NASA's Lessons from Loss:
Managing Risk for Bold New Missions and Building on a Unique Safety Culture

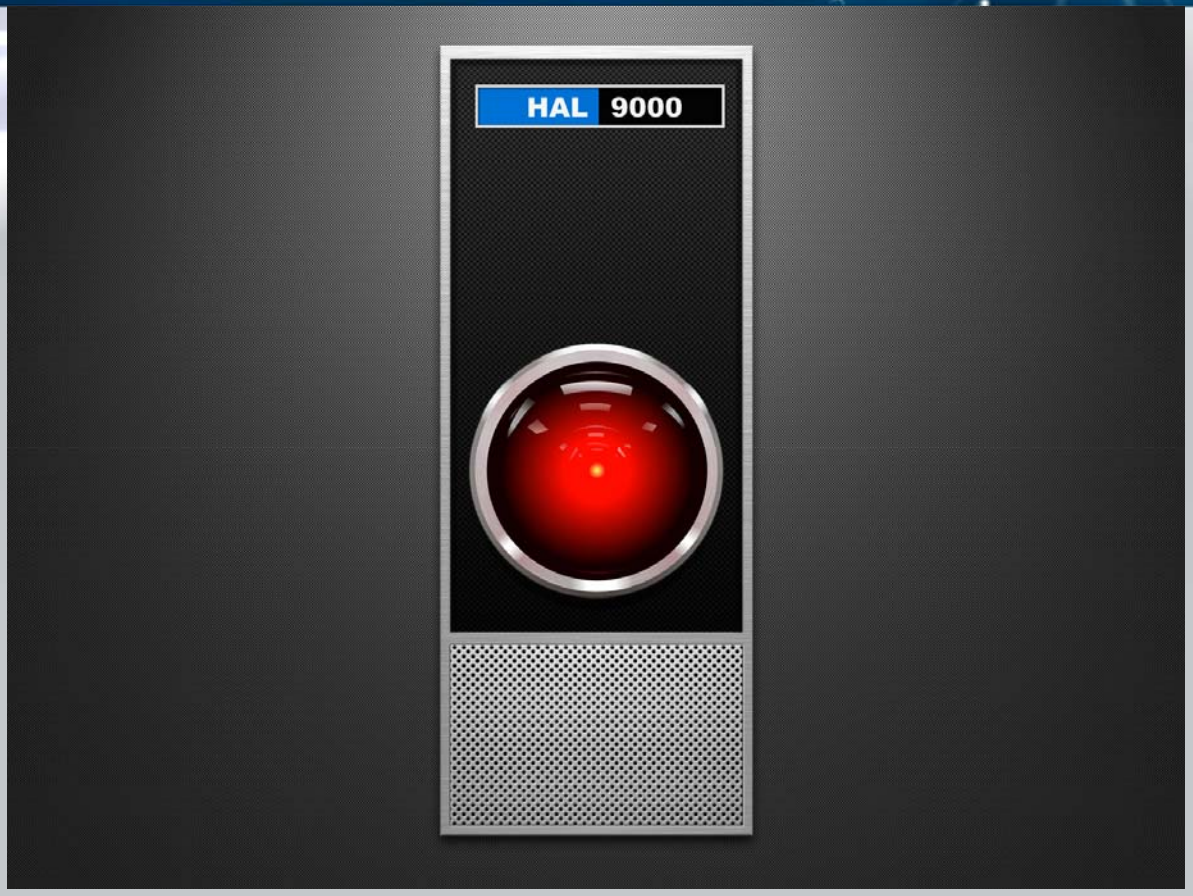
David Loyd
Johnson Space Center
Safety & Test Operations

ENERGIZING RISK MANAGEMENT
PRIMA'S 2015 ANNUAL CONFERENCE • JUNE 7–10, 2015 // HOUSTON, TX

NASA Johnson Space Center
HOUSTON, TEXAS

What's NASA Doing Now

Words of Wisdom



"It can only be attributable to human error."

-- HAL 9000 (2001: A Space Odyssey)

NASA Lessons Learned

- **NASA's Recent Losses in Space and on the Ground**
  - Failure is not an option we want to choose, but it is a reality….
- **The NASA Safety Culture**
  - Using the Safety Culture Model to Analyze NASA's History
  - Measuring Safety Culture
  - Safety "Beyond the Numbers"
- **A Rejuvenated Risk Management Environment**
  - Risk informed decision-making
  - A process for identifying and addressing dissent
  - Improved risk management processes in mission planning….

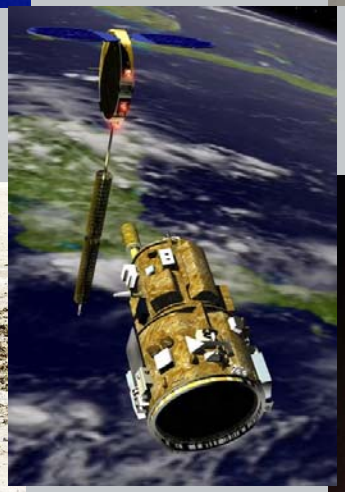
    …. and out in the trenches

NASA's Losses

Recent Mission Mishaps

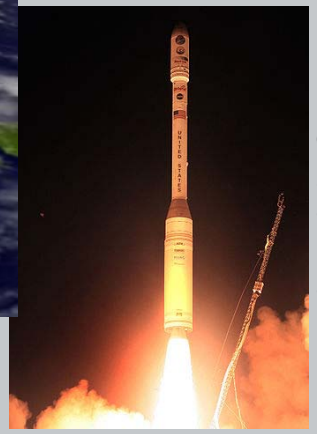
Columbia STS-107, February 1, 2003:
- 7 fatalities;
- $3 Billion vehicle loss;
- 2.5 year mission impact.

NOAA N-Prime, September 6, 2003:
- $135 Million vehicle damage;
- 5.5 year mission impact.

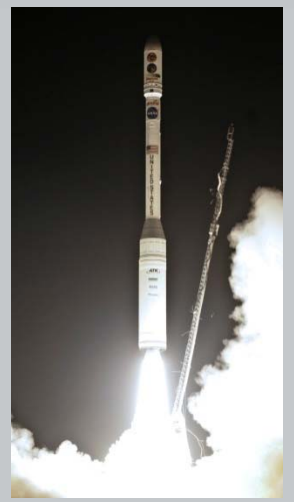


DART, April 16, 2005:
- Proximity operations mission objectives lost.

Genesis, September 8, 2004:
- Some sample retrieval materials lost.



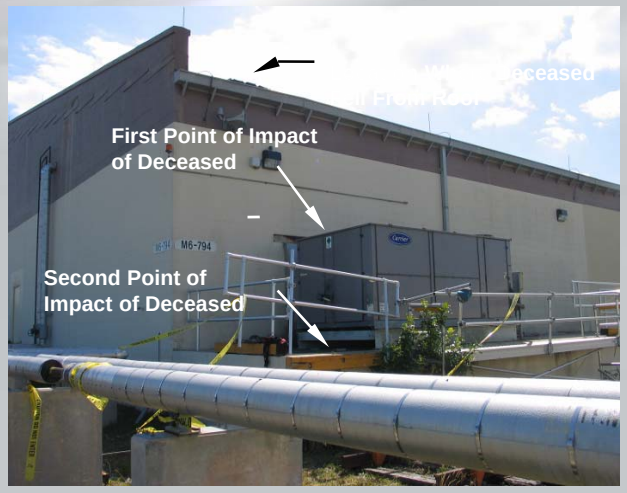
OCO, February 24, 2009:
- $280 Million vehicle loss;
- 5+ year mission impact.



Glory, March 4, 2011:
- $424 Million vehicle loss;
- ??? mission impact.

NASA's Losses

Recent Institutional Mishaps



KSC Roofing Fatality, March 17, 2006

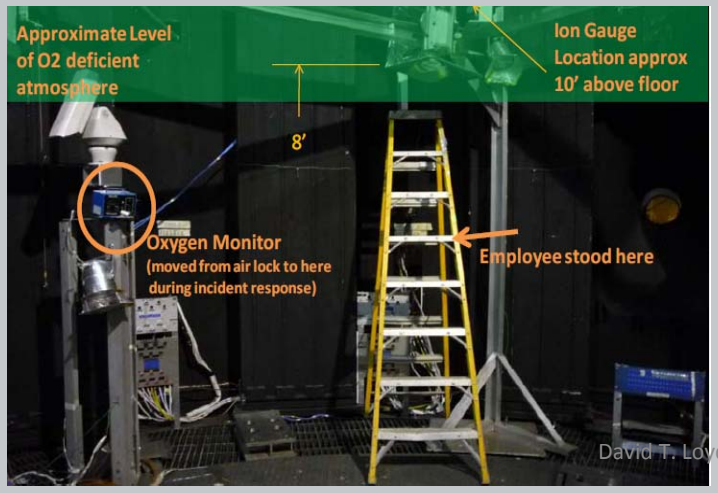
- Subcontractor died from head injuries suffered due to fall.

MSFC Freedom Star Tow-wire Injury, December 12, 2006

- Hospitalization due to internal injuries from impact with SRB tow-wire.

JSC Chamber B Asphyxiation, July 28, 2010

- Shoulder injury due to asphyxiation and fall.



WFF CNC Injury, October 28, 2010

- Sub-dermal tissue damage due to impact from machine tool shrapnel.

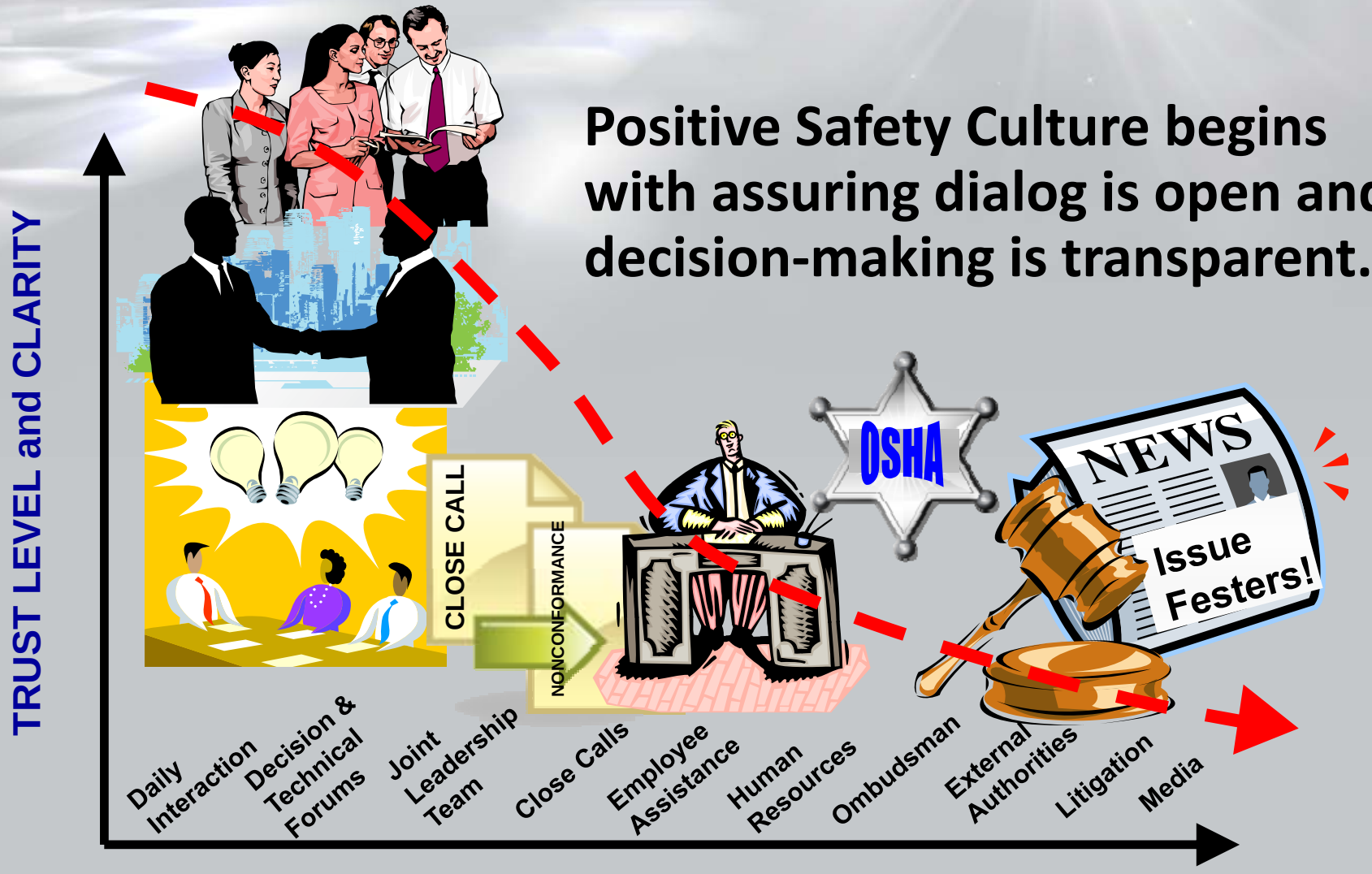
What is the impact of Human Factors and Safety Culture on the Mishap Environment?

- Estimates range from 65-90% of catastrophic mishaps are due to human error.
  - NASA's human factors-related mishaps causes are estimated at ~75%

- As much as we'd like to error-proof our work environment, even the most automated and complex technical endeavors require human interaction…and are vulnerable to human frailty.

- Industry and government are focusing not only on human factors integration into hazardous work environments, but also looking for practical approaches to cultivating a strong Safety Culture that diminishes risk.

Addressing Barriers to Trust

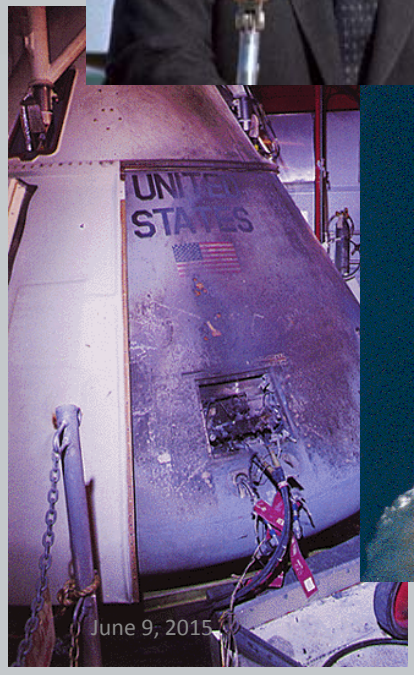


Positive Safety Culture begins with assuring dialog is open and decision-making is transparent.

The NASA Safety Culture

"I believe that this nation should commit itself to achieving the goal, before this decade is out, of landing a man on the moon and returning him safely to the earth."

– John F. Kennedy address to Congress, May 25, 1962



- **Space-related tragedies have marked our safety culture evolution.**
- **It's not possible to perpetuate a safety culture in space without taking care of each other on the ground and at home.**

The NASA Safety Culture

NASA Safety Culture Working Group, consisting of membership from each NASA Center, has been active since early 2009.

- **NASA's Definition of Safety Culture –**

  "An environment characterized by safe attitudes and behaviors modeled by leaders and embraced by all that fosters an atmosphere of open communication, mutual trust, shared safety values and lessons, and confidence that we will balance challenges and risks consistent with our core value of safety to successfully accomplish our mission."

NASA's Safety Culture Model

An effective safety culture is characterized by the following subcomponents:

Reporting Culture
We report our concerns

Just Culture
We have a sense of fairness

Flexible Culture
We change to meet new demands

Learning Culture
We learn from our successes and mistakes

Engaged Culture
Everyone does his or her part

Catastrophic Event Impact

Using the Safety Culture Model to Analyze NASA's History

Apollo 1 – January 27, 1967

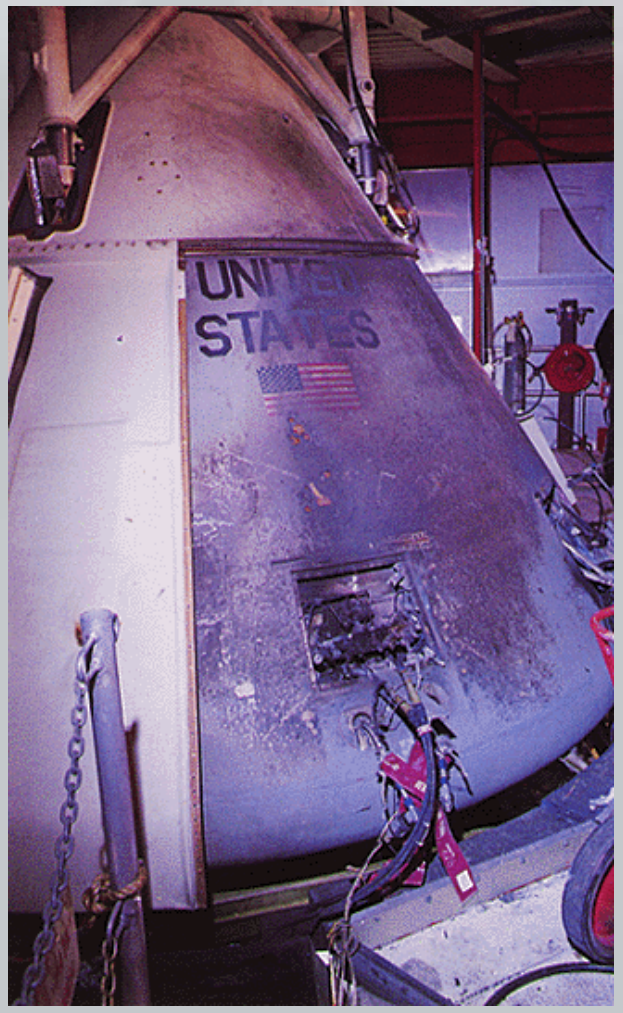
Reporting – Procedures were subjected to last-minute changes that were not tracked, recorded or communicated.

Just – Absence of information on this factor attests to the general neglect at the time of organizational behavior as a key factor in mishaps.

Flexible – Willingness to change was weak in the presence of compelling important information.

Learning – NASA failed to appreciate the significant hazards of a 100% oxygen environment.

Engaged – NASA provided insufficient surveillance over its own management functions.



Catastrophic Event Impact

Using the Safety Culture Model to Analyze NASA's History

Apollo 13 – April 13, 1970

Reporting – Incomplete and sometimes incorrect information was used in problem solving.

Just – Absence of information on this factor attests to the general neglect at the time of organizational behavior as a key factor in mishaps.

Flexible – Demonstrated ability to adapt quickly to an emergency although flexibility prior to the mishap is unclear.

Learning – While safeguards had been implemented following the Apollo 1 fire, key aspects of design, workmanship, and material use remained vulnerable to oxygen flammability.

Engaged – Solutions immediately following the oxygen tank explosion represent an engaged team.

Catastrophic Event Impact

Using the Safety Culture Model to Analyze NASA's History

Challenger – January 28, 1986

Reporting – Ineffective problem reporting requirements and practices.

Just – Stifled communication regarding O-ring susceptibility to cold conditions.

Flexible – Launch concerns were dismissed in the face of significant schedule pressure.

Learning – Trend analysis was inadequate as evidenced by identification of a number of burn-through events which occurred prior to STS-51L.

Engaged – NASA management lacked involvement in critical discussions.

Catastrophic Event Impact

Using the Safety Culture Model to Analyze NASA's History

Columbia – February 1, 2003

Reporting – Foam shedding was a known problem, yet foam impact data was sill being analyzed at the time of the flight, and not considered a serious hazard.

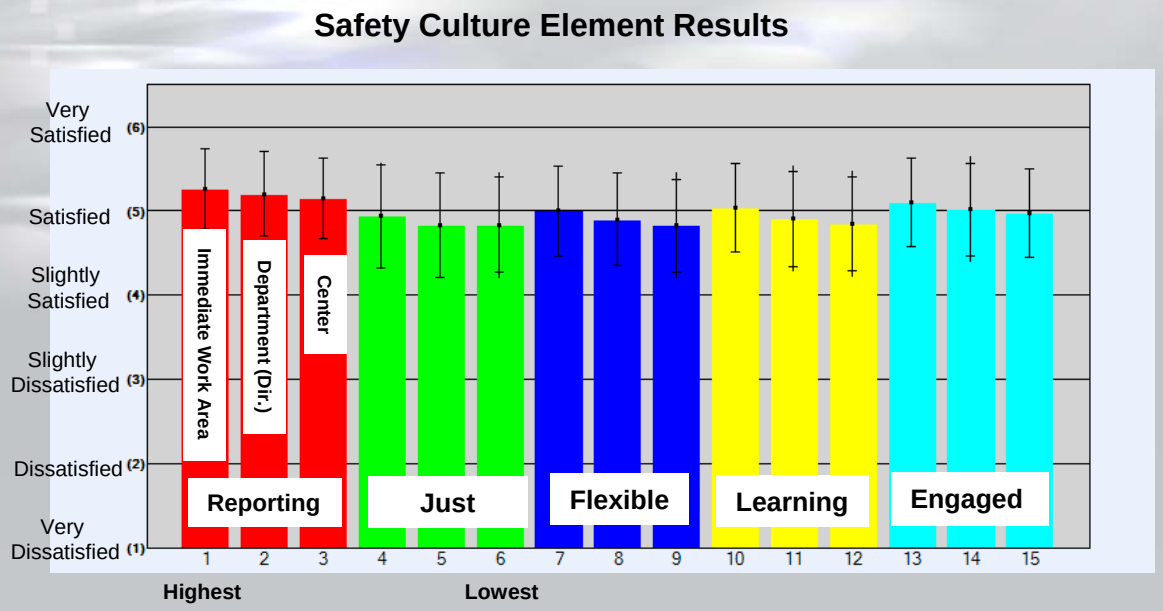
Just – Some engineers were reluctant to raise concerns when faced with a return of an "in God we trust - all others bring data" attitude.

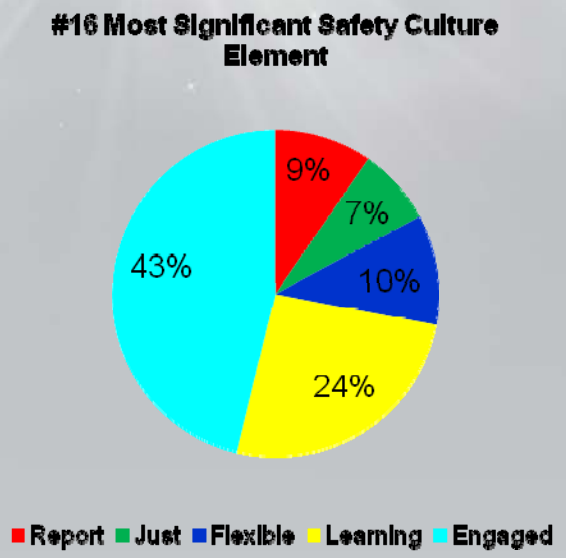
Flexible – Like the Challenger mishap, the Shuttle Program was experiencing schedule pressure challenges.

Learning – With "normalization of deviance," foam had become classified as "in-family" and as a negligible risk to the orbiter.

Engaged – "Echos" of the Challenger mishap were evident.

Measuring Safety Culture





JSC Results:

- **Ratings were VERY similar with KSC and MSFC – ratings in the satisfied range.**
- **"Reporting Culture" was rated highest, while "Engaged Culture" was valued most.**
- **97% of JSC employees feel safe working at the Center.**
- **95% of JSC employees agreed they are responsible for their safety and their co-worker's safety**
- **Comments were both positive and negative.**
- **Results have been communicated with senior staff and multiple employee forums.**

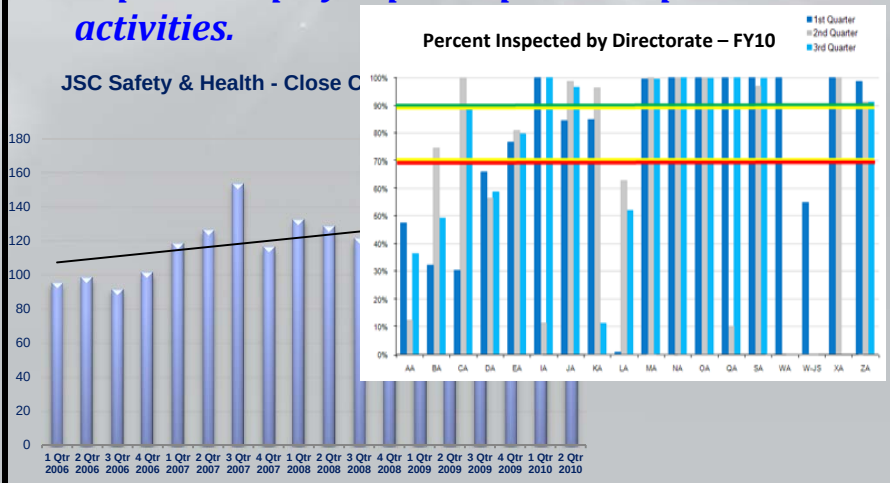
Safety "Beyond the Numbers"

Leadership

Continue to encourage safe behaviors, attitudes, and employee involvement.

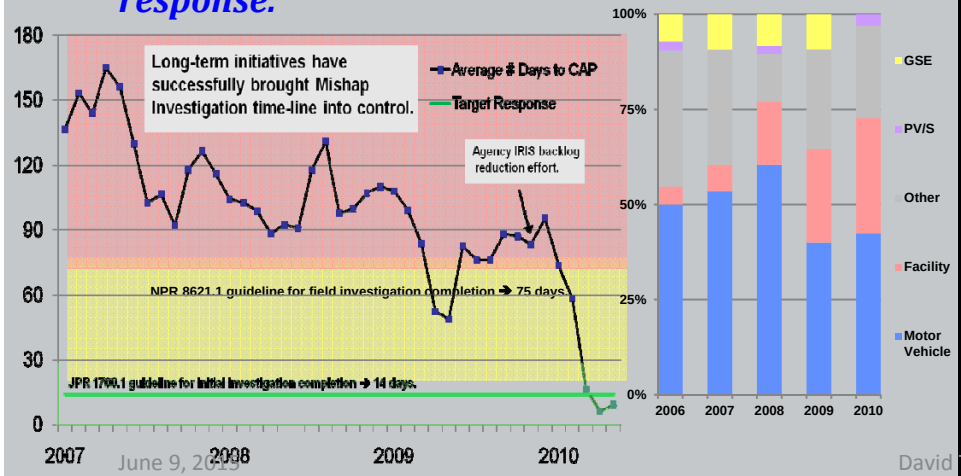
Prevention

Improve employee participation in prevention activities.



Reaction

Reduce mishaps and improve investigation response.



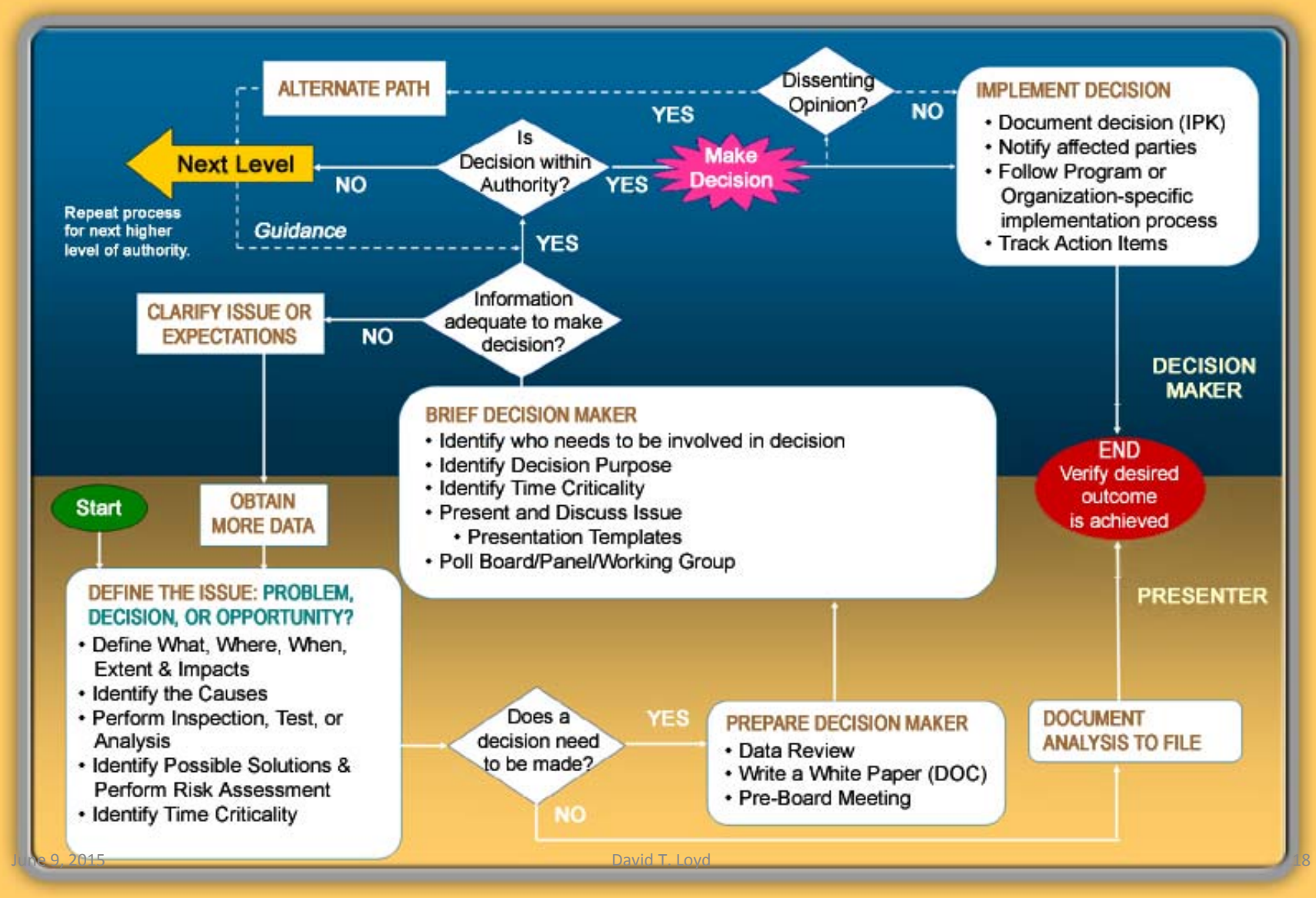
Issue Resolution

Assure response to challenges reflect thoughtful approach to risk mitigation.

PA-1 -- Challenging, safe and successful collaboration between:

- Johnson Space Center
- Dryden Flight Research Center
- Langley Research Center
- JSC White Sands Test Facility
- US Army White Sands Missile Range
- Orbital Sciences
- Alliant Techsystems
- Aerojet

NASA Decision Model



NASA Dissenting Opinion Process

NASA Policy Directive 1000.0, *"NASA Governance and Strategic Management Handbook"*

- In assessing a decision or action, there are three choices:
  1. agree,
  2. disagree but willing to support,
  3. or disagree and raise a *Dissenting Opinion*.
- A *"Dissenting Opinion"* is a substantive disagreement with a decision that is judged not in the best interest of NASA.
- A Dissenting Opinion must be supportable and based on a sound rationale.

NASA Dissenting Opinion Process - Resolution

Key steps of the Dissenting Opinion resolution process are:

1. Disagreeing parties must jointly establish the facts agreed upon;
2. The parties jointly present to the next higher level of authority; and
3. If the dissenter is not satisfied with the process or outcome, the dissenter may appeal to the next higher level of management. The dissenter has the right to take the issue upward through the organization, even to the NASA Administrator, if necessary.

Risk Assessment Concepts & Requirements

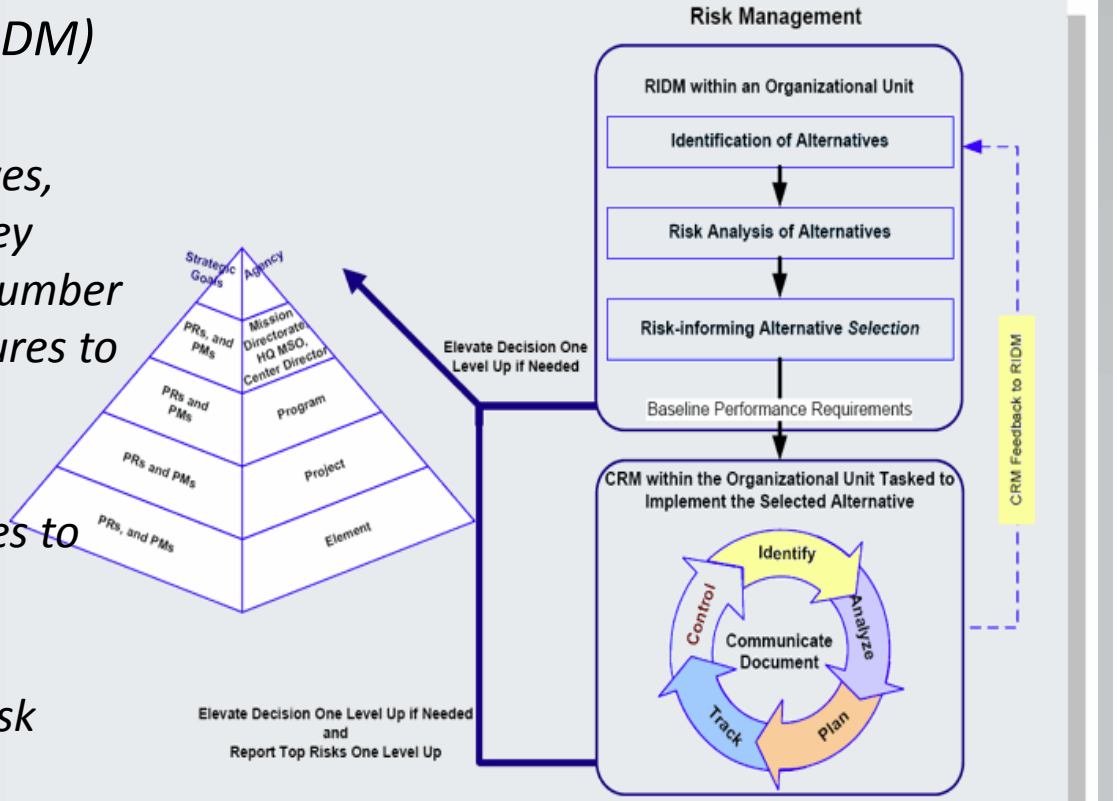
NPR 8000.4, *Agency Risk Management Procedural Requirements*

Risk Informed Decision-Making (RIDM) involves:

(1) Identification of decision alternatives, recognizing opportunities where they arise, and considering a sufficient number and diversity of performance measures to constitute a comprehensive set for decision-making purposes.

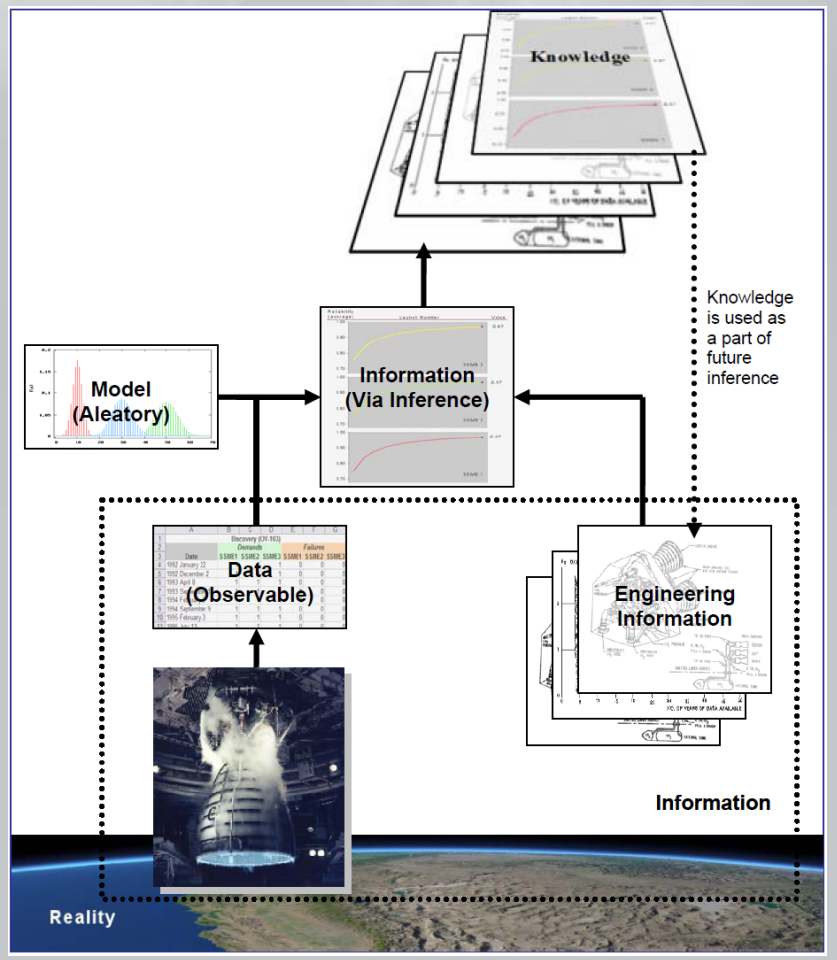
(2) Risk analysis of decision alternatives to support ranking.

(3) Selection of a decision alternative informed by (not solely based on) risk analysis results.



Probabilistic Risk Assessment (PRA)

- PRA integrates models based on systems engineering, probability and statistics, reliability and maintainability engineering, physical and biological sciences, decision theory, and expert opinion.
- PRA is needed when decisions need to be made that involve high stakes in a complex situation.
- The collection of risk scenarios allows the dominant risk factors to be identified, then modified or eliminated to improve the probability of success.



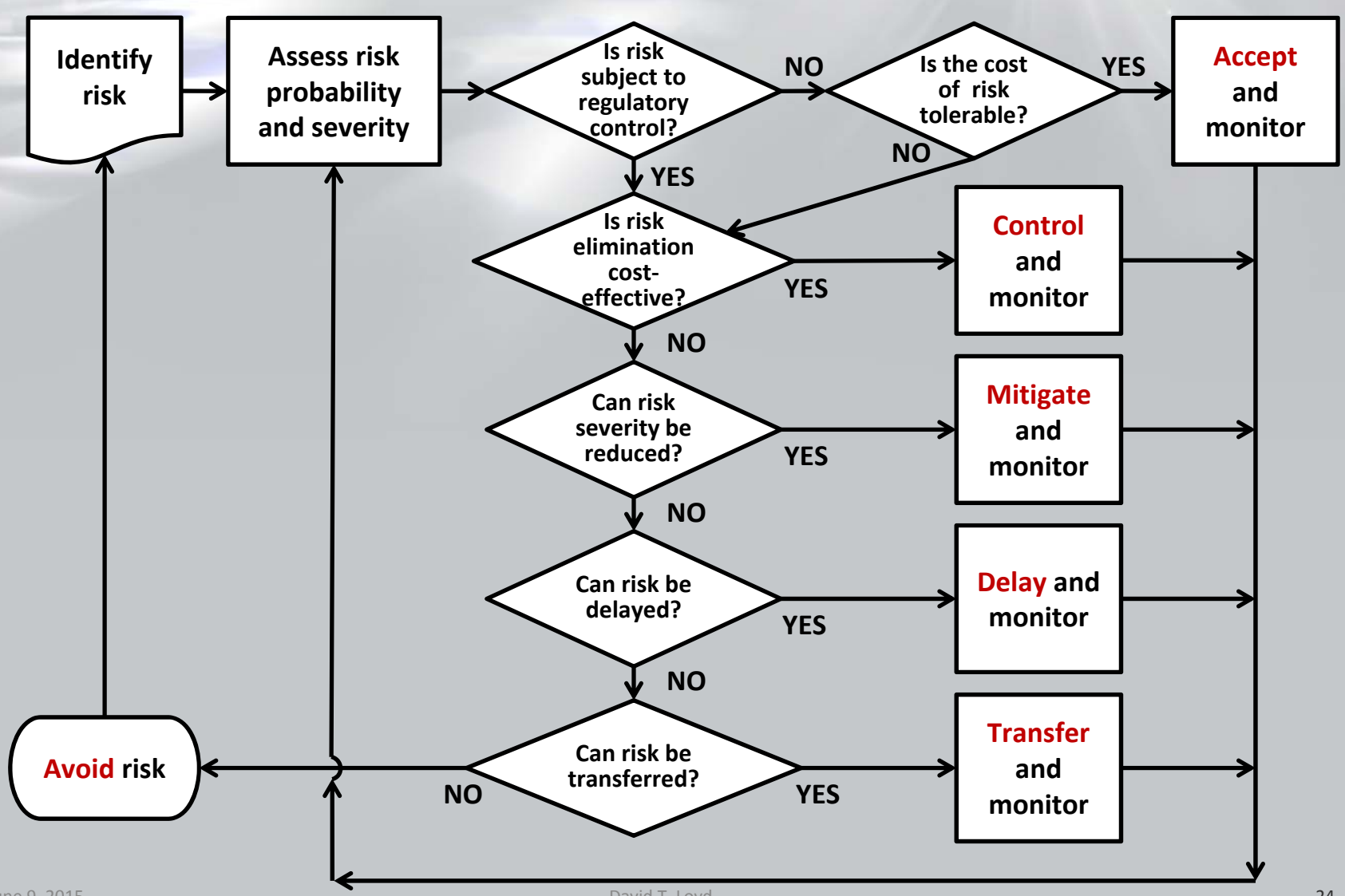
Representing the World via Bayesian Inference.

High Risk Occupations vs. Space Flight

Miner risk does not include fatalities due to chronic illnesses like “black lung”

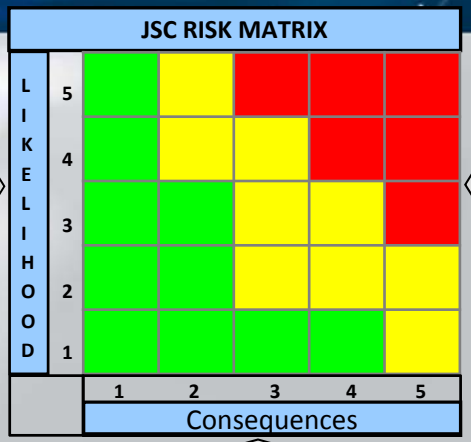
Risk increases as “drill down” into smaller and smaller groups that drive the risk. Shuttle Astronaut risk is a very small group that has high risk

Simplified Risk Management Flow



Risk Scorecard

LIKELIHOOD			
	5	Very Likely	Expected to happen. Controls have minimal to no effect.
	4	Likely	Likely to happen. Controls have significant limitations or uncertainties.
	3	Possible	Could happen. Controls exist, with some limitations or uncertainties.
	2	Unlikely	Not expected to happen. Controls have minor limitations or uncertainties.
	1	Highly Unlikely	Extremely remote possibility that it will happen. Strong controls in place.



SEVERITY

- High – Mitigate; implement new processes, change requirements, or re-baseline
- Moderate – Manage/consider alternative processes, or Accept
- Low – Manage within normal processes; or Close

CONSEQUENCE	*Subcategories*	1	2	3	4	5
HSE (Health, Safety, Environment)	*Personnel*	Minor injury; Minor OSHA violation	Short-term injury; Moderate OSHA violation	Long-term injury, impairment or incapacitation; Significant OSHA violation	Permanent injury or incapacitation; Major OSHA violation	Loss of life
	System, Facility	Minor damage to asset	Moderate impact or degraded performance	Loss of non-critical asset	Damage to a critical asset	Loss of critical asset or emergency evacuation
	Environment	Minor or non-reportable hazard or incident	Moderate hazard or reportable violation	Significant violation; Event requires immediate remediation	Major violation; Event causes temporary w ork stoppage	Catastrophic hazard
TECHNICAL	*Performance*	Minor impact to mission objectives or requirements	Incomplete compliance w ith a key mission objective	Noncompliance; Significant impact to mission	Noncompliance; Major impact on Center or Spaceflight mission	Failure to meet mission objectives
CENTER CAPABILITIES	*Infrastructure*	Minor impact or reduced effectiveness	Moderate impact or damage to infrastructure	Significant damage to infrastructure or reduced support	Mission delays or major impacts to Center operations	Extended loss of critical capabilities
	Workforce	Minor impact to human capital	Moderate impact to human capital	Significant impact; Loss of critical skill	Major impact; Loss of skill set	Loss of Core Competency
COST	*Organizational or CMO Impact*	<2% Budget increase or <$1M CMO Threat	2-5% Budget increase or $1M-$5M CMO Threat	5-10% Budget increase or $5M-10M CMO Threat	10-15% Budget increase or $10M-$60M CMO Threat	>15% Budget increase or >$60M CMO Threat;
SCHEDULE	--	Minor milestone slip	Moderate milestone slip; Schedule margin available	Project milestone slip; No impact to a critical path	Major milestone slip; Impact to a critical path	Failure to meet critical milestones

HSE Panel Review (Risk Validation)

Objectives:

- Better understanding of institutional risks with health, safety, environment (HSE) consequences
- Center-level consistency in HSE consequence assessment
- Better inform Center risk decision process about severity of HSE consequences

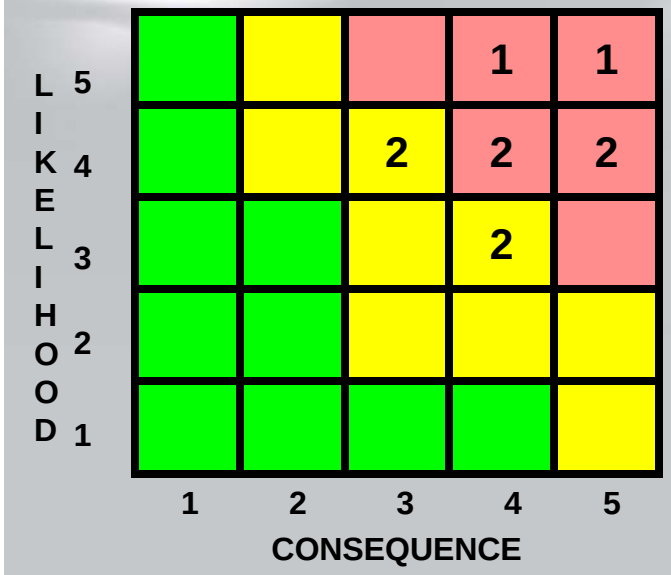
Approach:

- SMEs review risks in the HSE domain, and associated mitigation parameters
- SMEs advise risk owners and the JSC Risk Management Working Group (RMWG)
- Direct involvement by SMEs from Occupational Safety & Health, Environments, Facility Safety, and other disciplines in determining HSE consequence severity, analysis, and mitigation

Benefits:

- Helps risk owners assess consequence severity in HSE domain **and** improve mitigation plans
- Introduces quantitative methods commensurate to risk / uncertainty levels
- Helps risk-inform Center-level decisions related to: budget allocations, unfunded mandates, and compliance/ noncompliance with regulations, etc.
- Helps aggregate risks and consequences in the HSE domain

Institutional Risk Management



Legend

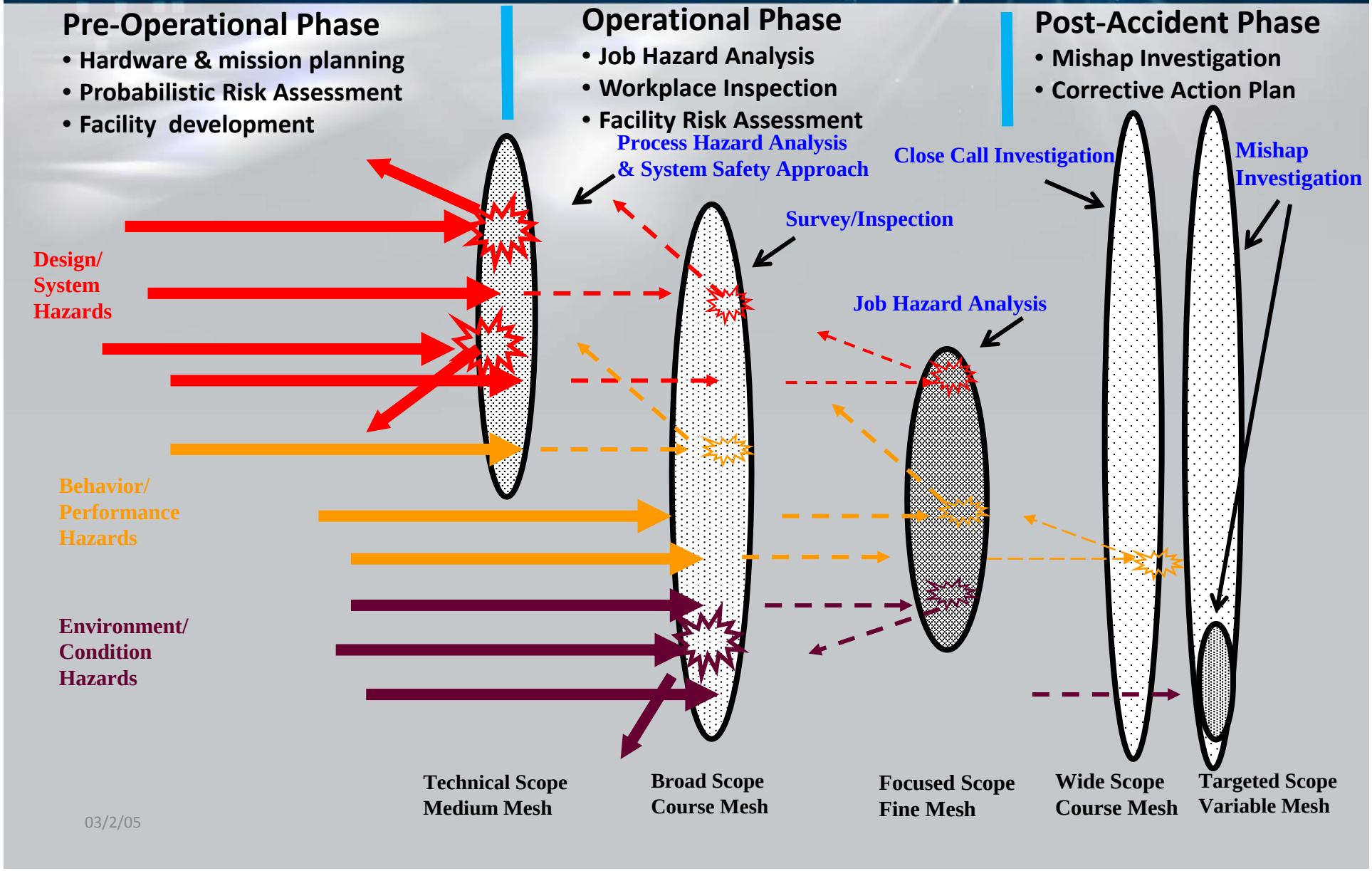
▲ Top Center Risk (TCR)

△ Proposed Top Center Risk (Proposed TCR)

L x C	Title (Notional Risk Titiles)	Org	LIKELIHOOD	Consequence				
				Cons Cap	SCHED	COST	HSE	TECH
3 x 4	▲ Test system maintenance	##	3	2	2	4	4	2
4 x 5	▲ Mission essential resource limitations	##	4	4	5	2	1	4
4 x 3	▲ Equipment End-of-Life	##	4	3	1	1		3
4 x 3	▲ Building Refurbishments	##	4	3	3	1	1	2
5 x 5	▲ Comm Systems End-of-Life	##	5	5	4	3	5	5
4 x 4	▲ Building Maintenance Shortfall	##	4	3	3	4	2	2
3 x 4	▲ Asbestos abatement	##	3	2	3	2	4	3
4 x 4	▲ Capability Threat	##	4	4	3	1		4
4 x 4	▲ Water System-Repairs/Upgrades	##	4	4	4	4	2	3
5 x 4	△ Research equipment failure threat	##	5		4	4		4

NOTIONAL DATA

Risk/Hazard Identification Processes



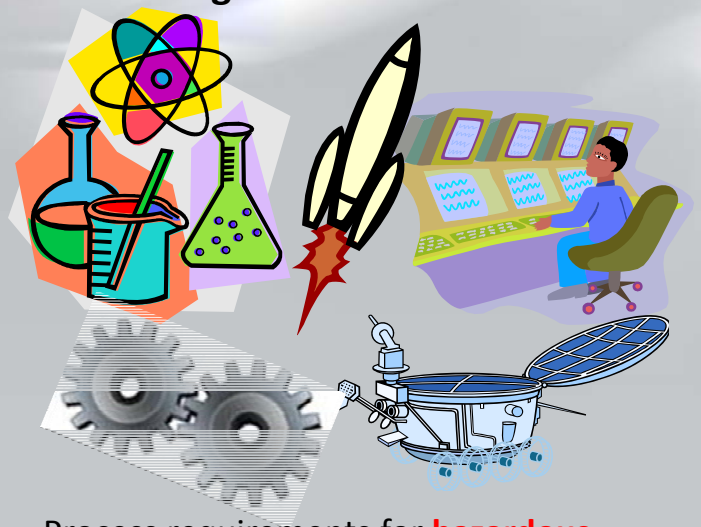
Process Measures for High-Risk Facilities

- Worldwide industry and government organizations have developed effective indicator programs, recognizing the value of leading indicators at reducing the risk of catastrophic mishaps.
- In the US, events such as the BP Texas City explosion and the Deep Water Horizon spill have compelled action to develop a standard for process safety-related leading indicators.
- Examples of leading measure areas for high-risk systems include:
  - Maintenance and system integrity conditions
  - Operational qualifications
  - Challenges to safety systems and monitoring equipment
  - Communication and reporting system conditions
  - Accuracy of configuration management
  - Maintenance of operational procedures and emergency response plans
- NASA has adapted this approach to assess risk controls associated with hazardous, critical, and complex infrastructure.

Facility Safety Risk Concept of Operations

"…Required life cycle safety program tasks for facilities judged as **hazardous**, **critical** or **complex** as a result of risk assessment."

High-Risk Facilities



Process requirements for **hazardous**, **critical**, or **complex** facilities:

- Organizational responsibilities,
- Personnel training,
- Operating procedures,
- Configuration management,
- Maintenance,
- Resources, schedules and milestones,
- Integration with other program engineering and management activities.

Facility Risk Criteria

Hazardous:
Facilities, by their standard operation/mission, subject personnel to risks/hazards that are not normally seen in the standard workplace environment.

Critical:

- Unique, irreplaceable facilities that support space flight activities.
- Facilities supporting unique facilities that provide utility services.
- Facilities which contain historically significant national treasures.

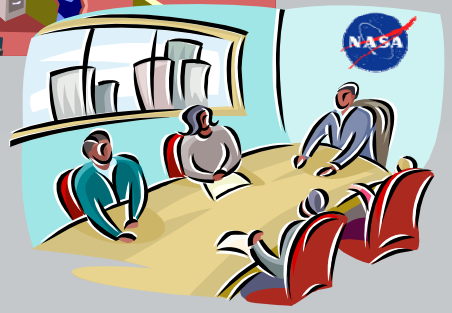
Complex :

- Require multiple organizations to conduct facility mission.
- Require extensive employee training.
- Have integrated systems using specialty and prototype equipment.
- Contain equipment that is specifically designed and high value.

Low-Risk Facilities

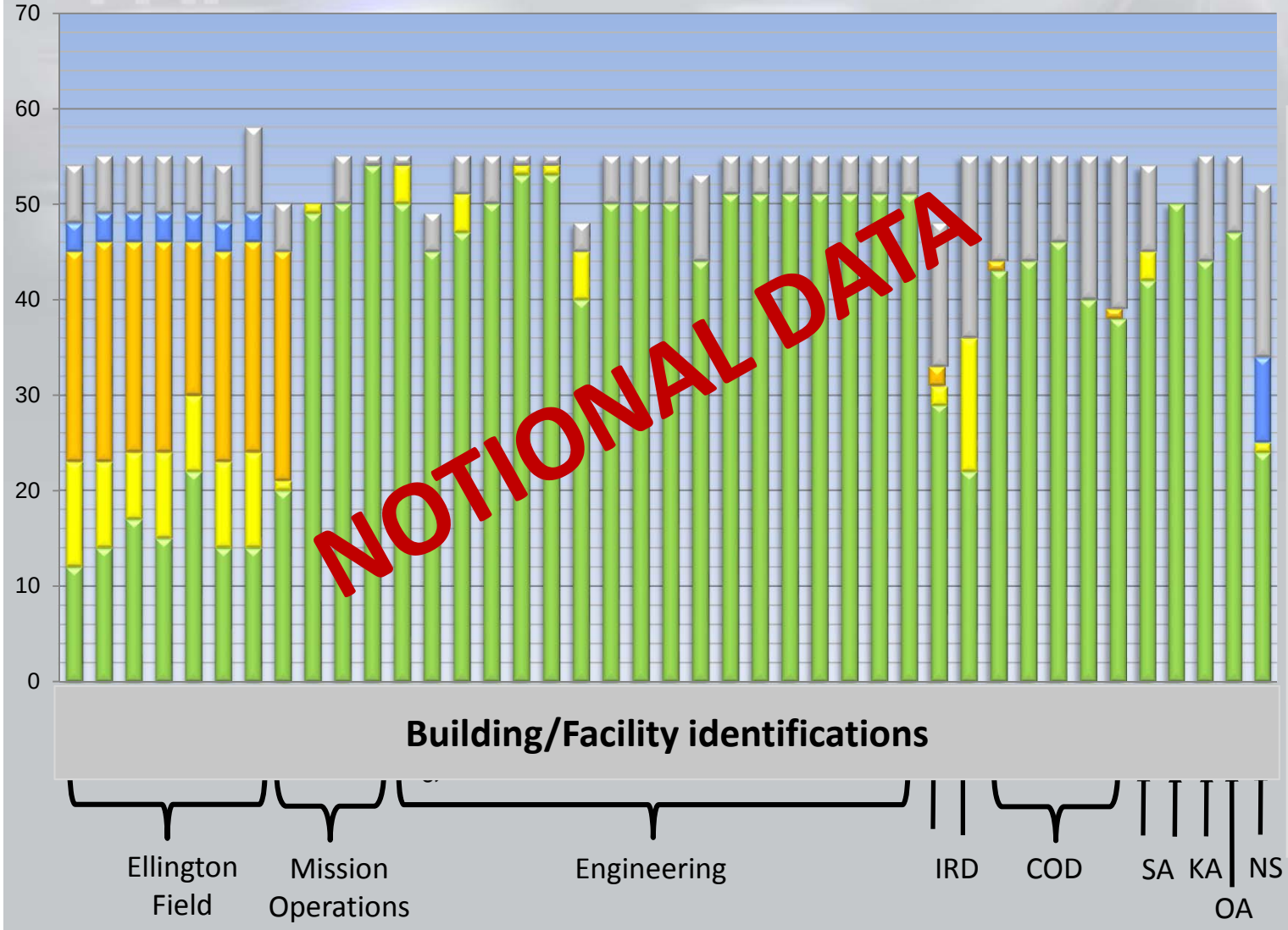
Office occupancies

Places of assembly



Facilities which do not meet the hazardous, critical, or complex criteria are subject to compliance with regulatory standards and national consensus codes.

Facility Safety Risk Control Assessment

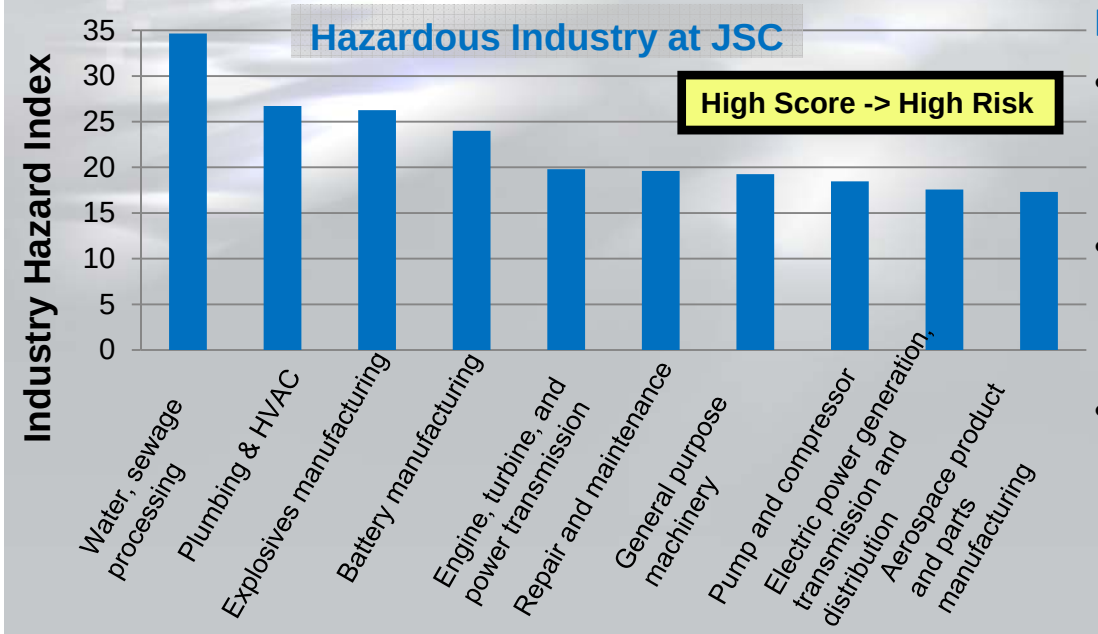


Characteristic Assessment Key

Not Applicable	Elements of Chapter 10.4 are not applicable to the associated facility mission.
2013 HATS Closed: Conforms	Items identified as nonconforming in 2013 were resolved.
* Non-conformance	Documentation does not exist to support the requirements of Chapter 10.4.
Partially conforms	Significant information is available, but does not meet the intent of Chapter 10.4, or it is out of date or unavailable.
Conforms	Documentation is available with the required information to meet Chapter 10.4.

*** In most instances non-conformances represented potentially uncontrolled RAC 3 or 4 hazards.**

Facility Risk Benchmarking with Insurance Industry

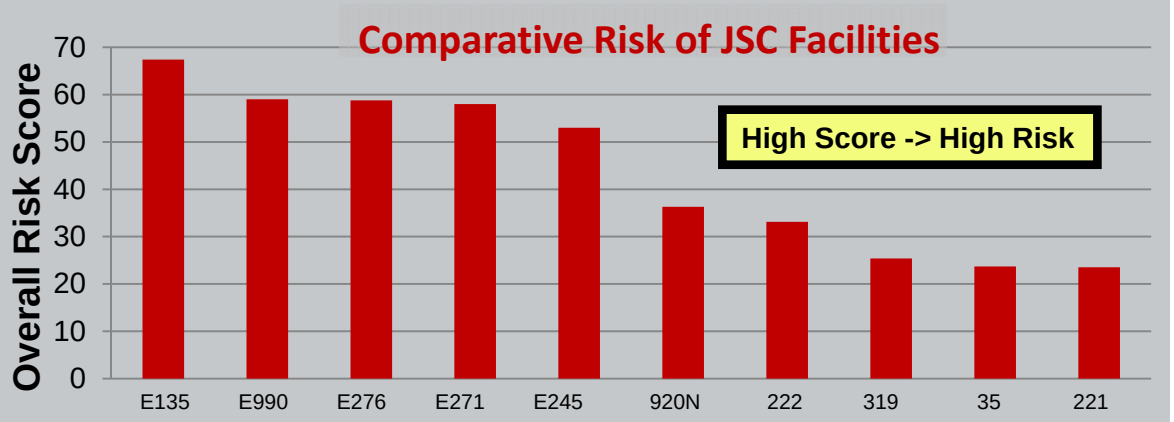


Industry Hazard Index:

- Industry Index is determined by the type of operation (by NAICS code) for each high-risk JSC facility.
- Incident rates are scaled 0-100 considering max value across all industries (not just those associated with JSC facilities).
- For example, if the industry hazard index is 30, then 30% of industries are less risky.

Overall Risk Score Considers:

- Industry Hazard Index
  - Weighted at 10%
- Hazard Deviation (JSC Mishap Rates)
  - Weighted at 30%
- FBD Score (Risk Control)
  - Weighted at 60%



Rules of Thumb for Managing Risk

- Accept risk only if it is low enough to tolerate and within regulations.
- NO ONE GETS HURT!!!
- Tolerate only the damage you can afford.
- Avoid risks you don't NEED to take.
- Risks change as often as the facility, people, and processes associated with them, so they must be monitored and reassessed periodically.

Backup Charts

Columbia STS-107, February 1, 2003:

- 7 fatalities;
- $3 Billion vehicle loss;
- 2.5 year mission impact.

Kalpana Chawla
Rick D. Husband
Laurel B. Clark
Ilan Ramon
Michael P. Anderson
David M. Brown
William C. McCool

NOAA N-Prime, September 6, 2003:

- $135 Million vehicle damage;
- 5.5 year mission impact.

Genesis, September 8, 2004:

- Some sample retrieval materials lost.

Orbiting Carbon Observatory, February 24, 2009:
- $280 Million vehicle loss;
- 5+ year mission impact.

Glory, March 4, 2011:
- $424 Million vehicle loss;
- ??? mission impact.

JSC Chamber B Asphyxiation, July 28, 2010

- Shoulder injury due to asphyxiation and fall.