NASA Engineering & Safety Center

NESC

December 8, 2005

Daniel Yuchnovicz
Systems Engineering Office

Presentation Purpose

- Provide a brief Overview of the NESC
- Describe NESC risk evaluation process
- Provide general observations of risk management issues based on engaging in100+ technical assessments

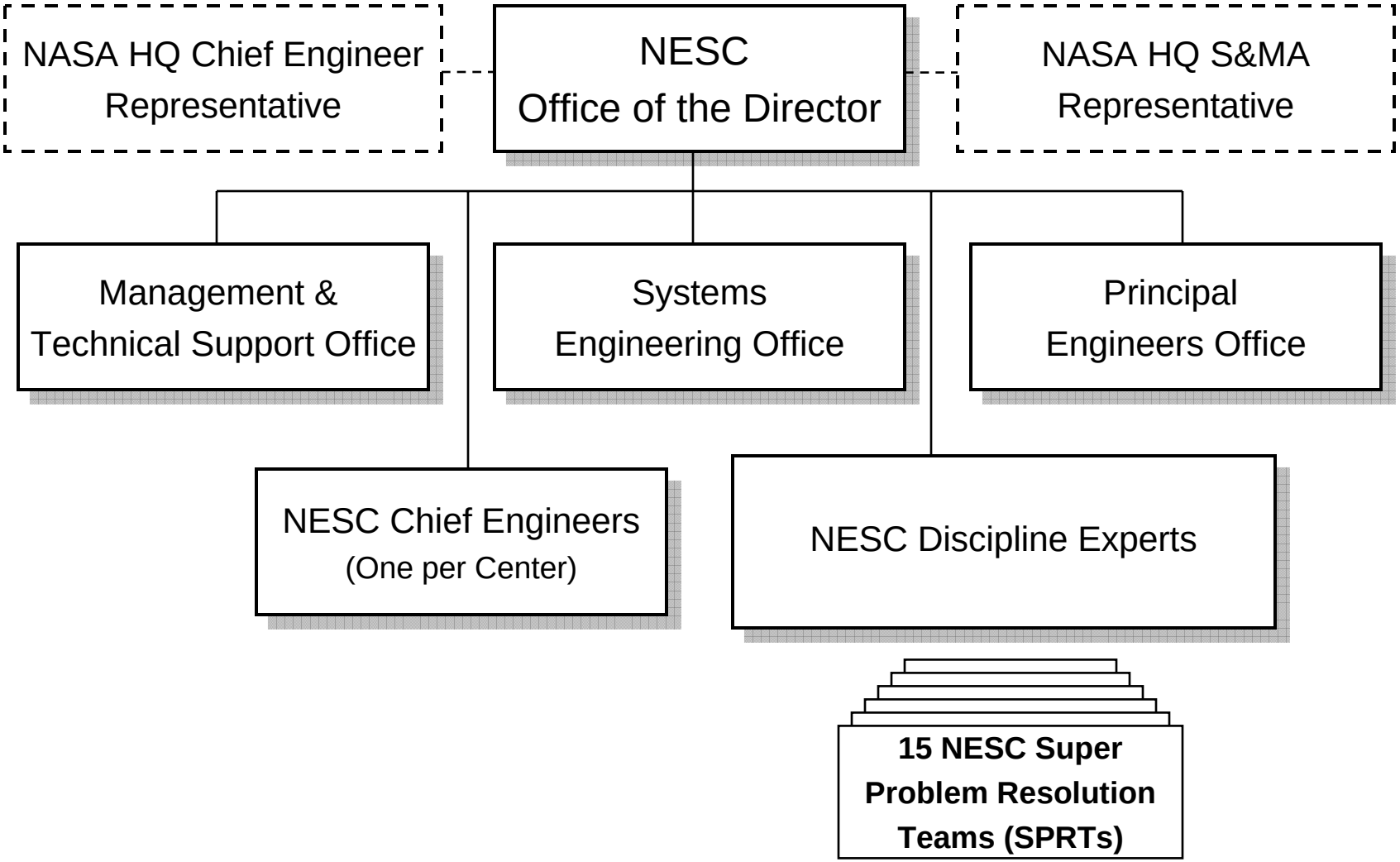
This briefing is for status only and does not represent complete engineering data analysis

What is the NESC?

- NESC's mission is to perform value-added independent testing, analysis, and assessments of NASA's high risk projects to ensure safety and mission success. We engage proactively to help NASA avoid future problems
- Includes the top technical talent from the Agency, industry, academia and other federal agencies

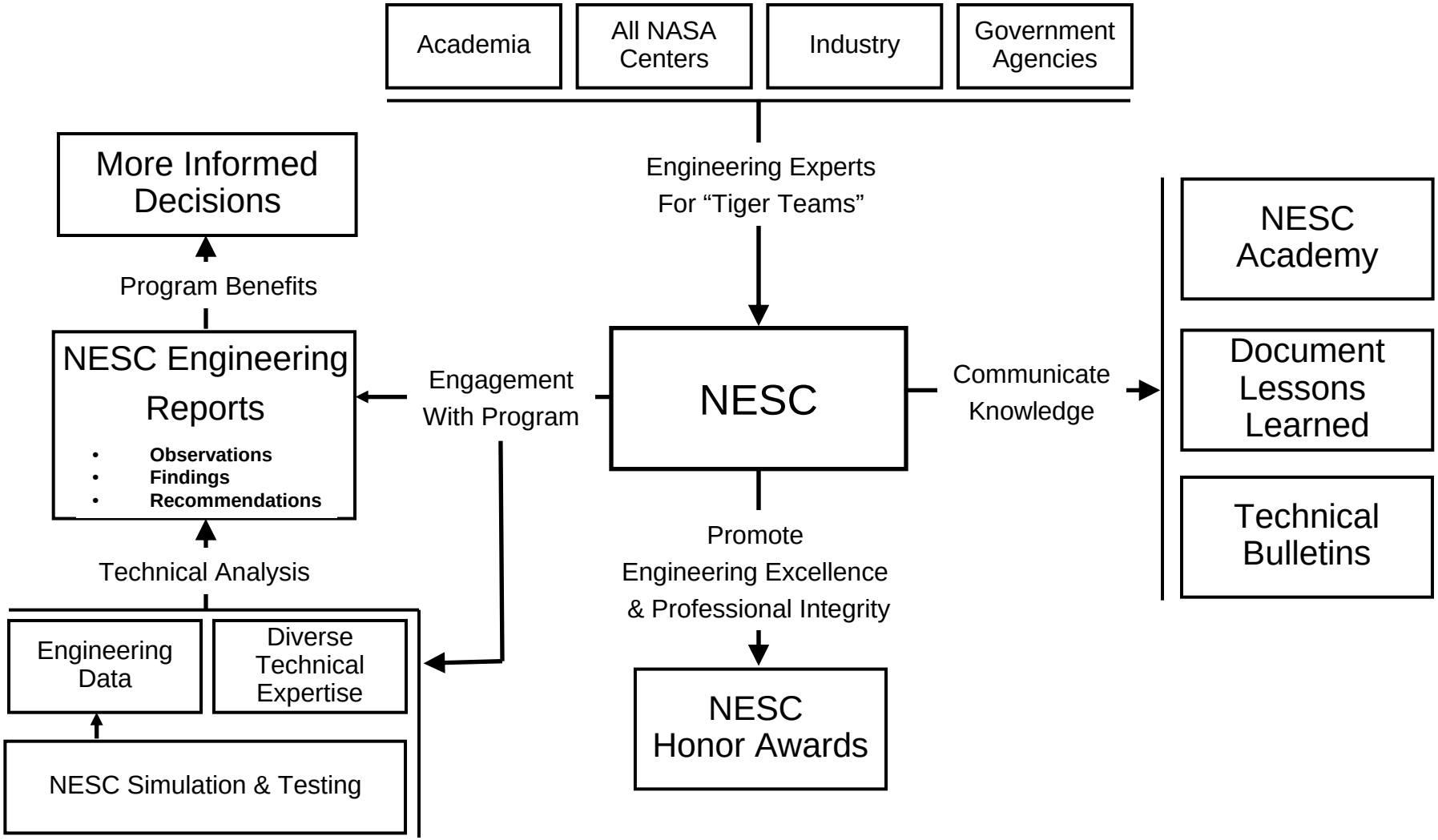
This briefing is for status only and does not represent complete engineering data analysis

NESC ORGANIZATION



This briefing is for status only and does not represent complete engineering data analysis

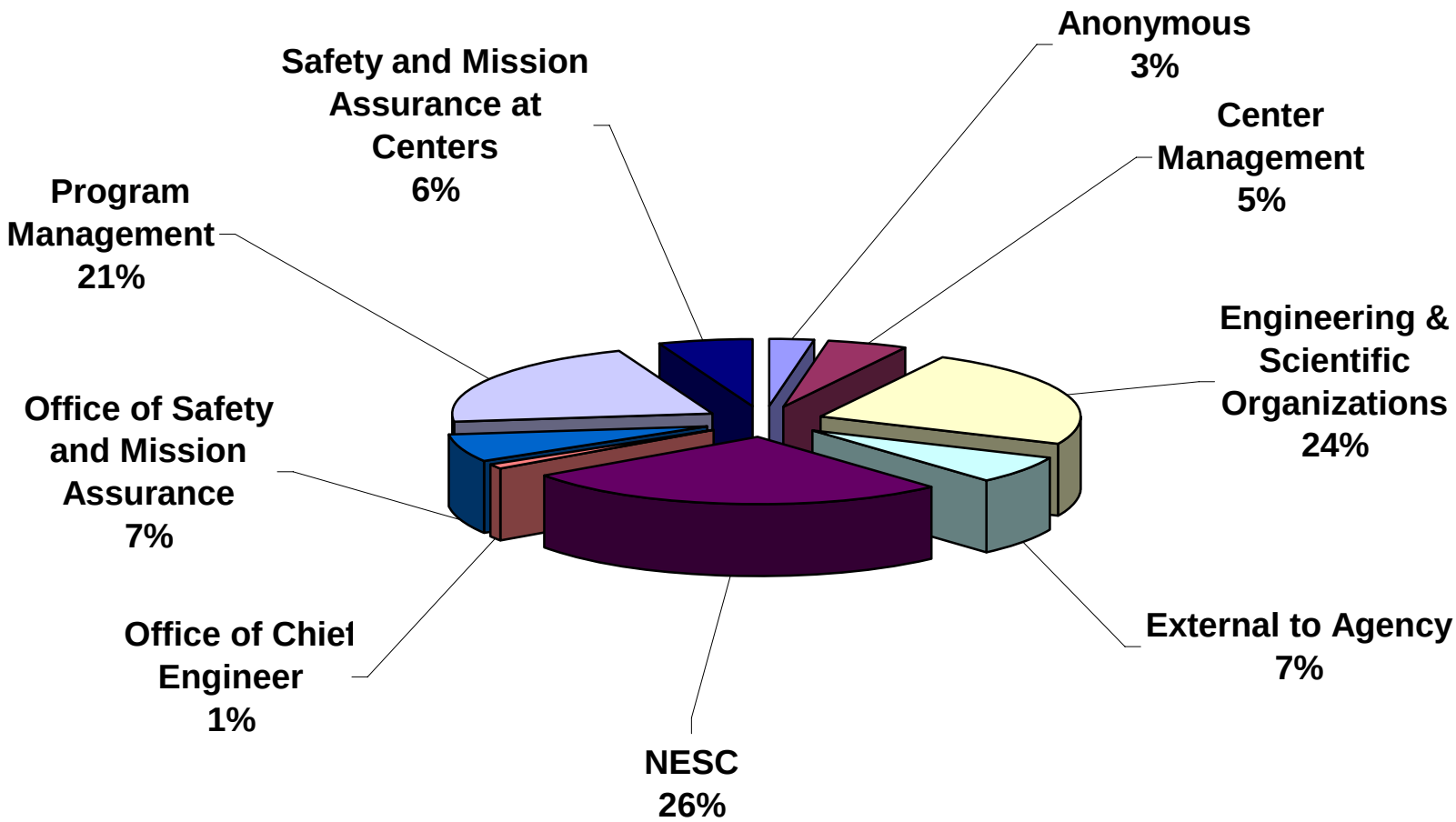
NESC Functional Model



This briefing is for status only and does not represent complete engineering data analysis

Sources of NESC Requests

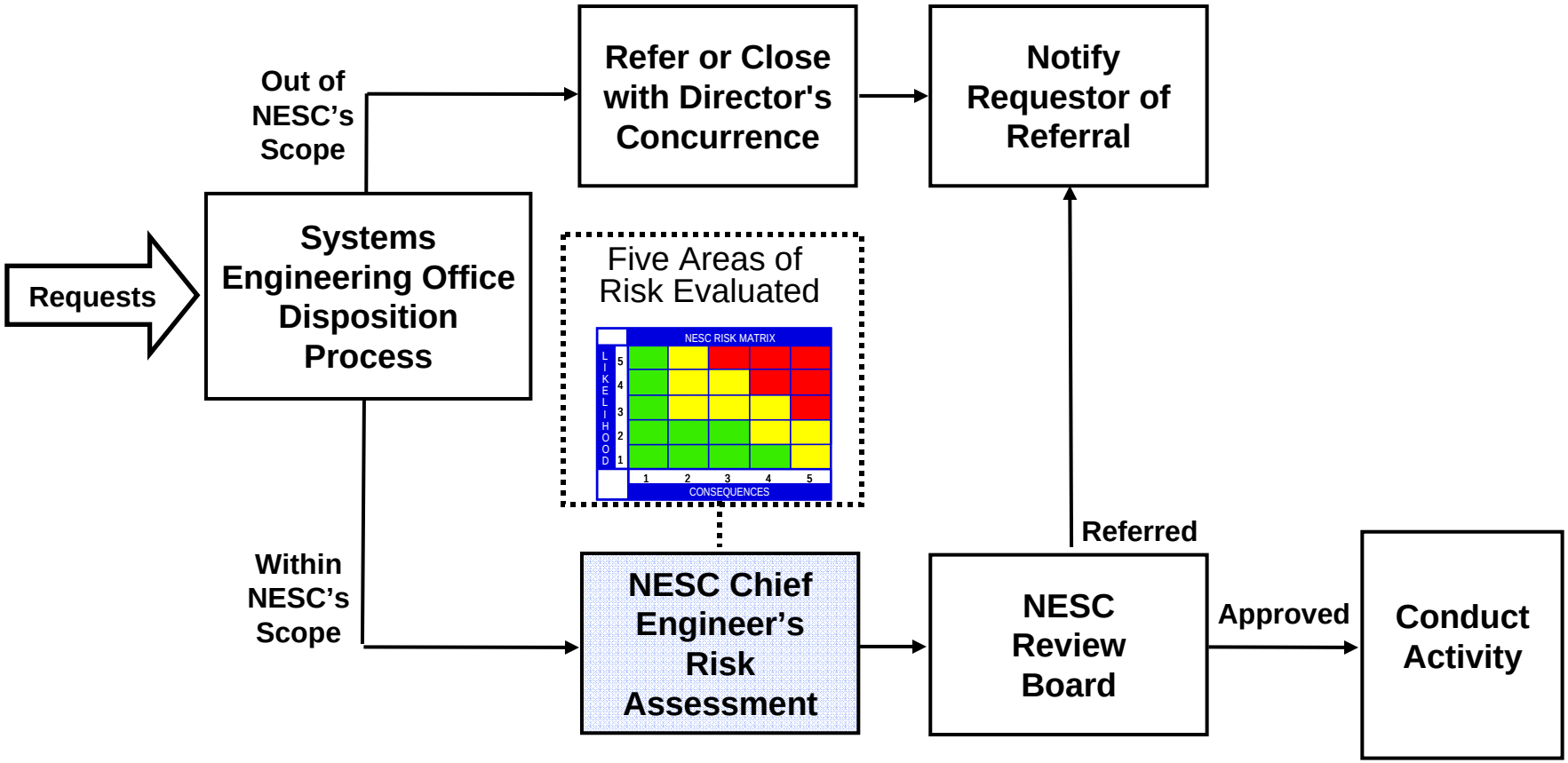
As of November 2005



This briefing is for status only and does not represent complete engineering data analysis

Request Processing

Request for NESC Assistance - Selection/Prioritization Process



This briefing is for status only and does not represent complete engineering data analysis

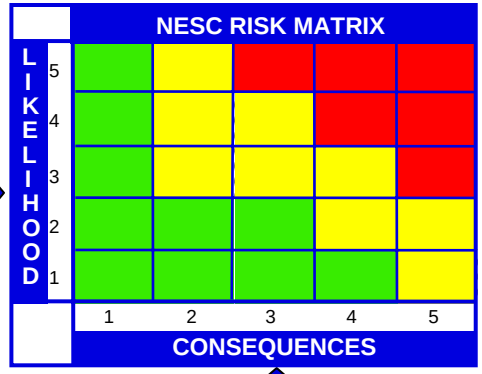
NESC Risk Assessment

Both Qualitative and Quantitative Definitions

What is the likelihood the situation or circumstance will happen?

LIKELIHOOD Level	Probability	. . . or –. . .	Example
5	Very Likely	Likely to occur often. Likelihood of occurrence is estimated to be greater than 0.10 (10-1) per operational opportunity	Lost work case per worker over a 20 year private industry career
4	High	Expected to occur some time in the life of the item. Likelihood of occurrence is estimated to be between 0.01 and 0.10 (10-2 and 10-1) per operational opportunity	Failures per US ELV Launch (1988 - 2001)
3	Moderate	Likely to occur some time in the life of the item. Likelihood of occurrence is estimated to be between 0.01 and 0.001 (10-2 and 10-3) per operational opportunity	Place holder
2	Low	Unlikely but possible to occur. Likelihood of occurrence is estimated to be between 0.001 and 0.000001 (10-3 and 10-6) per operational opportunity	Fatal crashes per automobile trip
1	Very Low	Likelihood of occurrence is estimated to be less than .000001 (<10-6) per operational opportunity	Fatal crashes per passenger airplane departure

NESC RISK MATRIX



LEGEND

- High – Accepted for NESC Board review. Probable NESC follow-on IA.
- Medium – Accepted for NESC Board review. NESC or other NASA IA action required.
- Low – Not Boarded by NESC. Direct referral to other NASA IA org.

Risk Consequence Scoring Terms

1	Safety, Health, Environment is defined as impact to life, health, working environment and natural environment
2	Mission Success definition includes impacts to Major Mission Objectives (MMOs) as well as hardware loss
3	National Significance is defined as the degree to which national prestige, visibility and public relations are impacted
4	Safety, Health, Environment, Mission Success and National Significance can exist concurrently and are not mutually exclusive
5	Risk scoring is accomplished by "multiplying" Likelihood (L) X Consequence (C). Note: numerical value is reflective of the ordered pair L, C. Care must be taken when using multiplied values as measures. When determining risk consequence among Cost, Schedule, and Technical, the highest score is represented in the NESC Risk Matrix as a single score value.

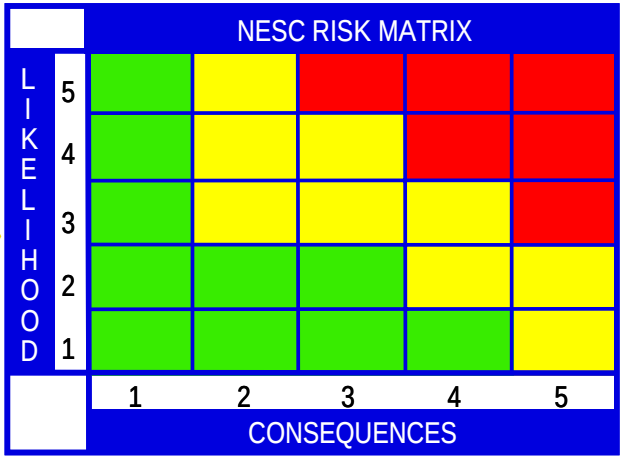
What is the Consequence of this NESC Risk?

CONSEQUENCE Level	1	2	3	4	5
Safety, Health, Environment	Minimal/no safety or health plan violations / Minimal to no environ impacts	Could result in injury or illness not resulting in lost work day / Minimal envirnmtl damage	Could result in injury or occupational illness resulting in one or more lost work day / Mit. envirnmtl damage w/o law viol	Could result in permanent partial disability, injuries or occupational illness / Reversible envinmt damage – violates law	Could result in death or perm. total disability / Irreversible severe environ damage that violates law or regulation
Mission Success	Hardware loss between $200K and $1 Million / Failure to any one MMO	Hardware loss between $1M and $10 Million / Failure to meet > 50% of supplemntl objectives	Hardware loss between $10M and $100 Million / Failure to meet any one MMO	Hardware loss between $100M and $250 Million / Failure to meet > 50% MMO's	Hardware loss exceeding $250 Million / Failure to meet all Major Mission Objectives (MMO's)
National Significance	Minimal or no identified National Prestige or Visibility	Low National Prestige and Visibility	Moderate National Prestige and Visibility	Significant National Prestige and Visibility	High National Prestige and Visibility

This briefing is for status only and does not represent complete engineering data analysis

NESC Chief Engineer's Initial Evaluation

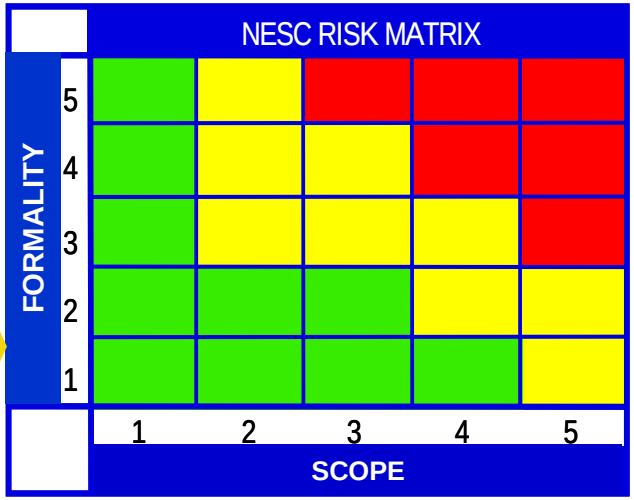
	Criteria
Risk	1. Risk – Safety
	2. Risk – Mission Success
	3. Risk – National Importance
	4. Involves Deviation from Accepted Specification, Standard, or Practice
Project	5. Project Not Actively Engaged in Resolving Issue
NESC Value	6. Potential for Advancing Discipline Knowledge Base
	7. Resolution Lends Itself to Test and Analysis
	8. Perceived Urgency



This briefing is for status only and does not represent complete engineering data analysis

NESC Chief Engineer's Initial Evaluation

	Criteria
Risk	1. Risk – Safety
	2. Risk – Mission Success
	3. Risk – National Importance
	4. Involves Deviation from Accepted Specification, Standard, or Practice
Project	5. Project Not Actively Engaged in Resolving Issue
NESC Value	6. Potential for Advancing Discipline Knowledge Base
	7. Resolution Lends Itself to Test and Analysis
	8. Perceived Urgency



Formality
- 1: Unpublished documentation
- 5: Published documentation

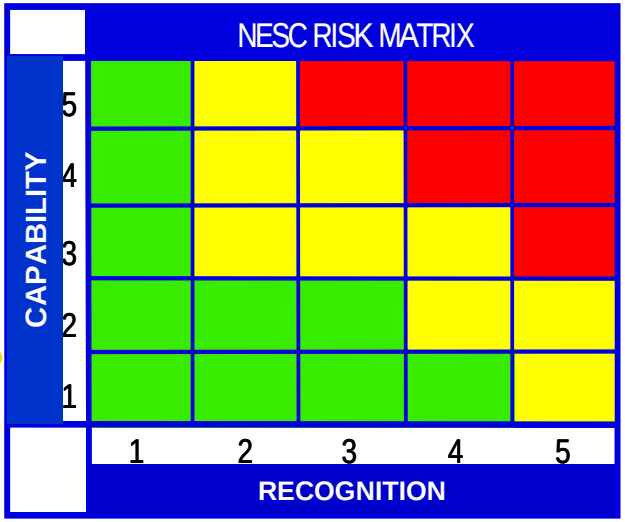
Scope
- 1: Local
- 5: Agency-level

This briefing is for status only and does not represent complete engineering data analysis

NESC Chief Engineer's Initial Evaluation

	Criteria
Risk	1. **Risk – Safety**
	2. **Risk – Mission Success**
	3. **Risk – National Importance**
	4. **Involves Deviation from Accepted Specification, Standard, or Practice**
Project	5. **Project Not Actively Engaged in Resolving Issue**
NESC Value	6. **Potential for Advancing Discipline Knowledge Base**
	7. **Resolution Lends Itself to Test and Analysis**
	8. **Perceived Urgency**

- Project Risk / Hazard Assessment and Proposed Solution Examined in Criterion #5



Capability
- 1: Project has at its disposal all resources required to resolve issue
- 5: Project does not have resources required to resolve issue

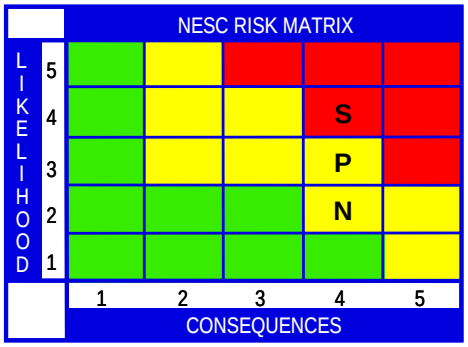
Recognition
- 1: Project is actively engaged in resolving issue
- 5: Project is not actively engaged in resolving issue

This briefing is for status only and does not represent complete engineering data analysis

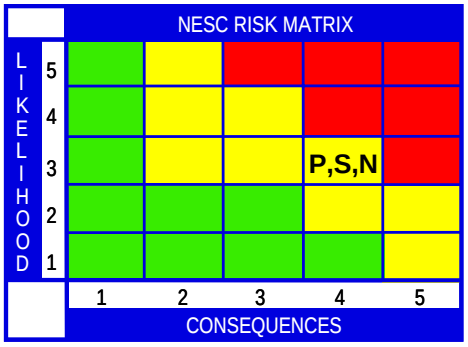
NESC Future Initial Risk Assessment Plans

- Perform three risk assessments (by Project, Center S&MA and NESC) before and after the NESC assessment to determine if risk quantification was improved
- Key Assumption – Common matrix and definitions

Example – An NESC Assessment Could Reduce Uncertainty in Likelihood



Pre-Assessment



Post-Assessment

P – Project, S – Center SMA, N - NESC

This briefing is for status only and does not represent complete engineering data analysis

NESC Risk Quantification

- NESC may evaluate a program's risk approach by reviewing the programs risk assessment (identification and analysis), and handling processes
- NESC may conduct qualitative and quantitative risk analysis including:
  - Probabilistic Risk Analysis (PRA)
    - Primarily to independently verify existing efforts, especially when existing, multiple PRAs of the same issue vary widely
      - e.g. 10E-4 to 10E-8 probability of event occurrence per operation
  - Qualitative / Quantitative Fault Tree Analysis
  - Review of Critical Items List (CIL) waiver rationale for adequacy
  - Other tools

This briefing is for status only and does not represent complete engineering data analysis

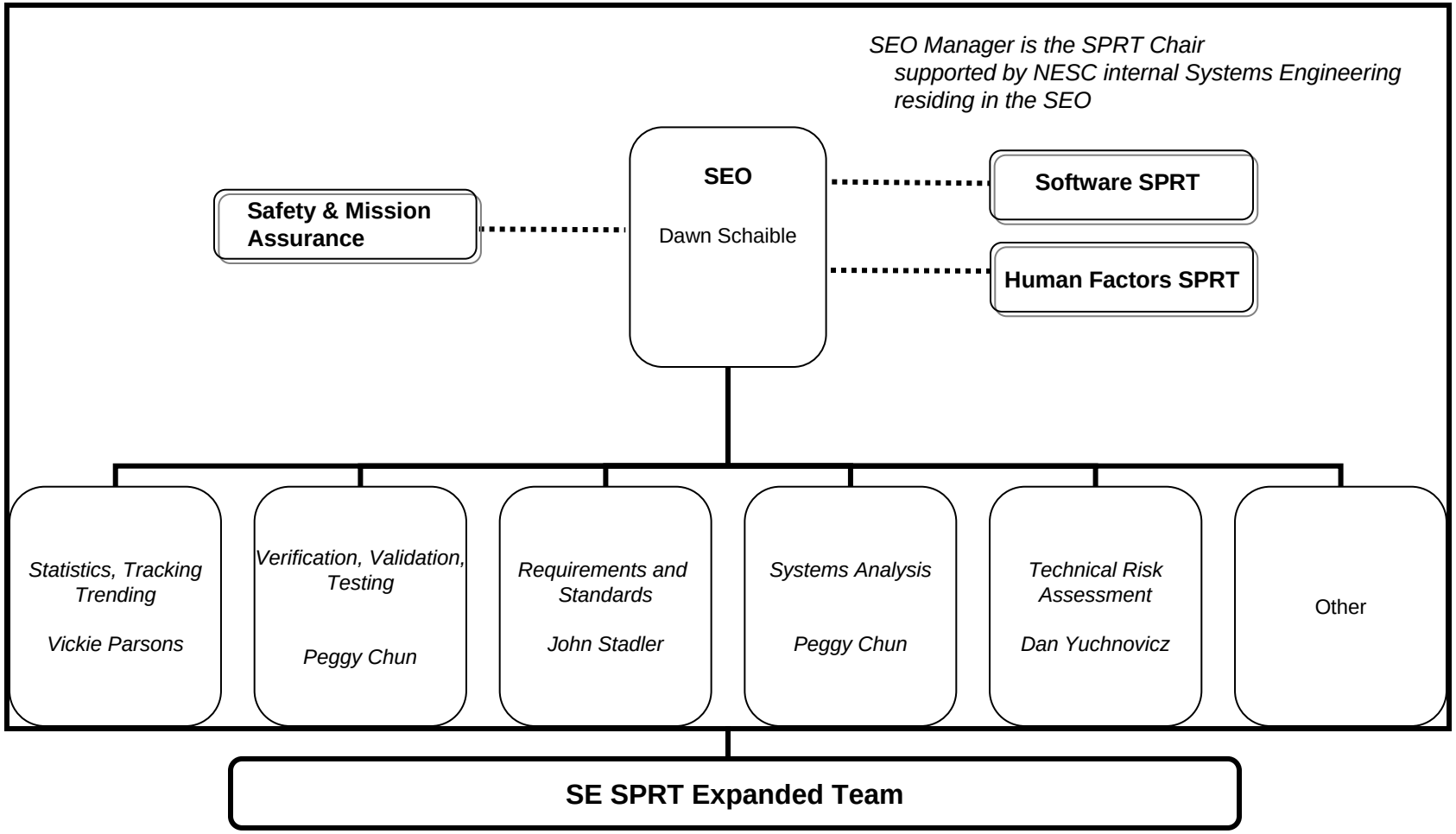
NESC Risk Quantification

- Many of the NESC technical assessments include test and simulation to generate engineering data that may reduce uncertainty or increase risk understanding /quantification
- NESC is developing a Technical Risk Analysis sub-team within the Systems Engineering Super Problem Resolution Team to maintain a ready list of qualified risk experts for use in assessments

This briefing is for status only and does not represent complete engineering data analysis

NESC ORGANIZATION

NESC Systems Engineering SPRT



This briefing is for status only and does not represent complete engineering data analysis

NESC Observations

- What is the program's understanding of risk?
  - Quantitative and qualitative approach to risk runs the range from very formal to very informal
  - New and unplanned risks develop as life extension programs are implemented and mission assets are "repurposed"
    - Waivers granted from specifications or safety requirements during initial system design can introduce unplanned risks for repurposed systems
    - Unplanned risks can be costly to mitigate
    - Effects of aging, operation, and environmental exposure not fully considered vehicle designs
    - Adequate screens for aging and/or degradation not fully considered when extending components beyond their original design life
  - Programs that share physical interfaces, therefore share risks
    - An accepted risk for one program could be an unacceptable risk for the other program

This briefing is for status only and does not represent complete engineering data analysis

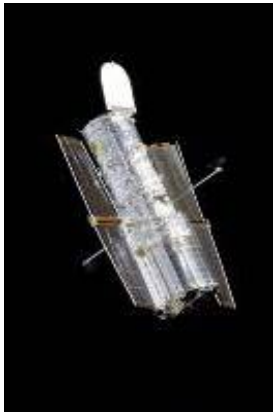
NESC Observations (continued)

- What issues have impeded programs' understanding of risk?
  - Lack of qualitative and quantitative analyses:
    - Hazard Analyses not available
    - Failure Modes and Effects Analyses not available
    - Incomplete understanding of potential errors that can occur (insufficient data for meaningful answer)
    - Lack of specialized technical discipline expertise available to the program
    - Lack of specialized expertise in the local Safety and Mission Assurance Community
    - Lack of formal engineering reports and related documentation
    - Lack of formal engineering data and analyses from international partners

This briefing is for status only and does not represent complete engineering data analysis

NESC Observations (continued)

- What issues cause disagreements in assessed risk?
  - Obvious – use of different tools among team
    - Example: 3x3, 3x4 or 4x5 matrix employed by some of the safety community and programs and the more recent 5x5 matrix
  - Less Obvious - Differences in Definitions (same tools)
    - Example: Use of quantitative definitions verses qualitative definitions sometimes result in different assessments
  - Even Less Obvious – Assessing Community's aversion to risk



This briefing is for status only and does not represent complete engineering data analysis

NESC Observations (concluded)

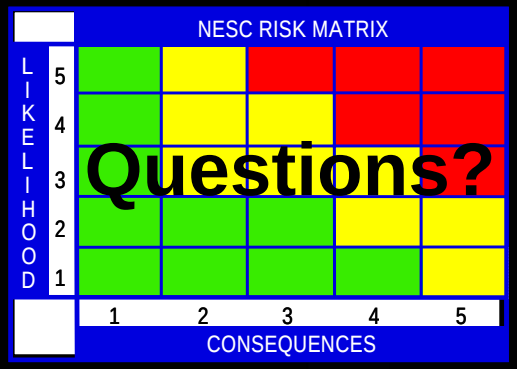
- Issues with Reliability/PRA Analyses
  - Must exercise caution when using MIL-HDBK-217 for developing point estimates of reliability for use in PRAs
    - MIL-HDBK-217 meant to be a design trade tool, not an absolute source for field (in-service) failure predictions
    - If sufficient field data is available it should always be used in lieu of a prediction
    - High imprecision and uncertainty in results (field experience agreement within 3 orders of magnitude generally considered to be good).
  - Does not consider aging effects for old parts

This briefing is for status only and does not represent complete engineering data analysis

Conclusions

- Still room for Agency-wide improvement in risk analysis
  - Currently improving and should continue to improve with management support
  - Update NPR 8400.4 Risk Matrix to standardize the assessment tool
- Many risk Lessons Learned are directly applicable to Exploration initiative
- Should continue efforts to collect Lessons Learned for Exploration initiative

This briefing is for status only and does not represent complete engineering data analysis



Questions?