Safety of Unmanned Systems

Sponsored by

Defense Safety Oversight Council Acquisition and Technology Programs Task Force (DSOC ATP TF)

Status Update

Michael H. Demmick

24 October 2007

Agenda

- Leadership
- Background
- Objectives
- Approach
- Progress
- Organization
- Workgroup participants
- Precepts Review
- Final Product
- Summary

Unmanned Systems Leadership

- **OSD Sponsor**
  - **Mr. Mark Schaeffer, Director, Systems and Software Engineering & Chairman, DSOC ATP TF**
  - **Dr. Liz Rodriquez-Johnson, Executive Secretary, DSOC ATP TF**

Why Safety of UMSs?

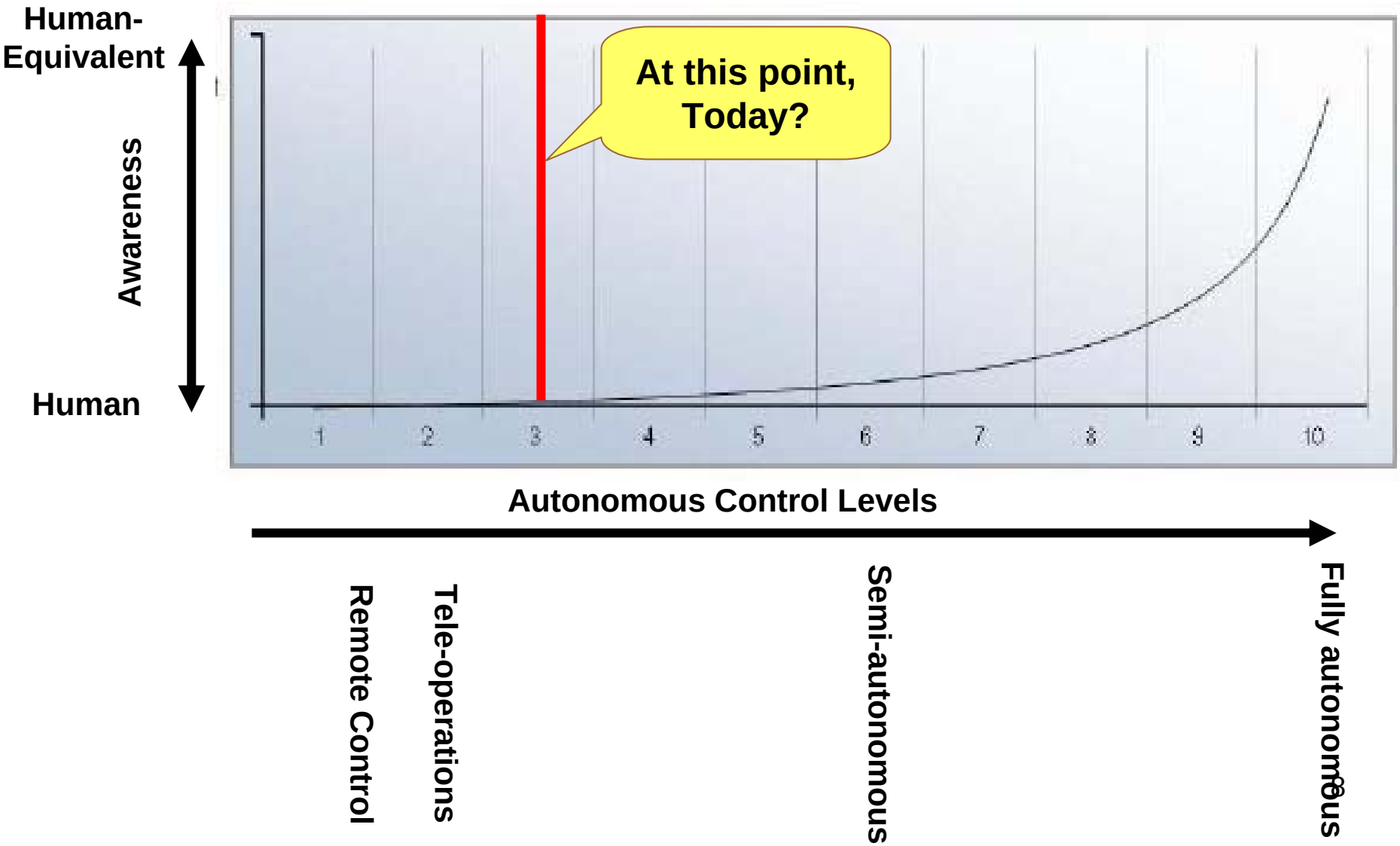
MQ-1 PREDATOR WITH HELLFIRES (USAF)

Talon Swords

UAV launch from MDARS

Raytheon UCAV

UMS Level of Awareness vs. Levels of Control



Background

- **In FY05, the OSD Joint Robotics Program Coordinator for ground systems tasked Navy to:**
  - **Provide unifying safety guidance across all ground robotic projects**
  - **Establish initial safety precepts for ground robotic systems**
    - **Program Safety Guidance**
    - **Operational Guidance**
    - **System Design Safety Guidance**
- **Results briefed at 2005 ISSC**

Background

- October 2005 briefed to OSD (DSOC ATP TF)
- ATP TF directed expansion of effort to include <u>all</u> Unmanned Systems (air, ground, and sea)
- Emphasized necessity of community input
  - Program Management
  - Design
  - Test
  - Operational
  - Safety
- Emphasized <u>guidance</u> vice direction

UMS Safety Objectives

- **Focus the technical community on the System Safety needs for UMS**
- **Specifically:**
  1. **Understand the safety implications, including legal issues, associated with the rapid development and use of a diverse family of unmanned systems both within, and external to, the DoD.**
  2. **Establish and agree upon a standardized set of safety precepts to guide the design, operation, and programmatic oversight of all unmanned systems.**
  3. **Develop safety guidance, such as design features, hazard controls and mitigators, for the design, development, and acquisition of unmanned systems.**

Approach

- ✓ **Involve technical community**
  - Six Workgroups
  - Approximately 80 technical experts
  - Government, Industry, Academia
- ✓ **Maximize Community Awareness**
  - March 2006 Workshop
    - 300 attendees
  - International Systems Safety Conference (ISSC)
  - Association of Unmanned Vehicles International (AUVSI)
  - NDIA Systems Engineering Conference
- ✓ **Obtain Feedback**
  - Web Page (http://www.ih.navy.mil/unmannedsystems)
  - Tech Panels & Reviews
    - ✓ ISSC (31 July - 4 Aug 2006)
    - ✓ AUVSI (29 – 31 Aug 2006)
    - ✓ NDIA Systems Engineering (23 – 26 Oct 2006)
    - ✓ Mr. Schaeffer's Systems Engineering Forum
    - ✓ NDIA Systems Engineering (22 – 25 Oct 2007)

Road to Completion

- ✓ **Held Three Workshops**
  - March 2006, Huntsville
  - May 2006, Crystal City
  - June 2006, Crystal City
- ✓ **Developed Safety Precepts**
  - Programmatic safety precepts (6)
  - Operational safety precepts (5)
  - Design safety precepts (19)
- ✓ **Developed more detailed design safety "best practices" (safety precept clarification tables) (ongoing)**
- ✓ **USD (AT&L) issued the Guide on 17 July 2007**

Workshop Organization

- **Six Workgroups**
  1. **Precept Development**
  2. **Weapons Control**
  3. **Situational Awareness**
     - **Human-Machine Interface**
     - **Machine-Machine Interface**
  4. **Command and Control**
  5. **States and Modes**
  6. **Definitions/Common Taxonomy**

Unmanned Systems Management Team

- **Members**
  - Mr. Dave Schulte
  - Mr. Ed Kratovil
  - Mr. Jim Gerber
  - Ms. Rhonda Barnes
  - Mr. Danny Brunson
  - Mr. Josh McNeil
  - Mr. Bill Pottratz
  - Dr. Tom English
  - Mr. Steve Mattern
  - Mr. John Canning
  - Mr. Bob Schmedake

Workgroup Participants

Precepts:

Mr. Josh McNeil (Army)

- Mr. Woody Eischens (OSD)
- Mr. Clif Ericson (EG&G)
- Mr. Tom Garrett (Navy)
- Mr. Hui-min Huang (NIST)
- Mr. Bob Jacob (Navy)
- Mr. Mike Logan (NASA)
- Mr. Ranjit Mann (APT)
- Mr. Jack Marett (Westar)
- Mr. Charles Muniak (LMCO)
- Ms. Kristen Norris (AOT)
- Mr. Alan Owens (Air Force)
- Mr. Scott Rideout (USMC)
- Ms. Peggy Rogers (Navy)
- Mr. Craig Schilder (APS)
- Mr. Arthur Tucker (SAIC)
- Mr. Frank Zalegowski (Navy)
- Mr. Jim Zidzik (Navy)
- Mr. Don Zrebieck (Navy)

Weapons Control:

Mr. Bill Pottratz (Army)

- Mr. Scott Allred (USMC)
- Mr. Bill Blake (ATK)
- Dr. Craig Bredin (Westar)
- Ms. Mary Ellen Caro (Navy)
- Mr. John Deep (USAF)
- Mr. Jon Derickson (BAE)
- Mr. John Filo (Navy)
- Mr. Mark Handrop (USAF)
- Mr. Chris Janow (Army)
- LTCOL Emil Kabban (USAF)
- Mr. Dave Magidson (Army)
- Mr. Chris Olson (APT)
- Mr. Preston Parker (USAF)
- Mr. Jack Waller (Navy)
- Mr. Mike Zecca (Army)

Workgroup Participants

Situational Awareness:

Dr. Tom English (Navy)

- Dr. Julie Adams (Vanderbilt University)
- Ms. Alicia Adams-Craig (Army)
- Mr. Brad Cobb (Navy)
- Mr. Mike Demmick (Navy)
- Mr. Travis Hogan (GVI)
- Mr. Hui-Min Huang (NIST)
- Mr. Frank Marotta (Army)
- Mr. Aaron Mosher (Boeing)
- Mr. Mike Pessoney (APT)
- Mr. Owen Seely (Navy)
- Mr. Hoi Tong (Foster Miller)
- Mr. Bill Transue (EOD)
- Dr. Anthony Tvaryanas (USAF)
- Mr. Alan Weeks (iRobot)

Command and Control:

Mr. Steve Mattern (Apogen Technologies)

- Mr. Frank Albert (Navy)
- Mr. Billy Arnold (General Dynamics)
- Mr. John Canning (Navy)
- Mr. Steve Castelin (Navy
- Mr. Michael Dunn (Army)
- Ms. Rachael Fabyanic (Navy)
- Mr. Eugene Gonzales (Navy)
- Ms. Martha Meek (Army)
- Mr. Helmut Portmann (Navy)
- Mr. Ron Price (Army)
- Mr. Ed Spratt (Navy)
- Mr. Mike Zemore (Navy)

Workgroup Participants

States and Modes:

Mr. Bob Schmedake (Boeing)

- Mr. Mike Brown (EG&G)
- Mr. Danny Brunson (EG&G)
- Mr. Jim Butler (L3)
- Mr. Bill Edmonds (Army)
- Ms. Melissa Emery (APT)
- Mr. Bart Fay (Westar)
- Mr. Steve Hosner (Titan)
- Mr. Bob McAllister (USAF)
- Mr. Lynece Pfledderer (LMCO)
- Mr. Henry Zarzycki (Army)

Definitions/Common Taxonomy:

Mr. Danny Brunson (EG&G)

- Mr. Scottie Allred (USMC)
- Ms. Mary Ellen Caro (Navy)
- Mr. Bill Christian (APT)
- Mr. Brad Cobb (Navy)
- Mr. Clif Ericson (EG&G)
- Mr. Ranjit Mann (APT)
- Mr. Steve Mattern (Apogen Technologies)

Special Thanks
"Heavy Lifters"

- ✓ Mr. Jim Gerber
- ✓ Mr. Mike Demmick
- ✓ Mr. Josh McNeil
- ✓ Ms. Rhonda Barnes
- ✓ Mr. Danny Brunson

Predator

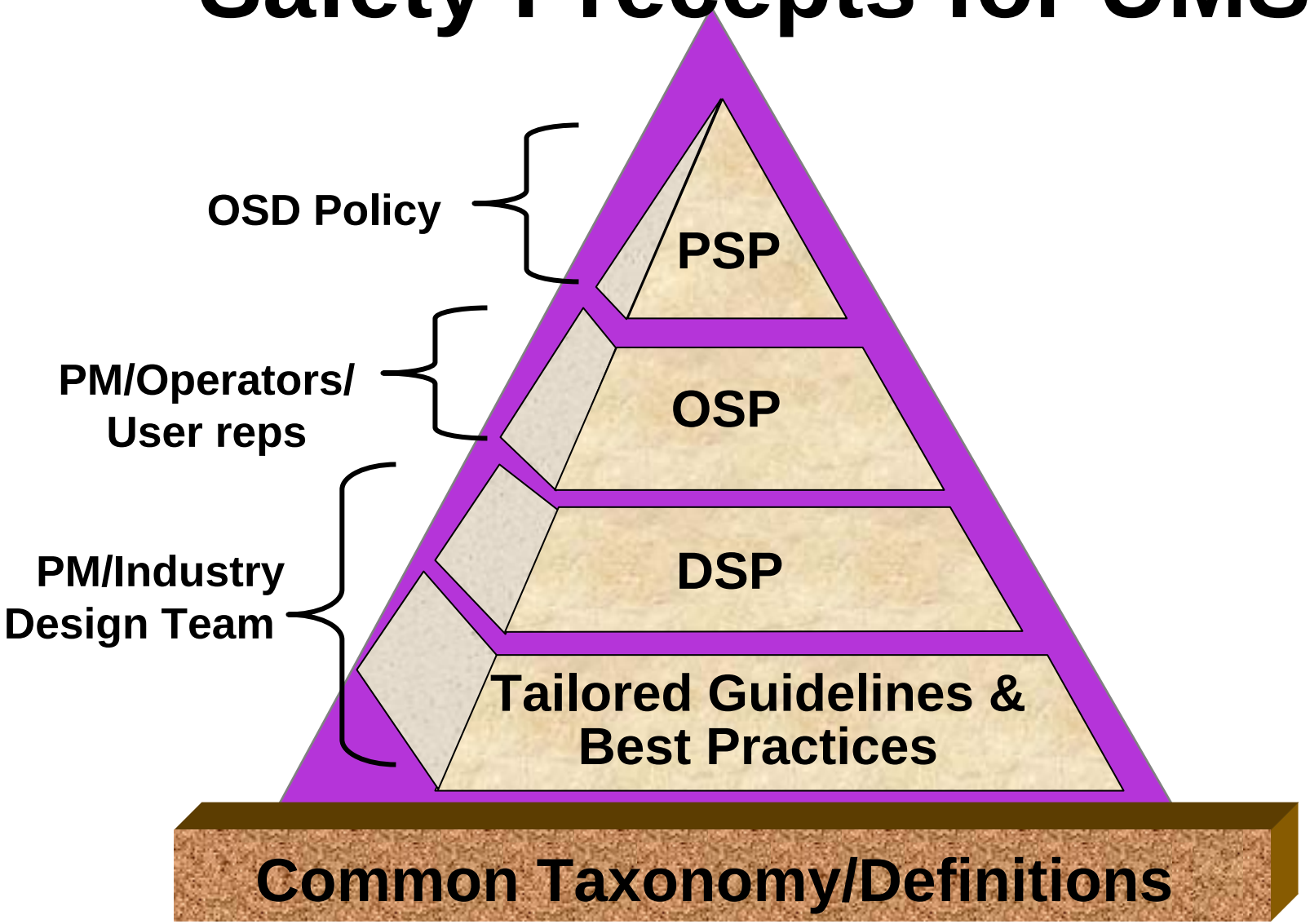
UMS Safety Precept Definitions

Programmatic Safety Precept (PSP) = **Program management principles & guidance that will help ensure safety is adequately addressed throughout the lifecycle process. (6)**

Operational Safety Precept (OSP) = **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. (5)**

Design Safety Precept (DSP) = **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. (19)**

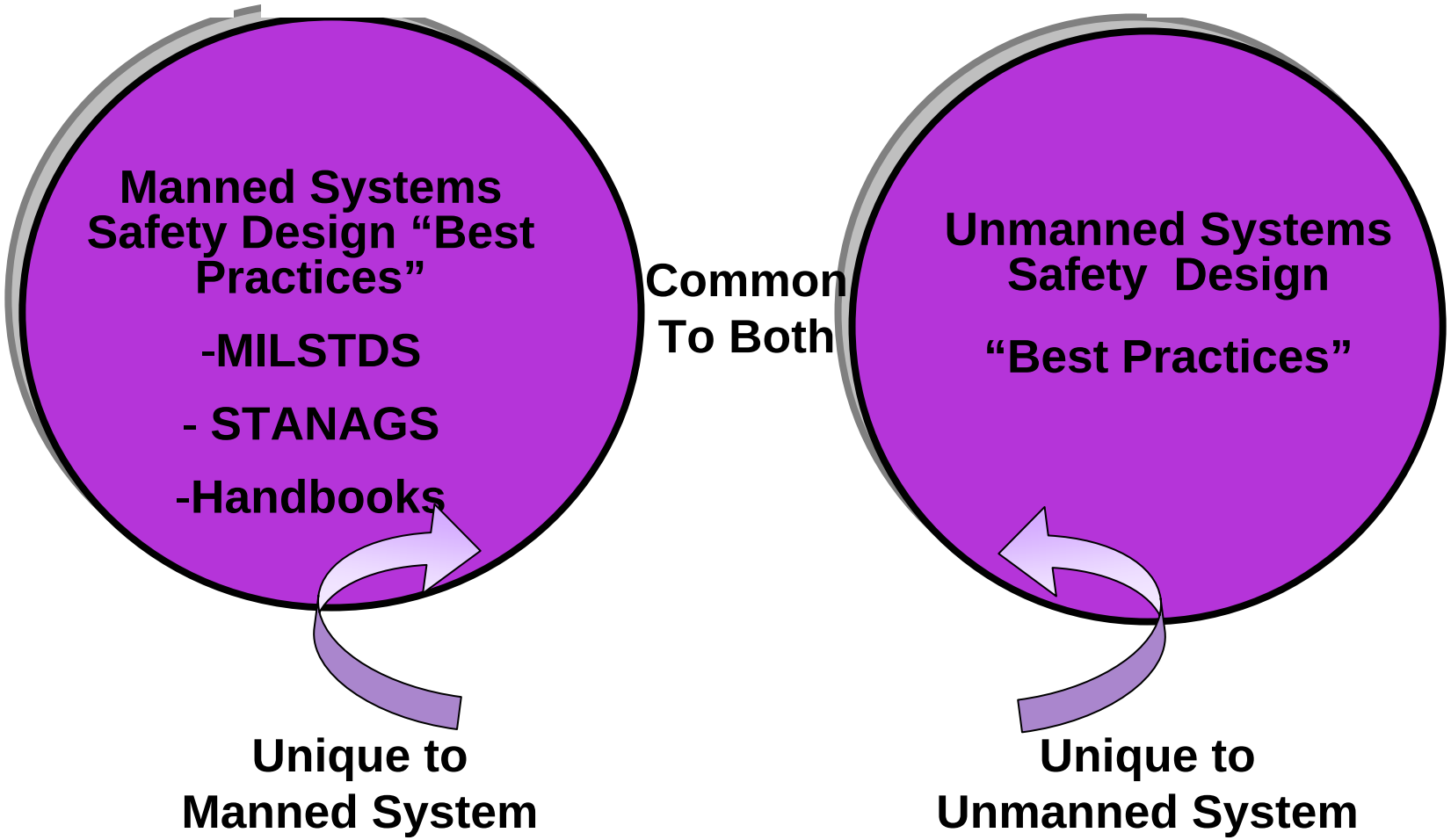
Safety Precepts for UMS



Provide PMs, designers, and systems safety managers with appropriate safety guidelines and best practices, while maintaining PM's flexibility

Safety Design Guidelines

Are we creating two sets of safety criteria:
one for manned systems, and one for unmanned systems??



Creating another set of safety requirements? No

Safety Precepts

- ✓ Did not previously exist
- ✓ Evolved through an arduous, but thorough, systems engineering process over the past 2 years
- ✓ Separate study was performed to determine if current DoD and/or Service-specific policies addressed each of the safety precepts

Safety Precepts (cont'd)

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.**
- ✓ **Four precepts (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.**

Final Product

UNMANNED SYSTEMS SAFETY GUIDE FOR DOD ACQUISITION

27 June 2007

- ✓ **Document contains descriptive and clarifying text for each precept.**
- ✓ **Includes definitions**
- ✓ **But,…comments/lessons learned are still requested for future updates**
  - **NOSSA Website (http://www.ih.navy.mil/unmannedsystems)**

USD (AT&L) UMS Memorandum

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

JUL 17 2007

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARY OF DEFENSE (NETWORKS & INFORMATION INTEGRATION)
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Unmanned Systems Safety Guidance

In March 2006, the Defense Safety Oversight Council Acquisition and Technology Programs Task Force (ATP TF) initiated a study to identify the unique safety challenges of unmanned systems (UMSs), especially those systems carrying and deploying weapons in a joint environment. These safety challenges significantly increase as more UMSs are fielded and used in the same warfighting environment.

Using a collaborative process with experienced personnel from all Services, the ATP TF developed the "Unmanned Systems Safety Guide for DoD Acquisition" to provide programmatic, operational, and design guidelines to support the development and fielding of safe UMSs. Please you use the Guide, found at http://www.acq.osd.mil/atptf/, to help identify and mitigate hazards and their associated risks for all UMS types.

For those UMSs that are ACAT 1D program, the UMS safety guidel[illegible] special interest item during OSD Program Support Reviews. UMS-specific guidelin[illegible] have been added to the Defense Acquisition Program Support methodology to guide the evaluation of how successfully programs have engineered UMSs to reduce safety risks to acceptable levels.

Kenneth J. Krieg

"… use the Guide to help identify and mitigate hazards and their associated risks for all UMS types."

"For those UMSs that are ACAT 1D Programs, the UMS safety guidelines will be a special interest item during OSD Program Support Reviews."

Table of Contents

Programmatic Safety Precepts

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, 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., 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.

Programmatic Safety Precepts
(Cont'd)

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

PSP-5: Compliance to and deviation from the safety precepts shall be addressed during all Milestone decisions and formal design 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.

Note: While the 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.

Operational Safety Precepts

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

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

OPS-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.

Design Safety Precepts

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(s).

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.

Design Safety Precepts
(Cont'd)

DSP-8*: The UMS shall be designed to provide for an authorized entity(s) 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.

Design Safety Precepts
(Cont'd)

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.

Precept Clarification Table

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.
Example: 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.

DSP-14 Loss of Command Link

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 perational 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.

DSP-14 Loss of Command Link (cont'd)

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.

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.

DSP-14 Loss of Command Link (cont'd)

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.

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.**

DSP-14 Loss of Command Link (cont'd)

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.

Detailed Considerations: (cont'd)

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.**

DSP-14 Loss of Command Link (cont'd)

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.

Existing Policy:

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

Need your help in identifying any other existing policy documents

Protector Unmanned Surface Vehicle

Summary

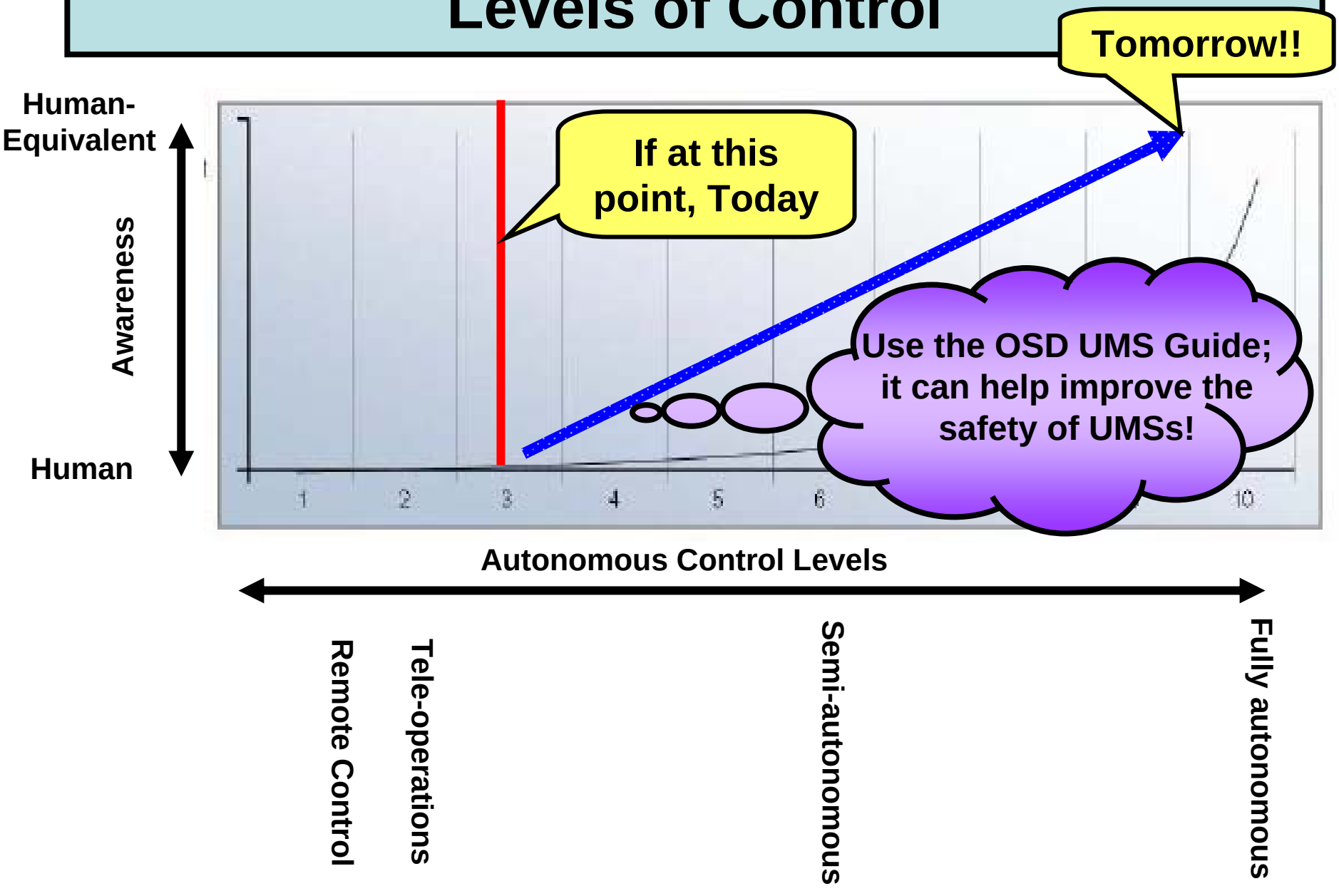
- ✓ **Held three workshops (March, May, June 2006)**
- ✓ **Government/industry/academia teams developed draft safety precepts, rationale & design guidance**
  - ➢ **All Services and numerous UMS program office reps participating**
- ✓ **Briefed**
  - ➢ **International Systems Safety Conference (2005, 2006 and 2007)**
  - ➢ **AUVSI (August 2006)**
  - ➢ **NDIA Systems Engineering (October 2006 and 2007)**
- ✓ **Comments Requested**
  - ➢ **NOSSA Website (http://www.ih.navy.mil/unmannedsystems)**

Summary (cont'd)

USD (AT&L) Memorandum of 17 July 2007

- ✓ **Forwarded the Guide to the Service Secretaries and other major DoD components as an enclosure to a memo strongly endorsing the use of the Guide for all UMS acquisitions.**
- ✓ **The Undersecretary directed that the UMS Safety precepts in the Guide be a special interest item for ACAT 1D Program Support Reviews.**
- ✓ **The Guide has been posted on the OSD ATP-TF Website at http://www.acq.osd.mil/atptf/**
- ✓ **Next steps:**
  - ➢ **Convert the Guide to a MIL-HDBK**
    - **Handbook is for guidance**
    - **Service ownership**
    - **Facilitate periodic updates**
    - **Formatting completed September 2007**
    - **Final Handbook completion 3rd Qtr 2008**
  - ➢ **Update Policy and Service Directives to address UMS Precepts, where appropriate. (Remember, 12 Safety Precepts not addressed at all in policy.)**

UMS Level of Awareness vs. Levels of Control



Navy WSESRB Command Vehicle

Safety of Unmanned Systems

Sponsored by
DSOC ATP TF

Questions and Comments