Advancing System Safety Precepts for Unmanned Systems

Design Guidance Development

2015 NDIA Brief

M. H. Demmick
NOSSA, N314
Michael.demmick@navy.mil
Abstract # 18062

Michael H. Demmick
(301) 744-4932
Naval Ordnance Safety and Security Activity (NOSSA)
Michael.demmick@navy.mil

Abstract # 18062, Advancing System Safety Precepts for Unmanned Systems

Agenda

- Background
- Precepts
- Precepts Gap Assessment
- Next Steps

Background

Development of UMS Precepts

- Circa 2003, OUSD/AT&L directed development of:
  - Unifying Safety Guidance Across All Robotics Projects
  - Establish Initial Safety Precepts for Robotic Systems
    - Program Safety Guidance
    - Design Safety Guidance
    - Test Safety Guidance
    - Operational Guidance
    - System Design Safety Guidance

Initial UMS Precepts Development Workshop

- 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

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 mitigations, for the design, development, and acquisition of unmanned systems.
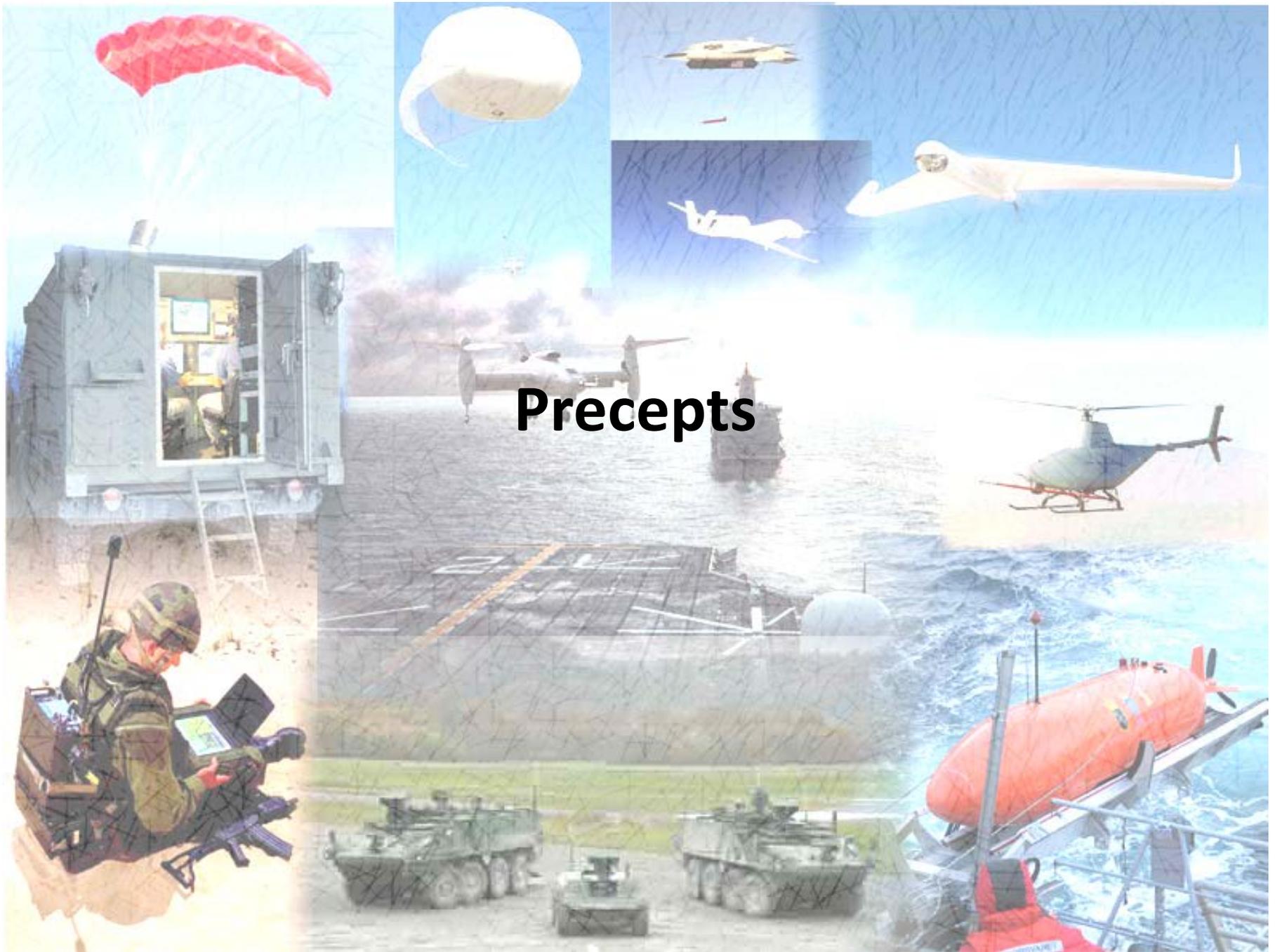
Precepts
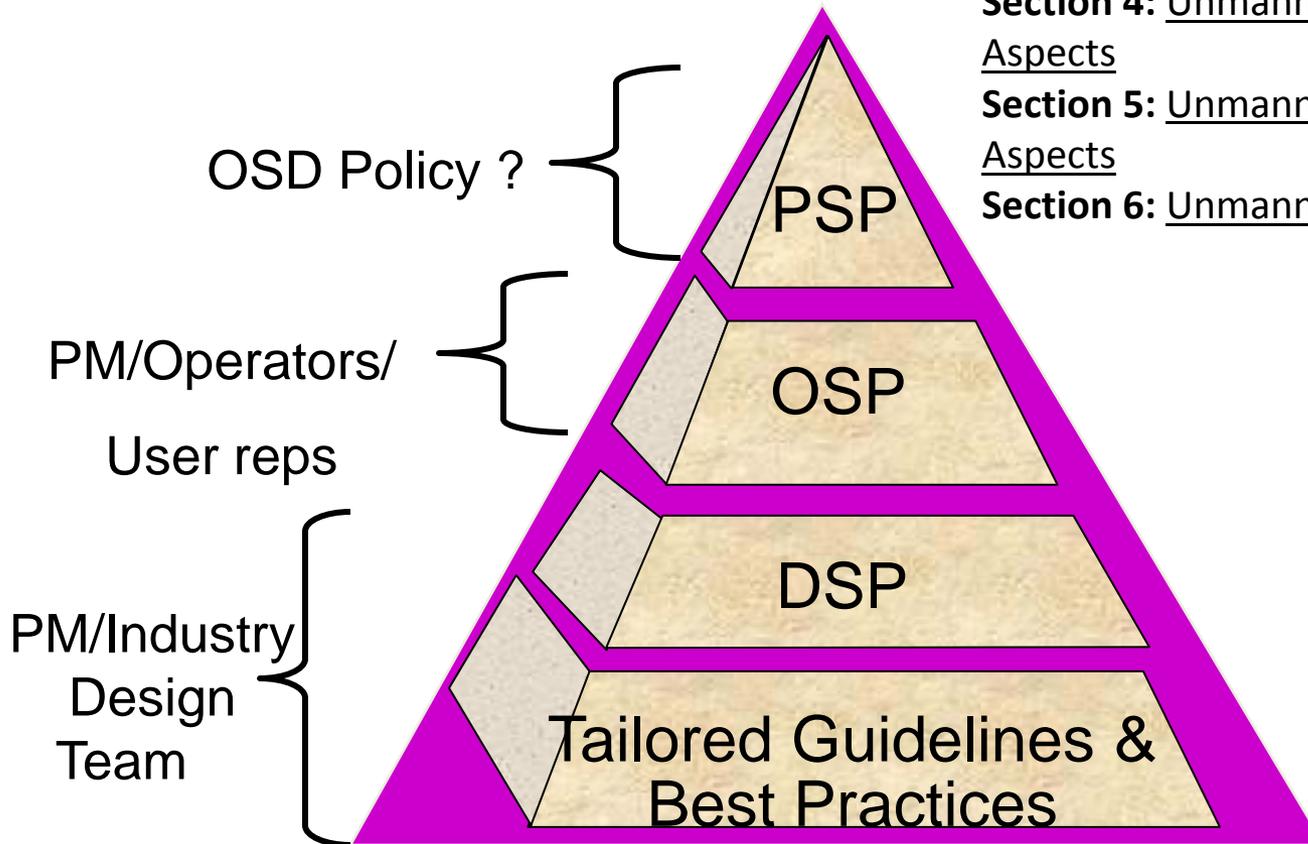
What is a UMS Safety Precept?

Programmatic Safety Precept (PSP) = Program management principles & guidance that will help insure 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.

**On-Going
GAP Assessment**

Inputs

Existing UMS Safety Guidance Document
- Dated 2007.
- Applies to UMS with and without autonomy.
- Enumerates 3 types of safety precepts:
    - Programmatic
    - Operational
    - Design

Drivers for UMS Safety Update
- Technical progress on autonomy (ongoing)
- DoD directive 3000.09 (2012).
- International discussion re LAWS and autonomy.
- DSB report on autonomy (2012).

Project

Ongoing UMS Safety Guidance Update Effort
- OSD funded via NOSSA
- Navy, Army, Air Force participation
- Identifying gaps in UMS safety guidance
- Providing preliminary solutions to some gaps

Report Outputs

Prioritized Guidance Gaps
- Process of gap identification.
- Critical, Substantial and Administrative Gaps.
- Rationale for each critical gap.
- Suggested precepts to fill some gaps.

External Factors, Constraints and Issues
Identification and discussion of other activities whose ongoing efforts may affect or be affected by update of the UMS Safety Guidance Document.

Other Output

Path Forward
Schedule, Milestones, Cost to Update the UMS Safety Guidance Document

Critical Gaps

Gap #	Critical Gap Name	Rationale for Critical Gap, and Gap Description (The Gap)	Impact on UMS Safety Document
1.	Diverging & Missing Definitions	Rationale: Ensure that safety guidance is interpreted and applied in a manner consistent with the intent of DoD directives and policy and mindful of international influences and potential backlash***. The Gap: The 2007 UMS Safety Guidance definition of "UMS" diverges from policy. Definitions are missing for: "autonomous system", "semi-autonomous system", "autonomous function", "cognitive autonomy", "LAWS", "LARS", "Human Control", "Human Judgment". (Based on preliminary research.)	Rewrite Section 1 with best available definitions.
2.	Authorized Entity Controls	Rationale: Ensure that unmanned systems include human judgment that is appropriate and meaningful, per DoD directive and U.N discussions and in accord with safety precepts. The Gap: Current guidance allows for any function to be taken over by autonomous systems. There is no guidance ensuring human in the loop at any level.	Changes throughout guide; New SPs, PSPs, OSPs, and possibly DSPs.

3.	Flexible Autonomy*	Rationale: Flexible autonomy*, per multiple recent analyses, has benefits. Safety has a potential role:
		    a. Facilitate dynamic system adaptation to evolving technologies, countering adversary's capabilities or threats, and Operational demands on autonomous systems by enabling safe, rapid insertion of autonomous functions, as well as use of autonomous functions [related to safety].
		    b. Enable continued safe and legal use of systems as policies regarding autonomy evolve.
		The Gap: Lack of safety guidance regarding design and implementation of flexible autonomy architectures.
			-Changes throughout guide; New DSP and perhaps OSP.
			-Addressing this Gap will facilitate contributions to Gaps 2, 4, and 5.

Critical Gaps

Gap #	Critical Gap Name	Rationale for Critical Gap, and Gap Description (The Gap)	Impact on UMS Safety Document
4.	Fail Safe Autonomy**	Rationale: Detection and safe response to anomalies is important to safe system use. Operators inherently perform this function; "fail safe autonomy" would require the autonomous systems to perform this anomaly detection function and the response. The Gap: Insufficient precepts addressing autonomy or autonomous systems detecting and responding to anomalies. Example hazards and responses include: a. Safe operation during compromised data or Microprocessor integrity events b. Safe operation when cyber fails to stop insider or enemy hack c. Autonomous system usurping by-design predetermined and intended functions or human control. d. Safe corrective reaction by autonomous system when its initial response fails to address the anomaly ****	New hazards, OSP(s) and DSP(s).
5.	Autonomous Function V&V***	Rationale: Per Defense Science Board (2012), "The DoD T&E workforce must be enhanced with new skills for robotics, artificial intelligence, networking and systems engineering for autonomous systems". The Gap: Lack of engineering guidance or discussion regarding V&V methods and techniques beyond existing software safety engineering levels of rigor.	-New guide section; New DSP, OSP, and edits -Relationship to Gap #2.
6.	Artificial Intelligence (AI)***	Rationale: Consider new precept[s] that address the use of AI in system decision making***; presently UMS precepts focus on Software based logical transitions that are pre-programmed and pre-determined to occur with pre-determined sequencing. AI would potentially impose unpredictability into the equation. The Gap: Lack of engineering guidance regarding safety analysis of AI level software or functions.	This Gap may have an effect on Gaps #2 – 5, i.e. precepts for Gaps #2 – 5 could be developed to address AI.

* Source of Critical Gap Name: Air Force doc "Autonomous Horizons" (June 2015), similar concepts also in DSB Report (2012) and DSB Summer Study (2015)
** See Airworthiness Certification Criteria Handbook MIL-HDBK-516c (Dec 2014) for further discussion regarding such hazards.
***Defense Science Board Task Force Report, "The Role of Autonomy in DoD Systems" (July 2012).
**** E.g. TCAS related Überlingen mid-air collision where both craft chose (via different mechanisms) to descend to avoid collision, and hence collided.

External Factors, Constraints, Issues, & Activities

- NATO MCDC (multi-national capabilities development campaign)

- G48 System Safety Committee

- Autonomous functions V&V development S&T

Policy & Papers

- Comprehensive Policy review planned for Phase II
  - Some of the references and policy papers considered or planned:
    - NATO STANDARD AEP-80, Rotary wing unmanned aerial systems airworthiness requirements
    - NAVAIRINST 13034.1E, Flight clearance policy for air vehicles and aircraft systems
    - DoDD 3000.09, Autonomy in Weapon Systems
    - Defense Science Board Study on Autonomy, August 2015
    - MIL-HDBK-516B, Airworthiness Certification Criteria

Next Steps

Path forward

- Phase II - Begin Developing Precepts to address GAPs
- Review original UMS Precepts Participants list
  - 75 + active participants
  - Draw expertise from all areas of professional community
  - Form a UMS System Safety Guidance IPT with broad participation
    - Seek Academia
    - Service Labs
    - FFRDC
    - UMS Operators
- Establish interfaces with pertinent Policy custodians
  - Provide consistent UMS guidance – ensure Policies are synchronized

Safety of Unmanned Systems

Questions and Comments