UNMANNED SYSTEMS SAFETY GUIDE FOR DOD ACQUISITION

27 June 2007

Department of Defense

Preface

The Department of Defense Instruction (DoDI) 5000.1 instructs Program Mangers (PMs) to prevent Environment, Safety, and Occupational Health (ESOH) hazards, where possible, and manage ESOH hazards where they cannot be avoided. Further guidance regarding the prevention and management of ESOH hazards is also provided in the Defense Acquisition Guidebook (DAG), Section 2.3.14. This guide focuses on safety and health hazards and supports the overall ESOH risk management tenets of DoDI 5000.2. This Guide should be used in conjunction with the DoD Standard Practice for System Safety prescribed in Military Standard (MIL-STD) 882.

To assist PMs, system design engineers, and system safety engineers in addressing the unique aspects of the holistic Unmanned Systems (UMSs) technology development environment, the Office of the Secretary of Defense (OSD) issued a call to government, industry, and academia to develop safety guidance. The objective of this guidance is to ensure the design and development of UMSs that incorporate the necessary safety design rigor to prevent potential mishaps, or mitigate potential mishap risk. OSD directed this safety guidance also consider real and potential Concepts of Operation (CONOPS) of UMSs and establish fundamental operational safety requirements necessary to support safe operation of the UMS. This guidance provides a generic set of safety precepts and safety design considerations and establishes a starting point toward ensuring safety is a fundamental pillar of the acquisition process and incorporates those necessary design considerations to safely sustain UMSs.

The safety precepts provided in this guide were developed by a select group of design and system safety engineers and PMs. Recognized expert representatives were selected from: OSD staff, Army, Navy, Air Force, Marine Corps, National Aeronautical and Space Administration (NASA), National Institute of Standards and Technology (NIST), private industry, and academia. These representatives were organized into six functional workgroups, which reported to an Executive Steering Group. The composition of these workgroups was carefully crafted to include appropriate safety expertise as well as participation across DoD services, industry, and academia. A list of contributors is provided as Appendix D.

PMs for UMS and unmanned variants of manned systems are encouraged to apply this guidance to all UMS acquisition efforts and to all levels and elements of a UMS design: system, subsystem, hardware, and software. PMs should address the applicable programmatic, operational, and design precepts defined in this Guide at design reviews to include Critical Design Review (CDR).

PMs should tailor their safety programs to fit their acquisition programs and applicable statutory requirements, ensuring every system safety program considers the system's entire lifecycle. This guide should be used in conjunction with related directives, instructions, policy memoranda, or regulations issued to implement mandatory requirements.

The Office of Primary Responsibility (OPR) for this guide is ODUSD (A&T) Systems and Software Engineering Directorate. This office will develop and coordinate updates to the guide, as required, based on policy changes and customer feedback. To provide feedback to the OPR, please e-mail the office at Elizabeth.Rodriguez-Johnson@osd.mil.

Table of Contents

List of Figures

List of Tables

1. Key Terms, Descriptions, and Principles

Unmanned Systems (UMSs) cross many boundaries, such as: all Department of Defense (DoD) services, industry contractors, academia, safety organizations, and development organizations. In order to assist development of UMS safety guidance, it is critical to establish consistent terminology for today's complex UMSs. New and unique terms have evolved as a result of on-going scientific research and development of UMSs. The terms provided and defined in this guideline are included as Appendix C and establish a common lexicon for UMS safety. The source for all existing terms and definitions was recorded and new terms are identified as such.

An understanding of the meaning of the following terms is key to properly applying this UMS safety guidance.

1.1 Unmanned System

A UMS is defined as: "An electro-mechanical system that is able to exert its power to perform designed missions and includes the following: (1) there is no human operator aboard, (2) manned systems that can be fully or partially operated in an autonomous mode, and (3) the system is designed to return or be recoverable. The system may be mobile or stationary, and includes the vehicle/device and the control station. Missiles, rockets and their submunitions, and artillery are not considered UMSs. UMSs include, but are not limited to: unmanned ground vehicles, unmanned aerial/aircraft systems, unmanned underwater vehicles, unmanned surface vessels, unattended munitions, and unattended ground sensors."

1.2 Safety Precept

A safety precept is defined as: "A safety precept is a basic truth, law or presumption intended to influence management, operations, and design activities but not dictate specific solutions. A safety precept is worded as a nonspecific and unrestricted safety objective that provides a focus for addressing potential safety issues that present significant mishap risk. Precepts are intentionally general and not prescriptive in nature; they provide a goal, which may be achieved via numerous possible options. They provide a focus and objective as opposed to a detailed solution. The need for a safety precept may result from the desire to mitigate certain hazards, hazard types or Top Level Mishaps."

Three levels of safety precepts have been established, as depicted in Figure 1:

- Programmatic Safety Precepts (PSPs) – Program management principles and guidance that will help insure safety is adequately addressed throughout the lifecycle process.
- Operational Safety Precepts (OSPs) – A safety precept directed specifically at system operation. Operational rules that must be adhered to during system operation. These safety precepts may generate the need for Design Safety Precepts (DSPs).
- DSPs – General design guidance intended to facilitate safety of the system and minimize hazards. Safety design precepts are intended to influence, but not dictate, specific design solutions.

Safety precepts are another building block in the system safety process.

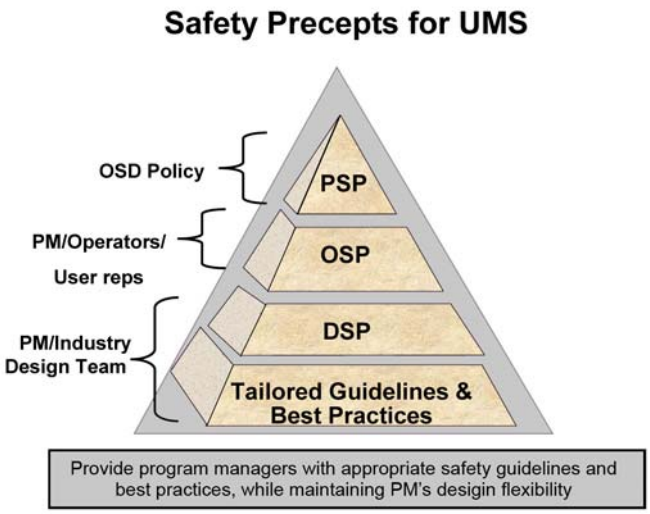

Figure 1. Levels of Safety Precepts for Unmanned Systems

1.3 Authorized Entity

An authorized entity is defined as: "An individual operator or control element authorized to direct or control system functions or mission."

As UMSs evolve and increase in their level of autonomy, a system operator or human controller may no longer be a valid assumption; control may be completely relinquished to the UMS. Systems may use man-to-machine or machine-to-machine control. In this context, the term "authorized entity" is used to denote the entity which, by design, exercises immediate control over the UMS.

2. System Safety Overview

Balancing the elimination or reduction of ESOH hazards with an informed and structured risk assessment and acceptance process is essential for positively contributing to a program's efforts in meeting the system's life cycle cost, schedule, and performance requirements. The program manager should strive to eliminate or reduce ESOH risks as part of the system's total life cycle risk reduction strategy. Without forethought during a system design process, or appropriate planning during operational events, ESOH risks can result in a mishap which may, in turn, result in any number of negative consequences to include loss of life, serious injury, major equipment damage, or failures with adverse impact on mission capability. System safety engineering practices are uniformly applied throughout the DoD acquisition process. System safety practices facilitate identification of hazards associated with potential ESOH hazards and provide techniques to manage, mitigate, or eliminate them. The UMS safety precepts, provided in Sections 4, 5, and 6 of this guide, represent a minimum set of safety considerations to address known, undesired UMS ESOH potential mishap risks and provide concepts for reducing the probability of occurrence, the potential consequences, or both. When risk are identified that are not addressed by these precepts, tailoring or creation of new precepts is encouraged.

A well-planned and executed system safety program is required to achieve the overall safety objectives of any DoD program. All DoD Program Managers (PMs) must establish and execute system safety programs using Military Standard (MIL-STD) 882 "DoD Standard Practice for System Safety" to manage the system's ESOH risks as part of the overall systems engineering process. Also, the program should address hazards posed during all phases of the system lifecycle, and should include risks posed to all assets with the potential to be harmed by the system.

2.1 System Safety and the UMS Precepts

Military Standard 882 delineates an approach to the practice of system safety engineering used in the management of environment, safety, and occupational health mishap risks encountered in the development, test, production, use, and disposal of DoD systems, subsystems, equipment, and facilities. This approach conforms to the acquisition procedures in DoDI 5000.2 and provides a consistent means of evaluating identified mishap risks. System safety requirements are performed throughout a systems life cycle, the primary benefits are realized when system safety practices are conducted prior to formal design efforts. This approach to safety ensures safety is designed into the system from the beginning of the item's development. When system safety practices are maintained throughout the systems lifecycle, the system's design and operation are further validated and improved upon when new efficiencies are discovered. When properly applied, system safety practices should ensure the identification and understanding of all known hazards and their mishap risk, and associated programmatic risks. Moreover, these practices will ensure identified mishap risks are eliminated or reduced to acceptable levels.

The UMS Precepts provided herein are most effective when they are applied in a manner that is in keeping with the system safety practices provided in MIL-STD-882. These UMS Precepts should be implemented as early in the systems acquisition process as possible, and executed in concert with a programs system safety effort.

These UMS safety precepts are guiding principles or doctrines that, when properly considered and applied, will serve to enhance or facilitate the implementation of safety into a system. These safety precepts are designed to influence the safety of system designs, and system design decisions by providing critical design safety requirements that can be assimilated into detailed design specifications during early and final system design machinations. The critical safety design guidance provided through these precepts has been developed to convey or articulate a desirable fundamental safeguard without constraining the design or design options. Verification of mishap risk reduction, claimed as a result of implementing these UMS safety precepts, should be conducted at appropriate points in a systems design.

2.2 Characteristics of Successful System Safety Programs

There are three (3) factors that are worthy of noting for their direct contribution to successful system safety programs; each feed and support the other.

a. Safety Participation Initiated Early in the Lifecycle Planning and Maintained Throughout the Program. The responsibility for safety needs to be clearly and unambiguously identified at the onset of the program. Early identification and control of safety-critical hardware, software and operations is the key to achieving a successful system safety program. Hazard analysis and assessment historically have been the most effective technique to determine hazards and develop safety requirements to mitigate risks. Coupled with use of the system safety mitigation order of precedence, hazard analysis lets a program identify early in the lifecycle those risks which can be eliminated by design, and those which must undergo mitigation by other controls in order to reduce risk to an acceptable level.

   Implementation of these precepts fosters early and continued safety involvement in the development of a system. By requiring early and continuous accountability of a UMS program to safety precepts, a positive impact can be achieved to the safety of UMSs.

b. Safety Expertise. MIL-STD-882 is the foundation for military safety guidance. It is effective in guiding what needs to be done, and in some instances, how to develop a safe system. Effective system safety programs are the result of system safety practitioners implementing the requirements of MIL-STD-882, and other appropriate safety guidance prescribed by their organizational management. This safety guide focuses specifically on UMSs and provides another resource to UMS safety practitioners.

c. Positive Safety Culture. Organizations that develop and maintain effective safety programs typically do so by institutionalizing a positive safety culture. Safety culture is a subset of the overall culture of the organization. It follows that the safety performance of organizations is greatly influenced by aspects of management that have not traditionally been seen as part of safety. As evidence, analytical reports of some major safety incidents have revealed a general lack of safety culture; for instance, the Chernobyl mishap, the Space Shuttle Columbia mishap, and the Ford Pinto design. In such cases, it is speculated that a positive safety culture would have significantly reduced the potential for these mishaps.

   A positive safety culture requires the interaction of all program participants, to include stakeholders and managers, in the safety process. Furthermore, it requires all program activities to set, as a tenet, the commitment to always consider potential safety implications

during any decision making processes. The PM must ensure the commitment of some individuals is not eviscerated by contradictory decision making philosophies or design processes. Various studies have clearly identified certain factors that characterize organizations with a positive safety culture. These factors include:

- Safety leadership and commitment of the chief executive
- Effective safety roles for line management
- Involvement of all employees in safety
- Effective communications and commonly understood and agreed-upon goals
- Good organizational learning and responsiveness to change
- Manifest attention to workplace safety and health
- A questioning attitude and a rigorous and prudent approach by all individuals.

The Advisory Committee on the Safety of Nuclear Installations (ACSNI) report contains a prompt-list of indicators of positive safety culture intended to assist organizations in reviewing their own culture. "Improving safety culture is something which must be seen as a long term and systematic process, based on an initial assessment of the existing safety culture, determining priorities for change, the actions necessary to effect the change and then going on to review progress before repeating the process indefinitely."[1]

3. Unmanned System Safety Overview

3.1 Unique Aspects of Military Unmanned Systems

Military UMSs provide numerous advantages to the DoD due to the variety of their applications, each of which presents unique safety challenges. Some military example applications include:

- Weapons platform (missiles, bombs, bullets, torpedoes) (air, ground and water)
- Explosive Ordnance Disposal (EOD)
- Breaching and clearing mine fields
- Surveillance/reconnaissance
- Search and rescue
- Delivering supplies to troops
- Automated repair/maintenance.

Most UMSs involve a vehicle that traverses ground, water, air, outer space or a combination of any of these modes to perform a desired task or goal. Along with the advantages of using a UMS as opposed to humans, significant safety concerns are also realized. Recent initiatives to employ UMSs as weapons delivery platforms revealed new or additional risk in the control of the weapons. For instance, without direct human control or intervention, a weapon could potentially be delivered to a target that is no longer hostile, whereas a human could have recognized the change in target profile and not delivered the weapon. Additionally, using UMS platforms to

[1] Institution of Electrical Engineers (IEE) – Health and Safety Briefing 07 – Safety Culture, http://www.iee.org/Policy/Areas/Health/hsb07.cfm

investigate or operate in dangerous environments present new risks when retrieving that UMS after its exposure to dangerous environmental conditions. For instance, employing a UMS to investigate an unknown environment, that turns out to be contaminated with Chemical, Biological, or Radiological (CBR) waste could result in exposing those humans retrieving the UMS to CBR contamination. Finally, a UMS itself, depending on its design, can present hazards to humans by its construction. Because of the reduced human interaction, a UMS may be constructed of materials and components that may present inherent hazards, such as hydraulics, pneumatics, or high-level Radio Frequency RF emitters. Safety concerns for these and other unique aspects of UMSs and their Concept of Operations (CONOPS) were addressed.

Understanding lifecycle phases, operational functions, and UMS subsystems aided in precept formulations. Various UMS lifecycle phases, illustrated in Figure 2, were studied to provide a characterization of a variety of demands and environments, anticipated across the lifecycle of a UMS. Characterization of these anticipated demands and environments aided greatly in the identification of potential UMS hazards and potential mishap risks.

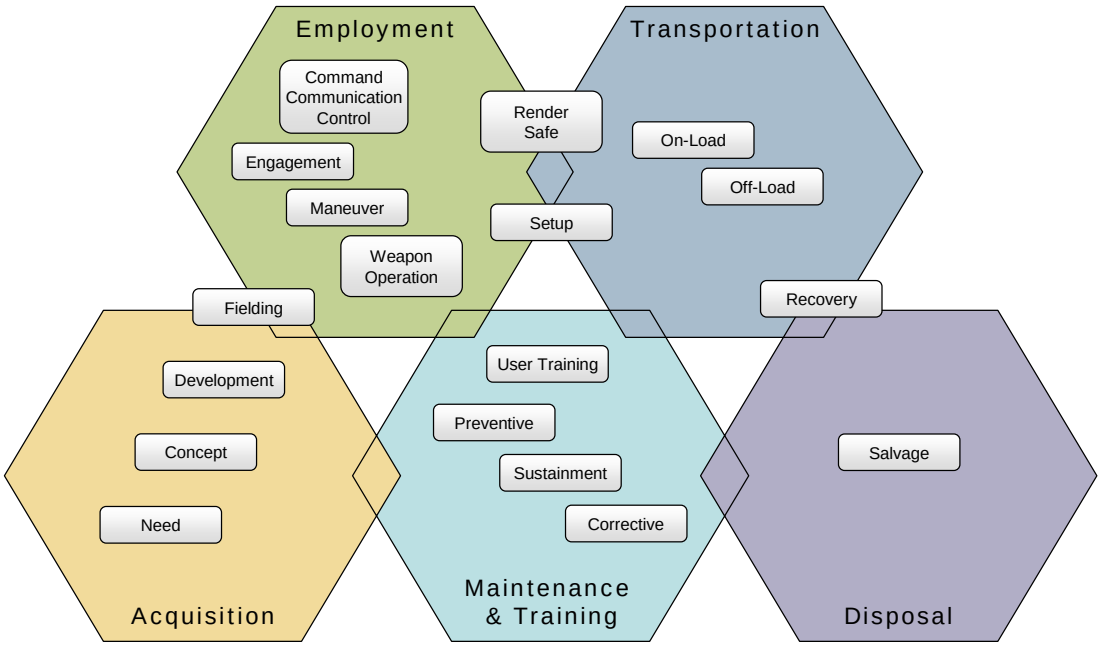

Figure 2. UMS Lifecycle Diagram

In manned systems, mishaps may ultimately be mitigated by a human operator. Because UMSs may not have a human in the loop, they possess unique safety concerns and issues. Autonomous UMSs are inherently hazardous to humans for many different reasons, ranging from unpredictable movements, to inherently hazardous components/subsystems, to loss of absolute control, to potential failures in both hardware and software. Weaponized UMSs present even more significant and complex dangers to humans. Typical safety concerns for military UMSs considered:

- Loss of control over the UMS.
- Loss of communications with the UMS.

- Loss of UMS ownership (lost out of range or to the enemy).
- Loss of UMS weapons.
- Unsafe UMS returns to base.
- UMS in indeterminate or erroneous state.
- Knowing when a UMS potentially is in an unsafe state.
- Unexpected human interaction with the UMS.
- Inadvertent firing of UMS weapons.
- Erroneous firing of UMS weapons.
- Erroneous target discrimination.
- UMS injures operators, own troops, etc.
- UMS equipment injures operators, own troops, etc.
- Enemy jamming or taking control of UMS.
- Loss of, or inadequate, situational awareness.
- Provision for emergency operator stop.
- Battle damage to UMS.
- UMS exposure to radiation, biological contamination, etc.

The aforementioned safety analysis and CONOPS studies provided the prerequisite underpinnings for development of the safety precepts provided in Sections 4, 5, and 6, and the detailed precept information provided in Appendix E of this guide. These Sections also provide additional details that were explored relating to the unique operational and functional challenges for UMSs such as situational awareness, command and control, and weaponization.

3.2 Top Level Mishaps for Unmanned Systems

A Top Level Mishap (TLM) is a mishap outcome that can be caused by one or more hazards; its purpose is to serve as a collection point for all of the potential hazards that can result in the same overall TLM outcome, but have different causal factors. TLMs provide a design safety focal point and help highlight and track major safety concerns. “Top level” does not necessarily imply a particular level of safety importance, but rather the common category visible at the system level (i.e. all hazards will fall within a particular TLM). As a result of this UMS safety initiative, nine TLMs presented in Table 1 were established for both general purpose and weaponized UMSs. These TLMs may be used by any UMS program to assist in identification of the crucial safety areas a PM should be concerned about. Each UMS may, and likely will, induce new or other TLMs, therefore considerable thought should be given to the use of each of these TLMs prior to its adoption.

Table 1. UMS Top Level Mishaps

	Top Level Mishaps (TLMs)
TLM-1	Unintended/Abnormal system mobility operation
TLM-2	Inadvertent firing or release of weapons
TLM-3	Engagement/Firing upon unintended targets
TLM-4	Self-damage of own system from weapon fire/release
TLM-5	Personnel injury

	Top Level Mishaps (TLMs)
TLM-6	Equipment damage
TLM-7	Environmental damage
TLM-8	Vehicle loss
TLM-9	Vehicle collision

The various safety precepts developed for UMSs have been specifically directed at resolving one or more of these TLMs. Safety precepts were developed to provide definitive indicators of where the primary program safety efforts will be required in development of UMSs. The precepts provide focus and guidance for design, and are the precursor for detailed design safety requirements. In addition, safety precepts are often used to help establish the tasks and priorities for a system safety program.

4. Unmanned System Safety Program Aspects

4.1 Safety Precepts

Safety precepts for UMSs did not previously exist; they evolved through an arduous, but thorough, systems engineering process performed as part of this Office of the Secretary of Defense (OSD) UMS safety initiative. The systems engineering process for establishing the safety precepts is shown in Figure 3. Through an iterative process of functionally assessing the safety of UMSs and continually comparing precepts, issues, definitions and causal factors, the precepts were refined resulting in the UMS safety precepts presented in Tables 2, 3, and 4 of this guide.

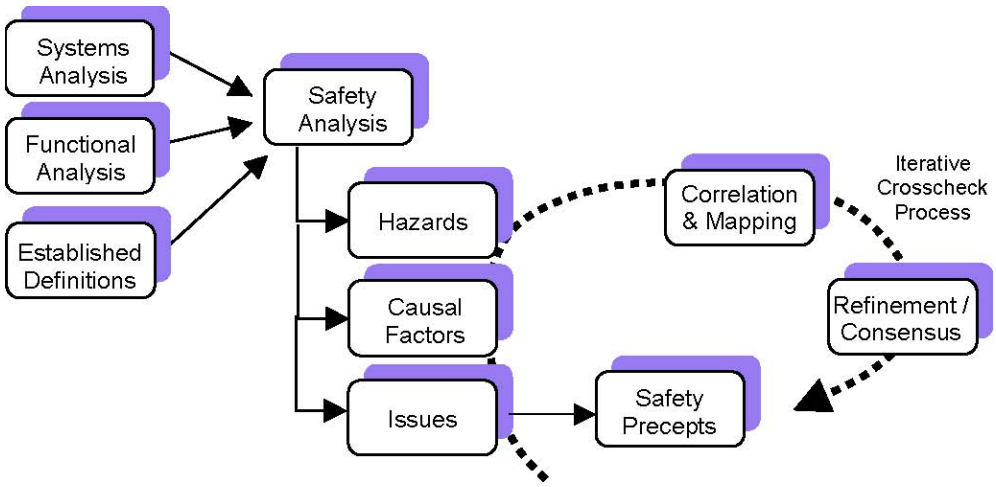

Figure 3. Safety Precept Development Process

A separate study was then performed to determine if current DoD and/or Service-specific policies addressed each of the safety precepts. This study included interviews with DoD and Service personnel and review of more than 115 DoD policy, guidance, instructions, standards, and best practices documents for applicability to the developed safety precepts. For each precept, the study provided an overall assessment of what policy exists (if any) and a detailed mapping of the precept to DoD policy. The results of this study indicate:

- Safety precept PSP-1 is completely addressed in both DoD and Service-specific policies.
- Three precepts (PSP-4, PSP-6, and DSP-1) are completely addressed in DoD policy and are partially addressed in Service-specific policies.
- Safety precept PSP-3, DSP-11, DSP-12, and DSP-19 are partially addressed in both DoD and Service-specific policies.
- Nine precepts (PSP-2, OSP-1, OSP-3, OSP-5, DSP-7, DSP-13, DSP-14, DSP-16, DSP-18) are not addressed in DoD policy but are partially addressed in Service-specific policy.

- Twelve precepts (PSP-5, OSP-2, OSP-4, DSP-2, DSP-4, DSP-5, DSP-6, DSP-8, DSP-9, DSP-10, DSP-15 and DSP-17) are not addressed in DoD nor Service-specific policies.

- One precept DSP-3 was not mapped to policy.

For each precept, the following was recorded: the policy document and associated section, applicable service, and comments indicating whether the policy document directly references the precept, partially references the precept, or implies the precept. The term "reference" is used when the text specifically states the safety precept. The term "partially references" is used when the text addresses some, but not all, of the elements of the precept or the scope of the document is limiting. The term "implies" is used when the text does not reference the precept specifically but the precept could be considered to be covered by the more general wording. This information has been included in the precept detailed clarification tables provided in Appendix E. The details of this study including the goals, objectives, methodology, accomplishments, results and conclusions can be found at http://www.acq.osd.mil/atptf/ .

The precepts, presented in this guide, are provided as a generic and minimum set of precepts for consideration for any UMS safety program. While deviation from these precepts be documented, it is fully anticipated new precepts could be established, or these precepts can be tailored, for individual safety programs in addition to, or in replacement of, these precepts.

Appendix E provides precept clarification tables that include:

- A scope statement addressing the applicability of each safety precept.
- A rationale statement explaining why each safety precept is required.
- Examples of system functions or operational events germane to the intent of each safety precept.
- Additional detailed considerations to assist in implementation of the safety precept.
- Identification of any existing policy, DoD or Service-specific, that addresses, partially addresses, or implies the intent of the safety precept.

4.2 Programmatic Safety Precepts

At the program level, UMS safety requirements reinforce what we have learned and do for manned systems. We are responsible for protecting the public, the warfighter, our assets, and the environment; safety is an integral part of this responsibility. For a program to be successful in developing a safe system, it is incumbent upon the Program Office to establish early safety lifecycle planning and participation, and to instill a robust safety culture in the program. The PSPs, presented in Table 2, provide a mechanism to accomplish this. PSPs are intended as program management principles and guidance; they are designed to ensure safety is adequately addressed throughout the UMS lifecycle process. Once the PSPs are adopted by a program, the success of developing a safe system relies upon the factors noted above in Section 2.2, Characteristics of Successful System Safety Programs; use of the DSPs and OSPs; and the commitment of management, at all levels, to safety.

Table 2. Programmatic Safety Precepts

	Programmatic Safety Precepts (PSPs)
PSP-1*	The Program Office shall establish and maintain a System Safety Program (SSP) consistent with MIL-STD-882.
PSP-2*	The Program Office shall establish unifying safety precepts and processes for all programs under their cognizance to ensure: • Safety consistent with mission requirements, cost and schedule. • Mishap risk is identified, assessed, mitigated, and accepted. • Each system can be safely used in a combined and joint environment. • That all safety regulations, laws, and requirements are met.
PSP-3*	The Program Office shall ensure that off-the-shelf items (e.g., Commercial Off The Shelf (COTS), Government Off The Shelf (GOTS), Non-Developmental Item (NDI)), re-use items, original use items, design changes, technology refresh, and technology upgrades (hardware and software) are assessed for safety, within the system.
PSP-4*	The Program Office shall ensure that safety is addressed for all life cycle phases.
PSP-5	Compliance to and deviation from these safety precepts shall be addressed during all Milestone decisions and formal reviews such as System Requirements Review (SRR), Preliminary Design Review (PDR), and Critical Design Review (CDR).
PSP-6*	The Program Office shall ensure UMS designs comply with current safety and performance criteria.

While this document serves only as a guide, usage of the terms “shall” and “should” reflects the level of concern of the safety community.

* Denotes applicability to both manned and unmanned systems.

5. Unmanned Systems Operational Aspects

The safety of a system is most evident when it is taken from the test environment and placed in an operational setting in the hands of the warfighter. Based on the study of several UMS CONOPS, several safety issues associated with the operation of UMSs were identified. Where appropriate, these safety issues were developed into OSPs. While the safety issues discovered were most frequently associated with a UMS being employed with weapons, the resultant OSPs should be considered for any UMS platform.

5.1 Unmanned Systems Operational Safety Functionality

Assessing the appropriate application of OSPs requires an understanding of UMS command and control authorities – who or what will be controlling the operation of the UMS. In some cases, the control of a UMS may be conducted by a human operator from a remote location through a remote control console. In other cases, control may be an autonomous function of the UMS or its operation may be the result of pre-programmed mission parameters and commands. In still other cases, control may be provided by another UMS or multiple UMSs in a networked environment. Thus, key to the proper application of OSPs is determination of whom or what the UMS controlling entity is. In developing the safety precepts provided in this guide, both human and autonomous methods of control were considered. The terms used throughout this guide and in the precepts to describe these two methods of control are authorized entity(ies) and controlling entity(ies). Both of these terms are briefly discussed in Section 1.4 and are defined in Appendix C. In short, an authorized and controlling entity is a design-intended control element of a UMS with decision making authority, human or machine, and designated to command the UMS.

Two fundamental UMS capabilities have significant impact on the system's operation: the intent for these systems to be recoverable; and, that there is no "person" on-board. The OSPs, presented in Table 3, address the safe operation and recovery of a UMS. These OSPs are intended to address operation functions and modes such as:

a. Asset recovery and decontamination. While out of sight and possibly out of communication, the UMS may have been exposed to a hazardous environment, or may return in such a manner that it presents the receiving entity with a hazard, such as having hazardous devices attached. Additionally, a battle damaged UMS may be hazardous to recover in itself. These pose hazardous situations to the recovery/maintenance team; therefore the system has to be designed to consider these operational safety issues.

b. Command and control. Communication with a UMS may have been severed, intentionally or unintentionally; there must be assurance the control link has not been broken or compromised and re-establishment of communications is executed safely. The controlling entity needs to assure he/she/it has regained communication with the intended system. As the levels of autonomy are increased for UMSs, we will need to define the levels of required control and communication. There are safety issues associated with hostile action and a need to assure a UMS does not fall into enemy hands and be used against friendlies. Certainly not least is assurance of clear access to sufficient bandwidth necessary to safely accomplish assigned missions.

c. Weaponization. The weaponization of UMSs presents critical safety issues. Each user may have different operational objectives, weapons resources, and weapons engagement

requirements. These unique objectives and requirements typically will be stated in the user's CONOPS. For instance, some CONOPS will reflect a need for weapons to be combat ready for engagement as soon as possible, whereas other CONOPS may not require immediate combat readiness. It is paramount that the projected UMS CONOPS be understood so safe operation of weapons can be designed into the system.

d. Situational Awareness. Situational Awareness (SA) is significantly influenced by the operational environment. Developmental and operational test procedures must emulate system operational environments and anticipated environmental stimuli. An evaluation of the required SA functionality must be conducted in the anticipated environment under realistic scenarios, and is a fundamental underpinning to any safety assessment of UMS operational readiness. There is currently no quantifiable data available on how many UMSs can be operated by one person and where the information saturation point lies. Stated simply, for a given level of autonomy, the Program must characterize and evaluate how much responsibility can safely be given to the system for its own operations.

Additionally, UMS controller training or certification presents unique challenges for each branch of the military. Each branch of the military has differences in their planned or ongoing UMS training and certification processes. For example, one Service may require a UMS operator to be a trained and experienced professional in the equivalent human operator role as a prerequisite to becoming a UMS operator; whereas, another Service may not require experience and expertise in a particular area of operations prior to operating a UMS in the same environment. These and other concerns are reflected in the OSPs.

5.2 Operational Safety Precepts

OSPs are safety precepts directed specifically at system operation: operational rules that must be adhered to during system operation. These safety precepts may generate the need for DSPs.

Table 3. Operational Safety Precepts

	Operational Safety Precepts (OSPs)
OSP-1	The controlling entity(ies) of the UMS should have adequate mission information to support safe operations.
OSP-2	The UMS shall be considered unsafe until a safe state can be verified.
OSP-3	The authorized entity(ies) of the UMS shall verify the state of the UMS, to ensure a safe state prior to performing any operations or tasks.

	Operational Safety Precepts (OSPs)
OSP-4*	The UMS weapons should be loaded and/or energized as late as possible in the operational sequence.
OSP-5*	Only authorized, qualified and trained personnel with the commensurate skills and expertise, using authorized procedures, shall operate or maintain the UMS.

While this document serves only as a guide, usage of the terms “shall” and “should” reflects the level of concern of the safety community.

* Denotes applicability to both manned and unmanned systems.

6. Unmanned Systems Design Aspects

Design safety precepts provide detailed and specific guidance to address safety issues associated with UMSs. This guidance is the direct result of experience and lessons learned on both manned and unmanned systems.

6.1 Unmanned Systems Design Safety Functionality

In evaluating UMS CONOPS for potential hazards, causes, and contributors, a categorization of functions is necessary. These general functions include, but are not limited to: Weaponization, Command and Control, Situational Awareness, and States and Modes. The following sections delineate these functional categories and are complementary to the UMS safety precepts associated with these categories.

6.1.1 Weaponization

A key safety concern of decision making authorities involved in the design, development, and operational use of UMSs, is the level of UMS weaponization. These DSPs apply to all UMSs, regardless of branch of Service, and complement the goals and objectives of any Service safety review authority.

Weapons technology and weapons associated functionalities pertinent to these DSPs include: conventional munitions, including guns and ammunition, fuzes, and dispenser munitions; “smart” munitions; suspension and release equipment; directed energy weapons; and RF and Infrared (IR) countermeasure systems. Issues addressed through these DSPs include:

- Weapons release authorization validation.
- Weapons release verification.
- Weapons release abort/back-out, including clean-up or reset of weapons inhibits.
- Embedded training inhibits.
- Safety-critical functions and data.
- The level of situational awareness in: display of target, target area, target-related information (accurate and true), target identification, use of Blue Force tracking data or Identification Friend or Foe (IFF) data.
- System state and its identification.
- Weapon state: safe or armed.
- Safe separation of weapons.
- Independent redundant safety features.

This safety functionality is primarily reflected in the DSPs and, to a lesser degree, in the PSPs and OSPs.

6.1.2 Situational Awareness (Information, Intelligence, and Method of Control (I2C))

Situational Awareness (SA) is another key safety concern in use of UMSs. Figure 4 depicts the SA challenge associated with levels of autonomous control. Without direct human control of a system, an exponential increase in awareness information must be gathered by the UMS and sent to, or used locally, by the controlling entity to fully understand the tactical environment. Initially, the working definition of situational awareness was selected by consensus from several available publications:

"Situational Awareness: The perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the future. In generic terms the three levels of situational awareness are level 1-perception, level 2-comprehension, and level 3-projection. There is both individual and group or team situational awareness."

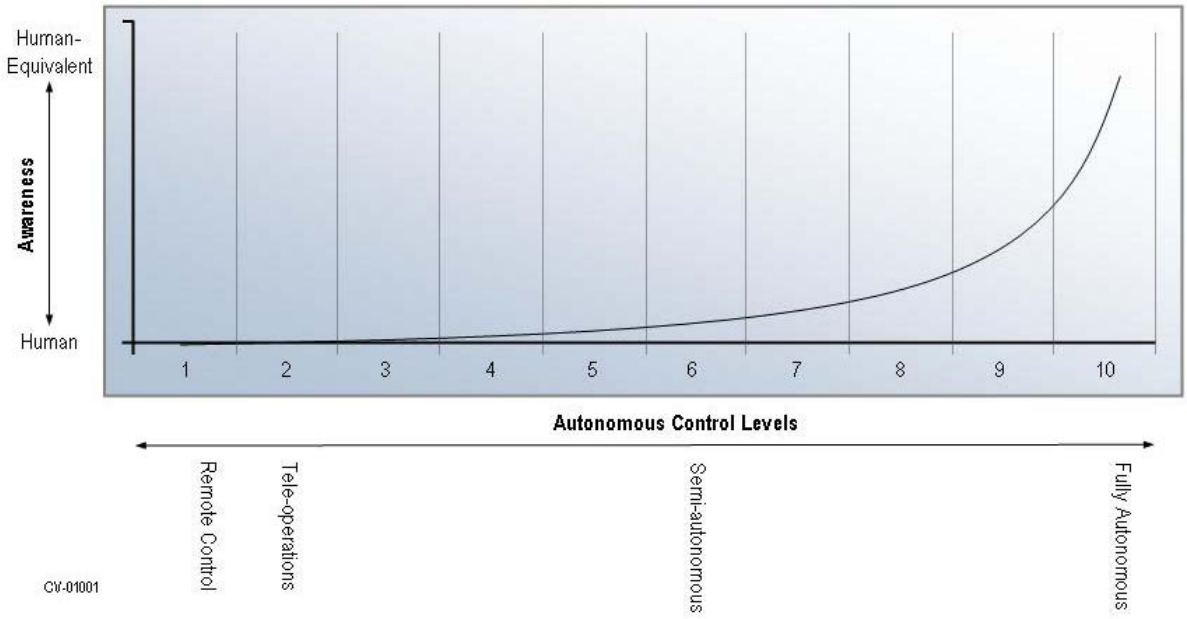

Figure 4. UMS Levels of Awareness vs. Levels of Control

A key problem encountered by human factors and SA practitioners is the variety of interpretations of what comprises adequate SA. In short, SA is most frequently driven by the internal and external environmental stimuli encountered within specific operational environments. The following more descriptive set of terms is provided to delineate some of the general considerations necessary to characterize what adequate SA is for UMSs:

Information, Intelligence, and Mode of Control (I2C):

"Information: Knowledge or data necessary for the safe operation of a UMS; obtained from the process of recognizing and interpreting data in the environment, memory and recall of facts, and/or communication."

"Intelligence: The capacity of a UMS to acquire, comprehend, and apply information."

"Method of Control: The means or manner in which an operator interacts, influences, or directs a UMS; a function of three non-exclusive systems attributes: mode of control, level of authority, and level of control."

"Mode of Control: The means by which a UMS receives instructions governing its actions and feeds back information, such as remote control, tele-operation, semi-autonomous, and fully autonomous."

"Level of Authority: The degree to which an entity is invested with the power to access the control and function of a UMS. Level I – Reception and transmission of secondary imagery or data. Level II – Reception of imagery or data directly from the UMS. Level III – Control of the UMS payload. Level IV – Full control of the UMS excluding deployment and recovery. Level V – Full control of the UMS including deployment and recovery."

"Level of Control: Locus (intersection) at which a controlling entity interacts, influences, or directs a UMS(s) such as: actuator, primitive, subsystem, vehicle, group of vehicles, or system of systems."

Potential mishaps that require a focus on SA include: collision and obstacle avoidance, maneuvering near or among people and equipment/assets, and knowledge of system states as related to weapons enable/fire/release or lasing. Additionally, adequate SA relies heavily upon system response to operator actions and input. Responses must indicate whether or not the intended information, input by the operator, was in fact received and effected the intended change in the UMS condition.

Likewise, the UMS responses (feedback) to the operator must foster the appropriate level of trust that the operator should have regarding the operation of the UMS. An example would be an instance where the operator relies on the UMS to distinguish between hostile and friendly elements. For an instance like this, an inappropriate level of trust could result in a fratricide event (i.e., friendly fire) depending on the operator's perception of an imminent threat. This implies that the operator may need to be aware of the reliability and validity of UMS feedback in order to know when (and when not) to use the information provided by the UMS.

6.1.3 Command and Control

Command and control of a UMS is heavily affected by SA. To address the level of adequacy of the controlling entity's/entities SA, the UMS program must characterize and address the following functionalities:

- The appropriate number of UMSs a human operator can safely control. (Related: For a given level of autonomy, there must be a complementary level of responsibility given to a UMS for its own safety.)
- Define what "Positive Control" means for higher levels of autonomy.
- Safely passing control of a UMS from one controller to another. (Related: "Forward Pass" of a weapon launched from one platform, with targeting provided by another.)
- Ensure control links to a UMS are maintained and appropriate notification is provided in the event control links are broken or compromised, while maintaining safe operations. (e.g. Electromagnetic Interference (EMI) or jamming).
- Loss and restoration of communications.
- Bandwidth, data latency, and data aging.
- Login and password authentication.
- Maintenance actions.
- Electro-mechanical or software upgrades.
- Failsafe features prohibiting enemy capture and re-use of a UMS.

6.1.4 States and Modes

A State identifies the conditions in which a system or subsystem can exist. A system or subsystem may be in only one state at a time. States are unique and may be binary (i.e., they are either true or not true). A state is a subset of a mode.

A Mode identifies operational segments within the system mission. Modes consist of one or more sub-modes. A system may be in only one mode, but may be in more than one sub-mode, at any given time.

The overall safety of a system depends upon understanding its states within various modes and during transitions between them; this is particularly true in UMSs. These include: training, maintenance, battlefield weapons-loaded embedded training, initialization, start-up, stop, test, and normal operations.

A safe state is a state in which the system poses an acceptable level of risk for the operational mode and environment. For example, "weapons armed" is not a safe state during logistics and pre-deployment modes but "weapons armed" is a safe state when engaging a target (except to the enemy).

An issue of particular concern with states and modes would include reprogramming or reconfiguration of Programmable Logic Devices (PLDs) or UMS software while in the field. This concern is compounded in cases where there is no human in the loop. Changes to UMS functionality could, and likely will, be introduced in UMSs as a result of new software loads to the system. These new software loads could occur in the field, and in fact, could occur via the Global Information Grid (GIG) or internet. If software upgrades or changes, including field expedient software upgrades or changes, are not considered during the design and development phase of UMS acquisition, failures could be introduced by incompatible hardware/software configurations or an incomplete or incorrect software load during state or mode transitions.

Functionality associated with states and modes is reflected in several DSPs.

6.2 Design Safety Precepts

Design safety precepts are general design guidance intended to facilitate safety of the system and minimize hazards. DSPs are intended to influence, but not dictate, specific design solutions. The nineteen (19) DSPs presented in Table 4 are intended to provide PMs with appropriate safety guidelines and best practices, while maintaining design flexibility.

Table 4. Design Safety Precepts

	Design Safety Precepts (DSPs)
DSP-1*	The UMS shall be designed to minimize the mishap risk during all life cycles phases.
DSP-2	The UMS shall be designed to only respond to fulfill valid commands from the authorized entity(ies).

	Design Safety Precepts (DSPs)
DSP-3	The UMS shall be designed to provide information, intelligence, and method of control (I2C) to support safe operations.
DSP-4*	The UMS shall be designed to isolate power until as late in the operational sequence as practical from items such as: a) Weapons, b) Rocket motor initiation circuits, c) Bomb release racks, or d) Propulsion systems.
DSP-5*	The UMS shall be designed to prevent release and/or firing of weapons into the UMS structure or other weapons.
DSP-6*	The UMS shall be designed to prevent uncommanded fire and/or release of weapons or propagation and/or radiation of hazardous energy.
DSP-7*	The UMS shall be designed to safely initialize in the intended state, safely and verifiably change modes and states, and prevent hazardous system mode combinations or transitions.
DSP-8*	The UMS shall be designed to provide for an authorized entity(ies) to abort operations and return the system to a safe state, if possible.
DSP-9*	Safety critical software for the UMS design shall only include required and intended functionality.
DSP-10*	The UMS shall be designed to minimize single-point, common mode or common cause failures that result in high and/or serious risks.
DSP-11*	The UMS shall be designed to minimize the use of hazardous materials.
DSP-12*	The UMS shall be designed to minimize exposure of personnel, ordnance, and equipment to hazards generated by the UMS equipment.
DSP-13*	The UMS shall be designed to identify to the authorized entity(ies) the weapon being released or fired, but prior to weapon release or fire.
DSP-14*	In the event of unexpected loss or corruption of command link, the UMS shall transition to a pre-determined and expected state and mode.

	Design Safety Precepts (DSPs)
DSP-15*	The firing of weapons systems shall require a minimum of two independent and unique validated messages in the proper sequence from the authorized entity(ies), each of which shall be generated as a consequence of separate authorized entity action. Both messages should not originate within the UMS launching platform.
DSP-16	The UMS shall be designed to provide contingencies in the event of safety critical failures or emergencies involving the UMS.
DSP-17	The UMS shall be designed to ensure safe recovery of the UMS.
DSP-18*	The UMS shall ensure compatibility with the test range environment to provide safety during test and evaluation.
DSP-19*	The UMS shall be designed to safely operate within combined and joint operational environments.

While this document serves only as a guide, usage of the terms “shall” and “should” reflects the level of concern of the safety community.

* Denotes applicability to both manned and unmanned systems.

Appendix A. References and Resource Guide

AAP-6, Revision 5, NATO Glossary of Terms and Definitions
ANSI/ITSDF B56.5-2005 Safety Standard for Guided Industrial Vehicles and Automated Functions of Manned Industrial Vehicles
ANSI/RIA 15.06-1999, American International Standard for Industrial Robots and Robot Systems – Safety Requirements (American National Standards Institute; Robotic Industries Association)
Allied Ordnance Publication (AOP)-38, Glossary of Terms and Definitions Concerning the Safety and Suitability for Service of Munitions, Explosives and Related Products, April 2002
Army Regulation 385-16, System Safety Engineering and Management, 2 November 2001
AT&L Knowledge Sharing System (AKSS) (http://deskbook.dau.mil/jsp/default.jsp)
Navy Handbook SWO20-AH-SAF-010 Weapons System Safety Guidelines Handbook
Defense Acquisition University (DAU) 11th Edition Glossary Defense Acquisition Acronyms And Terms, Sept 2003
Defense Acquisition Guidebook (http://akss.dau.mil/dag/)
Defense Acquisition University Continuous Learning Modules (https://learn.dau.mil/html/clc/Clc.jsp)
Department of Energy (DOE) M 440.1-1 Explosives Safety Manual, May 2000
DO-178B, Software Considerations in Airborne Systems and Equipment Certification, December 1992
Electronics Industries Association (EIA) Safety Engineering Bulletin (SEB) No. 6A System Safety Engineering in Software Development, April 1990
ESOH Special Interest Area on ACC (https://acc.dau.mil/esoh)
Federal Aviation Administration (FAA), System Safety Handbook: Practices and Guidelines for Conducting System Safety Engineering and Management, Dec 2000
Institute of Electrical and Electronics Engineers (IEEE) Std 1228-1994 for Software Safety Plans, March 17, 1994
International Council on Systems Engineering (INCOSE) Systems Engineering Handbook, INCOSE-TP-2003-016-02, version 2a, 1 June 2004
Joint Publication 1-02, DoD Definitions (http://www.dtic.mil/doctrine/jel/doddict/)
Joint Robotic Program Master Plan FY2005
Joint Software System Safety Committee Joint Software System Safety Handbook, Dec 1999

MIL-STD-882D, DoD Standard Practice for System Safety, 10 February 2000
MIL-HDBK-764, System Safety Engineering Design Guide for Army Materiel, 12 January 1990
MIL-STD-2105C, DoD Test Method Standard, Hazard Assessment Tests for Non-Nuclear Munitions, 14 July 2003
MIL-STD-464, DoD Interface Standard, Electromagnetic Environmental Effects Requirements for Systems, 18 March 1997
MIL-STD-1316E, DoD Design Criteria Standard, Safety Criteria for Fuze Design, 10 July 1998
MIL-STD-1901A, DoD Design Criteria Standard, Safety Criteria for Munition Rocket and Missile Motor Ignition System Design, 6 June 2002
MIL-STD-1910A
National Aeronautics and Space Administration NASA-GB-8719.13, NASA Software Safety Guidebook, March 31, 2004
National Institute of Standards and Technology (NIST) Special Publication 1011, Autonomy Levels for Unmanned Systems (ALFUS) Framework, version 1.1
Society of Automotive Engineers ARP 4754, Aerospace Recommended Practice, Certification Considerations for Highly-Integrated or Complex Aircraft Systems
Society of Automotive Engineers ARP 4761, Aerospace Recommended Practice, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
STANAG 4586, Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability
The Joint Architecture for Unmanned Systems (JAUS) Compliance Specification, version 1.1, 10 March 2005
The Navy Unmanned Undersea Vehicle (UUV) Master Plan, November 9, 2004
Unmanned Aircraft Systems Roadmap 2005 - 2030
USAF System Safety Handbook, Air Force Safety Agency, Kirtland AFB, July 2000

Appendix B. Acronyms

ACSNI	Advisory Committee on the Safety of Nuclear Installations
AT&L	Acquisition, Technology and Logistics
CBR	Chemical, Biological, or Radiological
CDR	Critical Design Review
CONOPS	Concept of Operations
COTS	Commercial Off The Shelf
DAG	Defense Acquisition Guidebook
DoD	Department of Defense
DoDI	Department of Defense Instruction
DSP	Design Safety Precept
EMI	Electromagnetic Interference
EOD	Explosive Ordnance Disposal
ESOH	Environment, Safety, and Occupational Health
GIG	Global Information Grid
GOTS	Government Off The Shelf
I2C	Information, Intelligence, and Method of Control
IF	Infrared
IFF	Identification Friend or Foe
INSAG	International Nuclear Safety Advisory Group
MIL-STD	Military Standard
NASA	National Aeronautical and Space Administration
NDI	Non-developmental Item
NIST	National Institute of Standards and Technology
OPR	Office of Primary Responsibility
OSD	Office of the Secretary of Defense
OSP	Operational Safety Precept
OUSD	Office of the Undersecretary of Defense
PDR	Preliminary Design Review
PLD	Programmable Logic Devices
PM	Program Manager
PSP	Programmatic Safety Precept

RF	Radio Frequency
SA	Situational Awareness
SRR	System Requirements Review
SSE/DTE	Systems and Software Engineering/Developmental Test and Evaluation
SSP	System Safety Program
TLM	Top Level Mishap
UMS	Unmanned System

Appendix C. Definitions

Reference Sources

1	MIL-STD-882C, Military Standard, System Safety Program Requirements, Jan1993
2	MIL-STD-882D, Department Of Defense, Standard Practice For System Safety, Feb 2000
3	Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms 12 April 2001 (As Amended Through 20 March 2006) (http://www.dtic.mil/doctrine/jel/doddict/)
4	ANSI/RIA 15.06-1999, American International Standard for Industrial Robots and Robot Systems – Safety Requirements (American National Standards Institute; Robotic Industries Association)
5	STANAG 4586, Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability, March 2005
6	INCOSE-TP-2003-016-02, INCOSE Systems Engineering Handbook, Version 2a, June 2004, copyright 2002, 2004 by INCOSE
7	Joint Software System Safety Committee Joint Software System Safety Handbook, Dec 1999
8	Joint Robotic Program Master Plan FY2005
9	Army Regulation 385-16, System Safety Engineering and Management, Nov 2001
10	System Safety Handbook: Practices and Guidelines for Conducting System Safety Engineering and Management, Federal Aviation Administration, Dec 2000
11	USAF System Safety Handbook, Air Force Safety Agency, Kirtland AFB, July 2000
12	Reprinted with permission from Society of Automotive Engineers ARP 4761 © 1996, Aerospace Recommended Practice, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
13	Reprinted with permission from Society of Automotive Engineers ARP 4754 © 1996, Aerospace Recommended Practice, Certification Considerations for Highly-Integrated or Complex Aircraft Systems
14	MIL-HDBK-764, System Safety Engineering Design Guide for Army Materiel, Jan 1990
15	AAP-6, Revision 5, NATO Glossary of Terms and Definitions, 2005
16	MIL-STD-1316E, Department Of Defense Design Criteria Standard Fuze Design, Safety Criteria for, July 1998
17	CECOM-TR-92-2, Software System Safety Guide, Us Army Communications And Electronics Command, May 1992
18	MIL-STD-1901A, Department Of Defense Design Criteria Standard, Munition Rocket and Missile Motor Ignition System Design, Safety Criteria for, June 2002
19	IEEE Std 1228-1994, IEEE Standard for Software Safety Plans, Aug 1994
20	EIA SEB-6A, System Safety Engineering in Software Development, April 1990
21	DOE M 440.1-1, DOE Explosives Safety Manual, May 2001
22	NASA-GB-8719.13, NASA Software Safety Guidebook, March 2004
23	AOP-38, Glossary Of Terms And Definitions Concerning The Safety And Suitability For Service Of Munitions, Explosives And Related Products, April 2002
24	Glossary Defense Acquisition Acronyms And Terms, Defense Acquisition University (DAU), 11th Edition,

	Sept 2003
25	Defense Acquisition Guidebook
26	MIL-STD-2105C, Department Of Defense Test Method Standard, Hazard Assessment Tests For Non-Nuclear Munitions, July 2003
27	MIL-STD-464, Department Of Defense Interface Standard, Electromagnetic Environmental Effects, Requirements for Systems, March 1997
28	MIL-STD-882D, Department Of Defense Standard Practice For System Safety, 10 Feb 2000
29	NIST Special Publication 1011, Autonomy Levels for Unmanned Systems, (ALFUS) Framework, Volume I: Terminology, Version 1.1, Sept 2004
30	MIL-STD-2088, Bomb Rack Unit(BRU), Aircraft, General Design Criteria For, May 1997
31	NAVSEA OP5 Volume 1, Ammunition and Explosives Safety Ashore
32	STANAG 4187 (Edition 3), Fuzing System – Safety Design requirements, Nov 2001
33	MIL-STD-483A, Military Standard, Configuration Management Practices for Systems, Equipment, Munitions and Computer Programs, June 1985
34	Cognitive System Engineering Consortium (http://kn.gdais.com/ASPs/CoP/EntryCoP.asp?Filter=GD-WB-CS)
35	MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects and Criticality Analysis (FMEA), 24 Nov 1980
36	Unmanned Systems Safety Working Group

Definitions

Term	Ref	Definition
Abort	36	The premature termination of a function, procedure or mission.
Acceptable Risk	10	Acceptable risk is the part of identified risk that is allowed to persist without further engineering or management action. Making this decision is a difficult yet necessary responsibility of the managing activity. This decision is made with full knowledge that it is the user who is exposed to this risk.
Accident	36	An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment
Actuator	4	A mechanism used to effect motion: (1) A power mechanism which converts electrical, hydraulic or pneumatic energy to effect motion. (2) A mechanical mechanism within a control device (e.g. a rod which opens contacts.) (3) A device (e.g. specialized key) which initiates a (un)locking sequence.
Airworthiness	12	The condition of an item (aircraft, aircraft system, or part) in which that item operates in a safe manner to accomplish its intended function.
Anomalous Behavior	10	Behavior which is not in accordance with the documented requirements
Anomaly	22	A state or condition which is not expected. It may or may not be hazardous, but it is the result of a transient hardware or coding error.
Architecture	10	The organizational structure of a system, identifying its components, their interfaces and a concept of execution between them.

Arm	21	A general term that implies the energizing of electronic and electrical circuitry, which in turn controls power sources or other components used to initiate explosives. The arming operation completes all steps preparatory to electrical initiation of explosives except the actual fire signal.
Armed	23	The state of the (sub-) system when all safety breaks and switches have been made ineffective with the exception of the single function which would initiate *the* intended operation of the system.
Artificial Intelligence	8	The programming and ability of a robot to perform functions that are normally associated with human intelligence, such as reasoning, planning, problem solving, pattern recognition, perception, cognition, understanding, learning, speech recognition, and creative response. Artificial intelligence is an inherent requirement in all future robotics systems and will support a range of evolving requirements.
Assembly	13	A number of parts, subassemblies, or any combination thereof, joined together to perform a specific function and which can be disassembled without destruction of designed use.
Authorized Entity	36	An individual operator or control element authorized to direct or control system functions or mission.
Automatic Mode	4	Operating mode in which the control system operates in accordance with the task program.
Automatic Operation	4	The state in which the robot is executing its programmed task as intended.
Automation	8	The capability of a machine or its components to perform tasks previously done by humans. Usually accomplished by a subsystem of a larger system or process, performance of tasks can be cued by humans or a point in the process. Examples are an autoloader in an artillery system or the welding of parts on an assembly line by machines.
Autonomous	29	Operations of an Unmanned System (UMS) wherein the UMS receives its mission from the human and accomplishes that mission with or without further Human-Robot Interaction (HRI). The level of HRI, along with other factors such as mission complexity, and environmental difficulty, determine the level of autonomy for the UMS. Finer-grained autonomy level designations can also be applied to the tasks, lower in scope than mission.
Autonomy	29	(1) The condition or quality of being self-governing. (2) A UMS's own ability of sensing, perceiving, analyzing, communicating, planning, decision-making, and acting, to achieve its goals as assigned by its human operator(s) through designed HRI. Autonomy is characterized into levels by factors including mission complexity, environmental difficulty, and level of HRI to accomplish the missions.
Backout and Recovery	14	The action(s) necessary in a contingency to restore normal safety conditions and to avoid a potential accident.
Barrier	10	A material object or set of objects that separates, demarcates, or services as a barricade; or something immaterial that impedes or separates. Both physical and non-physical barriers are utilized and applied in hazard control; i.e. anything used to control, prevent or impede unwanted adverse energy flow and/or anything used to control, prevent or impede unwanted event flow.
Baseline	36	The approved, documented configuration of a software, hardware, or firmware configuration item, that thereafter serves as the basis for further development and that can be changed only through change control procedures.
Blast	14	The shock wave emitted from a point of detonation. Includes a shock front, a high-pressure area behind the shock front, and a rarefaction.
Booster	3	(1) A high-explosive element sufficiently sensitive so as to be actuated by small explosive elements in a fuze or primer and powerful enough to cause detonation of the main explosive filling. (2) An auxiliary or initial propulsion system which travels with a missile or aircraft and which may or may not separate from the parent craft when its impulse has been delivered. A booster system may contain, or consist of, one or more units.

Build	7	(1) A version of software that meets a specified subset of the requirements that the completed software will meet. (2) The period of time during which such a version is developed. [MIL-STD-498]
Built-in Test	29	Equipment or software embedded in operational components or systems, as opposed to external support units, which perform a test or sequence of tests to verify mechanical or electrical continuity of hardware, or the proper automatic sequencing, data processing, and readout of hardware or software systems.
Burning	26	The least violent type of explosive event (reaction Type V). The energetic material ignites and burns, non-propulsively. The case may open, melt or weaken sufficiently to rupture nonviolently, allowing mild release of combustion gases. Debris stays mainly within the area of the fire. This debris is not expected to cause fatal wounds to personnel or be a hazardous fragment beyond 15 m (49 feet).
Cascading Failure	13	A failure for which the probability of occurrence is substantially increased by the existence of a previous failure.
Causal Factor	36	See Hazard Causal Factor
Cease-Fire	3	(1) A command given to any unit or individual firing any weapon to stop engaging the target. (2) A command given to air defense artillery units to refrain from firing on, but to continue to track, an airborne object. Missiles already in flight will be permitted to continue to intercept.
Certification	10	Legal recognition by the certification authority that a product, service, organization or person complies with the applicable requirements. Such certification comprises the activity of checking the product, service, organization or person and the formal recognition of compliance with the applicable requirements by issue of certificate, license, approval or other document as required by national law or procedures. In particular, certification of a product involves: (a) the process of assuring the design of a product to ensure that it complies with a set of standards applicable to that type of product so as to demonstrate an acceptable level of safety, (acceptable risk); (b) the process of assessing an individual product to ensure that it conforms to the certified type design; (c) the issue of any certificate required by national laws to declare that compliance or conformity has been found with applicable standards in accordance with item (a).
Certification Authority	10	The organization or person responsible within the state (country) concerned with the certification of compliance with applicable requirements.
Cognitive Overload	36	A situation where an individual's information processing capability is exceeded, resulting in an increased likelihood of inappropriate action or inappropriate response.
Cognitive Systems Engineering	34	A design discipline that uses analyses of work (practice, structure, purposes and constraints) to inform the design of process and technology for Human-System integration.
Cognizance Levels	29	The levels of what a UMS can know or understand based on its sensory processing capability: ▪ Level 1: Data, or observed data. In initially processed forms after measured by sensors. ▪ Level 2: Information. Further processed, refined and structured data that is human understandable. ▪ Level 3: Intelligence, knowledge, combat and actionable information. Further processed for particular mission needs. Directly linked to tactical behaviors.
Collaboration	29	The process by which multiple manned or unmanned systems jointly work together by sharing data, such as coordinates of their maneuver(s) and local Common Relative Operational Picture (CROP), or by acquiring intelligence to perform a mission synergistically, i.e., perform better than each could have alone.
Combined	3	Between two or more forces or agencies of two or more allies. (When all allies or services are not involved, the participating nations and services shall be identified, e.g., combined navies). See also "Joint".

Commercial-Off-The-Shelf (COTS)	2	Commercial items that require no unique government modifications or maintenance over the life cycle of the product to meet the needs of the procuring agency.
Common Cause	12	Event or failure which bypasses or invalidates redundancy or independence.
Common Mode Failure	13	An event which simultaneously affects a number of elements otherwise considered to be independent.
Complexity	12	An attribute of systems or items which makes their operation difficult to comprehend. Increased system complexity is often caused by such items as sophisticated components and multiple interrelationships.
Component	13	Any self-contained part, combination of parts, subassemblies or units, that perform a distinctive function necessary to the operation of the system.
Computer Firmware	24	The combination of a hardware device and computer instructions of computer data that reside as a read-only software on the hardware device. The software cannot be readily modified under program control. See also "Firmware".
Computer Hardware	7	Devices capable of accepting and storing computer data, executing a systematic sequence of operations on computer data, or producing control outputs. Such devices can perform substantial interpretation, computation, communication, control, or other logical functions. [MIL-STD-498]
Computer Program	7	A combination of computer instructions and data definitions that enables computer hardware to perform computational or control functions. [MIL-STD-498]
Computer Software Component (CSC)	24	A functional or logically distinct part of a Computer Software Configuration Item (CSCI), or Software Configuration Item (SCI). A CSC is typically an aggregate of two or more Computer Software Units (CSU).
Computer Software Configuration Item (CSCI)	7	An aggregation of software that satisfies an end-use function and is designated for separate configuration management by the acquirer. CSCIs are selected based on tradeoffs among software function, size, host or target computers, developer, support concept, plans or reuse, criticality, interface considerations, need to be separately documented and controlled, and other factors. [MIL-STD-498]
Computer Software Unit (CSU)	36	The smallest subdivision of a Computer software configuration Item (CSCI) for the purposes of engineering management. CSUs are typically separately compiled and testable pieces of code.
Concept of Operations (CONOPS)	3	A verbal or graphic statement, in broad outline, of a commander’s assumptions or intent in regard to an operation or series of operations. The concept of operations frequently is embodied in campaign plans and operation plans; in the latter case, particularly when the plans cover a series of connected operations to be carried out simultaneously or in succession. The concept is designed to give an overall picture of the operation. It is included primarily for additional clarity of purpose. Also called commander’s concept or CONOPS.
Concurrent Operations	21	Operations performed simultaneously and in close enough proximity that an incident with one operation could adversely influence the other.
Configuration	10	The requirements, design and implementation that define a particular version of a system or system component.
Configuration Baseline	6	The configuration documentation formally designated by the Government at a specific time during a system’s or configuration item’s life cycle. Configuration baselines, plus approved changes from those baselines, constitute the current configuration documentation. There are three formally designated configuration baselines, namely the functional, allocated, and product baselines.
Configuration Item (CI)	24	An aggregation of hardware, firmware, computer software, or any of their discrete portions, which satisfies an end use function and is designated by the government for separate configuration management. CIs may vary widely in complexity, size, and type, from an aircraft, electronic, or ship system to a test meter or round of ammunition. Any item required for Logistics Support (LS) and designated for separate procurement is a CI.

Configuration Management	22	The process of identifying and defining the configuration items in a system, controlling the release and change of these items throughout the system life cycle, recording and reporting the status of configuration items and change requests, and verifying the completeness and correctness of configuration items.
Conformance	13	Established as correct with reference to a standard, specification or drawing, (derived from Computer Aided Software Testing (CAST) discussions).
Contingency	36	A situation requiring special plans, rapid response, and special procedures to ensure the safety of personnel, equipment and facilities.
Contingency Analysis	14	A type of analysis conducted to determine procedures, equipment, and materials required to prevent a contingency from deteriorating into an accident.
Control Element	36	An electro-mechanical element of a UMS designed to control the UMS and has decision making capability. (A computer would be considered an electro-mechanical element.)
Control Entity	36	An individual operator or control element directing or controlling system functions or mission.
Cooperative Operations	36	The ability of two or more systems to share data, coordinate maneuvers, and perform tasks synergistically.
Coordination	29	The ability for UMSs or manned systems to work together harmoniously through common data such as mission or task plans, coordinates of maneuver(s), local CROP, etc. A common way is for a superior to coordinate the task execution of the subordinates to accomplish the missions.
Crashworthiness	14	The capability of a vehicle to protect its occupants against an accidental impact.
Credible Environment	16	An environment that a device may be exposed to during its life cycle (manufacturing to tactical employment, or eventual demilitarization). These include extremes of temperature and humidity, electromagnetic effects, line voltages, etc. Combinations of environments that can be reasonably expected to occur must also be considered within the context of credible environments.
Credible Failure	22	A condition that has the potential of occurring based on actual failure modes in similar systems.
Critical Failure	36	A failure that may cause a mission abort, mission failure, personal death or injury, equipment damage, or environmental damage.
Critical Temperature	21	Temperature above which the self-heating of an explosive causes a runaway reaction. It is dependent on mass, geometry, and thermal boundary conditions.
Criticality	13	Indication of the hazard level associated with a function, hardware, software, etc., considering abnormal behavior (of this function, hardware, software, etc.) alone, or in combination with external events.
Damage	36	The undesired effects or consequences of a mishap or enemy action.
Danger	10	Danger expresses a relative exposure to a hazard. A hazard may be present, but there may be little danger because of the precautions taken.
Danger Zone	36	Physical area where injury, loss of life, or system damage may potentially result.
Data	6	(1) Recorded information, regardless of form or characteristics, including administrative, managerial, financial, scientific, technical, engineering, and logistics data, whether required to be delivered to the Government or retained by the contractor, as well as data developed by the Government. (MIL-STD-480B, Para 3.1.23) (2) Recorded information, regardless of form or method of the recording. (MIL-STD-961C, Para 3.8; MIL-HDBK-59A, App A, Para 30.4.1) (3) The raw materials from which a user extracts information. Data may include numbers, words, pictures, etc. (MIL-STD-1472D, Para 3.12)
Data Link	3	The means of connecting one location to another for the purpose of transmitting or receiving data.

Deactivated Code	22	(1) A software program or routine or set of routines, which were specified, developed and tested for one system configuration and are disabled for a new system configuration. The disabled function(s) is/are fully tested in the new configuration to demonstrate that if inadvertently activated the function will result in a safe outcome within the new environment. (2) Executable code (or data) which by design is either (a) not intended to be executed (code) or used (data), or (b) which is only executed (code) or used (data) in certain configurations of the target system.
Dead Code	22	(1) Dead Code is code (a) unintentionally included in the baseline, (b) left in the system from an original software configuration, not erased or overwritten and left functional around it, or (c) deactivated code not tested for the current configuration and environment. (2) Executable code (or data) which, as a result of design, maintenance, or installation error cannot be executed (code) or used (data) in any operational configuration of the target system and is not traceable to a requirement (e.g., embedded identifier is OK).
Defect	36	State of an item consisting of the non-performance or non-conformance with specified requirements by a characteristic of the item. A defect may, but need not, lead to a failure.
Deflagration	26	The fourth most violent type of explosive event (Reaction Type IV). Ignition and burning of the confined energetic materials leads to nonviolent pressure release as a result of a low strength case or venting through case closures (loading port/fuze wells, etc.). The case might rupture but does not fragment; closure covers might be expelled, and unburned or burning energetic material might be thrown about and spread the fire. Propulsion might launch an unsecured test item, causing an additional hazard. No blast or significant fragmentation damage to the surroundings; only heat and smoke damage from the burning energetic material.
Derived Requirements	6	Those characteristics typically identified during synthesis of preliminary product or process solutions and during related trade studies and verifications. They generally do not have a parent function and/or performance requirement but are necessary to have generated system elements accomplish their intended function.
Design Safety Precept (DSP)	36	General Design Guidance intended to facilitate safety of the system and minimize hazards. Safety design precepts are intended to influence, but not dictate, specific design solutions.
Detonation	26	The most violent type of explosive event (Reaction Type I). A supersonic decomposition reaction propagates through the energetic material to produce an intense shock in the surrounding medium (air or water for example) and very rapid plastic deformation of metallic cases, followed by extensive fragmentation. All energetic material will be consumed. The effects will include large ground craters for munitions on or close to the ground, holing/plastic flow damage/fragmentation of adjacent metal plates, and blast overpressure damage to nearby structures.
Detonation, Partial	26	The second most violent type of explosive event (Reaction Type II). Some, but not all of the energetic material reacts as in a detonation. An intense shock is formed; some of the case is broken into small fragments; a ground crater can be produced, adjacent metal plates can be damaged as in a detonation, and there will be blast overpressure damage to nearby structures. A partial detonation can also produce large case fragments as in a violent pressure rupture (brittle fracture). The amount of damage, relative to a full detonation, depends on the portion of material that detonates.
Dormant Code	22	Similar to dead code, it is software instructions that are included in the executable but not meant to be used. Dormant code is usually the result of COTS or reused software that includes extra functionality over what is required.
Dud	16	A munition which has failed to function, although functioning was intended.
Electrical Bonding	21	Electrical connection between two conductive objects intended to prevent development of an electrical potential between them.
Electrically Initiated Device (EID)	27	Any component activated through electrical means and having and explosive, pyrotechnic, or mechanical output resulting from an explosive or pyrotechnic action, and electro-thermal devices having a dynamic mechanical, thermal, or electromagnetic output. Examples

		include bridgewire Electro-Explosive Devices (EEDs), conductive composition electric primers, semiconductor bridge EEDs, laser initiators, exploding foil initiators, slapper detonators, burn wires and fusible links.
Electro Explosive Device (EED)	23	A one shot explosive or pyrotechnic device used as the initiating element in an explosive or mechanical train and which is activated by the application of electrical energy.
Electromagnetic Environmental Effects (E^3)	27	The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including electromagnetic compatibility; electromagnetic interference, electromagnetic vulnerability, electromagnetic pulse, electronic protection, hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning and p-static.
Emergency Stop	36	The operation of a circuit that overrides controls, removes drive power, causes all moving parts to stop, and removes power from other hazardous functions but does not cause additional hazards.
Emulator	10	A combination of computer program and hardware that mimic the instruction and execution of another computer or system.
Enabling	16	The act of removing or activating one or more safety features designed to prevent arming, thus permitting arming to occur subsequently.
End-Effector	4	An accessory device or tool specifically designed for attachment to the robot wrist or tool mounting plate to enable the robot to perform its intended task. (Examples may include gripper, spot weld gun, arc weld gun, spray paint gun, or any other application tools.)
Envelope	4	The three dimensional volume of space encompassing the movements of all robot parts. See also "Space".
Environment	6	The natural environment (weather, climate, ocean conditions, terrain, vegetation, space conditions); combat environment (dust, fog, nuclear-chemical-biological); threat environment (effects of existing and potential threat systems to include electronic warfare and communications interception; operations environment (thermal, shock, vibration, power variations); transportation and storage environment; maintenance environment; test environments; manufacturing environments (critical process conditions, clean room, stress) and other environments (e.g. software engineering environment, electromagnetic) related to system utilization.
Error	22	(1) Mistake in engineering, requirement specification, or design. (2) Mistake in design, implementation or operation which could cause a failure.
Expendable	36	An item that may be consumed in use and may be dropped from stock record accounts when it is issued or used.
Exploding Bridgewire (EBW)	21	An EED that is initiated by the discharge of a high current through the device bridgewire, causing the wire to explode and produce a shockwave. An EBW as defined herein is a device containing no primary explosive.
Explosion	26	The third most violent type of explosive event (Reaction Type III). Ignition and rapid burning of the confined energetic material builds up high local pressures leading to violent pressure rupturing of the confining structure. Metal cases are fragmented (brittle fracture) into large pieces that are often thrown long distances. Unreacted and/or burning energetic material is also thrown about. Fire and smoke hazards will exist. Air shocks are produced that can cause damage to nearby structures. The blast and high velocity fragments can cause minor ground craters and damage (breakup, tearing, gouging) to adjacent metal plates. Blast pressures are lower than for a detonation.
Explosion Proof	36	An item enclosed in a case that is capable of withstanding an explosion of a specified gas or vapor that may occur within it and of preventing the ignition of a specified gas or vapor surrounding the enclosure by sparks, flashes, or explosion of the gas or vapor within and that operates at such an external temperature that the surrounding flammable atmosphere will not be ignited thereby.
Explosive	26	A solid or liquid energetic substance (or a mixture of substances) which is in itself capable,

		by chemical reaction, of producing gas at such temperature, pressure and speed as to cause damage to the surroundings. Included are pyrotechnic substances even when they do not evolve gases. The term explosive includes all solid and liquid energetic materials variously known as high explosives and propellants, together with igniter, primer, initiation and pyrotechnic (e.g., illuminant, smoke, delay, decoy, flare and incendiary) compositions.
Explosive Train	23	(1) The detonation or deflagration transfer mechanism (i.e., train) beginning with the first explosive element (e.g., primer, detonator) and terminating in the main charge. (2) A set of functionally linked explosive components which receive, from the surroundings, a non-explosive input of energy, which provide the transmission of explosive phenomena and which produces as output one or several non-explosive effects (light, noise, shock waves, etc). The input energy may be: electrical, mechanical, photonic, heat, etc. The explosive phenomena are: combustion, deflagration, detonation. Their induced effects are: temperature, pressure, and shock. The output effects are: mechanical, thermal, photonic, etc.
Exposure Time	36	The period of time when an entity is vulnerable to some stated condition or event, e.g. hazard, failure, mishap.
Fail-Operational	10	A characteristic design which permits continued operation in spite of the occurrence of a discrete malfunction.
Fail-safe	10	A characteristic of a system whereby any malfunction affecting the system safety will cause the system to revert to a state that is known to be within acceptable risk parameters.
Failure	22	The inability of a system or component to perform its required functions within specified performance requirements.
Failure Cause	14	The physical or chemical processes, design defects, quality defects, part misapplication, or other processes that are the basic reason for failure or that initiate the physical process by which deterioration proceeds to failure.
Failure Rate	14	The total number of failures within an item population divided by the total number of life units expended by that population during a particular measurement interval under slated conditions.
Failure Tolerance	22	The ability of a system or subsystem to perform its function(s) or maintain control of a hazard in the presence of failures within its hardware, firmware, or software.
Fault	22	Any change in state of an item that is considered to be anomalous and may warrant some type of corrective action. Examples of faults included device errors reported by Built-In Test (BIT)/Built-In Test Equipment (BITE), out-of-limits conditions on sensor values, loss of communication with devices, loss of power to a device, communication error on bus transaction, software exceptions (e.g., divide by zero, file not found), rejected commands, measured performance values outside of commanded or expected values, an incorrect step, process, or data definition in a computer program, etc. Faults are preliminary indications that a failure may have occurred.
Fault Injection Process	20	The process of deliberately inserting faults into a system (by manual or automatic methods) to test the ability of the system to safely handle the fault or to fail to a safe state. Usually, fault injection criteria is defined by system safety and is implemented by the software test engineering group to measure the system's ability to mitigate potential mishaps to an acceptable level of risk.
Fire Classes	14	Classification of fires are according to the type of combustible involved: Class A: Ordinary combustibles such as wood, cloths, paper, rubber, and certain plastics. Class B: Flammable or combustible liquids, gases, greases, and similar materials. Class C: Energized electrical equipment. Class D: Combustible metals such as magnesium, titanium, zirconium, sodium, or potassium.
Fire Point	14	The lowest temperature at which a liquid gives off sufficient flammable vapor to produce sustained combustion after removal of the ignition source.

Firebrand	21	A projected burning or hot fragment whose thermal energy is transferred to a receptor.
Firmware	7	The combination of a hardware device and computer instructions and/or computer data that reside as read-only software on the hardware device. [MIL-STD-498]
Flammability Limits	14	The maximum and minimum amounts of combustible gas in air, i.e., concentrations (by volume), that are capable of propagating a flame. Flammability Range. The range between the lower and upper flammability limits.
Flammable Liquid	21	Any liquid having a flash point below 60°C and a vapor pressure not exceeding 280 kPa (41 psia) at 37.8°C. This is the definition as applied in this manual; it includes some materials defined as combustible liquids by the Department of Transportation (DOT).
Flash Point	14	The minimum temperature at which a liquid vaporizes sufficiently to form an ignitable mixture with air.
Fully Autonomous	29	A mode of operation of an UMS wherein the UMS is expected to accomplish its mission, within a defined scope, without human intervention. Note that a team of UMSs may be fully autonomous while the individual team members may not be due to the needs to coordinate during the execution of team missions.
Function	6	A task, action, or activity that must be performed to achieve a desired outcome.
Functional Requirement	6	The necessary task, action, or activity that must be accomplished. The initial set of top-level functions is the eight primary system life-cycle functions. Top-level functions are identified by requirements analysis and subdivided by functional analysis.
Fusion	29	(1) The combining or blending of relevant data and information from single or multiple sources (sensors, logistics, etc.) into representational formats that are appropriate to support the interpretation of the data and information and to support system goals like recognition, tracking, situation assessment, sensor management, or system control. Involves the process of acquisition, filtering, correlation, integration, comparison, evaluation and related activities to ensure proper correlations of data or information exist and draws out the significance of those correlations. The processes can be performed with a combination of human analysis/judgment and system processing. Also referred to as Information Fusion or Data Fusion. (2) Information processing that deals with the association, correlation, and combination of data and information from single and multiple sources to achieve refined position and identity estimation, complete and timely assessments of situations and threats, and their significance in the context of mission operation. The process is characterized by continuous refinement of its estimates and assessments, and by evaluation of the need for additional sources, or modification of the process itself, to achieve improved results.
Fuze	16	A physical system designed to sense a target or respond to one or more prescribed conditions, such as elapsed time, pressure, or command, and initiates a train of fire or detonation in a munition. Safety and arming are primary roles performed by a fuze to preclude ignition of the munition before the desired position or time.
GOTS	22	Government-Off-The-Shelf. This refers to government created software, usually from another project. The software was not created by the current developers (see also "Reusable Software Products"). Usually, source code is included and all available documentation, including test and analysis results.
Graceful Degradation	22	(1) A planned stepwise reduction of function(s) or performance as a result of failure, while maintaining essential function(s) and performance. (2) The capability of continuing to operate with lesser capabilities in the face of faults or failures, or when the number or size of tasks to be done exceeds the capability to complete.
Hang Fire	3	A malfunction that causes an undesired delay in the functioning of a firing system.
Hardware	13	An item that has physical being. Generally refers to such items as line replaceable units or modules, circuit cards, and power supplies.

Hazard	2	Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment.
Hazard Analysis	23	The systematic examination of a system or an item and its life cycle to identify hazardous situations and events including those associated with human, product and environmental interfaces, and to assess their consequences to the functional and safety characteristics of the system or the item.
Hazard Causal Factor (HCF)	36	Causal factors are the particular and unique set of circumstances, or initiating mechanisms, that transform a hazard into a mishap. Causal factors may be the result of failures, malfunctions, external events, environmental effects, errors, poor design or a combination thereof. Causal factors generally break down into categories of hardware, software, human action, procedures and/or environmental factors. The causal factors are the items that act as the initiating mechanism upon the hazard source to make it result in the actualized mishap. For example, aircraft fuel is a hazard source, and a fuel leak and a spark are the initiation mechanisms, or causal factors, that create a fire mishap event. When the fuel leak and spark occur together under the proper conditions, the mishap event immediately results. The mishap event results in some sort of loss consequence and severity, such as personnel death or injury.
Hazard Control	36	Any technique, device, or method designed to eliminate or reduce the mishap risk of hazards, unsafe conditions, or unsafe acts.
Hazard Description	36	A brief narrative description of a potential mishap attributable to the hazard. A hazard description contains three elements that express the threat: a source, an activity or a condition that serves as the root; the mechanism, a means by which the source can bring about the harm; and an outcome, the harm itself that might be suffered.
Hazard Risk Level	36	A relative measure of the mishap risk presented by a hazard.
Hazard Severity	22	An assessment of the consequences of the worst credible mishap that could be caused by a specific hazard.
Hazardous Function	36	A function whose operation, incorrect operation or failure to operate can result in a hazard.
Hazardous State	22	A state that may lead to an unsafe state.
Hidden Failure	14	Failure that is undetectable during operation by the operator or crew.
High Explosive	14	A material that normally detonates when subjected to heat or shock that initiates a violent disassociation of its molecules.
High-Energy Initiator	21	Exploding bridge wire systems, slapper detonators, and EEDs with similar energy requirements for initiation.
Human Engineering	6	The area of human factors that applies scientific knowledge to achieve effective user-system integration. (MIL-H-46855B, Para 6.2.6).
Human Error	14	Mistakes that are representative of the sympathies and frailties of man's nature.
Human Factors	6	A body of scientific facts about human characteristics. The term covers all biomedical and psycho-social considerations; it includes, but is not limited to, principles and applications in the areas of human engineering, personnel selection, training, life support, job performance aids, and human performance evaluation. (MIL-H-46855B, Para 6.2.7)
Human Systems Integration	36	A technical process, which ensures that the system is compatible with the warfighter's physical and cognitive attributes. It integrates the disciplines of Human Factors Engineering (HFE), Manpower, Personnel, Training, Habitability, Survivability, and Environmental, Safety, and Occupational Health (ESOH) into the systems engineering of a material system to ensure safe, effective operability and supportability
Human-Machine Interface	36	The means by which the human operator interacts with the UMS system. It includes the software applications, graphics, and hardware that allow the operator to effectively give instructions to or receive data from the UMS.
Identified Risk	10	Identified risk is that risk which has been determined through various analysis techniques. The first task of system safety is to identify, within practical limitations, all possible risks.

		This step precedes the determination of the significance of the risk (severity) and the likelihood of its occurrence (hazard probability). The time and costs of analysis efforts, the quality of the safety program, and the state of technology impact the number of risks identified.
Incident	10	A near miss accident with minor consequences that could have resulted in greater loss. An unplanned event that could have resulted in an accident, or did result in minor damage, and which indicates the existence of, though may not define, a hazard or hazardous condition. Sometimes called a mishap.
Independence	12	(1) A design concept which ensures that the failure of one item does not cause a failure of another item. (Derived from JAA AMJ 25.1309.) (2) Separation of responsibilities that assures the accomplishment of objective evaluation.
Independent Inhibit	22	Two inhibits are independent if no SINGLE failure, error, event, or environment can eliminate more than one inhibit. Three inhibits are independent if no TWO failures, errors, events or environments (or any pair of one of each) can eliminate more than two inhibits.
Independent Safety Feature	16	A safety feature is independent if its integrity is not affected by the function or malfunction of other safety features.
Independent Verification &Validation (IV&V)	10	Confirmation by independent examination and provision of objective evidence that specified requirements have been fulfilled, and that the particular requirements for a specific intended use are fulfilled.
Industrial Robot	4	An automatically controlled, reprogrammable multipurpose manipulator programmable in three or more axes which may be either fixed in place or mobile for use in industrial automation applications.
Inert Materials	21	Materials that shows no exothermic decomposition when tested by Differential Scanning Calorimeter (DSC) or Differential Thermal Analysis (DTA). Moreover, the inert material shall not show any incompatibility with energetic material with which it may be combined when tested by recognized compatibility tests. Inert material shall neither alter the onset of exotherm of the DSC or DTA trace of the energetic material nor increase the rate of decomposition or gas evolution of the energetic material.
Information	36	Knowledge or data necessary for the safe operation of a UMS; obtained from the process of recognizing and interpreting data in the environment, memory and recall of facts, and/or communication.
Infrared Radiation	14	Thermal radiation of wavelengths longer than those of visible light.
Inhibit	22	A design feature that provides a physical interruption between an energy source and a function (e.g., a relay or transistor between a battery and a pyrotechnic initiator, a latch valve between a propellant tank and a thruster, etc.).
Integration	12	(1) The act of causing elements of an item to function together. (2) The act of gathering a number of separate functions within a single implementation.
Intelligent Mobility	8	The ability to move up and over obstacles, avoid obstacles in the vehicle's path, and to move in novel ways using advanced locomotion.
Interface	6	The specifically defined physical or functional juncture between two or more configuration items.
Interface Requirement	6	The functional performance, electrical, environmental, human, and physical requirements and constraints that exist at a common boundary between two or more functions, system elements, configuration items, or system.
Interlock	14	A protective device to prevent human access to a hazardous area or to prevent or interrupt equipment operation unless other required conditions are satisfied.
Interoperability	3	(1) The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. (2) The condition achieved among communications-electronics systems or items of

		communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases.
Intrinsically Safe	21	An apparatus or system whose circuits are incapable of producing any spark or thermal effect capable of causing ignition of a mixture of flammable or combustible material under test conditions described in ANSI/UL913.
Ionization	14	The formation of electrically charged particles; can be produced by high-energy radiation, such as light or ultraviolet rays, or by collision of particles in thermal agitation.
Ionizing Radiation	14	Electromagnetic radiation having sufficiently large photon energy to ionize atomic or molecular systems directly with a single quantum event.
Item	6	A non-specific term used to denote any product, including systems, subsystems, assemblies, subassemblies, units, sets, parts, accessories, computer programs, or computer software. In this standard, it also denotes any process that includes a series of actions, changes, or functions to achieve an end or result.
Joint	3	Connotes, activities, operations, organizations, etc., in which elements of two or more Military Departments participate.
Joint Architecture for Unmanned Systems (JAUS)	8	An upper-level design for the interfaces within the domain of unmanned vehicles. It is a component-based, message-passing architecture that specifies data formats and methods of communication among computing nodes. It defines messages and component behaviors that are independent of technology, computer hardware, and vehicle platforms, and are isolated from mission. JAUS is prescribed for use by the Joint Requirements Panel (JRP) in the research, development, and acquisition of Unmanned Ground Vehicles (UGVs).
Latent Failure	14	A failure that is not inherently revealed at the time it occurs.
Level of Authority	36	The degree to which an entity is invested with the power to access the control and functions of a UMS. ▪ Level I: Reception and transmission of secondary imagery or data. ▪ Level II: Reception of imagery or data directly from the UMS. ▪ Level III: Control of the UMS payload. ▪ Level IV: Full control of the UMS excluding deployment and recovery. ▪ Level V: Full control of the UMS including deployment and recovery.
Level of Autonomy	29	Set(s) of progressive indices, typically given in numbers, identifying a UMS's capability for performing autonomous missions. Two types of metrics are used, Detailed Model for Autonomy Levels, and Summary Model for Autonomy Levels.
Level of Control	36	Locus at which a controlling entity interacts, influences, or directs a UMS(s). ▪ Actuator ▪ Primitive ▪ Subsystem ▪ Vehicle ▪ Group of vehicles ▪ System of systems
Levels of Fusion	29	Each of the six levels of fusion adds progressively greater meaning and involves more analysis: ▪ Level 0: Organize. This is the initial processing accomplished at or near the sensor that organizes the collected data into a usable form for the system or person who will receive it. ▪ Level 1: Identify/Correlate. This level takes new input and normalizes its data; correlates it into an existing entity database, and updates that database. Level 1 Fusion tells you what is there and can result in actionable information. ▪ Level 2: Aggregate/Resolve. This level aggregates the individual entities or elements, analyzes those aggregations, and resolves conflicts. This level captures or derives

		events or actions from the information and interprets them in context with other information. Level 2 Fusion tells you how they are working together and what they are doing. ▪ Level 3: Interpret/Determine/Predict. Interprets enemy events and actions, determines enemy objectives and how enemy elements operate, and predicts enemy future actions and their effects on friendly forces. This is a threat refinement process that projects current situation (friendly and enemy) into the future. Level 3 Fusion tells you what it means and how it affects your plans. ▪ Level 4: Assess. This level consists of assessing the entire process and related activities to improve the timeliness, relevance and accuracy of information and/or intelligence. It reviews the performance of sensors and collectors, as well as analysts, information management systems, and staffs involved in the fusion process. This process tells you what you need to do to improve the products from fusion level 0-3. ▪ Level 5: Visualize. This process connects the user to the rest of the fusion process so that the user can visualize the fusion products and generate feedback/control to enhance/improve these products.
Likelihood	10	Likelihood defines in quantitative or qualitative terms, the estimated probability of the specific Hazardous event under study. Likelihood is one element of associated risk. Fault Trees and other models can be constructed and individual Hazard Probabilities are estimated, and likelihood can be calculated via Boolean Logic. It should be noted that estimated likelihood defined in conventional hazard analysis may be appropriate due to the variability, conference, resources, and other factors.
Limiting Device	4	A device that restricts the maximum space by stopping or causing to stop all robot motion and is independent of the control program and the task programs.
Line-of-Sight	8	(1) Visually, a condition that exists when there is no obstruction between the viewer and the object being viewed. (2) In radio frequency communications, a condition that exists when transmission and reception is not impeded by an intervening object, such as dense vegetation, terrain, man-made structures, or the curvature of the earth, between the transmitting and receiving antennas.
Lockin	14	A protective device that restricts personnel inside specific limits to prevent contact with a hazard outside those limits or that maintains the hazard inside those limits so that it cannot affect anything outside.
Lockout	14	A protective device that restricts personnel outside specific limits to prevent contact with a hazard inside those limits or that maintains the hazard outside those limits so it cannot affect anything inside.
Lower Explosive Limit (LEL)	21	The concentration of vapor or dust in air below which an explosion cannot occur.
Lower Flammable Limit (LFL)	21	The concentration of a vapor or dust in air below which a burning reaction cannot be sustained.
Maintenance	6	The physical act of preventing, determining, and correcting equipment or software faults. It includes all actions taken to retain system/equipment/product in a useful serviceable condition or to restore it to usefulness/serviceability. Maintenance includes inspection, testing, servicing, classification as to serviceability, repair, rebuilding, and reclamation. (MIL-STD-1379D, Para 3.90)
Malfunction	12	The occurrence of a condition whereby the operation is outside specified limits.
Manipulator	8	In robotics, a mechanism consisting of an arm and an end-effector. It contains a series of segments, jointed or sliding relative to one another, for the purpose of modifying, grasping, emplacing, and moving objects. A manipulator usually has several degrees of freedom.
Man-Machine Interface	36	See "Human-Machine Interface".
Man-Portable	3	Capable of being carried by one man. Specifically, the term may be used to qualify:

		(1) Items designed to be carried as an integral part of individual, crew-served, or team equipment of the dismounted soldier in conjunction with assigned duties. Upper weight limit: approximately 14 kilograms (31 pounds.) (2) In land warfare, equipment which can be carried by one man over long distance without serious degradation of the performance of normal duties.
Man-Transportable	3	Items that are usually transported on wheeled, tracked, or air vehicles, but have integral provisions to allow periodic handling by one or more individuals for limited distances (100-500 meters). Upper weight limit: approximately 65 pounds per individual.
Marginal Failure	14	A failure that can degrade performance or result in degraded operation. (Special operating techniques or alternative modes of operation involved by the loss can be tolerated throughout a mission but should be corrected upon its completion.)
Marsupial	36	A design concept for UMS where a larger UMS carries one or more smaller UMS, either inside it or attached to it for later deployment.
Maximum Credible Event (MCE)	21	The MCE from a hypothesized accidental explosion or fire is the worst single event that is likely to occur from a given quantity and disposition of explosives/explosives devices. The event must be realistic with a reasonable probability of occurrence considering the explosive propagation, burning rate characteristics, and physical protection give to the items involved.
Maximum No-Fire Stimulus (MNFS)	16	The stimulus level at which the initiator will not fire or unsafely degrade with a probability of 0.995 at a confidence level of 95 percent. Stimulus refers to the characteristic(s) such as current, rate of change of current (di/dt), power, voltage, or energy which is (are) most critical in defining the no-fire performance of the initiator.
Maximum space	4	The volume of space encompassing the maximum designed movements of all robot parts including the end-effector, workpiece and attachments.
Mean Time Between Failures (MTBF)	13	Mathematical expectation of the time interval between two consecutive failures of a hardware item. The definition of this statistic has meaning only for repairable items. For non-repairable items, the term “mean life” is used.
Method of Control	36	The means or manner in which an operator interacts, influences, or directs an unmanned system; a function of three non-exclusive system attributes: ▪ Mode of control ▪ Level of authority ▪ Level of control
Misfire	3	(1) Failure to fire or explode properly. (2) Failure of a primer or the propelling charge of a round or projectile to function wholly or in part.
Mishap	2	An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.
Mishap Risk	36	An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence.
Mishap Risk Assessment	20	The process of determining the potential of a mishap in terms of severity and probability of occurrence; and, the results of that determination.
Mishap Risk Control	36	The Risk associated with the hazardous event under study is adequately controlled, by the reduction of severity and/or likelihood, via the application of engineering and/ or administrative hazard controls. Anything that mitigates or ameliorates the risk.
Mishap Risk Severity	36	The harm expected should the hazardous event occur, i.e.: loss, consequence, adverse outcome, damage, fatality, system loss, degradation, loss of function, injury; considering the risk associated with the hazardous event under evaluation.
Mission Module	36	A self-contained assembly installed on a UMS that enables the unmanned platform to perform special functions. It can be easily installed and replaced by another type of mission module.

Mission Planning	36	The generation of tactical goals, routes (general or specific), commanding structure, coordination, and timing for one or teams of UMSs. The mission plans can be generated either in advance by operators or in real-time by the onboard, distributed software systems. The latter case is also referred to as dynamic mission planning.
Mitigator	36	Any design changes, processes, or procedures used to eliminate or manage risks.
Mobility	29	The capability of a UMS to move from place to place, with its own power and while under any mode or method of control. Characteristics: the UMS's speed, location, and fuel availability [2]. Refueling could be performed either as a part of the HRI or autonomously by a fuel management autonomy task at a higher level.
Mobility	36	The capability of a UMS to move from place to place, while under any method of control, in order to accomplish its mission or function.
Mode	36	Modes identify operational segments within the system mission. Modes consist of one or more sub-modes. A system may be in only one mode, but may be in more than one sub-mode, at any given time.
Mode Confusion	36	Incorrect/erroneous awareness of the operational mode of system components at the subsystem, system, or system of systems level.
Mode of control	36	The means by which a UMS receives instructions governing its actions and feeds back information: ▪ Remote control ▪ Teleoperation ▪ Semi-autonomous ▪ Fully autonomous
Modularity	8	The property of flexibility built into a system by designing discrete units (hardware and software) that can easily be joined to or interfaced with other parts or units.
Navigation	36	The process whereby a UMS makes its way along a route that it planned, that was planned for it or, in the case of teleoperation, that a human operator sends it in real time.
Near Miss	14	An occurrence in which accidental injury or damage was narrowly avoided by chance and not by design.
Negative Obstacle	8	A terrain feature that presents a negative deflection relative to the horizontal plane of the UGV such that it prevents the UGV's continuation on an original path. Examples are depressions, canyons, creek beds, ditches, bomb craters, etc.
Network Latency	36	The time it takes for information to be transferred between computers in a network. In a non-trivial network, a data packet will be forwarded over many links via many gateways, each of which will not begin to forward the packet until it has been completely received. In such a network, the minimal latency is the sum of the minimum latency of each link, plus the transmission delay of each link except the final one, plus the forwarding latency of each gateway.
Non-Developmental Item (NDI)	6	(1) Any item of supply that is available in the commercial marketplace including COTS; (2) Any previously developed item of supply that is in use by a department or agency of the United States, a State or local government, or a foreign government with which the United States has a mutual defense cooperation agreement; (3) Any item of supply described in definition 1 or 2, above, that requires only minor modification in order to meet the requirements of the procuring agency; or (4) Any item of supply that is currently being produced that does not meet the requirements of definition 1, 2, or 3 above, solely because the item is not yet in use or is not yet available in the commercial marketplace.
Non-Developmental Software (NDS)	6	Deliverable software that is not developed under the contract but is provided by the contractor, the Government or a third party. NDS may be referred to as reusable software, Government Furnished Software (GFS), or commercially available software, depending on its service.

Non-Line-of-Sight	8	(1) Visually, a condition that exists when there is an obstruction between the viewer and the object being viewed. (2) In radio frequency communications, a condition that exists when there is an intervening object, such as dense vegetation, terrain, man-made structures, or the curvature of the earth, between the transmitting and receiving antennas, and transmission and reception would be impeded. An intermediate ground-, air-, or space-based retransmission capability may be used to remedy this condition.
Non-Safety-Critical Computer Software Component	20	Computer software component (unit) which does not control safety-critical hardware systems, subsystems, or components, and does not provide safety-critical information.
N-Version Software	22	Software developed in two or more versions using different specifications, programmers, languages, platforms, compilers, or combinations of some of these. This is usually an attempt to achieve independence between redundant software items. Research has shown that this method usually does not achieve the desired reliability, and it is no longer recommended.
Obstacle	29	(1) Any physical entity that opposes or deters passage or progress, or impedes mobility in any other way [12]. (2) Any obstruction designed or employed to disrupt, fix, turn, or block the movement of an opposing force, and to impose additional losses in personnel, time, and equipment on the opposing force. Obstacles can be natural, manmade, or a combination of both. [13] They can be positive, negative (e.g., ditches), or groupings (e.g., areas with high security alert) and can be moving or still.
Obstacle Avoidance	36	The action of a UMS when it takes a path around a natural or man-made obstruction that prevents its continuation on its original path.
Obstacle Detection	36	The capability of a UMS or its operator to determine that there is an obstruction, natural or man-made, positive or negative, in its path.
Obstacle Negotiation	36	The capability of a UMS or its operator to navigate through or over an obstacle once it is detected and characterized as negotiable.
Operating Space	36	The three dimensional volume encompassing the movements of all UMS parts through their axes.
Operational Area	3	An overarching term encompassing more descriptive terms for geographic areas in which military operations are conducted. Operational areas include, but are not limited to, such descriptors as area of responsibility, theater of war, theater of operations, joint operations area, amphibious objective area, joint special operations area, and area of operations.
Operational Environment	3	A composite of the conditions, circumstances, and influences that affect the employment of military forces and bear on the decisions of the unit commander.
Operational Safety Precept (OSP)	36	A safety precept directed specifically at system operation. Operational rules that must be adhered to during system operation. These safety precepts may generate the need for DSPs.
Operational Test and Evaluation (OT&E)	6	Test and evaluation, initial operational test and evaluation, and follow-on OT&E conducted in as realistic and operational environment as possible to estimate the prospective system military utility, operational effectiveness, and operational suitability. In addition, OT&E provides information on organization, personnel requirements, doctrine, and tactics. Also, it may provide data to support or verify material in operating instructions, publications, and handbooks. (MIL-STD-1785, Para 3.15)
Operations Function	6	The tasks, actions, and activities to be performed and the system elements required to satisfy defined operational objectives and tasks in the peacetime and wartime environments planned or expected.
Operator	4	The person designated to start, monitor and stop the intended operation of a robot or robot system. An operator may also interface with a robot for production purposes.
Operator Control Unit	29	The computer(s), accessories, and data link equipment that an operator uses to control, communicate with, receive data and information from, and plan missions for one or more

(OCU)		UMSs.
Operator Error	22	An inadvertent action by an operator that could eliminate, disable, or defeat an inhibit, redundant system, containment feature, or other design features that is provided to control a hazard.
Override	22	The forced bypassing of prerequisite checks on the operator commanded execution of a function. Execution of any command (whether designated as a “hazardous command” or not) as an override is considered to be a hazardous operation requiring strict procedural controls and operator safing.
Particular Risk	13	Risk associated with those events or influences that are outside the system(s) and item(s) concerned, but which may violate failure independence claims.
Patch	22	A modification to a computer sub-program that is separately compiled inserted into machine code of a host or parent program. This avoids modifying the source code of the host/parent program. Consequently the parent/host source code no longer corresponds to the combined object code.
Payload	36	See "Mission Module".
Performance Requirement	6	The extent to which a mission or function must be executed, generally measured in terms of quantity, quality, coverage, timeliness or readiness. Performance requirements are initially defined through requirements analyses and trade studies using customer need, objective, and/or requirement statements. Performance requirements are defined for each identified customer (user and supplier) mission and for each primary function (and sub-function). Performance requirements are assigned to lower level system functions through top-down allocation, and are assigned to system elements, CIs and the system through synthesis.
Personnel Barrier	21	A device designed to limit or prevent personnel access to a building or an area during hazardous operations.
Physical Architecture	6	The hierarchical arrangement of product and process solutions, their functional and performance requirements; their internal and external (external to the aggregation itself) functional and physical interfaces and requirements, and the physical constraints that form the basis of design requirements. The physical architecture provides the basis for system/CI baselines as a function of the acquisition phase. It documents one or more physical designs as required to: (1) accomplish effectiveness analysis, risk analysis, and technology transition planning; (2) establish the feasibility of physically realizing the functional architecture; (3) identify manufacturing verification, support and training requirements; (4) document the configuration of prototypes and other test articles, and (5) define in increasing detail the solution to identified needs.
Positive Control	36	Positive control requires the completion of the following functions: (1) a valid command is issued, (2) the command is received, (3) the command is acknowledged, (4) the command is verified, (5) the command authority is authenticated, (6) the command is executed, and (7) notification of command execution is sent and received.
Positive Target ID	36	The condition or state when a target is successfully acquired and identified.
Preliminary System Safety Assessment (PSSA)	12	A systematic evaluation of a proposed system architecture and implementation based on the Functional Hazard Assessment and failure condition classification to determine safety requirements for all items.
Premature Function	16	A fuze function before completion of the arming delay.

Primary Hazard	10	A primary hazard is one that can directly and immediately result in loss, consequence, adverse outcome, damage, fatality, system loss, degradation, loss of function, injury, etc. The primary hazard is also referred to as catastrophe, catastrophic event, critical event, marginal event, and negligible event.
Primary High Explosive	14	An explosive that is extremely sensitive to heat and is normally used to initiate a secondary high explosive.
Process	7	An organized set of activities performed for a given purpose. [MIL-STD-498]
Product	13	Hardware, software, item, or system generated in response to a defined set of requirements.
Product Baseline	6	The initially approved documentation describing all of the necessary functional, performance, and physical requirements of the CI; the functional and physical requirements designated for production acceptance testing; and tests necessary for deployment, support, training, and disposal of the CI. This baseline normally includes product, process, and material specifications, engineering drawings, and other related data. In addition to the documentation, the product baseline of a configuration item may consist of the actual equipment and software. The DoD normally places this baseline under control after completion of the Physical Configuration Audit (PCA). There is a product baseline for each.
Programmatic Safety Precept (PSP)	36	Program Management Principles and Guidance that will help insure safety is adequately addressed throughout the lifecycle process.
Propellant	23	Substance or mixture of substances used for propelling projectiles and missiles, or to generate gases for powering auxiliary devices. When ignited, propellants burn or deflagrate to produce quantities of gas capable of performing work, but in their application are required not to undergo a deflagration-to-detonation transition.
Pyrotechnic Composition	23	Substance or mixture of substances which when ignited, undergo an energetic chemical reaction at a controlled rate intended to produce on demand and in various combinations, specific time delays or quantities of heat, noise, smoke, light, or infrared radiation. Pyrotechnic compositions may be used to initiate burning reactions such as in igniters.
Radiation	14	The transfer of heat in the form of electromagnetic waves between two bodies, substances, or surfaces that are not in contact.
Random Failure	14	Failure whose occurrence is predictable only in a probabilistic or statistical sense. (This applies to all distributions.)
Reaction Time	10	Human response movement time plus response initiation time.
Recovery	3	Actions taken to extricate damaged or disabled equipment for return to friendly control or repair at another location.
Redundancy	12	Multiple independent means incorporated to accomplish a given function.
Redundant System	14	A system composed of two or more components below major item level that are capable of performing the same mission or function independently of each other.
Regression Testing	22	The testing of software to confirm that functions, that were previously performed correctly, continue to perform correctly after a change has been made.
Reliability	13	The probability that an item will perform a required function under specified conditions, without failure, for a specified period of time.
Remote Control	29	A mode of operation of a UMS wherein the human operator, without benefit of video or other sensory feedback, directly controls the actuators of the UMS on a continuous basis, from off the vehicle and via a tethered or radio linked control device using visual line-of-sight cues. In this mode, the UMS takes no initiative and relies on continuous or nearly continuous input from the user.
Remotely Guided	29	An unmanned system requiring continuous input for mission performance is considered remotely guided. The control input may originate from any source outside of the unmanned system itself. This mode includes remote control and teleoperation.

Render Safe	3	The interruption of functions or separation of essential components of unexploded explosive ordnance to prevent an unacceptable detonation.
Requirement	12	An identifiable element of a specification that can be validated and against which an implementation can be verified.
Requirements Specification	10	Specification that sets forth the requirements for a system or system component.
Requirements, Derived	22	(1) Essential, necessary or desired attributes not explicitly documented, but logically implied by the documented requirements. (2) Condition or capability needed, e.g. due to a design or technology constraint, to fulfill the user's requirement(s).
Requirements, Safety	22	Those requirements which cover functionality or capability associated with the prevention or mitigation of a hazard.
Residual Mishap Risk	2	The remaining mishap risk that exists after all mitigation techniques have been implemented or exhausted, in accordance with the system safety design order of precedence.
Residual Risk	10	Residual risk is the risk left over after system safety efforts have been fully employed. It is not necessarily the same as acceptable risk.
Restricted Space	4	That portion of the maximum space to which a robot is restricted by limiting devices. The maximum distance that the robot, end-effector, and work piece can travel after the limiting device is actuated defines the boundaries of the restricted space of the robot.
Retro-Traverse	8	A behavior of a UGV in which, having recorded navigation data on where it has been, it autonomously retraces its route to a point from which it can continue its mission.
Reusable Software Products	7	A software product developed for one use but having other uses, or one developed specifically to be usable on multiple projects or in multiple roles on one project. Examples include, but are not limited to, commercial-off-the-shelf software products, acquirer-furnished software product, software products in reuse libraries, and pre-existing developer software products. Each use may include all or part of the software product and may involve its modification.
Risk	6	A measure of the uncertainty of attaining a goal, objective, or requirement pertaining to technical performance, cost, and schedule. Risk level is categorized by the probability of occurrence and the consequences of occurrence. Risk is assessed for program, product, and process aspects of the system. This includes the adverse consequences of process variability. The sources of risk include technical (e.g., feasibility, operability, producibility, testability, and systems effectiveness); cost (e.g., estimates, goals); schedule (e.g., technology/material availability, technical achievements, milestones); and programmatic (e.g., resources, contractual).
Risk Assessment	10	The process by which the results of risk analysis are used to make decisions.
Risk Management	6	An organized, analytic process to identify what can go wrong, to quantify and assess associated risks, and to implement/control the appropriate approach for preventing or handling each risk identified.
Robot/Robotic	29	An electro-mechanical system that can react to sensory input and carry out predetermined missions. A robot is typically equipped with one or more tools or certain capabilities, including knowledge, so that it can perform desired functions and/or react to different situations that it may encounter.
Robotics	8	The study and techniques involved in designing, building, and using robots.
Root Cause	10	The contributory and initiating events, which started the adverse event flow, are considered root causes. Had these causes been eliminated, the hazardous event would not have occurred. It should be noted that accidents are the result of many contributors, both unsafe acts and /or unsafe conditions. See also "Contributory Hazards" and "Hazard".
Safe	36	General term denoting an acceptable level of risk of, relative freedom from, and low probability of harm. The associated risks that have been identified have been accepted

		provided that all identified controls are implemented and enforced.
Safe Separation Distance	16	The minimum distance between the delivery system (or launcher) and the launched munition beyond which the hazards to the delivery system and its personnel resulting from the functioning of the munition are acceptable.
Safe State	36	A state in which the system poses an acceptable level of risk for the operational mode and environment. For example, "weapons armed" is not a safe state during logistics and pre-deployment modes, but "weapons armed" is a safe state when engaging a target (except to the enemy).
Safeguard	4	A barrier guard, device or safety procedure designed for the protection of personnel.
Safeguarded space	4	The space defined by the perimeter safeguarding devices.
Safety	2	Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.
Safety Analysis	36	A systematic examination to determine system functionality, to identify potential hazards, and analyze the adequacy of measures taken to eliminate, control, or mitigate identified hazards; and analyze and evaluate potential accidents and their associated risks
Safety and Arming Device	16	A device that prevents fuze arming until an acceptable set of conditions has been achieved and subsequently effects arming and allows functioning.
Safety and Arming Mechanism	3	A dual function device which prevents the unintended activation of a main charge or propulsion unit prior to arming, but allows activation thereafter upon receipt of the appropriate stimuli.
Safety Assessment Report (SAR)	14	A formal summary of the safety data collected by the contractor or materiel developer during the design and development of the system. In it the contractor or materiel developer states the hazard potential of the item and recommends procedures or corrective actions to reduce these hazards, and to avoid personnel loss or injury or equipment damage during development testing.
Safety Critical Failure	36	A failure that may cause personal death or injury, equipment damage, or environmental damage.
Safety Critical Function	36	A function whose failure to operate, or incorrect operation, will directly result in a high risk mishap (i.e., death, serious injury, system loss, environmental damage).
Safety Design Measures	36	Any technique, device, or method designed to eliminate or reduce the risk of hazards, unsafe conditions, or unsafe acts (same as hazard control and hazard countermeasure).
Safety Device	3	A device which prevents unintentional functioning.
Safety Factor	14	Ratio of ultimate strength of a material to the allowable stress.
Safety Feature	16	An element or combination of elements that prevents unintentional arming or functioning.
Safety Integrity	20	The ability of a control system to work safely (this includes shutting down safely if a fault occurs), which depends on the entire system, not just the computer.
Safety Kernel	22	An independent computer program that monitors the state of the system to determine when potentially unsafe system states may occur or when transitions to potentially unsafe system states may occur. The Safety Kernel is designed to prevent the system from entering the unsafe state and return it to a known safe state.
Safety Precept	36	A safety precept is a basic truth, law or presumption intended to influence management, operations, and design activities but not dictate specific solutions. A safety precept is worded as a nonspecific and unrestricted safety objective that provides a focus for addressing potential safety issues that present significant mishap risk. Precepts are intentionally general and not prescriptive in nature; they provide a goal which may be achieved via numerous possible options. They provide a focus and objective as opposed to a detailed solution. The need for a safety precept may result from the desire to mitigate certain hazards, hazard types or Top Level Mishaps. Three levels of safety precepts have been established:

		▪ Programmatic Safety Precepts (PSPs) ▪ Operational Safety Precepts (OSPs) ▪ Design Safety Precepts (DSPs)
Safety Rated	4	Tested, evaluated, and proven to operate in a reliable and acceptable manner when applied in a function critical to health and welfare of personnel.
Safety Stop	4	A type of interruption of operation that allows an orderly cessation of motion for safeguarding purposes. This stop retains the program logic for trouble shooting purposes and to facilitate a restart.
Safety-Critical (SC)	2	A term applied to any condition, event, operation, process, or item whose proper recognition, control, performance, or tolerance is essential to safe system operation and support (e.g., safety critical function, safety critical path, or safety critical component).
Safety-Critical Computer Software Component (SCCSC)	22	Those computer software components (processes, modules, functions, values or computer program states) whose errors (inadvertent or unauthorized occurrence, failure to occur when required, occurrence out of sequence, occurrence in combination with other functions, or erroneous value) can result in a potential hazard, or loss of predictability, or control of a system.
Safety-Critical Computing	22	Those computer functions in which an error can result in a potential hazard to the user, friendly forces, materiel, third parties, or the environment.
Safety-Critical Computing System	22	A computing system containing at least one Safety-Critical Function.
Safety-Critical Software	19	Software that falls into one or more of the following categories: (1) Software whose inadvertent response to stimuli, failure to respond when required, response out-of-sequence, or response in combination with other responses, can result in an accident. (2) Software that is intended to mitigate the result of an accident. (3) Software that is intended to recover from the result of an accident.
Safety-Related (SR)	7	A term applied to anything that is safety-critical or safety-significant.
Safety-Significant	7	A term applied to any system, subsystem, component, function, process or item whose failure to operate, or incorrect operation, will contribute to a mishap causing death and/or serious injury, but will not cause it directly. Safety-significant items may also directly lead to the occurrence of marginal or negligible hazards (Category III or IV).
Safing	22	The sequence of events necessary to place systems or portions thereof in predetermined safe conditions.
Safing and Arming Mechanism	3	A mechanism whose primary purpose is to prevent an unintended functioning of the main charge of the ammunition prior to completion of the arming delay and, in turn, allow the explosive train of the ammunition to function after arming.
Semi-Autonomous	29	A mode of operation of a UMS wherein the human operator and/or the UMS plan(s) and conduct(s) a mission and requires various levels of HRI.
Sensor	29	Equipment that detects, measures, and/or records physical phenomena, and indicates objects and activities by means of energy or particles emitted, reflected, or modified by the objects and activities.
Sequence Interlocks	14	An interlock or series of interlocks that insures that it is mechanically or electrically impossible to activate equipment in an improper sequence.
Severity	14	The consequences of a failure mode. Severity considers the worst potential consequence of a failure, which is determined by the degree of injury, property damage, or system damage that could ultimately occur.
Similarity	12	Applicable to systems similar in characteristics and usage to systems used on previously certified aircraft. In principle, there are no parts of the subject system more at risk (due to environment or installation) and that operational stresses are no more severe than on the

		previously certified system.
Single Point Failure	36	The failure of an item that is not compensated for by redundancy or an alternative design measure.
Single Point of Control	4	The ability to operate the robot such that initiation of robot motion from one source of control is only possible from that source and cannot be overridden from another source.
Situational Awareness	29	The perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the future. In generic terms, the three levels of situational awareness are level 1-perception, level 2-comprehension, and level 3-projection. There is both individual and group or team situational awareness.
Software (Or Computer Software)	20	A combination of associated computer instructions and computer data definitions required to enable the computer hardware to perform computational or control functions.
Software Code	10	A software program or routine or set of routines, which were specified, developed and tested for a system configuration.
Software Development File (SDF)	6	A repository for a collection of material pertinent to the development or support of software. Contents typically include (either directly or by reference) design considerations and constraints, design documentation and data, schedule, and status information, test requirements, test cases, test procedures and test results.
Software Development Library (SDL)	6	A controlled collection of software, documentation, and associated tools and procedures used to facilitate the orderly development and subsequent support of software. The SDL includes the Development Configuration as part of its contents. A software development library provides storage of and controlled access to software and documentation in human-readable form, machine-readable form, or both. The library may also contain management data pertinent to the software development project.
Software Engineering Environment (SEE)	6	The set of automated tools, firmware devices, and hardware necessary to perform the software engineering effort. The automated tools may include, but are not limited to, compilers, assemblers; linkers, loaders, operating system, debuggers, simulators, emulators, test tools, documentation tools, and data base management system(s).
Software Error	22	The difference between a computed, observed or measured value or condition, and the true, specified, or theoretically correct value or condition.
Software Fault	20	An undetected error in the software instruction set or logic that renders the software dysfunctional, possibly to the point of suspending processing operations. System safety analysis of software is intended to decrease the number of safety-critical software faults.
Software Hazard	19	A software condition that is a prerequisite to an accident.
Software Partitioning	22	Separation, physically and/or logically, of (safety-critical) functions from other functionality.
Software Reliability	20	Currently there is no industry consensus definition of software reliability. However, for the purposes of system safety analysis of software, it is assumed that software never wears out, while hardware will wear out or fail at some time. Therefore, software is given a uniform, unchanging reliability and software reliability is not a factor in system safety analyses.
Software Requirements Specification (SRS)	22	Documentation of the essential requirements (functions, SRS performance, design constraints, and attributes) of the software and its external interfaces. [IEEE Standard 610.12-1990]
Software Safety	22	The application of the disciplines of system safety engineering techniques throughout the software lifecycle to ensure that the software takes positive measures to enhance system safety and that errors that could reduce system safety have been eliminated or controlled to an acceptable level of risk.
Software Safety Program	19	A systematic approach to reducing software risks.
Software Safety	22	Analysis performed to examine system and software SSRA requirements and the

Requirements Analysis (SSRA)		conceptual design in order to identify unsafe modes for resolution, such as out-of-sequence, wrong event, deadlocking, and failure-to-command modes.
Software Verification	36	The process of evaluating the products of a given software development activity to determine correctness and consistency with respect to the products and standards provided as input to that activity. See also "Verification".
Specification	12	A collection of requirements which, when taken together, constitute the criteria that define the functions and attributes of a system, or an item.
State	36	States identify conditions in which a system or subsystem can exist. A system or subsystem may be in only one state at a time. States are unique and may be binary (i.e., they are either true or not true). A state is a subset of a mode.
Sterilization	16	A design feature which permanently prevents a fuze from functioning.
Subsystem	2	A grouping of items satisfying a logical group of functions within a particular system.
Support Software	20	All software used to aid the development, testing, and support of applications, systems, test, and maintenance software. Support software includes, but is not limited to: ▪ Compilers, assemblers, linkage editors, libraries and loaders required to generate machine code and combine hierarchical components into executable computer programs. ▪ Debugging software. ▪ Stimulation and simulation software. ▪ Data extraction and data reduction software. ▪ Software used for management control, software configuration management, or documentation generation and control during development. ▪ Test software used in software development. ▪ Design aids, such as program design language tools, and problem statement analysis tools. Test and maintenance software is used to assist in fault diagnosis and isolation, operational readiness verification, and system alignment checkout of the system or its components. It may be used to check out and certify equipment and total system at installation, reinstallation, or after maintenance. It is also used in accordance with prescribed procedures to maintain the system throughout its operational life.
System	2	An integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective.
System Architecture	6	The arrangement of elements and subsystems and the allocation of functions to them to meet system requirements.
System Elements	6	The basic constituents (hardware, software, facilities, personnel, data, material, services, or techniques) that comprise a system and satisfy one or more requirements in the lowest levels of the functional architecture.
System Hazard	19	A system condition that is a prerequisite to an accident.
System safety	2	The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.
System Safety Engineering	2	An engineering discipline that employs specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated mishap risk.
System Safety Group/Working Group (SSWG)	1	A formally chartered group of persons, representing organizations initiated during the system acquisition program, organized to assist the MA system program manager in achieving the system safety objectives. Regulations of the military components define requirements, responsibilities, and memberships.
System Safety Management	2	All plans and actions taken to identify, assess, mitigate, and continuously track, control, and document environmental, safety, and health mishap risks encountered in the

		development, test, acquisition, use, and disposal of DoD weapon systems, subsystems, equipment, and facilities.
System Safety Program (SSP)	1	The combined tasks and activities of system safety management and system safety engineering implemented by acquisition project managers.
System Safety Program Plan (SSPP)	1	A description of the planned tasks and activities to be used by the contractor to implement the required system safety program. This description includes organizational responsibilities, resources, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems.
System Software	20	The totality of operational software resident in a computer (operating system, executive programs, application programs and data bases) associated with a system.
Systems Engineering	6	An interdisciplinary approach and means to enable the realization of successful systems. Systems engineering: (1) Encompasses the scientific and engineering efforts related to the development, manufacturing, verification, deployment, operations, support, and disposal of system products and processes; (2) Develops needed user training equipments, procedures, and data; (3) Establishes and maintains configuration management of the system; (4) Develops work breakdown structures and statements of work; and (5) Provides information for management decision making.
Task	29	A named activity performed to achieve or maintain a goal. Mission plans are typically represented with tasks. Task performance may, further, result in subtasking. Tasks may be assigned to operational units via task commands.
Task Decomposition	29	A method for analyzing missions and tasks and decomposing them into hierarchical subtask structures according to the criteria of command/authority chain, control stability, computational efficiency, and management effectiveness.
Task program	4	Set of instructions for motion and auxiliary functions that define the specific intended task of the robot system.
Technical Data Package	6	The engineering drawings, associated lists, process descriptions, and other documents that define system product and process physical geometry; material composition; performance characteristics; and manufacture, assembly, and acceptance test procedures.
Teleoperation	29	A mode of operation of a UMS wherein the human operator, using video feedback and/or other sensory feedback, either directly controls the actuators or assigns incremental goals, waypoints in mobility situations, on a continuous basis, from off the vehicle and via a tethered or radio linked control device. In this mode, the UMS may take limited initiative in reaching the assigned incremental goals.
Telepresence	29	The capability of a UMS to provide the human operator with some amount of sensory feedback similar to that which the operator would receive if he were in the vehicle.
Terrain	29	The physical features of the ground surface, to include the subsurface. These physical features include both natural (e.g., hills) and manmade (e.g., pipelines) features. Major terrain types are delineated based upon local relief, or changes in elevation, and include flat to rolling, hilly and mountainous. Other important characteristics used to describe the terrain include hydrologic features (e.g., swamps), vegetation characteristics (e.g., forests) and cultural features (e.g., cities). Complex terrain includes any characteristic or combination of characteristics that make military action difficult. Mobility classes are also used to describe the trafficability of the terrain. The terrain should also be rated as to its trafficability by class of vehicle; this is especially relevant to the use of different classes of UGVs. The three mobility classes are unrestricted, restricted, and severely restricted.
Test	13	A quantitative procedure to prove performance using stated objective criteria with pass or fail results.
Test Case	22	A set of test inputs, execution conditions, and expected results used to determine whether

		the expected response is produced.
Test Procedure	22	(1) Specified way to perform a test. (2) Detailed instructions for the set-up and execution of a given set of test cases and instructions for the evaluation of results executing the test cases.
Testing	10	The process of operating a system under specified conditions, observing or recording the results, and making an evaluation of some aspect of the system.
Tether	29	A physical communications cable or medium that provides connectivity between an unmanned system and its controlling element that restricts the range of operation to the length of the physical medium.
Threat Avoidance	29	Ability to detect/degrade/defeat threats. The continual process of compiling and examining all available information concerning threats in order to avoid encounter.
Top Level Mishap (TLM)	36	A TLM is a generic mishap category for collecting and correlating related hazards that share the same general type of mishap outcome event. A TLM is a common mishap outcome that can be caused by one or more hazards; its purpose is to serve as a collection point for of all the potential hazards that can result in the same overall TLM outcome, but have different causal factors. TLMs provide a design safety focal point. TLMs help highlight and track major safety concerns. “Top Level” implies an inherent level of safety importance, particularly for visibility at the system level for a risk acceptance authority. The TLM severity will be the same as that of the highest contributing hazard’s severity. Most hazards within the TLM will have the same severity level as the TLM, however, some may have a lesser severity. The TLM is derived by extracting the significant and common generic outcome event portion of the contributing hazard’s mishap description.
Traceability	13	The characteristic by which requirements at one level of a design may be related to requirements at another level.
Training	36	Learning process by which personnel individually or collectively acquire or enhance pre-determined job-relevant knowledge, skills, and abilities.
Unacceptable Risk	10	Unacceptable risk is that risk which cannot be tolerated by the managing activity. It is a subset of identified risk that must be eliminated or controlled.
Unattended System	29	Any manned/unmanned, mobile/stationary, or active/passive system, with or without power that is designed to not be watched, or lacks accompaniment by a guard, escort, or caretaker.
Undetectable Failure	14	A postulated failure mode in the failure mode and effects analysis for which there is no failure detection method by which the operator is made aware of the failure.
Undocumented Code	22	Software code that is used by the system but is not documented in the software design. Usually this pertains to COTS because the documentation is not always available.
Unexploded Ordnance (UXO)	21	Explosive ordnance which has been primed, fuzed, armed, or otherwise prepared for action, and which has been fired, dropped, launched, projected, or placed in such a manner as to constitute a hazard to operations, installations, personnel, or material and remains unexploded either by malfunction, design, or for any other cause.
Unidentified Risk	10	Unidentified risk is the risk not yet identified. Some unidentified risks are subsequently identified when a mishap occurs. Some risk is never known.
Unintended Function	13	A function that is visible at the airplane level and was neither intended nor a predicted fault condition in the PSSA. Only when an unintended function leads to an airplane-level hazard ,or a degradation of an intended function, is it considered significant relative to certification.
Unmanned Aerial Vehicle	3	A powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or non-lethal payload. Ballistic or semi-ballistic vehicles, cruise missiles, and artillery projectiles are not considered unmanned aerial vehicles.
Unmanned Ground Vehicle (UGV)	8	A powered, mobile, ground conveyance that does not have a human aboard; it can be operated in one or more modes of control (autonomous, semiautonomous, teleoperation, remote control); it can be expendable or recoverable; and it can have lethal or non-lethal

		mission modules.
Unmanned System (UMS)	36	An electro-mechanical system that is able to exert its power to perform designed missions, and includes the following three common characteristics: (1) there is no human operator aboard, (2) manned systems that can be fully or partially operated in an autonomous mode, and (3) the system is designed to return or be recoverable. The system may be mobile or stationary, and includes the vehicle/device and the control station. Missiles, rockets and their submunitions, and artillery are not considered unmanned systems. UMSs include, but are not limited to unmanned ground vehicles, unmanned aerial/aircraft systems, unmanned underwater vehicles, unmanned surface vessels, and unattended systems.
Valid	36	Founded on truth or fact; capable of being justified or defended (dictionary).
Valid Command	36	A command that meets the following criteria: (1) Originates from an authorized entity. (2) The received command is identical to the sent command. (3) The command is a valid executable.
Valid Message	36	A message that meets the following criteria: (1) Originates from an authorized entity. (2) The received message is identical to the sent message.
Validation	12	The determination that the requirements for a product are sufficiently correct and complete.
Verification	12	The evaluation of an implementation to determine that applicable requirements are met.
Waypoint	29	An intermediate location through which a UMS must pass, within a given tolerance, en route to a given goal location.
Waypoint Navigation	36	The process whereby a UMS makes its way along a route of planned waypoints that it planned or that were planned for it.

Appendix D. Major Contributors

Dr. Julie Adams (Academia)	Mr. Bart Fay (Industry)	Mr. Alan Owens (USAF)
Ms. Alicia Adams-Craig (Army)	Mr. John Filo (Navy)	Mr. Preston Parker (USAF)
Mr. Frank Albert (Navy)	Mr. Tom Garrett (Navy)	Mr. Mike Pessoney (Industry)
Mr. Billy Arnold (Industry)	Mr. Jim Gerber (Navy)	Mr. Lynece Pfledderer (Industry)
Mr. Scottie Allred (USMC)	Mr. Eugene Gonzales (Navy)	Mr. Helmut Portmann (Navy)
Ms. Rhonda Barnes (Industry)	Mr. Mark Handrop (USAF)	Mr. Bill Pottratz (Army)
Mr. Bill Blake (Industry)	Mr. Travis Hogan (Industry)	Mr. Ron Price (Army)
Dr. Craig Bredin (Industry)	Mr. Steve Hosner (Industry)	Mr. Scott Rideout (USMC)
Mr. Mike Brown (Industry)	Mr. Huimin Huang (NIST)	Ms. Peggy Rogers (Navy)
Mr. Danny Brunson (Industry)	Mr. Bob Jacob (Navy)	Mr. Craig Schilder (Industry)
Mr. Jim Butler (Industry)	Mr. Chris Janow (Army)	Mr. Bob Schmedake (Industry)
Mr. John Canning (Navy)	LTCOL Emil Kabban (USAF)	Mr. Dave Schulte (Navy)
Ms. Mary Ellen Caro (Navy)	Mr. Ed Kratovil (Navy)	Mr. Owen Seely (Navy)
Mr. Steve Castelin (Navy)	Mr. Mike Logan (NASA)	Mr. Ed Spratt (Navy)
Mr. Bill Christian (Industry)	Mr. Dave Magidson (Army)	Mr. Hoi Tong (Industry)
Mr. Brad Cobb (Navy)	Mr. Ranjit Mann (Industry)	Mr. Bill Transue (Navy)
Mr. John Deep (USAF)	Mr. Jack Marett (Industry)	Mr. Arthur Tucker (Industry)
Mr. Mike Demmick (Navy)	Mr. Frank Marotta (Army)	Dr. Anthony Tvaryanas (USAF)
Mr. Jon Derickson (Industry)	Mr. Steve Mattern (Industry)	Mr. Jack Waller (Navy)
Mr. Michael Dunn (Army)	Mr. Bob McAllister (USAF)	Mr. Alan Weeks (Industry)
Mr. Bill Edmonds (Army)	Mr. Josh McNeil (Army)	Mr. Frank Zalegowski (Navy)
Mr. Woody Eischens (OSD)	Ms. Martha Meek (Army)	Mr. Henry Zarzycki (Army)
Ms. Melissa Emery (Industry)	Mr. Aaron Mosher (Industry)	Mr. Mike Zecca (Army)
Dr. Tom English (Navy)	Mr. Charles Muniak (Industry)	Mr. Mike Zemore (Navy)
Mr. Clif Ericson (Industry)	Ms. Kristen Norris (Industry)	Mr. Jim Zidzik (Navy)
Ms. Rachael Fabyanic (Navy)	Mr. Chris Olson (Industry)	Mr. Don Zrebieck (Navy)

Appendix E. Safety Precept Clarification Tables

TABLE FORMAT

Precept Number Statement of the precept in the form of a requirement or general guidance.
Scope: Answers the question of "What?" the precept is for; often can be answered by "This precept addresses…."
Rationale: Answers the question of "Why?" the precept is required. This provides addition clarification of the intent of the precept.
Examples: Provide as many clarifying explicit/real-world examples to demonstrate the issues and specific hazards the precept addresses.
Detailed Considerations: Answers the question of "How?" by providing details to assist with implementation of the precept. These are specific statements written in the form of a requirement or guideline which capture lessons learned and experience from other programs. Some of these considerations can be tailored for specific programs and incorporated into system specifications as safety requirements.
Existing Policy: Provides applicable policy documents (including associated section). service. and comments as to the level of reference. The term "references" will be used when the text specifically states the safety precept; the term "partially references" when the text addresses some, but not all, of the elements of the precept, or the scope of the document is limiting; and the term "implies" when the text does not reference the precept specifically, but the precept could be considered to be covered by the more general wording.

While this document serves only as a guide, usage of the terms "shall" and "should" reflects the level of concern of the safety community.

* Denotes percepts that apply to both manned and UMSs.

PROGRAMMATIC SAFETY PRECEPTS

PSP-1* The Program Office shall establish and maintain a System Safety Program (SSP) consistent with MIL-STD-882.

Scope: The intent of this precept is for all programs to establish and maintain a System Safety Program compliant with the requirements and guidance in MIL-STD-882 or an equivalent standard.

Rationale: This precept is in keeping with the DoD 5000 series that requires system safety be integrated into systems engineering for every program, regardless of Acquisition Category (ACAT) level. The DoD-wide accepted standard for system safety program requirements is MIL-STD-882.

Examples: None

Detailed Considerations:

- MIL-STD-882 must be tailored for each program as appropriate.
- Ensure the human system interface is designed appropriately and that all the necessary Information, Intelligence, and Method of Control (I2C) data requirements are considered in the UMS design. Human System Integration analysis and an I2C analysis should be integrated with the SSP.
- Software safety processes and guidelines should be an integral part of the SSPP and Software Development Plan (SDP) and should include items such as:
  - Safety critical software requirements and data must be identified. Traceability of safety critical software and data must be provided to include their identification in the SRS and the software code files.
  - Safety critical software requirements and data must be configuration controlled to ensure the integrity of those requirements and data throughout the UMS lifecycle.
  - The level of software test assessment should be commensurate with its safety criticality levels to demonstrate that design level objectives have been satisfied. For example, testing of safety critical software should include enough test cases to ensure error handling does not induce unintended functionality. Safety critical testing is intended to try and “break” the software and induce the fault. This is done by such things as fault insertion, data range and out-of-bounds tests, and simulations.
- There are many excellent industry safety references that can be used in developing an effective system safety program, such as: SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, SAE ARP 4754, Certification Considerations for Highly-Integrated or Complex Aircraft Systems; and DoDI 6055.1 DoD Safety and Occupational Health Program which encompasses risk management, aviation safety, ground safety, traffic safety, occupational safety, and occupational health.

Existing Policy:

Service	Document	Section	Comment
DoD	DoD 5000.2	Section E7.1.6	Text implies precept.
DoD	USD (AT&L) Wynne Memo	Section b	Text references precept.
Air Force	AFI 63-101	Section 5.2.2.7.2	Text references precept.
Air Force	AFPD 91-2	Section 9.6.1	Text implies precept.
Army	AR 385-16	Section 5.e	Text references precept.
Army	AR 70-1	Section 2-3.3.p	Text implies precept.
Marine Corps	MCO 5100.29A	Section 4.a.1.b	Text implies precept.
Navy	SECNAVINST 5000.2C	Section 2.4.6.1 (para 4)	Text references precept.

PSP-2* The Program Office shall establish unifying safety precepts and processes for all programs under their cognizance to ensure:

- Safety consistent with mission requirements, cost and schedule.
- Mishap risk is identified, assessed, mitigated, and accepted.
- Each system can be safely used in a combined and joint environment.
- That all safety regulations, laws, and requirements are met.

Scope: This precept requires the program to establish a common approach to UMS safety in a systems-of-systems environment. The Office of the Secretary of Defense (OSD) UMS precepts, contained herein, provide the foundation for a common approach for this unification. ***All*** UMS programs must demonstrate traceability to these precepts, and assess the potential mishap risk of any non-compliance. Compliance to or deviation from these precepts is addressed in PSP-5 which requires the program office to review each of the UMS precepts in this document for applicability to their program and incorporate requirements derived from the precepts into program documentation (i.e. contract statement of work, program plans, requirement specifications, etc.). This precept implements the requirement to establish UMS safety precepts while PSP-5 provides for tailoring of UMS safety precepts presented in this guide. The precepts, presented in this guide, are provided as a generic and minimum set of precepts for consideration for any UMS safety program. While deviation from these precepts must be justified, it is fully anticipated new precepts could be established for individual safety programs in addition to, or in replacement of, these precepts.

Rationale: These precepts are intended to influence UMS program management, design, and operation, thereby mitigating potential mishap risk.

Examples:

1. The Joint Architecture for Unmanned Systems (JAUS) is an attempt to establish a standardized architecture that is applicable to UMSs.

Detailed Considerations:

- Safety criteria should be identified early to ensure they are flowed into performance requirements and design solutions.
- Service Safety Centers typically maintain accident data that should be examined early in the system life cycle in an attempt to incorporate UMS lessons-learned.
- Consider developing joint lessons-learned databases and common processes that can be shared among the UMS community.
- Consider common human system interfaces for UMSs.
- The operational usage of UASs in the United States should ensure that the FAA Air Route Traffic Control Center (ARTCC) and/or Terminal Radar Approach Control (TRACON) be notified of planned usage of the UAS. These processes are in place

IAW FAA JO 7610.4.

Existing Policy:

Service	Document	Section	Comment
Army	AR 70-1	Section 2-1.o	Text implies precept.
Navy	NAVSEAINST 8020.6E (Draft)	Section E13	Text partially references precept.

PSP-3* The Program Office shall ensure that off-the-shelf items (e.g., COTS, GOTS, NDI), re-use items, original use items, design changes, technology refresh, and technology upgrades (hardware and software) are assessed for safety, within the system.

Scope: This precept applies to every component of a system; all components must be assessed for safety WITHIN the context of the overall system. The level of assessment should be commensurate with its safety criticality.

Rationale: Significant accidents have occurred related to the re-use of components within a different system. A safety review of off-the-shelf items must provide insight to the hazards and control of these items.

Examples:

1. Ariane V Rocket – The 4 June 1996 maiden flight ended in complete destruction 40 seconds into flight. High aerodynamic loads, due to a high angle of attack, caused the booster to separate from main stage, triggering self-destruct. A high angle of attack was caused by full nozzle deflections commanded by the On-Board Computer (OBC). The OBC received a diagnostic bit pattern from the inertial reference system due to a software exception. The software exception was generated by overflow from a 64 bit floating point that was converted to a 16 bit signed integer. The Module responsible for the fault was not used during flight, but was intended for use only for alignment of strap-down of the inertial system on the launch pad; it was reused from Ariane IV.
2. A research fly-by-wire aircraft experienced a failure on the flight-line during a group test, the day before the flight. That failure caused the flight control computer to crash resulting in an erroneous response from the flight computer (fortunately the failure occurred while on the flight-line rather than during flight). A memory conflict occurred causing safety critical data to be overwritten by non-safety critical code.

Detailed Considerations:

- Ensure that full integration end-to-end testing is performed on systems containing legacy and/or re-use items.
- Any off-the-shelf items (e.g., COTS, GOTS, NDI), re-use items, original use items, design changes, technology refresh and technology upgrades (software) must be thoroughly assessed and tested for safety within the system into which it is being inserted.
- Correct implementation of software exception handlers is safety critical.
- Safety concerns from the software system safety analysis must be addressed in Software Test Plans and Procedures (Boundary value testing, Full integration end-to-end testing)
- Components, including legacy systems and subsystems, that have been proven safe in an earlier application, cannot be assumed safe in another application. Special attention should be paid to the interfaces.

Existing Policy:

Service	Document	Section	Comment
DoD	MIL-STD-882D	Section 4	Text partially references precept.
Air Force	AFI 91-205	Section 2.1.5	Text partially references precept.
Army	AR 385-16	Section 5.B	Text implies precept.
Navy	NAVSEAINST 8020.6E (DRAFT)	Section 6.a.1	Text partially references precept.

PSP-4* The Program Office shall ensure that safety is addressed for all life cycle phases.

Scope: System safety must be an integral part of the Defense Acquisition life cycle management process that begins with concept refinement and ends with disposal. This precept is related to PSP-1; if PSP-1 is done correctly, this precept will be accomplished.

Rationale: DoDD 5000.1 directs that safety be addressed throughout the acquisition process. Early involvement ensures safety is designed into the system as opposed to late involvement and potential redesign to meet safety requirements, or acceptance of unnecessary risk. The majority of safety issues are the direct result of safety requirements not being identified due to lack of early involvement.

Examples:

1. Many current UMSs have been developed as prototypes and, due to their value to the warfighter, their fielding to theatre is accelerated without the benefit of an effective safety program. This is also evident during the recovery and disposal of these UMSs.

Detailed Considerations:

- With the life of defense systems being extended through block upgrades, technology refresh programs, etc., system designs must consider post-deployment support that will ensure the safety of the system.
- Program managers must commit resources to the safety efforts beyond Milestone C to ensure the appropriate level of safety support is maintained.
- Safety issues which arise beyond Milestone C, generally result in the use of Tactics, Techniques, and Procedures (TTP) to mitigate mishap risk. TTP frequently limits the system's operational utility and effectiveness and should only be considered as the last resort.

Existing Policy:

Service	Document	Section	Comment
DoD	DoD 5000.1	Section E1.1.23	Text references precept.
DoD	MIL-STD-882D	Section 4	Text references precept.
Navy	SECNAVINST 5000.2C	Section 7.f	Text implies precept.
Army	AR 70-1	Section 1-4.15.e	Text implies precept.
Army	AR 385-16	Section 6.d	Text references precept.

PSP-5 Compliance to and deviation from the safety precepts shall be addressed during all Milestone decisions and formal reviews such as SRR, PDR, and CDR.

Scope: This precept, along with PSP-2, requires the program office to review each of the UMS precepts in this document for applicability to their program; incorporate requirements derived from the precepts into program documentation (i.e. contract statement of work, program plans, requirement specifications, etc.); and show compliance to or deviation from the precept. Compliance to or deviation from these precepts as documented within this OSD UMS Safety Guidance document should be addressed and approved at the first program major review. Should the program office choose to tailor the OSD issued UMS safety precept guidance, then that tailored set becomes the baseline upon which the subsequent major reviews address continued compliance.

Rationale: These precepts were developed in a joint government, industry, and academia forum by subject-matter experts. They represent best safety practices and are intended to influence design activities but not dictate specific design solutions.

Examples: None

Detailed Considerations:

- The Program Office should document compliance to or deviation from each precept, including the associated rationale, as part of the design review technical data package. This information is also critical for continuous improvement to these precepts and expansion of UMS lessons learned.

ExistingPolicy:

Service	Document	Section	Comment
DoD	DAPS	Section Sub-Area 4.2 (2nd Para)	Text implies precept.
DoD	DAG	Section 4.2.3.4	Text implies precept.

PSP-6* The Program Office shall ensure UMS designs comply with current safety and performance standards and criteria.

Scope: The intent of this precept is to ensure the Program Office considers appropriate existing Military Standards in the design of the UMSs, consistent with its intended life cycle use. This precept is related to PSP-3.

Rationale: While today's systems' designs are performance driven, design standards specific to potentially hazardous systems such as munitions/weapons/suspension and release equipment, aviation systems, and laser systems are mandatory. Compliance with these standards is reviewed for adequacy by Service Safety Organizations and the Joint Weapon Safety Technical Advisory Panel (JWSTAP) during the Joint Capabilities and Integration Decision System (JCIDS) process for Joint Service programs.

Examples:

1. Acquisition efforts for reuse or redesign must consider these safety standards. For instance, a gun mount mechanical safety can be easily verified in a manned system by the operator, but moving it to an UMS platform takes the operator out of the loop resulting in the loss of a safety feature.
2. Using a legacy system in a new UMS application can create new interface issues that may not have been considered in its previous application. In such a case, safety redundancy may not have been ported.

Detailed Considerations:

- Additional references include but are not limited to: MIL-HDBK-516 including DO-178, MIL-STD-2105, MIL-STD-2088, MIL-STD-1316, MIL-STD-1901, STANAG 4187, STANAG 4586, MIL-STD-1472, MIL-STD-1908, MIL-STD-4297

Existing Policy:

Service	Document	Section	Comment
DoD	DoD 5000.2	Section 3.9.2.2	Text implies precept.
Air Force	AFI 91-205	Section 2.1.1 and 2.1.2	Text implies precept.
Army	Guidance for AFSRB Safety Certification	Section 7.5.b	Text partially references precept.
Navy	NAVSEAINST 8020.6E (Draft)	Section 8.b.1	Text implies precept.

OPERATIONAL SAFETY PRECEPTS

OSP-1 The controlling entity(ies) of the UMS should have adequate mission information to support safe operations.

Scope: The intent of this precept is to ensure safe operation of the UMS, given adequate mission information is provided. Adequate mission information includes, but is not limited to, specific data requirements for all operational phases influenced by mission, mission objectives, CONOPS, Rules Of Engagement (ROE), TTPs, available intelligence, environmental and metrological conditions, and UMS status and health. Fundamental to this precept is the clear identification of the controlling entity(ies) applicable to all phases of operation. In the case of multiple controlling entities, an order of precedence and authorization is required. This OSP is related to DSP-3.

Rationale: The availability of adequate mission information is critical for safe UMS operation. This precept is dependent upon a thorough job of defining and displaying adequate mission information, and thorough TTPs.

Examples:

1. Early UMS user involvement ensures the identification of adequate mission information and the incorporation of this information into system requirements specification.
2. Involvement of the user in prototype developmental testing.

Detailed Considerations:

- Identify what information is needed for a given operation, and develop contingency plans if needed information becomes unavailable.
- Provide user feedback as soon as possible in the development process.
- Ensure CONOPS incorporate unique UMS requirements.

Existing Policy:

Service	Document	Section	Comment
Air Force	AFPD 10-4	Section 1.5.2	Text implies precept.
Army	FMI 3-04.154	Section 1-37	Text partially references precept.
Army	FMI 3-04.155	Section 4-136	Text partially references precept.
Marine Corps	MCWP 3-42.1	Section 3-8 (para 4)	Text partially references precept.
Navy	OPNAVINST 3710.7T	Section 4.3.1	Text implies precept.

OSP-2 The UMS shall be considered unsafe until a safe state can be verified.

Scope: The intent of this OSP is to ensure that any personnel approaching a UMS can positively determine if the UMS is in a physically safe state, ref. DSP-17. Positive determination of state must be identified by any controlling entity(ies) to include humans in physical contact with a UMS. Determination of state includes, but is not limited to, weapons, hazardous system appendages, items retrieved by the UMS during operations, and the system following exposures to hazardous environments such as Chemical, Biological, and Radiological (CBR).

Rationale: Identifiable safe transitioning between operational states must be addressed through appropriate tactics, techniques, and Standard Operating Procedures (SOPs), controlling entity(ies) training, and user guidelines to ensure safe human and UMS interface during any operational mode. Identifiable state requirements also encompass UMSs that have been out of sight, or communication from the controlling entity(ies).

Examples:

1. When operating out of direct line of sight of the operator, the UMS onboard sensors cannot provide the necessary information for the receiving operator to determine potentially hazardous situations.
2. During operations, a UMS may have been exposed to hazardous chemicals or radiation creating a hazard to human exposure.
3. A UMS may have "picked up" an Unexploded Ordinance (UXO) that could present a hazard to human contact.
4. Weapons armed when the UMS is in logistics or pre-deployment mode is not a safe state, whereas weapons armed in tactical operational mode is a safe state.
5. A UMS, used to retrieve hazardous materials or items such as UXO, could present a hazard to human contact.

Detailed Considerations:

- CONOPS must identify UMS physical exclusion zones and surface danger zones for all friendly personnel that could potentially encounter the UMS.
- CONOPS should address the training of all personnel that could potentially encounter the UMS.
- Safe state is a state in which the system poses an acceptable level of risk for the operational mode.
- CONOPS should incorporate the safe transitioning between modes and states for the UMS.
- When a UMS fails after employment, operational procedures should be developed to ensure safe recovery of the UMS, ancillary equipment, and unexpended weapons stores.

Existing Policy: None

OSP-3 The authorized entity(ies) of the UMS shall verify the state of the UMS, to ensure a safe state prior to performing any operations or tasks.

Scope: The intent of this OSP is to ensure that during operations, the operator is aware of the state of the UMS prior to changing to another state. This OSP implies the operator has the requisite competencies to ensure the state of the UMS prior to performing operations. Appropriate tactics, techniques, and SOPs, and training and user guidelines address the relationship of the state of the UMS or its weapons, hazardous system appendages, and items retrieved by the UMS during operations and human interface with the UMS. Reference DSP-7.

Rationale: While identifiable safe transitioning between operational states must be addressed through design to ensure safe human and UMS interface during any operational mode, the same state requirements must be enforced through TTPs. These TTPs should also enforce the identifiable state requirements for UMSs that have been out of sight or communication from the controlling entity(ies).

Examples: None

Detailed Considerations:

- TTP development should begin as early in the system design process as possible. Following TTP development, but during system design, an Operational and Support Hazard Analysis (O&SHA) should be conducted, highlighting among other things, traceability from TTPs to design features. Traceability of O&SHA identified hazards to system design features will identify any design shortfalls that may be corrected to mitigate operational and support hazards, or tailored TTPs necessary to mitigate operational and support hazards.
- Independent verification of the UMS mode and state may be considered, where possible.

Existing Policy:

Service	Document	Section	Comment
Army	FMI 3-04.155	Section 4-136	Text implies precept.

OSP-4* The UMS weapons should be loaded and/or energized as late as possible in the operational sequence.
Scope: This OSP addresses weapons, lasers, and other hazardous devices such as emitters.
Rationale: This OSP limits the exposure of personnel to a potentially high risk condition and is in keeping with the standard procedure for manned systems.
Examples: None
Detailed Considerations: • Utilize existing procedures for manned systems that define weapons loading and arming areas, free-fire areas, etc. • Reference design standards that address portions of this precept: DoD MIL-STD-1316 Section 4.2a; DoD MIL-STD-1901A Section 4.3d; and NATO STANAG 4187 Section 7.c.3.
Existing Policy: None

OSP-5* Only authorized, qualified and trained personnel with the commensurate skills and expertise, using authorized procedures, shall operate or maintain the UMS.

Scope: This OSP addresses requisite operator competencies in operating and maintaining UMSs. This OSP relates to DSP-7.

Rationale: Appropriate skills and expertise is consistent with DoD policy and reduces the potential for mishaps caused by human error. Appropriate authorizations prevent unnecessary exposure of unqualified personnel.

Examples: None

Detailed Considerations:

- Particular attention should be given to level of authorizations for operations, and the training of those authorized personnel, to preclude inappropriate use of the UMS.
- The operational manuals, training manuals, and training sessions should include safe modes and states, mode requirements, and tactical versus training operations and/or separations.

Existing Policy:

Service	Document	Section	Comment
Air Force	AFI 63-1201	Section 1.5	Text partially references precept.
Marine Corps	MCWP 3-42.1	Section 1-2 (2nd bullet)	Text partially references precept.
Navy	OPNAVINST 3710.7T	Section 4.1.3	Text partially references precept.
Navy	OPNAVINST 3750.6R	Section 205.j	Text partially references precept.

DESIGN SAFETY PRECEPTS

DSP-1* The UMS shall be designed to minimize the mishap risk during all life cycles phases.

Scope: The intent of this Design Safety Precept (DSP) is to ensure the safety order of precedence, as prescribed in MIL-STD-882, is applied. The preferred solution is always the elimination of mishap risk through design.

Rationale: Mishap risk mitigation is an iterative process that culminates when the residual mishap risk has been reduced to a level acceptable to the appropriate authority. The system safety design order of precedence for mitigating hazards is to eliminate hazards through design selection, incorporate safety devices, provide warning devices, and develop procedures and training.

Examples: None

Detailed Considerations:

- The UMS should be designed to safely operate across environments, as defined in its CONOPS.
- The UMS design should provide adequate personnel protection against hazardous conditions such as:
  1. Unintended Weapons Firing and Blast Effects.
  2. Radiation of Transmitters and Emitters.
  3. Hazardous or Toxic Materials.
  4. Rotating Equipment.
  5. Excessive (High) Voltages.
  6. Excessive Noise Levels.
  7. Explosive Environments and Ordnance.
  8. Excessive RF Energies.
  9. X-Rays or Laser Radiations.
  10. Sharp Corners and Edges on Equipment.
  11. Hydraulic and Pneumatic Pressures.
- The UMS design should consider design requirements from existing Military Standards and Industry best practices such as:
  - MIL-STD-461E, MIL-STD-464, STANAG 4586, etc.
  - “Lessons learned”.
  - Fail-safe mechanisms such as redundancy or safety interlocks.

Existing Policy:

Service	Document	Section	Comment
DoD	USD (AT&L) Wynne Memo	Section b	Text implies precept.
DoD	MIL-STD-882D	Section 4	Text references precept.
Air Force	AFPD 91-2	Section 9.3	Text implies precept.
Army	AR 385-16	Section 6.c	Text references precept.
Marine Corps	MCO 5100.29A	Section 4.k.2.g	Text partially references precept.

DSP-2 The UMS shall be designed to only respond to fulfill valid commands from the authorized entity(ies).

Scope: The UMS should be designed to fulfill or execute commands through a process that, at a minimum, contains these three steps: accept commands only from authorized entities; determine whether the command is valid; and perform only valid commands.

Rationale: The precept is foundational for ensuring only authorized entity(ies), using valid commands, will command the system. All other precepts will assume this is already a design feature. Note that usage and placement of the word "only" in the precept is important. This precept addresses the hostile, inadvertent, or unauthorized control of the system asset and its weapon systems (see also authorized user guidance), and unauthorized or invalid (garbled signals, cross-talk, inappropriate for current mode or state) commands which may lead to unintended or inadvertent motion or weapon action resulting in injury, death, system damage, or environmental damage.

Examples:

1. Inadvertent control of another UMS. While conducting UMS test operations with two ground control stations and two UGVs, the ground controller for UGV1 was able to log in and control UGV2 without the ground controller for UGV2 passing control to the other ground controller. Ineffective validation of the authorized entity caused this hazard.
2. Fulfillment of invalid command. Arming of a weapon system when it is the maintenance mode; this should not be a valid command for a maintenance mode. A safety lock should have been defined for prevention of arming while in maintenance mode.
3. Performs commands in a timely manner. Flying a UAV in teleoperational mode, the operator commands a hard-right turn, UAV does not respond in a timely manner resulting in a collision.
4. Performs valid commands even if ill-advised. Controlling entity commands UMS to navigate off a cliff; UMS complies if defined as a valid command.

Detailed Considerations:

- Valid commands/input are commands that the system is capable of performing in the current mode (a system can not do any more than it is designed to do).
- The system should be designed to preclude the likelihood of hostile control of the system asset and its weapon systems. See also "authorized user guidance".
- The system should be designed to preclude the unintended control of the system and its weapon systems by unauthorized (friendly) personnel or multiple sources of authorized personnel at the same time.
- The system should be designed to provide identification and cross check verification between the platform and the command and control systems. Provisions should be made to address conflicting simultaneous control commands. It may be necessary to specify a hierarchy of control.
- The system should be designed to challenge commands that exceed system capabilities, command set parameters, or violate safety protocol.
- The UMS should be designed to minimize tampering with or the unauthorized physical reconfiguration of the UMS.
- Reference NATO STANAG 4404 Section 7.9.

Existing Policy: None

DSP-3 The UMS shall be designed to provide information, intelligence, and method of control (I2C) to support safe operations.

Scope: This precept addresses operational situational awareness and control feedback of the system to make decisions for all modes of operation and levels of autonomy. This DSP supports OSP-1.

Rationale: The intent of this precept is to address critical safety elements of situational awareness required for safe operation to:

- Ensure the operation remains within safe performance limits.
- Provide alerts related to performance anomalies which could lead to hazards.
- Use monitoring to ensure non-propagation of hazards throughout the vehicle.
- Update guidance to avoid potential hazard scenarios in changing situations.

Examples:

1. While conducting UMS test operations with two ground control stations and two UGVs, the ground controller for UGV1 was unaware it was viewing video feed from UGV2. UGV1 was fulfilling commands from an authorized entity (ground control station 1) based on incorrect data. Ineffective validation of the authorized entity as well as lack of display notifications caused this safety issue.
2. A UAV operator was remote-controlling the UAV using a handheld controller with two joysticks. The operator had turned the UAV around and was preparing to land the UAV as it was headed toward the operator. The UAV crashed into a nearby pond. The accident occurred because the control inputs, to maneuver the UAV left and right, were opposite what they were when the UAV was moving away from the operator. The operator was not provided with an optimal method of control to safely maneuver the UAV.
3. A UAV had just successfully landed on a runway. Unknown to the operator, a taxi speed of 130 knots was input in the mission plan at a designated waypoint. The UAV accelerated to the waypoint and was unable to make the turn and therefore, ran off the runway causing extensive damage to the UAV. The error resulted from the automated generation of mission plans and the operator's inability to interpret mission plans as they were encoded in hexadecimal and provided no overview or trend data to the operator.

Detailed Considerations:

- Communication reliability, network availability/quality of service and data/information assurance shall be commensurate with the safety criticality of the functions supported by the communication.
- Delivery of the information to the controlling entity(ies) includes, but is not limited to, selection of data to be collected, the means of conveyance, ordering of importance, and reliability and timeliness of data.
- The human machine interface should be designed using a defined set of symbols and terms common to platforms and

operational services.

- The level of onboard information processing capability should be adequate and commensurate with the intended method of control.
- Both human and UMS intelligence and information processing capabilities and constraints are appropriate and compatible for the operation being performed.
- UMS workload should not exceed human or UMS intelligence and information processing capabilities. As the number of controlled items increases for the operator, operator actions should be prioritized and minimized to ensure critical tasks are performed first.
- UMSs should be designed to optimize the proficiency of the controlling entity in all operations, training configurations, and environments.
- The system should be designed to detect degraded performance of the controlling entity(ies) and provide notifications.
- The system should be designed to provide positive identification of the asset, and its existing configuration, modes, and states to command and control authorities. This should include confirming pre-set or entity entered mission parameters, settings, and operator actions.
- The UMS should provide actual system status, in addition to the commanded status, to the controlling entity(ies).
- The UMS should provide control and informational feedback necessary to support safe movement and navigation of the system. UMSs require safe movement assurance in order to discriminate between potential obstacles and humans (e.g., wounded soldier fallen in vicinity of UMSs).
- The human machine interface should be designed to minimize the use of complex operational procedures to ensure safe operations. Operational procedures should not be used to replace safe design practices.
- System design should consider separation of weapon systems and sensor locations to preclude interference that could result in degradation of situational awareness. For example, the design should ensure no auditory or visual degradation as the result of weapons fire.
- Reference STANAG 4586 Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability for additional guidance.

Existing Policy: None. This precept is unique to UMSs, as such previous policy has not addressed this critical aspect of UMS design.

DSP-4* The UMS shall be designed to isolate power until as late in the operational sequence as practical from items such as: a) Weapons, b) Rocket motor initiation circuits, c) Bomb release racks, or, d) Propulsion systems.

Scope: This precept applies to systems and subsystems utilizing energetic materials, explosives, propellant, directed energy equipment, harmful Radio Frequency (RF) radiation, lasers, etc., and the preparations for the release of energy.

Rationale: The intent of this precept is to preclude the inadvertent release of hazardous energy.

Examples:

1. Isolating power to firing and/or releasing a missile from a UAV prevents the unintentional ignition of the rocket motor from an electrical short until as late as possible in the operation.
2. For a defensive system, inadvertent release of energy could occur if a false radar image was detected and the power source has not been isolated.

Detailed Considerations:

- The UMS should be designed to provide positive safety design measures to isolate power from weapons or ordnance initiation circuits until intent to initiate.
- Reference design standards that address portions of this precept: MIL-STD-1901A (a & b) Section 4.3a & d; MIL-STD-1316 (a) Section 4.2a; and NATO STANAG 4187 (a) Section 7.c.3.

Existing Policy: None.

DSP-5* The UMS shall be designed to prevent release and/or firing of weapons into the UMS structure or other weapons.
Scope: This precept addresses potential damage by firing a weapon into the UMS structure or firing a weapon into a second weapon being fired. It is not intended to address one UMS firing into another UMS.
Rationale: The intent of this precept is to prevent damage by the UMS to itself from an on-board weapon.
Examples: 1. The UMS used the incorrect No-point/No-fire area and fired a weapon into the UMS platform. 2. A self-defense UMS weapon opened fire, immediately after launch of an offensive system, and results in a weapon-to-weapon collision. Timing and definition of the target cut-out-area must consider the dynamics of the operational environment.
Detailed Considerations: • The design should identify and define the specific No-point/No-fire requirements for the weapons systems. • Design of hard and/or soft stops should preclude entering the designated target cut-out area (No-point/No-fire areas). • System design should consider separation of weapon systems and sensor locations to preclude interference that could result in degradation of weapon targeting. • The design should consider dynamic No-point/No-fire zones created by the weapon timing sequences. • Reference: NATO STANAG 4404 Section 13.2.
Existing Policy: None

DSP-6* The UMS shall be designed to prevent uncommanded fire and/or release of weapons or propagation and/or radiation of hazardous energy.

Scope: This precept applies to both offensive and self defense weapons and is intended to address failure modes common to all weapon systems.

Rationale: Standard design practice for any weapon system is to minimize the probability of uncommanded weapon activation. Existing STANAGs and MIL-STD's address design and analysis processes for this hazard. This precept is related to DSP-15.

Examples:

1. Smoke grenades on UGVs require the authorized entity(ies) to take multiple actions to fire the weapon so inadvertent contact with the fire command or an inadvertent action by the authorized entity(ies) does not fire the weapon.

Detailed Considerations:

- A UMS should mitigate through design the uncommanded or unintended arm/fire/release of weapons or radiation of hazardous emitters.
- The on-board weapons systems for UMSs should be designed to minimize tampering with, or the unauthorized physical reconfiguration of, the weapon.
- Final initiation switch should be allocated to one and only one function.
- New UMS designs shall comply with appropriate design safety requirements of the STANAGs/MIL-STDs for initiation systems and hand emplaced munitions.
- Each weapon/platform should have a unique identifier and should respond only to commands with its identifier in the command.
- UMS should provide weapon safety status to the authorized entity.
- Utilize environmental forces, wherever possible, to enable safety features.
- Reference design standards that address portions of this precept: MIL-STD-882D Section A.4.3.3.1.2.d (non-mandatory section); MIL-STD-1911 Sections 4.1.3; and Section MIL-STD-1901A Section 4.3.a. MIL-STD-1911 addresses hand emplaced munitions, and MIL-STD-1901A addresses requirements to prevent inadvertent rocket motor initiation.

Existing Policy: None.

DSP-7* The UMS shall be designed to safely initialize in the intended state, safely and verifiably change modes and states, and prevent hazardous system mode combinations or transitions.

Scope: This precept applies to all states and modes, reference the OSD UMS Safety Guide definitions for state and mode, related to every phase of UMS CONOPS including storage, transport, servicing, launch, transit, operation, and recovery. Both initialization and re-initialization must establish a known safe state. Degraded modes and states as well as operation in environmental exceptions are considered.

Rationale: This precept provides for modes and states management to ensure the system modes, states, and their transitions and combinations are designed for safe operation of the UMS.

Examples:

1. Selection of improper flight control mode may cause air vehicle loss of control and damage.
2. Some UAVs require the air vehicle to be placed in auto-launch mode prior to launch.
3. System power-up mode should ensure propulsion is deactivated and weapons system is disabled to prevent uncommanded movement and firing.
4. Transition from a training mode to an operational mode necessitates clearing registers, otherwise invalid tracks could be left in the weapon control system.

Detailed Considerations:

- The design should include specific measures to test and verify safe mode and state transitions.
- "Verifiably" may mean it is adequate that the logic of the system requires an interlock be satisfied before it proceeds.
- Any reconfiguration capability (any hardware or software changes to the system configuration) shall ensure that the UMS remains in a safe state.
- The UMS should ensure that priority message processing cannot cause transition to, or remain in, an unsafe mode, state or combination thereof.
- Ensure latency conditions of mode and/or state transitions do not adversely affect safety.
- The system should be in a verifiable safe state before transitioning between modes. Mode transitions may occur without verification of safe state if the resulting mode is “safer” in the operational context. There may be various safe states depending upon the system operational and physical environments (i.e. training, test, underwater, airborne).
- Independent verification may be considered for mode transitions from a hazardous state to a safer state. For multiple independent UMSs, operating in a Systems of Systems (SoS) environment, the UMSs may be used together to achieve

independent verification of mode transitions.

- System may require information on last known state and/or configuration to recover from an unintended shutdown or abort.
- The system should be designed to include reset capabilities, such as warm boot of individual functions or subsystems, which support safe transitions between states and modes.
- The UMS should ensure command messages are prioritized, and processed in the correct sequence within the intended state and/or mode.
- System initialization and re-initialization should not result in motion, weapons loss, or unwanted energy transfer which may harm servicing personnel or operators.
- Consideration should be given for a time of validity all safety critical commands.
- Reference NATO STANAG 4404 Sections 7.7, 8.1, 8.2, and 11.1.

Existing Policy:

Service	Document	Section	Comment
Navy	NAVSEAINST 8020.6E (Draft)	Section E13.5.a.	Text partially references precept.

DSP-8* The UMS shall be designed to provide for an authorized entity(ies) to abort operations and return the system to a safe state, if possible.

Scope: The primary intent of this precept is to provide an ability to abort an operation such as cease fire, mobility, and weapon fire sequences. The secondary intent is for the system to automatically transition to a safe state upon abort.

Rationale: The dynamics of the operational environment require all systems to provide an ability to immediately cease the current function and safe the system, if possible.

Examples:

1. A kill switch can be used to immediately cease weapons fire or vehicle movement.
2. The UMS should provide an override capability to abort specific semi and fully autonomous commanded actions. If a UMS is about to hit a soldier, an abort capability is necessary.
3. If a UAV is flying a fixed pattern and encounters an aircraft in the area, an abort is needed to stop that flight pattern and go to another waypoint.

Detailed Considerations:

- The design should include specific measures to test and verify abort transitions.
- The program needs to identify what functions can be aborted and should be included in the abort command.
- The UMS shall ensure command messages are prioritized and processed in the correct sequence and in the intended state/mode.
- The design must consider out of sequence commands, race conditions, and the timeliness of commands.
- For range testing or training consider the need for multiple operators to have ability to cease fire or abort weapon fire.
- Reference design standards that address portions of this precept: MIL-STD-1911 Section 4.1.6.4.

Existing Policy: None

DSP-9* Safety critical software for the UMS design shall only include required and intended functionality.

Scope: This precept specifically addresses the design and implementation of safety critical software particular to reuse, COTS, GOTS, and NDI.

Rationale: The intent of this precept is to ensure safety critical code does not contain "dead code", otherwise there is a risk of invoking unintended functionality. Any software deemed to have an effect on safety critical functionality should be labeled as safety critical software and should be isolated from non-safety critical software as a design mitigation against invoking possibly hazardous unintended functionality. This precept is related to PSP-3.

Examples:

1. The Therac 25 Medical Linear Accelerator – Between June 1985 and January 1987, six patients were massively overdosed. Reuse code from previous Therac models was incorporated in this model. Improper operator screen refresh routines did not pick up prescription changes and malfunction codes were not defined in user documentation.

Detailed Considerations:

- "Dead code" (code never intended for any system use) should be eliminated from any software executable image.
- Software may contain code that is "deactivated", for instance, code that may be required for qualification (flight test parameter monitoring). "Deactivated" code is not considered the same as "dead code". Removal of deactivated code requires retesting.
- Physical and functional partitioning of safety critical software, from non-safety critical software, may be necessary to ensure the integrity of safety critical processing.
- Reference NATO STANAG 4404 Section 14.6.

Existing Policy: None

DSP-10* The UMS shall be designed to minimize single-point, common mode or common cause failures that result in high and/or serious risks.

Scope: This precept is intended to mitigate potential mishap risk through safety design. Reference the OSD UMS Safety Guidance definitions for common mode failures and common cause failures. This is related to DSP-15.

Rationale: MIL-STD 882 requires two-fault tolerance and is a proven technique for reducing risk.

Examples:

1. A weaponized (machine guns, smoke grenades, etc,) UMS requires the authorized entity(ies) to take three independent actions to fire weapons. Therefore, to inadvertently fire the weapon, three inadvertent actions or errors by the authorized entity(ies) would be necessary.

Detailed Considerations:

- The design should incorporate a minimum of two independent safety features, each of which will prevent subsequent commanded (or uncommanded) launch/release/firing/arm enable of the weapon.
- Reference MIL-STD-882D Section A.4.3.3.1.2.b. (non-mandatory section)

Existing Policy: None.

DSP-11* The UMS shall be designed to minimize the use of hazardous and toxic materials.

Scope: The intent is to ensure the program is in compliance with all ESOH hazardous materials management regulations and policies.

Rationale: Compliance with DoDI 5000.2and other DoD policy to ensure that materials, which, because of quantity, concentration, or physical, chemical, or infectious characteristics, may pose a substantial hazard to human health, safety or the environment, are identified, eliminated, or minimized, managed, and mitigated.

Examples:

1. Handling procedures for ammunition, explosives, dangerous articles, munitions, and hazardous and/or toxic materials [including the collection, recycling, treatment, disposal of, and safety/occupational requirements (e.g., engineering controls, training, personal protective equipment, etc.)].
2. Identifying safety and health regulatory requirements as a result of design, operation, test, maintenance, operations, and disposal of the system. Analysis of system safety and occupational health hazards to identify, mitigate, and manage safety and occupational health risks are regulatory requirements.

Detailed Considerations:

- Plan for hazardous materials management and impacts of hazardous materials usage during system design, and plan for their subsequent safe disposal.
- Develop and implement a Hazardous Materials Management Plan (HMMP) in accordance with NAS 411. Document hazardous materials used in or required for system maintenance in the hazard tracking system.
- Comply with OSHA occupational exposure limitations.
- Ensure waste stream life cycle analysis is considered when selecting hazardous materials.
- Document program hazardous materials usage and management in each updated UMS Programmatic Environmental, Safety, and Health Evaluation (PESHE).
- Reference MIL-STD-882D Section A.4.3.1.f, and A.4.3.3.a.

Existing Policy:

Service	Document	Section	Comment
DoD	DoDI 5000.2	2.5.4.9.2, 3.9.3, E1.1.23, E.7.1.6	Text implies precept.
DoD	DoDI6050.05		Text implies precept.

DSP-12* The UMS shall be designed to minimize exposure of personnel, ordnance, and equipment to hazards generated by the UMS equipment.

Scope: This precept addresses injury from personnel exposure to hazards resulting from UMS equipment failure, damage, malfunction, overstress, etc.

Rationale: The UMS equipment should be designed to be as safe as possible during normal operations. Where it is not possible or practical to eliminate, or mitigate, hazards by design to an acceptable level for exposure of personnel to known or suspected failure modes or hazards, exposure of those personnel to these failure modes or hazards should be controlled or managed in some manner. While contact with battle damaged UMSs may be necessary or unavoidable, depending on the nature of the damage, personnel exposure to known or suspected hazards could be controlled and should be considered during the design of the UMS. Personnel exposure to hazards, risk mitigation, and residual risk acceptance, are three different yet related aspects of safety management.

Examples:

1. Overstress of a UMS hydraulic pump may result in a ruptured line, thereby causing personnel injury due to high-pressure release of hydraulic fluid.

Detailed Considerations:

- The UMS design should provide positive measures to minimize the probability of personnel injury during all life cycle phases.
- Risk acceptance and personnel exposure to hazards are two different yet related aspects of program safety management.
- The system design should provide adequate personnel protection against hazardous conditions such as:
    1. Unintended Weapons Firing and Blast Effects
    2. Radiation of Transmitters and Emitters
    3. Rotating Equipment
    4. Excessive (High) Voltages
    5. Excessive Noise Levels
    6. Explosive Environments and Ordnance
    7. Excessive RF Energies
    8. X-Rays or Laser Radiations
    9. Sharp Corners and Edges on Equipment
    10. Hydraulic and Pneumatic Pressure
- Reference MIL-STD-882D Section A.4.3.3.f. (non-mandatory section)

Existing Policy:

Service	Document	Section	Comment
US Code	Title 10, Armed Forces	Subtitle A; PART I; CHAPTER 7 & 8	Text implies precept.
US Code	29 CFR; OSHA	29 CFR Appendix A to § 1910	Text implies precept
DoD	MIL-STD-882D	All	Text implies precept
DoD	DoDI 5000.2	2.5.4.9.2, 3.9.3, E1.1.23, E.7.1.6 5.6.1, 7.3, 7.3.4	Text implies precept
Executive Order	EO 12196	Appears in: 3 CFR, 1980 Comp.; 45 FR 12769, p. 145,	Text implies precept

DSP-13* The UMS shall be designed to identify to the authorized entity(ies) the weapon being released or fired, but prior to weapon release or fire.

Scope: The intent of this precept is to mitigate the potential of releasing or firing the wrong weapon. Reference DSP-3 and DSP-6.

Rationale: Identifying the weapon being released or fired to the authorized entity(ies) assists in the mitigation of releasing and firing an unintended weapon.

Examples:

1. Due to no feedback from the UGV: the authorized entity(ies) fires a machine gun when the authorized entity(ies) thought the smoke grenade had been selected.

Detailed Considerations:

- Consider assigning a unique identifier to each weapon as mitigation to selecting the incorrect weapon. Each weapon should respond only to commands with its unique identifier in the command. The weapon should provide its unique identifier to the authorized entity.
- The UMS design should provide a means to ensure compatibility between the on-board weapons and platform.

Existing Policy:

Service	Document	Section	Comment
Navy	NAVSEAINST 8020.6E (Draft)	Section E.13.4	Text references precept.

DSP-14* In the event of unexpected loss or corruption of command link, the UMS shall transition to a pre-determined and expected state and mode.

Scope: This precept addresses the overall UMS design architecture and states and mode management in the event of unexpected loss or corruption of the command, control, and communications link (i.e. loss of data link, loss of command and control). The objective is for the UMS to be in the anticipated/expected state when recovery occurs. It is not the intended communication loss as in the case of underwater vessels or other fully autonomous UMS. The system should have the capability of storing a set of actions to take, or states to transition to, when the command link is lost. Predetermined means we have them in the plan. Expected means we intend that portion of the plan to go into effect for this condition. It applies to both the test and operational environments. This precept is related to DSP-3 and DSP-16.

Rationale: The intent of this precept is to assure that, by design; the controlling entity can anticipate the status, mode and state of the UMS, and any on-board weapons during a loss of link period, corruption of link, and the subsequent recovery of link. Determination of pre-determined and expected status should be based on analysis of such things as CONOPS, mission profile, and threat hazard assessments.

Examples:

1. A UAV would continue to fly out of range upon loss of command link if no contingency provisions are designed into the system.
2. A UAV has been directed upon loss of link to return to base. It currently has mission parameters loaded, weapons have been energized, and commanded to fire when communications link has been lost. The UAV responds to its mission parameters and is returning to base when it re-establishes communications….what state are the weapons in? Will it now execute its command to fire? If communications are lost and re-established, the UAV and weapons should default to an expected state.

Detailed Considerations:

- The design should define state and mode transitions, including a desired and/or predictable course of action (such as move physically to a safe zone or crash in a safe zone), in the event of loss of link or intermittent command and control. The criteria for pre-determined and expected states and modes, and the courses of action include:
  - the UMS CONOPS and application;
  - the level of autonomy and level of control;
  - the operating environment (i.e. training, test, underwater, airborne, etc.);
  - the adequacy of communication link.
- The UMS design should consider retention of pertinent mission information (such as last known state and configuration, etc.)

for the UMS and the controlling entity(ies) to recover from loss of the communications link.

- The UMS design must consider limiting the duration for which undelivered messages are considered valid.
- The UMS design must consider undelivered messages that can exist within the communication system.
- The UMS should ensure command messages are prioritized and processed in the correct sequence and in the intended state and mode.
- Reference NATO STANAG 4404 Section 7.4 and 8.3. DoD 8500.1 Section 4.1; and DoD 5000.1 Section E1.1.9.

Existing Policy:

Service	Document	Section	Comment
Navy	NAVSEA SWO20-AH-SAF-10	Section 14.8.3	Text partially references precept.

DSP-15* The firing of weapon systems shall require a minimum of two independent and unique validated messages in the proper sequence from the authorized entity(ies), each of which shall be generated as a consequence of separate authorized entity action. Both messages should not originate within the UMS launching platform.

Scope: This precept is intended to ensure the safe command and control of the UMS weapon release through a prescribed sequence of independent commands. Firing includes enabling and firing as discrete functions. This precept ensures a single point failure will not result in a weapons arm and fire.

Rationale: The intent of this precept is to mitigate, through design, the potential for uncommanded or unintended arm, fire, or release of weapons. This precept addresses compliance with MIL-STD-1316 and MIL-STD-1901 and supports DSP-2 and DSP-6.

Examples:

1. Mission parameters for a UAV allows weapons to be armed only within a selected area. A Global Positioning System (GPS) arm inhibit, at the UAV, may be used to disable weapons-arming function until the UAV is within the selected area. The fire command would then come from a different entity.
2. Mission parameters for a UAV allows weapons to be fired only within a selected area. A GPS fire inhibit, at the UAV, may be used to disable weapons-firing function until the UAV is within the selected area. The arming command would have been provided by a different entity.
3. A Navy weapons system contains a mode of operation, called the AUTO-SPECIAL mode, that, when enabled, will allow the weapons system to automatically acquire air contacts, perform threat evaluation on these contacts, declare contacts that meet certain threat criteria to be targets, assign weapons to engage these targets, and manage the engagement of these targets with weapons until destroyed. Once the system has been placed in AUTO-SPECIAL mode, all this takes place without human input.

Detailed Considerations:

- The arm and fire commands shall each require a unique verified message generated as a consequence of a distinct authorized entity action; both messages should not originate within the UMS launching platform.
- The arm and fire command messages shall be sent in the proper sequence and acted upon only after being recognized as being in the proper sequence.
- The UMS should be capable of determining the order in which the arming and firing messages were issued.
- UMS subsystems should not subvert or compromise the independence of weapon arm and fire safety features. For clarification:
  - A UMS cannot pick up an arm command from the authorized entity and automatically fire based solely on this arm command. This would be a dependent action.

- A UMS, having selected a target to fire upon, cannot fire when it receives an arm command. This would be an improper sequence.

- Consideration should be given for a time of validity for the arm and fire commands. Reference DSP-7.
- Reference NATO STANAG 4404 Section 13.2.

Existing Policy: None

DSP-16 The UMS shall be designed to provide contingencies in the event of safety critical failures or emergencies involving the UMS.

Scope: This precept addresses the need for design features which support operational contingencies in the event of a system malfunction or in the event of a safety emergency (a situation that arises that requires immediate attention or action). Safety critical failures must result in safe and graceful degradation of the system upon system-level or sub-system-level failures. This precept is related to OSP-1.

Rationale: The intent of this precept is to compel analysis of failure modes to anticipate their safety criticality and develop necessary contingency actions which may result in design solutions or TTPs. Such actions may include contingencies for a UMS system failure, sub-system failure, or operational or environmental condition that would ensure safe operations.

Examples:

1. When a UAV operating in autonomous mode lost propulsion, it attempted to glide to a pre-planned safe waypoint for recovery.
2. When a UGV lost its command signal it defaulted to pre-planned navigation in autonomous mode to a preset egress waypoint. This UGV has a rear obstacle avoidance system and egresses at a reduced speed.
3. Upon detection of a safety critical failure, a snapped steering cable, an UM sea-craft transitioned to a pre-set safe state resulting in "spinning" until it ran out of gas An alternate design could have provided a remote shut-off switch.

Detailed Considerations:

- The system should be designed to allow for safe and graceful degradation of the system upon system-level or sub-system-level failures.
- System faults may mandate the UMS transition to an alternate safe mode of operation.
- The UMS should provide design features that accommodate battle damage of safety-critical functionality.
- Reference NATO STANAG 4586 Sections 2.5.6 and 2.6.1.

Existing Policy:

Service	Document	Section	Comment
Navy	NAVSEA SWO20-AH-SAF-10	Section 14.8.3	Text partially references precept.

DSP-17 The UMS shall be designed to ensure safe recovery of the UMS.

Scope: This precept covers three main points: the design supports a recovery process that is adequately safe in normal operations; the design supports a recovery process in degraded or damaged mode; and the system is designed to be "safed". This precept addresses the recovery of an UMS when the state of the UMS and/or weapons may not be known, which includes the return of UMSs with weapons unexpended and possibly armed, and platform and equipment configuration upon landing and/or recovery. Methods for recovery may include back-up systems or procedural controls. OSP-2 addresses the operational aspects of safe recovery of the UMS. DSP-8 addresses some potential design considerations.

Rationale: UMSs typically represent valuable assets. Their value can be represented by such things as cost, sensitive information, and if captured, their re-use by unauthorized entities. Therefore, design features should be included to ensure safe recovery of the UMS, ancillary equipment and unexpended weapons stores.

Examples:

1. A UAV with a jettisonable weapon attempts to release weapon unsuccessfully creating a hang-fire situation. Upon UAV recovery, the design should allow for safing of the jettison rack and weapon stores.

Detailed Considerations:

- The UMS design should consider the recovery site may have assets that need to be protected from injury, death, system damage, or environmental damage.
- The UMS design should allow the weapons to be identifiably safed upon recovery.
- The UMS design should provide a means for securing movable equipment during recovery.
- UMS CBR contamination or UXO threats could exist in association with recovery.

Existing Policy: None

DSP-18* The UMS design shall ensure compatibility with test and training range environments to provide safety during test and evaluation, and training evolutions.

Scope: This precept addresses range safety requirements to ensure they are implemented and adhered to for all UMSs during test and evaluation, and training.

Rationale: Range safety requirements are essential to ensure the UMS can be safely tested and operated within the range safety envelope. Failure to comply with range safety requirements may result in denied access to the test range.

Examples:

1. Range safety required the addition of independent shutoff of propulsion and parachute activation for initial UAV tests to ensure the UAV remained within the range safety envelope. These features were removed after safe operational envelope and safety features were verified by test.
2. Range safety required an emergency shutoff button for UGV.
3. Range safety required self-destruct for UMS missile tests.
4. Range safety required a commander and driver for initial UGV tests.

Detailed Considerations:

- The design should consider a "panic stop" for training and testing operations, where possible.
- Reference the Range Safety Council manuals and contact should be made with the Range Safety Officer (RSO).

Existing Policy:

Service	Document	Section	Comment
Army	RCC 323-99	Section 1	Text partially references precept.
Air Force	EWR 127-1 (Replaced by AFSPC)	Section 2.2.6	Text references precept.
Air Force	AFSPC 91-710 (Volume 2)	Section 1.6	Text references precept.

DSP-19* The UMS shall be designed to safely operate within combined and joint operational environments.

Scope: The intent of this precept is to consider interoperability of the UMS with manned systems (unmanned undersea systems with ships, UAVs with manned military or commercial aircraft). This precept addresses de-confliction of air corridors and use of UMSs for non-military peace-time operations such as disaster relief and boarder patrol. This also addresses potential ad-hoc combinations of systems by the field commander(s) that may not have originally intended to operate as combined systems or as an SoS.

Rationale: The intent of this precept is to provide safety compatibility among independently developed systems operating in a combined or joint operational environment

Examples:

1. Use of a UAV within the National Air Space (NAS).
2. Use of UMSs for non-military peace-time operations such as disaster relief and border patrol.
3. Multiple UMSs, operating in a net-centric environment, could tax the communications network bandwidth.

Detailed Considerations:

- Communication reliability, network availability/quality of service and data/information assurance shall be commensurate with the safety criticality of the functions supported.
- The system should be designed to be operated and transported during non-wartime conditions within normal transportation and commercial airspace environments meeting the requirements of the DOT, FAA, ETS 300-019, Part 1-2, IEC 721.
- Reference the Society of Automotive Engineers AS-4 Joint Architecture for Unmanned Systems (JAUS) Working Group related to interoperability.
- In accordance with CJCSI 3170 directives, all systems will be reviewed for safety within the joint, combined, and SoS environments.
- Reference NATO STANAG 4586 Section 1.1 (para 6).

Existing Policy:	Service	Document	Section	Comment
	Joint Chiefs of Staff	CJCSI 3170.01E	4	Text implies precept.
	DoD	DoDD 4630.05	4.1	Text implies precept.