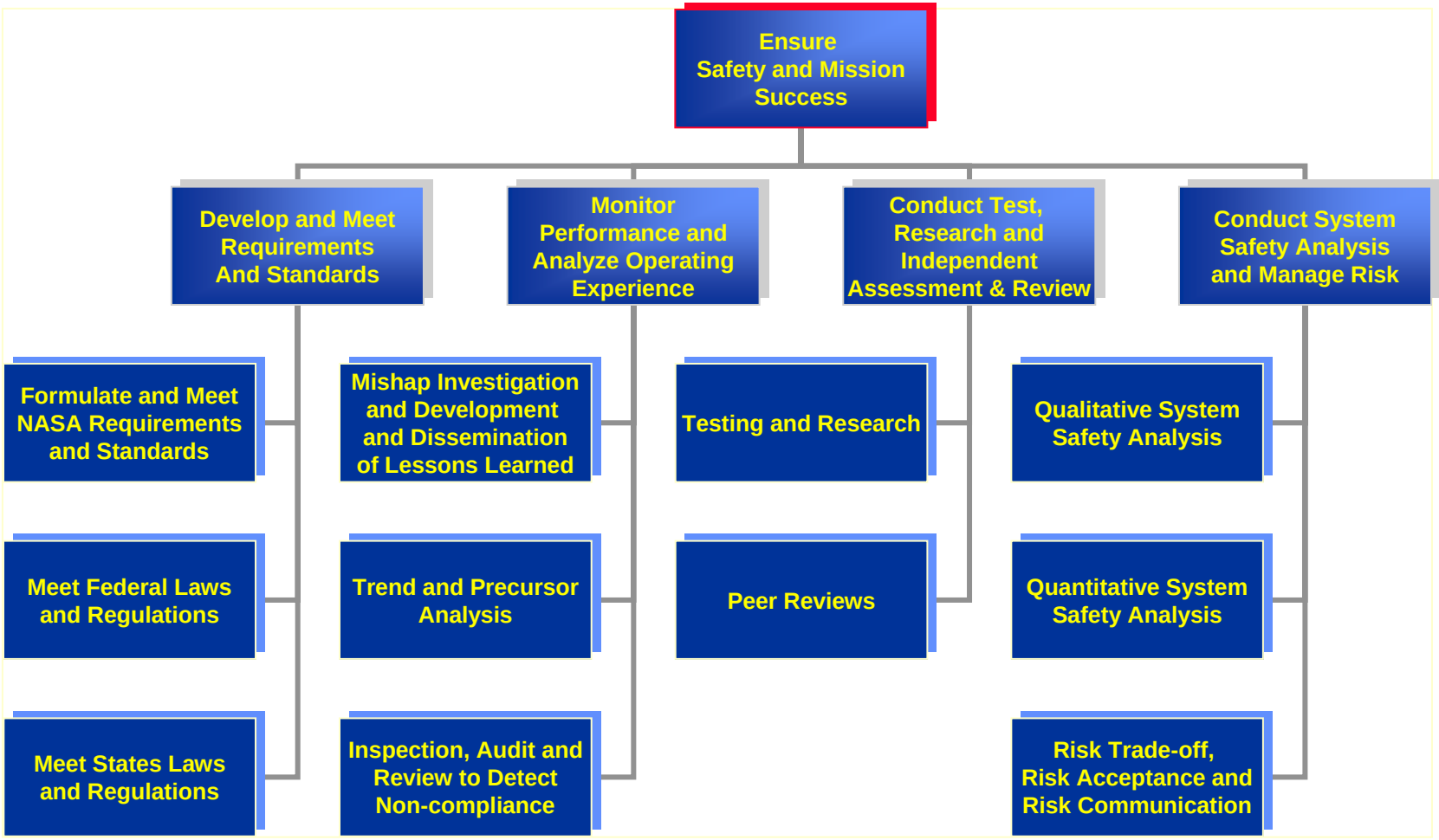
Implementation of Risk-Informed Decision Making at NASA

NASA Risk Management Conference 2005
RMC-VI, Orlando, Florida

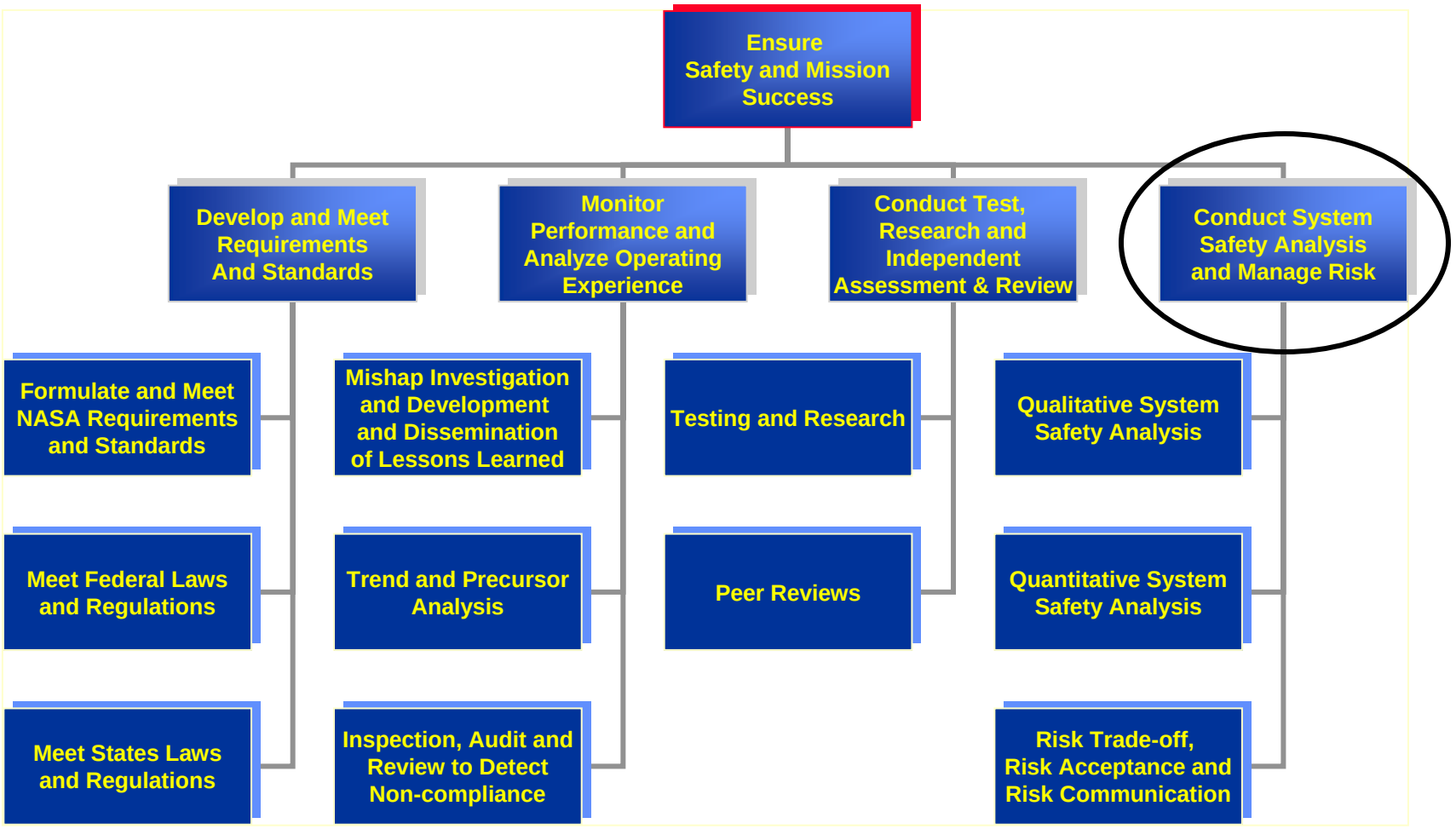
December 7, 2005

Dr. Michael Stamatelatos, Director
Safety and Assurance Requirements Division
Office of Safety and Mission Assurance
NASA Headquarters

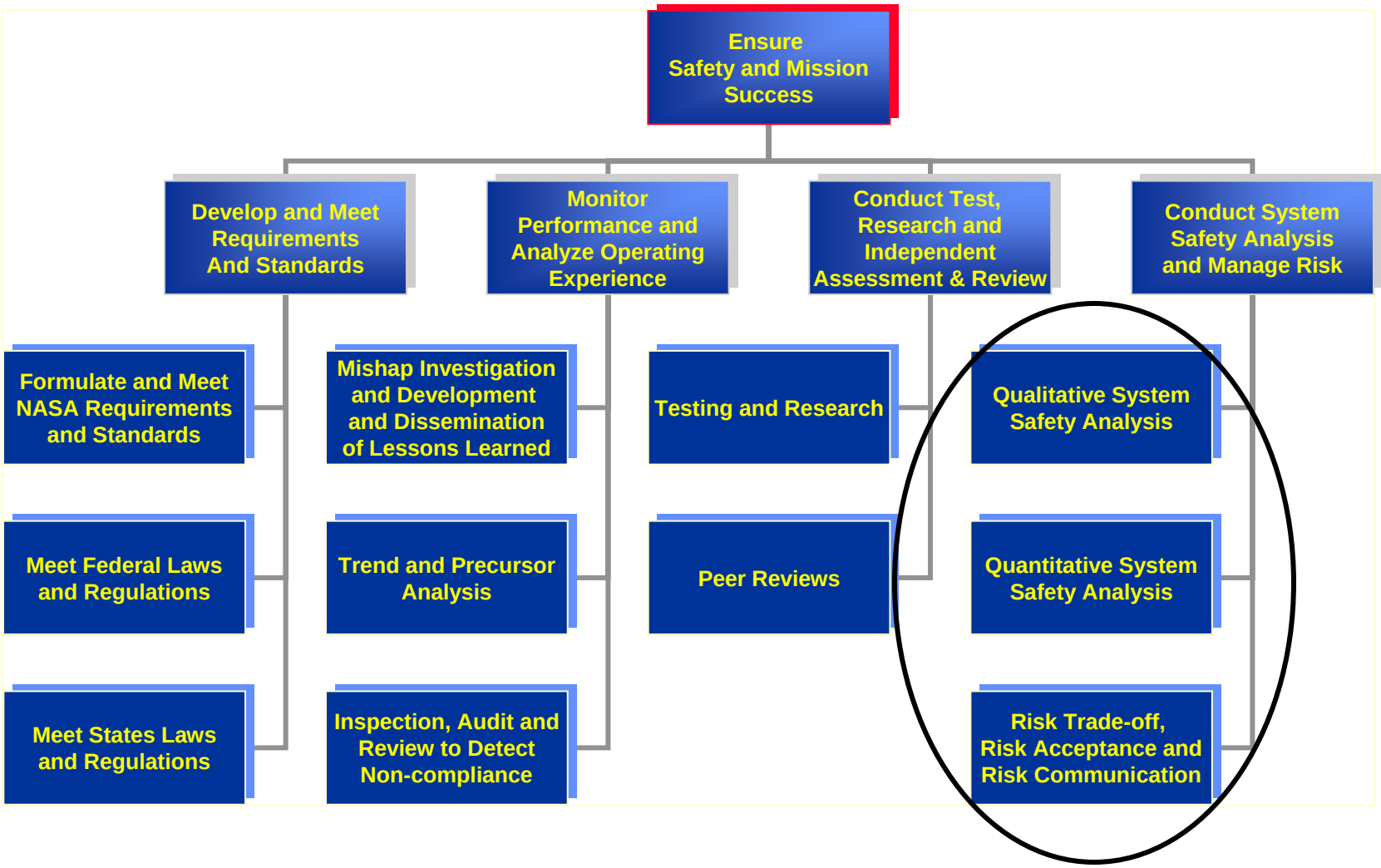
Framework for the OSMA Activities to Assure Safety and Mission Success



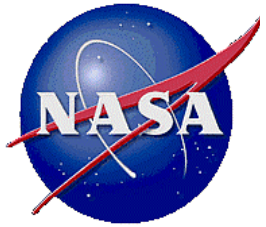
Safety, Risk Assessment & Management



Activities in Safety, Risk Assessment & Management

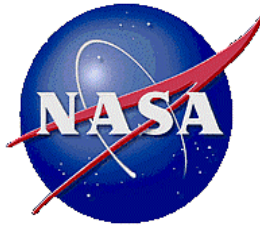


Current Status of Risk and Safety Assessment at NASA



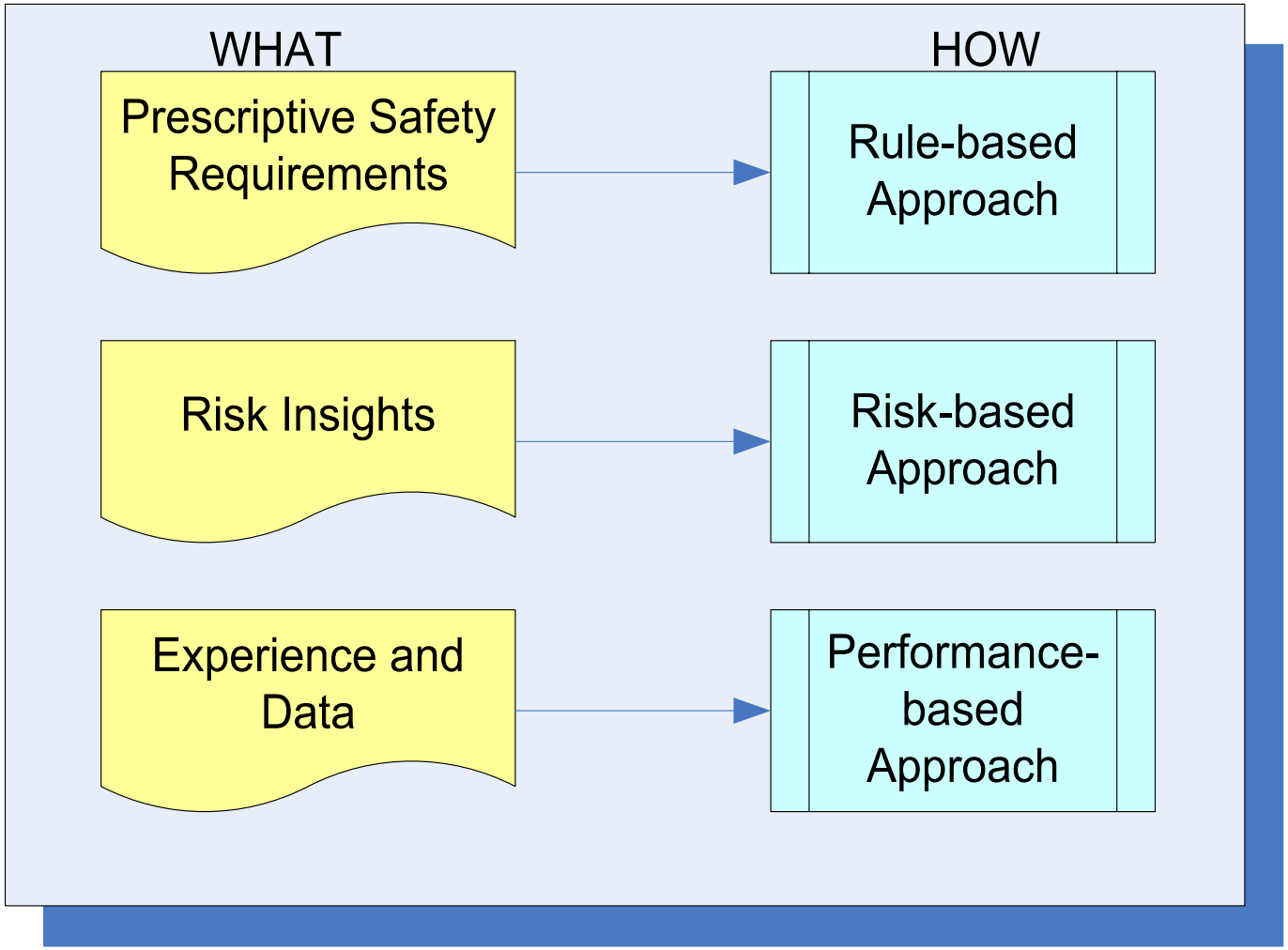
- Experience with traditional Failure Modes and Effects Analysis, Hazards Analysis and Fault Tree Analysis.
- Use of qualitative risk assessment and management (4X3 or 5X5 risk matrices) for project and program management.
- Improper use of a risk matrix for quantitative risk evaluation. It should be a communication tool, not an evaluation tool. It also does not reflect uncertainty because of abrupt changes of color.
- Overall Agency interest in and management support for performing quantitative risk assessments (QRA).
- Limited civil servant experience with and resources for QRA.
- Minimal corporate memory for QRA work and data.
- Minimal use of quantitative risk assessments in baseline safety assessments.

Goal: Incorporate Quantitative Techniques into Traditional System Assessments

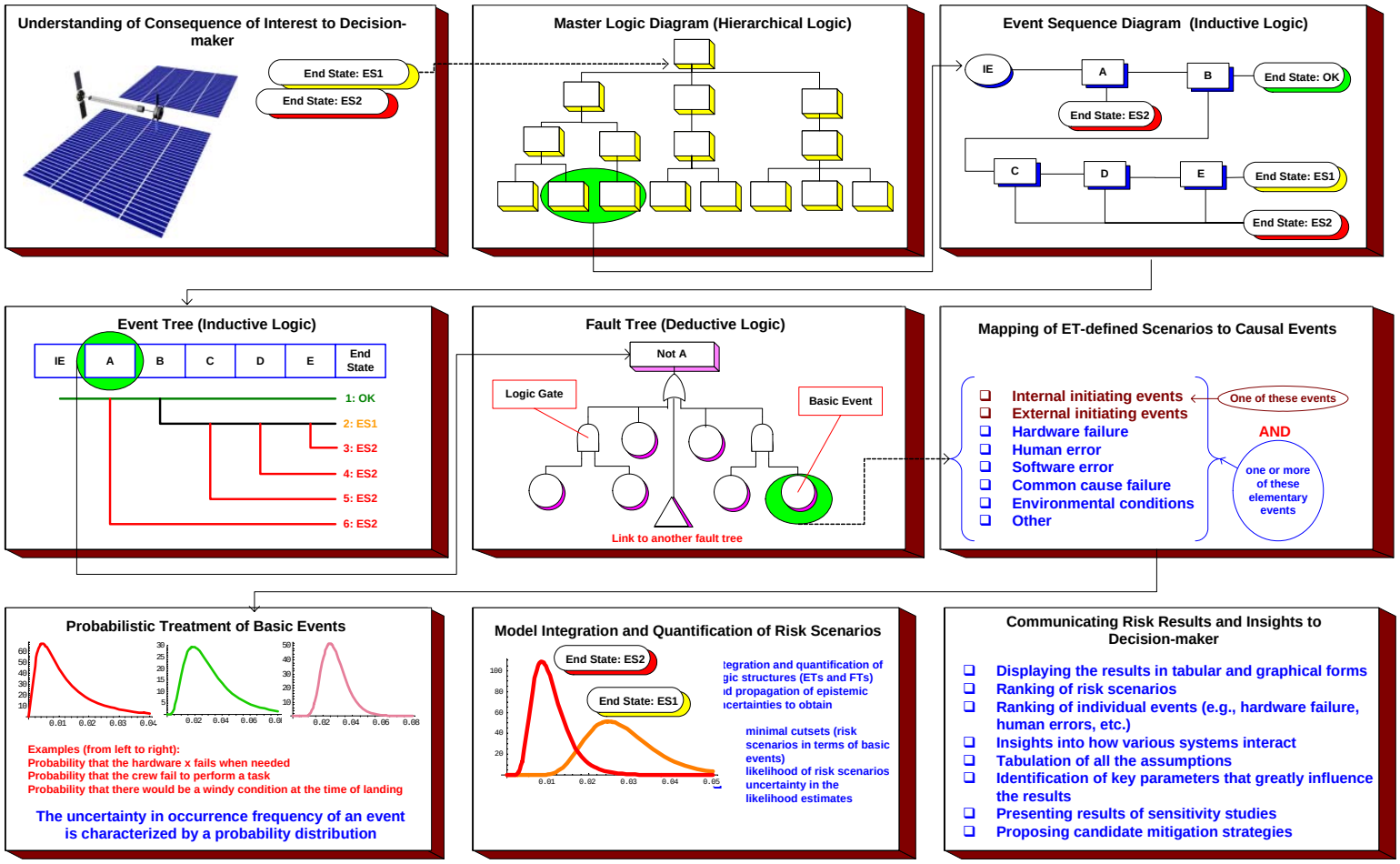


- **Quantitative Risk Assessment to be used to complement qualitative assessment of hazards.**
  - Traditional system safety analyses (hazard analysis, fault-tree analysis, and failure-modes-and-effects analysis) to be integrated into a coherent assessment process
- **Quantitative Risk Assessment (QRA) quantifies risk in terms of the likelihood and severity of (generally rare) events that are adverse to safety or mission success:**
  - Identifies a complete set of credible system failure modes
  - Captures interactions between events/systems/crews in an integrated modeling framework
  - Quantifies uncertainties and identifies what the system safety analysts know or do not know
  - Facilitates decision-making by identifying the dominant risk contributors, so that risk management decisions are targeted toward risk significant hazards

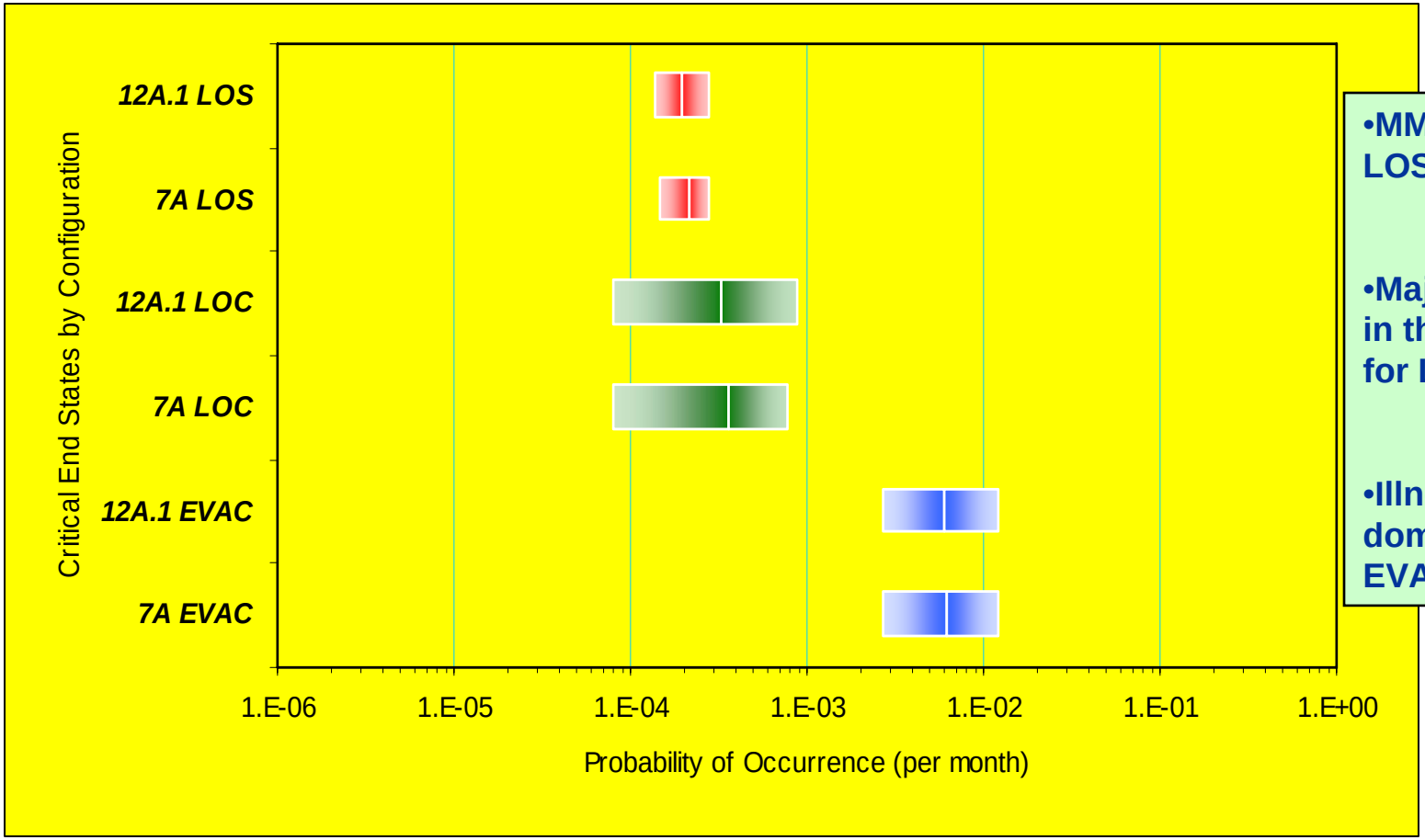
Different Approaches to Safety Assessment



Quantitative Risk Assessment Process



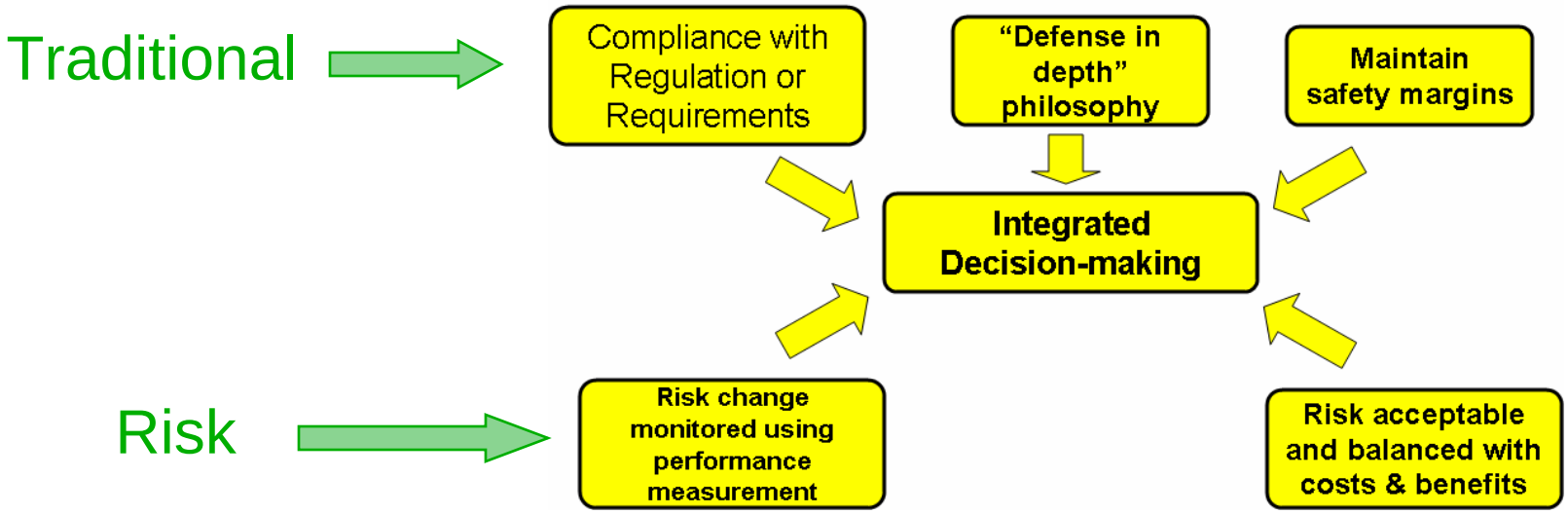
Conclusions from International Space Station QRA Results: Comparison of 7A with 12A.1



- **MMOD dominates LOS both cases**
- **Major uncertainties in the risk estimates for LOC both cases**
- **Illness in space dominates LOC and EVAC both cases**

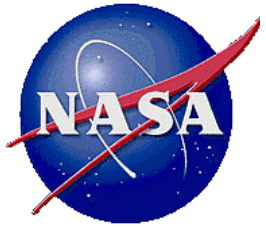
(Such conclusions could have not been drawn from traditional safety analyses)

Risk-Informed Decision Making Combines Traditional and Risk Concepts



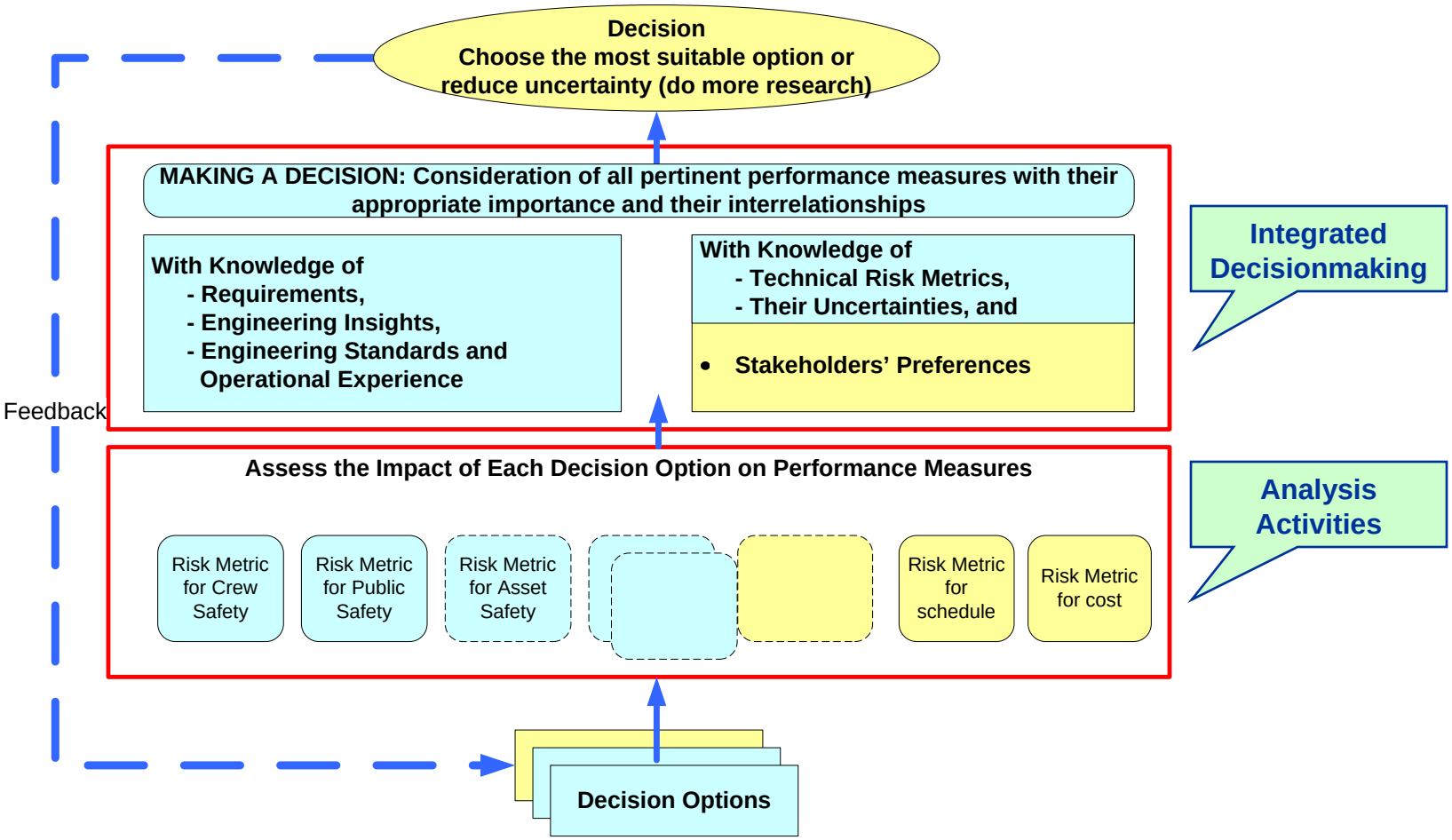
(Based on Nuclear Regulatory Commission approach)

How Risk-Informed Decision Making Works



- Consequences of decision options are modeled in terms of the performance measures or metrics (PM) relating to the program fundamental objectives
  - PM are attributes or their surrogates that are measurable
  - Example: PM for crew safety can be the probability of loss of crew
- Preferences (relative weights of key performance measures) are obtained from each stakeholder
  - Incorporate stakeholder views into the decision process
- Decision options are ranked according to their desirability
  - Compare consequences of decision options on the PM
- The most suitable decision option is selected through deliberation among stakeholders
  - Deliberate is any formal or informal process for communication and collective consideration of issues

Use of Risk Information to Support Decision Processes

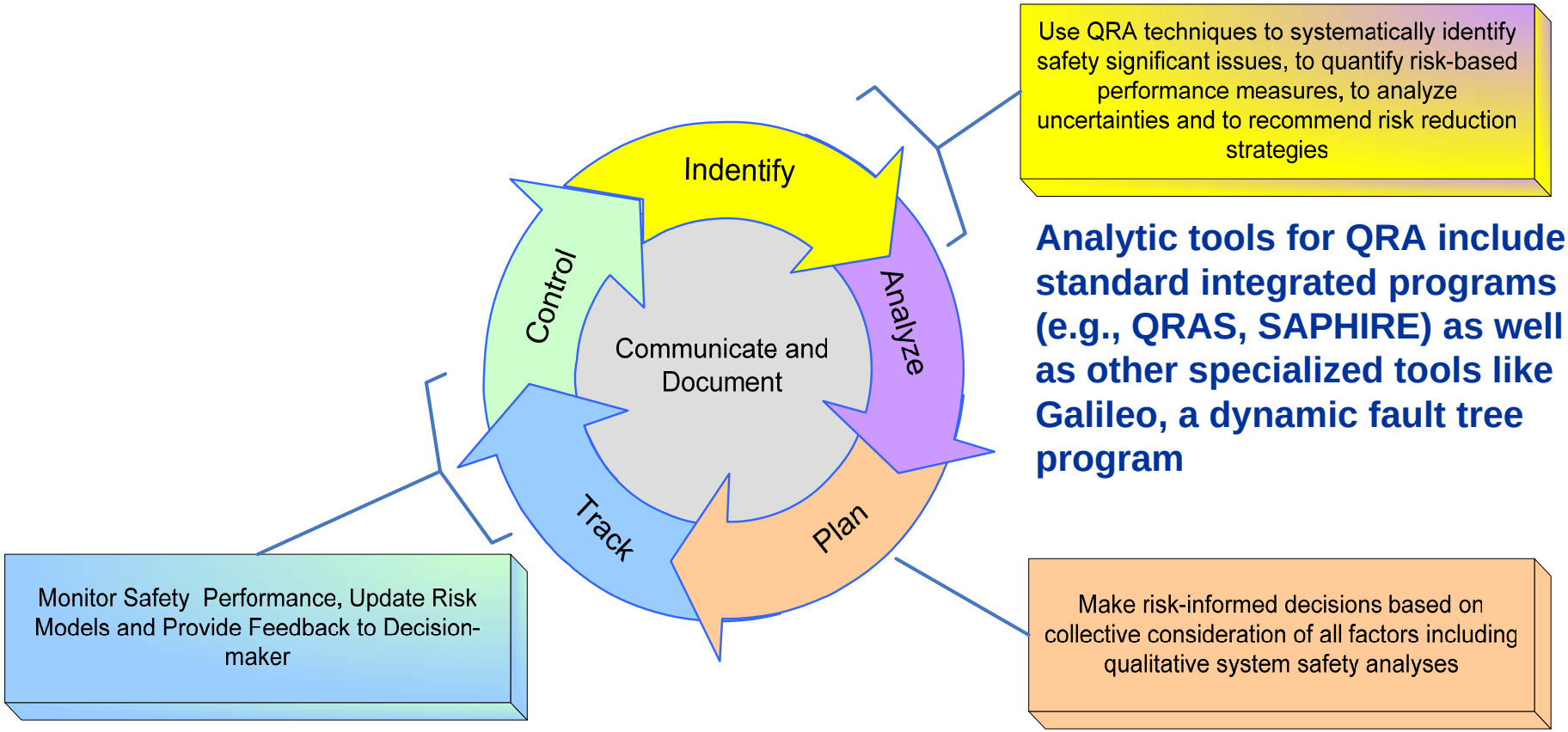


Example of Risk-Informed Decision in the International Space Station PRA

Postponed maintenance activities based on ISS PRA

- What are the risks in delaying maintenance actions until Orbiter arrives in order to increase the number of hours the crew can devote to science?
- Analysis showed that deferring all maintenance would decrease the number of science hours available because of increased probability of evacuation.
- PRA showed that science hours can be increased when maintenance is focused on risk drivers.
- Delaying non-essential maintenance actions does not impact safety

Risk-Informed Decision Making is Consistent with the CRM Process

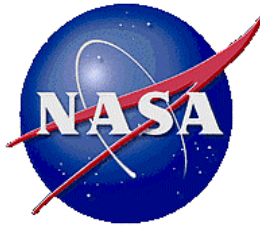


Analytic tools for QRA include standard integrated programs (e.g., QRAS, SAPHIRE) as well as other specialized tools like Galileo, a dynamic fault tree program

Analytic tools to monitor safety performance include assessment of precursors, failure trends, and root cause analysis of mishaps and accidents

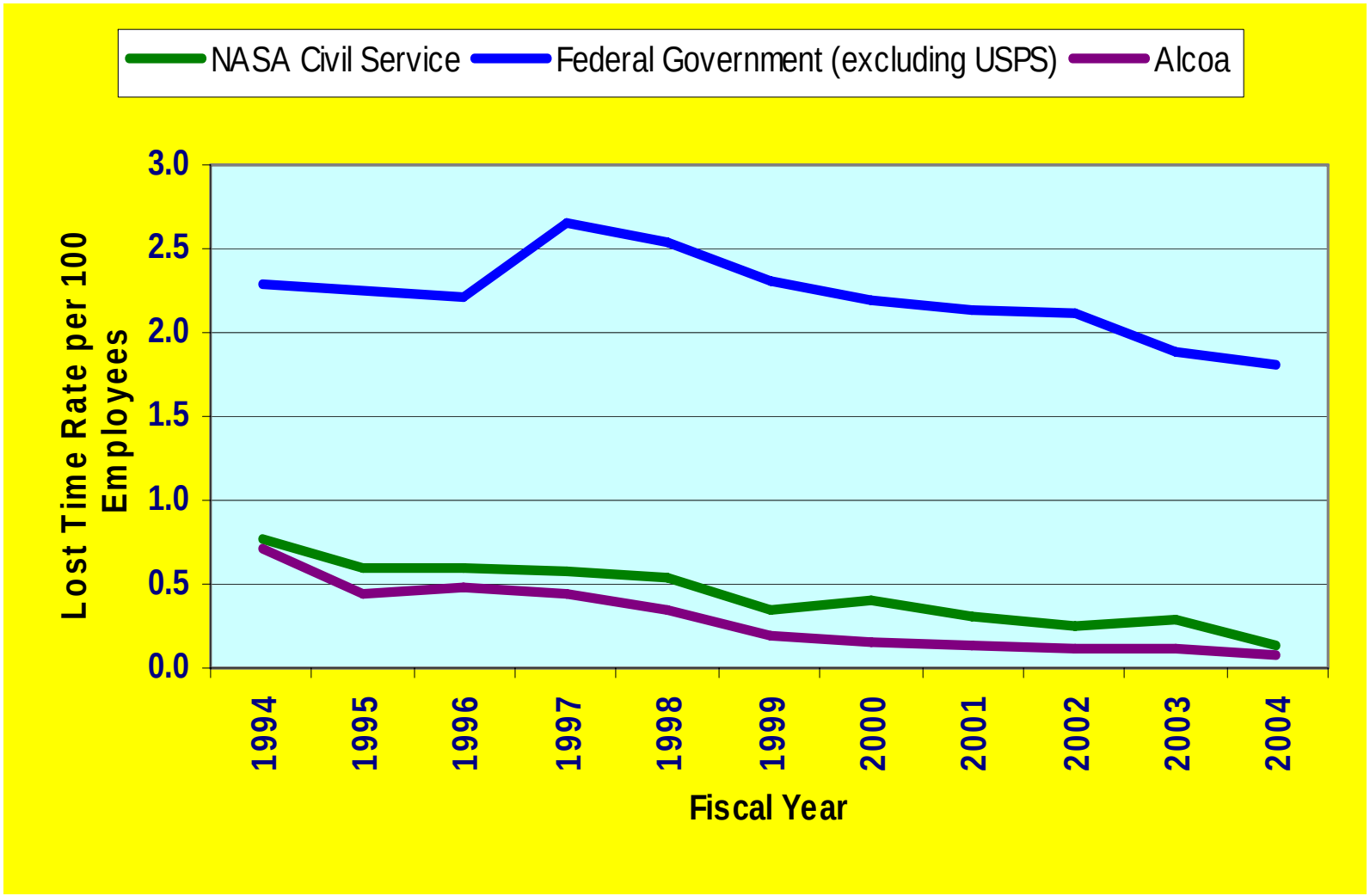
Analytic tools for risk-informed decision include methods like the Analytic Hierarchy Process (AHP) and associated software

Recent Use of Metrics in Safety

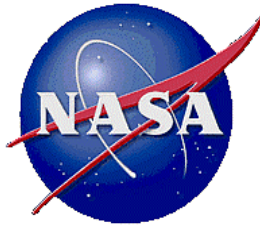


- Currently NASA monitors and periodically reports occupational health and safety performance of NASA workforce and contractors.
- The occupational safety metrics (use statistical data to) measure the adequacy of performance in protecting the safety and health of workforce.
- The reported metrics cover on a periodic basis
  - Deaths
  - Injuries
  - Property damage
  - Close calls
  - Lost time

Lost Time Rate Comparison: NASA vs. Federal Government and Industry Leader

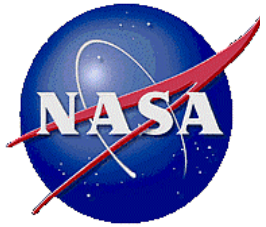


Higher Level Safety Performance Measures Are Needed



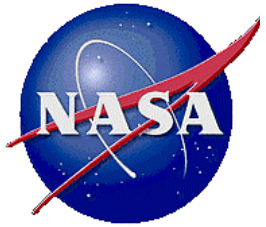
- To improve monitoring and to optimize safety
- We need systematic and comprehensive ways to directly measure safety performance in all life-cycle phases of missions including design.
- We perform FMEA, hazards, and other safety analyses for systems and programs but the results of these analyses do not readily reveal whether safety is improving, getting worse or staying the same unless the analyses are explicitly performed for comparison “before and after” a change.
- Also, it is difficult to establish if the improvement measures used are indeed the best that could be applied given available time and money.

Risk-Based Approach to Safety Performance Measures



- **Quantitative risk assessment (QRA) provides a systematic and logical quantitative basis for analyzing scenarios that can lead to mishaps and accidents and for sorting them into system and component contributions.**
- **Therefore, a QRA approach provides a convenient framework for identifying, structuring, and evaluating safety performance measures at different stages of design or operation.**
- **Also, QRA provides a convenient basis for linking safety performance with reliability performance.**

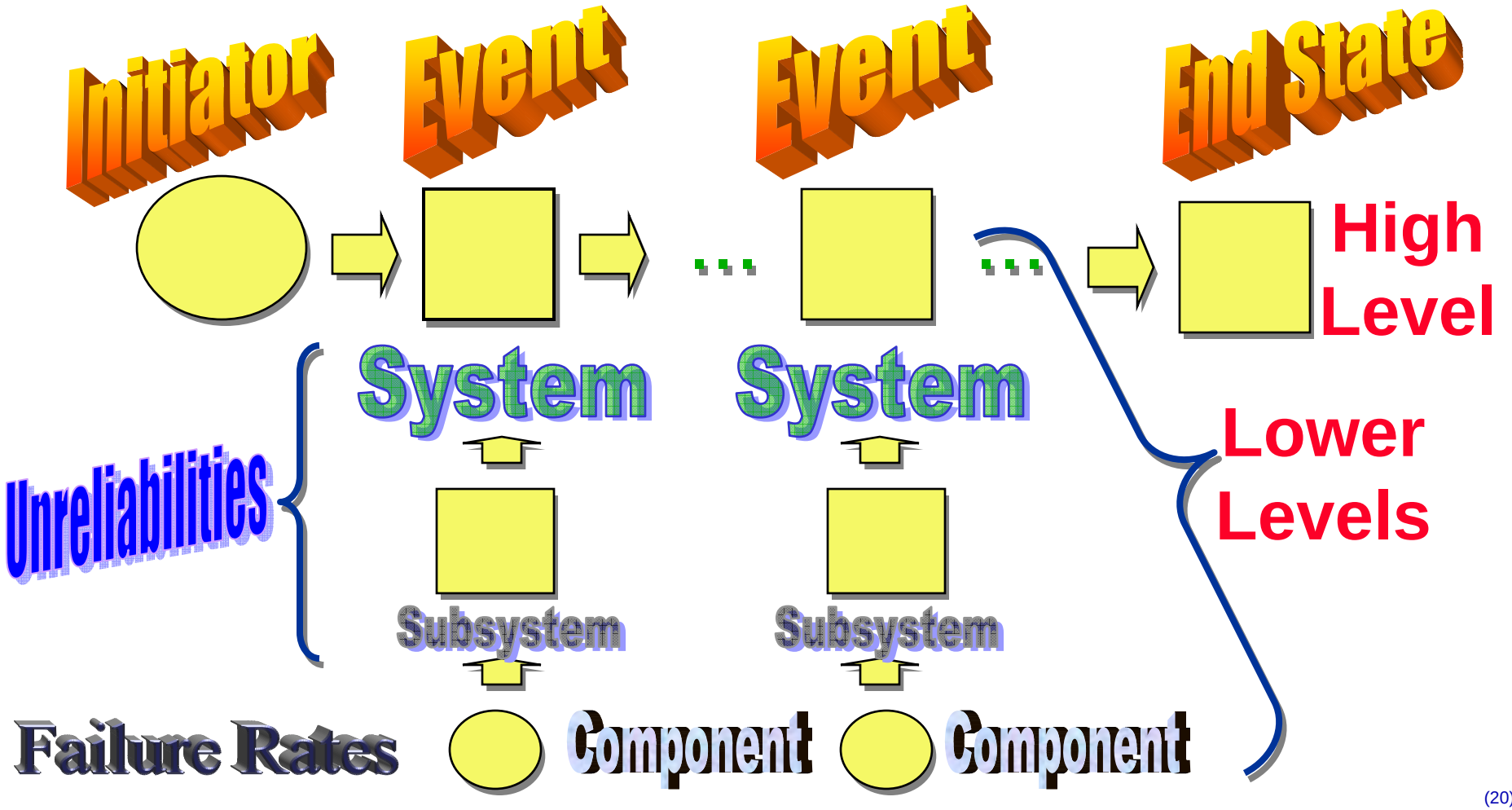
Tiers or Levels of Performance Measure



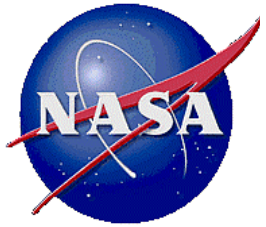
- **High-level safety performance measures are those that directly impact safety. These are often the undesired "end states" in a quantitative risk assessment.**
  - Examples: Loss of crew probability, loss of vehicle probability, loss of module probability, injury probability
- **Lower-level safety performance measures are described in terms of fundamental events or conditions that are determined to indirectly impact safety.**
  - Examples: System, subsystem, or component unreliability or unavailability

Structure of Performance Measure Levels through QRA

Consider an illustrative accident scenario:



Probabilistic Design



- Depends on *statistical or probabilistic characterization* of a variable to determine its *magnitude (or severity) and frequency (or probability)*
- Uses *best-estimate* values rather than conservative deterministic values
- Accounts for variability and other forms of uncertainty in a natural way, through calculated *uncertainty distributions*
- The *levels of redundancy* recommended are not arbitrary but dictated by *risk importance*
- If significant amounts of historical data exist, risk metrics can be calculated using *statistical (actuarial)* methods
- For *new designs* and for preventing/mitigating *rare high-consequence events*, *probabilistic risk assessment (PRA)* methods are used.

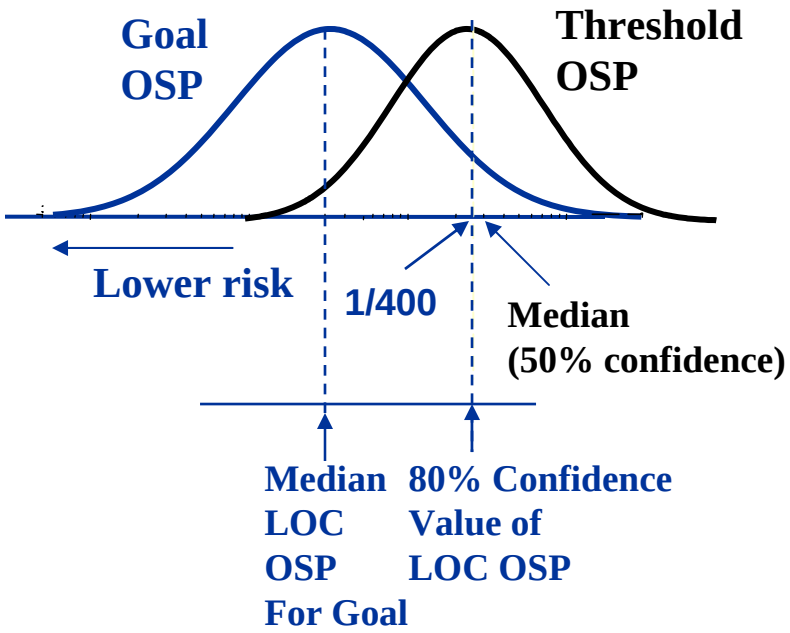
Orbital Space Plane Design Safety Requirements Stated through QRA

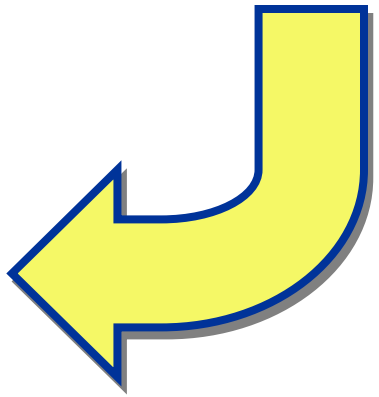
Threshold {

Goal {

Orbital Space Plane (OSP)

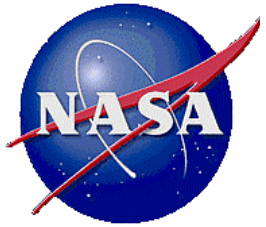
English:	Design safer than Shuttle
QRA:	1/400 for LOC @ 50% confidence
English:	High confidence that design is safer than Shuttle
QRA:	1/400 for LOC @ 80% confidence





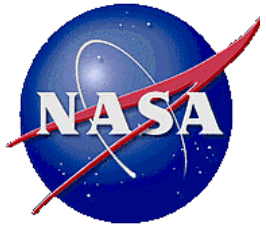
LOC – Loss of Crew

Transition to a Risk-Informed Environment



- Develop and maintain a larger cadre of experienced center risk assessment personnel who can understand and participate in risk informed decision making. NASA HQ to lead the effort. Expert PRA Groups, one at each center
- Adopt NASA-wide baseline risk-informed procedures, standards and tools
- Incorporate QRA into system safety
- Baseline performance based safety assessment into safety assessment
- Establish and maintain risk-informed databases for NASA application categories
- Incorporate performance based safety assessment into design
- Integrate and coordinate risk-informed safety assessments throughout NASA

Safety and Risk Capabilities Needed to Support Exploration Programs



- Failure rate database for reliability and risk assessments
- Expanded phenomenological models and data
- Performance based safety and reliability design methods
- Human reliability methods and data
- Nuclear safety assessment methods and data
- Methods and data to assess nuclear criticality hazards in space
- Models to assess accidental reentries and outer space contamination (expand current planetary protection program beyond biohazard)
- Structured decision-making tools to integrate performance, safety, risk, and cost