ARMY RESEARCH LABORATORY

The System Capabilities Analytic Process (SCAP) as Presented at the National Defense Industrial Association (NDIA) 26th Annual National Test and Evaluation (T&E) Conference on March 2, 2010

by Kevin S. Agan

ARL-SR-0217 **December 2010**

NOTICES

Disclaimers

Army Research Laboratory
Aberdeen Proving Ground, MD 21005-5066

ARL-SR-0217 **December 2010**

The System Capabilities Analytic Process (SCAP) as Presented at the National Defense Industrial Association (NDIA) 26th Annual National Test and Evaluation (T&E) Conference on March 2, 2010

Kevin S. Agan
Survivability/Lethality Analysis Directorate, ARL

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
December 2010

2. REPORT TYPE
Final

3. DATES COVERED (From - To)
August 2009–March 2010

4. TITLE AND SUBTITLE
The System Capabilities Analytic Process (SCAP) as Presented at the National Defense Industrial Association (NDIA) 26th Annual National Test and Evaluation (T&E) Conference on March 2, 2010

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Kevin S. Agan

5d. PROJECT NUMBER
D675

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory
ATTN: RDRL-SLB-E
Aberdeen Proving Ground, MD 21005-5066

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-SR-0217

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

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The System Capabilities Analytic Process (SCAP) is an emerging methodology, which allows a person who is analyzing a system to determine that system's remaining capability after the loss of critical components. The methodology was presented at the National Defense Industrial Association (NDIA) 26th Annual National Test and Evaluation (T&E) Conference on March 2, 2010 with the intent to share this paradigm with the Department of Defense (DoD) community and to solicit feedback on ways to improve SCAP. The conference theme was how to improve the ways the DoD will analyze, test, and evaluate networked system-of-systems (SoS). SCAP was shown as a way to correlate how the dysfunction of one system can impact the capabilities of a SoS.

15. SUBJECT TERMS
MBT&E, SCAP, capability, component, task, loss of function

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON / 19b. TELEPHONE NUMBER (*Include area code*)
Unclassified	Unclassified	Unclassified	UU	50	Kevin S. Agan / (410) 278-4458

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Contents

List of Figures

INTENTIONALLY LEFT BLANK.

1. Introduction

The System Capabilities Analytic Process (SCAP) is an emerging methodology that allows an individual who is analyzing a system to determine that system's remaining capability after the loss of critical components. SCAP is currently undergoing several trials in support of Army Test and Evaluation Command's (ATEC)'s Mission-Based Test and Evaluation (MBT&E) initiative.

On March 2, 2010, Mr. Kevin Agan of the U.S. Army Research Laboratory, Survivability/Lethality Analysis Directorate (ARL/SLAD) presented *"A Process for Mapping Component Function to Mission Completion"*, which is an overview of the SCAP methodology. This presentation occurred at the National Defense Industrial Association (NDIA) 26th Annual Test and Evaluation (T&E) conference, located in San Diego, CA from March 1–4, 2010. As the conference was unclassified, all material had to be public release. Therefore, all examples of the live-fire analysis that were then used to test SCAP outputs were not briefed and are not included in this report.

The conference was sponsored by the National Defense Industrial Association (NDIA) and supported by the Office of the Under Secretary of Defense (AT&L) and the Director, Operational Test and Evaluation (DOT&E). The theme of the conference was "defense test and evaluation in a net-centric world". The intent of the conference was to share ideas and methodologies within the Department of Defense (DoD), supporting contracts and system developers that could improve Test and Evaluation (T&E) of combat systems that operate in the net-centric combat environment that currently exists on the modern battlefield. As the conference postulated that T&E of a combat system as an isolated entity may not provide adequate results, SCAP was presented as a way to bridge capabilities between multiple systems and ultimately provide a means to identify remaining mission utility when a system within a family of systems is attacked.

The presentation was well attended by representatives from multiple DoD organizations, contract support companies, and hardware developers. Also in attendance were about 10 individuals of either the Senior Executive Service (SES) or retired General officers. The audience actively engaged in a question and answer session with follow-on discussions that lasted about 1/2 h after the concluding remarks. Several organizations have expressed interest in acquiring the completed methodology and considerable feedback was received on ways to improve SCAP so that it could be utilized across the DoD.

It was assumed that the audience at the workshop was familiar with traditional methodologies for T&E, as well as vulnerability analysis. Because of this familiarity, the enclosed briefing does not describe the traditional methodology. The traditional methodologies are well documented and some sources are identified in the references.

The following report is the presentation as it was presented at the conference. All of the figures are the briefing slides as they were shown at the conference, and the body of the report is the talking points related to each slide.

2. Slides

The objective of the presentation is to inform the T&E community of how SCAP could be applied to the analysis of combat vehicles. The general process will be explained and some sample compilations will be provided. For a system of systems (SoS), it will be shown how the map between the component and capability for each vehicle can connect to correlating capabilities of another system. Feedback will be solicited that can be used to improve and enhance this process.

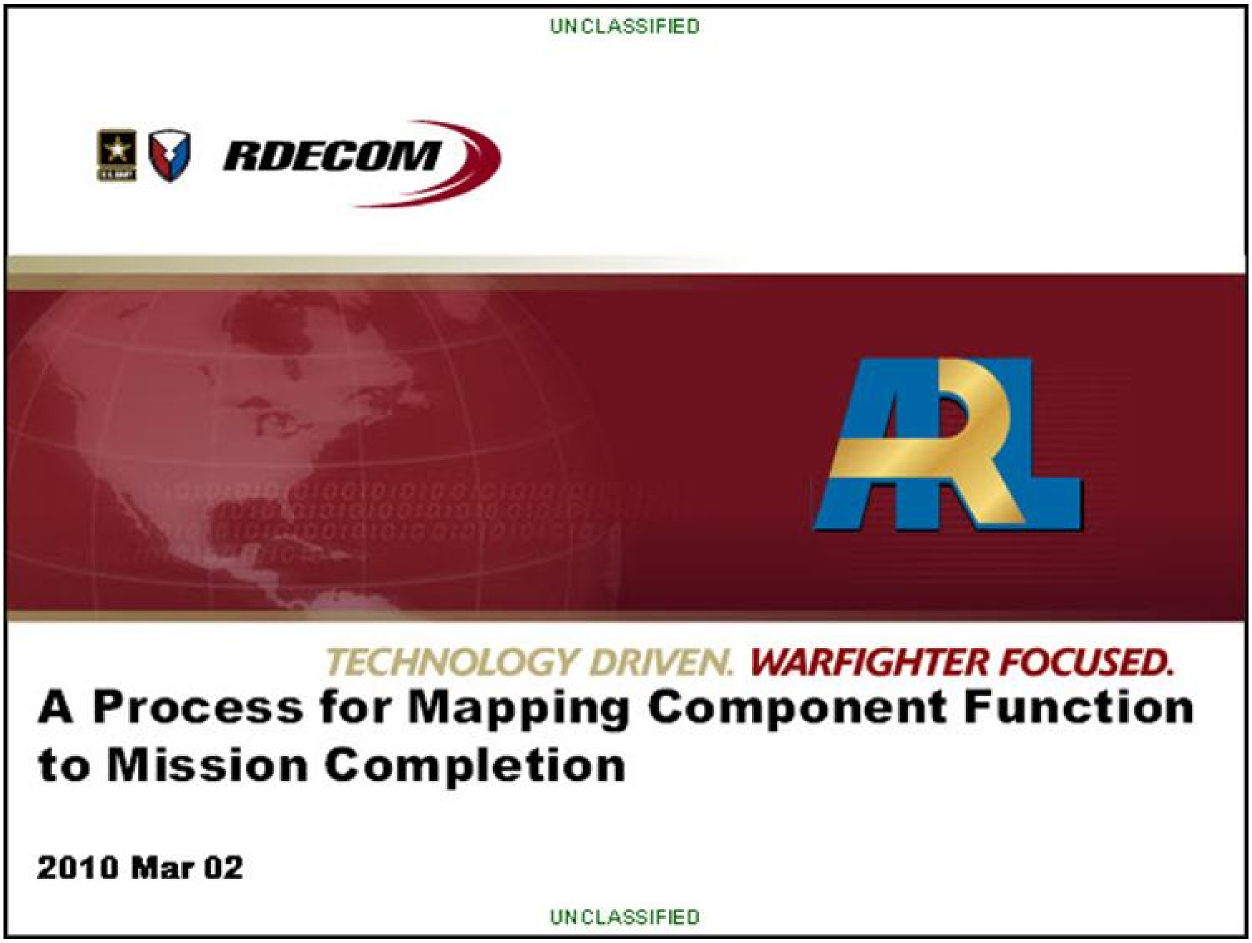

Figure 1. Title slide.

Figure 1 depicts the title slide of the presentation.

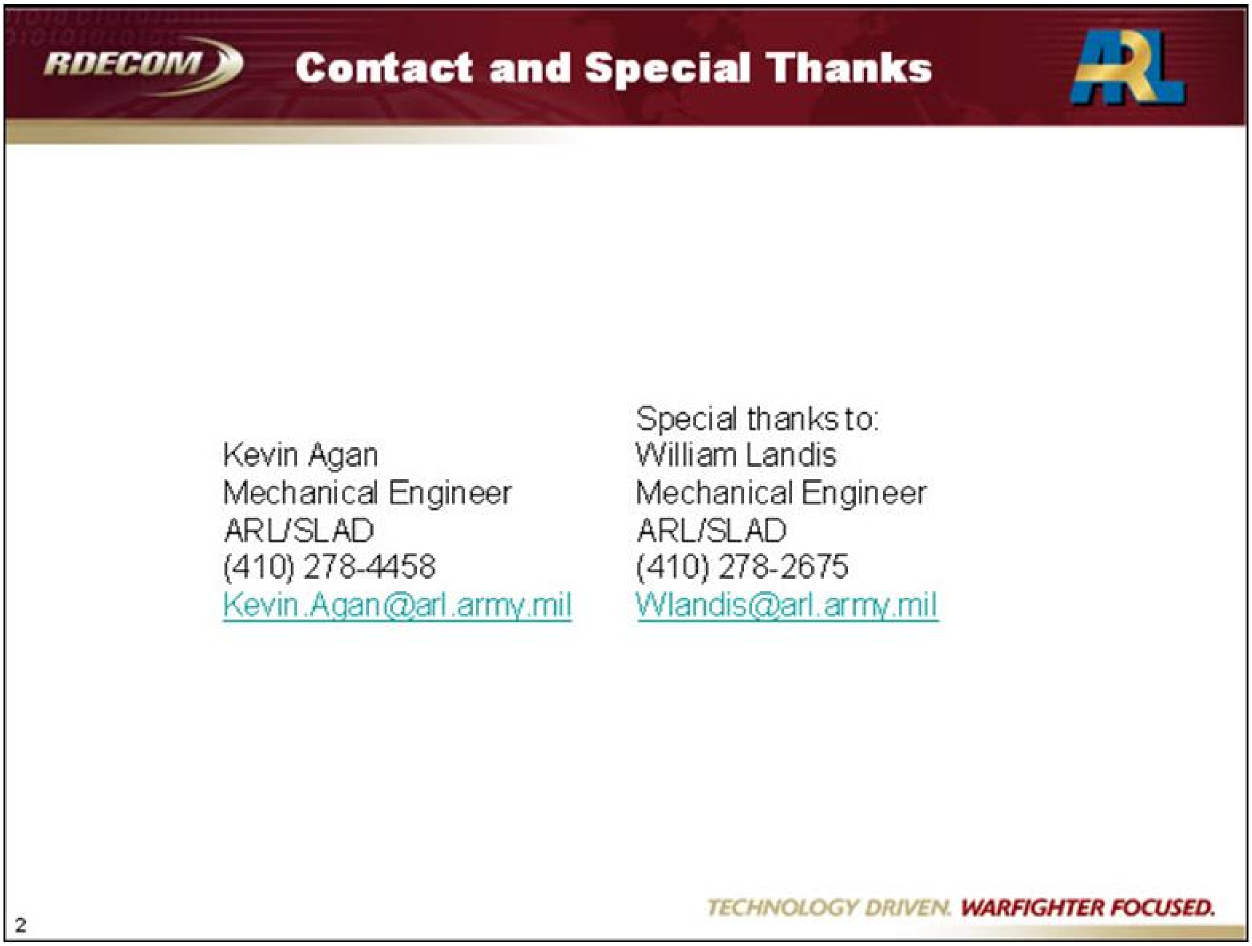

Figure 2. Contact and special thanks.

Kevin Agan is a mechanical engineer for the ARL/SLAD. Primary responsibilities include engineering analysis of ground combat systems and live-fire damage assessments in support of Title X. Prior to his career with SLAD, Mr. Agan worked for 12 years in the private sector under various roles. These roles include new product design, manufacturing, reliability engineering, finite element analysis, and electrical-mechanical packaging.

William Landis works alongside of Mr. Agan and has similar primary responsibilities. Over the last several months Mr. Landis has been a major contributor to the development of the SCAP methodology. His efforts on the development of sample data using on a pilot program have been significant and invaluable.

The contact information for both Mr. Agan and Mr. Landis can be found in figure 2.

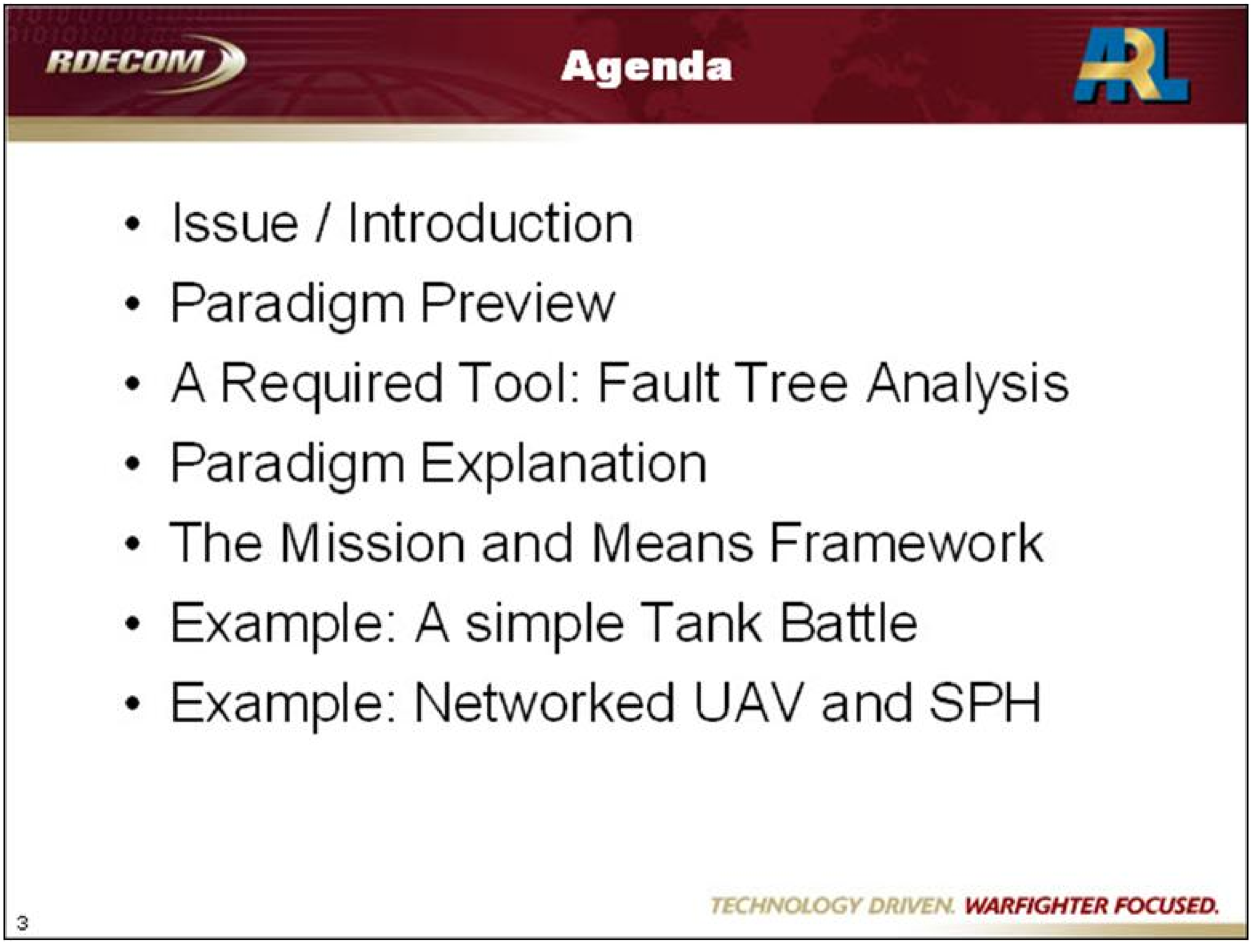

Figure 3. Agenda.

The agenda for this presentation is depicted in figure 3.

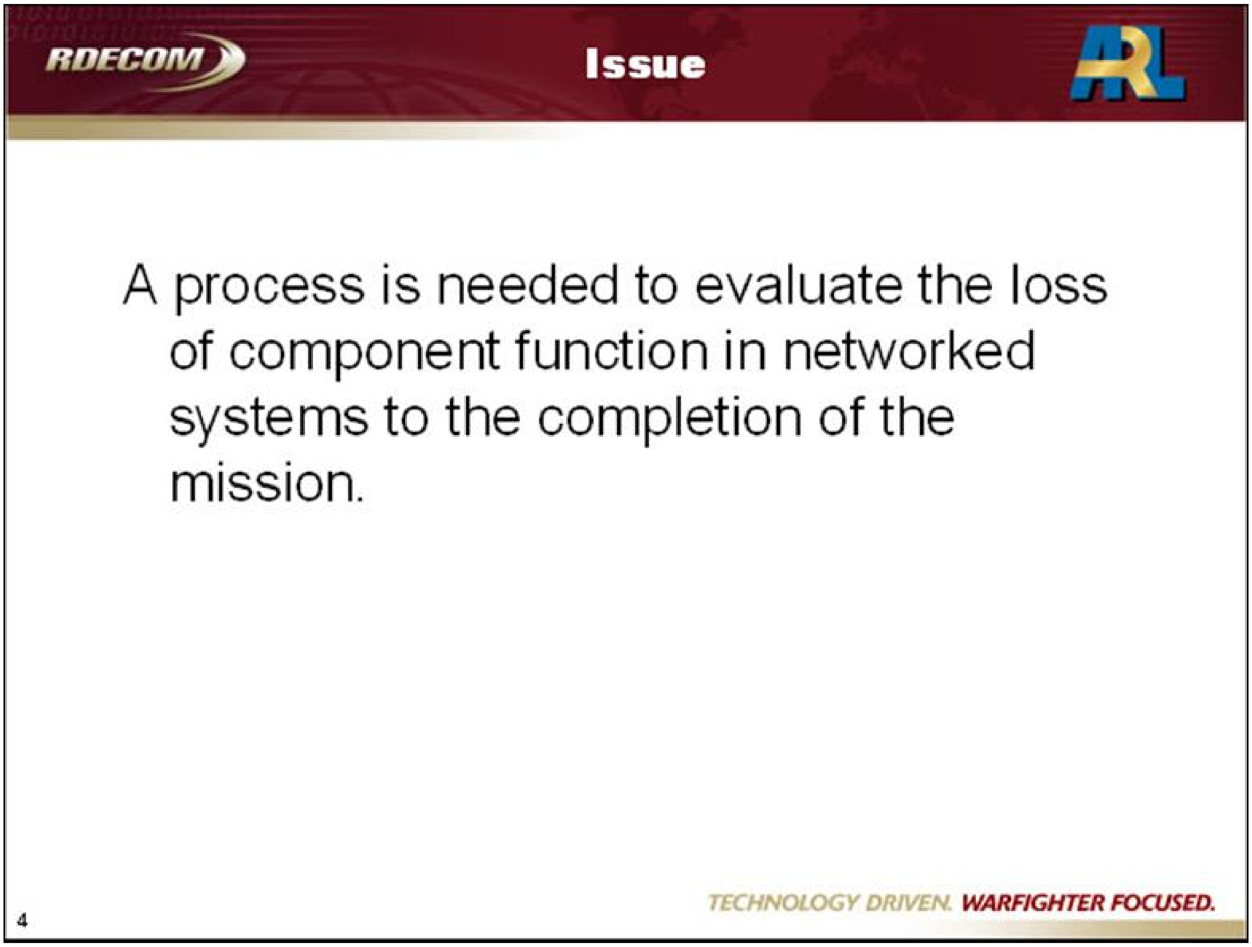

Figure 4. Identification of the primary issue.

The primary issue that SCAP is intended to address is shown in figure 4. If a system, or a group of systems known as a SoS, receives damage significant enough to render critical components dysfunctional, what will be the impact to the system's capabilities, as well as the ability to complete of the required tasks and missions?

Figure 5. An established industry process.

Depicted in figure 5 is a generic view of the approach as used by the consumer-product industry to correlate the needs of the user to the design of the system. When a user has identified what mission (goals, job, etc.) they want to accomplish, an analyst will determine what tasks are required to complete that mission. For the sake of this presentation, an "analyst" is defined as any individual who is analyzing a system utilizing SCAP. After the required tasks are identified, the analyst will then identify what functionality would be required to complete each task. This functionality is what each portion of the design will have to do and is an observable performance of some kind. The analyst will then identify what components will produce each functionality.

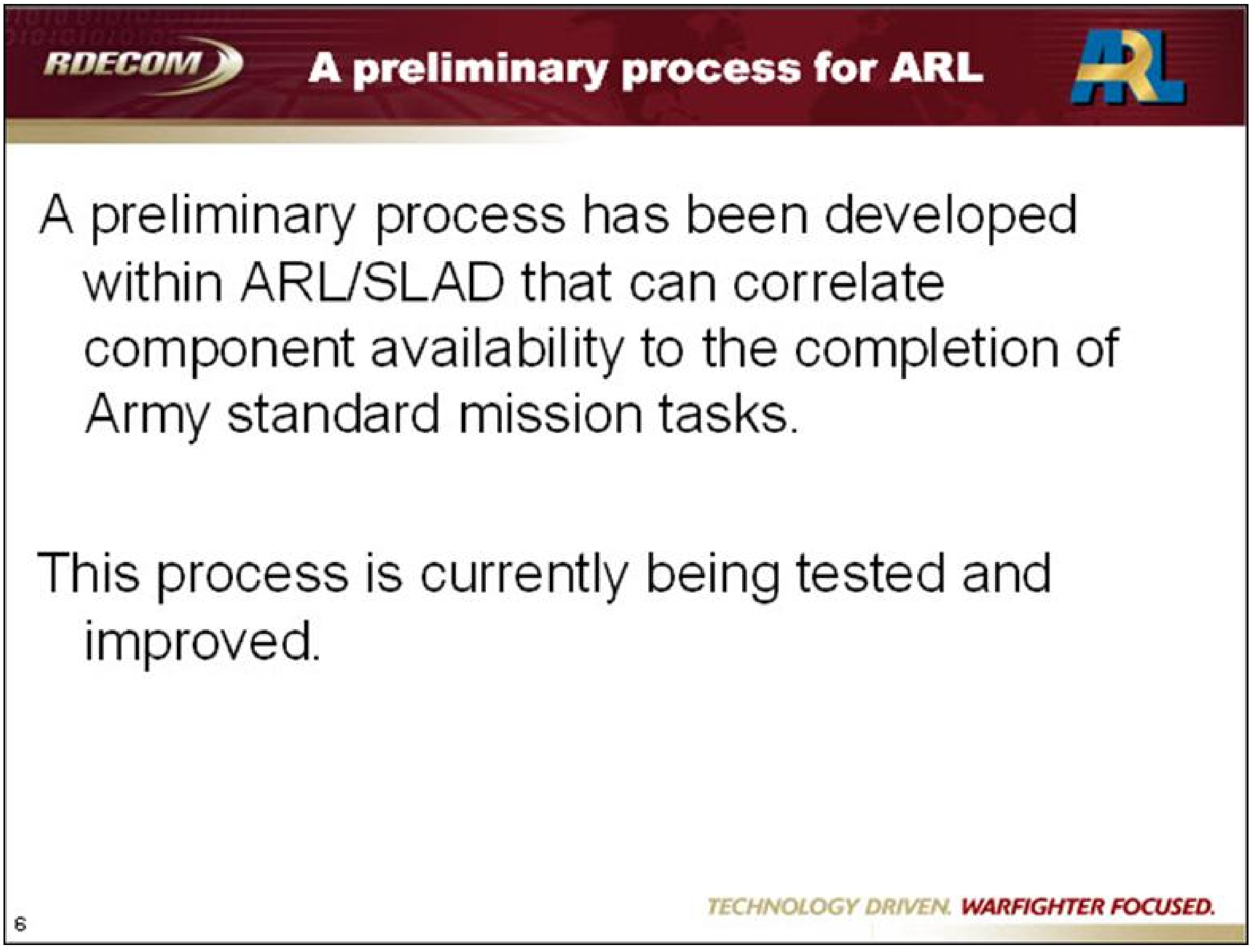

Figure 6. A preliminary process for ARL.

By utilizing relevant private industry experience, existing government efforts, and applying concepts from systems and reliability engineering, the consumer product process has been adapted to fit with efforts already in use by various Army organizations. The adapted process is known as SCAP.

To test the preliminary SCAP methodology, two trials are underway at ARL/SLAD. The prominent trial is conducting a vulnerability analysis of a common ground vehicle using the SCAP methodology and is leading the development of vulnerability outputs from our traditional simulation tools that are in the terms of system capabilities (SCs). The second trial is on a ground vehicle of much higher complexity. The intent of the second trial is to determine if the investment of resources—for personnel, time, and computing hardware—would be prohibitive for this form of analysis.

The synopsis of the preceding two discussions is depicted in figure 6.

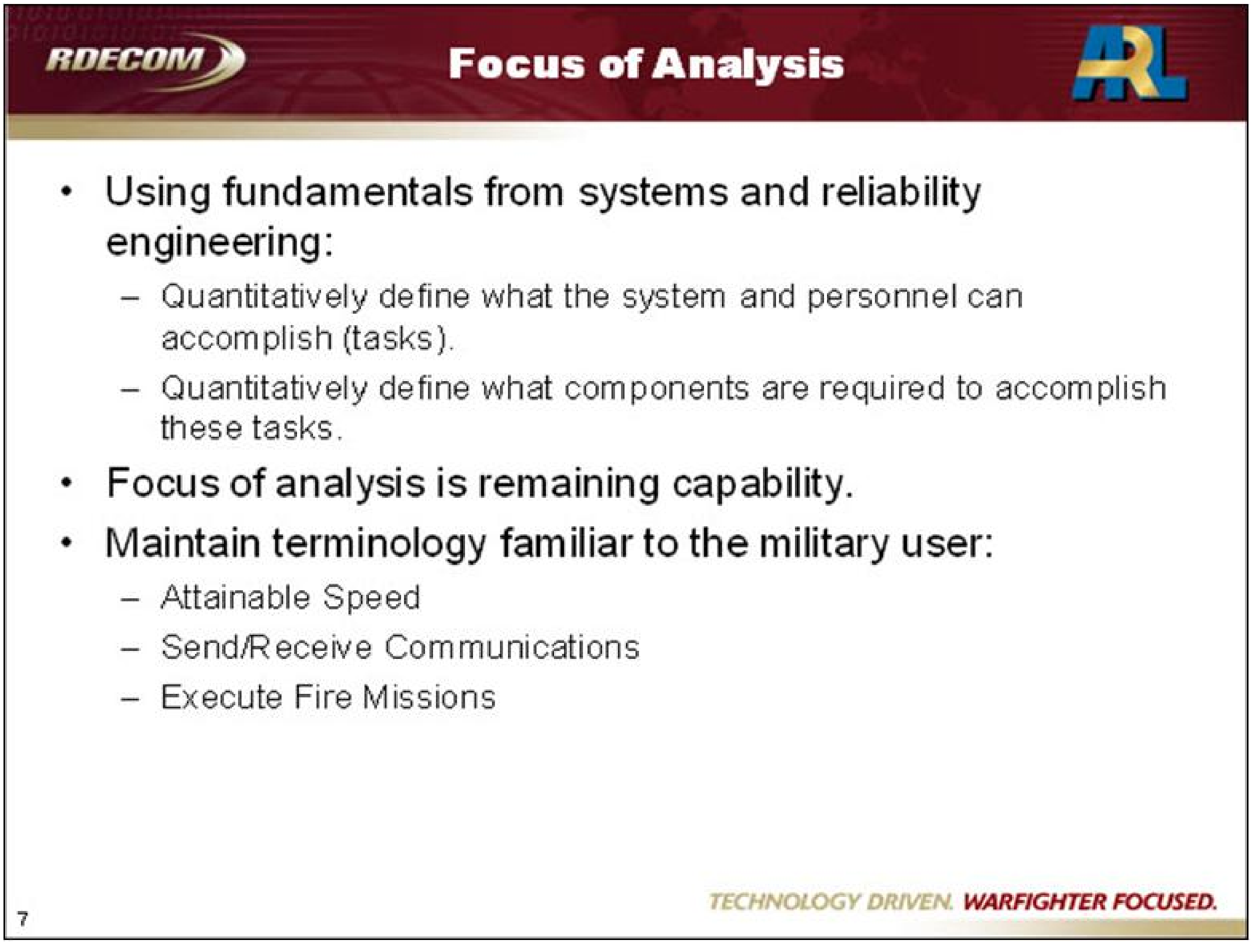

Figure 7. The focus of the new methodology.

The focus of the emerging SCAP methodology is depicted in figure 7.

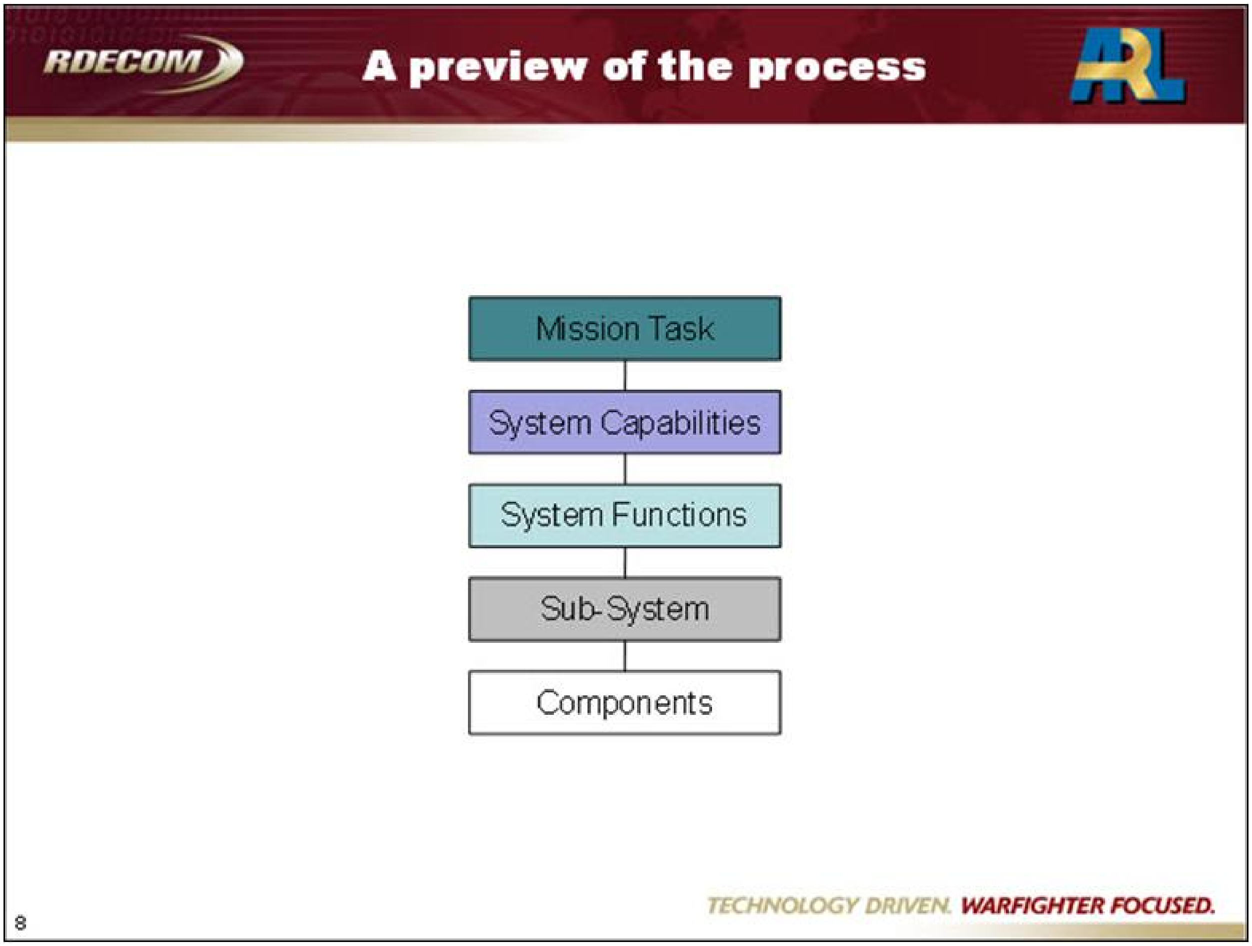

Figure 8. A preview of the process.

Depicted in figure 8 is the foundation of the SCAP methodology. At the bottom are the two layers that immediately relate to the design of the system: the components and the sub-system. The top layer, representing the mission task, is from the Army Universal Task List (AUTL). The following slides will explain each of these levels in more detail.

A pneumonic that was recently developed to describe these layers is: "When Components are assembled into Sub-Systems, they produce the Functions that provide the Capability to complete the Task."

Although SCAP was developed for the vulnerability analysis of a ground combat vehicle, early discussions and trials during methodology development indicate potential use of SCAP in a SoS (or force-on-force) simulations. The theory is that this map may be able to identify what components are critical on individual systems based on the mission performance of the networked systems after an attack. These same conversations indicate that SCAP could be used to map the results of a threat interaction into a mission scenario—otherwise known as a vignette—and determine how well the family of vehicles can perform their task after an attack.

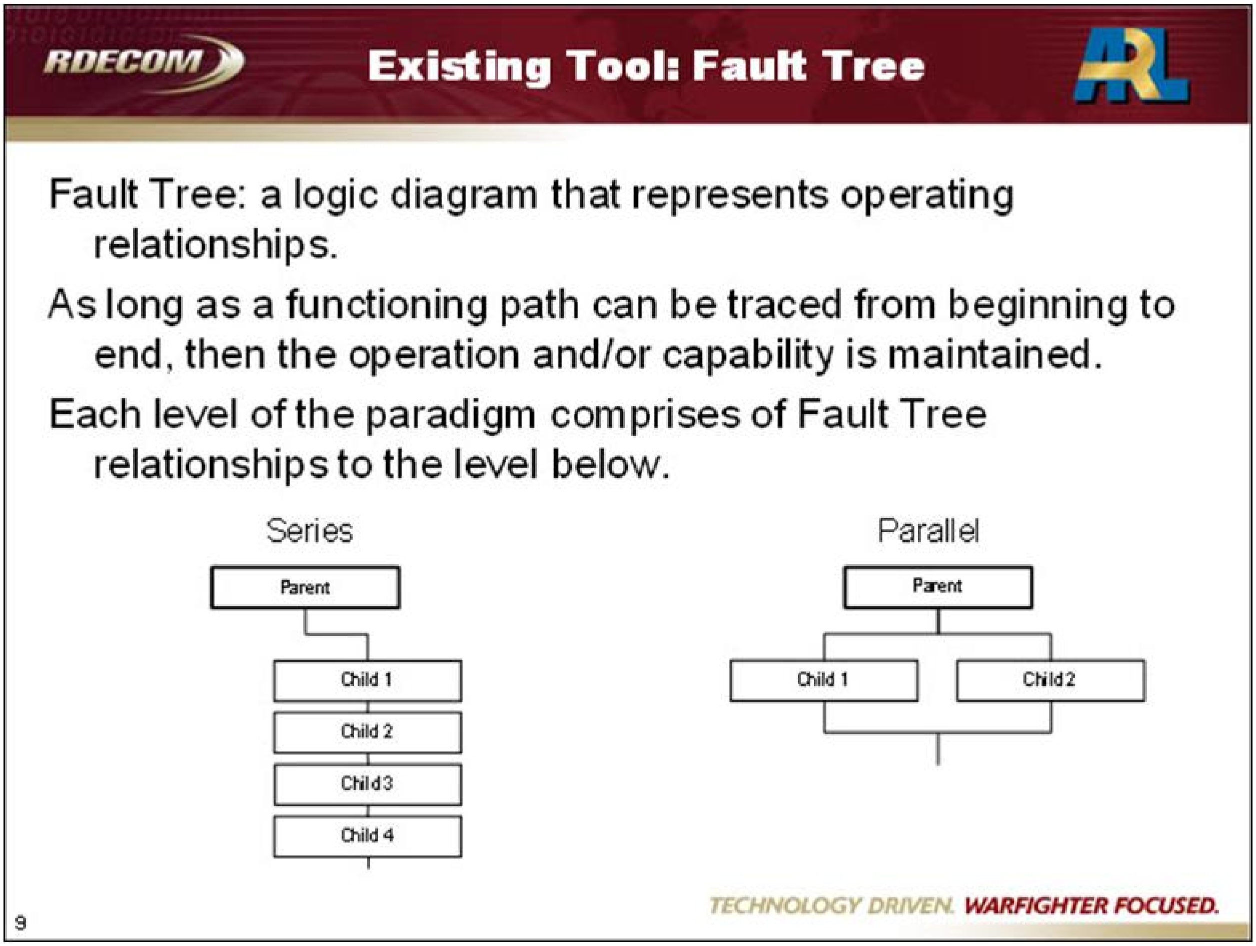

Figure 9. The use of an existing tool: fault trees.

To map between the layers of SCAP, a tool known as the fault tree is required. A fault tree, also known as a deactivation diagram, is a logic diagram the represents the operating (functional) relationships of the critical components within the design of the system. As long as a functioning path can be traced from the beginning of the diagram to the end, then the operation and/or the capability represented by the fault tree's "parent" element is maintained and available. If this was the case, then we say that the parent is functioning as intended. However, if the trace through the fault tree cannot be maintained due to a dysfunctional child, then the parent is dysfunctional as well.

There are two fundamental forms of a fault tree, and both forms are depicted in figure 9. The first is a series tree, which means the dysfunction of any child on the string will result in a dysfunction of the parent. Note that if multiple children are dysfunctional, there is no additional severity of the dysfunction of the parent than if only one child was dysfunctional.

The second form of the fault tree is the parallel tree. In this case, the children share the functionality represented by the in the fault tree relationship. To render the trace through the fault tree dysfunctional, all children on the parallel branches must be rendered dysfunctional.

It is possible to combine series and parallel relationships in a single fault tree. This combination approach can allow for the creation of highly complex relationships within a design.

Within SCAP, a functional child and parent are represented as a binary value of “1”. If a child or a parent is dysfunctional, then they are represented as a binary value of “0”. This allows for a representation of “available” and “unavailable” in statistical and mathematical representations of the maps. This convention is able to change based on the tools that are used to complete an analysis or simulation, but will be maintained for the rest of this presentation.

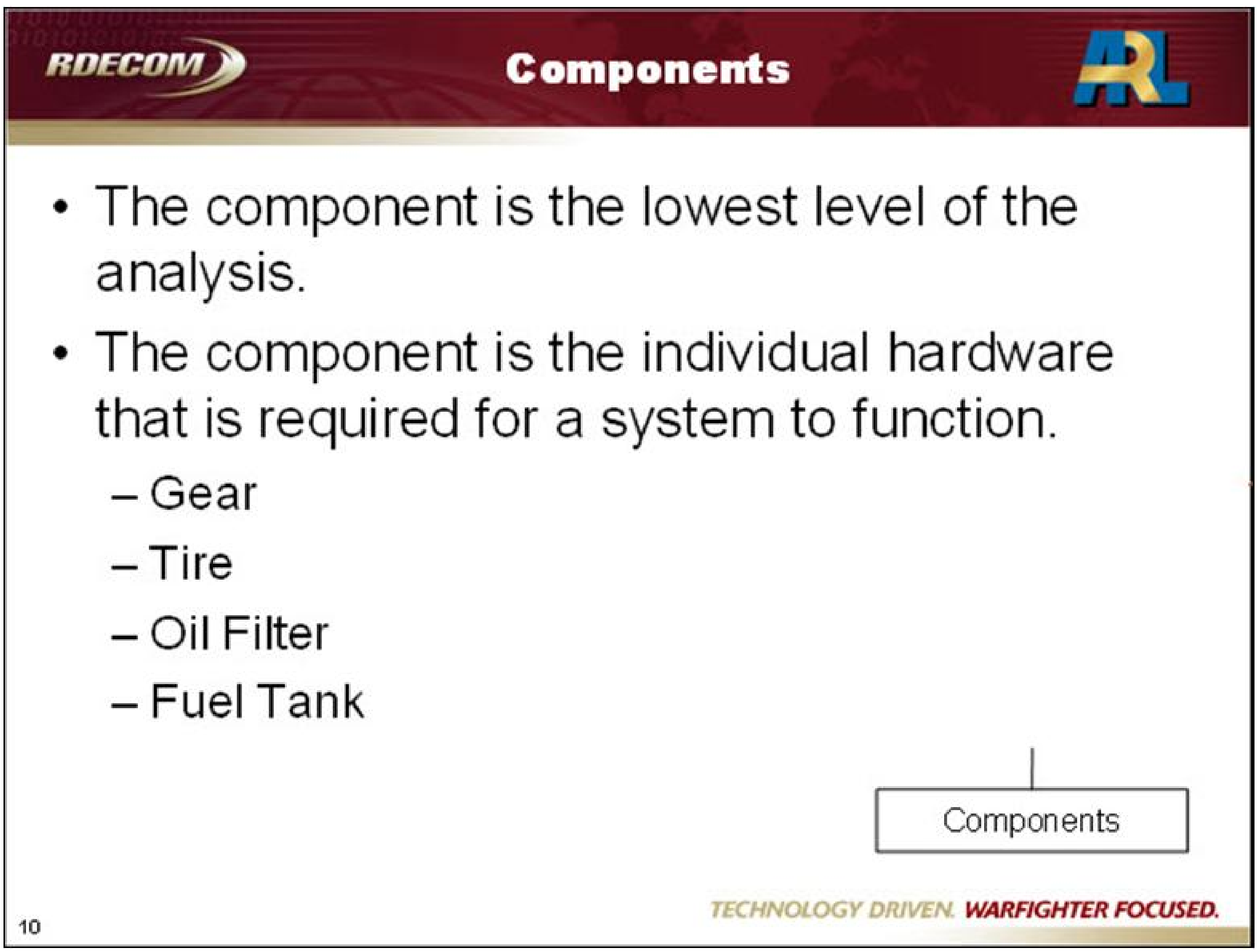

Figure 10. Definition of components.

The components are the lowest level of the analysis. They are the physical parts of the system being analyzed. For most vulnerability analyses, data of some level of fidelity is known about the design and the function of the components of the system.

Some sample components are listed in figure 10.

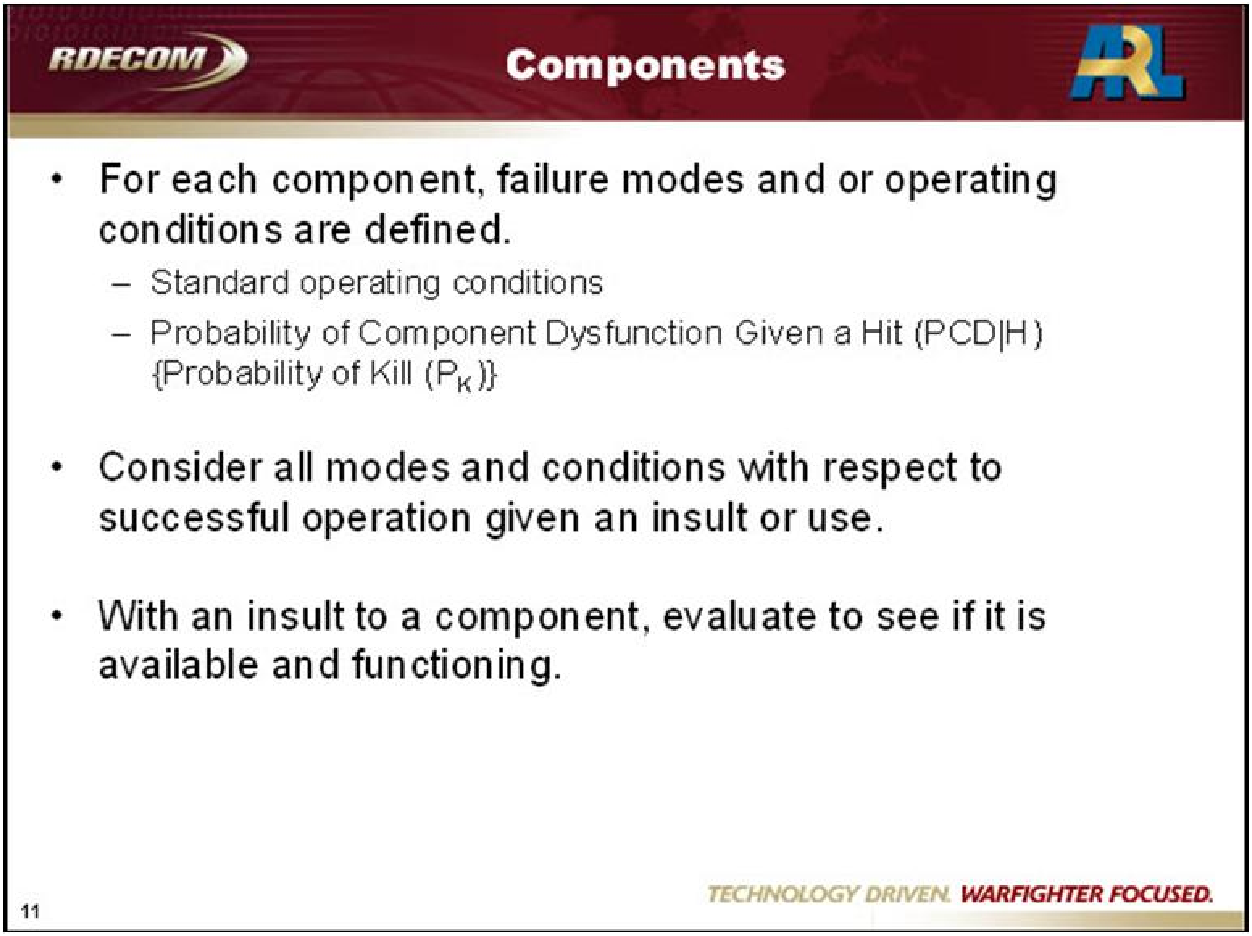

Figure 11. Components: further discussion.

Figure 11 depicts the highlights of a further discussion of components. Existing methodologies and tools used in vulnerability analysis are able to predict component losses based on an interaction with a known threat. In vulnerability models of a ground combat system, the Probability of Component Dysfunction Given a Hit ($P_{cd|h}$) and Probability of Kill (P_K) represent the probability that the component will be rendered dysfunctional, or "killed", when a threat is applied to the components. If the component is found to be dysfunctional in a SCAP application, a value of "0" will be assigned in the map.

In SCAP, a component can be rendered dysfunctional by any means, not just by ballistic insult. In other words, the fault tree doesn't track why a component will be dysfunctional, just that it is. This allows for additional failure modes that are not typical in the traditional vulnerability methodologies, such as:

- Environmental effects.
- A component operating above or below its standard operating conditions.
- Reliability failure.

- Nuclear, chemical or biological contamination.

This will also allow for the map generated by applying SCAP to a system to be useful in many forms of analysis beyond the scope of ballistic vulnerability.

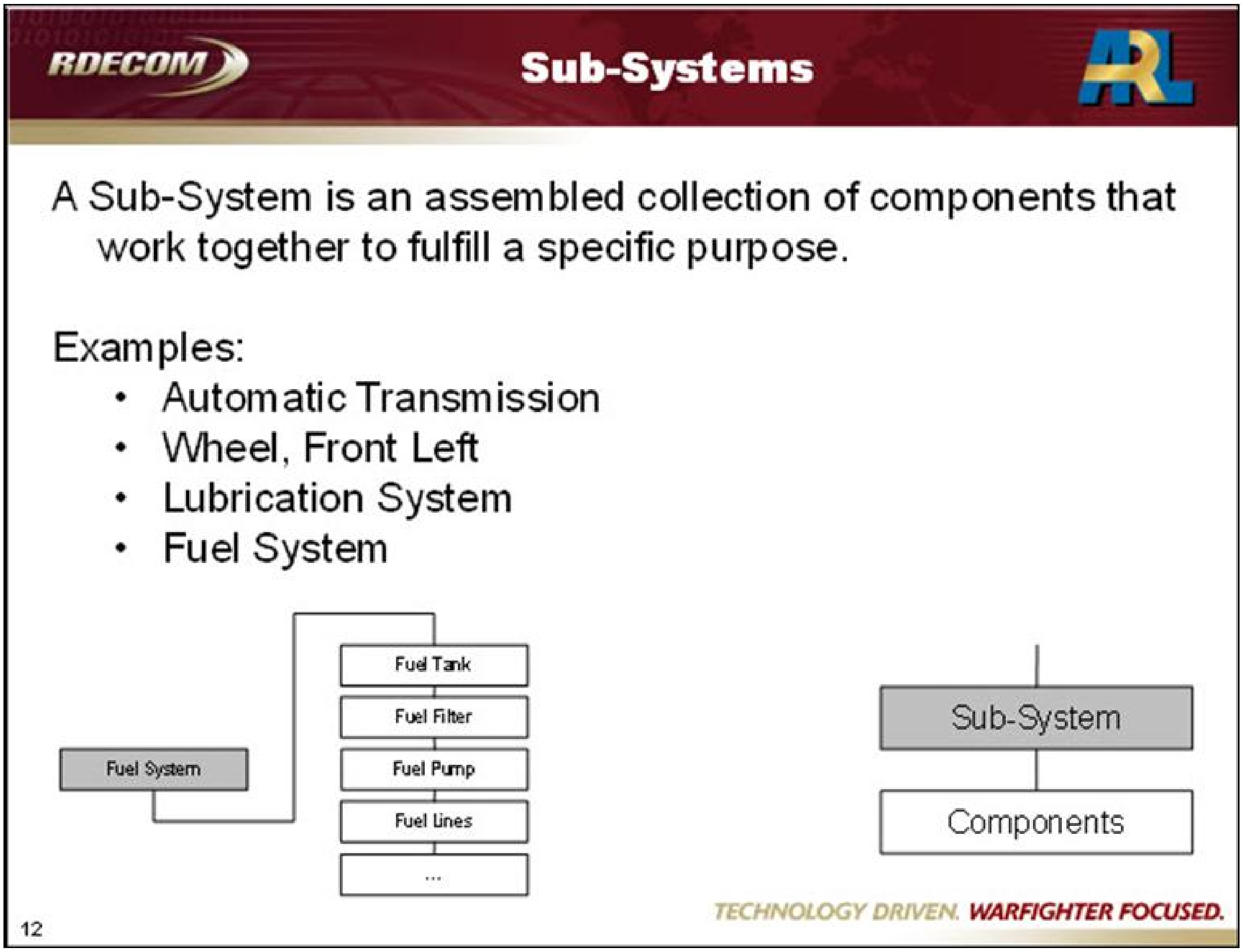

Figure 12. Definition of sub-systems.

A sub-system can also be a complex component, such as a fuel pump. Note that a sub-system may contain both components and sub-systems, but components cannot contain sub-systems. This is the only place in the map that two levels may be mixed within the fault trees. Figure 12 depicts the sample of a sub-system.

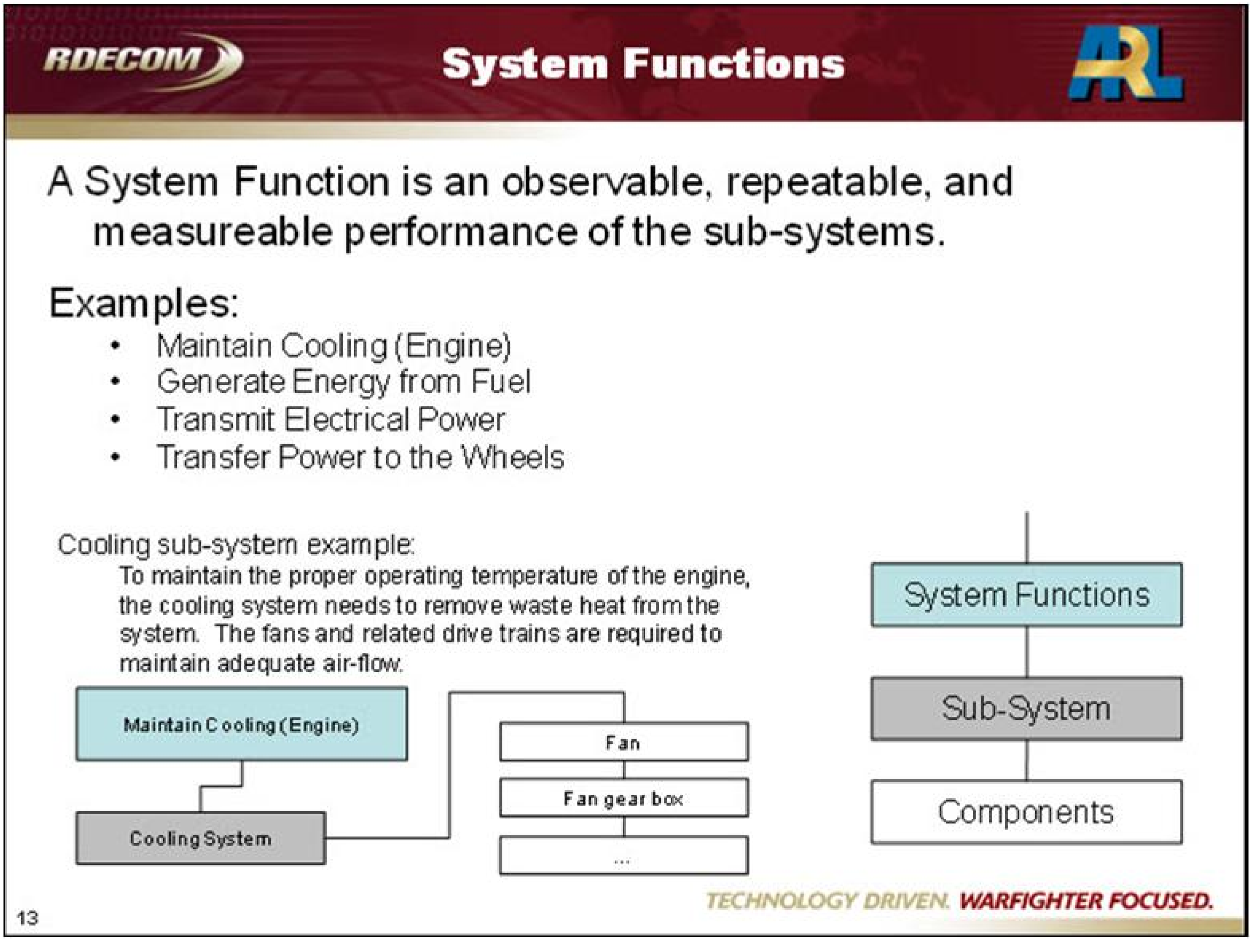

Figure 13. Definition of system functions.

A system function is defined in figure 13. The children within a system function fault tree can be either sub-systems or other system functions. It is very important to note that one should never include a child represented by a system function with another child represented by a sub-system within the same fault tree for a single system function. A system function will have only either other system functions or sub-systems as immediate children in the fault tree. This is essential to maintaining the integrity of the data analysis when all fault trees are compiled into a large-scale model.

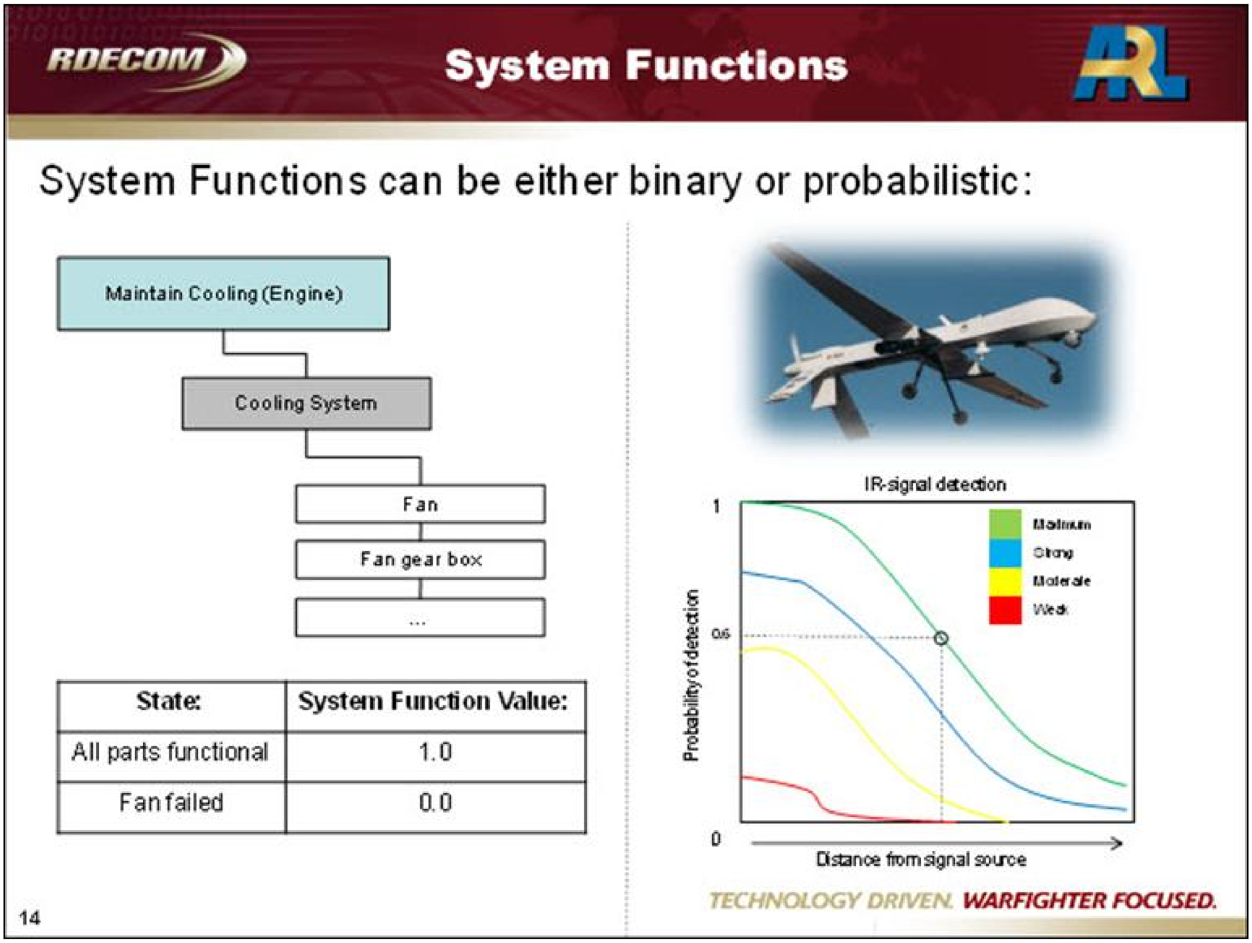

Figure 14. Representation of system functions.

A further discussion of system functions occurs within figure 14. In most mechanical systems, the representation of the system function availability will be a binary set: either functional or dysfunctional. Early feedback from the lethality analysis community has introduced the concept of probabilistic system functions (PSF). For a PSF, if all components and sub-systems are functional, then the probability of a system function being available will be based on some conditions of the system.

In the abstract example of an infrared (IR) sensor system, it is assumed all the components are fully functional; therefore, the IR signal detection sub-system (IR sensor system) is fully functional. To determine if the system function “detect IR signal” is functional or dysfunctional, conditions, such as the strength of the signal—weak to maximum—and distance to the signal will determine the probability of functional or the probability the system will function as intended. If a signal is too weak to be detected, the system function “detect IR signal” would be dysfunctional even if all the components are functioning correctly. In the example shown, it can be seen that a “maximum” signal will be detected about 60% of the time for a given distance for the sensor of interest. Therefore, about 60% of the time when these conditions exist the “detect

IR signal" system function will be functional, and about 40% of the time it will be dysfunctional. Note that sometimes the probability of a functioning system function can be modified if the conditions are changed in some way. In a theoretical case of electronic warfare (EW), the presence of flares could provide a stronger IR signal than the intended target. In this case, the probability of detection would decrease as the sensor may detect the wrong signal, thus rendering a system function as dysfunctional even though all components are functioning as intended.

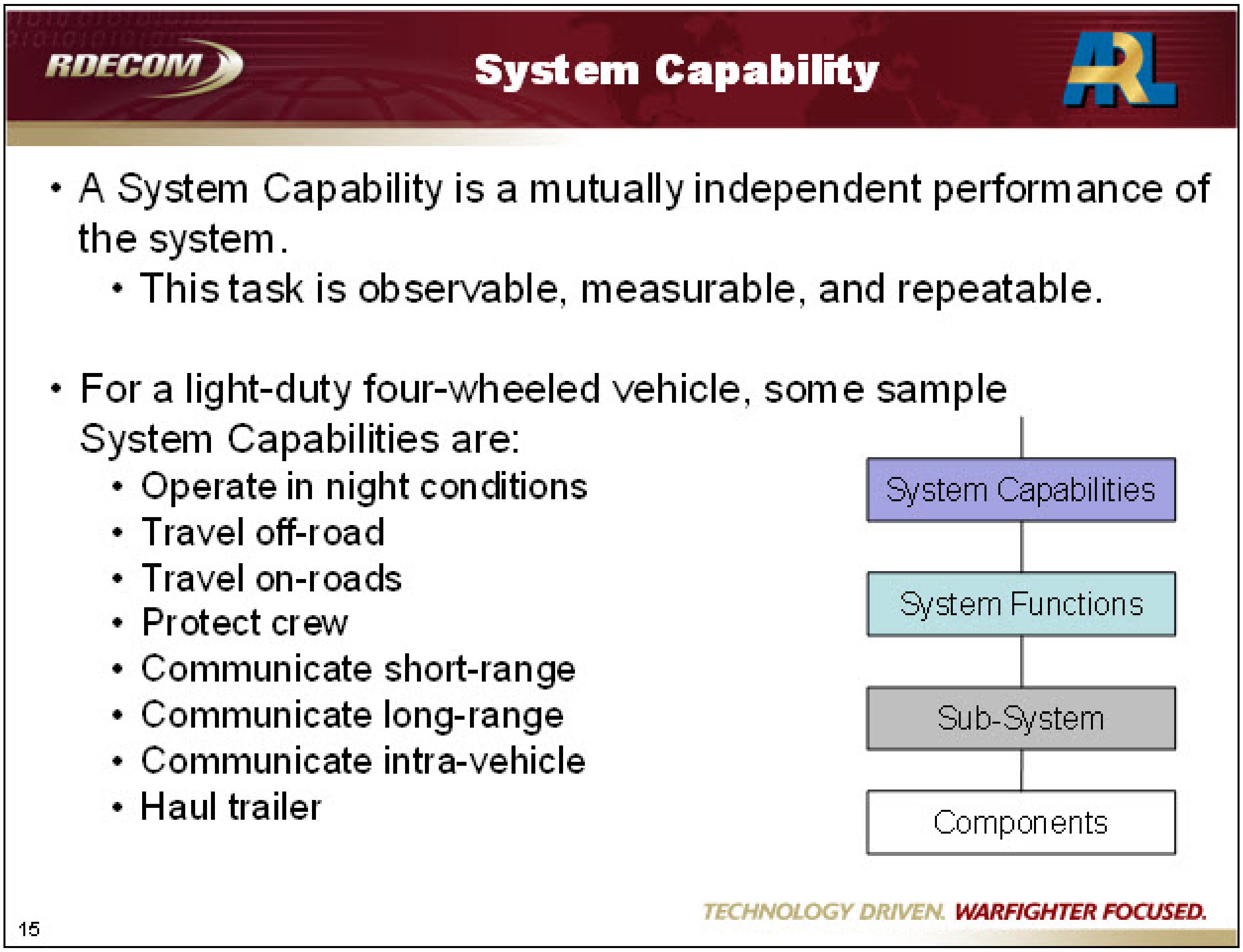

Figure 15. Definition of SCs.

The SC is defined in figure 15. The children of a SC fault tree are the required system function to produce that SC. Note that these SCs are in a language familiar to the military user, e.g., attained speed, engagement range, protection limits.

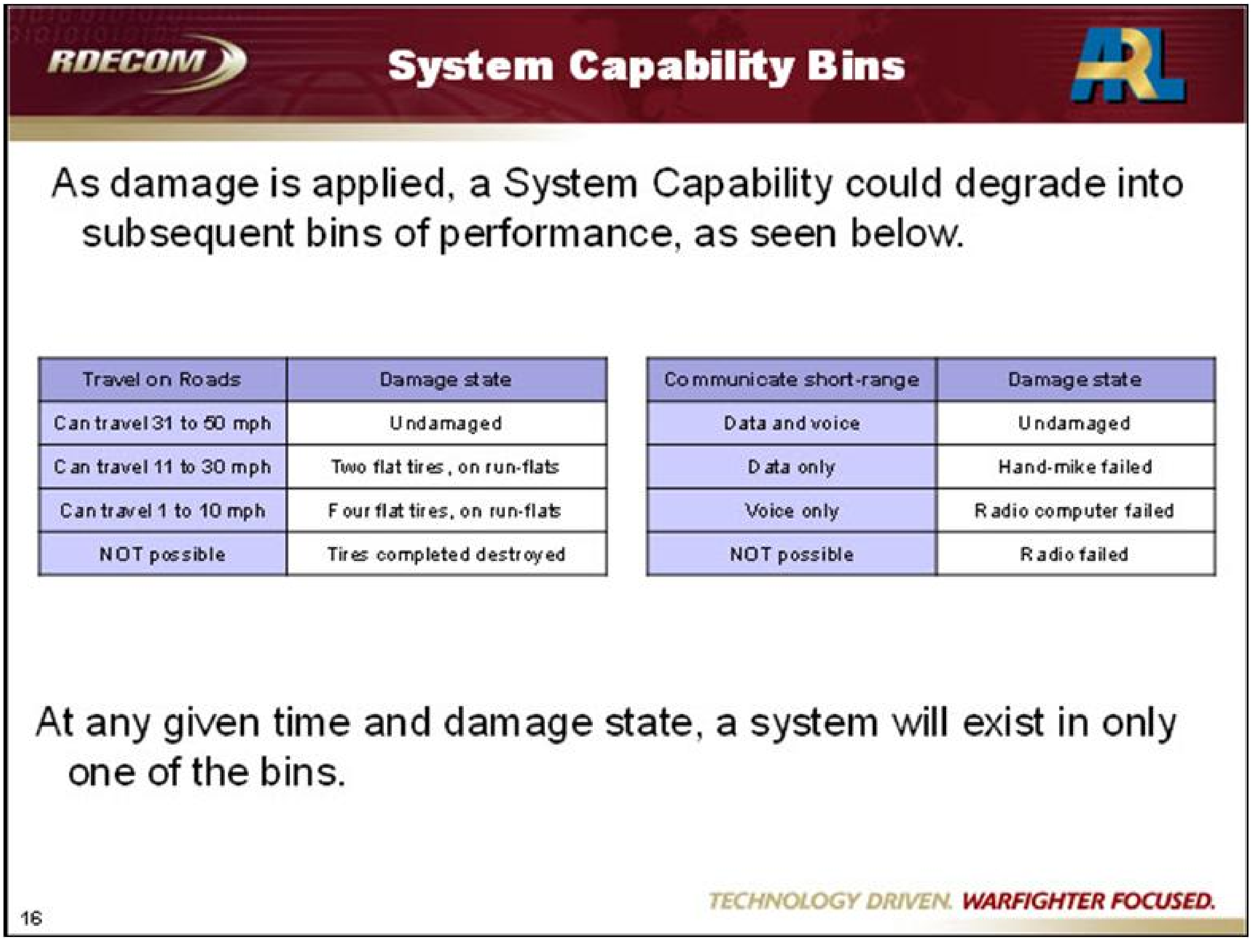

Figure 16. SC bins.

When compiling SC from the required system function, the initial effort will map top performance bin, otherwise known as the undamaged state. After the top performance bin is compiled, it is easier, based on industry experience, to compile the lower performance bins. These lower performance bins are usually achieved by copying the top level bin and removing system function as required. The levels of the bins are dependent on the design of the system and on the context of the capability. For example, the speed of a wheeled vehicle is dependent on whether it is either two- or four-wheel drive and in the context of either on- or off-road. An example of SC bins is depicted in figure 16.

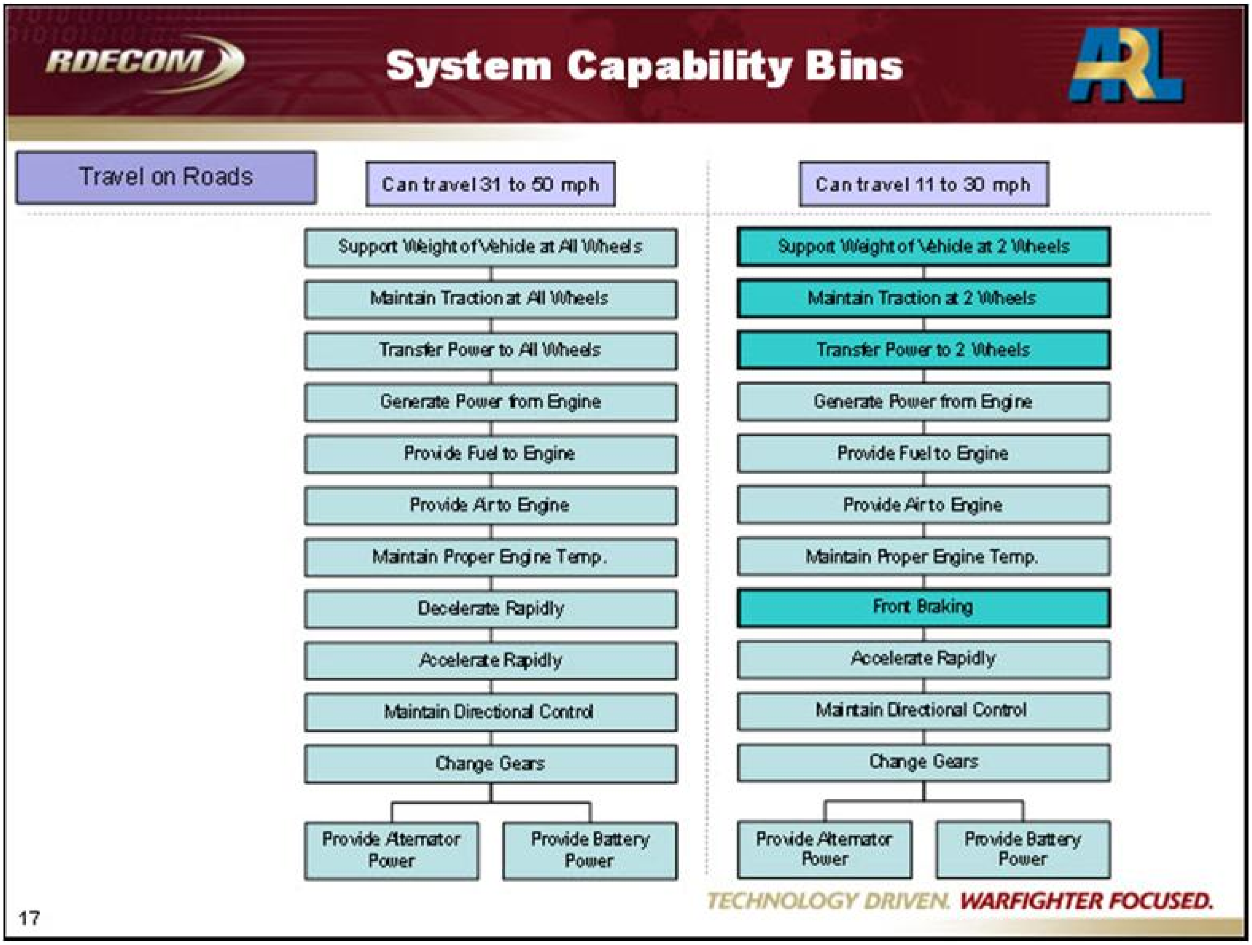

Figure 17. Sample of SC bins.

The differences between two SC bins are depicted in figure 17. This example is for a theoretical light-duty pickup truck found at a used car lot. Note the difference between the two bins. The highlighted blocks in the "can travel 11 to 30 mph" depict which system functions are either missing or different than the top performance bin, the "can travel 31 to 50 mph".

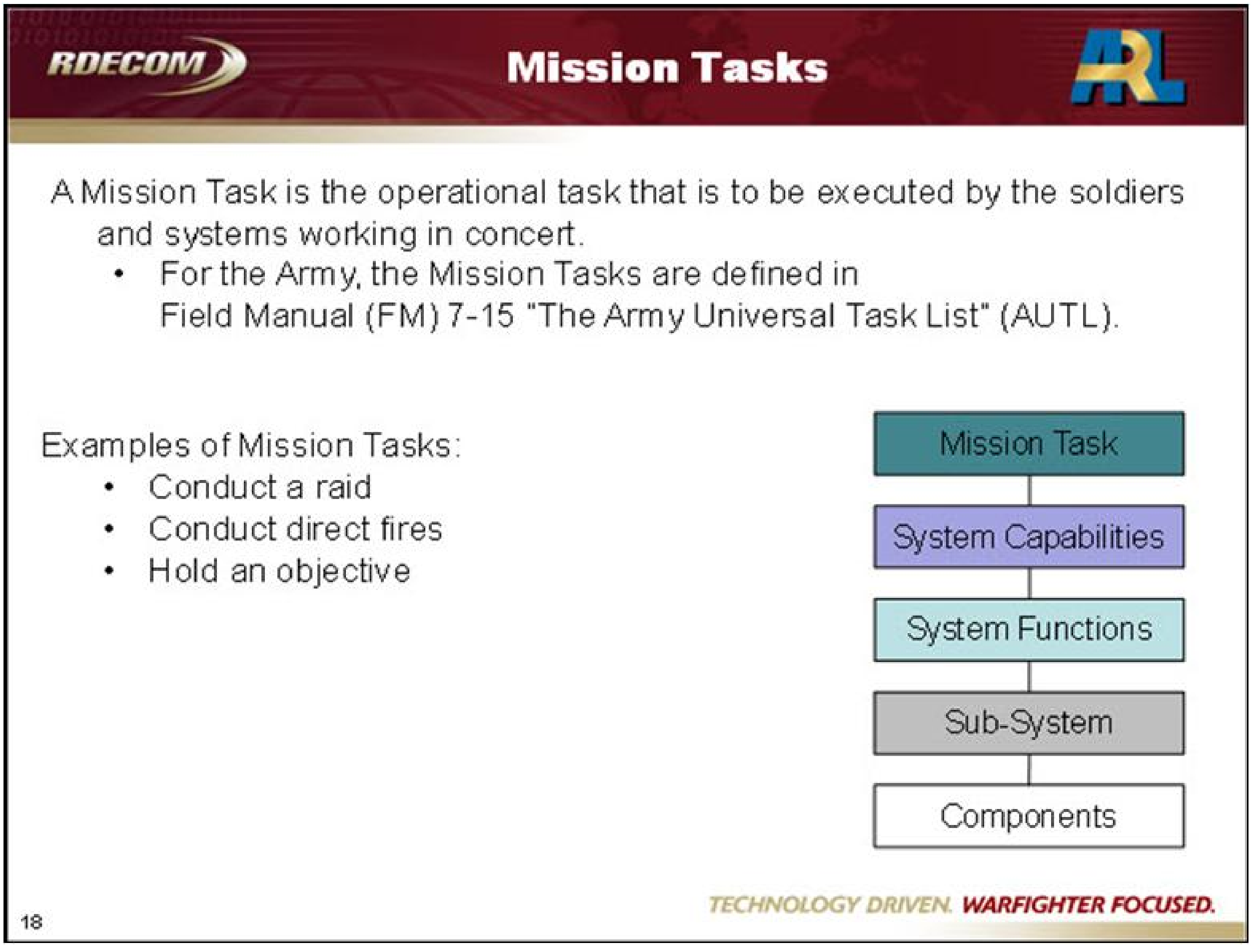

Figure 18. Definition of mission tasks.

Mission tasks are defined in figure 18. All mission tasks are composed of a set of required SC.

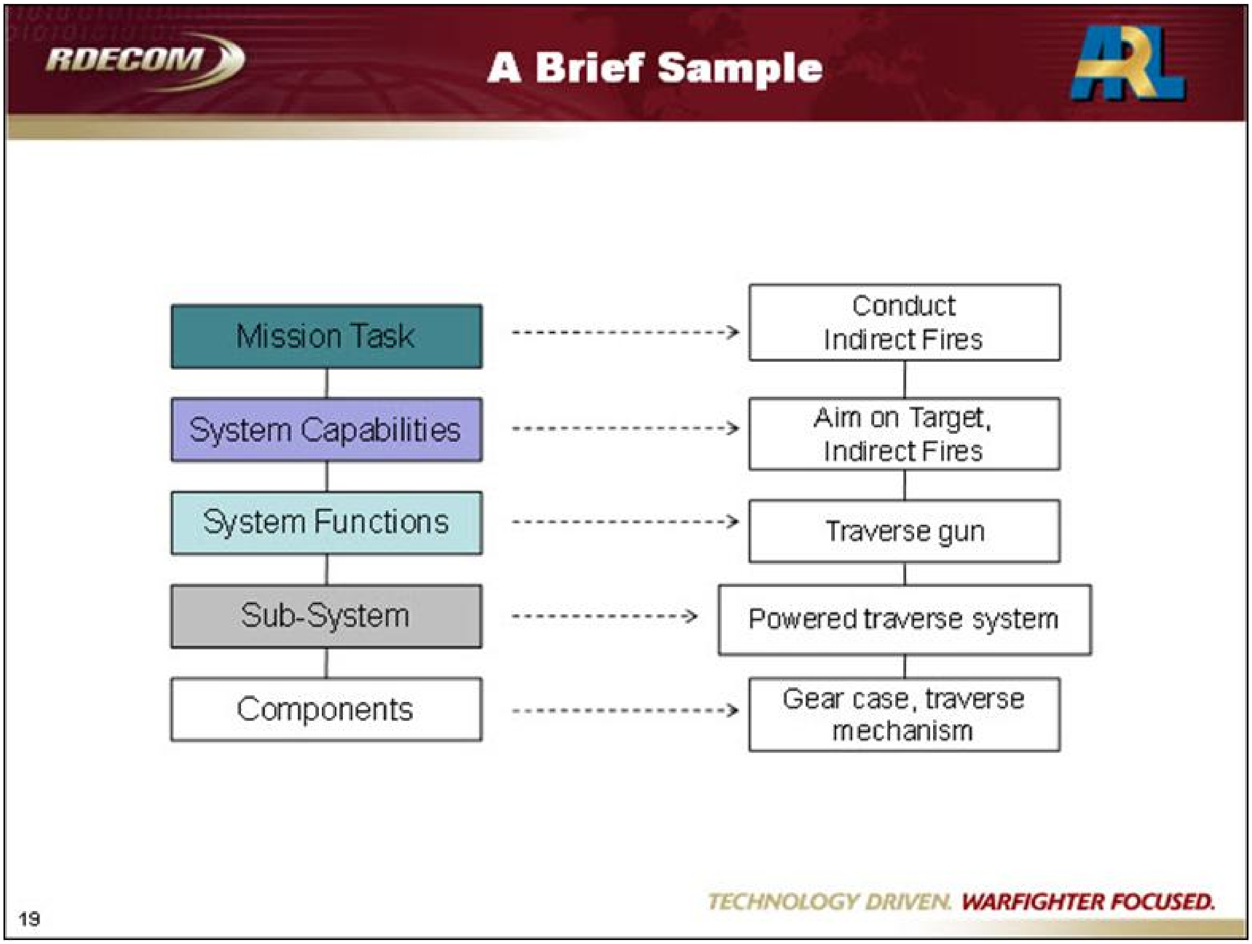

Figure 19. A sample SCAP map.

Since all five levels of the SCAP methodology are defined, a sample map is depicted in figure 19. This map shows how components can be used to define the accomplishment of a mission task.

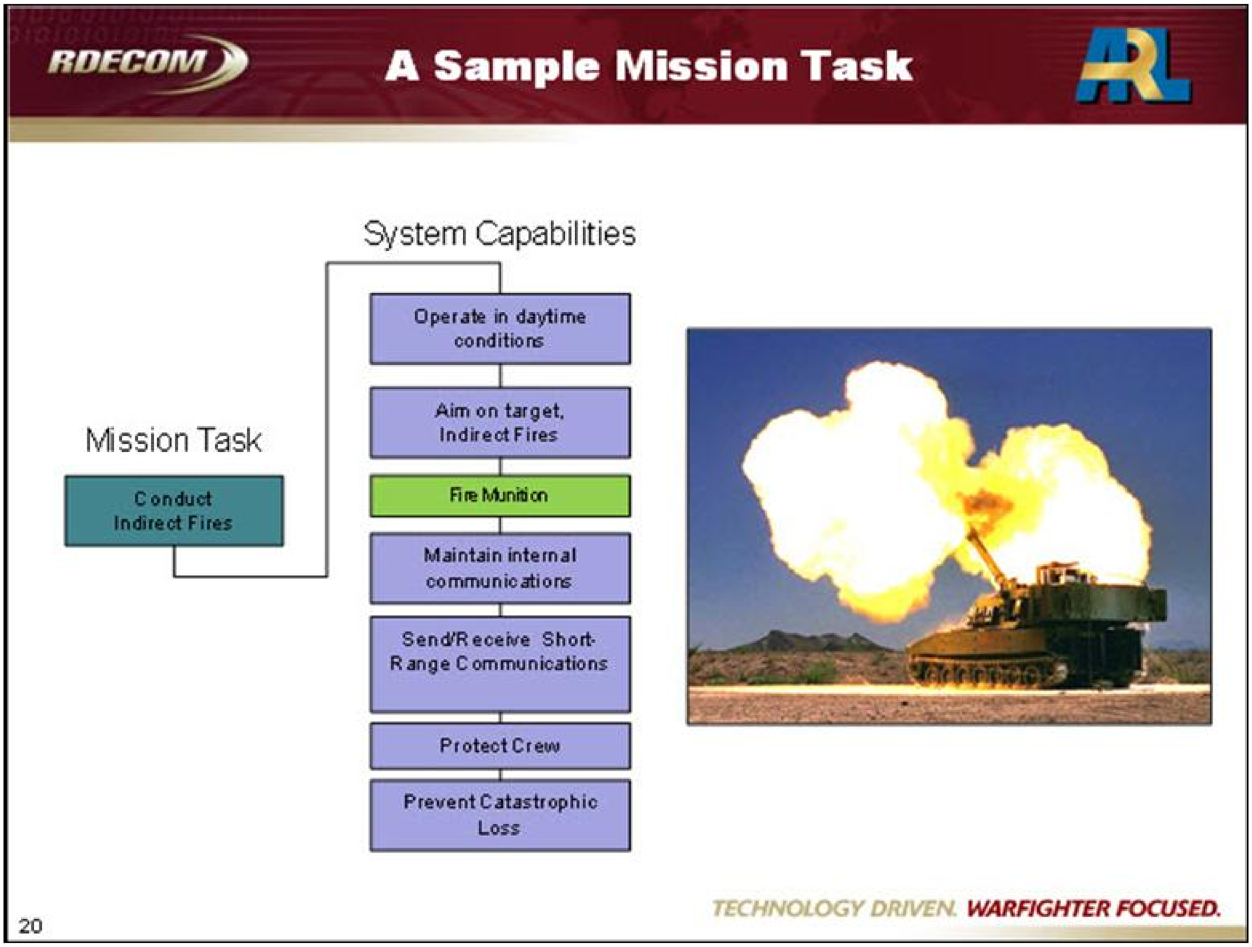

Figure 20. A sample mission task decomposition to SCs.

Depicted in figure 20 is a theoretical example of a self-propelled howitzer (SPH). The SPH has a mission to support troops with indirect fire support, hence the AUTL "conduct indirect fires". In the fault tree that is compiled for this example, "fire munition" is green because it highlights the SC of interest from the picture shown.

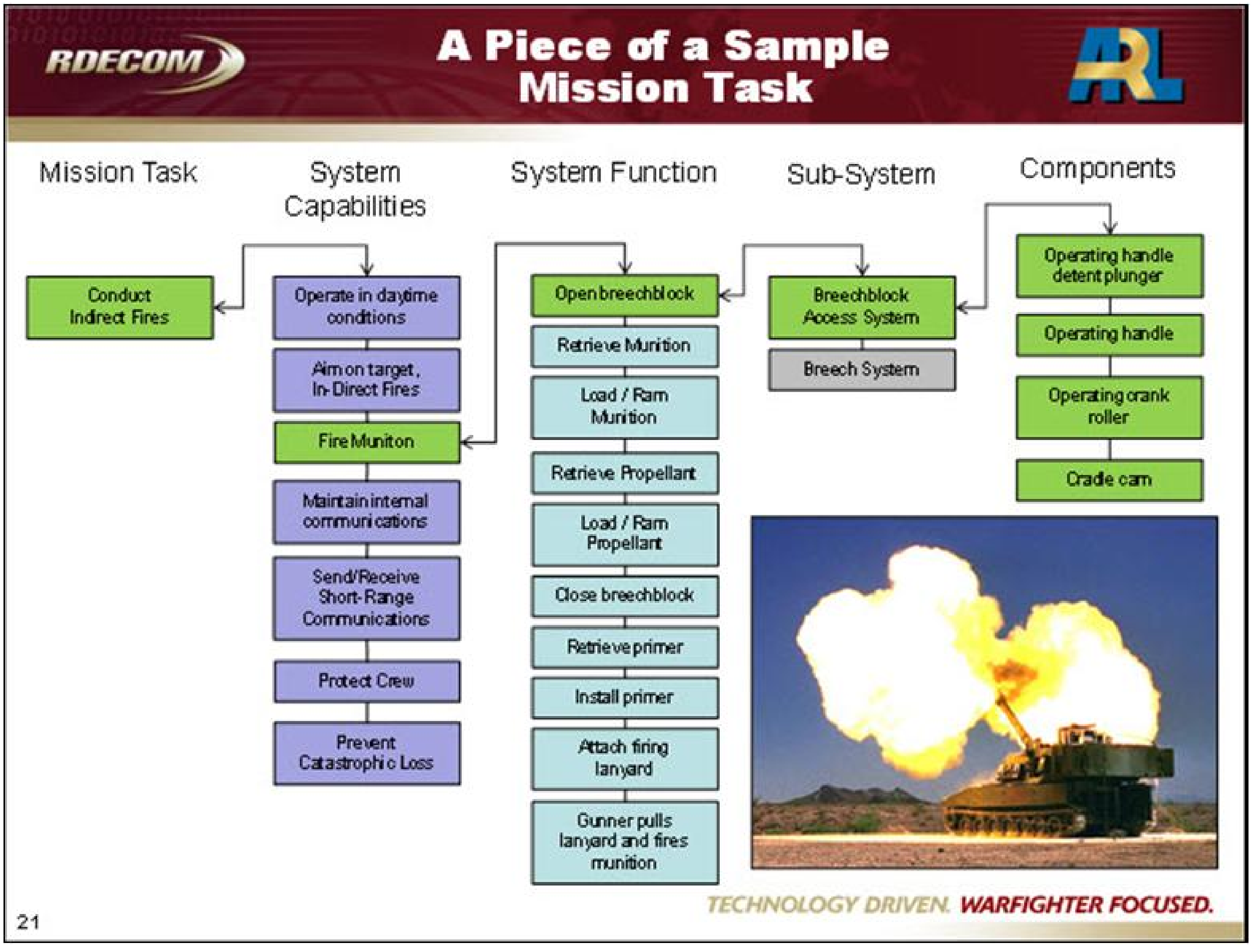

Figure 21. A sample of the map from mission task to components.

The multi-layered tree depicted in figure 21 is a sample of the map for a theoretical SPH. This map shows how the components required to open the breech of the cannon are related to the SC of "fire munition" and the mission task of "conduct indirect fires". For the sake of simplicity, the SC bins are not depicted in this example, particularly for the SC of "fire munition".

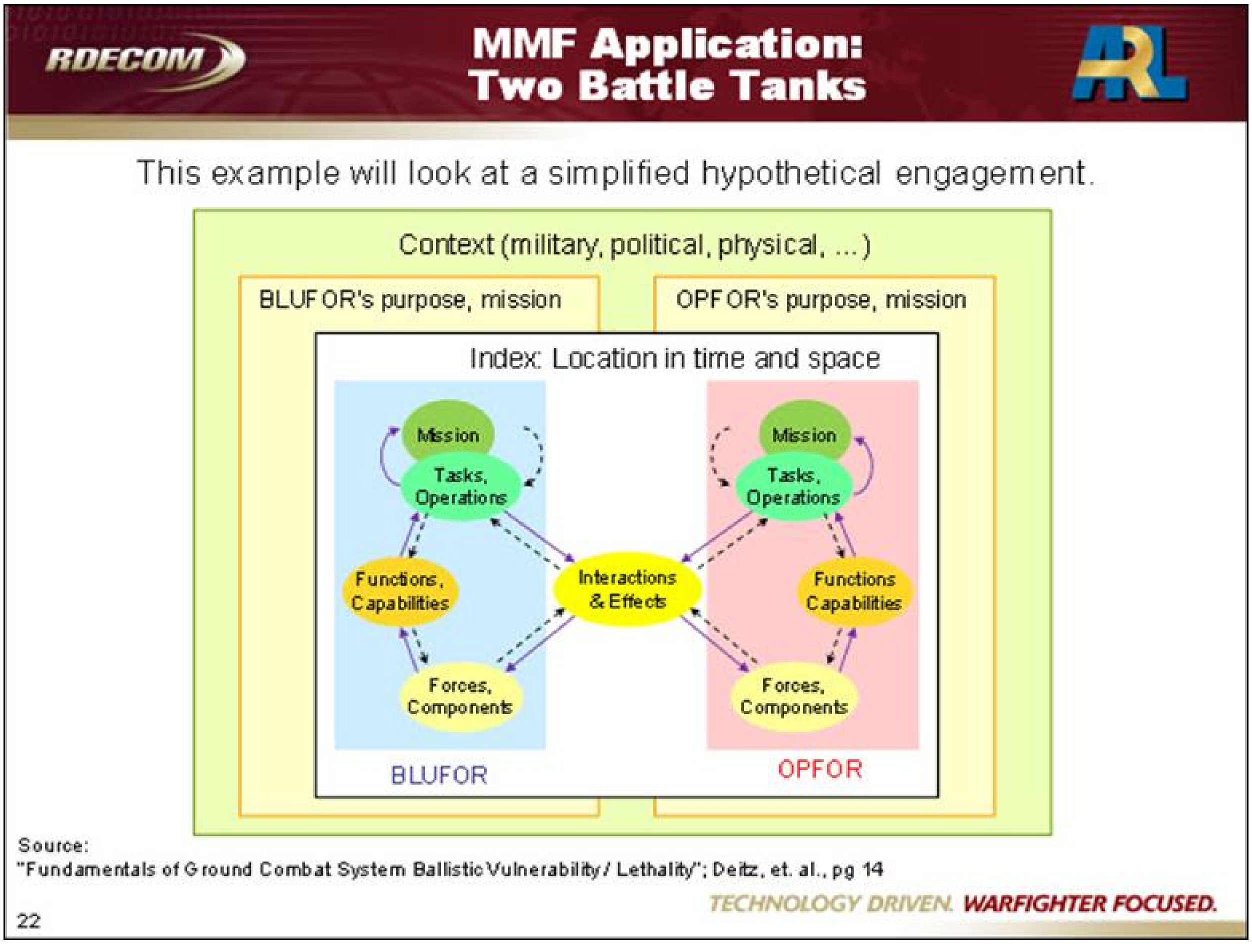

Figure 22. An application using MMF−two main battle tanks.

The second example in this briefing will review how SCAP can be used to model the relationships between two systems in a force-on-force engagement. To represent the actions and timing in this engagement, the Missions and Means Framework (MMF) will be employed in collaboration with SCAP. MMF is a well-documented construct and is a foundation principle of Dietz, et al.[1] The seven levels of MMF are depicted in figure 22. As MMF had been discussed in earlier sessions of the conference, as well as previous conferences, it was assumed the audience was already familiar with the framework. Therefore, the details MMF were not discussed in this presentation at the conference.

For the benefit of this report, a very brief review of MMF follows that was not covered at the conference. A full treatment and explanation of MMF can be found in Dietz et al.[1] By studying MMF as depicted in the second chapter of the above-mentioned book, it appears MMF is a construct of three underlying paradigms. The first paradigm will define the relationships of a system's component damage state, through a system's capabilities, to the system's combat

[1] Dietz, P.; Reed, H.; Klopcic, T.; Walbert, J. *Fundamentals of Ground Combat System Ballistic Vulnerability/Lethality*; American Institute of Aeronautics and Astronautics, Inc.: Reston, VA, 2009.

utility. The second paradigm is how do systems, as they engage and interact with each other, either improve or degrade components and capabilities of another system via their respective combat utility. The third paradigm is focused on the larger scale operations. As the component damage state and the combat utility of the hardware changes through interactions, the effects will integrate into the higher-level relationships that will affect changes to the mission, purpose, and context. It can be noted that MMF is not a static process, but rather a dynamic application of ever-changing and potentially complex relationships between systems.

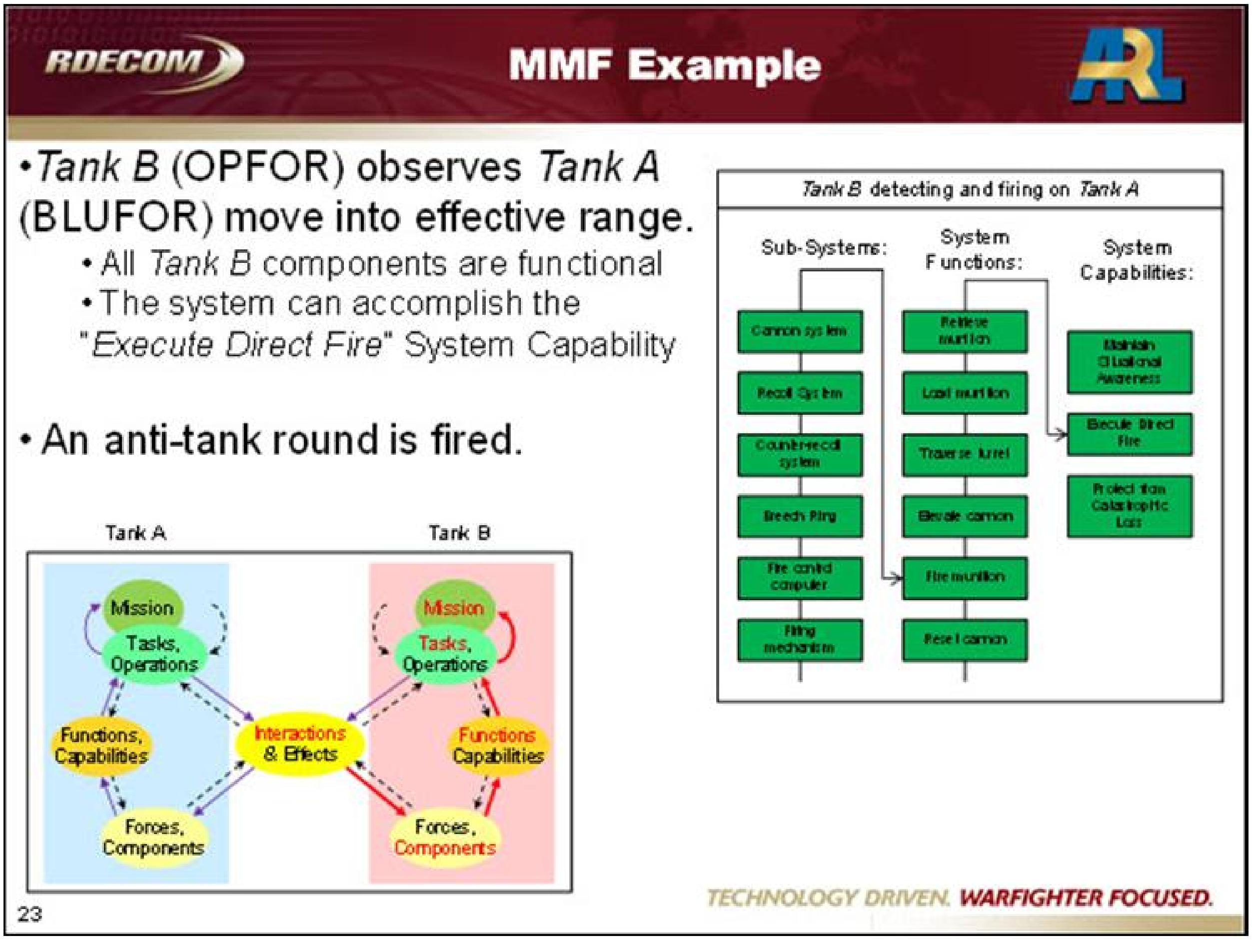

Figure 23. MMF Example–the first round is fired.

The initial index of this engagement is depicted in figure 23. It is assumed that the Opposition Force (OPFOR) tank (Tank B) is sitting in defilade in a combat zone. The primary mission of Tank B is to wait for a possible tank from the Blue Force (BLUFOR) and prevent it from entering a specific zone. Assume a BLUFOR tank (Tank A) is in the area and unknowingly enters the effective combat range of Tank B.

It is assumed that all components of Tank B are functioning properly; therefore, it has the capability to observe Tank A move into range. A decision is made by the commander of Tank B to fire on Tank A. At this point, the map of Tank B is referenced (and displayed on the slide) to see if Tank B has the capability to fire on Tank A. As all firepower components and sub-systems are functional; therefore, all system functions are functional, Tank B is capable of firing on Tank A. Therefore, Tank B fires an anti-tank munition at Tank A.

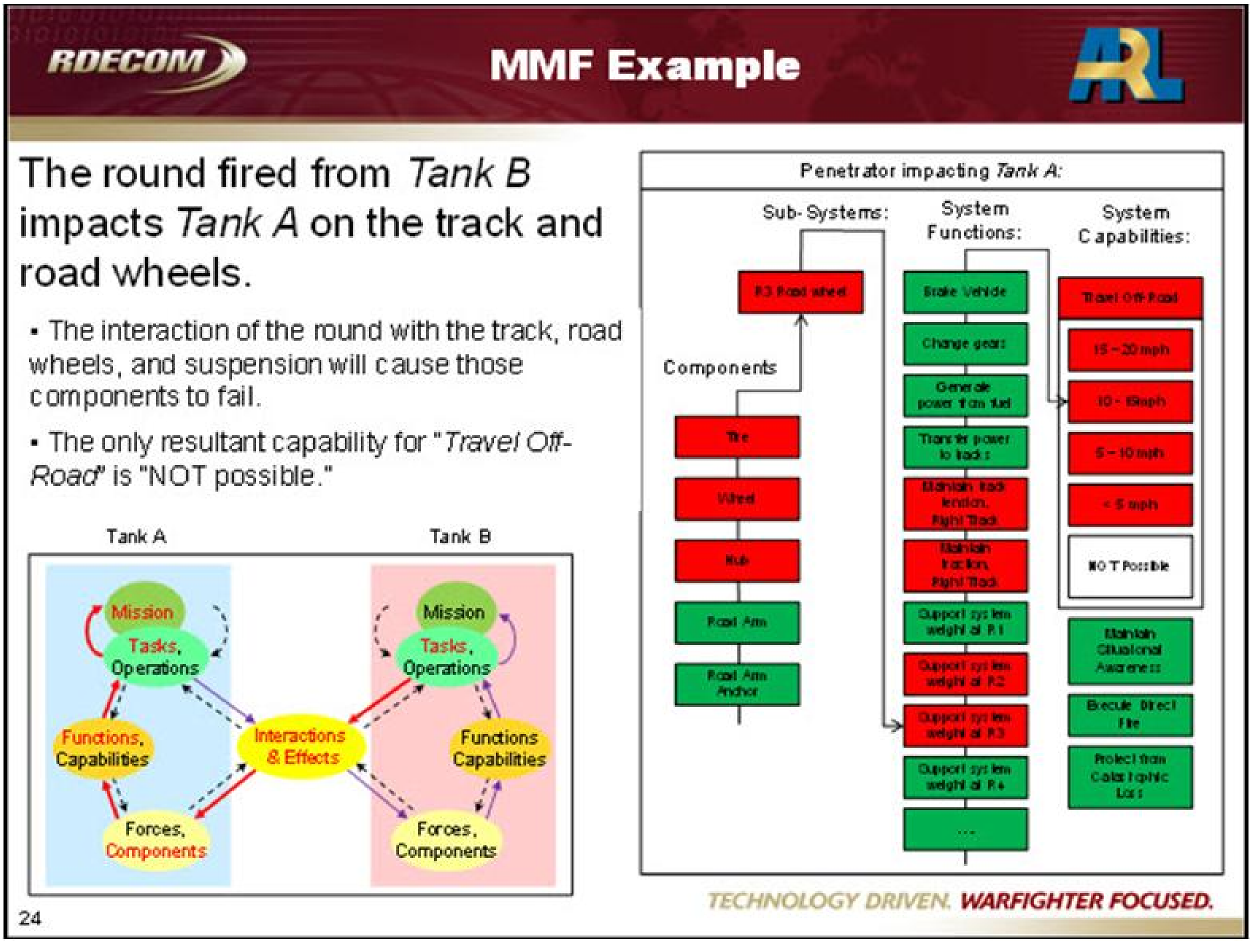

Figure 24. MMF example–results of the first round.

It is possible to show how the decision and action of Tank B firing a round will affect Tank A. This is done by advancing the index within MMF to the time that the round from Tank B impacts Tank A. By utilizing existing methodologies in vulnerability analysis, it is possible to predict the effect of the munition interacting with the components of Tank A. The resultant damage state of the components, either functional or dysfunctional, can then be supplied into the map of Tank A. By tracing the effect of dysfunctional components through the fault trees, it is concluded that Tank A is unable to travel further, which is a traditional Mobility Loss of Function (MLoF). The portion of the map for Tank A, focusing on some of the mobility components, is shown in figure 24.

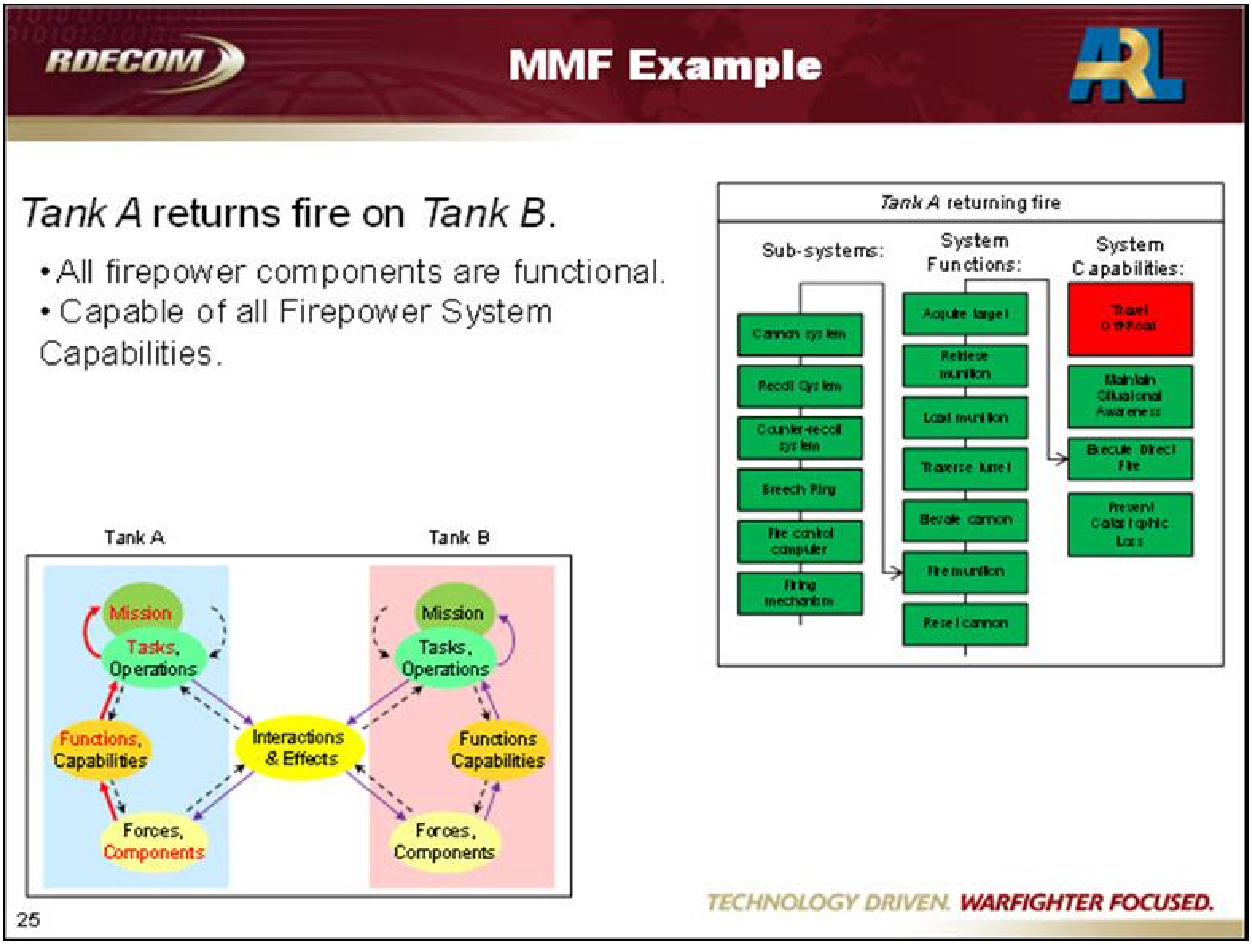

Figure 25. MMF example–the second round is fired.

After the damage from the first round is assessed, MMF will advance to the next time index, which is depicted in figure 25. The first interaction between the two tanks did result in a complete loss of capability for Tank A to move out of combat zone, but all components for the main gun are undamaged. Therefore, using the map for Tank A as shown in this graphic, it is evident that Tank A is able to fire directly on Tank B in a return-fire capacity. A decision is made by the commander of Tank A to return fire, and a munition is sent down-range to Tank B.

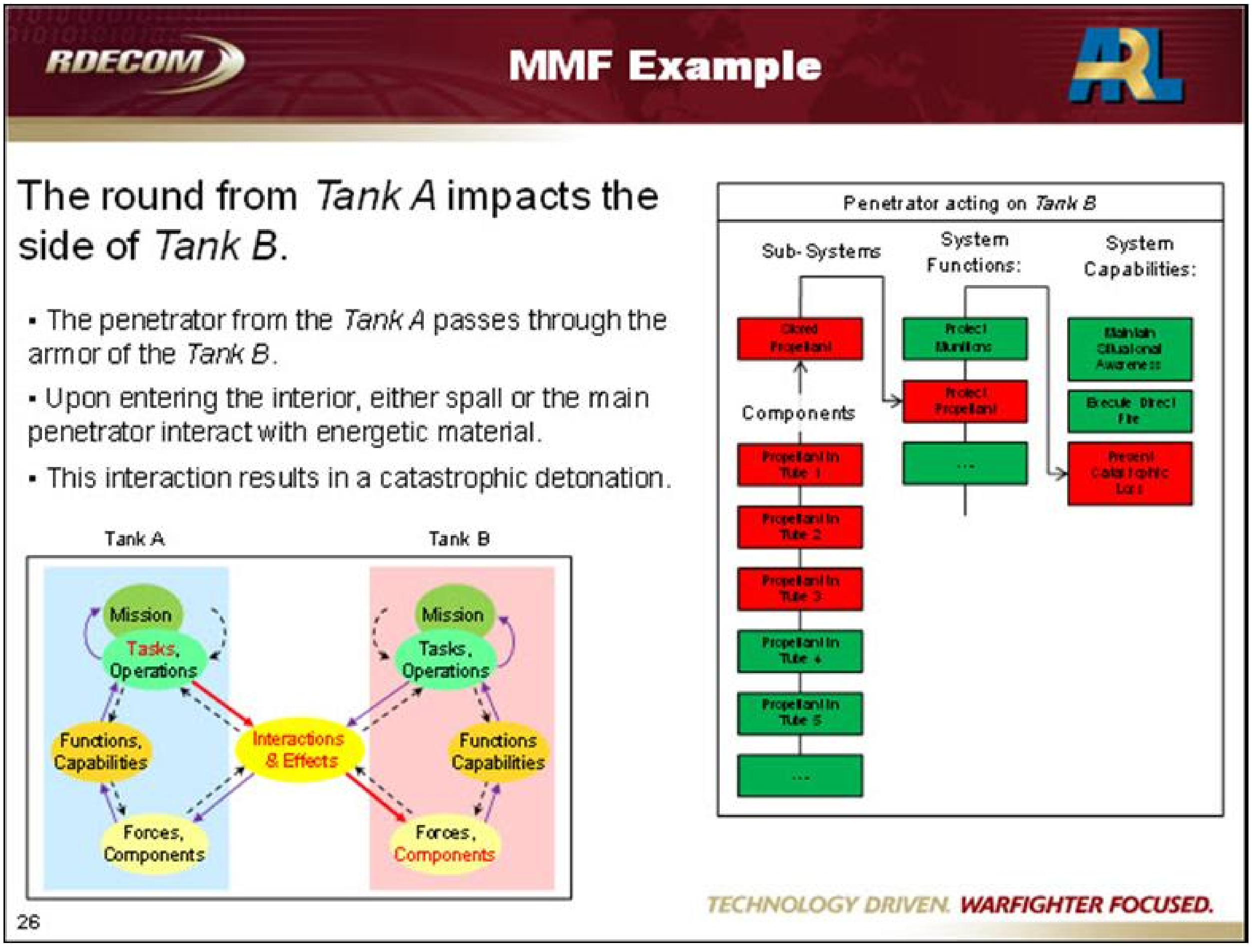

Figure 26. MMF example–the results of the second round.

The next time index in MMF is when the round from Tank A impacts on Tank B, which is depicted in figure 26. By again utilizing existing methodologies, it is possible to determine what components in Tank B will be damaged and rendered dysfunctional. In this example, it is assumed that the damaged components will be some form of energetic material inside of Tank B and will result in a catastrophic detonation.

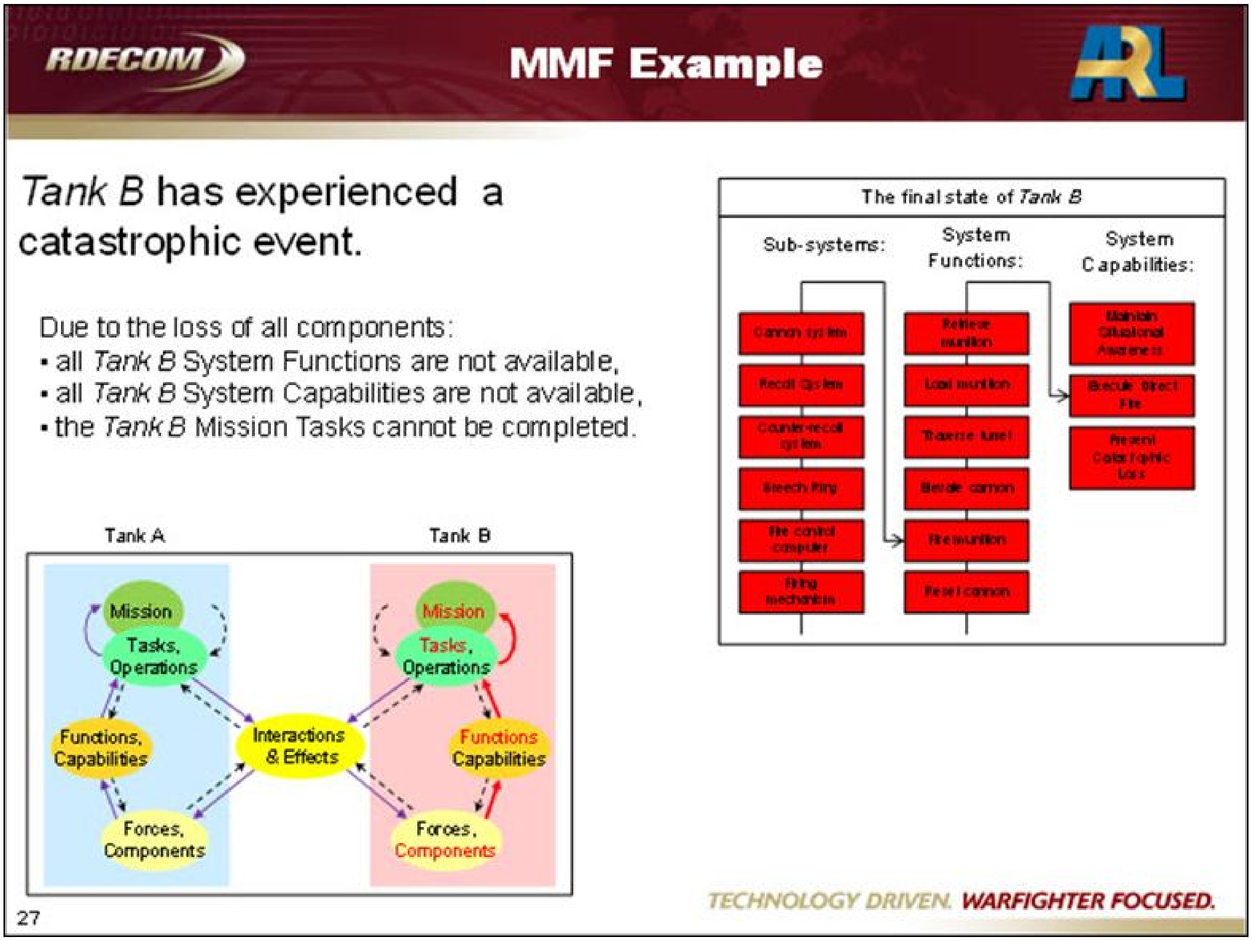

Figure 27. MMF example–the final outcome.

The final time index in this engagement is the resultant state of Tank B after the interaction of the munition from Tank A interacts with the components of Tank B. This index is depicted in figure 27. As a catastrophic detonation has occurred in Tank B, it is assumed all components of Tank B are destroyed and, therefore, dysfunctional. Utilizing the map from the SCAP, one can see that Tank B has no remaining SC. By referencing these lost SC into MMF, it is shown that Tank B has no remaining combat utility. As Tank B is unable to perform any further activities in MMF, it has failed in its missions and is no longer able to affect the outcome of the conflict.

Figure 28. Networked forces example – introduction.

Figure 28 introduces the third and final example of this presentation. We will explore how an unmanned aerial vehicle (UAV) can support a SPH in an indirect fire support mission. This example was inspired by an example in “Fundamentals of Ground Combat Vulnerability/Lethality” where a UAV is serving as a forward observer for a ground combat vehicle when explaining possible ways to depict vulnerability analysis of a SoS.

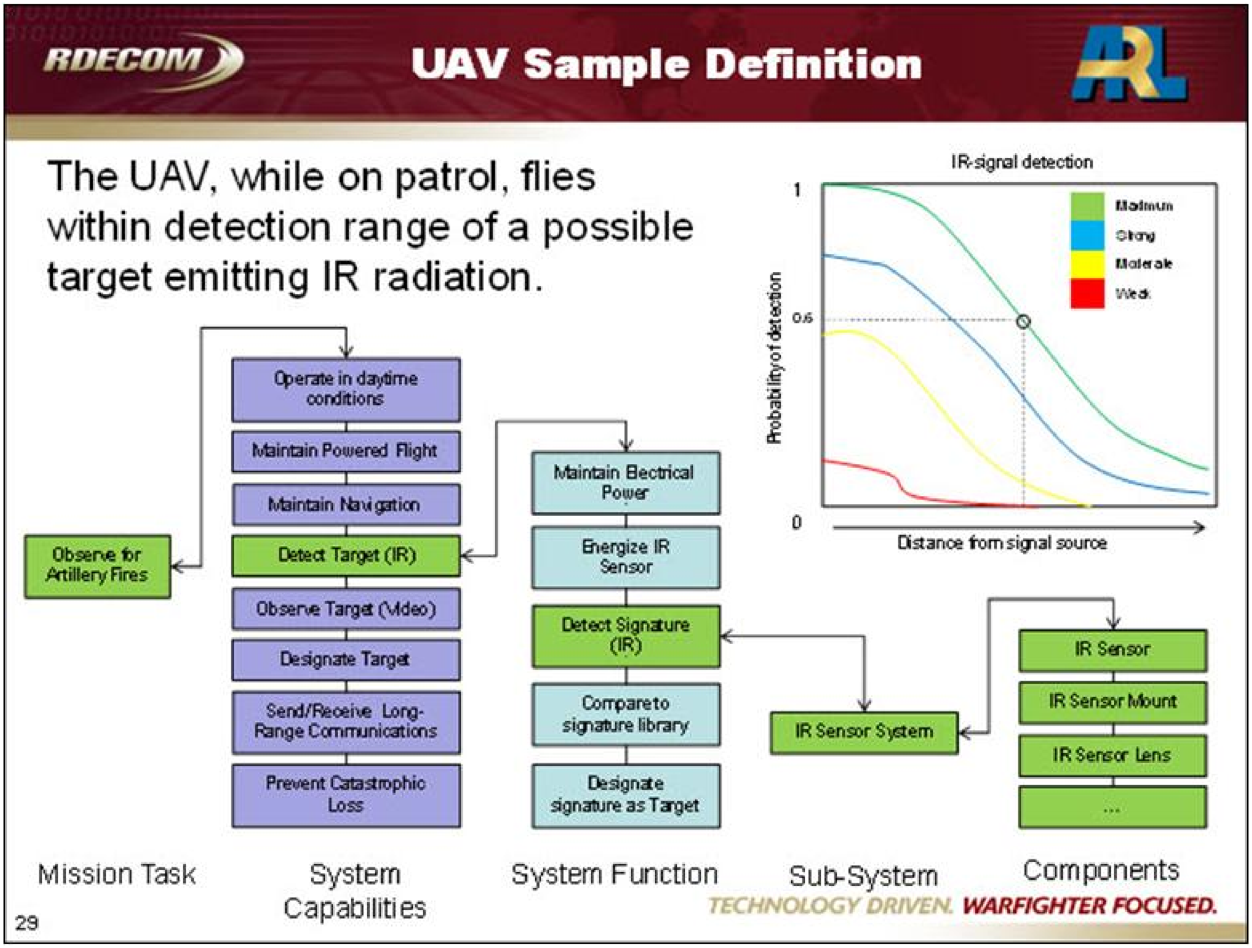

Figure 29. Networked forces example−UAV on patrol.

Assume a UAV is on a persistent surveillance mission in an isolated combat zone. No BLUFOR units are in the vicinity of the UAV's observed zone. As the UAV patrols, the IR sensor on the UAV moves closer to an object on the ground that is emitting an IR signature. We will assume that all components on the UAV are functional, as seen in figure 29. Therefore, the IR sensor system is functional and will use the probability of detection as shown in the graph for all signals it encounters. Assume the IR sensor system is at a known distance from the potential target, and the IR signal is considered "maximum" due to inadequate thermal shielding of the object on the ground. Using the discussion from earlier, we will see that conditions on the UAV (range, signal strength) shows that it is capable of detecting the IR signature with a success rate of about 60%.

As we assume this would be the situation as currently described in a hypothetical SoS simulation, a random draw will occur to see if the UAV detects the target using a Bernoulli trial with a probability of success of 60%. In this case it is assumed that the Bernoulli trial produces a successful result, and, therefore, the system function of "detect signature" is successful and the UAV detects a target of opportunity.

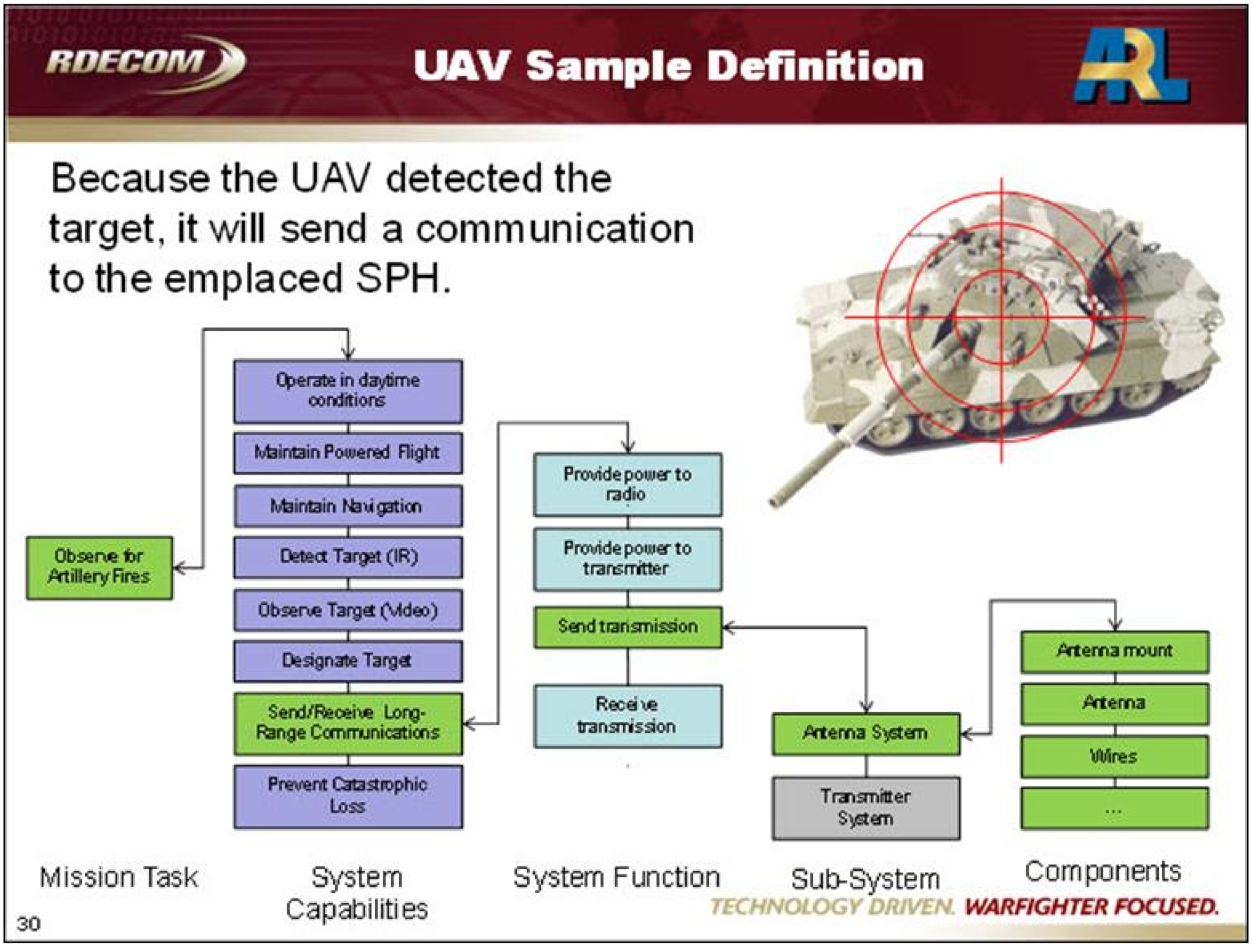

Figure 30. Networked forces example−UAV sending communication.

As the UAV has successfully detected a target of opportunity, a communication will be sent to a fire support battalion. The map depicted in figure 30 shows components for the antenna sub-system. These components are shown to be functional, and it is assumed all other critical communications sub-systems are also functional. Therefore, the UAV has the capability to send a long-range communication.

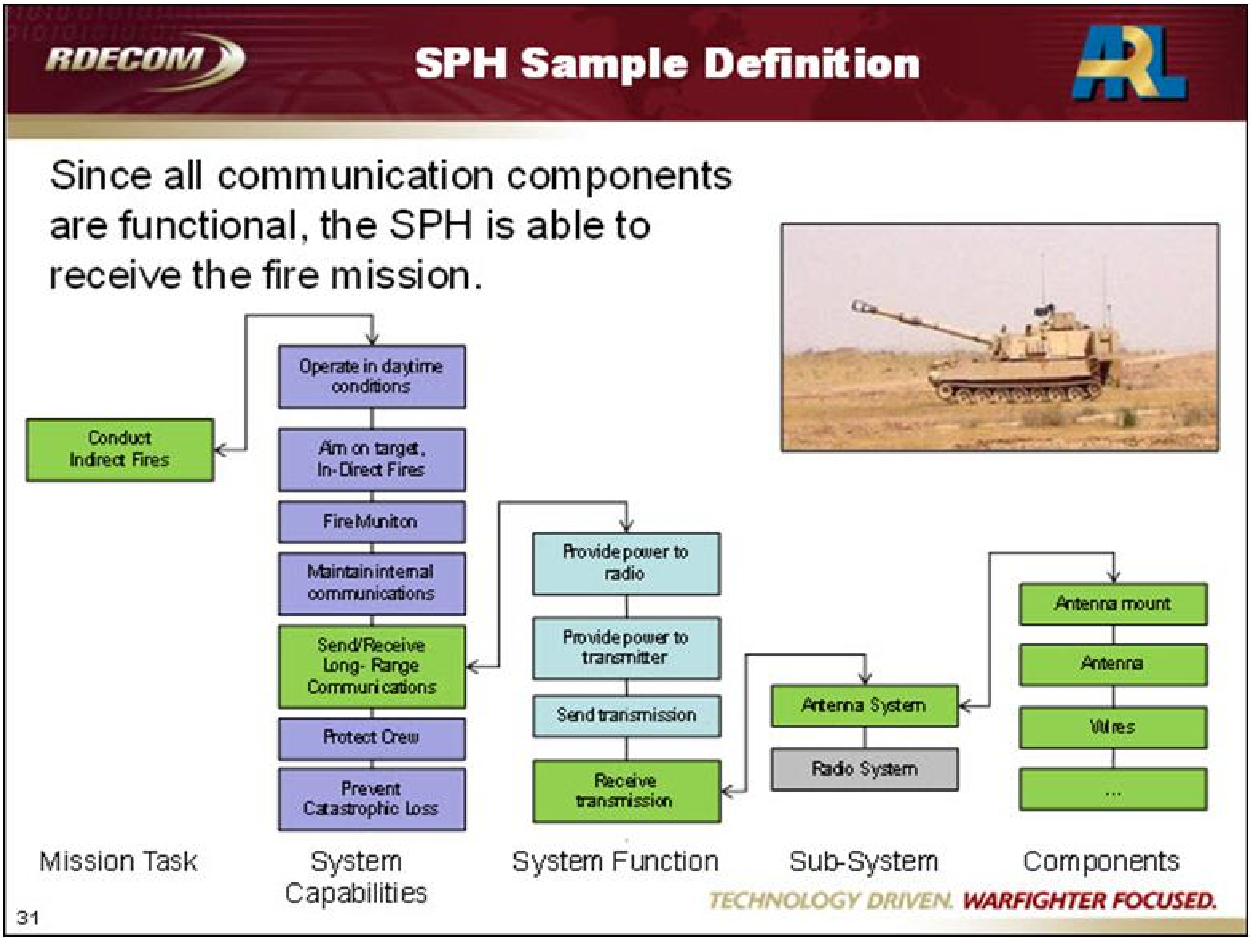

Figure 31. Networked forces example–howitzer receives communication.

Changing our attention to the emplaced fire support battalion, it is assumed that all components critical to communication are functional. This assumption is depicted in figure 31. Therefore, the SPH of interest is capable of receiving the communication from the UAV.

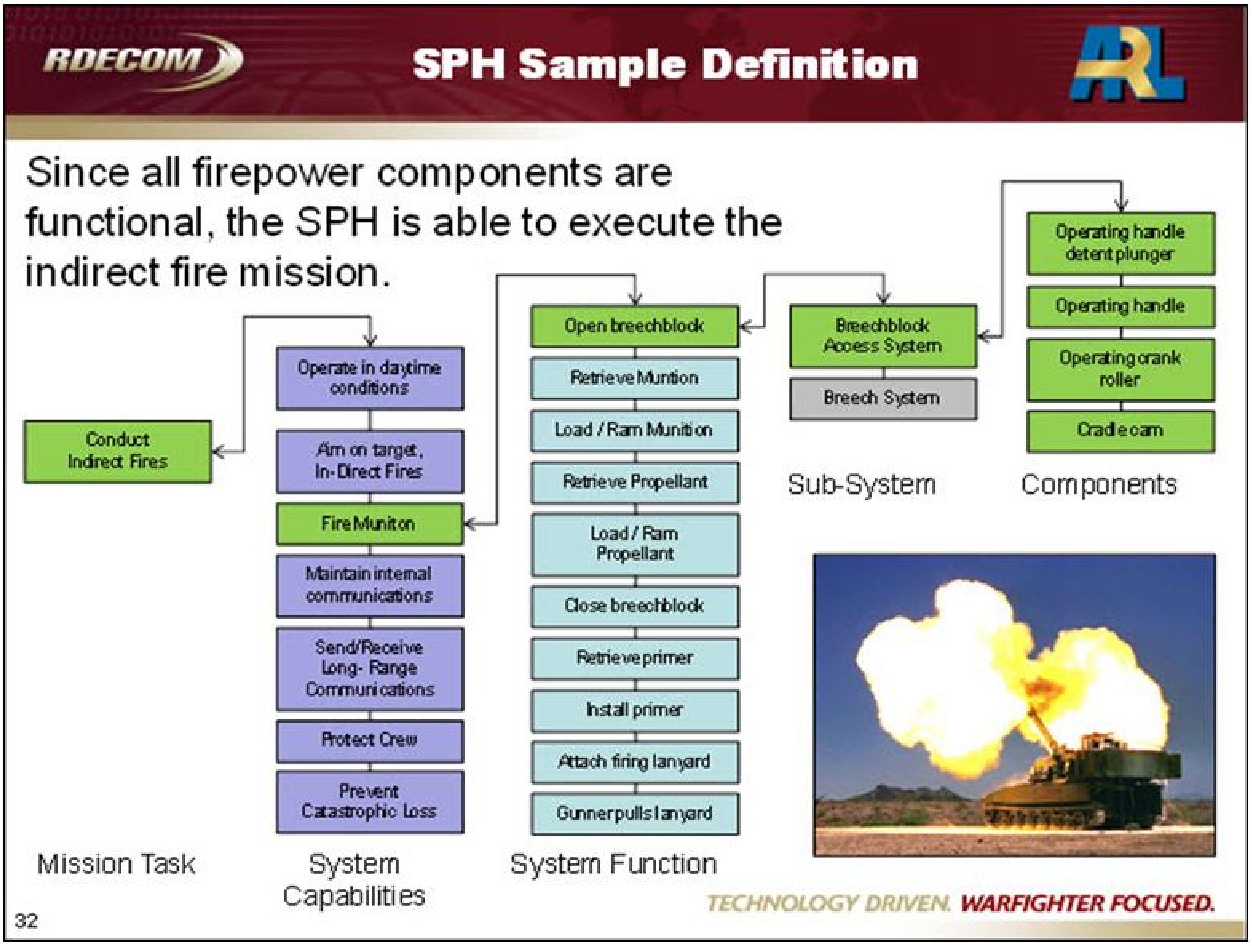

Figure 32. Networked forces example–howitzer fires munition.

Recalling the sample definition from earlier in the presentation, we can see in figure 32 that the SPH is capable of firing on the target in an indirect fire mission.

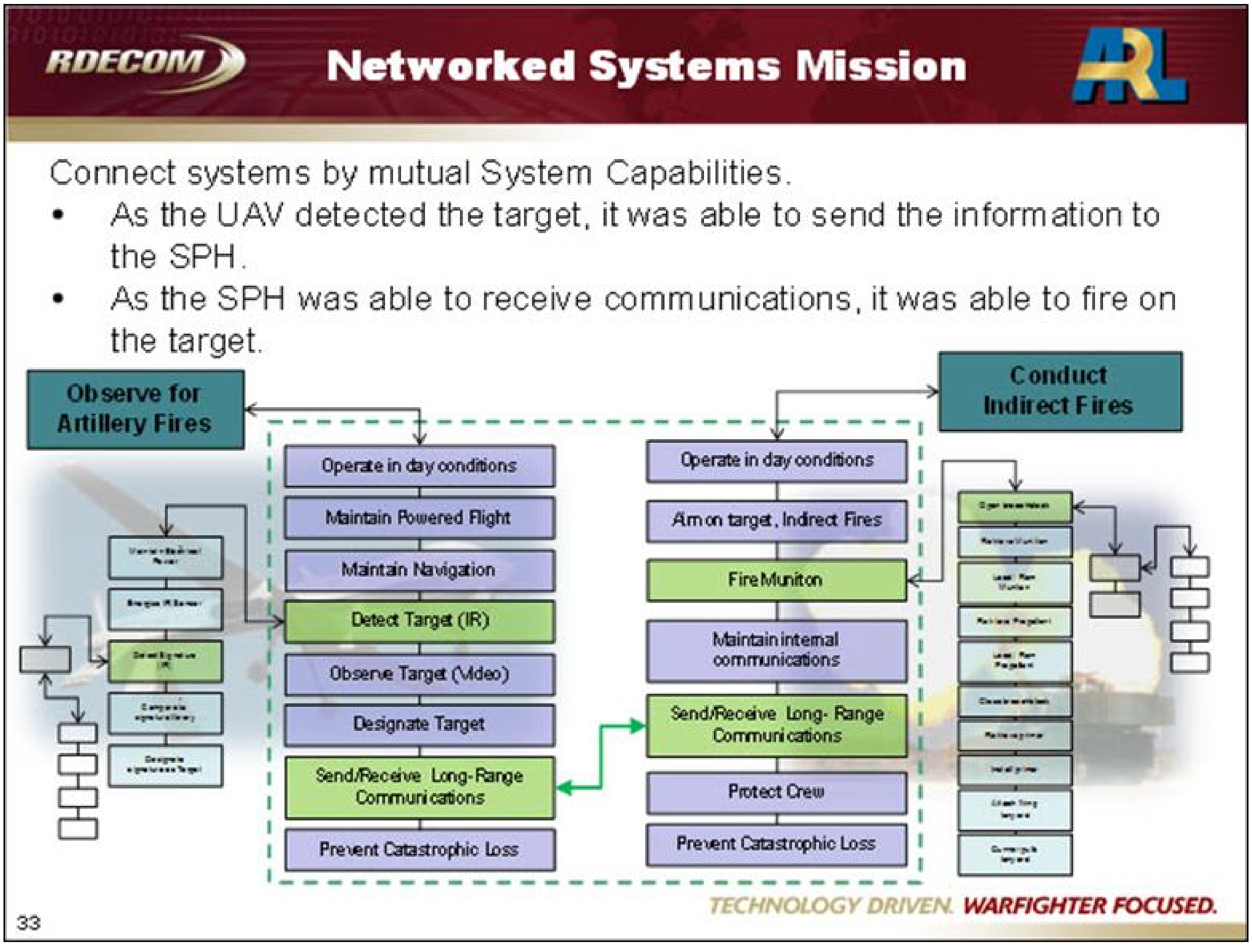

Figure 33. Networked forces example–linking systems by SCs.

As discussed in this example, and depicted in figure 33, the maps for systems within a system-of-systems are linked by mutual SC. Due to this linkage, it is possible to directly correlate the component state of one system to the capability of a networked system and also to determine the overall effect on a mission vignette. This has not been possible with traditional vulnerability/lethality (V/L) methodologies.

If a critical communications component of either system was dysfunctional, then it would be possible to determine the overall combat utility of the SoS due to the lost communication. In this example the fire mission would not occur, and a mission to suppress hostile activity in a remote region would be unsuccessful even though one system would be fully functional.

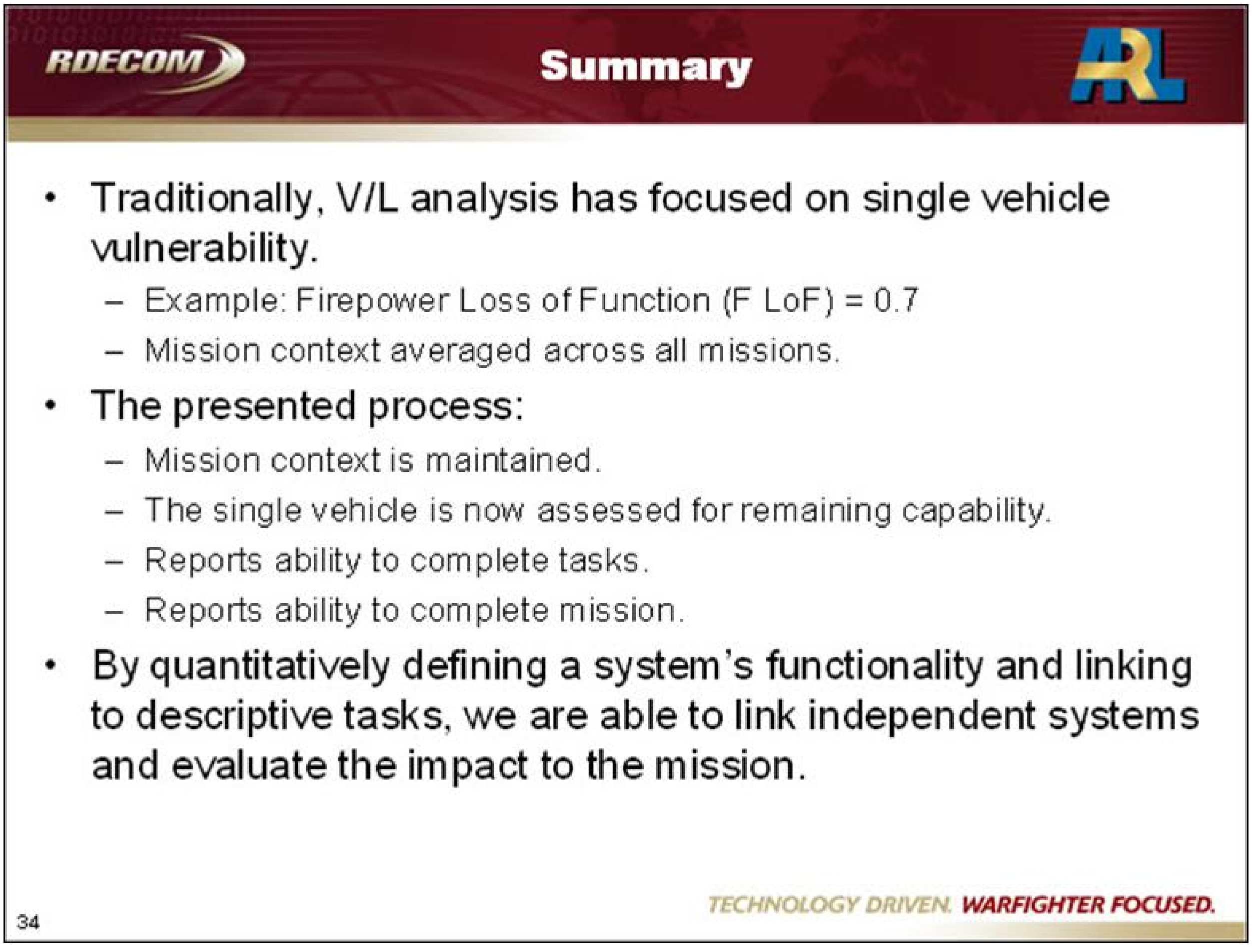

Figure 34. Summary.

The summary of the presentation is in figure 34.

Bibliography

Agan, K. *A Process for Mapping Component Function to Mission Completion.* Presented at the 26th Annual National Test & Evaluation Conference, San Diego, CA, 2010.

Agan, K; *A First Review of an Emerging Methodology: The System Capabilities Analytic Process (SCAP), as Presented at the Mission-Based Test & Evaluation (MBT&E) Workshop on 20 January 2010 (U)*; in progress; Army Research Laboratory.

Dietz, P.; Reed, H.; Klopcic, T.; Walbert, J. *Fundamentals of Ground Combat System Ballistic Vulnerability/Lethality*, American Institute of Aeronautics and Astronautics, Inc.: Reston, VA, 2009.

Field Manual 7-15, The Army Universal Task List; Headquarters of the Army, 2003.

Field Manual 7-15, The Army Universal Task List; Headquarters of the Army, 2009.

Gilmore, M. Memorandum: Reporting of Operational Test and Evaluation (OT&E) Results. *Director*, *OT&E*, 2010.

Klopcic, J.; Reed, H. *Historical perspectives on Vulnerability/Lethality Analysis;* ARL-SR-90; Army Research Laboratory: 1999.

Kruse, L.; Brizzolara, P. *An Analytical Method for Deriving Conditional Probabilities of Kill for Target Components*; BRL-1563; Ballistics Research Laboratory, 1971.

Landis, W.; *Applying the System Capabilities Analytic Process (SCAP) to the Mission-Based Test & Evaluation (MBT&E) of the Joint Light Tactical Vehicle (JLTV)*; ARL-SR-206; Army Research Laboratory: Aberdeen Proving Ground, MD, 2010.

Muehl, T.; Robertson, J. *Criticality Analysis of the M109A3E2 155mm Self-Propelled Howitzer*; ARL-TR-179; Army Research Laboratory: Aberdeen Proving Ground, MD, 1993.

Ploskonka, J.; Kuss, P.; Pierson, R. *Application of Degraded States Methodology to the Advanced Field Artillery Systems (AFAS)*; ARL-TR-711; Army Research Laboratory, 1995.

Saucier, R. *Fault Tree Representation and Evaluation;* ARL-TR-2923; Army Research Laboratory: Aberdeen Proving Ground, 2003.

Ward, B.; Abel, J.; Burdeshaw, M.; *Degraded States Vulnerability Analysis of a Self-Propelled Howitzer*; ARL-TR-613; Army Research Laboratory: 1994

Wilcox, C. Mission Based T&E, Tutorial. *25th Annual NDIA T&E Conference*, Atlantic City, NJ, March 2, 2009.

Wilcox, C. Mission Based T&E. *25th Annual NDIA T&E Conference*, Atlantic City, NJ, March 3, 2009.

Wilcox, C. ATEC Initiatives in Response to the Office of the Secretary of Defense Policy Guidelines for Test and Evaluation. *ITEA Journal* **2009**, *30*, 361−368.

Wilcox, C. *Mission Based T&E*, undated, unpublished work.

Wilcox, C. *MB T&E ATEC-HQ Perspective*, undated, and unpublished work.

List of Symbols, Abbreviations, and Acronyms

ARL	U.S. Army Research Laboratory
AT&L	Office of the Under Secretary of Defense
ATEC	Army Test and Evaluation Command
AUTL	Army Universal Task List
BLUFOR	Blue Force
DoD	Department of Defense
DOT&E	Director, Operational Test and Evaluation
EW	electronic warfare
IR	Infrared
MLoF	Loss of Function
MBT&E	Mission-Based Test and Evaluation
MMF	Missions and Means Framework
NDIA	National Defense Industrial Association
OPFOR	Opposition Force
Pcd|h	Probability of Component Dysfunction given a Hit
P_k	Probability of Kill
PSF	probabilistic system function
SC	system capability
SCAP	System Capabilities Analytic Process
SES	Senior Executive Service
SLAD	Survivability Lethality Analysis Directorate
SoS	system of systems

SPH	Self-propelled howitzer
T&E	Test and Evaluation
UAV	Unmanned Aerial Vehicle
V/L	vulnerability/lethality

NO. OF COPIES	ORGANIZATION
1 (PDF only)	DEFENSE TECHNICAL INFORMATION CTR DTIC OCA 8725 JOHN J KINGMAN RD STE 0944 FORT BELVOIR VA 22060-6218
1	DIRECTOR US ARMY RESEARCH LAB IMNE ALC HRR 2800 POWDER MILL RD ADELPHI MD 20783-1197
1	DIRECTOR US ARMY RESEARCH LAB RDRL CIM L 2800 POWDER MILL RD ADELPHI MD 20783-1197
1	DIRECTOR US ARMY RESEARCH LAB RDRL CIM P 2800 POWDER MILL RD ADELPHI MD 20783-1197
1	DIRECTOR US ARMY RESEARCH LAB RDRL D 2800 POWDER MILL RD ADELPHI MD 20783-1197
	ABERDEEN PROVING GROUND
1	DIR USARL RDRL CIM G (BLDG 4600)

NO. OF COPIES	ORGANIZATION
1 (CD only)	ASST SECY ARMY ACQSTN LOGISTICS & TECH SAAL ZP RM 2E661 103 ARMY PENTAGON WASHINGTON DC 20310-0103
1 (CD only)	ASST SECY ARMY ACQSTN LOGISTICS & TECH SAAL ZS RM 3E448 103 ARMY PENTAGON WASHINGTON DC 20310-0103
1 (CD only)	DIRECTOR FORCE DEV DAPR FDZ RM 3A522 460 ARMY PENTAGON WASHINGTON DC 20310-0460
1	US ARMY TRADOC ANL CTR ATRC W A KEINTZ WSMR NM 88002-5502
1	USARL RDRL SLE R FLORES WSMR NM 88002-5513

ABERDEEN PROVING GROUND

NO. OF COPIES	ORGANIZATION
1	US ARMY DEV TEST COM CSTE DTC TT T 314 LONGS CORNER RD APG MD 21005-5055
1	US ARMY EVALUATION CTR CSTE AEC SVE R LAUGHMAN 4120 SUSQUEHANNA AVE APG MD 21005-3013
30	DIR USARL RDRL SL J BEILFUSS J FEENEY J FRANZ M STARKS P TANENBAUM RDRL SLB A D FARENWALD (1 PDF) G MANNIX A BOMBOY L BUTLER R YOUNG RDRL SLB D R GROTE RDRL SLB E M MAHAFFEY M PERRY D LYNCH W LANDIS K AGAN (1 PDF, 1 HC) RDRL SLB G P MERGLER C KUHNS M ROTHWELL RDRL SLB S S SNEAD RDRL SLB W L ROACH R MOYER S COARD RDRL SLE J SMITH RDRL SLE M J NEALON B RUTH RDRL WMM D L GIBBONS RDRL HRM B D MITCHELL C SAMMS
1	US ARMY RSRCH LAB RDRL HRT M C GAUGHAN 12423 RESEARCH PRKWY ORLANDO FL 32826
1	US ARMY MATERIEL SYSTEMS ANALYSIS ACTIVITY RDAM TD DR PAUL DEITZ 392 HOPKINS ROAD APG MD 21005-5071
1	DR. FORREST CRAIN DIRECTOR AMSAA AMSRD AMS D BLDG 392 APG MD 21005-5071
1	US ARMY EVALUATION CENTER: TEAE SV J MUELLER 4120 SUSQUEHANNA AVE APG MD 21005

NO. OF
COPIES ORGANIZATION

NO. OF COPIES	ORGANIZATION
1	US ARMY EVALUATION CTR TEAE SV P A THOMPSON 4120 SUSQUEHANNA AVE APG MD 21005-3013
1	US ARMY TEST AND EVALUATION COMMAND CSTE CG DR. JAMES STREILEIN 4501 FORD AVE STE 600 ALEXANDRIA VA 22302
1	US ARMY EVALUATION CENTER TEAE D B SIMMONS 4120 SUSQUEHANNA AVE APG MD 21005
1	US ARMY EVALUATION CENTER TEAE SE C WILCOX 4120 SUSQUEHANNA AVE APG MD 21005
1	SURVICE ENGINEERING COMPANY J N WALBERT 3700 FETTLER PARK DRIVE STE 401 DUMFRIES, VA 22025