Safety Versus Survivability

by Gary D. Braman, Joe Dowd and Tyler Dorning
Huntsville, Alabama

Over the years, people in the defense industry and government have used the terms "system safety" and "survivability" interchangeably. The misunderstanding of these terms has created issues when preparing system safety analysis documents, such as Functional Hazard Assessments (FHA), System Safety Hazard Analysis (SSHA), and Safety Assessment Reports (SAR). In the past, customers have expected that survivability issues will be assessed in these system safety documents. This results in an extensive amount of time to prepare the document and to meet customer expectations. "System safety" is defined as "the design and operational characteristics of a system that minimize the possibilities for accidents or mishaps caused by human error or system failure." "Survivability" is defined as "the characteristics of a system that prevent fratricide, as well as reduce detectability of the soldier, prevent attack if detected, prevent damage if attacked, minimize medical injury if wounded or otherwise injured, and minimize mental and physical fatigue." It is clear, though, by these definitions that the two terms are not the same and should not be used interchangeably. This paper will provide indisputable substantiation that *system safety* and *survivability* are two distinct domains, and that an assessment of survivability issues is not documented in system safety analyses reports.

Introduction

On several occasions over the past several years, representatives from U.S. government agencies have stated that tactical (crew and aircraft survivability) hazards be assessed and documented in system safety analysis reports, specifically the Mission Equipment Package (MEP) Functional Hazard Assessment (FHA). Sikorsky System Safety Engineering (SSE) has repeatedly stated that tactical hazard assessments are not part of a system safety analysis and that a separate tactical crew and aircraft survivability assessment should be conducted, with the results captured in a separate document. This has resulted in an excessive amount of time required to prepare the MEP FHA documents often well beyond the time estimated for the document's preparation. Additionally, numerous working group meetings had to be conducted to discuss and hopefully resolve this issue, resulting in an unnecessary expenditure of funds and a shifting of the schedule to accommodate new delivery dates for the document. The purpose of this paper is to provide indisputable substantiation that safety and survivability are two distinct domains, and that crew and aircraft survivability hazards are not assessed and documented in safety analysis reports.

Definition of Terms

The terms "system safety" and "survivability" have been used interchangeably, but to show how different the terms are, the terms must first be defined. Research showed the terms being defined independently in Department of Defense (DoD) and U.S. Army documents. These documents include Department of Defense Instruction (DoDI) 5000.02, "Operation of the Defense Acquisition System" [Ref. 1]; Army Regulation (AR) 385-10, "The Army Safety Program" [Ref. 2] and AR 602-2, "Human Systems Integration (HSI) in the Acquisition Process" [Ref. 3]. Additionally, Clifton Ericson's book, *Concise Encyclopedia of System Safety: Definition of Terms and Concepts* [Ref. 4], was consulted for definitions of the two terms. These definitions are discussed in the text that follows.

(DoDI) 5000.02: This document does not provide specific definitions of "safety" and "survivability" in the glossary; however, the discussions of the two terms are provided as follows:

- **Safety and Occupational Health:** The Program Manager will ensure that appropriate human systems integration and environmental, safety and occupational health efforts are integrated across disciplines and into systems engineering to determine system design characteristics that can minimize the risks of acute or chronic illness, disability, or death or injury to operators and maintainers; and enhance job performance and productivity of the personnel who operate, maintain, or support the system.
- **Force Protection and Survivability:** The Program Manager will assess risks to personnel and address, in terms of system design, protection from direct threat events and accidents (such as chemical, biological and nuclear threats). Design consideration will include primary and secondary effects from these events and consider any special equipment necessary for egress and survivability [Ref. 1].

Though not specifically defined in the previous documents, it can be concluded from the discussions in these paragraphs that "safety" and "survivability" are separate and not interchangeable terms. To provide conclusive and indisputable substantiation that safety and survivability are separate domains, the two terms ("safety" and "survivability") are defined using U.S. Army documents and a reference encyclopedia of system safety terms and definitions.

Safety: AR 385-10, The Army Safety Program [Ref. 2], defines "safety" as "Freedom from those conditions that can cause death, injury, occupational illness, or damage to, or loss of, equipment or Property." This exact definition is repeated in the Department of the Army (DA) Pamphlet (PAM) 385-16, "System Safety Management Guide" [Ref. 5], and again in the Utility Helicopter Project Office's (UHPO) "System Safety Management Plan (SSMP)," dated March 1, 2016 [Ref. 6]. AR 602-2, "Human Systems Integration (HSI) in the Acquisition Process" [Ref. 3], describes the HSI program and highlights the program's seven domains: manpower, personnel capabilities, training, human factors engineering, *system safety*, health hazards and *soldier survivability*. "System safety" is defined as "the design and operational characteristics of a system that minimize the possibilities for accidents or mishaps caused by human error or system failure." In Clifton Ericson's Book, *Concise Encyclopedia of System Safety: Definition of Terms and Concepts* [Ref. 4], "safety" is defined as "freedom from unacceptable mishap risk."

Survivability: Army Regulation (AR) 602-2, "Human Systems Integration (HSI) in the Acquisition Process" [Ref. 3], describes the HSI program and highlights the program's seven domains: manpower, personnel capabilities, training, human factors engineering, *system safety*, health hazards and s*oldier survivability*. "Personnel survivability" is defined as "the characteristics of a system that prevent fratricide, as well as reduce detectability of the Soldier, prevent attack if detected, prevent damage if attacked, minimize medical injury if wounded or otherwise injured, and minimize mental and physical fatigue." Clifton Ericson's book defines "survivability" as "the capability of a system or crew to avoid or withstand a man-made hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission."

Survivability consists of three elements: susceptibility (the likelihood of being detected, identified and hit), vulnerability (the effects of being hit by a weapon) and recoverability (the longer-term post-hit effects, damage control and firefighting, capability restoration or escape and evacuation. Department of the Army (DA) Pamphlet (PAM) 385-16, "System Safety Management Guide" [Ref. 6], defines "survivability" as "the capability of a system and crew to avoid or withstand a man-made hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission. Survivability considers ballistic effects; nuclear, biological, and chemical weapons; information assurance; countermeasures; electromagnetic environmental effects; obscurants; and atmosphere and vulnerability."

In Clifton Ericson's Book, *Concise Encyclopedia of System Safety: Definition of Terms and Concepts* [Ref. 4], "survivability" is defined as "the capability of a system and crew to avoid or withstand a man-made hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission. Survivability consists of susceptibility, vulnerability, and recoverability."

Though previously shown to be distinct terms, there is some common ground between "system safety" and "survivability." One area of mutual interest is crash survivability. Crash survivability is defined as the capability of a vehicle to protect its occupants against an accidental impact, such that they receive no serious injury, thereby surviving the crash. Survivability design features will affect both crashworthiness and emergency egress. Additionally, system safety assessments are conducted if modifications to the system affect these items, and the results are documented in the system safety analysis.

"Survivability" is still a general term used to describe a system's ability to avoid and/or withstand manmade damage-causing mechanisms. However, Aircraft Survivability Equipment (ASE) is installed on the aircraft and is described in the following paragraphs.

Aircraft Survivability Equipment (ASE)

The role of Aircraft Survivability Equipment (ASE) is to reduce the vulnerability of aircraft, thus allowing aircrews to survive in a combat environment and accomplish their mission. The methodology for achieving survivability is supported by the ASE philosophy. The ASE philosophy is a five-step approach ensuring that Army aircrews are able to accomplish their mission continuously. These five steps are described as follows:

- **Step 1: Tactics.** Proper tactics reduce exposure times to enemy weapons. Low-level flight limits line-of-sight (LOS) exposure to hostile weapons systems. Low-level flight tactics, combined with ASE protection, allow combat aircraft to survive and perform their mission. ASE protection is severely degraded when the aircraft is not flown in a tactically sound manner (e.g., against a sky-blue background).
- **Step 2: Signature Reduction.** These measures are implemented through engineering or design changes, such as flat canopies, exhaust suppressers and coating the aircraft with low-infrared reflective paint. Signature reduction alone greatly increases survivability. Without signature reduction, ASE effectiveness is degraded and, in some cases, erased. Signature reduction is also influenced by the aviator controlling how much signature to expose to the threat.
- **Step 3: Warning.** The next step in the ASE philosophy is to provide warning to aircrews when they are about to be engaged, allowing them time to react. Examples include radar-detecting sets, laser-detecting sets and infrared missile warning systems.
- **Step 4: Jamming and Decoying.** When aircrews must stay on station despite warnings, there is a requirement for countermeasures capable of jamming and/or decoying the fire control or guidance systems

of threat weapons. Chaff, flares, and radar and IR jammers provide this type of protection.

- **Step 5: Aircraft Hardening.** Aircraft hardening provides for ballistic tolerance, redundant critical flight systems, and crashworthy features to assist in minimizing the damage to an aircraft after it has been hit [Ref. 7].

Tactical aircraft are protected with ASE while operating and conducting their assigned missions throughout the battlefield. Aircraft survivability equipment encompasses a vast array of systems. Described below are several pieces of ASE installed on combat/tactical aircraft:

- **Advanced Threat Infrared Countermeasure (ATIRCM) Set, AN/ALQ-144A(V)1 —** The ATIRCM detects missile launches/flights, protects aircraft from infrared (IR) guided missiles and provides threat awareness and IR countermeasures using an airborne self-protection system. It uses the AN/AAR-57 Common Missile Warning System (CMWS), which detects the missile, rejects false alarms and cues the onboard infrared jamming system's jam head to the missile's location. When the jam head finds the missile with its IR tracking system, it emits a high-energy infrared beam to defeat the missile's infrared seeker (see Figure 1) [Ref. 8]. More detailed information on the operation of the system can be found in technical manual TM 1-1520-280-10, "Operator's Manual for Helicopters, Tactical Utility Transport" with Change 8, dated April 30, 2016 [Ref. 9].
- **AN/AAR-57 Common Missile Warning System (CMWS) and Improved Countermeasures Dispenser (ICMD) System —** The AN/AAR-57 provides missile warning, and automated or manual dispersion of countermeasure munitions. The operator can manually dispense munitions to protect against Target Tracking Radar (TTR) or the CMWS can detect surface-to-air and air-to-air IR-guided missiles and automatically deploy countermeasures. The AN/AAR-57 provides missile warning, and automated or manual dispersion of countermeasure munitions. The operator can manually dispense munitions to protect against Target Tracking Radar (TTR) or the CMWS can detect surface-to-air and air-to-air IR-guided missiles and automatically deploy IR or RF expendables countermeasures (chaff or flares) via the Electronic Control Unit (ECU). The CMWS consists of up to six electro-optic missile sensors (EOMSs), one ECU and the Improved Countermeasure Dispenser (ICMD). The ICMD consists of up to four GFE ALE-47 Sequencers (SEQ) and up to two Smart Dispensers (SD) per SEQ. The plume of the missiles is detected by the EOMS's Ultraviolet (UV) detectors. The CMWS declares those missiles which are a threat to the host platform, provides aircrew warning and cues on-board dispensers which will in turn deploy IR or RF expendables. The CMWS contains the Improved Countermeasures Dispenser (ICMD) that is controlled by the CMWS to initiate dispensing of expendable countermeasures (see Figure 2) [Ref. 10]. More detailed information on the operation of the system can be found in technical manual TM 1-1520-280-10, "Operator's Manual for Helicopters, Tactical Utility Transport" with Change 8, dated April 30, 2016 [Ref. 9].

Figure 1 – Advanced Threat Infrared Countermeasure (ATIRCM) Set, AN/ALQ-144A(V)1.

Figure 2 – AN/AAR-57 Common Missile Warning System (CMWS).

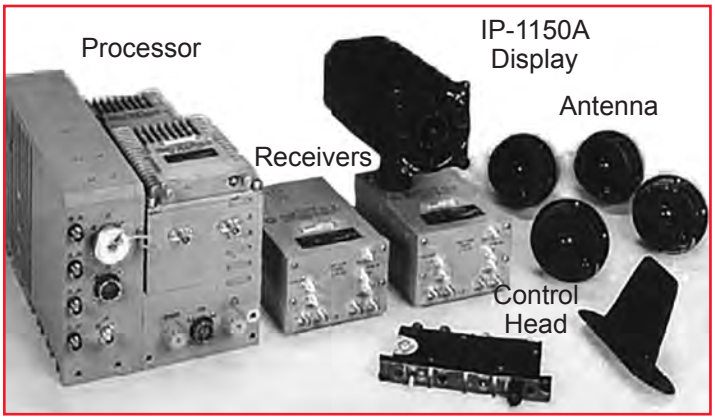

Figure 3 – AN/APR-39A(V)-1 Radar Signal Detecting Set.

Table 1 – Hazard Severity Definitions.

Recommended Safety Requirements				
Severity Category (Level)	**Negligible (IV)**	**Marginal (III)**	**Critical (II)**	**Catastrophic (I)**
Severity Definition	Less than minor injury or occupational illness (less than one lost workday), minimal environmental damage or monetary loss less than $100K. A slight reduction in rotorcraft safety margins or functional capabilities (including degraded or lack of mission success) or involving crew actions that are well within their capabilities with only a slight increase in crew workload, such as routine flight plan changes.	Minor injury or minor occupational illness (no permanent environmental damage or monetary loss exceeding $100K, but less than $1M). Reduction in the capability of the rotorcraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be a significant reduction in aircraft safety margins or functional capabilities (including immediate or almost immediate mission abort), a significant increase in crew work load or in conditions impairing crew efficiency, or physical discomfort to the flight crew.	Severe injury or severe occupational illness (permanent partial disability) or hospitalization of three or more personnel, reversible significant environmental damage or monetary loss exceeding $1M, but less than $10M. Reduction in the capability of the rotorcraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be: Physical distress or excessive workload such that the flight crew's ability is impaired to where they could not be relied on to perform their tasks accurately or completely; or a large reduction in aircraft safety margins or functional capabilities.	Death or permanent total disability; aircraft loss; irreversible significant environmental damage; or monetary loss exceeding $10M.
Note: A "No Safety Effect" Development Assurance Level "E" exists, which may span any probability range.				

- **AN/APR-39A(V)-1 Radar Signal Detecting Set —** The AN/APR-39(V) is a passive omnidirectional radar receiver. The equipment receives and displays to the aircraft pilot, or other observer, information concerning the radar environment surrounding the aircraft. The equipment responds to those radars usually associated with hostile fire control tracking radars by providing visual and aural indications of the presence of, and the direction to, emitters. Non-threat radars are generally excluded. The radar receiver also accepts missile guidance radar signals. Visual and aural displays are uniquely identified to warn the observer that an emitter has become a potential threat. Input power requirement for the AN/APR-39(V) is 28 volts DC at 1.1 amps [Ref. 11]. More detailed information on the operation of the system can be found in technical manual TM 1-1520-280-10, "Operator's Manual for Helicopters, Tactical Utility Transport" with Change 8, dated April 30, 2016 [Ref. 9].

It must be noted that none of the descriptions for the ASE listed here indicate any connection to safety. The purpose and operation of this equipment is to reduce the vulnerability of aircraft, thus allowing aircrews to survive in a combat environment and accomplish their mission.

Assessment of Safety and Survivability Hazards

When assessing various hazards or failures, or loss of functions, the system safety engineer will consider their resulting effect on the safe operation of the aircraft. Survivability is assessed in SER-70160204, "UH/HH-60M Aircraft-Level Functional Hazard Assessment (AFHA)," Revision 2, dated April 14, 2017 [Ref. 12]. In the AFHA, the function of the aircraft assessed is titled "provide threat protection." The loss of this function was assessed as a safety hazard and was assessed as having no safety effect. It was assessed in terms of its effect on the crew, passengers, ground personnel and aircraft in the event of a failure or malfunction (a safety hazard). The definitions listed in Table 1 were used in assessing the loss of the various aircraft functions.

Aircraft Survivability Equipment is also assessed in SER-70160135, "Mission Equipment Package (MEP) Functional Hazard Assessment (FHA)," Revision 2, dated October 15, 2015 [Ref. 13]. In the MEP FHA, the Com-

mon Missile Warning System (CMWS) is assessed if it malfunctions (inadvertent firing) on the ground or in the air (an accident, which is unintentional). What is not assessed is the failure or malfunction of the CMWS if engaged by a missile (an intentional act), an aircraft survivability hazard.

Conclusions

It can be clearly seen that the two terms "system safety" and "survivability" are distinguishable and separate. Through the numerous similar definitions, in some cases exact definitions, it is clearly seen that the two terms are clearly two separate domains. This is reinforced through the discussion and descriptions of the various aircraft survivability equipment. None of the system descriptions referred to aircraft or aircrew safety. The descriptions referred to counteracting hostile threats in a combat environment. Safety/system safety analyses are conducted to influence design changes, thus preventing accidents and mishaps (unintended events) as opposed to survivability/personnel survivability analyses, which are conducted to ensure aircraft crews can survive when conducting operations in a hostile threat environment. Based on the evidence presented, one can only conclude that *system safety* and *survivability* are two separate terms.

About the Authors

Gary Braman is system safety manager with Sikorsky in Huntsville, Alabama. He is responsible for the system safety engineering process associated with the installation of new systems or the modification of legacy systems installed on the U.S. Army's Black Hawk helicopter fleet. Mr. Braman is a retired U.S. Army Master Aviator with more than 33 years in the aviation and safety professions. He holds a Master of Aeronautical Science (MAS) Degree in Aviation/Aerospace Management from Embry-Riddle Aeronautical University (ERAU) and a Master of Science (MS) Degree in Industrial Engineering Technology and Safety Management from Texas A&M University. He is a Certified Safety Professional (CSP) and holds certifications in hazard control management (CHCM); environmental auditing in health and safety (CPEA), and safety and health management (CSHM).

Joe Dowd is a system safety engineer with Sikorsky Aircraft Corporation in Huntsville, Alabama. He is responsible for safety assessments in accordance with SAE ARP 4761, SAE ARP 4754A, and MIL-STD-882 for modified hardware or software, or integration of new systems in the U.S. Army's Black Hawk helicopter fleet. He holds a Bachelor of Science (BS) Degree in Mechanical Engineering from the University of Alabama in Huntsville (UAH).

Tyler Dorning is a system safety engineer with Sikorsky Aircraft Corporation in Huntsville, Alabama. He is responsible for implementing the system safety engineering process set forth by the guidelines of SAE-ARP-4761 and SAE-ARP- 4754 that are associated with the installation of new systems or the modification of legacy systems installed on the U.S. Army's Black Hawk helicopter fleet. He holds a Bachelor of Science (BS) Degree in Industrial and Systems Engineering from Auburn University.

References

1. Department of Defense Instruction (DODI) 5000.02, "Operation of the Defense Acquisition System," January 7, 2015, http://www.dtic.mil/whs/directives/corres/pdf/500002_dodi_2015.pdf, accessed May 22, 2017.
2. Army Regulation (AR) 385-10, "The Army Safety Program," November 27, 2013, http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN2099_AR385- 10_Web_FINAL.pdf, accessed May 22, 2017.
3. Army Regulation 602-2, "Human Systems Integration (HSI) in the Acquisition Process," January 27, 2015, http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/r602_2.pdf, accessed May 22, 2017.
4. Ericson, C. *Concise Encyclopedia of System Safety: Definition of Terms and Concepts*, John Wiley and Sons, Inc., Hoboken, New Jersey, 2011.
5. Department of the Army (DA) Pamphlet (PAM) 385-16, "System Safety Management Guide," August 13, 2013, http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/p385_16.pdf, accessed May 22, 2017.
6. Utility Helicopter Project Office (UHPO). "System Safety Management Plan (SSMP)," March 1, 2016.
7. FM 1-114. "Air Cavalry Squadron and Troop Operations," February 1, 2000, http://www.bits.de/NRANEU/others/amd-us-archive/fm1-114%2800%29.pdf, accessed May 22, 2017.
8. BAE Systems. "AN/ALQ-144 Infrared Countermeasure Set," 2017, http://www.baesystems.com/en-us/product/analq144-infrared-countermeasure-set, accessed May 23, 2017.
9. TM 1-1520-280-10, "Technical Manual: Operator's Manual for Helicopters, Tactical Utility Transport with Change 8," April 30, 2016, http://www.dtic.mil/whs/directives/corres/pdf/500002_dodi_2015.pdf, accessed May 22, 2017.
10. BAE Systems, "AN/AAR-57 Common Missile Warning system (CMWS)," 2017, http://www.baesystems.com/en-us/product/anaar57-common-missile-warning-system-cmws, accessed May 23, 2017.
11. Military Analysis Network. "AN/APR-39 Radar Warning Receiver," 2017, https://fas.org/man/dod-101/sys/acequip/am-apr-39.htm, accessed May 23, 2017
12. SER-70160204, "UH/HH-60M Aircraft-Level Functional Hazard Assessment (AFHA)," Revision 2, April 14, 2017.
13. SER-70160135, Rev 2, "UH/HH-60M Mission Equipment Package (MEP) Functional Hazard Assessment (FHA)," October 15, 2015.