

## 13th ICCRTS: C2 for Complex Endeavors

The Safety of Unmanned Systems:  
The Development of Safety Precepts for Unmanned Systems (UMS)

### Authors

Dr. Thomas P. English, Naval Surface Warfare Center, Panama City, FL  
Mr. David J. Shampine, Naval Ordnance Safety and Security Activity, Indian Head, MD  
Dr. Julie A. Adams, Vanderbilt University, Nashville, TN  
Dr. Charles G. Muniak, Lockheed Martin, Syracuse, NY  
Mr. Edward W. Kratovil, SAIC, Waldorf, MD

### Point of Contact

Dr. Thomas P. English  
Naval Surface Warfare Center  
Naval Coastal Systems Station  
Panama, City, FL  
(850) 235-5403 office  
thomas.english@navy.mil

## 13th ICCRTS: C2 for Complex Endeavors

### **The Safety of Unmanned Systems: The Development of Safety Precepts for Unmanned Systems (UMS)**

#### **Abstract**

In October 2005, the Defense Safety Oversight Council (DSOC), Acquisition and Technology Programs Task Force (ATP TF) established an initiative to help ensure the safety of unmanned systems (UMS). This initiative was established in response to the proliferation of UMS within the Department of Defense (DoD), and a concern for safety when these systems, primarily unmanned air vehicles, were operated over populated areas, or in proximity to other aircraft, both military and civilian, and when configured with weapons or ordnance items. This paper discusses the process that was followed in developing the UMS safety precepts and the associated DoD UMS safety guidelines document. It will also discuss the environment in which UMS are currently employed, the safety concerns with those operational environments and designs, UMS guide objectives, and conclude with an example of a Command and Control/Situational Awareness precept.

**Keywords:** unmanned systems, UMS, safety precepts, OSD UMS safety guide

#### **Introduction**

It is anticipated that unmanned systems will play a transformational role in all aspects of warfare including command and control (reference 1). The successful development and acquisition of these systems of systems, which may be composed of a multitude of platforms, will require new engineering and management concepts (reference 2). One specific engineering discipline that must develop new approaches to this transformation is system safety. To this end, in 2005, the Defense Safety Oversight Council (DSOC), Acquisition and Technology Programs Task Force (ATP TF) established an initiative to help ensure the safety of unmanned systems (UMSs). This initiative was established in response to the proliferation of UMS within the Department of Defense (DoD), and a concern for safety when these systems, primarily unmanned air vehicles, were operated over populated areas, or in proximity to other aircraft, both military and civilian, and when configured with weapons or ordnance items.

Numerous UMSs are currently under development in each of the Services, as well as other government agencies. The traditional view that a specific Service's UMS, for example, will never have to interface or coordinate with the other Services' systems is no longer true in today's Joint warfighting environments. Addressing such issues as integrated operations, system control, communication, safe navigation, security, and target identification/verification are major

challenges for all UMSs (e.g., references 3 and 4); however, there is no unified system safety approach to address these kinds of issues.

In order to develop safe UMSs, this safety initiative had the goal of establishing safety guidelines that are tailored to, and focused on the safety of UMSs regardless of the environment in which they are used. This safety project had over 80 participants from across the safety community including Army, Navy, Air Force, Marine Corps, NASA, Industry, and Academia. The intent was for the government and industry safety community to develop a set of safety guidelines that will be accepted and effectively utilized by acquisition program managers and operators during the development and operation of UMSs.

## **Discussion**

An 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.”

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

- Weapons platforms (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 system 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 an UMS as opposed to humans, significant system 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 recognize the change in target profile and not delivered the weapon. Additionally, using UMS platforms to investigate or operate in dangerous environments present new risks when retrieving that UMS after its exposure to dangerous environmental conditions. For instance, employing an UMS to investigate an unknown environment, that turns out to be contaminated with Chemical, Biological, or Radiological (CBR) waste could result in exposing the humans retrieving the UMS to CBR contamination. Finally, an UMS itself, depending on its design, can present hazards to humans by its construction. Because of the reduced human interaction, an UMS may be constructed of materials and components that may present inherent hazards, such as hydraulics, pneumatics, or high-level Radio Frequency RF emitters.

### **Why System Safety is critical in UMS**

In manned systems, mishaps may ultimately be mitigated by a human operator. UMSs possess unique safety concerns and issues because they may not have a human in the loop. 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 system 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 an 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.

A key system safety concern of decision making authorities involved in the design, development, and operational use of UMSs, is the level of UMS weaponization, and how to establish and maintain positive control of these weaponized systems. Weapons technology and weapons associated functionalities include, but are not limited to, the following: 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. Typical system safety issues associated with UMS weaponization 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.

Appendix A of this paper contains a sample of the many different system safety issues that the working groups considered when developing their proposed safety precepts.

When designing an UMS, actually any system, system engineering will design and test for the “right” data, at the “right” time. System safety engineering, however, will consider three different scenarios and the consequences. As shown in Figure 1 below, these three scenarios are:

- a. right data at the wrong time
- b. wrong data, but at the right time
- c. wrong data at the wrong time

<b>Data</b>	<i>boolean</i>	<b>Time</b>	<i>boolean</i>	<i>Requirements Responsibility</i>
RIGHT	1	RIGHT	1	Sys Eng
RIGHT	1	WRONG	0	Safety
WRONG	0	RIGHT	1	Safety
WRONG	0	WRONG	0	Safety

**Figure 1. Requirements Responsibility for Systems vs. Safety Engineering**

From a command and control perspective, understanding and designing for these three scenarios is critical for the safe and effective operation of UMSs.

Due to the anticipated advancement in weapon system design and operation, several key areas where identified as posing complex and complicated safety evaluation issues:

- Weapon Interaction
- Software
- Communications concepts
- Security
- Fuzing
- Unmanned Systems as systems
- Autonomy Levels
- Advances in command and control
- System of systems
- Net Centric warfare

In order to be prepared to adequately assess these systems in the future, the concept of a guide for the development of Unmanned Systems was initiated.

The objective in the development of this guidance was to ensure the design and development of UMSs incorporated the necessary system safety design rigor to prevent potential mishaps, or mitigate potential mishap risk. Director, Systems and Software Engineering (SSE), Acquisition Technology and Logistics (AT&L), Office of the Secretary of Defense (OSD), provided the leadership for this initiative, and 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 that system safety is a fundamental pillar of the acquisition process and incorporates those necessary design considerations to safely sustain UMSs.

The safety precepts provided in the OSD guide were developed by a select group of design and system safety engineers and Program Managers. 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.

The current OSD UMS safety guide, which is officially titled, “UNMANNED SYSTEMS SAFETY GUIDE FOR DOD ACQUISITION”, dated 27 June 2007, can be found at <http://www.acq.osd.mil/atptf/>. The UMSs Safety Guide currently contains the following Table of Contents:

1. Key Terms, Descriptions, and Principles
  - 1.1 Unmanned System
  - 1.2 Safety Precept
  - 1.3 Authorized Entity
2. System Safety Overview
  - 2.1 System Safety and the UMS Precepts
  - 2.2 Characteristics of Successful System Safety Programs
3. Unmanned System Safety Overview
  - 3.1 Unique Aspects of Military Unmanned Systems
  - 3.2 Top Level Mishaps for Unmanned Systems
4. Unmanned System Safety Program Aspects
  - 4.1 Safety Precepts
  - 4.2 Programmatic Safety Precepts
5. Unmanned System Operational Aspects
  - 5.1 Unmanned Systems Operational Safety Functionality
  - 5.2 Operational Safety Precepts

- 6. Unmanned Systems Design Aspects
  - 6.1 Unmanned Systems Design Safety Functionality
    - 6.1.1 Weaponization
    - 6.1.2 Situational Awareness (Information, Intelligence, and Method of Control (I2C))
    - 6.1.3 Command and Control
    - 6.1.4 States and Modes
  - 6.2 Design Safety Precepts

- Appendix A. References and Resource Guide
- Appendix B. Acronyms
- Appendix C. Definitions
- Appendix D. Major Contributors
- Appendix E. Safety Precept Clarification Tables

## **Development of the UMS Safety Precepts**

During the development of the proposed OSD UMSs Safety Guide, the question was often asked by UMS program managers, “Why do we need safety precepts for UMSs”? Safety precepts are the starting point for system development. These precepts provide an indicator of where the program needs to focus its attention in order to develop a safe system. In addition, the precepts also provide guidance for the safe design of UMS, and are the precursor for design safety requirements. Safety precepts are often used to help establish the tasks and priorities for a system safety program. Safety precepts should be considered building blocks in the system safety process, that is, they provide a “foundation” upon which a system safety program can be built to help ensure the safety of UMSs.

As part of this UMS safety initiative, it was recognized, early in the process that safety precepts basically fall into three categories:

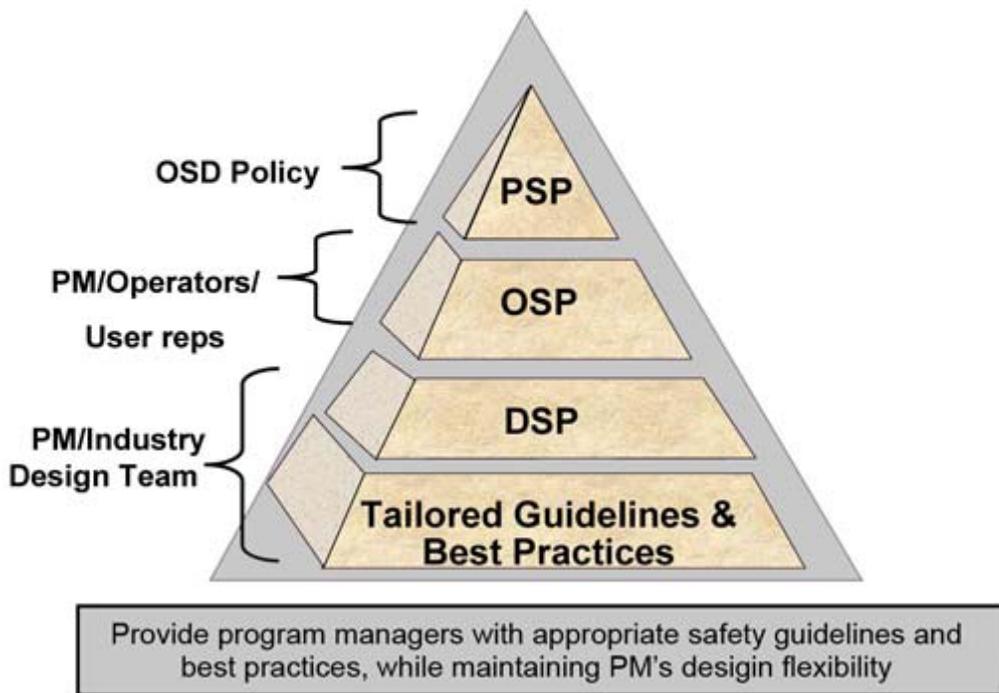
1. programmatic
2. operational
3. design

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 or hazard types.”

The three categories of safety precepts are defined, as follows, and are depicted in Figure 2:

- 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).
- Design Safety Precepts (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 for UMS



**Figure 2. Levels of Safety Precepts for Unmanned Systems**

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.

Safety precepts for UMSs did not previously exist; they evolved through an arduous, but thorough, systems engineering process performed as part of this OSD UMS safety initiative. The precepts, presented in the OSD guide, are provided as a generic and minimum set of precepts for the design, development, and operation of any UMS system. Appendix B provides a complete listing of all 30 precepts.

In addition to these precepts, the Draft OSD UMS Safety Guide also includes an Appendix E, titled “Safety Precept Clarification Tables”. These clarification tables provide additional information regarding the scope, rationale, examples, detailed design considerations, and existing policy for each precept. These clarification tables are intended to provide the program manager with a better understanding as to the thought process behind each of these one-sentence precepts. And by better understanding the thought process behind each of these precepts, it was felt that program managers could be more creative in how the precept was actually implemented. Appendix C provides an example of a typical precept clarification table that is contained in the OSD UMS Safety Guide.

### **Situational Awareness/Command and Control Precept**

In developing the precepts for the guide, a basic understanding was needed of UMS command and control authorities, and who or what will be controlling the individual phases of operation of the UMS, both in the near term and in the future. Consequently, several working groups were established to develop the precepts by function, to include all aspects of unmanned system operation.

The working groups quickly realized that in some cases, the control of an UMS may be conducted by a human operator from a remote location through a remote control console. In other cases, operation may be the result of pre-programmed mission parameters and commands, or control may even be a fully autonomous function of the UMS. In still other cases, control may be provided by another UMS or multiple UMSs in a networked environment. When developing the safety precepts provided in the DoD UMS Guide, both human and autonomous methods of control were considered. The interaction of humans with various levels of automation is an area of active research (e.g., reference 5) which is needed for operators to properly conceptualize the tactical situation. 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). Following are the definitions for these two terms:

- An authorized entity is defined as: “An individual operator or control element authorized to direct or control system functions or mission.”
- A controlling entity is defined as: “An individual operator or control element directing or controlling system functions or mission.”

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.

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 one or more UMSs. 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.

When operating an UMS, the authorized entity must not only maintain positive command and control, but also must have “situational awareness” to operate the UMS in an effective and safety manner. Situational Awareness (SA) as defined by Endsley (reference 6) is “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.” There can be both individual and group or team situational awareness.

SA in this context typically is defined in relation to a particular mission that must be attained over time; therefore knowledge of the associated mission goals and objectives determine the information required by the human to successfully complete the mission. Endsley’s SA definition encompasses three levels of SA relative to the assigned mission:

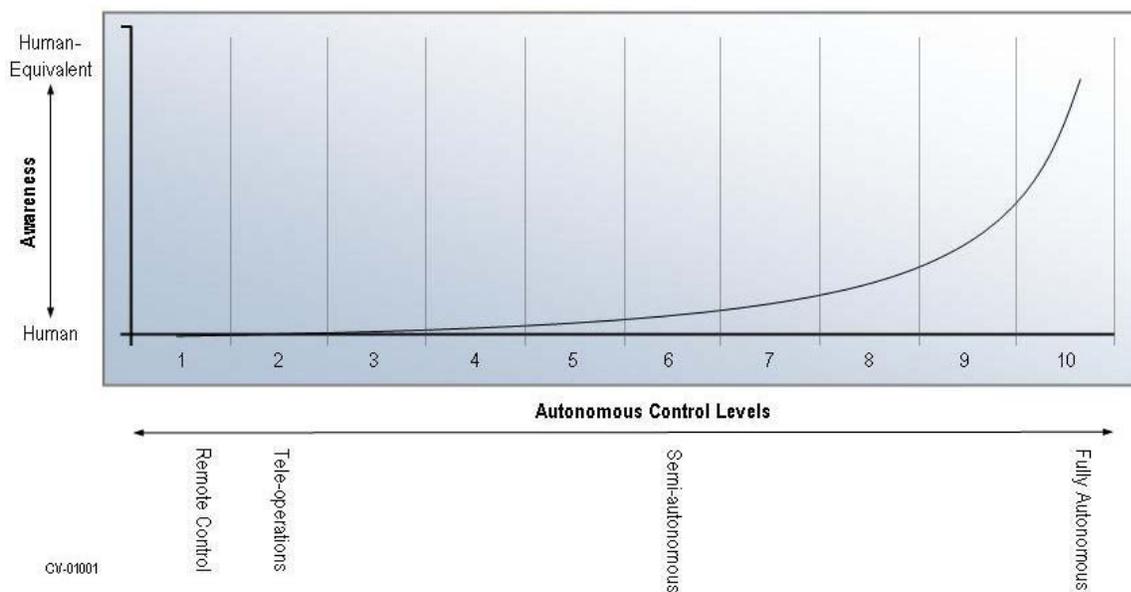
1. Level 1 – perception of the environment;
2. Level 2 – comprehension of the situation; and,
3. Level 3 – projection into the near future.

Level 1 SA requires that the UMS perceive the environment relative to the assigned mission, including the environmental status, attributes, and dynamics. Various combinations of sensor capabilities are necessary to perceive the relevant environmental aspects that vary across application domains. A complete implementation of this level of SA requires a number of components. First, UMS SA requires a suite of sensing capabilities along with the sensor feedback, update rates, information resolution levels, and sensor fusion. Communications from other UMSs or humans must be fed into the SA processing as such information also represents percepts. UMS SA must also incorporate the capacity for UMSs to provide adaptive sensing. Adaptive sensing incorporates the ability to determine which sensor to use at a particular time, modification of the sensor processing, or combination of sensors required based upon the task. Additionally, UMS SA must provide the capability for the sensors to direct attention.

Level 2 SA requires the UMS to integrate a large number of percepts (level one SA) and prioritize the importance and meaning of the integrated information with regard to mission goals. This level of SA requires the UMS to develop situational comprehension based upon a number of comprehension components including: expectations (perhaps a side-effect of human programming), an UMS equivalent of human mental models, working memory, long-term memory, redirecting attentional focus, prior decisions, and prior plans. Some of these components have been individually developed but a holistic comprehension capability does not currently exist.

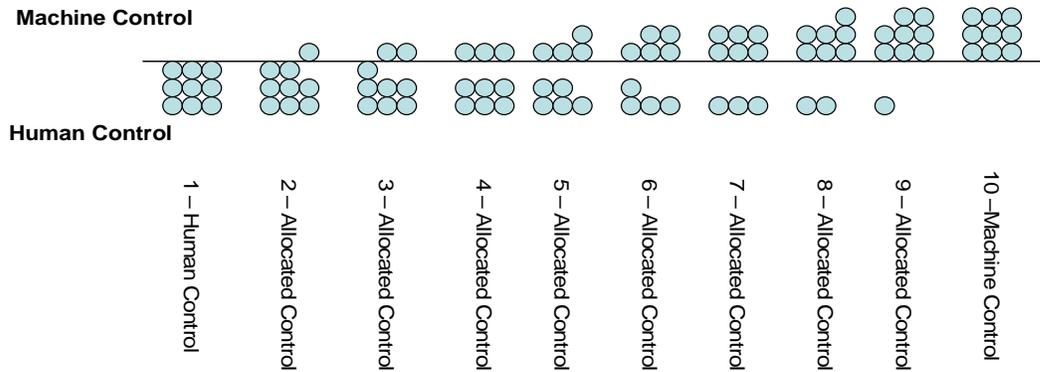
Level 3 SA requires UMSs to predict what will occur in the near future based upon their perception and comprehension of the current mission situation, thus level three SA is directly dependent upon attaining good level 1 and 2 SA. This projection requires an excellent understanding of the mission domain and is a highly demanding cognitive activity for humans, and current UMSs have limited, if any, ability to emulate level three SA.

Figure 3 depicts the shift in SA associated with changing levels of autonomous control. Without direct human control of a system, an 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. This increase in autonomy and awareness represents a shift from the UMS needing level 1 SA only, at lower levels of autonomy, to level 3 SA at the highest levels of autonomy.



**Figure 3. Levels of Control for UMS**

Another way to think of the concept of “man control” and “machine control” is depicted in Figure 4 below. The shaded circles (●) denote the potential level of control from full human control to fully autonomous control. The position of the shaded circles on the chart show whether the human or the machine has SA / Information, Intelligence, and Method of Control (I<sup>2</sup>C). It is noted that human SA requires performance measurement criteria to evaluate, however, machine I<sup>2</sup>C requires an original characterization since it is not currently defined.



**Figure 4. Control Allocation**

The development of fully autonomous UMSs with human-like SA requires a holistic development approach, rather than stove pipe technology development. Thus far, stove pipe development of artificial intelligence and autonomy has not provided the integration required to attain UMS SA. Current approaches that attempt to improve operator interaction, intelligence, and/or autonomous behaviors will not solely lead to human-like UMS SA.

A key problem encountered during development of precepts addressing the SA and Command and Control was the variety of interpretations of what comprises adequate SA or Command and Control. It was this aspect of the relationship that the precept developers finally combined into one set of definitions, which resulted in development of one of the fundamental design safety precepts for unmanned systems.

To demonstrate how these safety precepts are directly related to command and control, the following discussion addresses one of the design safety precepts, DSP 3.

### **Design Safety Precept #3: Situational Awareness / Command and Control**

DSP #3 states: “The unmanned system shall be designed to provide information, intelligence, and method of control (I2C) to support safe operations.”

In order to understand this precept, the following definitions were established for formulating the basis of the precept.

Definitions:

1. Information: Knowledge or data necessary for the safe operation of an UMS; obtained from the process of recognizing and interpreting data in the environment, memory and recall of facts, and/or communication.
2. Intelligence: The capacity of an UMS to acquire, comprehend, and apply information.
3. Method of control: 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: The means by which an UMS receives instructions governing its actions and feeds back information.
    - Remote control
    - Tele-operation
    - Semi-autonomous
    - Fully autonomous
  - Level of command authority: The degree to which an entity is invested with the power to access the control and functions of an 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: The level at which a controlling entity interacts, influences, or directs an UMS(s).
    - Actuator
    - Primitive
    - Subsystem
    - Vehicle
    - Group of vehicles
    - System of systems

With the establishment of the frame work with which to qualitatively define SA/Command and Control, the group developed a three-dimensional composite relationship between SA and Command and Control. Using the definitions above, and as shown in figure 5 below, there is a direct relationship among “level of control”, “mode of control”, and “level of command authority” that must be recognized and considered when designing UMSs.

As previously mentioned, the OSD UMS Guide contains “precept clarification tables” to help the design engineers better understand the rationale for the precept. Appendix C of this paper provides, as an example, the precept clarification table for DSP #3. As shown in Appendix C,

there is a section titled, “Detailed Considerations” that lists several key design issues that affect command and control as it relates to the safe and operationally effective use of UMSs.

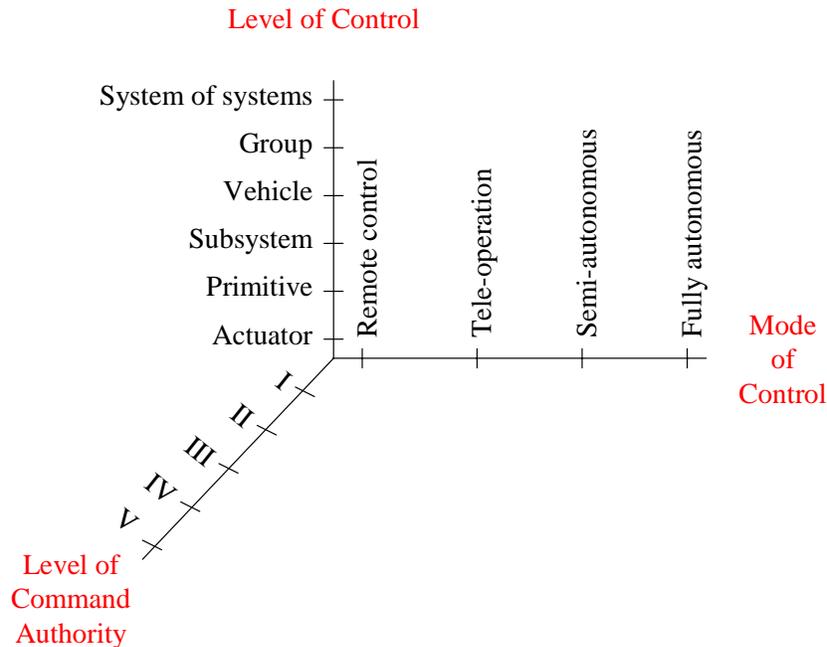


Figure 5. UMS Command and Control Elements

**Summary**

As a result of the process described above, a credible list of safety precepts for UMSs has been developed. These precepts are general in nature to include as many different types of military UMSs as possible, and can provide a solid foundation upon which to design, build and operate UMSs that safe and operationally effective. This list can be applied to current UMS development projects for program and design safety guidance. Through the use of these precepts, however, it is anticipated that these current precepts may need to be modified, or new precepts developed to maintain safety and positive command and control of future UMSs. These precepts were published in an OSD UMS safety guideline manual, titled Unmanned Systems Safety Guide for DOD Acquisition, dated 27 June 2007. This OSD UMS Safety Guide will be referenced in DoDI 5000.2 to ensure that these precepts are at least considered by program managers during the acquisition process for UMSs.

Great work has been accomplished to date regarding the safety of UMS; more needs to be accomplished to make these precepts relevant to new C2 approaches

The challenge to the C2 community is to review and use these precepts when designing C2 systems for UMS, and modify these existing precepts, or develop new precepts, as necessary, to better meet your needs.

## References

1. Hudson E.C., Johnson G., Summey D. C., & Portman H.H. (2004). Shaping Future Naval Warfare with Unmanned Systems - The Impact Across the Fleet and Joint Considerations. *Engineering the Total Ship Symposium*, Gaithersburg Maryland
2. Software Engineering Institute, (2006). *Ultra-Large Scale Systems The Software Challenge of the Future*. Carnegie Mellon University
3. Castelin S., & Bernstein P. (2004). A Notional Scenario for the Use of Unmanned System Groups in Littoral Warfare. *IEEE/OES Autonomous Underwater Vehicles*, Sebasco Maine pp.4-19
4. Benjamin M.R.,& Curcio J.A., (2004). OLREGS-Based Navigation of Autonomous Marine Vehicles. *IEEE/OES Autonomous Underwater Vehicles*, Sebasco Maine pp.32-39
5. Bruni S., Marquez J., Brzezinski A.,Nehme C.,& Boussemart Y. (2007). Introducing a Human-Automation Collaboration Taxonomy (HACT) in Command and Control Decision-Support Systems. *12th International Command and Control Research and Technology Symposium*
6. Endsley, M. R. (1988) Design and Evaluation for Situation Awareness Enhancement. *Proceedings of the Human Factors Society 32<sup>nd</sup> Annual Meeting*. 1: 97-101.

**Appendix A.**

Typical System Safety Issues and Considerations for UMSs

<b>Safety Concerns</b>	<b>Causal Factors</b>	<b>Safety Objectives</b>
<p>Loss of UMS vehicle ownership.</p> <p>Implications:</p> <ul style="list-style-type: none"> <li>• Out of sight</li> <li>• Out of control range</li> <li>• No remote control</li> <li>• Unknown safety state</li> <li>• Theft of weapons/explosives</li> <li>• A destruct system is inherently hazardous for normal operation</li> <li>• Enemy takes control</li> <li>• Results in crash, falling into enemy hands, loss of vehicle, weapons, equipment, etc.</li> </ul>	<ul style="list-style-type: none"> <li>• Escapes control range</li> <li>• Loss of situational awareness</li> <li>• Loss of communications</li> <li>• Loss/failure of critical subsystems</li> <li>• Enemy communications takeover</li> <li>• Enemy physical takeover</li> </ul>	<ul style="list-style-type: none"> <li>• Prevent losing control of vehicle</li> <li>• Prevent losing ownership of vehicle</li> <li>• Prevent enemy takeover of vehicle control</li> <li>• Prevent enemy from taking weapons aboard a vehicle</li> <li>• Secure communications</li> <li>• Vehicle self-attempts to return to base</li> <li>• Ensure vehicle is safe when it returns</li> </ul>

<b>Safety Concerns</b>	<b>Causal Factors</b>	<b>Safety Objectives</b>
<p>Loss of safe control over a UMS vehicle.</p> <p>Implications:</p> <ul style="list-style-type: none"> <li>• In sight; In range</li> <li>• Partial or no remote control</li> <li>• Unknown safety state</li> <li>• Ownership maintained</li> <li>• UMS refuses to obey remote control commands</li> <li>• UMS performs tasks erroneously</li> <li>• Enemy jams control frequency</li> <li>• Results in fratricide, crash, collision, weapons fire, etc.</li> </ul>	<ul style="list-style-type: none"> <li>• Enters unsafe state</li> <li>• Loss of communications</li> <li>• Loss/failure of critical subsystems</li> <li>• Failure of self test subsystem</li> </ul>	<ul style="list-style-type: none"> <li>• Prevent losing control of vehicle</li> <li>• Establish safe states for varying losses of control</li> <li>• Secure communications</li> <li>• Maintain communications</li> <li>• Maintain vehicle situational awareness</li> <li>• Emergency operator stop</li> <li>• Maintain awareness of UMS status</li> </ul>
<p>Loss of communications with UMS vehicle.</p>	<ul style="list-style-type: none"> <li>• Loss of communication links</li> <li>• Loss/failure of critical subsystems</li> <li>• Communication</li> </ul>	<ul style="list-style-type: none"> <li>• UMS detects and takes action to reestablish communication (e.g., homing path)</li> </ul>

<b>Safety Concerns</b>	<b>Causal Factors</b>	<b>Safety Objectives</b>
<p>Implications:</p> <ul style="list-style-type: none"> <li>• Unable to remotely safe</li> <li>• Allows vehicle to get out of control range</li> <li>• Loss of control</li> <li>• Results in crash, collision, fratricide, erroneous weapon fire, loss of status, loss of control, etc.</li> </ul>	<ul style="list-style-type: none"> <li>• jamming</li> <li>• Excessive noise</li> <li>• Battle damage</li> </ul>	<ul style="list-style-type: none"> <li>• Communications redundancy or backup system</li> <li>• Prevent jamming</li> </ul>
<p>UMS Inadvertently initiates firing of weapon or explosive systems without intent or authorization.</p> <p>Implications:</p> <ul style="list-style-type: none"> <li>• Unauthorized firing of weapons or explosives</li> <li>• Unintended firing of weapons or explosives</li> <li>• Risk present</li> </ul>	<ul style="list-style-type: none"> <li>• Failure of critical subsystems</li> <li>• Communications jamming</li> <li>• Battle damage</li> <li>• Due to failures, personnel error, RF energy, etc.</li> </ul>	<ul style="list-style-type: none"> <li>• Minimize potential for inadvertent launch or firing</li> <li>• Detect and report weapon safe states</li> </ul>

<b>Safety Concerns</b>	<b>Causal Factors</b>	<b>Safety Objectives</b>
<p>during operation, transportation, standby modes</p> <ul style="list-style-type: none"> <li>• Results in launch/firing of weapons, causing death/injury, publicity, etc.</li> </ul>		
<p>Personnel injury due to inadvertent or erroneous operation of critical or hazardous systems on the UMS vehicle.</p> <p>Implications:</p> <ul style="list-style-type: none"> <li>• Personnel exposure to unexpected movements</li> <li>• Personnel exposure to released energy sources</li> <li>• e.g., hydraulics, RF energy, fuel, toxicity, noise,</li> </ul>	<ul style="list-style-type: none"> <li>• Failure of hazardous subsystems</li> <li>• Erroneous operation of hazardous subsystems</li> <li>• Battle damage</li> </ul>	<ul style="list-style-type: none"> <li>• Minimize potential for erroneous operation of UMS</li> <li>• Monitor hazardous subsystems</li> <li>• UMS and/or subsystem shutdown</li> </ul>

<b>Safety Concerns</b>	<b>Causal Factors</b>	<b>Safety Objectives</b>
vibration <ul style="list-style-type: none"> <li>• Results in personnel injury</li> </ul>		
Personnel injury due to an unsafe UMS state.  Implications: <ul style="list-style-type: none"> <li>• UMS enters an unsafe state</li> <li>• Safety state may be known or unknown</li> <li>• UMS must be secured and made safe before mishap</li> <li>• States may include fire, armed weapon, toxic fumes, erratic movement, etc.</li> <li>• Results in personnel injury</li> </ul>	<ul style="list-style-type: none"> <li>• Failure of critical subsystems</li> <li>• Failure of hazardous subsystems</li> <li>• Loss of unsafe state warning</li> <li>• Battle damage</li> </ul>	<ul style="list-style-type: none"> <li>• Establish UMS safe states</li> <li>• Emergency operator stop</li> <li>• Provide method for awareness of safe state (local &amp; remote)</li> <li>• UMS and/or subsystem shutdown</li> </ul>
UMS vehicle runs over friendly troops or civilians.	<ul style="list-style-type: none"> <li>• Loss of situational awareness</li> <li>• Loss of</li> </ul>	<ul style="list-style-type: none"> <li>• Maintain vehicle situational awareness</li> <li>• Operator awareness</li> </ul>

<b>Safety Concerns</b>	<b>Causal Factors</b>	<b>Safety Objectives</b>
<p>Implications:</p> <ul style="list-style-type: none"> <li>• Due to incorrect heading, failures, proximity, human error, etc.</li> <li>• Incorrect situational awareness</li> <li>• Remote operator unaware of closeness of personnel</li> <li>• Remote operator error</li> <li>• Results in personnel death/injury</li> </ul>	<p>communications</p> <ul style="list-style-type: none"> <li>• Loss/failure of critical subsystems</li> <li>• Operator HSI error</li> </ul>	<ul style="list-style-type: none"> <li>• UMS and/or subsystem shutdown</li> </ul>
<p>UMS erroneously fires weapons or explosive systems on friendly troops or civilians.</p> <p>Implications:</p> <ul style="list-style-type: none"> <li>• Planned or authorized firing of weapons or</li> </ul>	<ul style="list-style-type: none"> <li>• Personnel error</li> <li>• Loss of situational awareness</li> <li>• Failure of critical subsystems</li> <li>• Battle damage</li> </ul>	<ul style="list-style-type: none"> <li>• Maintain vehicle situational awareness</li> <li>• Maintain operator in the fire control loop</li> <li>• UMS and/or subsystem shutdown</li> </ul>

<b>Safety Concerns</b>	<b>Causal Factors</b>	<b>Safety Objectives</b>
<p>explosives, but done incorrectly or untimely</p> <ul style="list-style-type: none"> <li>• Due to incorrect heading, failures, proximity, human error, etc.</li> <li>• Incorrect situational awareness</li> <li>• Results in death/injury, publicity, etc.</li> </ul>		
<p>Remote operator places robot vehicle in hazardous mission situation.</p> <p>Implications:</p> <ul style="list-style-type: none"> <li>• Results in personnel injury, damage to weapons, etc.</li> <li>• HSI interface causes operator confusion</li> <li>• Operator</li> </ul>	<ul style="list-style-type: none"> <li>• Video/control feedback too slow</li> <li>• Loss of situational awareness</li> <li>• Reduction in communications quality</li> <li>• Poor HSI design</li> </ul>	<ul style="list-style-type: none"> <li>• Maintain vehicle situational awareness</li> <li>• Optimize HSI interface for safety</li> <li>• Establish required skill levels</li> <li>• Emergency stop</li> </ul>

<b>Safety Concerns</b>	<b>Causal Factors</b>	<b>Safety Objectives</b>
<p>training/experience is inadequate for level of difficulty</p> <ul style="list-style-type: none"> <li>• Results in launch/firing of weapons, causing death/injury, publicity, etc.</li> </ul>		

## Appendix B

### Listing of the 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.

\* Denotes applicability to both manned and unmanned systems.

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.
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.

<b>Design Safety Precepts (DSPs)</b>	
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).
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 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.
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.

## Appendix C

### Example Safety Precept Clarification Table

<p><b>DSP-3:</b> The UMS shall be designed to provide information, intelligence, and method of control (I2C) to support safe operations.</p>
<p><b>Scope:</b> 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.</p>
<p><b>Rationale:</b> The intent of this precept is to address critical safety elements of situational awareness required for safe operation to:</p> <ul style="list-style-type: none"><li>• Ensure the operation remains within safe performance limits.</li><li>• Provide alerts related to performance anomalies which could lead to hazards.</li><li>• Use monitoring to ensure non-propagation of hazards throughout the vehicle.</li><li>• Update guidance to avoid potential hazard scenarios in changing situations.</li></ul>
<p><b>Examples:</b></p> <ol style="list-style-type: none"><li>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.</li><li>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.</li><li>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.</li></ol>
<p><b>Detailed Considerations:</b></p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li><li>• The human machine interface should be designed using a defined set of symbols and terms common to platforms and</li></ul>

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