Risk-Informed Quality Assurance

NASA Goddard Space Flight Center

Supply Chain Quality Assurance Conference

October 14, 2009

Bryan O'Connor

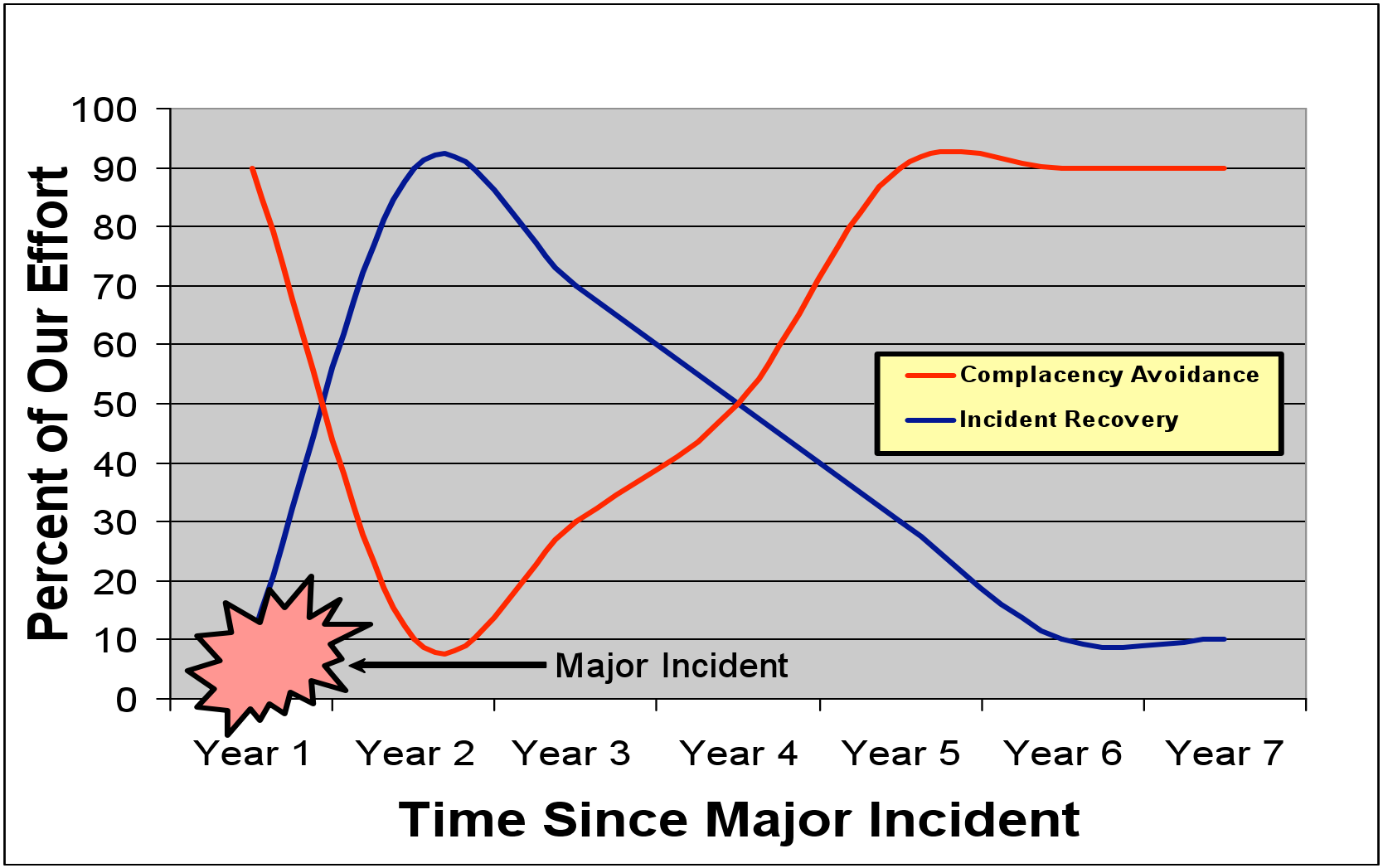
Office of Safety and Mission Assurance

Thought of the Day

The whole problem with the world is that fools and fanatics are always so certain of themselves, but wiser people so full of doubts

Bertrand Russell

The Two Modes of Mishap Prevention



Avoiding Complacency

1. Know the enemy within:

Know your internal quality system weaknesses, and be continually working to remedy them.

2. Know the enemy without:

Know your external quality risks, and be continually working to mitigate them.

3. Focus on risk:

Plan and execute around risk. Don't waste time/resources assuring minimal-risk attributes.

4. Connect the dots:

Think system…know mission and context…

AS9100: 2009

A New (and needed) Focus on Risk

7.1.2 Risk Management

The organization shall establish, implement and maintain a process for managing risk to the achievement of applicable requirements, that includes as appropriate to the organization and the product

a) assignment of responsibilities for risk management,

b) definition of risk criteria (e.g., likelihood, consequences, risk acceptance),

c) identification, assessment and communication of risks throughout product realization,

d) identification, implementation and management of actions to mitigate risks that exceed the defined risk acceptance criteria,

e) acceptance of risks remaining after implementation of mitigating actions.

critical items … key characteristics … special requirements

The Risk Iceberg

Risk Management for Exploration

- Known Knowns: *(Systems Engineering, Quality Processes and Program Management)*
  - Disciplined program and mission **management processes and people**
- Known Unknowns: *(Continuous Risk Management)*
  - **Reduce uncertainties** with analysis, ground and flight test
  - Prioritize and manage **residual risk** (including uncertainty) with training, conservative procedures and quality plans
- Unknown Knowns: *(Continuous Process Improvement)*
  - **Communications , Communications, Communications**
  - Improve data **analysis** tools and techniques (e.g. trending)
- Unknown Unknowns: *(Continuous Research, Test and Eval)*
  - Exercise ***Engineering Curiosity***
  - Continuously **challenge assumptions,** models and analyses
  - Be ready for adverse effects (emergency systems)

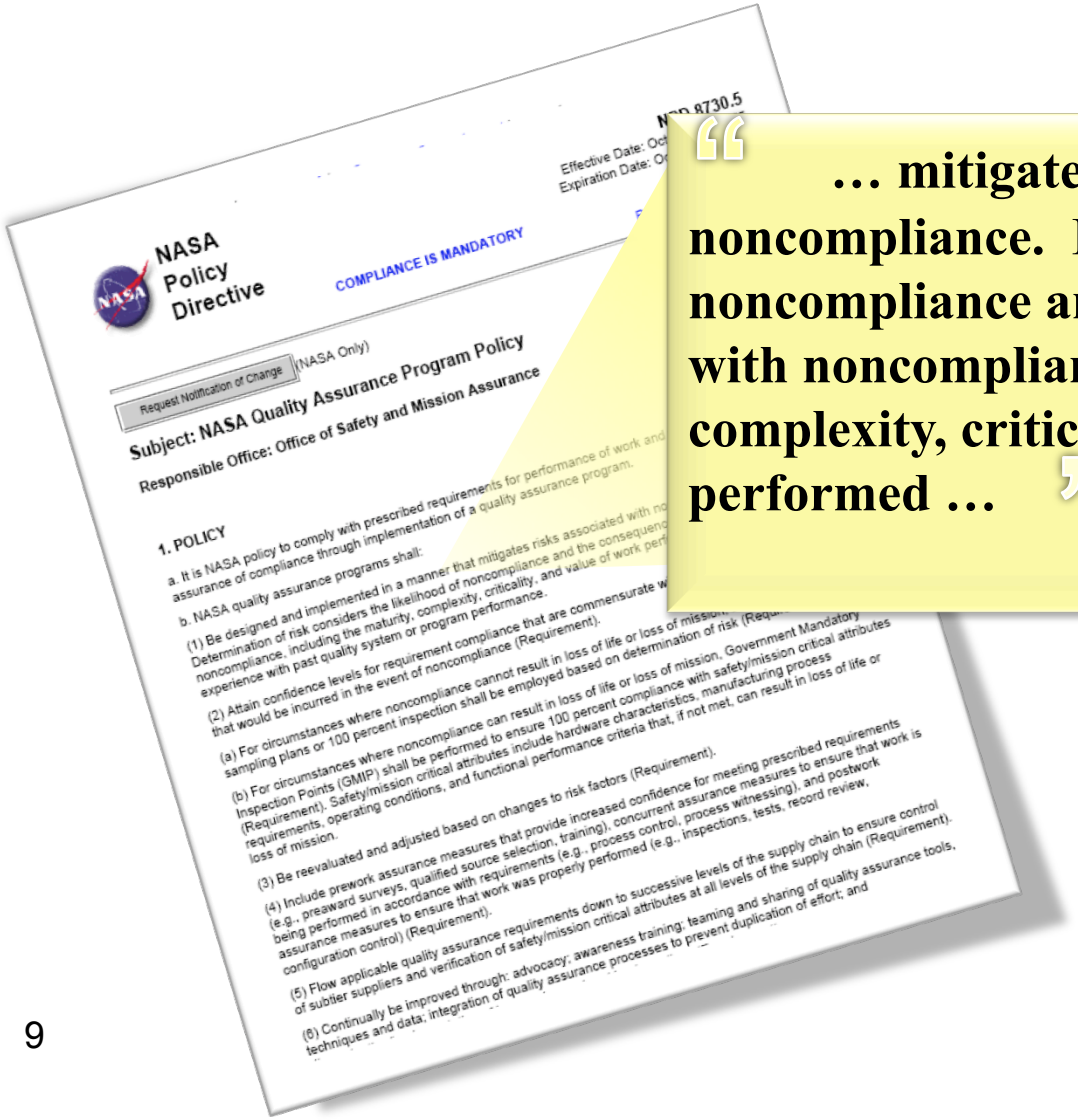
High Residual Risk* Acceptance at NASA

- Tech Authority (relevant tech requirement owner) approves based on technical merit, and
- Safety Tech Authority approves based on risk acceptability, and
- Risk Taker (and supervisory chain of command) volunteers to take the risk, and
- Only then does Program or Ops Manager get to “accept the risk”

*Residual risk is that extra level of risk over and above what is inherent in the design requirements

NASA Quality Policy

NPD 8730.5


NASA Policy Directive

COMPLIANCE IS MANDATORY

Request Notification of Change (NASA Only)

Subject: NASA Quality Assurance Program Policy

Responsible Office: Office of Safety and Mission Assurance

1. POLICY

a. It is NASA policy to comply with prescribed requirements for performance of work and assurance of compliance through implementation of a quality assurance program.

b. NASA quality assurance programs shall:

(1) Be designed and implemented in a manner that mitigates risks associated with noncompliance. Determination of risk considers the likelihood of noncompliance and the consequences associated with noncompliance, including the maturity, complexity, criticality, and value of work performed, experience with past quality system or program performance.

(2) Attain confidence levels for requirement compliance that are commensurate with the risk that would be incurred in the event of noncompliance (Requirement).

(a) For circumstances where noncompliance cannot result in loss of life or loss of mission, Government Mandatory Inspection Points (GMIP) shall be employed based on determination of risk (Requirement). Safety/mission critical attributes include hardware characteristics, manufacturing process requirements, operating conditions, and functional performance criteria that, if not met, can result in loss of life or loss of mission.

(b) For circumstances where noncompliance can result in loss of life or loss of mission, Government Mandatory Inspection Points (GMIP) shall be performed to ensure 100 percent compliance with safety/mission critical attributes (Requirement).

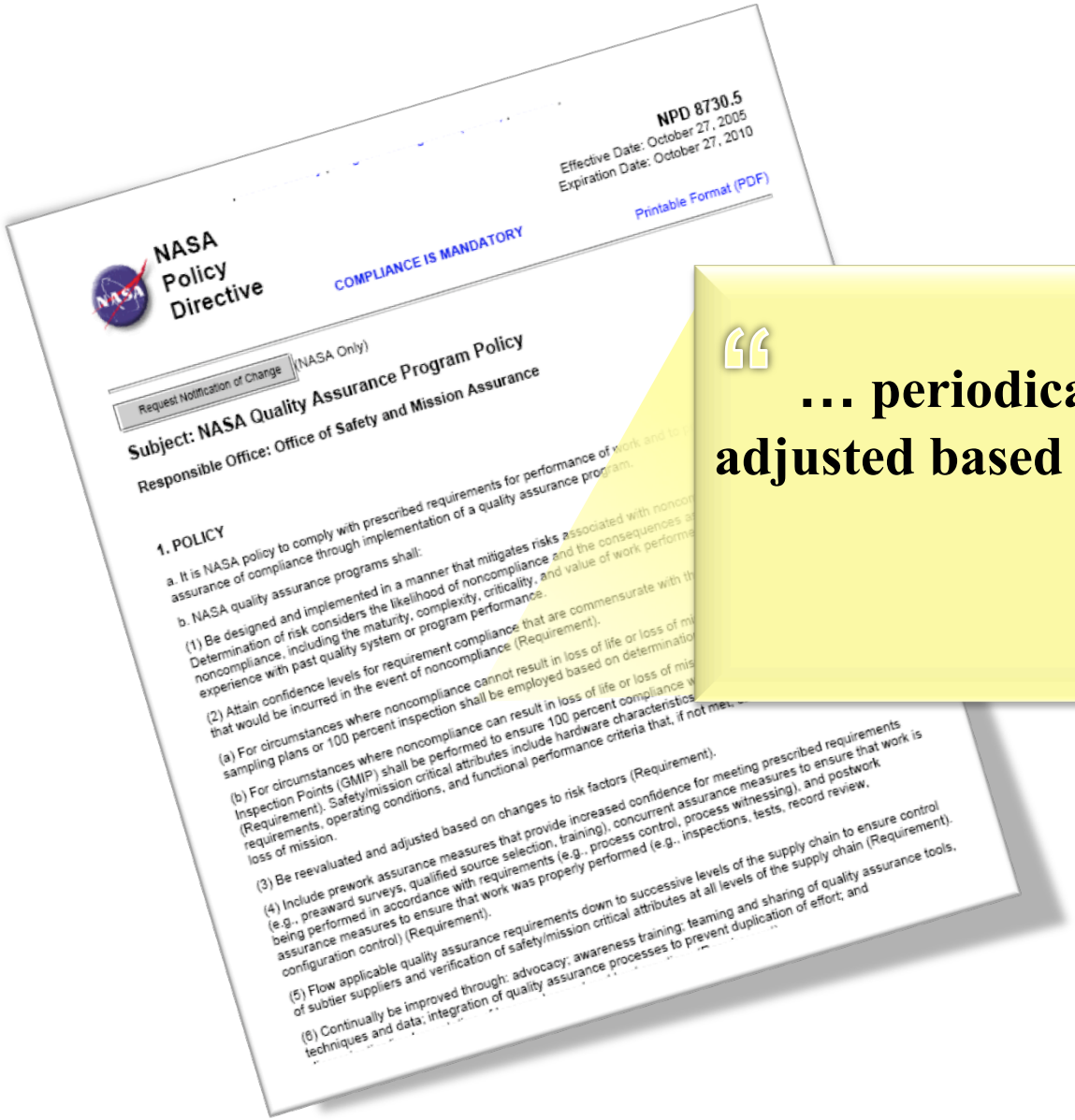
(3) Be reevaluated and adjusted based on changes to risk factors (Requirement).

(4) Include prework assurance measures that provide increased confidence for meeting prescribed requirements (e.g., preaward surveys, qualified source selection, training), concurrent assurance measures to ensure that work is being performed in accordance with requirements (e.g., process control, process witnessing), and postwork assurance measures to ensure that work was properly performed (e.g., inspections, tests, record review, configuration control) (Requirement).

(5) Flow applicable quality assurance requirements down to successive levels of the supply chain to ensure control of subtier suppliers and verification of safety/mission critical attributes at all levels of the supply chain (Requirement).

(6) Continually be improved through: advocacy; awareness training; learning and sharing of quality assurance tools, techniques and data; integration of quality assurance processes to prevent duplication of effort; and

> **"… mitigate risks associated with noncompliance. Risk considers the likelihood of noncompliance and the consequences associated with noncompliance, including the maturity, complexity, criticality, and value of work performed …"**



NASA Policy Directive

COMPLIANCE IS MANDATORY

NPD 8730.5
Effective Date: October 27, 2005
Expiration Date: October 27, 2010

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Quality Assurance Program Policy

Responsible Office: Office of Safety and Mission Assurance

1. POLICY

a. It is NASA policy to comply with prescribed requirements for performance of work and to assurance of compliance through implementation of a quality assurance program.

b. NASA quality assurance programs shall:

(1) Be designed and implemented in a manner that mitigates risks associated with noncompliance. Determination of risk considers the likelihood of noncompliance and the consequences of noncompliance, including the maturity, complexity, criticality, and value of work performed, experience with past quality system or program performance.

(2) Attain confidence levels for requirement compliance that are commensurate with the that would be incurred in the event of noncompliance (Requirement).

(a) For circumstances where noncompliance cannot result in loss of life or loss of mi sampling plans or 100 percent inspection shall be employed based on determinatio

(b) For circumstances where noncompliance can result in loss of life or loss of mis Inspection Points (GMIP) shall be performed to ensure 100 percent compliance w (Requirement). Safety/mission critical attributes include hardware characteristics requirements, operating conditions, and functional performance criteria that, if not met loss of mission.

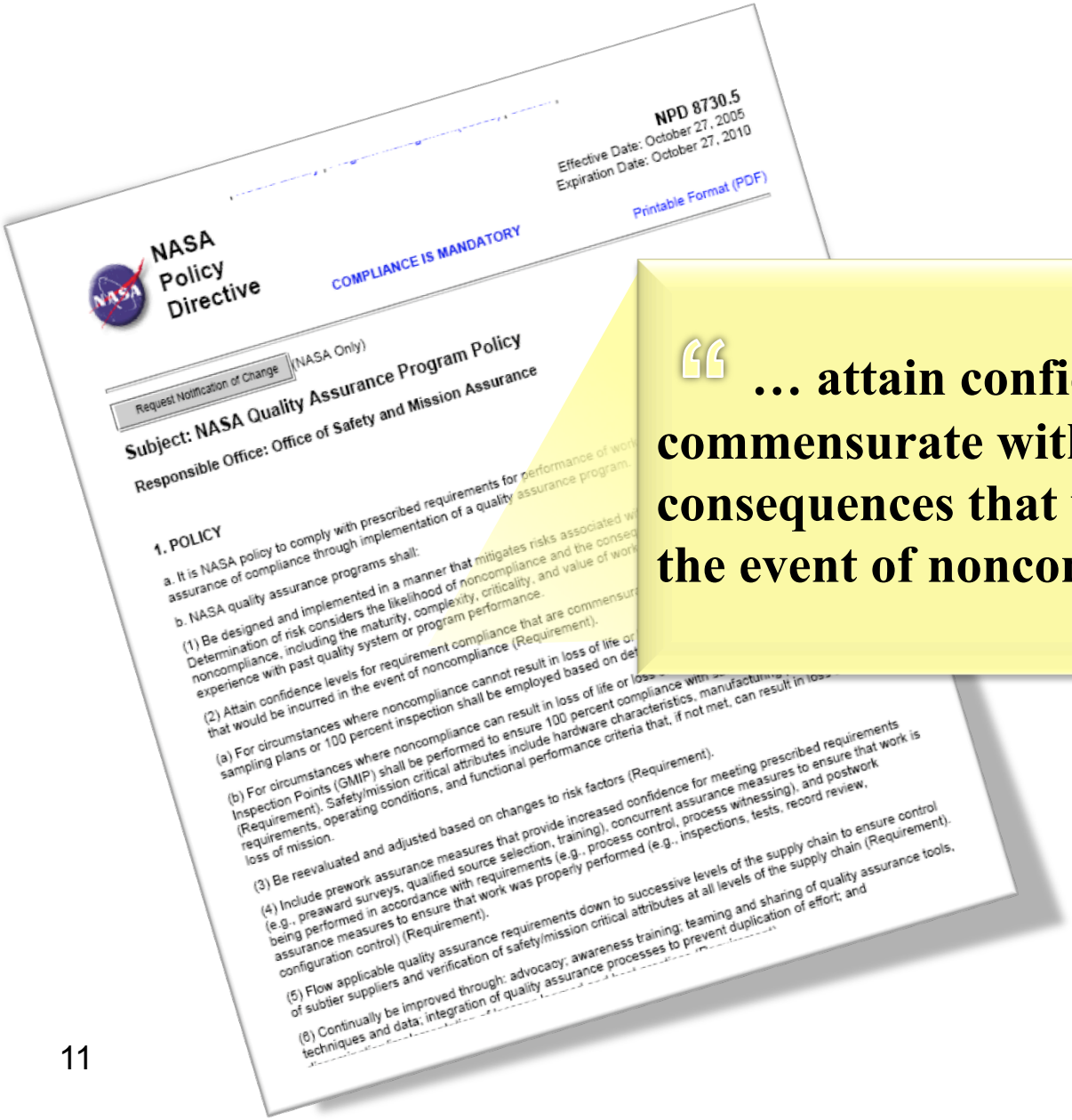
(3) Be reevaluated and adjusted based on changes to risk factors (Requirement).

(4) Include prework assurance measures that provide increased confidence for meeting prescribed requirements (e.g., preaward surveys, qualified source selection, training), concurrent assurance measures to ensure that work is being performed in accordance with requirements (e.g., process control, process witnessing), and postwork assurance measures to ensure that work was properly performed (e.g., inspections, tests, record review, configuration control) (Requirement).

(5) Flow applicable quality assurance requirements down to successive levels of the supply chain to ensure control of subtier suppliers and verification of safety/mission critical attributes at all levels of the supply chain (Requirement).

(6) Continually be improved through: advocacy; awareness training; teaming and sharing of quality assurance tools, techniques and data; integration of quality assurance processes to prevent duplication of effort; and

> **"… periodically reevaluated and adjusted based on changes to risk factors."**


NASA Policy Directive

COMPLIANCE IS MANDATORY

NPD 8730.5
Effective Date: October 27, 2005
Expiration Date: October 27, 2010

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Quality Assurance Program Policy

Responsible Office: Office of Safety and Mission Assurance

1. POLICY

a. It is NASA policy to comply with prescribed requirements for performance of work assurance of compliance through implementation of a quality assurance program.

b. NASA quality assurance programs shall:

(1) Be designed and implemented in a manner that mitigates risks associated with Determination of risk considers the likelihood of noncompliance and the consequences noncompliance, including the maturity, complexity, criticality, and value of work experience with past quality system or program performance.

(2) Attain confidence levels for requirement compliance that are commensurate that would be incurred in the event of noncompliance (Requirement).

(a) For circumstances where noncompliance cannot result in loss of life or loss sampling plans or 100 percent inspection shall be employed based on defined

(b) For circumstances where noncompliance can result in loss of life or loss Inspection Points (GMIP) shall be performed to ensure 100 percent compliance with (Requirement). Safety/mission critical attributes include hardware characteristics, manufacturing requirements, operating conditions, and functional performance criteria that, if not met, can result in loss of mission.

(3) Be reevaluated and adjusted based on changes to risk factors (Requirement).

(4) Include prework assurance measures that provide increased confidence for meeting prescribed requirements (e.g., preaward surveys, qualified source selection, training), concurrent assurance measures to ensure that work is being performed in accordance with requirements (e.g., process control, process witnessing), and postwork assurance measures to ensure that work was properly performed (e.g., inspections, tests, record review, configuration control) (Requirement).

(5) Flow applicable quality assurance requirements down to successive levels of the supply chain to ensure control of subtier suppliers and verification of safety/mission critical attributes at all levels of the supply chain (Requirement).

(6) Continually be improved through: advocacy; awareness training; teaming and sharing of quality assurance tools, techniques and data; integration of quality assurance processes to prevent duplication of effort; and

> **“ … attain confidence levels that are commensurate with the severity of consequences that would be incurred in the event of noncompliance.”**

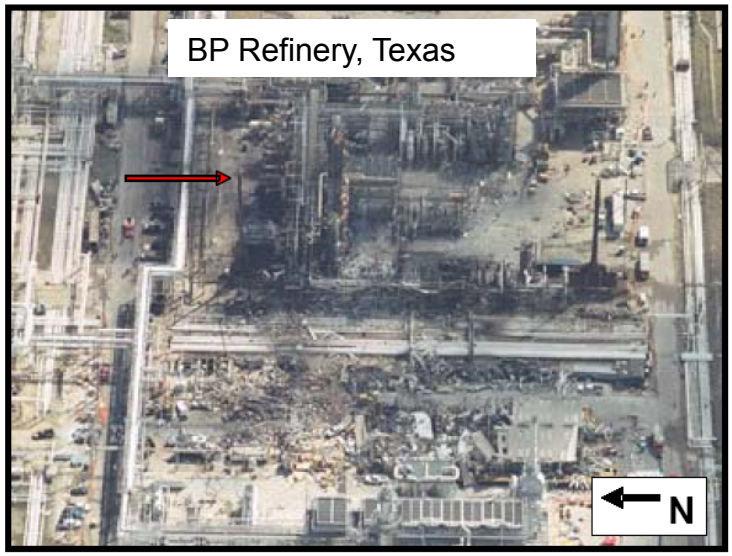
Remember Past Lessons

No one wants to learn by mistakes, but we cannot learn enough from successes to go beyond the state of the art.

Henry Petroski

To Engineer is Human

Become a Student of Past Quality System Failures



Vacuum Chamber thought to have been a pressure vessel

Control rod lodged in ceiling of SL-1 reactor building.

USS THRESHER

First in her class

She was fast, quiet, and deep diving.

The leading edge of US Submarine Technology

Apollo 1 Command Module

First in her class

She was larger & far more complex than any previous design.

The leading edge of US Spacecraft Technology

Contributing Causal Factors

- Inadequate Workmanship -

THRESHER

Improperly brazed pipe joint

Poorly brazed pipes led to the electrical shortage that led to the loss of the USS THRESHER.

Apollo 1

"The board found numerous examples in the wiring of poor installation and poor workmanship".

Figure 2: Wires where the fire was suspected to have started.

Contributing Causal Factors

- Inadequate Fabrication Processes -

THRESHER	Apollo 1
Brazed piping joints exposed to full submergence pressure	Teflon wire coating could be easily damaged or penetrated by abrasion

Contributing Causal Factors

- Ineffective Quality Program -

THRESHER

Portsmouth Naval Shipyard inspectors using newly developed ultrasonic testing techniques identified numerous instances of faulty brazed joints. Many brazed joints on the THRESHER were never UT'd.

Apollo 1

Kennedy Space Center inspectors cited multiple instances of deficient parts, equipment, and workmanship.

Contributing Causal Factors

- Vulnerable Design -
- Inadequate Emergency Recovery -
- Unforeseen Failure Mode -

THRESHER

- Reactor shutdown
- Impaired access to vital equipment
- Compromised ballast tank blow

Wreckage from the USS THRESHER's sonar dome can be seen on the ocean floor.

Apollo 1

- Single gas atmosphere
- Flammable materials
- Inward opening hatch

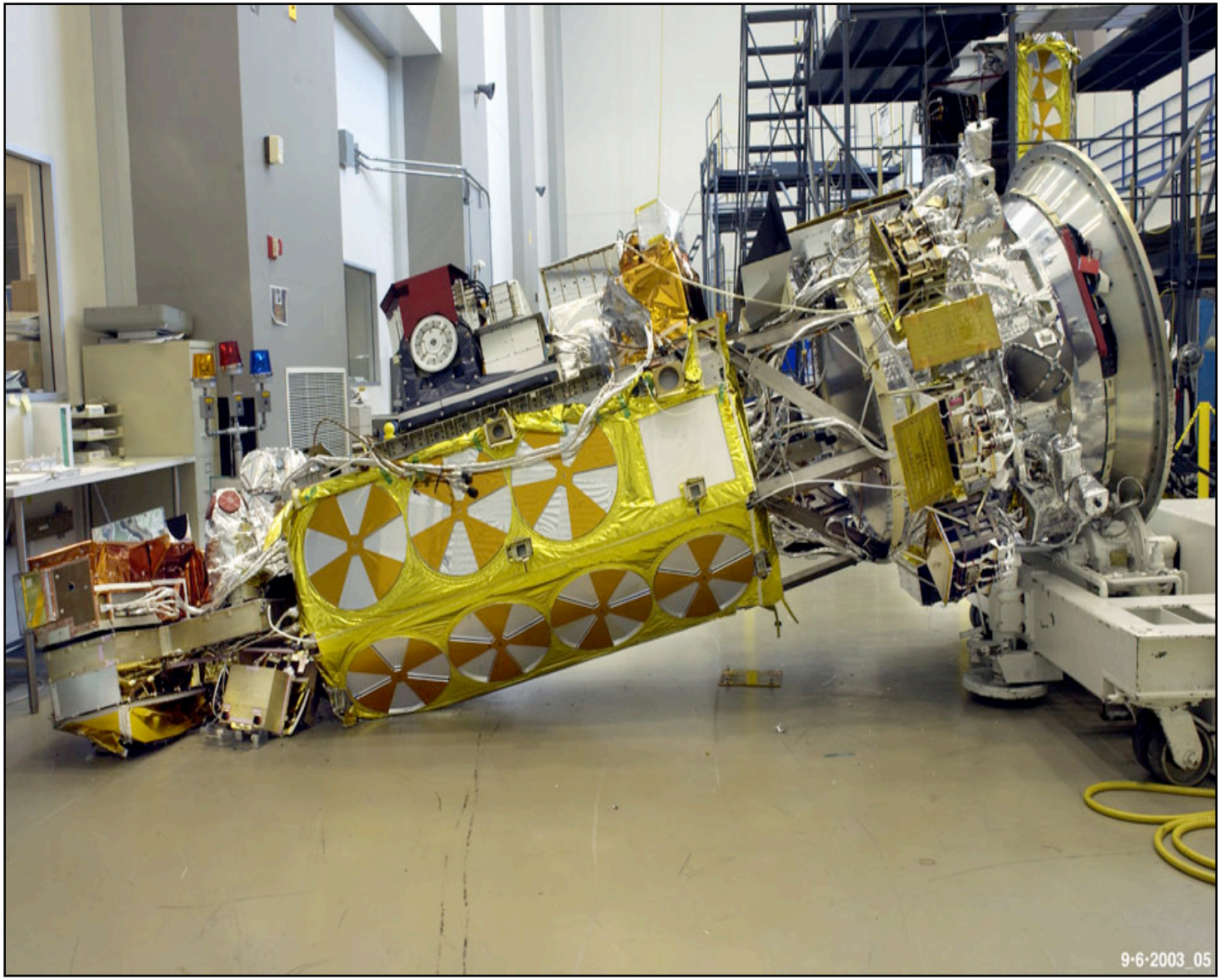
The Enemy Within

- Know your Quality System Weaknesses -

	Documentation - AS9100 Para 4.0	Management Responsibility - AS9100 Para 5.0	Resource Management - AS9100 Para 6.0	Planning/Customer Interface - AS9100 Para 7.1, 7.2	Design - AS9100 Para 7.3	Supply Chain - AS9100 Para 7.4	Production/ Process - AS9100 Para 7.5	Calibration/Metrology - AS9100 Para 7.6	General Quality Assurance - AS9100 Para 8.1	Monitoring/Audit - AS9100 Para 8.2	Control of NCM - AS9100 Para 8.3	Analysis of Data - AS9100 Para 8.4	Corrective and Preventive Action - AS9100 Para 8.5	QA SCORE
BP Oil Refinery Blast	X	X	X	X	X		X	X	X	X	X	X	X	13
Lewis Spins Out of Control		X	X	X	X	X	X			X		X	X	11
USS Thresher				X	X	X	X		X	X				7
Supercritical - SL-1 Reactor	X	X	X		X		X	X			X	X	X	10
US Forrestal in flames	X	X	X	X	X	X	X							8
	3	4	5	4	7	3	8	2	2	3	2	3	3	

Proximate Causes
Underlying Causes
Score
0 = not a contributing cause
1 = underlying cause
2 = Proximate/primary cause

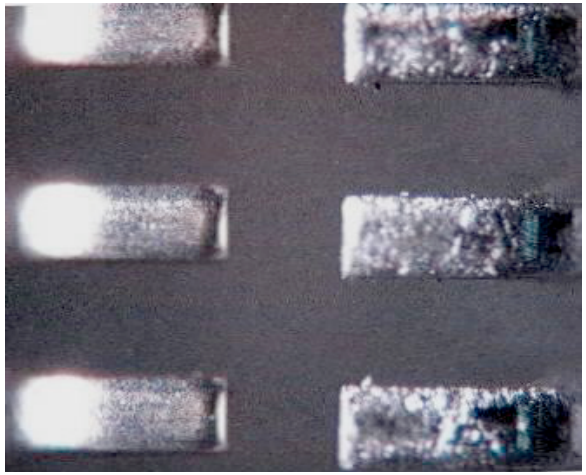
The marked boxes indicate ineffective QMS elements and a failure of quality assurance auditing to identify & correct these shortcomings.


9·6·2003_05

The Enemy Without

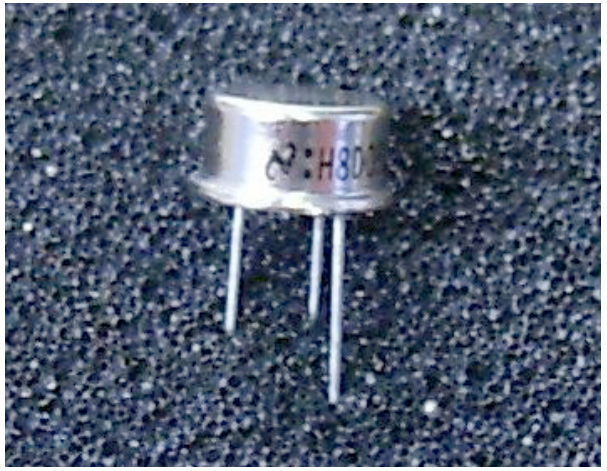
- Counterfeit Parts -

New versus Refurbished leads

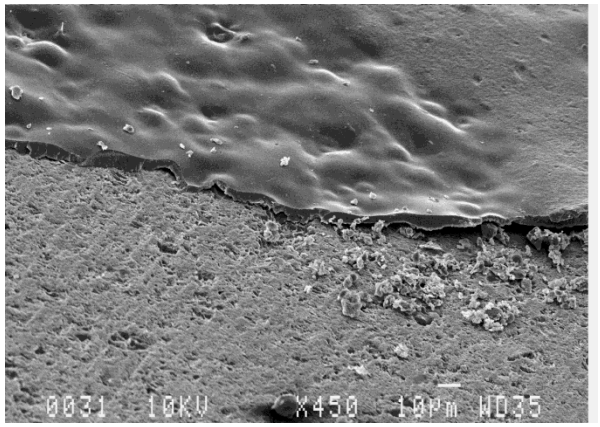


Dual Markings

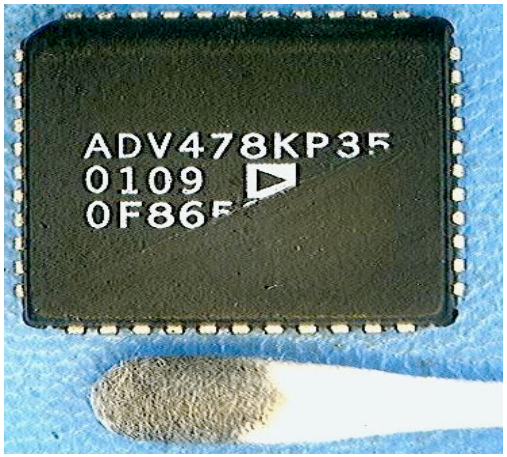
National Semiconductor does not use " : " in part numbers



Backtop peeling away. Sand marks evident



Acetone Swipe

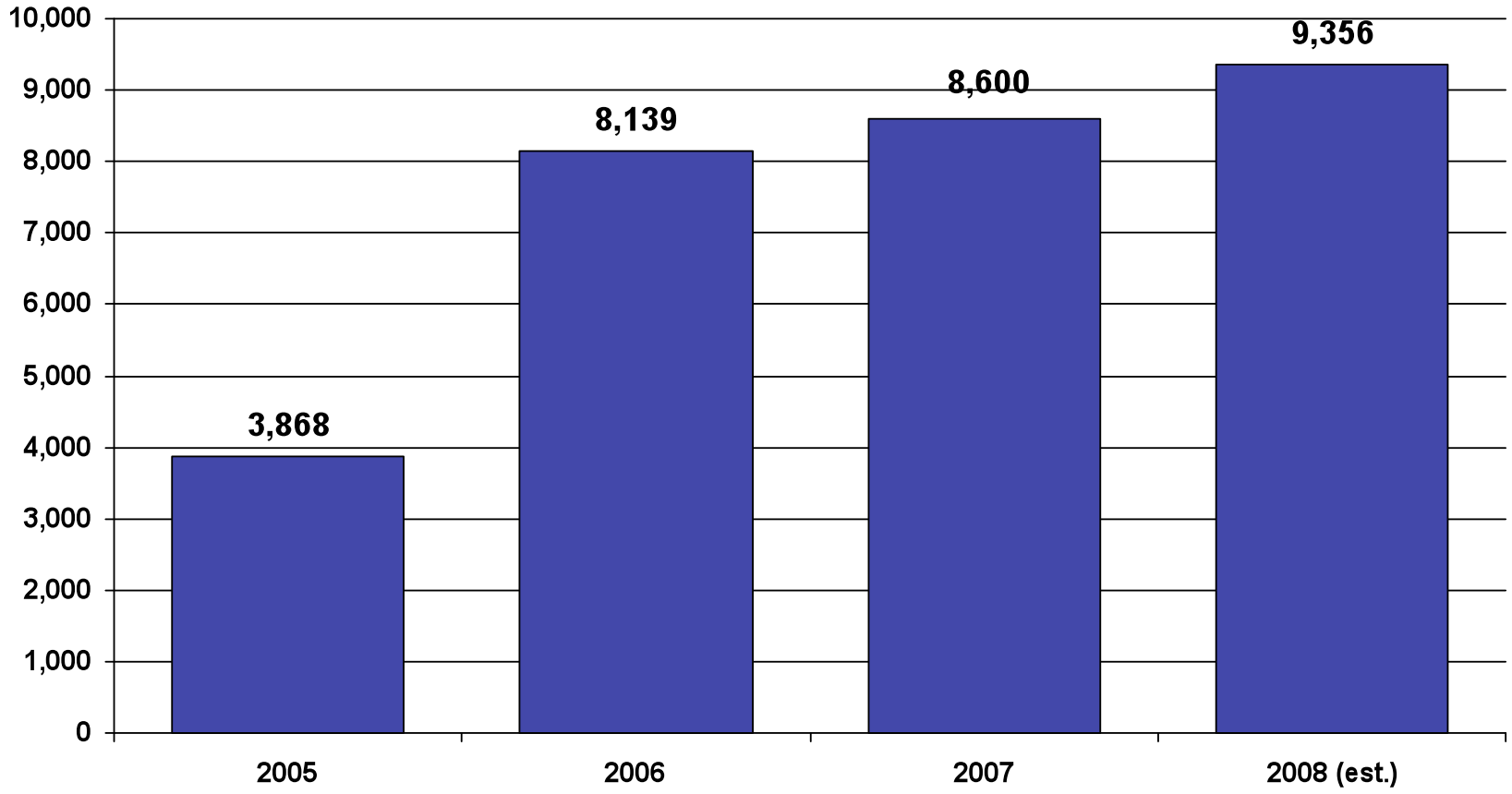


Missing Serial Number

Workers extract plastics from discarded electronics in Guiyu, a few hours' drive northeast of Hong Kong. The city has 5,500 family workshops handling e-waste.

Laborer de-soldering circuit boards over a coal-fired grill. Rock in the box is where boards are hit to remove solder. Pliers are used to pluck off chips which go into various buckets. The boards are then tossed into a pile for open burning. © BAN

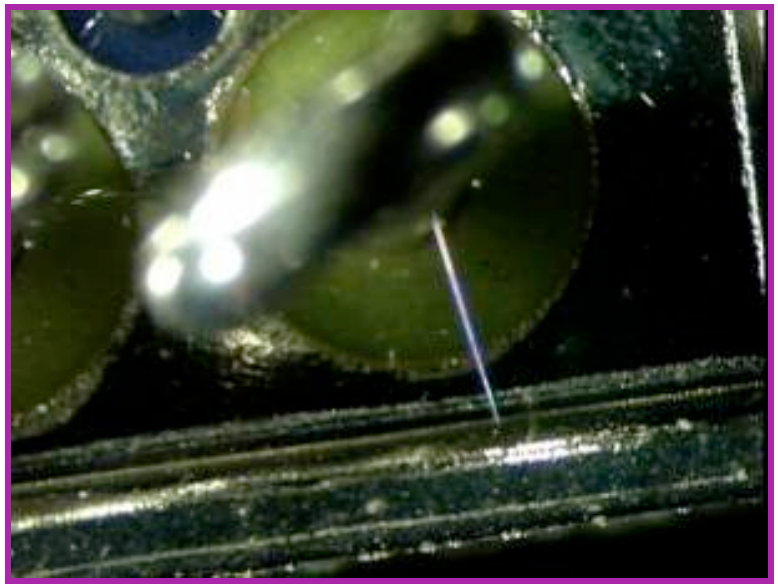
Total Counterfeit Incidents:



U.S. Department of Commerce
March, 2009

The Enemy Without (cont)

- Metal Whiskers -



Tin Whisker on Electromagnetic Relay Shorting Terminal to Case

Zinc Whiskers on Hot Dip Galvanized Steel Pipe

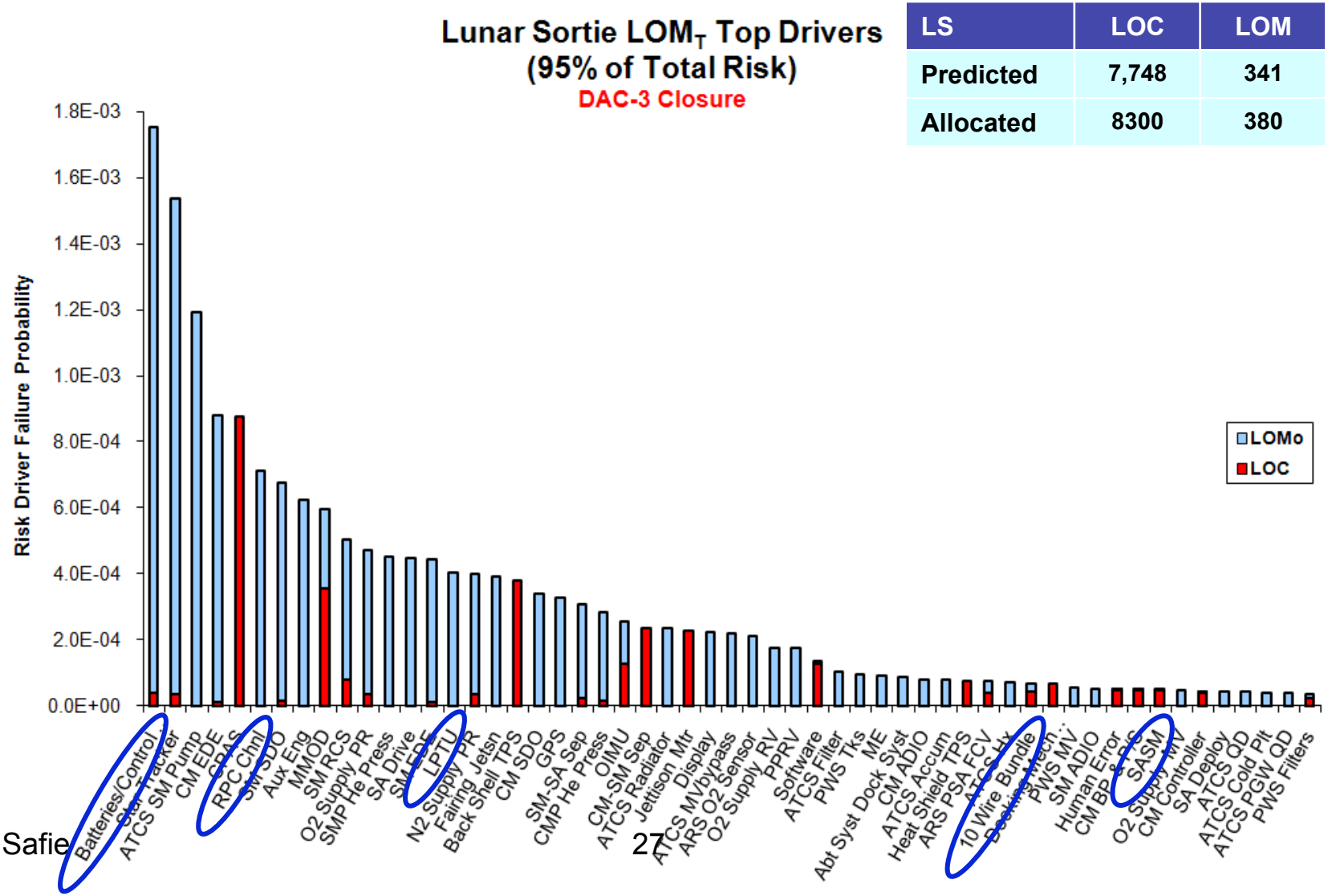
Using Risk to Prioritize

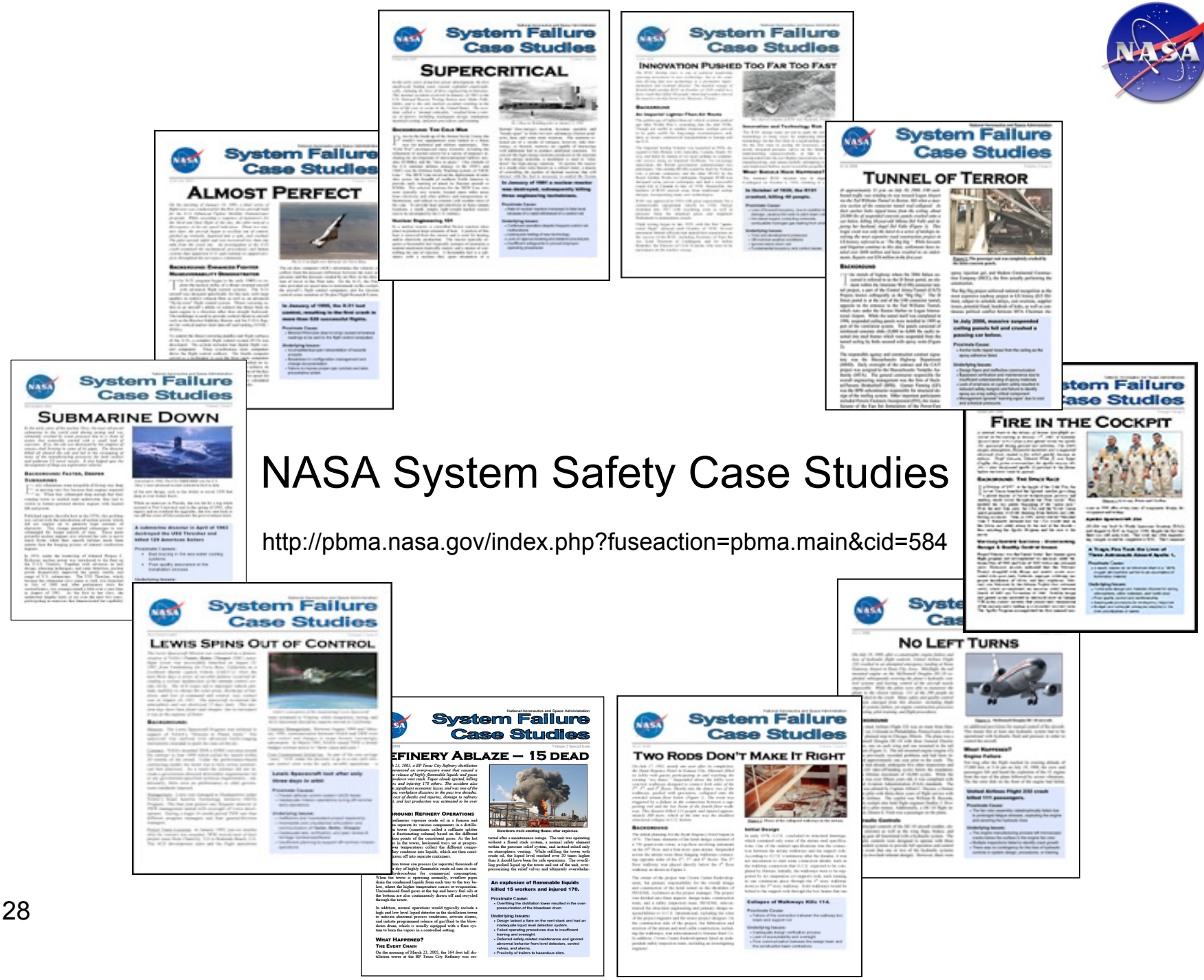
Separate the vital few from the trivial many

Joseph Juran

606F System Design
Top LS Mission Risk Drivers

LS	LOC	LOM
Predicted	7,748	341
Allocated	8300	380





NASA System Safety Case Studies

http://pbma.nasa.gov/index.php?fuseaction=pbma.main&cid=584

Risk Informed, or Risk Averse?

To your own discretion therefore must be left the degree of danger you risk, and the point at which you should decline, only saying we wish you to err on the side of your safety, and to bring back your party safe even if it be with less information.

Thomas Jefferson
Letter to Meriwether Lewis: 1803

GITTERDUNN…