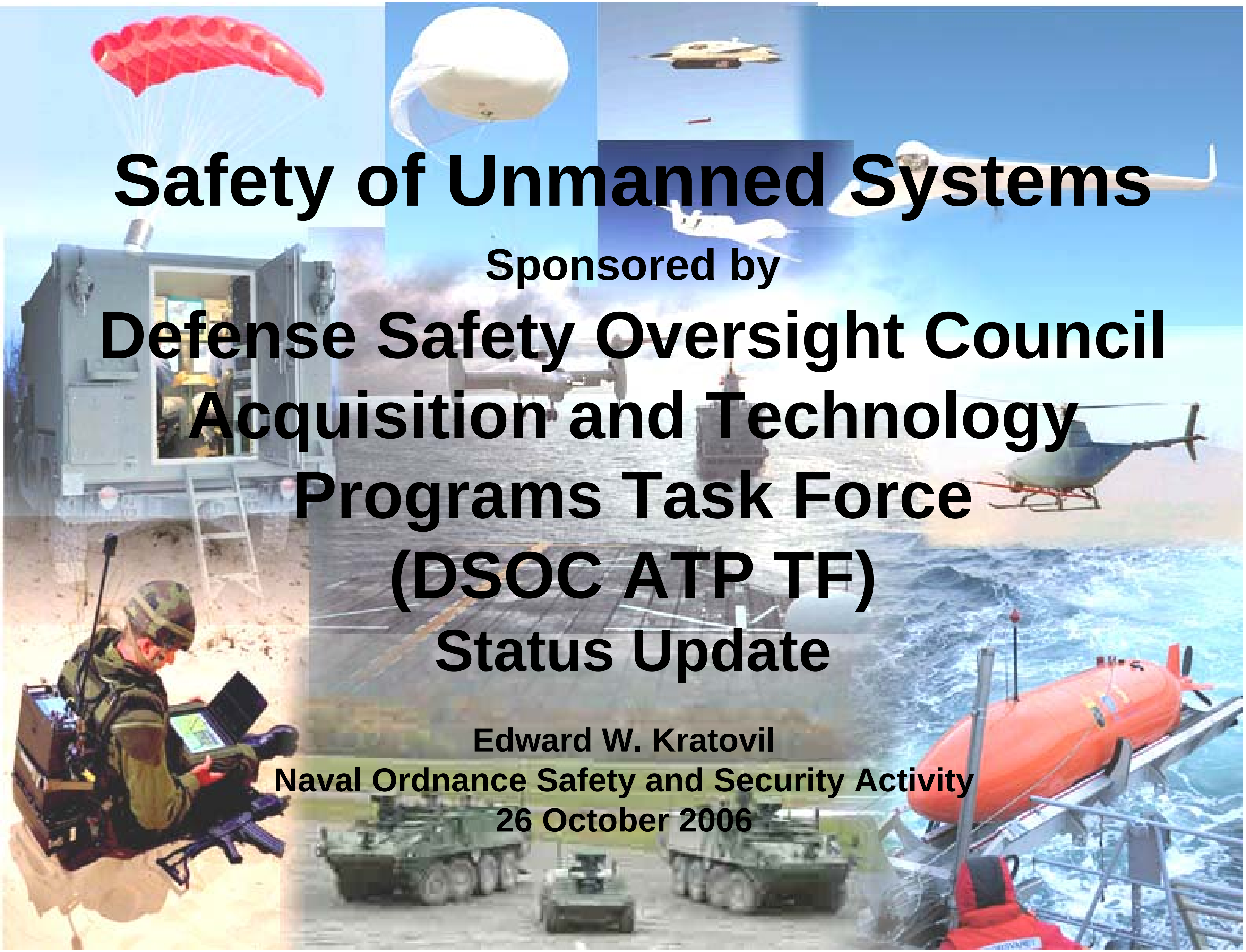


Safety of Unmanned Systems

Sponsored by

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

Status Update

Edward W. Kratovil
Naval Ordnance Safety and Security Activity

26 October 2006

Panel Members

Mr. Danny Brunson
EG&G Services, Inc.
Dahlgren, VA

Ms. Rhonda Barnes
APT Research, Inc.
Huntsville, AL

Agenda

- Background
- Objectives
- Approach
- Progress
- Leadership
- Organization
- Workgroup participants
- Precepts Review
- Product
- Precepts; detailed discussion
- Summary

Background

- In FY05 Joint Robotics Program Coordinator tasked Navy to:
  - Provide Unifying Safety Guidance Across All Robotic Projects
  - Establish Initial Safety Precepts for Robotic Systems
    - Program Safety Guidance
    - Operational Guidance
    - System Design Safety Guidance
- Results briefed at 2005 ISSC

Background

- OSD (DSOC ATP TF) directed expansion of effort to include all Unmanned Systems
- Emphasized necessity of community input
  - Program Management
  - Design
  - Test
  - Operational
  - Safety
- Emphasized guidance vice direction

UMS Safety Objectives

- Focus the technical community on the System Safety needs for UMS
- Specifically
  - 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.
  - Establish and agree upon a standardized set of safety precepts to guide the design, operation, and programmatic oversight of all unmanned systems.
  - 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 60 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

✓ISSC (31 July - 4 Aug 2006)
✓AUVSI (29 – 31 Aug 2006)
✓NDIA Systems Engineering (23 – 26 Oct 2006)

Progress

- Held Three Workshops
  - March 2006, Huntsville
  - May 2006, Crystal City
  - June 2006, Crystal City
- Developed Draft Safety Precepts
  - Programmatic safety precepts
  - Operational safety precepts
  - Design safety precepts
- Developing design safety “best practices”

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

Unmanned Systems Leadership (Cont'd)

- Others
  - 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

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

Workgroup Participants

Precepts:

Mr. Josh McNeil (Army)

- 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)
- Mr. Woody Eischens (OSD)

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)

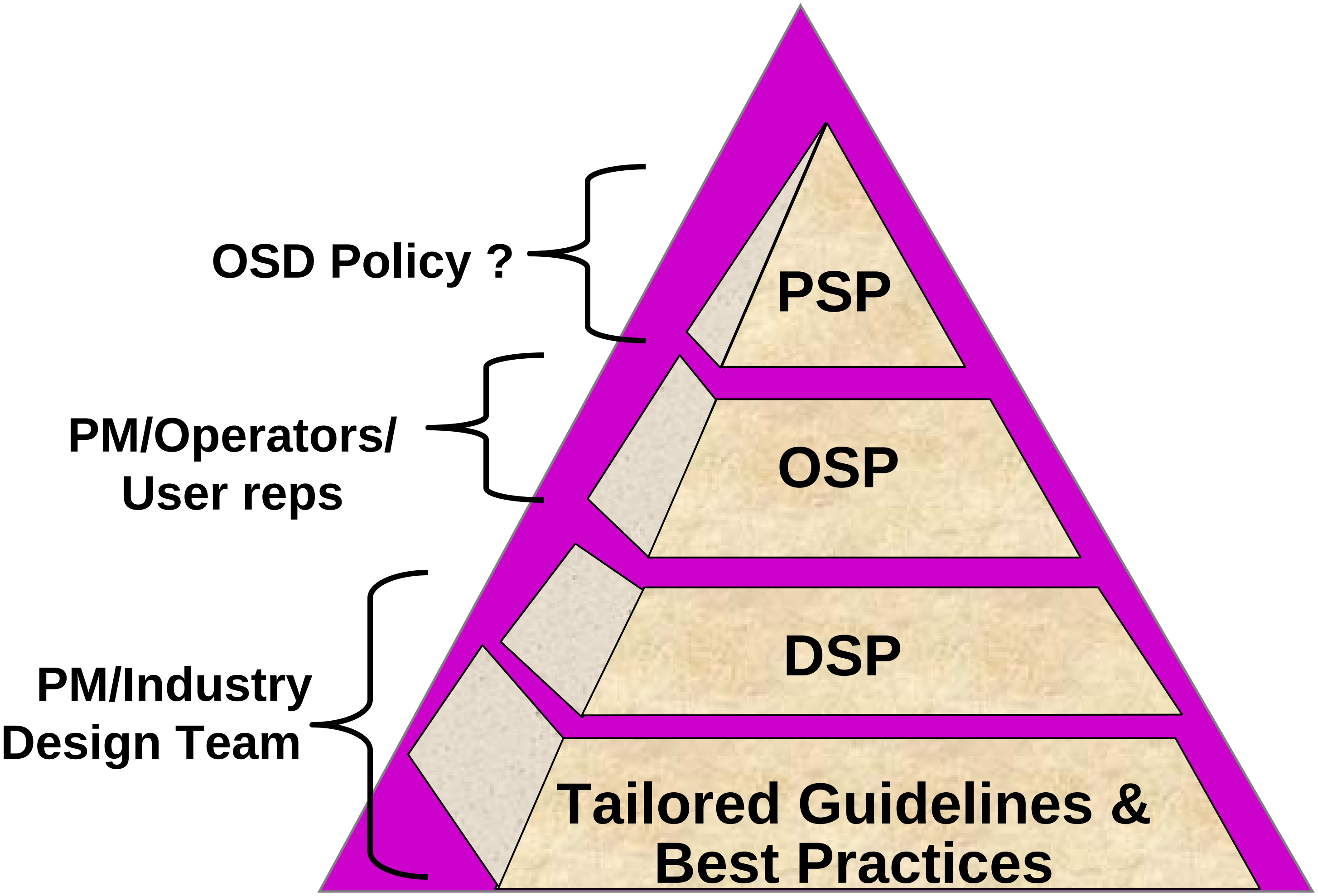
UMS Safety Precept Definitions

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

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 DSPs.

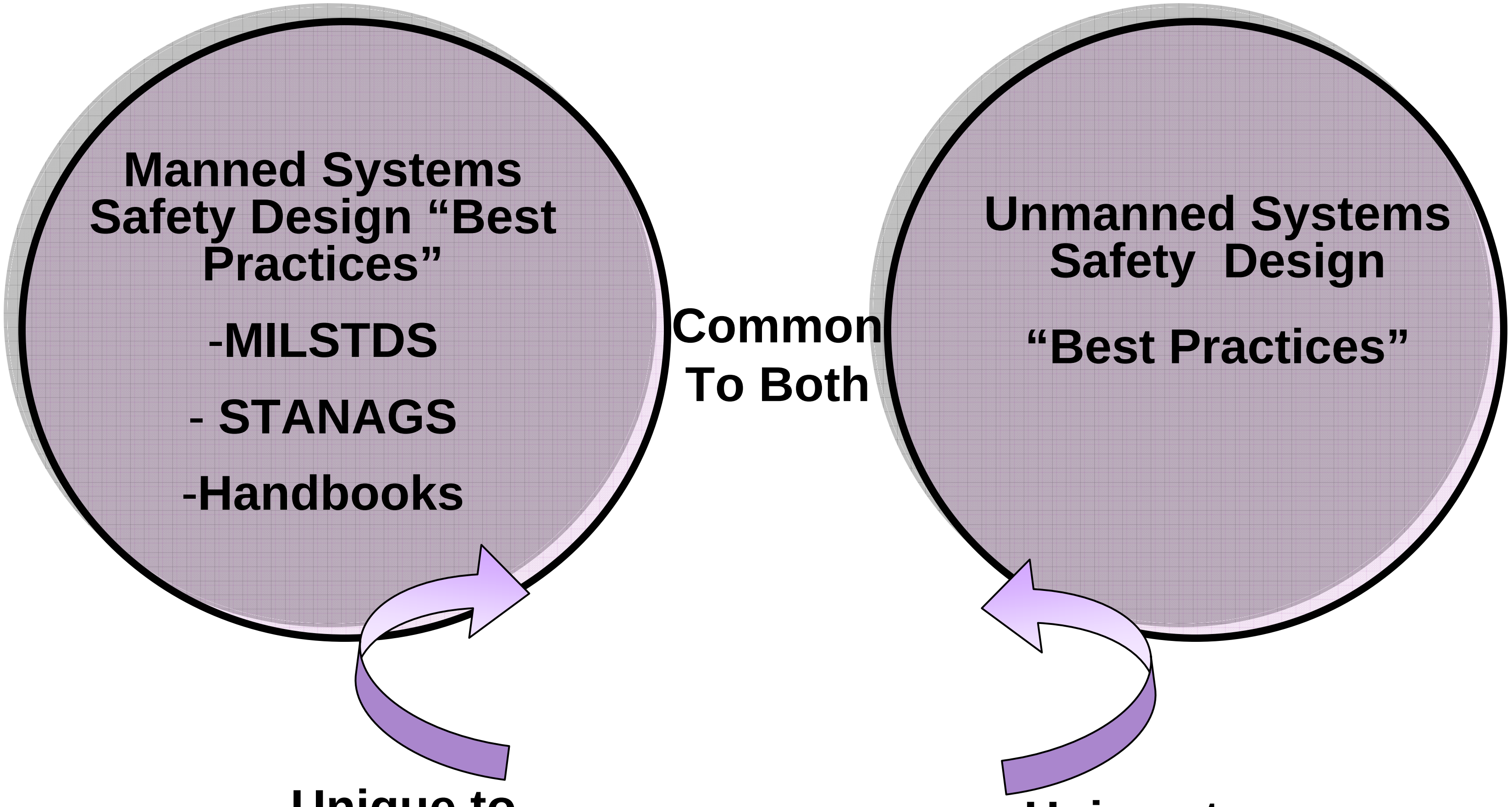
Design Safety Precept (DSP) = General design guidance intended to facilitate safety of the system and minimize hazards. Safety design precepts are intended to influence, but not dictate, specific design solutions.

Safety Precepts for UMS



Provide program managers, designers, and systems safety managers with appropriate safety guidelines and best practices, <u>while maintaining PM's flexibility</u>

Safety Design Guidelines



Manned Systems Safety Design "Best Practices"

-MILSTDS

- STANAGS

-Handbooks

Common To Both

Unmanned Systems Safety Design

"Best Practices"

Unique to Manned System

Unique to Unmanned System

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 statutory 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.

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 formal design reviews to include SRR, PDR, and CDR.**

PSP-6: **The Program Office shall ensure that munitions/weapons/suspension and release equipment shall be designed to comply with current design safety and performance criteria.**

Operational Safety Precepts

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

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

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

OSP-4: The unmanned system weapons should be loaded/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 unmanned system.

Design Safety Precepts

DSP-1: The unmanned system shall provide safety design features to minimize the mishap risk during all life cycles phases.

DSP-2: The unmanned system shall be designed to only respond to fulfill valid commands from the authorized entity(s).

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

DSP-4: The unmanned system shall be designed to isolate power until as late in the operational sequence as practical from: a): Weapons b): Rocket motor initiation circuits c): Bomb release racks.

DSP-5: The unmanned system shall be designed to prevent release/firing of weapons into unmanned system structure or other weapons.

DSP-6: The unmanned system shall be designed to prevent uncommanded fire/release of weapons or propagation/radiation of hazardous energy.

DSP-7: The unmanned system shall be designed to prevent hazardous system mode combinations or transitions.

Design Safety Precepts
(Cont'd)

DSP-8: The unmanned system shall be designed to provide for an authorized entity(s) to abort a weapon fire sequence and return the system to a safe state.

DSP-9: The unmanned system shall be designed to safely change states and modes.

DSP-10: Safety critical software for the unmanned system design should not include unintended/non-required functionality.

DSP-11: The unmanned system should be designed to provide means to identify state and/or mode of the system to the authorized entity(s).

DSP-12: The system shall be designed to minimize single-point, common mode or common cause failures for high (catastrophic) and serious (critical) risks.

DSP-13: The unmanned system shall be designed to minimize the use of hazardous materials.

Design Safety Precepts

(Cont'd)

DSP-14: The unmanned system shall be designed to minimize exposure of personnel, ordnance, and equipment to hazards generated by the unmanned system equipment.

DSP-15: The unmanned system shall be designed to initialize/re-initialize in a known safe state.

DSP-16: The unmanned system shall be designed to identify to the authorized entity(s) the weapon being released/fired.

DSP-17: In the event of unexpected loss of command link, the unmanned system shall transition to a pre-determined and expected state and mode.

DSP-18: The launching/arm-enabling of weapon systems shall require a minimum of 2 independent and unique validated messages in the proper sequence from an authorized entity (e.g. messages shall not originate within a launcher platform), each of which shall be generated as a consequence of separate authorized entity action.

Design Safety Precepts

(Cont’d)

DSP-19: The unmanned system should be designed to support options for operational or emergency contingencies.

DSP-20: The unmanned systems shall provide safety design features to ensure safe recovery of all unmanned system equipment to include the platform and equipment.

DSP-21: The system should be designed to allow for safe and graceful degradation of the system upon system-level or sub-system-level failures.

DSP-22: 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.

DSP-23: The unmanned system design shall consider compatibility with the test range environment to ensure safety during test and evaluation.

DSP-24: The UMS shall be designed to safely operate within the combined and joint environments.

Precept Clarification Table

Hyperlinked 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.

Final Precept Product
(OSD Guide)

- Document containing descriptive and clarifying text for each precept.
- Contains hyperlinks to navigate within the document.
- Will include definitions
- Comments requested; draft OSD guide out for comment
  - Web site (http://www.ih.navy.mil/unmannedsystems)
  - Comment forms at back of room

Discussion on Each Precept

Mr. Danny Brunson
EG&G Services, Inc., Dahlgren VA

Discussion of Precepts

- Process for developing precepts
- Clarification of precepts
- Limited time for discussion and feedback, but…
  - – Web site (http://www.ih.navy.mil/unmannedsystems)
  - – Comment forms at back of room

Precept Workgroup Participants

Mr. Josh McNeil, Moderator (Army)

- 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)
- Mr. Woody Eischens (OSD)

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 statutory 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.
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 formal design reviews to include SRR, PDR, and CDR.
PSP-6	The Program Office shall ensure that munitions/weapons/suspension and release equipment shall be designed to comply with current design safety and performance criteria.

Operational Safety Precepts

OSP-1	The controlling entity(ies) of the unmanned system should have pertinent mission information to support safe operations.
OSP-2	The unmanned system shall be considered unsafe until a safe state can be verified.
OSP-3	The authorized entity(ies) of the unmanned system shall verify the state of the UMS, to ensure a safe state prior to performing any operations or tasks.
OSP-4	The unmanned system weapons should be loaded/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 unmanned system.

Design Safety Precepts

DSP-1	The unmanned system shall provide safety design features to minimize the mishap risk during all life cycles phases.
DSP-2	The unmanned system shall be designed to only respond to fulfill valid commands from the authorized entity(s).
DSP-3	The unmanned system shall be designed to provide information, intelligence, and method of control (I2C) to support safe operations.
DSP-4	The unmanned system shall be designed to isolate power until as late in the operational sequence as practical from: a): Weapons b): Rocket motor initiation circuits c): Bomb release racks.
DSP-5	The unmanned system shall be designed to prevent release/firing of weapons into unmanned system structure or other weapons.
DSP-6	The unmanned system shall be designed to prevent uncommanded fire/release of weapons or propagation/radiation of hazardous energy.
DSP-7	The unmanned system shall be designed to prevent hazardous system mode combinations or transitions.

Design Safety Precepts

DSP-8	The unmanned system shall be designed to provide for an authorized entity(s) to abort a weapon fire sequence and return the system to a safe state.
DSP-9	The unmanned system shall be designed to safely change states and modes.
DSP-10	Safety critical software for the unmanned system design should not include unintended/non-required functionality.
DSP-11	The unmanned system should be designed to provide means to identify state and/or mode of the system to the authorized entity(s).
DSP-12	The system shall be designed to minimize single-point, common mode or common cause failures for high (catastrophic) and serious (critical) risks.
DSP-13	The unmanned system shall be designed to minimize the use of hazardous materials.
DSP-14	The unmanned system shall be designed to minimize exposure of personnel, ordnance, and equipment to hazards generated by the unmanned system equipment.

Design Safety Precepts

DSP-15	The unmanned system shall be designed to initialize/re-initialize in a known safe state.
DSP-16	The unmanned system shall be designed to identify to the authorized entity(s) the weapon being released/fired.
DSP-17	In the event of unexpected loss of command link, the unmanned system shall transition to a pre-determined and expected state and mode.
DSP-18	The launching/arm-enabling of weapon systems shall require a minimum of 2 independent and unique validated messages in the proper sequence from an authorized entity (e.g. messages shall not originate within a launcher platform), each of which shall be generated as a consequence of separate authorized entity action.
DSP-19	The unmanned system should be designed to support options for operational or emergency contingencies.

Design Safety Precepts

DSP-20	The unmanned systems shall provide safety design features to ensure safe recovery of all unmanned system equipment to include the platform and equipment.
DSP-21	The system should be designed to allow for safe and graceful degradation of the system upon system-level or sub-system-level failures.
DSP-22	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.
DSP-23	The unmanned system design shall consider compatibility with the test range environment to ensure safety during test and evaluation.
DSP-24	The UMS shall be designed to safely operate within combined and joint environment.

Precept Clarification Table

Hyperlinked 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.

PSP-2 Safety Precepts

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 statutory safety regulations, laws, and requirements are met .

Scope: This precept applies to all programs, not unique to unmanned systems. This precept emphasizes the need for a Risk Assessment process and is intended to require program offices to establish safety precepts early in their development process and addresses some basic issues with UMS Safety. This precept 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.). Compliance to or deviation from these precepts is addressed in PSP-5.

Rationale: Supports DoD 5000

An unmanned system design, development, test, operations, maintenance, support and decommissioning program will have an adequately funded system safety program in accordance with DOD 5000.2 and Mil-Std 882 criteria.

PSP-2 Safety Precepts cont’d

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 statutory safety regulations, laws, and requirements are met .

Example:

Detailed Considerations: The UMS Program planning documentation should consider incorporating programmatic and design requirements from the applicable Military standards and Industry best practices as appropriate (e.g. standards for EMI, HERO, weapon systems, software development, test planning, etc.)

Industry best practices should be tailored as appropriate for ACAT level

To ensure the Human system interface is designed appropriately and that all the necessary “I2C” data requirements are considered in the UMS design a Human System Integration analysis and an I2C analysis should be integrated with the SSP.

PSP-5 Safety Precepts

PSP-5 Compliance to and deviation from the safety precepts shall be addressed during all formal design reviews to include 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 should be addressed at the program major design reviews.

Rationale: This is a requirement for all UMS programs to incorporate the necessary UMS safety requirements in program documentation and ensure the appropriate program planning (i.e. cost and schedule) for each life cycle phase.

PSP-5 Safety Precepts cont’d

PSP-5 Compliance to and deviation from the safety precepts shall be addressed during all formal design reviews to include SRR, PDR, and CDR.

Example:

Detailed Considerations:

The UMS Program Office should document compliance for each precept and incorporate this evidence into a Safety Assessment Report (SAR) IAW MIL-STD-882 which is presented at each design review.

The UMS Program Office should develop detailed rationale for deviation from any precept and present this evidence at each design review.

DSP-17 Loss of Comm cont’d

DSP-17 In the event of unexpected loss of command link, the unmanned system shall transition to a pre-determined and expected state and mode.

Scope: This precept addresses unexpected loss of communications link (i.e. loss of data link, loss of remote command and control) and not the intended communication loss as in the case of underwater vehicles or other fully autonomous UMS. This precept must consider the level of control authority (i.e. tele-op, semi-autonomous, fully autonomous, etc.). This precept might not apply for fully autonomous systems, because there is no communication with the UMS. This precept addresses vehicle movement or weapon hazards in the event command link is lost.

Rationale: This precept addresses loss of the communications link which may lead to unintended or inadvertent motion or weapon action resulting in injury, death, system damage, or environmental damage. To prevent transition to or remaining in an unsafe mode, sub-mode, state or combination thereof and ensure the system transitions to a safe mode, sub-mode, state or combination. Also supports out of sequence commands and "race" commands. Unmanned vehicle design shall include capabilities for end game scenarios as appropriate for the unmanned vehicle system

DSP-17 Loss of Comm cont’d

DSP-17 In the event of unexpected loss of command link, the unmanned system shall transition to a pre-determined and expected state and mode.

Example:

Operator perception and thus information processing would be improved if the operator could anticipate the unmanned vehicle status or state during the loss-link for all systems and sub-systems.

The concern is that we might send a priority "cease fire" message that is received prior to the "fire message". In that case it could think it has been given a new fire message.

The system performs pre-planned operation upon loss of link (e.g. ground vehicle retrogress).

DSP-17 Loss of Comm cont’d

DSP-17 In the event of unexpected loss of command link, the unmanned system shall transition to a pre-determined and expected state and mode.

Detailed Considerations:

- The UMS design team should define the state and mode the UMS should transition to, if loss of or intermittent command and control is experienced.
- The UMS design team should define the “desired/predictable course of action” and its criteria, if loss of or intermittent command and control is experienced.
- The “pre-determined and expected state and mode” and the “desired/predictable course of action” and its criteria should be based on: the UMS CONOPS and application; the level of autonomy and level of control; the operating environment (i.e. training, test, underwater, airborne,…).
- Predefined COA is required when conducting operations & test.
- The UMS design should consider retention of pertinent mission information (such as last known state/configuration, etc.) for the UMS and the controlling entity(ies) to recover from the loss of comm. Link.

DSP-17 Loss of Comm cont’d

DSP-17 In the event of unexpected loss of command link, the unmanned system shall transition to a pre-determined and expected state and mode.

Detailed Considerations:

- The unmanned system shall ensure command messages are prioritized and processed in the correct sequence and in the intended state/mode.
- The reconfiguration capability, when implemented, shall ensure that the UMS remains in a safe state for the operational mode.
- Priority message processing shall ensure that the UMS cannot transition to or remain in an unsafe mode, sub-mode, state or combination thereof.
- Ensure that the system transitions to a safe mode, sub-mode, state or combination thereof in a timely manner.
- The design team should consider specific safety measures for the test environment to test and verify state mode transitions to safe states.
- The UMS shall incorporate features that determine the longest time that undelivered messages can exist within the communication system.
- The UMS design should include robustness for intermittent communications.

Summary

- Held three workshops
- Government/industry/academia teams developed draft safety precepts, rationale & design guidance
  - All Services and numerous program reps participating
- Briefed
  - International Systems Safety Conference
  - AUVSI
  - NDIA Systems Engineering
- Comments Requested
  - **Web Page (http://www.ih.navy.mil/unmannedsystems)**
  - **Comment forms back of room**
- Draft OSD Guidance developed 30 September 2006
- OSD issued draft guidance for review and comment
- Thank you for your participation and comments

Safety of Unmanned Systems

Sponsored by
DSOC ATP TF

Questions and Comments