing." BRL-MR-3755, U.S. Army Ballistics Research Laboratory, Aberdeen Proving Ground, MD, May 1989.
- Deitz, P. H., M. W. Starks, J. H. Smith, and A. Ozolins. "Current Simulation Methods in Military Systems Vulnerability Assessment." BRL-MR-3880, U.S. Army Ballistics Research Laboratory, Aberdeen Proving Ground, MD, November 1990.
- Hughes, W. J. "A Taxonomy for the Combined Arms Threat." *Chemical Biological/Smoke Modeling and Simulation Newsletter*, vol. 1, no. 3, Chemical Biological Information Analysis Center, Fall 1995.
- Kinsler, R. E. "Criticality Analysis of the M2A1 Bradley for the New Close Combat Methodology (NCCM)." ASI International, 15 March 1989.
- Klopčic, J. T., M. W. Starks, and J. N. Walbert. "A Taxonomy for the Vulnerability/Lethality Analysis Process." BRL-MR-3972, U.S. Army Ballistic Research Laboratory, Aberdeen Proving Ground, MD, May 1992.
- Kunkel, R. W., Jr. "Degraded States and Fault Tree Analysis of LONGBOW APACHE." ARL-TR-801, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, July 1995.
- Kunkel, R. W., Jr., and B. G. Ruth. "Fault Tree Analysis of Bradley Linebacker." U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, in publication.
- Murray, K. R., Moss, G. S., and Coates, S. A. "Modular Unix-Based Vulnerability Estimation Suite (MUVES) Analyst's Guide (Release 2.0)." U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, 1994, unpublished.

- Myers, J., B. G. Ruth, and R. E. Kunkel. "Integrated Vulnerability/Lethality Analysis of the Bradley Linebacker System." U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, in review.
- Roach, L. K. "Fault Tree Analysis and Extensions of the V/L Process Structure." ARL-TR-149, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, June 1993.
- Roach, L. K. "The New Degraded States Vulnerability Methodology (DSVM): A Change in Philosophy and Approach." ARL-TR-1223, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, November 1996.
- Ruth, B. G. "A Nuclear EMP Vulnerability/Lethality Taxonomy With Focus on Component Assessment." ARL-TR-205, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, November 1994.
- Saucier, R. "Methodology for Vehicle Vulnerability Assessment: A Synthesis of the Damage Assessment List Process and Degraded States Vulnerability Methodology. U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, in publication.
- Walbert, J. N. "The Mathematical Structure of the Vulnerability Spaces." ARL-TR-634, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, November 1994.
- zum Brunnen, R. L. "Introducing Chemical/Biological Effects Into the Ballistic Vulnerability/Lethality Taxonomy." ARL-TR-715, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, March 1995.

**Appendix A:
Fault Trees**

INTENTIONALLY LEFT BLANK.

A fault tree is defined as a process linking one or more critical component (or capability) functional levels with logical operations (AND, OR, NOT) that determines overall subsystem (or system) functionality. The term "tree" refers to the flow structure within the process, with one input node at the "top" and one output node at the "bottom" of the tree; severing the logical flow within the tree will serve to deactivate the tree. This last process occurs when one or more of the functionality metrics contained within the tree are set to a value of 0, thus severing the flow between fault tree nodes. Figure A-1 illustrates a simple fault tree.



A-1. Example of a Simple Fault Tree

The nature of the logical operations within a fault tree depends on whether the positive- or negative-logic convention is followed in regard to fault-tree metrics. For example, the logical AND/OR operations following the positive- and negative-logic conventions are applied to the fault tree in Figure A-1 (shown in Figures A-2(a) and (b), respectively). Following the

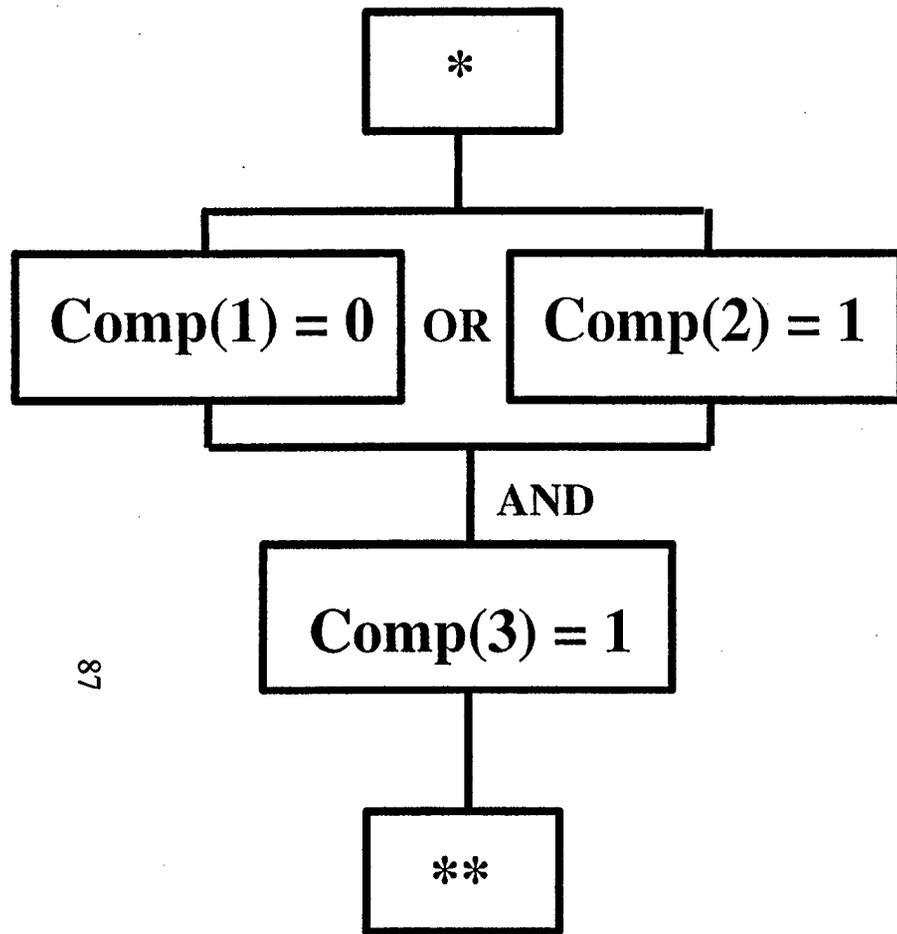
positive-logic convention (Figure A-2(a)), Comp(1) is dysfunctional, while Comp(2) and Comp(3) are functional; the fault tree evaluates to

$$([Comp(1) = 0] \mid [Comp(2) = 1]) \& [Comp(3) = 1] \rightarrow 1, \quad (A-1)$$

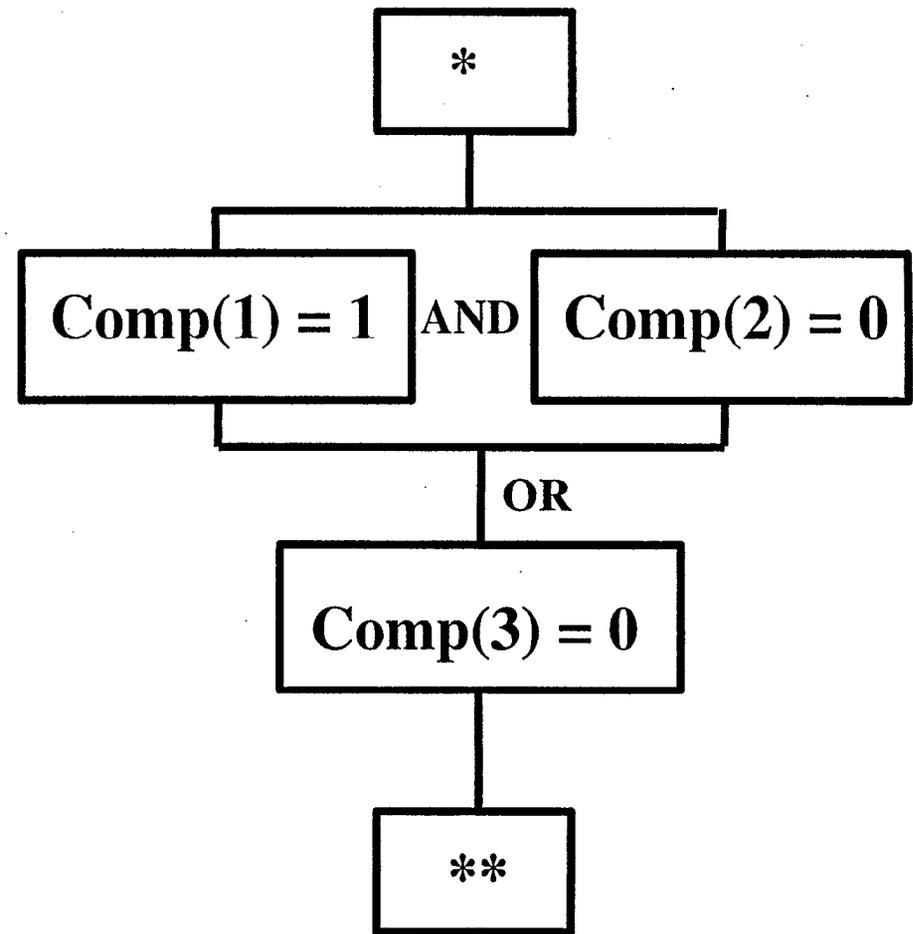
where \mid and $\&$ are the logical OR and AND operators, respectively. Following the negative-logic convention (Figure A-2(b)), again, Comp(1) is dysfunctional and Comp(2) and Comp(3) are functional but component functional metrics have reversed (e.g., $0 \rightarrow 1$ and $1 \rightarrow 0$); in this case, the fault tree evaluates to

$$([Comp(1) = 1] \& [Comp(2) = 0]) \mid [Comp(3) = 0] \rightarrow 0. \quad (A-2)$$

In this example, both logic conventions indicate residual functionality, either positively (the positive logic convention yields a 1) or negatively (the negative logic convention yields a 0).



(a)



(b)

Figure A-2. Example of Two Different Boolean Logic Conventions Applied to the Fault Tree in Figure A-1: (a) Positive Logic, (b) Negative Logic.

INTENTIONALLY LEFT BLANK.

Appendix B:
A Lukasiewicz Trinary Logic

INTENTIONALLY LEFT BLANK.

Since the conventional fault-tree methodology used in a vulnerability/lethality V/L analysis utilizes Boolean operations on binary (two-valued) logic, the conventional methodology needs to be extended to accommodate undetermined states. Thus, within the context of nonmeasured Level 2] metrics, the extended methodology is required to address three different allowed values of component functionality: 1, 0, and u (for an undetermined damage/dysfunction state reflecting either some unknown amount of component damage or functional disruption that may or may not result in temporary or permanent loss of component function). In the threat-specific instances where the state of a component cannot be evaluated, an undamaged component is assumed to be functional, while a damaged component can only be represented by an undetermined state (a state of u); in the case where a catastrophic component kill is likely due to Level 1] threat initial conditions, the analyst might choose to estimate the component state as fully nonfunctional.

Logical operations on 1, 0, and u follow the rules of a trinary (three-valued) logic as originally proposed by Lukasiewicz in 1920.¹ Tables B-1, B-2, and B-3 illustrate the logical AND, OR, and NOT (negation) operators, respectively, from the Lukasiewicz logic. As is seen from these tables, removal of the u state collapses the Lukasiewicz logic to the standard Boolean logic.

Table B-1. The AND Operation (Using the Lukasiewicz Trinary Logic)

AND	0	u	1
0	0	0	0
U	0	u	u
1	0	u	1

Table B-2. The OR Operation (Using the Lukasiewicz Trinary Logic)

OR	0	u	1
0	0	u	1
U	U	u	1
1	1	1	1

¹ Borkowski, L., and J. Slupecki. "The Logical works of Jan Lukasiewicz." *Studia Logica*, vol. 8, pp. 7-56, 1958.

Table B-3. The NOT Operation (Using the Lukasiewicz Logic)

NOT	
0	1
u	u
1	0

Appendix C:
Example of a Mission Profile

INTENTIONALLY LEFT BLANK.

A mission profile for a military system (as included in the Operational Mode Summary/Mission Profile [OMS/MP]) is a table identifying the tasks, number of occurrences of each task, and task duration associated with a particular mission. Table C-1 illustrates the "attack" mission profile for a generic ground combat system. The operating time (OT) is the length of time that a subsystem within the ground combat system takes to execute a required mission task. The calendar time (CT) is the total amount of time within a mission time frame. The total OT for all occurrences of a specific task within the mission profile is

$$\text{Total task OT} = \text{number of task occurrences} * \text{task OT.}$$

The total OT for all required tasks within the mission profile is then the sum of the total task OTs for each mission task. The mission profile does not specify at what point within the mission time frame that a task must be executed but, rather, only the total number of task occurrences within the mission. Dividing the total OT for a specific task by the mission CT yields the fraction of mission time required for execution of all occurrences of that task.

Table C-1. Example of an “Attack” Mission Profile for a Generic Ground Combat System (CT = 24 hr)

Tasks/Events	No. of Occurrences	Task OT (min)	Total OT (min)
M2 Carrier			
Road March	4	20.00	80.00
Tactical	20	5.00	100.00
Overwatch	30	10.00	300.00
Weapons			
Search	36	0.50	18.00
Acquire	14	0.08	1.12
Identify	12	0.08	0.96
Track	8	0.10	0.80
Primary Firepower			
Engage	6	0.25	1.50
Rearm	2	2.00	4.00
Secondary Firepower			
Engage	2	0.56	1.12
Rearm	0	4.00	0.00
Tertiary Firepower			
Engage	2	0.33	0.66
Rearm	0	2.00	0.00
Total (min)	—	—	508.16
Total (hrs)	—	—	8.47

Glossary

Average Fitness: The level of military system fitness averaged over either (1) a set of threat profiles (where an average fitness is assigned to each time bin within a mission time frame) or (2) all of the time bins within a specific fitness profile (where the average fitness conveys the fraction of mission time that the military system is fit to fulfill a requirement).

Average Fitness Profile: A discrete time series that is calculated by averaging fitness values in a specific time bin over a set of threat profiles, and then time-sequencing the results for all time bins within a mission time frame.

Evaluation Mapping: A submapping within the $O_{1,2}$ mapping that assigns a component functionality metric to all critical components within a military system based on the damage incurred by a component through interaction with a battlefield threat.

Fault Tree: A logical construct that maps Level 2] component functional metrics to Level 3] subsystem capability metrics. Logic within a fault tree is governed through the use of the Boolean AND, OR, and NOT operators.

Fitness: The ability of a military system to execute a required mission task based on the system's capability state.

Fitness Profile: A discrete time series that conveys the fitness of a military system to execute a required mission task at any point of time within a mission time frame. A fitness profile is based upon a specific threat profile.

Fitness Tree: A logical construct that maps Level 3] system capability metrics to requirement metrics, as specified in the system OMS/MP. The logical operations within a fitness tree include the use of the standard AND, OR, and NOT, operators, as well as conditional logic statements.

Interaction Mapping: A submapping within the O_{1,2} mapping that models the physical interaction between a battlefield threat and the target military system, which can result in physically measurable damage to components within the system.

Interthreat Synergy: A damage amplification process involving two sequential battlefield threats, where weapon system modification due to the preceding threat enhances the damage potential of the succeeding threat.

Mission Fitness Mapping: A process that maps Level 3] capability metrics to requirement metrics for a military system.

Mission Profile: A table identifying the tasks, number of occurrences of each task, and task duration associated with a particular mission.

Mission Time Frame: The window of time defined by the length of a particular mission as specified by the system Operational Mode Summary/Mission Profile (OMS/MP).

Negative Logic: A system of logic governing Level 2], Level 3], and requirement metrics that follows the convention that a functional metric (1) equals 0 if function remains during and/or after system interaction with a threat or (2) equals 1 if function is lost during and/or after system interaction with a threat.

Operational Mode Summary/Mission Profile (OMS/MP): A document for a military system that quantitatively specifies required operational performance across a spectrum of battlefield missions.

Positive Logic: A system of logic governing Level 2], Level 3], and requirement metrics that follows the convention that a functional metric (1) equals 1 if function remains during and/or after system interaction with a threat or (2) equals 0 if function is lost during and/or after system interaction with a threat.

Requirement: An operational battlefield task or function that may be required of a military system at any time during the course of a mission; essentially, a required mission capability is based on one or more Level 3] system capabilities. Requirements are referred to as “tasks/events” within the context of the system Operational Mode summary/Mission Profile (OMS/MP).

Threat Event: A Level 1] metric that describes the conditions of a battlefield threat just as it is about to interact with a target system.

Threat Profile: A sequence of threat events that occurs along a discrete time axis; a threat scenario.

Time-Averaged State: The average value of a transient Level 2], Level 3], or requirement metric within a single time bin.

Time Bin: A discrete unit or interval of time within a mission time frame.

Trinary Logic: An extension to the conventional binary state Boolean logic that posits a third state “u” representing an undetermined binary metric.

INTENTIONALLY LEFT BLANK.

<u>NO. OF COPIES</u>	<u>ORGANIZATION</u>
2	DEFENSE TECHNICAL INFORMATION CENTER DTIC DDA 8725 JOHN J KINGMAN RD STE 0944 FT BELVOIR VA 22060-6218
1	HQDA DAMO FDQ D SCHMIDT 400 ARMY PENTAGON WASHINGTON DC 20310-0460
1	OSD OUSD(A&T)/ODDDR&E(R) R J TREW THE PENTAGON WASHINGTON DC 20301-7100
1	DPTY CG FOR RDE HQ US ARMY MATERIEL CMD AMCRD MG CALDWELL 5001 EISENHOWER AVE ALEXANDRIA VA 22333-0001
1	INST FOR ADVNCD TCHNLGY THE UNIV OF TEXAS AT AUSTIN PO BOX 202797 AUSTIN TX 78720-2797
1	DARPA B KASPAR 3701 N FAIRFAX DR ARLINGTON VA 22203-1714
1	NAVAL SURFACE WARFARE CTR CODE B07 J PENNELLA 17320 DAHLGREN RD BLDG 1470 RM 1101 DAHLGREN VA 22448-5100
1	US MILITARY ACADEMY MATH SCI CTR OF EXCELLENCE DEPT OF MATHEMATICAL SCI MAJ M D PHILLIPS THAYER HALL WEST POINT NY 10996-1786

<u>NO. OF COPIES</u>	<u>ORGANIZATION</u>
1	DIRECTOR US ARMY RESEARCH LAB AMSRL DD J J ROCCHIO 2800 POWDER MILL RD ADELPHI MD 20783-1145
1	DIRECTOR US ARMY RESEARCH LAB AMSRL CS AS (RECORDS MGMT) 2800 POWDER MILL RD ADELPHI MD 20783-1145
3	DIRECTOR US ARMY RESEARCH LAB AMSRL CI LL 2800 POWDER MILL RD ADELPHI MD 20783-1145
	<u>ABERDEEN PROVING GROUND</u>
4	DIR USARL AMSRL CI LP (305)

<u>NO. OF COPIES</u>	<u>ORGANIZATION</u>	<u>NO. OF COPIES</u>	<u>ORGANIZATION</u>
2	DEFENSE TECH INFO CTR DTIC OCA J CHIRAS (2CPS) 8725 JOHN J KINGMAN RD STE 0944 FT BELVOIR VA 22060-6218	1	USA TRADOC ATCD B FT MONROE VA 23561-5000
2	OUSD AT STR TAC SYS AIR WARFARE R MUTZEL RM 3E139 LAND WARFARE MR VIIIU RM 3B1060 3090 DEFENSE PENTAGON WASHINGTON DC 20310-3090	1	USA TRAC ATRC W MR KEINTZ WSMR NM 88002-5502
1	OASD C31 DR SOOS RM 3E194 6000 DEFENSE PENTAGON WASHINGTON DC 20310-6000	1	USARL SLAD AMSRL SL PLANS AND PGMS MGR WSMR 88002-5513
1	DUSA OR RM 2E660 102 ARMY PENTAGON WASHINGTON DC 20310-0102	7	USARL SLAD AMSRL SL EA R FLORES (5 CPS) L MORRISON Y YEE WSMR NM 88002-5513
3	ASST SECY ARMY AL&T SARD ZD RM 2E661 SARD ZT RM 3E374 103 ARMY PENTAGON WASHINGTON DC 20310-0103	6	USARL SLAD AMSRL SL EM J PALOMO (5 CPS) R DELRIO WSMR NM 88002-5513
1	OADCSOPS FORCE DEV DIR DAMO FDW RM3C630 460 ARMY PENTAGON WASHINGTON DC 20310-0460	1	OSD DUSD (S&T) SENSORS J LUPO THE PENTAGON WASHINGTON DC 20301-7100
1	HQ USAMC PRINCIPAL DEP FOR ACQSTN AMCDCG A 5001 EISENHOWER AVE ALEXANDRIA VA 22333-0001	1	CECOM SP & TRRSTRL COMMCTN DIV AMSEL RD ST MC M H SOICHER FT MONMOUTH NJ 07703-5203
1	HQ USAMC PRINCIPAL DEP FOR TECH AMCDCG T 5001 EISENHOWER AVE ALEXANDRIA VA 22333-0001	1	CECOM PM GPS COL S YOUNG FT MONMOUTH NJ 07703
		1	CECOM RDEC ELECTRONIC SYS DIV DIR J NIEMELA FT MONMOUTH NJ 07703

NO. OF
COPIES ORGANIZATION

NO. OF
COPIES ORGANIZATION

2 DIR USARL
AMSRL SL EI
J NOWAK
P BOTHNER
FT MONMOUTH NJ 07703-5602

1 GPS JOINT PROG OFC DIR
COL J CLAY
2435 VELA WAY STE 1613
LOS ANGELES CA 90245-5500

1 AIR FORCE RESEARCH LABORATORY
AFRL/MNO INTEGRATION & OPS DIV
101 WEST EGLIN BLVD STE 128
EGLIN AFB FL 32542-6810

1 AIR FORCE RESEARCH LABORATORY
MUNITIONS DIRECTORATE (ARFL/MN)
101 WEST EGLIN BLVD STE 101
EGLIN AFB FL 32542-6810

ABERDEEN PROVING GROUND

2 DIR USA TECOM
AMSTE TA
AMSTE TMS

7 DIR USOPTEC/EAC
CSTE EAC MR HUGHES
CSTE EAC DR HASKELL
CSTE EAC DR J STREILEIN
CSTE EAC SV
DR D HASKELL
R LAUGHMAN
J MYERS
T FLORY

3 DIR USAMSAA
AMXSY D
AMXSY ST
AMXSY TD DR P DEITZ

69 DIR USARL
AMSRL SL
J J WADE
J BEILFUSS
M MUUSS

AMSRL SL B
J SMITH
R SANDMEYER
W WINNER (10 CPS)
M VOGEL
J FRANZ

AMSRL SL BA
M RITONDO
L ROACH
R HENRY
D DAVIS
B WARD
R DIBELKA
E DAVISSON
R BOWERS
J SHORT

J JUARASCIO
AMSRL SL BE
D BELY
T KLOPCIC
M MAHAFFEY
R SAUCIER
P TANENBAUM
E DAVIS
D NEADES

AMSRL SL BD
L MORRISSEY
S POLYAK
R GROTE
T BROWN
W BAKER

AMSRL SL BG
A YOUNG
T MUEHL
S PRICE
R MURRAY
W HRUZ
L WILSON
J ROBERTSON

J PLOSKONKA
AMSRL SL BN (E3331)
D FARENWALD
E FIORAVANTE
M KAUFMAN
R KUNKEL
R PARSONS
B RUTH (10 CPS)

NO. OF
COPIES ORGANIZATION

ABERDEEN PROVING GROUND CONT

AMSRL SL E
DR STARKS
AMSRL SL EM (E3331)
DR FEENEY
J ANDRESE
W KLIMEK
AMSRL SL EI (E3331)
D BAYLOR
R ZUM BRUNNEN
AMSRL SL EC
E PANUSKA (B328)

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE

July 1999

3. REPORT TYPE AND DATES COVERED

Final, Oct 97-Jun 98

4. TITLE AND SUBTITLE

Discrete Time Integrated Analysis Methodology for a Ground Combat System

5. FUNDING NUMBERS

665604D670

6. AUTHOR(S)

Brian G. Ruth

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Research Laboratory
ATTN: AMSRL-SL-BN
Aberdeen Proving Ground, MD 21010-5423

8. PERFORMING ORGANIZATION REPORT NUMBER

ARL-TR-2017

9. SPONSORING/MONITORING AGENCY NAMES(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

In this report, a methodology is presented for the integrated analysis of a military weapon system across all classes of battlefield threats addressed by the Survivability/Lethality Analysis Directorate (SLAD) of the U.S. Army Research Laboratory (ARL). The target audience for this report is vulnerability/lethality (V/L) analysts who might participate in such an integrated analysis. The integrated analysis methodology is based on the V/L taxonomy, which provides a framework for the analysis of a military system. Available system capability states are mapped to required mission tasks as described in the military system's Operational Mode Summary/Mission Profile (OMS/MP) and then tracked along a discrete time axis, allowing for both threat sequencing and interthreat synergy on required battlefield performance to be studied and analyzed. Since the discrete time integrated analysis methodology is a mechanism for aggregating survivability measures of performance (MOP) and measures of effectiveness (MOE), the integrated analysis product provides the decision maker with a means to evaluate the overall impact of battlefield threats on potential combat system effectiveness.

14. SUBJECT TERMS

Integrated analysis, discrete time process, V/L taxonomy, ground combat system

15. NUMBER OF PAGES

109

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT

UNCLASSIFIED

18. SECURITY CLASSIFICATION OF THIS PAGE

UNCLASSIFIED

19. SECURITY CLASSIFICATION OF ABSTRACT

UNCLASSIFIED

20. LIMITATION OF ABSTRACT

UL

INTENTIONALLY LEFT BLANK.

USER EVALUATION SHEET/CHANGE OF ADDRESS

This Laboratory undertakes a continuing effort to improve the quality of the reports it publishes. Your comments/answers to the items/questions below will aid us in our efforts.

- 1. ARL Report Number/Author ARL-TR-2017 (Ruth) Date of Report July 1999
- 2. Date Report Received _____
- 3. Does this report satisfy a need? (Comment on purpose, related project, or other area of interest for which the report will be used.) _____

- 4. Specifically, how is the report being used? (Information source, design data, procedure, source of ideas, etc.) _____

- 5. Has the information in this report led to any quantitative savings as far as man-hours or dollars saved, operating costs avoided, or efficiencies achieved, etc? If so, please elaborate. _____

- 6. General Comments. What do you think should be changed to improve future reports? (Indicate changes to organization, technical content, format, etc.) _____

CURRENT ADDRESS	_____	Organization	
	_____	Name	E-mail Name
	_____	Street or P.O. Box No.	
	_____	City, State, Zip Code	

7. If indicating a Change of Address or Address Correction, please provide the Current or Correct address above and the Old or Incorrect address below.

OLD ADDRESS	_____	Organization
	_____	Name
	_____	Street or P.O. Box No.
	_____	City, State, Zip Code

(Remove this sheet, fold as indicated, tape closed, and mail.)
(DO NOT STAPLE)

DEPARTMENT OF THE ARMY

OFFICIAL BUSINESS

BUSINESS REPLY MAIL
FIRST CLASS PERMIT NO 0001,APG,MD

POSTAGE WILL BE PAID BY ADDRESSEE

**DIRECTOR
US ARMY RESEARCH LABORATORY
ATTN AMSRL SL BN
ABERDEEN PROVING GROUND MD 21005-5068**



**NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES**

