Advancing System Safety Precepts for Unmanned Systems

OSD Design Guidance Development

2016 NDIA Brief

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

Advancing System Safety Precepts for Unmanned Systems

Presenting for: Mr. Shad Reese, OUSD, AT&L, LW&M

Agenda

- Background
- Precepts
- Precepts Gap Assessment
- Next Steps


Background

Development of UxS 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 UxS Precepts Development Workshop

- Six Workgroups comprising ~ 80 SME's
  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

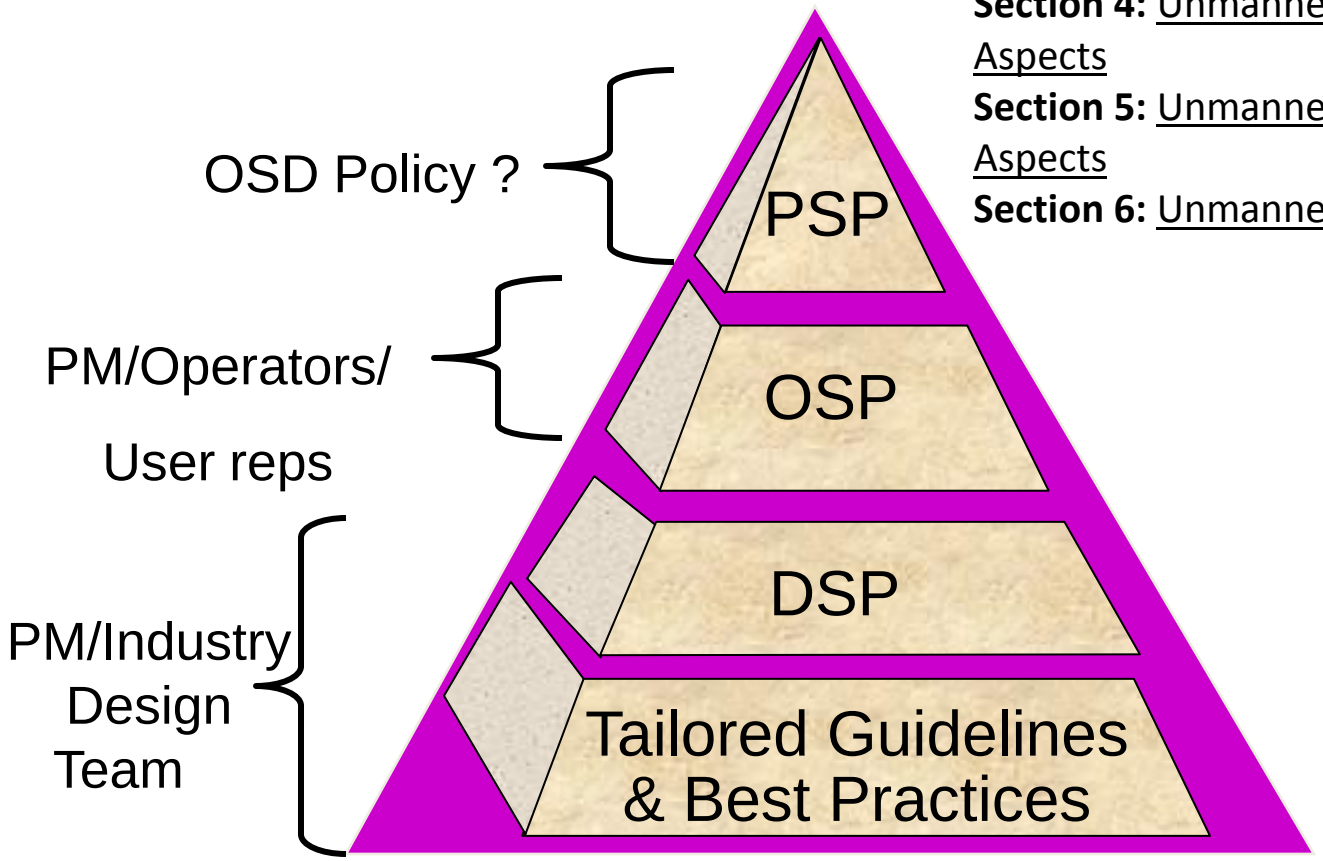
UxS Safety Objectives

- Focus the technical community on the System Safety needs for UxS
- 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

Safety Precepts for UxS

Section 1: Key Terms, Descriptions, and Principles
Section 2: System Safety Overview
Section 3: Unmanned System Safety Overview
Section 4: Unmanned System Safety Program Aspects
Section 5: Unmanned Systems Operational Aspects
Section 6: Unmanned Systems Design Aspects



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

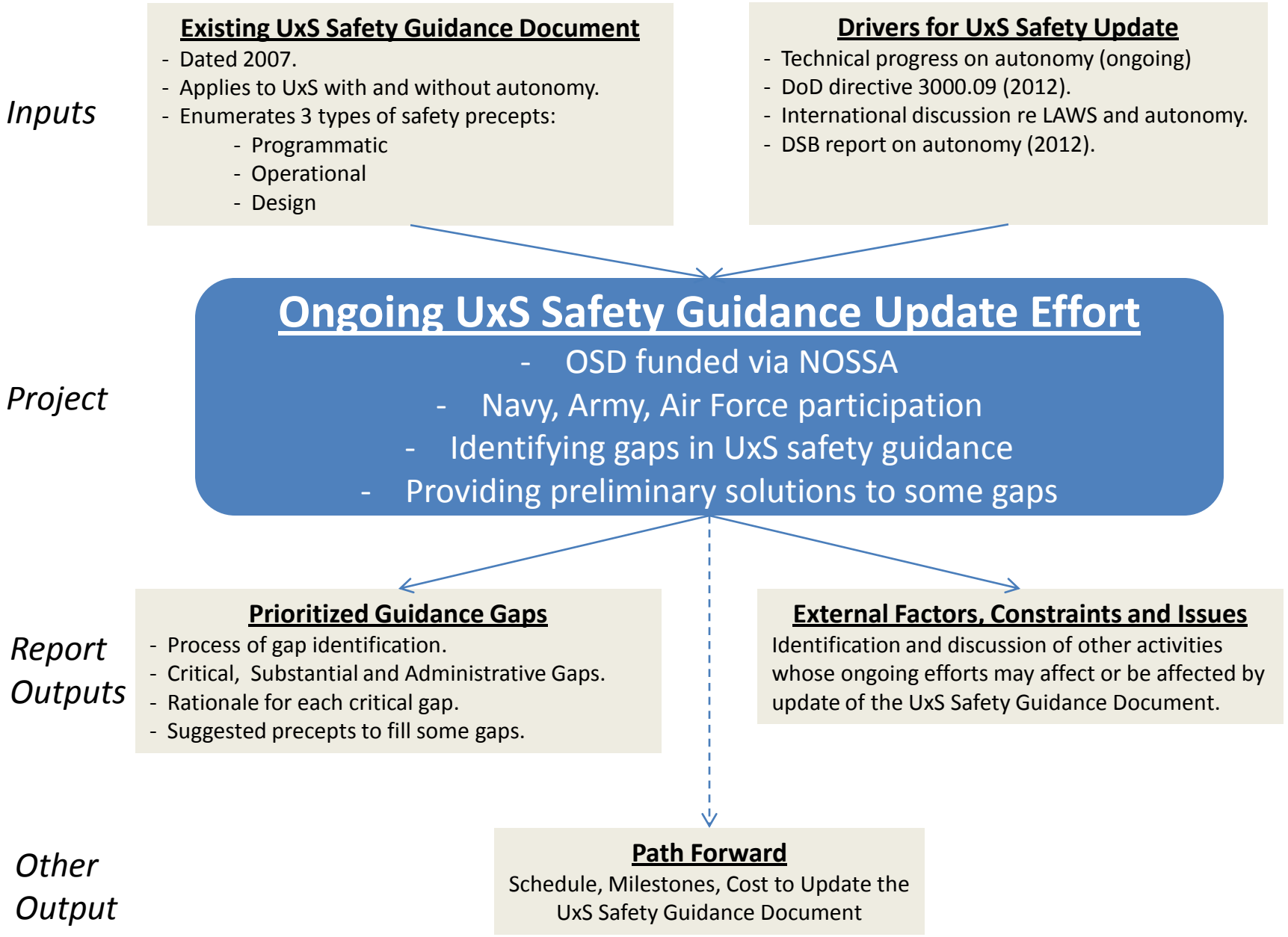
What is a UxS Safety Precept?

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 UxS Safety Guidance Document
- Dated 2007.
- Applies to UxS with and without autonomy.
- Enumerates 3 types of safety precepts:
  - Programmatic
  - Operational
  - Design
Drivers for UxS 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 UxS Safety Guidance Update Effort
- OSD funded via NOSSA
- Navy, Army, Air Force participation
- Identifying gaps in UxS 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 UxS Safety Guidance Document.
Other Output
Path Forward
Schedule, Milestones, Cost to Update the UxS 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	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.) 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***.	Obtain or develop definitions as appropriate & incorporate
2.	Authorized Entity Controls	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. 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.	New SPs, PSPs, OSPs, and possibly DSPs.
3.	Flexible Autonomy*	The Gap: Lack of safety guidance regarding design and implementation of flexible autonomy architectures. 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.	-New DSP and perhaps OSP. -Contributes 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**	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 **** 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.	New hazards, OSP(s) and DSP(s).
5.	Autonomous Function V&V***	The Gap: Lack of engineering guidance or discussion regarding V&V methods and techniques beyond existing software safety engineering levels of rigor. 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".	-New guide section; New DSP, OSP -Relationship to Gap #2.
6.	Artificial Intelligence (AI)***	The Gap: Lack of engineering guidance regarding safety analysis of AI level software or functions. 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.	Relationship to Gaps #2 – 5

* 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

- Update of the UxS safety guide will survey the community of SMEs and deign authorities
  - Collect and distill into one source, all pertinent technical progress; specifically, guidance pertinent to safety engineering of systems that use autonomy and/or AI
    - NATO MCDC (multi-national capabilities development campaign)
    - DoD / DOS technical direction
    - G48 System Safety Committee
    - Autonomous functions V&V development S&T

Policy & Papers

- Preliminary review of numerous policy and Studies conducted to identify and validate Gaps
- 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 UxS Precepts Participants list
  - 75 + active participants
  - Draw expertise from all areas of professional community
- Form a UxS IPT with broad participation
  - Seek Academia
  - Service Labs
  - FFRDC
  - UMS Operators
- Form UxS IPT technical expert Subgroups
  - Begin Developing Precepts to address GAP areas.
  - Develop expert recommendations and new precepts
- Establish interfaces with pertinent Policy custodians
  - Provide consistent UxS guidance – ensure Policies are synchronized

Safety of Unmanned Systems

Questions and Comments