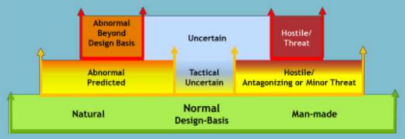
SAND2020-1766PE

Applying the Always/Never Framework to Safety in Satellite Rendezvous and Proximity Operations and On-Orbit Servicing



PRESENTED BY

Celeste A. Drewien, Ph.D.

Roger Byrd, Ph.D.

Scott E. Slezak, Ph.D.

Mark Ackerman, Ph.D.

Washington DC
November 15, 2019

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Issue

- Space environment is uncertain—congested, contested
  - RPOs/OOS create uncertainty
- High consequence of unsafe RPO/OOS operations—national security implications
  - Mission failure
  - System break-up
  - Space debris
- Safe RPOs/OOS must prevent accidents and their ensuing wreckage
- Guidelines for safety of unmanned satellite RPOs and OOS are emerging
- Technical framework and standards are needed for/would benefit safety for government and commercial RPOs/OOS

Purpose

- Consider the adaptation of nuclear weapon (NW) Always/Never safety framework to satellite RPOs and OOS
- What is necessary to apply Always/Never safety framework to RPOs/OOS?
- What can be learned by applying the framework to RPOs/OOS?

In the Cold War, NW safety technology was unclassified
to encourage sharing and use of US NW safety technology by other nuclear states

NW Always/Never Framework

- "NWs are subject to the most precise and stringent command and control, safety, and security possible to prevent accidental or inadvertent nuclear explosions"

> NWs must **always** be available for use when needed and **never** go off unless authorized.

- Achieving assured safety—Safety Principles
  - Implementation of **NW safety design principles** or **"3I's"** in design and operation
    - **Isolation**—the predictable separation of weapon elements from compatible energy
    - **Incompatibility**—the use of energy or information that will not be duplicated inadvertently
    - **Inoperability**—the predictable inability of weapon elements to function
    - plus, the little "i" for **independent** (differing properties and functions) safety subsystems or components
  - **Elimination** of safety hazards from design selection, operation, and logistics

NW Environments and Safety Requirements over Stages of System Lifetime

Design-Basis Environment	Definition	Reliability Requirement	Safety Requirement
Normal	Planned and expected	Meet system reliability requirement	Remain safe
Abnormal	Accident or beyond design basis for mission reliability	Treated as unreliable	Remain safe
Hostile	Deliberate threats	No severe degradation in reliability for design basis	Remain safe, per mission-specific needs

Safety Requirements:

no accidental explosion greater than four pounds (4 lbs) TNT equivalent
no dispersal of special nuclear materials

First: Define RPO/OOS Safety

- The Consortium for Execution of Rendezvous and Servicing Operations (CONFERS) provides guidance for RPO safety of **minimize likelihood of and adverse consequences from collisions and generating space debris.**[6]

- NPR 8715.7A[7] and Mil-Std-882D[8] define safety as **freedom from those conditions that can cause** death, injury, occupational illness, **damage to or loss of equipment or property, or damage to the environment.**

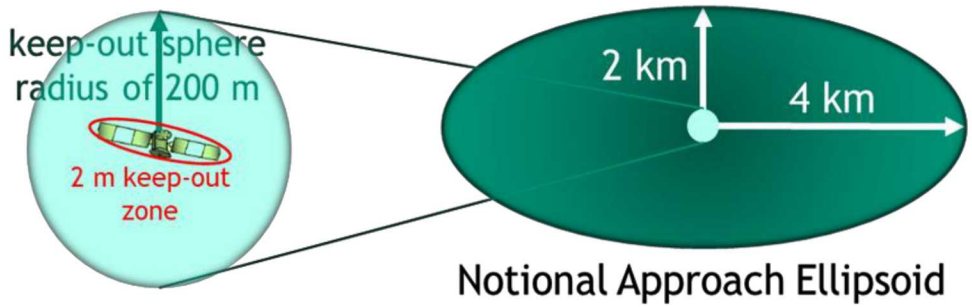
- NASA Safety Standard Volume 1[9] adds **freedom from conditions that cause loss of mission.**

- RPO/OOS safety focuses on distance and "velocity for as an important factor for the final approach maneuver prior to braking"[5].

The RPO community abides by "do no harm", where harm is an ambiguous term but understood to mean minimize debris and do not impact the mission of the satellite.

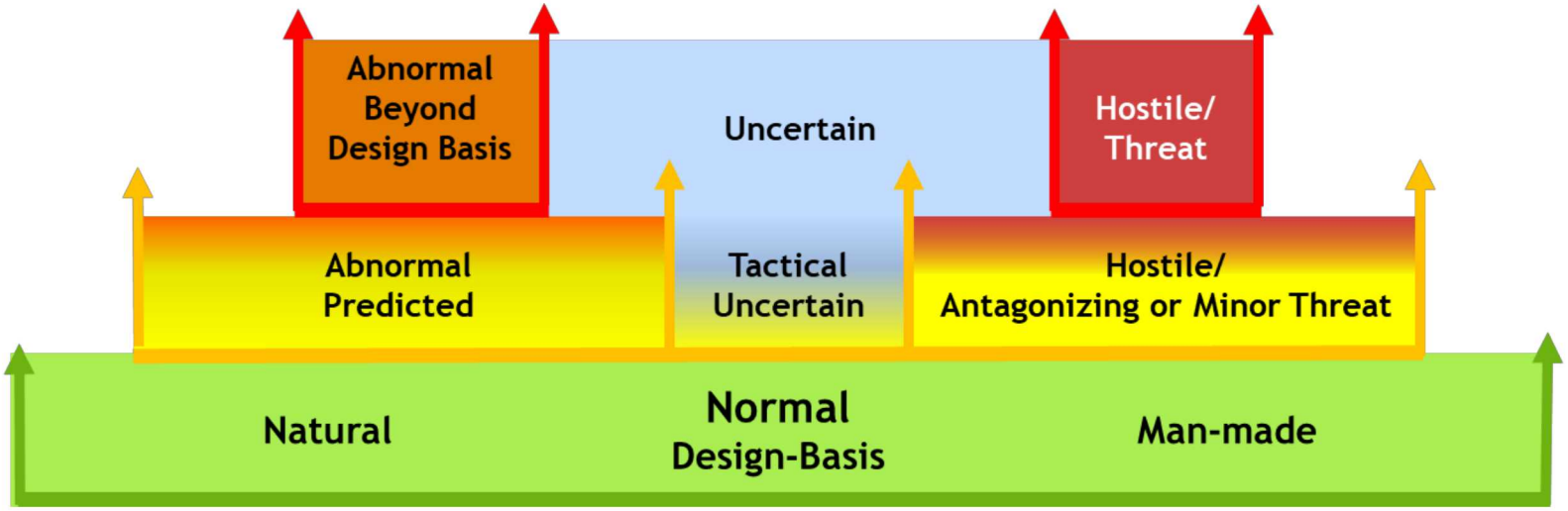
Second: Identify RPO and OOS Stages of Operation

Stage	Definition
Transit	Flight outside the approach ellipsoid surrounding a space object; may include phasing
Approach	Movement within the approach ellipsoid (e.g., 4x2x2 km) and keep-out sphere; final approach is within meters to contact
Docking	Physical contact, including soft docking with an extendible interface and hard docking in which full physical connection is achieved, and de-spin
Service/Capture	Integrated operations
Undocking	Release of physical connections and separation
Depart	Movement away, exiting the approach ellipsoid



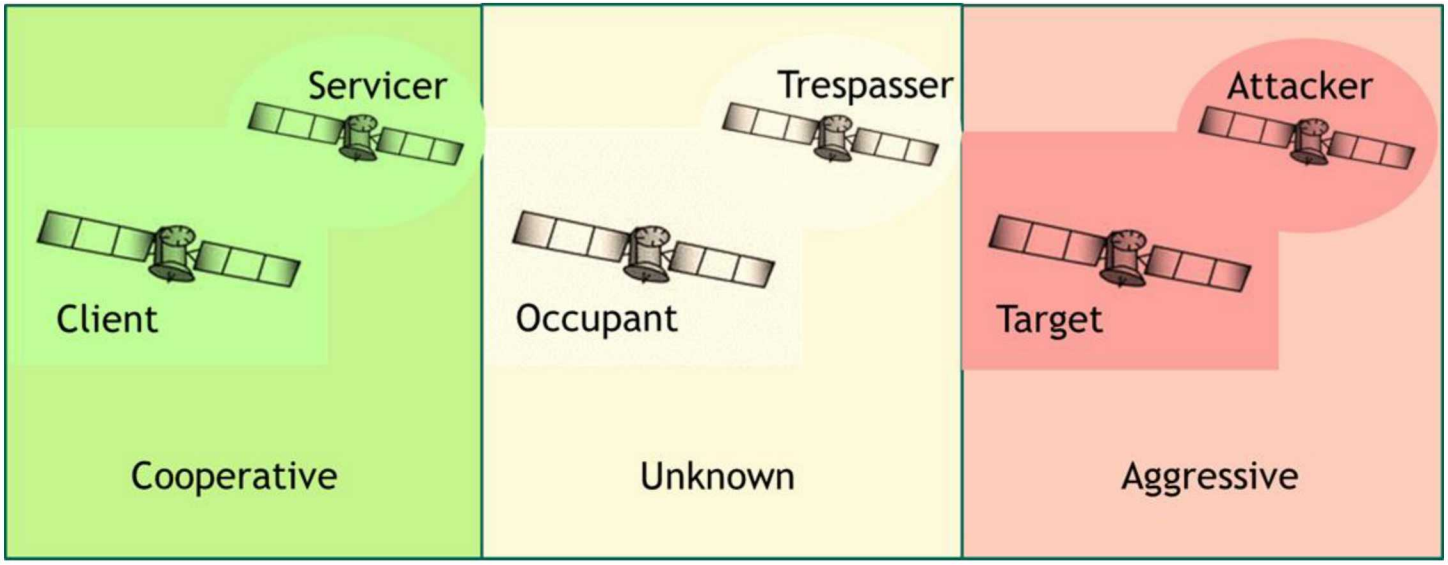
Third: Define RPO/OOS Environments

Normal	Tactical	Abnormal	Hostile/Threat
Environments in which operations and associated activities are expected to be performed over the satellite's lifetime	Temporary environments created by tactics, such as mitigating actions to avoid or respond to a (potential) attack, or a predicted extreme environment	Environments that are not expected to occur during operations, are beyond design basis, or arise from accidents	Environments created by unreasonable interference or attack may exceed the survival threshold

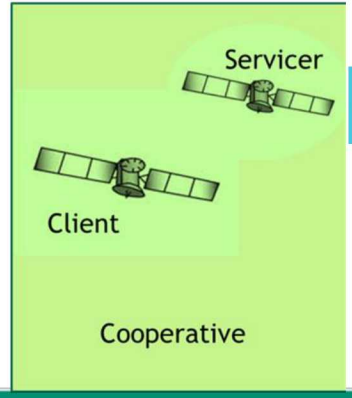


Fourth: Recognize RPO/OOS Scenarios

- Development of scenarios aids identification of specific environment types and highlights the credibility of accident and hostile environments



Applying the Safety Framework



Client and Servicer Reliability and Safety in Normal Environments

	Client		Servicer	
Normal Environment	**Reliability**	**Safety**	**Reliability**	**Safety**
Transit			Operational Mode	Passive safety collision avoidance (PSCA)
Approach	Signal authority to proceed, change to Service mode	Change to Safe mode	Given authority to proceed, change to Service mode	Change to Safe mode
Docking	Service mode	Safe mode	Service mode	Safe mode
Service				
Undock				
Depart	Change to Operational Mode	Remove Safe mode	Change to Operational Mode	Remove Safe mode, move to PSCA

Application of safety framework generates creation of modes, such as Operational, Safe, and Service mode for the OOS

Applying the Safety Framework

Client and Servicer Reliability in Safety and Abnormal Environments

	Client		Servicer	
Abnormal Environment	**Reliability**	**Safety**	**Reliability**	**Safety**
Transit			Withdraw	PSCA
Approach	Operate through, abort authority to proceed	Change to Safe mode	Abort and withdraw	Remain safe and/or change to Safe mode if needed
Docking	Depending on SOH, operate critical systems through in Service mode and/or apply Recovery mode as needed	Operate other systems in Safe mode	Depending on SOH, attempt service or detach, otherwise change to Recovery mode as needed	Remain in Safe mode
Service				
Undocking				
Depart	Check SOH and change to Operational mode	Check SOH and remove Safe mode	Check SOH and change to Operational mode	Set PSCA and remove Safe mode if applicable

Ability to determine state of health (SOH) benefits safe operations and mission resumption

Applying the Safety Framework

Hostile Environment Stages of Servicer-Client Scenario

Hostile environments for RPOs/OOS would be possible threat environments

- kinetic energy threats
- orbital threats
- optical backgrounds
- conducted, radiated e-field and h-field (EMR) interference
- dispersed high altitude electromagnetic pulse (EMP)
- atmospheric ionization
- prompt burst radiation (x-rays, gamma rays, and neutrons)
- debris decay radiation (short-lived emissions)
- trapped debris decay betas (electrons)
- deposited debris

Logic is similar to abnormal conditions, but the Client and Servicer may operate through the hostile environment

Applying the Safety Framework

Occupant-Trespasser and Target-Attacker Scenarios

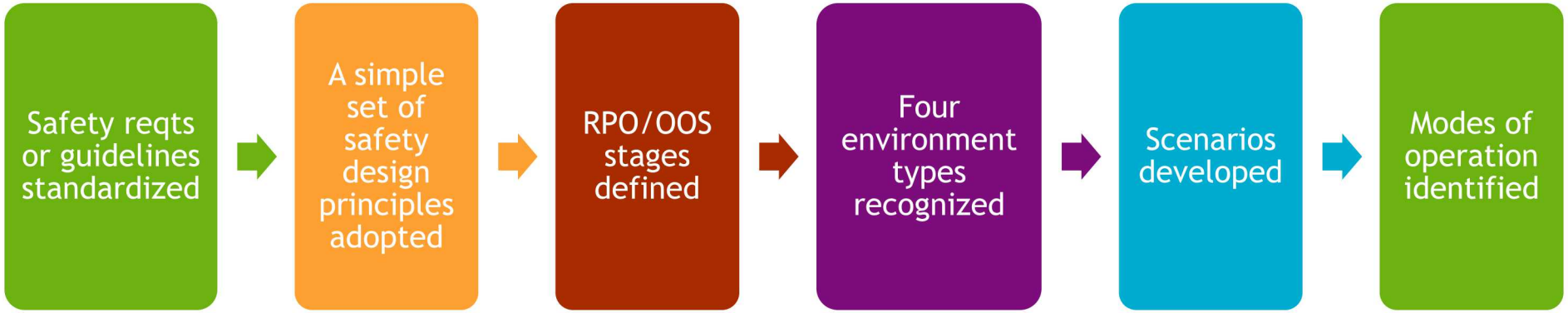
	Occupant		Trespasser/Attacker	
	Reliability	Safety	Reliability	Safety
Approach	Change to Alert mode	Change to Safe mode	No Control	
Docking	Signal Alert and change to Survival mode	Survival mode		
Capture				
Undocking				
Depart	Change to Operational mode using Recovery mode as needed	Remove Survival mode		

Tactical scenarios are affected by Survival mode options:

- Maneuvering to escape, where orbital parameters are changing
- Generating defensive counterspace actions[10] to impede the Attacker
- Other tactics

Summary

- Elements of the NW Always/Never safety framework could be useful for RPOs/OOS
  - Reminds community of uncertain environments in space
  - Provides rigor consistent with needs for high consequence situations
  - Drives common safety language and standardization for broader community
- Adapting the framework led to our identifying many missing elements for RPOs/OOS
- Applying the framework generated the need for modes of operation
- To develop an equivalent framework for RPOs/OOS, the following steps would be necessary



References

- [1] Rebecca Reesman and Andrew Rogers, "Getting in Your Space: Learning from Past Rendezvous and Proximity Operations", Center for Space Policy and Strategy, The Aerospace Corporation (May 2018)
- [2] Alton Donnell, "A Robust Approach to Nuclear Weapon Safety", SAND2011-4123C, Sandia National Laboratories, Albuquerque, NM (2011)
- [3] NASA Goddard Space Flight Center, "General Environment Verification Standard (GEVS)", GSFC-STD-7000A, Greenbelt, MD (March 28, 2018)
- [4] Department of Defense, "The Satellite System Natural and Nuclear Environment Standard", MIL-STD-3053 (April 2016)
- [5] David Barnhart et al., "Using Historical Practices to Develop Safety Standards for Cooperative On-Orbit Rendezvous and Proximity Operations", 69th International Astronautical Congress (IAC), Bremen, Germany (1-5 October 2018)
- [6] Consortium for Execution of Rendezvous and Servicing Operations, "CONFERS Recommended Design and Operational Practices", (February 1, 2019)
- [7] NASA, "Expendable Launch Vehicle (ELV) Payload Safety Program", NASA Procedural Requirements, NPR 8715.7A (February 24, 2014)
- [8] Department of Defense, "Standard Practice for System Safety", MIL-STD-882E (May 11, 2012)
- [9] NASA, "NASA System Safety Handbook, Volume 1, System Safety Framework and Concept Implementation", version 1.0, NASA/SP-2010-580 (November 2011)
- [10] Defense Intelligence Agency, "Challenges to Security in Space" (January 2019)