



Mission Success Starts with Integrated Risk Management

SPACE AND MISSILE SYSTEMS CENTER

A Proposed Systems/Space Safety Approach **- Integrating Safety & Mission Assurance for RD** **& Prototyping Programs/Missions**

Dr. Feng Hsu

SSM, SSC/SZI

Innovation & Prototyping Directorate (I&P)

US Space Force

Adapting Mission Assurance Conference

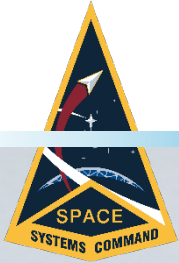
Oct. 19, 2022

Aerospace Corporation

KAFB Albuquerque, NM



Mission Success Starts with Integrated Risk Management



SPACE AND MISSILE SYSTEMS

Outline

- **Background**
- **Challenges of small & low budget satellites & space missions**
- **The need of an Integrated Safety & MA approach on RD & Prototyping**
- **The old practice vs proposed approach**
- **Introduction of proposed Min-Max methodology for system safety**
- **Risk matrix proposed for tailoring of mishaps risk per criticality index**
- **Concluding Summary**



Mission Success Starts with Integrated Risk Management



SPACE AND MISSILE SYSTEMS CENTER

Background

- **The newly established SSC/USSF is confronted with challenges from many technical and programmatic aspects**
- **Several recent occurrences of space system mishaps cultivated the need and urgency for exploring an innovative approach on safety & mission assurance tasks**
- **SSC's EPIC development strategy necessitates the need for an innovative framework for tailoring safety risk acceptance without sacrificing technical & programmatic rigor**
- **The old paradigm of systems/space safety approach doesn't bolt well with the EPIC strategy or R&D and prototyping type of programs/missions under-taking by SSC/SZI**



Mission Success Starts with Integrated Risk Management



SPACE AND MISSILE SYSTEMS CENTER

Mission Assurance Challenges for RD & Prototypes

- Complexity & innovative nature of systems and mission architectures
- High uncertainty & system/mission risks not only due to less technology maturity but more on programmatic constraints
- Not sure how much assurance & system safety tasks is enough?
- Need trade-offs between Cost of failure & Value of mission success
- Mission Assurance needs to be mission specific
- Environment –mechanical, thermal, radiation, EMI/EMC hazard risks
- Experimental nature of SV Life & mission duration ranging from 1 year to 10 years
- Budgetary Value gaps ranging from \$5m to \$500m
- Stringent schedule & cost constraints for Rapid development and deployment
- Scoping/tailoring difficulties - no standard SMA process could fit for all programs



Mission Success Starts with Integrated Risk Management




SPACE AND MISSILE SYSTEMS CENTER

Why Integrating System Safety and Mission Assurance (SMA) is needed ?

Understanding and implementing the SMA trade space for prototype satellites is important to improve success rates, tackle more challenging missions while managing expectations, scope missions, and minimize oversight burden that inhibits innovation

Key elements & activities of Mission Assurance and System Safety tasks are inherently the same, overlapping or intertwined:

- *Mission/Sys Concept definition*
- *Design/Architecture*
- *SRR and associated hazard risk Assessment*
- *Part, Material, & Process*
- *Hazard identification, mitigations*
- *Quality Assurance*
- *Verification*
- *Risk Assessment & Management*



key tasks,
processes
critical to
both system
safety &
mission
assurance
objectives



Mission Success Starts with Integrated Risk Management



SPACE AND MISSILE SYSTEMS CENTER

Why Integrating System Safety and Mission Assurance (SMA) ? (Cont'd)

- System Safety effort need to be balanced in the Mission Assurance trade space
- Need of a risk-based Mission Assurance framework – Integrated Risk Management (risks are in various aspects of a mission, and need to be traded holistically)
- I&P Programs necessitate a flexible & disciplined tailoring in regulatory compliances (AFIs, DoDIs and ODMSP etc.)
- Programmatic constraints, mission objectives and system safety efforts need to be optimized for maximum probability of mission success
- Cost and schedule are often the key driving factors; however, understanding what SS technical practices and MA processes should be leveraged in riskier categories is vital
- Never loss sight on Mission Success, as it is the ultimate goal – more vital to a war-fighting organization like us
- Taking smart risk to achieve mission objectives is all we care



Mission Success Starts with Integrated Risk Management



SPACE AND MISSILE SYSTEMS CENTER

Why An Integrated Risk Management Framework is Critical to Mission Success?

● *The New Reality & Challenges in the High Frontier*

- Vital to see whole risk posture in wide angle views
- Greater Complexity in technology & mission systems
- Confronting multifaceted & capable enemies in space
- Criticality of Space in Modern Warfighting
- Uncertainty from all aspects



Mission Success Starts with Integrated Risk Management

SPACE AND MISSILE SYSTEMS CENTER



The Old Approach to System Safety & Mission Assurance

- System Safety function at the I&P Directorate level is separate from MA function
- Mission Assurance function is missing or delegated at the contract level only
- Risk Management only tracks risk, but not integrating S&MA to support trade-off or risk-based decision-making for mission success
- Stove-pipped system safety & mission assurance tasks based on Mil-Std-882E
- Focus in small SV/Payload assurance was simply on ignoring the standards all together or tailoring from old core standards such as MIL-STD-882E, MIL-HDBK-343 etc.
- Tailoring risks either through manipulating likelihood scales of ingenuine probability estimate or creating numerous matrices on every requirement found in every AFI/DoDI documents



Mission Success Starts with Integrated Risk Management



SPACE AND MISSILE SYSTEMS CENTER

Proposed S&MA Strategy & Solutions for RD & Prototyping Programs/Projects

- 1- Integrating System Safety and Mission Assurance functions at the I&P Directorate level
- 2- Update Risk Classification for Risk-based Safety & Mission Assurance framework with PRA tools
- 3- Defining and developing a new S&MA paradigm to struck a balance between doing nothing or follows on traditional standards and practices only
- 4- Redefining SMA criteria IAW risk classification for the I&P based not only on \$ amount, but mission objectives, technology maturity, stakeholder importance and urgency of needed capability development etc.
- 5- Implementation of a reduced risk-acceptance approval authority structure
- 6- PM to bound proper expectations for leadership and stakeholders, as this is critical to helping prevent leadership from wanting a low risk (requires higher dollar, longer schedule, etc.) program, with the lower funding profile of a high risk mission, which is unrealistic in the get-go



Introduction of Proposed Min-Max Methodology



SPACE AND MISSILE SYSTEMS CENTER

➤ **To overcome challenges and enable the fullest potential for mission success with programmatic constraints, three critical tasks need to be resolved simultaneously and innovatively:**

1. **Establishment of a systematic and consistent methodology and criteria for ranking and categorizing program types based on key program attributes.**
2. **Creation of adequate and unified system safety process with pertinent risk assessment criteria for each categorization of program/mission criticality class.**
3. **Establishment of a codified system safety and hazard risk assessment tasks that are consistent with the criticality and risks to be treated by implementing these tasks accordingly.**



A Systematic and consistent method for program characterization & classification

(1) Program criticality based on ACAT level

- (a) ACAT – D, C, B, A (program criticality increases as ACAT level moves upward)***
- (b) Non-ACAT programs based on mission objectives or success criteria (this criticality attribute represent the majority of DCI programs and it will be the focus of this proposed methodology)***
- (c) Non-ACAT program with significance in cost (based on dollar amount)***



Introduction of Proposed Min-Max Methodology (Cont'd)



SPACE AND MISSILE SYSTEMS CENTER

A Systematic and consistent method for program characterization & classification (Cont'd)

(2) Program criticality based on level of Technology Maturity

(a) Experimental (proof of concept program; TRL 5 – 6)

(b) Prototyping program (TRL 7 – 8)

(c) Capability demo (pre-operational; TRL 9 or greater)

(3) Program criticality based on Mission Importance

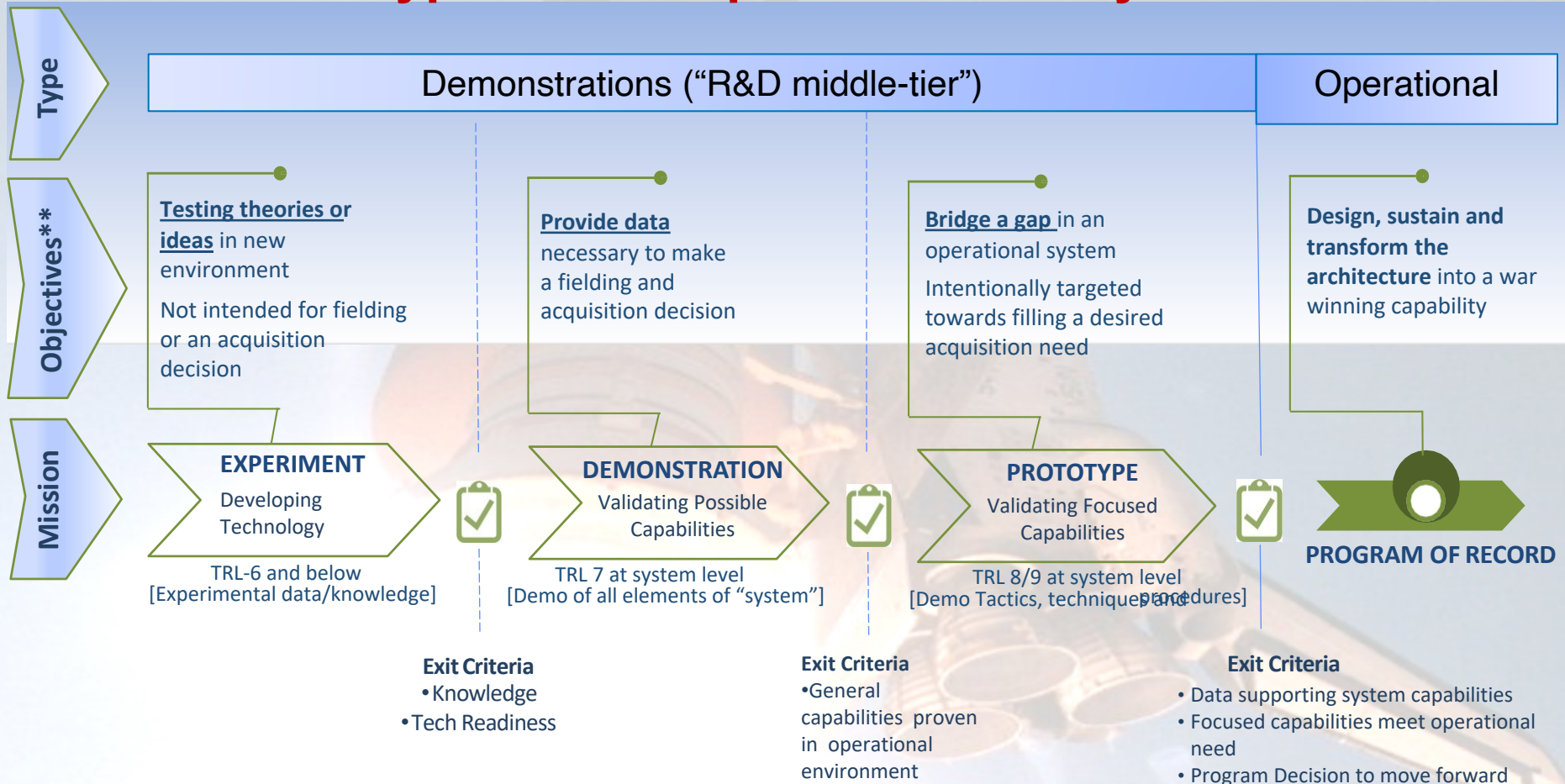
(a) Significant impact on space war fighting future capability

(b) Urgency of program timing required

(c) Level of stakeholder interests relevant to war fighting requirement



Example of Program Classification Based on TRL & Mission Types – A Simplified Criticality Assessment





Proposed Matrix for aggregated program criticality index

<i>Program ID & Level of criticality</i>	<i>ACTA level or dollar \$ amount</i>	<i>Technology maturity</i>	<i>Mission importance</i>	<i>Total assessed criticality indices/score</i>
Level 1 (High)	\$50-\$500k	x	x	2
Level 2 (Med)	\$500k-\$10m	x		3
Level 3 (Low)	x (\$10m X->100 mil)		x	3
Final weighting factor for aggregated overall program criticality score (+- %): -5%				7.6

Example matrix for assessment of aggregated program/mission criticality

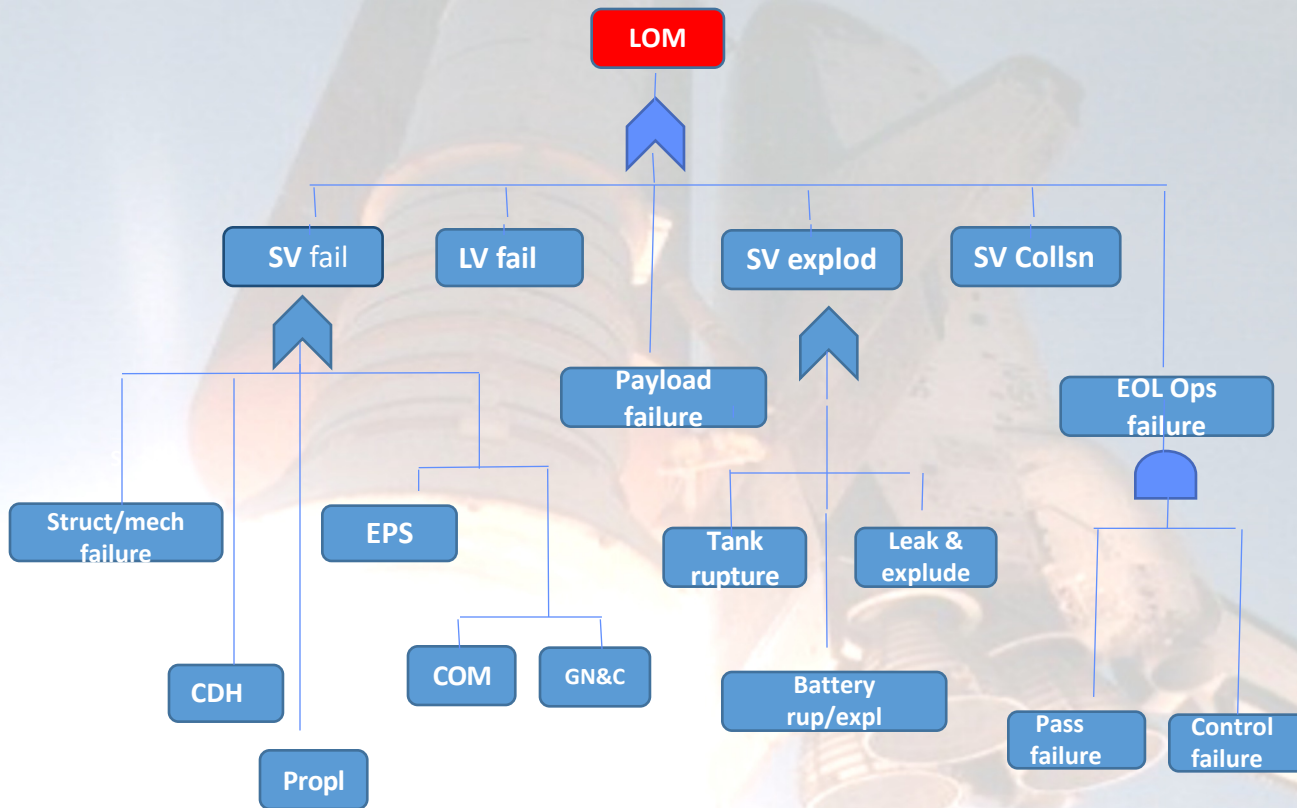


Program safety risk assessment IAW program criticality index determination

- **Assessment of technical safety risks at the program (mission) level**
- **Assessment of technical safety risks at the system/subsystem level**
- **Assessment of technical risks at the component & internal fault level**
- **Formulation of a codified system safety tasks according to program criticality index determination**



An Example MLD which Ties Mission Requirement with Design Spec & Safety Risk Tolerance





A Codified System Safety Task Control Strategy IAW Level of Program Criticality Index

- Enables a well-disciplined & SE-based Mishap Prevention process
- Assures mission success at fullest potential under all constraints

Summary of a codified system safety & risk assessment tasks ranked by applicability to programs of various mission criticality level

<i>Task name & application</i>	<i>Task requirement via program/mission criticality index</i>		
Program/Mission level	Task-1-H *	Task-2-H *	Task-3-H *
Systems/subsystem level	Task-4-H	Task-5-M +	Task-6-L *
Component/part level	Task-7-H *	Task-8-M +	Task-9-L

Note: task priority ranks: H- high, M-medium, L- low, * means minimal tasks needed for Low criticality mission; * plus + means tasks need for Mid criticality mission; all 9 tasks need for High criticality mission



Examples of Minimal Sys/Space Safety Tasks Required Based on Aggregated Level of Program Criticality Index

Task 1 (rank H) - Hazard identification & risk assessment using high level MLD & ESD techniques. Either MLD or ESD are qualitative elements of PSA (probabilistic safety assessment) techniques, which can be easily and effectively utilized to identify high level hazard risks from a system architecture and mission operational concept aspect.

Task 5 (rank M) – Perform qualitative risk assessment on system level hazards (including functional or external hazards), which identified as dominant risk contributors to LOM from Task 1 using FTA or FMEA analysis focusing on critical single point system or subsystem and interface failures that will lead to direct loss of system function or resulting in degradation of system capability and performances.

Task 9 (rank L) – Perform component or part level reliability and failure rate analysis with focuses on common cause failure (CCF) risk effects, including cascading failures on multiple component failure risk scenarios. Combination of two or more component or part failure risk scenarios should be identified for risk mitigation considerations whenever resources are available.

- **Based on this codified sys/space safety task control platform, all 9 tasks are needed for High criticality programs; 7 or 5 minimal tasks needed for Med or Low criticality programs/projects respectively**



Example Tailoring of Systems/Space Safety Documentation Requirement IAW Level of Program Criticality Index

- Sys/Space Safety Compliance documentation requirement can also be tailored to align with the program's level of criticality wrt effort/risk posture and programmatic constraint

Required Safety Docs Program/Mission Criticality Level	<i>Tailored Regulatory Systems and Space Safety Documents Required as Minimal Program Compliance</i>							
	Systems Safety Docs				Space Safety Docs			
	SSPP	SAR	HTS	MSPSP	SDAR /EOLP	SFWC	DNH	PESHE / AF F813
Level-1: HIGH	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Level-2: MED		Yes	Yes	Yes	Yes	110	Yes	813
Level-3: LOW		Yes	Yes	Yes			Yes	



Key Features & Advantages of the Proposed Methodology & Associated Risk Tailoring

- Risk matrix only need to be defined at mission risk level
- Design requirements are tied to loss of mission risk elements via a systems engineering framework
- Risk tailoring based on mission criticality, therefore adequately tied to mission importance, objectives or mishap consequence
- Risk matrices not needed for each requirement found in AFI/DoDI
- Tailor/measure risks consistent to Mil-Std-882E with true prob est.
- More flexible, logical, adequate and robust to tailor risks at severity level, instead of manipulating and skewing the true event occurrence likelihood, which doesn't reflect reality
- False risk perception or miscommunications among PMs and decision-makers or stakeholders can be avoided



Risk Matrices defined/proposed for the Mini-Max methodology (Cont'd)



SPACE AND MISSILE SYSTEMS CENTER

The Right Strategy & Approach for Risk Tailoring in SMA Applications

- The term “risk tailoring” has been used quite loosely in our space safety and mission assurance community by PMs or leadership, as it has often been miss used or misunderstood
- The objective of “risk tailoring” is to achieve sound risk management based on programmatic constraint and realistic stakeholder expectations, it is therefore a very challenge technical & programmatic endeavor
- The right approach for risk tailoring is to tailor within the domain space of mishap severity with respect to level of expected risk acceptance by PMs or stakeholders
- It is simply inadequate or wrong to tailor risk by manipulating likelihood or probability numbers because it gives false event occurrence perception, and could be misleading & problematic to decision makers
- Our proposed risk tailoring methodology is to tailor on the mishap severity definitions by integrating S&MA consistently, while keeping risk likelihood defined consistently for all level of mission criticality programs
- Avoid manipulating the event occurrence probability categories arbitrarily for each safety compliance requirement



Risk Matrices defined/proposed for the Mini-Max methodology (Cont'd)



SPACE AND MISSILE SYSTEMS CENTER

Risk Likelihood defined for all level of mission criticality programs (consistent to Mil-Std-882E)

Description	Descriptive Probability Definitions	likelihood ranges
Frequent	Likely to occur often in the life of a pre-defined mission/program domain	Probability of occurrence in the range $1E-1 < Pr < 1$
Probable	Likely to occur several times in the life of a pre-defined mission/program domain	Probability of occurrence in the range $1E-2 < Pr < 1E-1$
Occasional	Likely to occur sometime in the life of a pre-defined mission/program domain	Probability of occurrence in the range $1E-3 < Pr < 1E-2$
Remote	Unlikely, but possible to occur in the life of a pre-defined mission/program domain	Probability of occurrence in the range $1E-5 < Pr < 1E-3$
Improbable	Very unlikely, it can be assumed none occurrence in the entire lifecycle of a pre-defined mission/program	Probability of occurrence in the range $Pr < 1E-5$



Risk Matrices defined/proposed for the Mini-Max methodology (Cont'd)



SPACE AND MISSILE SYSTEMS CENTER

Risk Severity (at mission level) defined for HIGH mission criticality programs

<i>Description</i>	<i>Mishap Result Definitions (Severity Category H)</i>
Catastrophic	Could result in one or more of the following: Death, permanent total disability, irreversible significant environment impact, or loss of primary mission objectives, Loss of \$ > 10M
Critical	Could result in one or more of the following: Permanent partial disability, injuries or occupational illness that may result in hospitalization of at least 3 personnel, reversible significant environment impact, or loss of secondary mission objectives, Loss of 1M <= \$ < 10M
Marginal	Could result in one or more of the following: Injury or occupational illness resulting in one or more lost work day(s), reversible moderate environment impact, or loss of tertiary mission objectives, Loss of 100K <= \$ < 1M
Negligible	Could result in one or more of the following: Injury or occupational illness not resulting in a lost work day, minimal environment impact, or loss of system functions with no mission impact, Loss of \$ < 100K



Risk Matrices defined/proposed for the Mini-Max methodology (Cont'd)



SPACE AND MISSILE SYSTEMS CENTER

Risk Severity (at mission level) defined for MEDIUM mission criticality programs

<i>Description</i>	<i>Mishap Result Definitions (Severity Category M)</i>
Catastrophic	<i>Could result in one or more of the following: Death, permanent total disability, irreversible significant environment impact, or monetary loss 5M <= \$ < 10M</i>
Critical	<i>Could result in one or more of the following: Permanent partial disability, injuries or occupational illness that may result in hospitalization of at least 3 personnel, reversible significant environment impact, or loss of primary mission objectives, monetary loss 1M <= \$ < 5M</i>
Marginal	<i>Could result in one or more of the following: Injury or occupational illness resulting in one or more lost work day(s), reversible moderate environment impact, or loss of secondary mission objectives, monetary loss 100K <= \$ < 1M</i>
Negligible	<i>Could result in one or more of the following: Injury or occupational illness not resulting in a lost work day, minimal environment impact, or loss of tertiary mission objectives, Monetary loss of \$ < 100K</i>



Risk Matrices defined/proposed for the Mini-Max methodology (Cont'd)



SPACE AND MISSILE SYSTEMS CENTER

Risk Severity (at mission level) defined for LOW mission criticality programs

<i>Description</i>	<i>Mishap Result Definitions (Severity Category L)</i>
Catastrophic	<i>Could result in one or more of the following:</i> Death, permanent total disability, irreversible significant environment impact, or monetary loss $2M \leq \\$ < 5M$
Critical	<i>Could result in one or more of the following:</i> Permanent partial disability, injuries or occupational illness that may result in hospitalization of at least 3 personnel, reversible significant environment impact, or monetary loss $1M \leq \\$ < 2M$
Marginal	<i>Could result in one or more of the following:</i> Injury or occupational illness resulting in one or more lost work day(s), reversible moderate environment impact, or loss of primary mission objectives, monetary loss $500K \leq \\$ < 1M$
Negligible	<i>Could result in one or more of the following:</i> Injury or occupational illness not resulting in a lost work day, minimal environment impact, or loss of secondary mission objectives, Monetary loss of $\\$ < 500K$

Risk Matrices defined/proposed for the Mini-Max methodology (Cont'd)



SPACE AND MISSILE SYSTEMS CENTER

Proposed Risk Matrix Consistent to Mil-Std-882E to be Used Across All DCI's Mission Criticality Programs

A Unified Risk Assessment Matrix

Severity Probability	Catastrophic	Critical	Marginal	Negligible
Frequent	High	High	Serious	Medium
Probable	High	High	Serious	Medium
Occasional	High	Serious	Medium	Low
Remote	Serious	Medium	Low	Low
Improbable	Medium	Medium	Low	Low



Concluding Summary

- An innovative system safety methodology is proposed for managing mishap risks under resource limit for R&D Missions
- System Safety effort need to be balanced and Integrated in the Mission Assurance trade space
- A risk-based S&MA approach is critical to achieve higher mission success rate
- Implementation of a reduced risk-acceptance approval authority structure is necessary thus provided for I&P programs
- Acceptance of prudent R&D risk with fullest potential for mission success is the keystone of this methodology
- Taking smart risk should be the hallmark of our approach to space programs, while fully attending to safety considerations without impeding our capacity to win in space war-fighting