Quality Lessons Learned From the Space Shuttle Program (SSP)

Keith W. Jones

United Space Alliance

SSP Quality Lessons Learned

- Post Columbia Accident Investigation
  - Engineering PRT and Quality reviewed all STS 107 and 109 paper
  - Reviews identified work instruction technical errors and performance errors
    - Technical errors presented greatest potential risk for impact to hardware fidelity for intended use
    - Performance errors presented the greatest potential risk to causing hardware damage and processing delays
  - KSC NASA Chief Engineer requested Process Assurance Engineering (PAE) determine cause and corrective actions to improve work instruction accuracy
  - Joint USA and NASA Corrective Action Implementation Team (CAIT) established to implement CA
  - #1 Recommendation - Build a monitoring System
- Separate joint effort by PAE and NASA QE to understand causes of Processing Induced errors in relation to Process Escapes.

I_d = Inefficiencies of Design

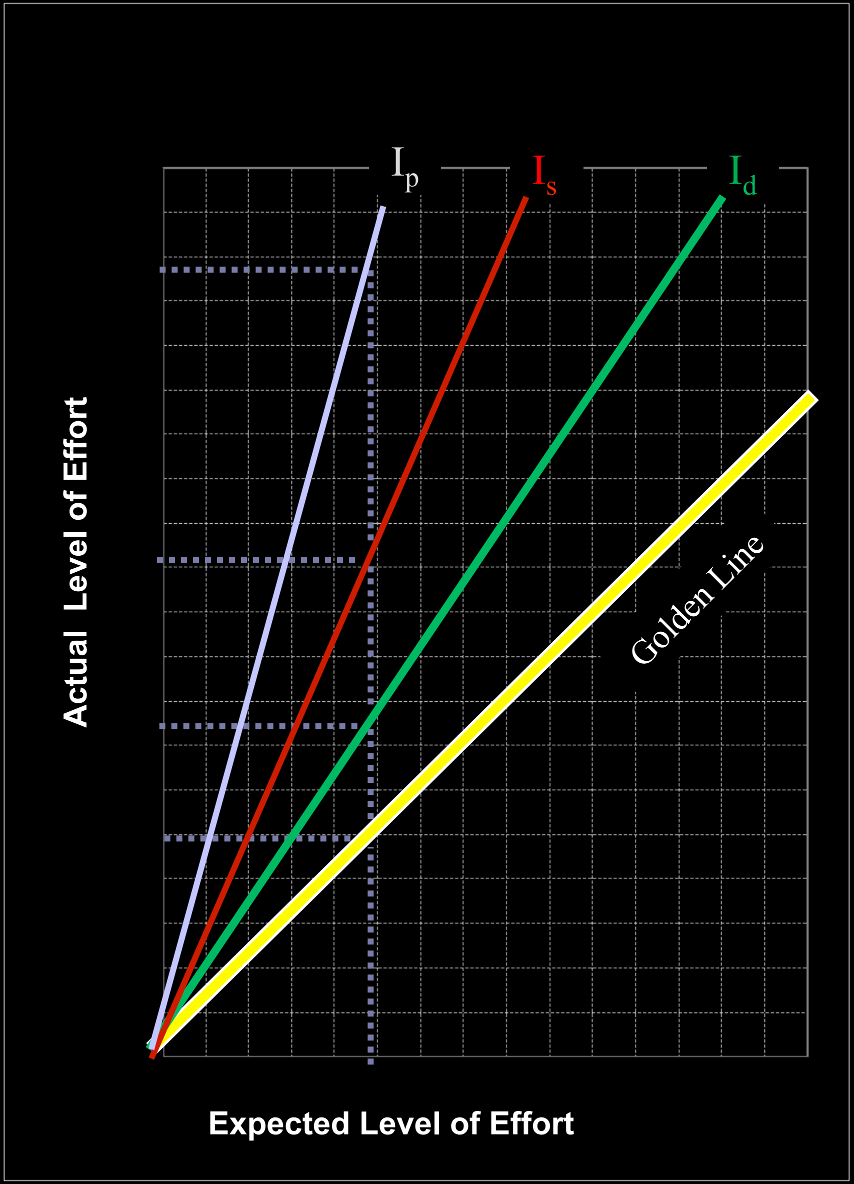
(process crutches, process waste, errors)

I_s = Inefficiencies of Supply

(defective parts, excess storage, wrong part)

I_p = Inefficiencies of Process

(excess testing, unrecognized maintenance, tolerance buildup

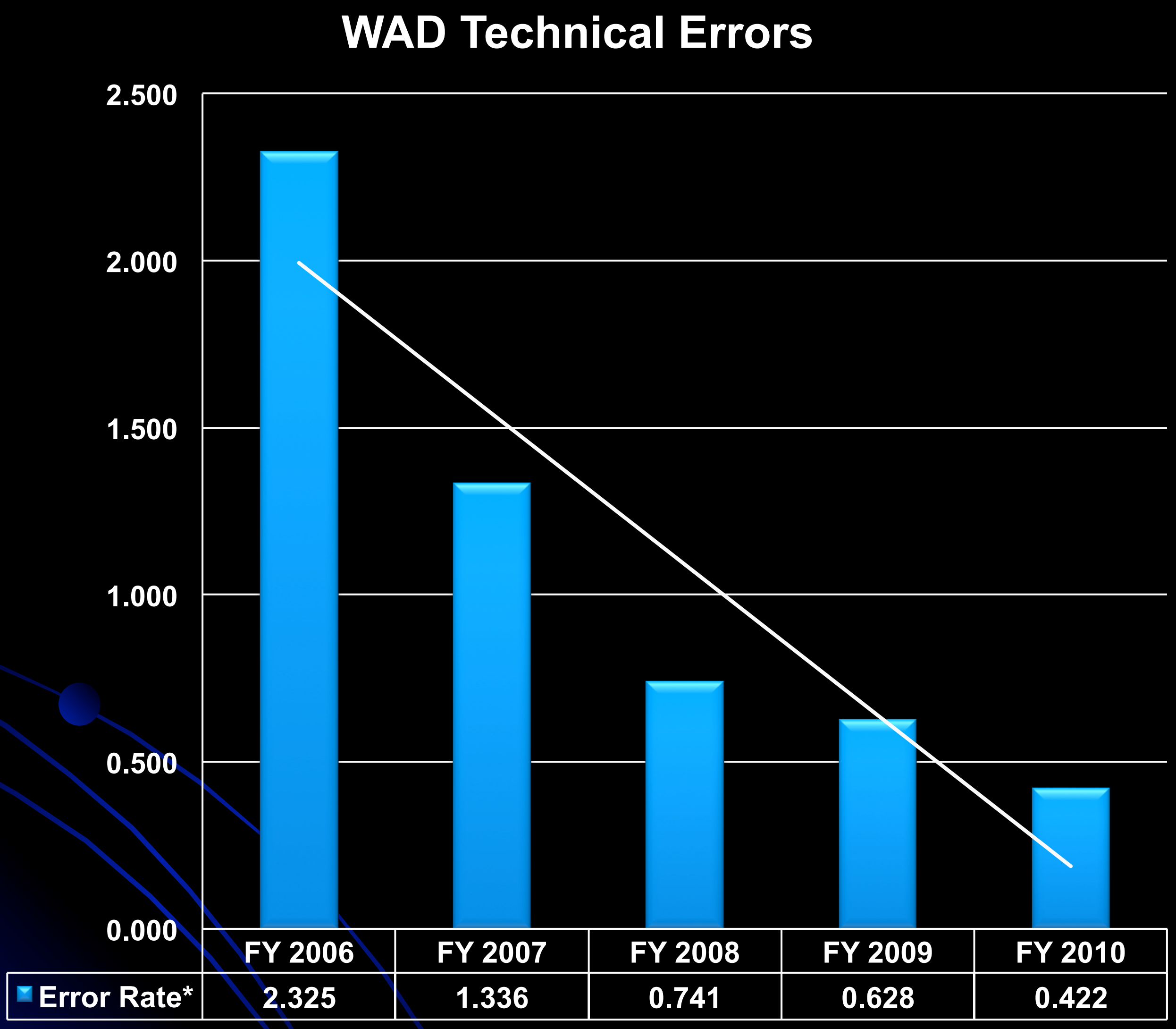


SSP Quality Lessons Learned

- **Risk Based Quality System (RBQS)**
  - Process Assurance Engineering implemented a Risk Based Quality System that assesses risks based on controls
  - Controls are assessed to determine capability and repeatability based on a hierarchy of control strength and 5 elements of a well designed behavioral control

  A Risk Based Quality System ensures that processes are Capable and Repeatable and will be performed successfully independent of additional individual knowledge or experience requirements
- The tenets of the Risk Based Quality System were used to implement monitoring and assessment processes to reduce errors and risk
  - Revised monitoring and measurement systems as well as use of some RBQS tools fully implemented prior to FY06

SSP Quality Lessons Learned



WAD Technical Errors

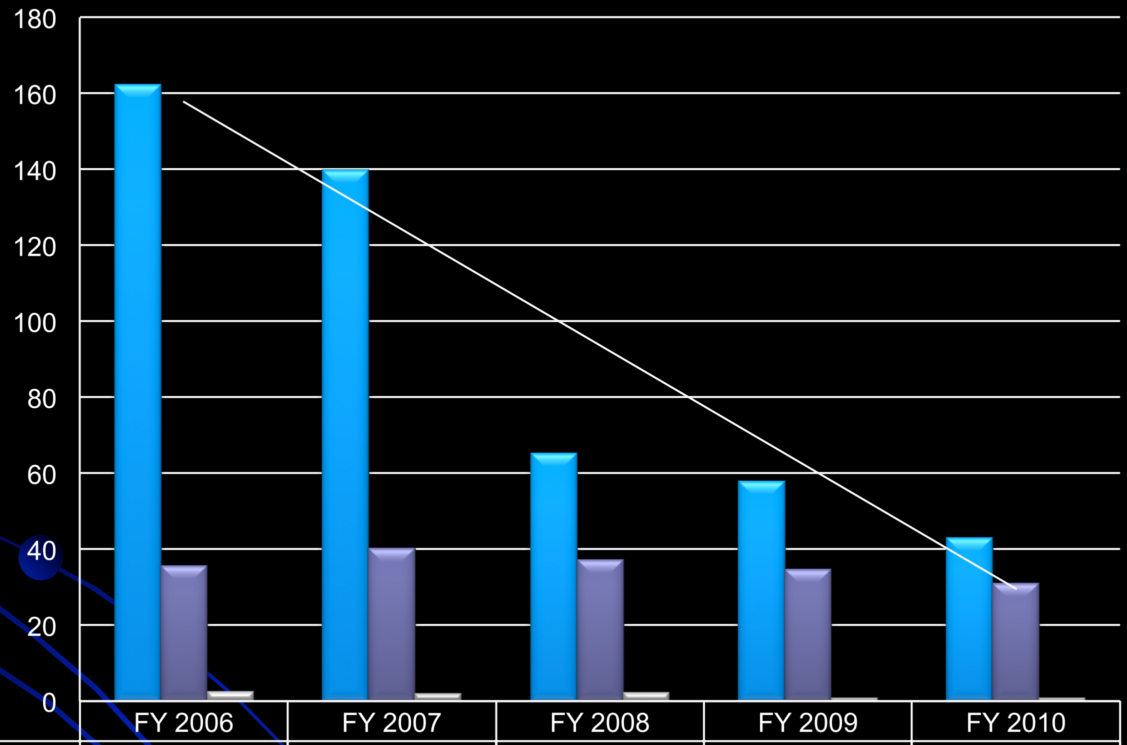
	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010
Error Rate*	2.325	1.336	0.741	0.628	0.422

* Errors Per 1000 pages

Since implementation of the combined TAMS and Process Sampling Monitoring System in FY06 the error rate declined over 80% through FY 2010

SSP Quality Lessons Learned - RBQS Results

Process Induced Categories Monthly Average



	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010
Task Related	162	140	65	58	43
Collateral	36	40	37	35	31
Found FOD	3	2	2	1	1

Process Induced Errors – Nonconformances caused as a direct result of processing activities

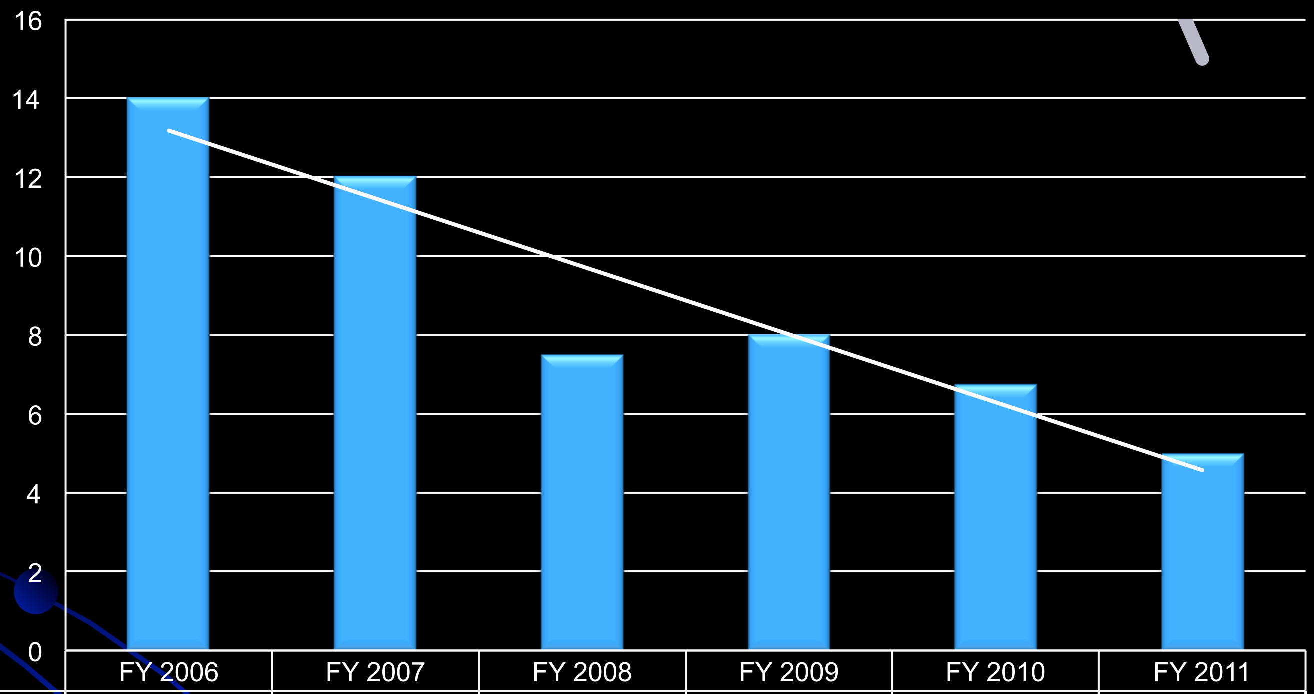
3 categories –
Task Related
Collateral Damage
FOD

Task Related Errors reduced by over 64% by FY09

Total Process Induced errors reduced by over 53% by FY09

SSP Quality Lessons Learned - RBQS Results

Process Escape FY Rate



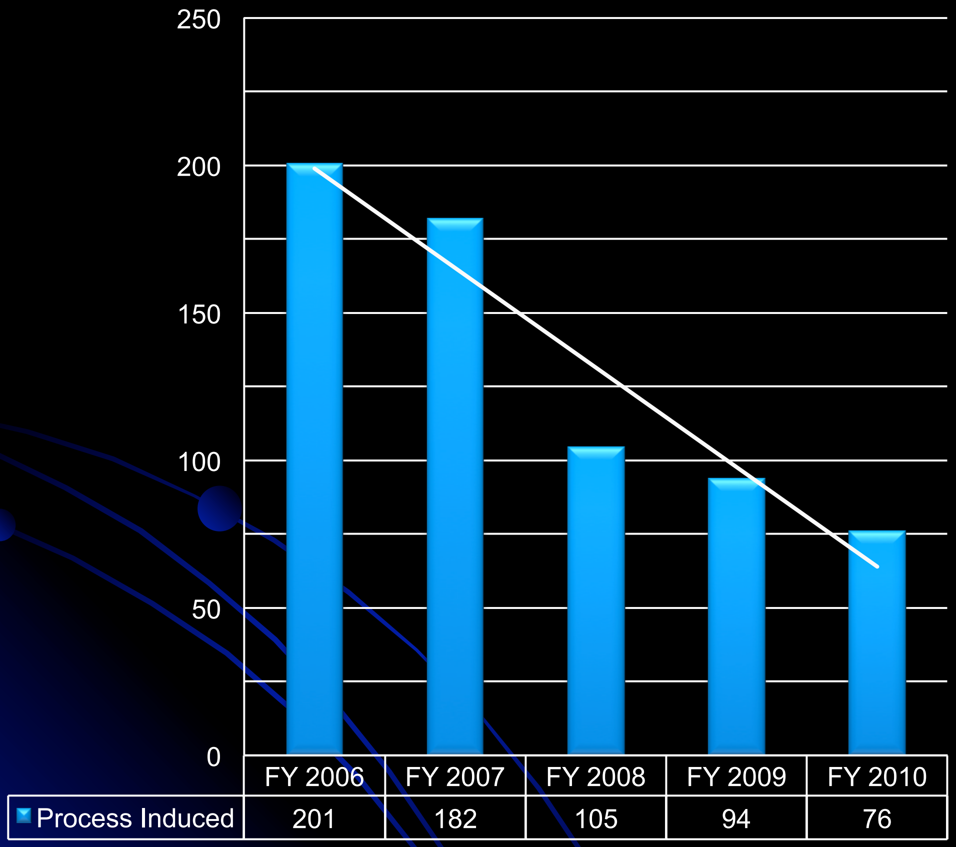
	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
PEs per flow	14	12	7.5	8	6.75	5
STS Flows	2	3	4	5	4	3
Total PEs	28	36	30	40	27	15

Process Escapes per flow declines over 60% through FY 2010

Note: Rate based on the average of Total Process Escapes per STS Flow (PEs per flow)

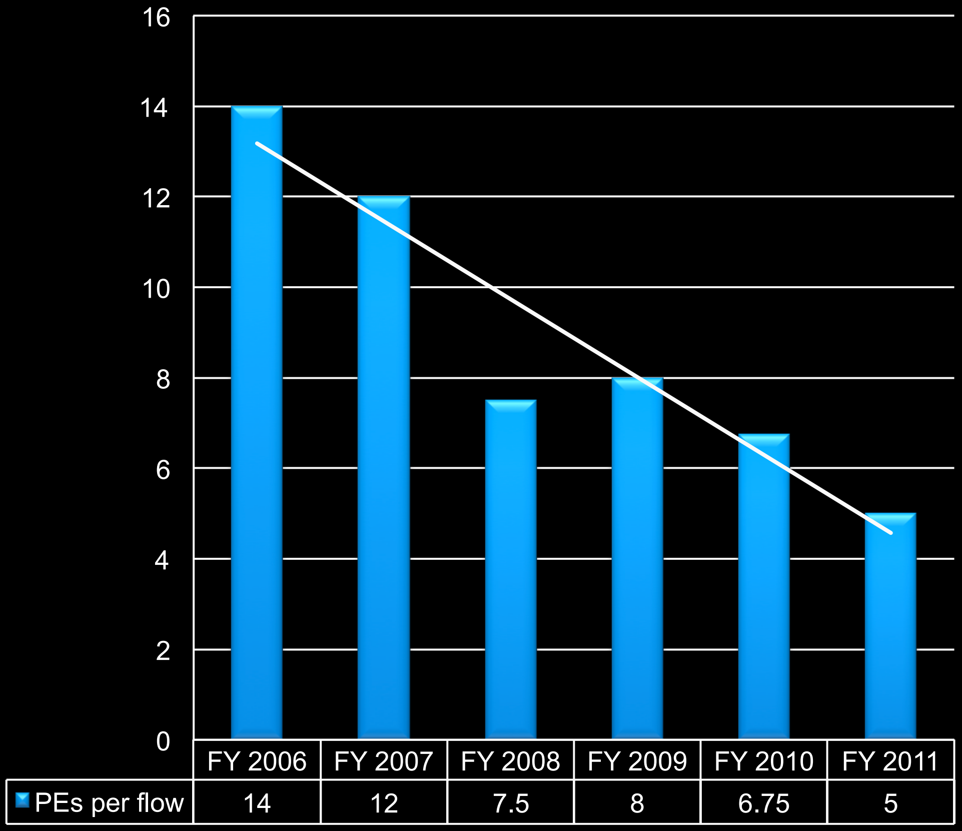
SSP Quality Lessons Learned - RBQS Results

Process Induced Monthly Average



	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010
Process Induced	201	182	105	94	76

Process Escape FY Rate



	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
PEs per flow	14	12	7.5	8	6.75	5

SSP Quality Lessons Learned

1. **Risk Score Card**
   - Provides a standardized method for calculation of likelihood and consequence
2. **Hierarchy of Controls**
   - Ranks controls based on retention, vulnerability and distribution
3. **DATOM Analysis**
   - Analyzes key attributes of a process to determine potential success
4. **Control Based Risk Assessment (CoBRA)**
   - Performs Risk Assessments by analyzing control strength instead of depending on probabilities for likelihood determination
5. **Control Based Cause Analysis**
   - Analyzes failures related to controls (missing, weak or bypassed)
6. **Predictive Control Analysis**
   - Predicts where controls are likely to fail
7. **Process Design Tool**
   - Maps processes to align contractual and regulatory requirements with operational actions
8. **Risk Integrated Process Design (RIPD)**
   - Develops and analyzes processes based on potential consequences of actions
9. **Process Sampling**
   - Measures the health of a process through continuous monitoring

SSP - Quality Lessons Learned

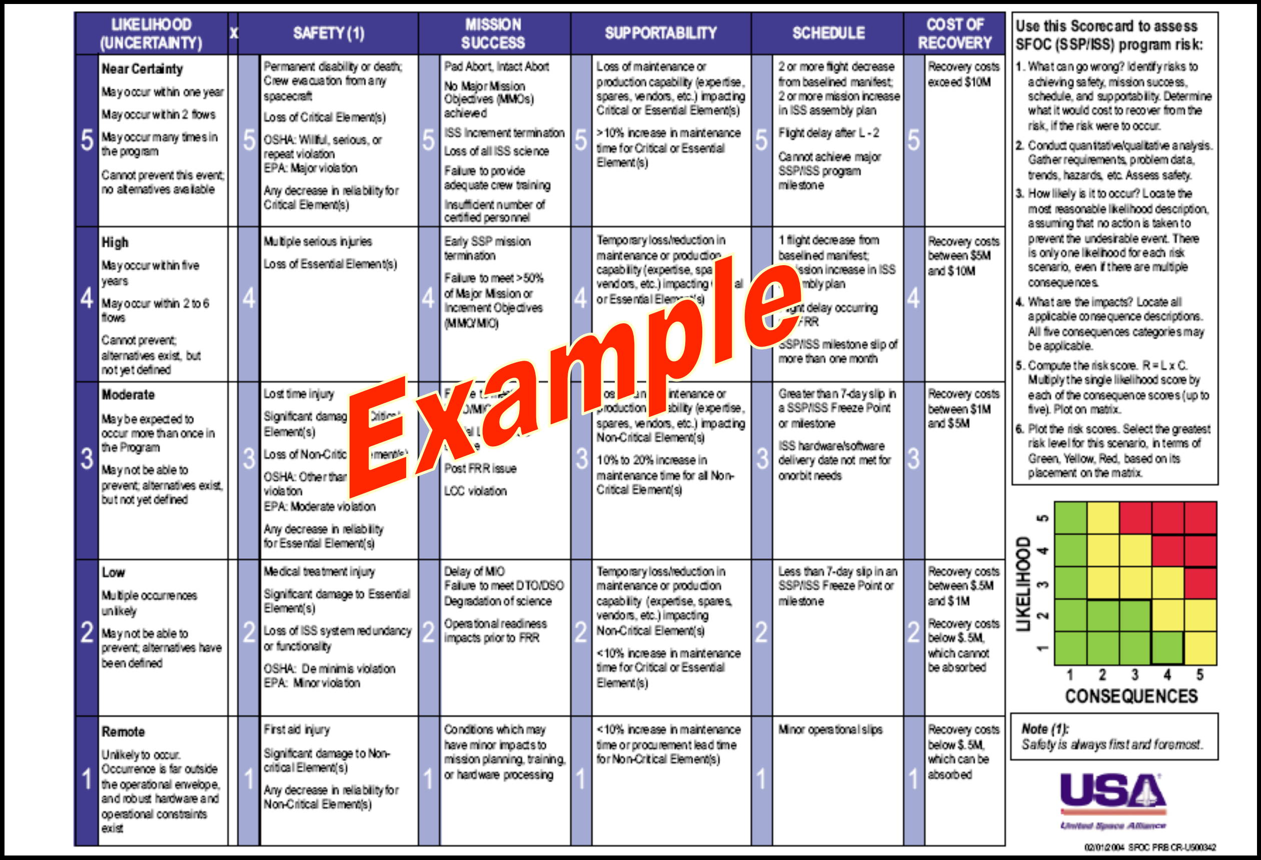
Risk Score Card

Risk is calculated as a product of:

(The severity of a potential consequence)

X

(The likelihood of each consequence occurring)



LIKELIHOOD (UNCERTAINTY)		x	SAFETY (1)		MISSION SUCCESS		SUPPORTABILITY		SCHEDULE		COST OF RECOVERY	
5	**Near Certainty** May occur within one year May occur within 2 flows May occur many times in the program Cannot prevent this event; no alternatives available		5	Permanent disability or death; Crew evacuation from any spacecraft Loss of Critical Element(s) OSHA: Willful, serious, or repeat violation EPA: Major violation Any decrease in reliability for Critical Element(s)	5	Pad Abort, Intact Abort No Major Mission Objectives (MMOs) achieved ISS Increment termination Loss of all ISS science Failure to provide adequate crew training Insufficient number of certified personnel	5	Loss of maintenance or production capability (expertise, spares, vendors, etc.) impacting Critical or Essential Element(s) >10% increase in maintenance time for Critical or Essential Element(s)	5	2 or more flight decrease from baselined manifest; 2 or more mission increase in ISS assembly plan Flight delay after L - 2 Cannot achieve major SSP/ISS program milestone	5	Recovery costs exceed $10M
4	**High** May occur within five years May occur within 2 to 6 flows Cannot prevent; alternatives exist, but not yet defined		4	Multiple serious injuries Loss of Essential Element(s)	4	Early SSP mission termination Failure to meet >50% of Major Mission or Increment Objectives (MMO/MIO)	4	Temporary loss/reduction in maintenance or production capability (expertise, spa[illegible] vendors, etc.) impacting [illegible]al or Essential Elem[illegible](s)	4	1 flight decrease from baselined manifest; [illegible]ission increase in ISS [illegible]mbly plan [illegible]ght delay occurring [illegible]FRR SSP/ISS milestone slip of more than one month	4	Recovery costs between $5M and $10M
3	**Moderate** May be expected to occur more than once in the Program May not be able to prevent; alternatives exist, but not yet defined		3	Lost time injury Significant damag[illegible] Critical Element(s) Loss of Non-Critic[illegible]ment(s) OSHA: Other than [illegible] violation EPA: Moderate violation Any decrease in reliability for Essential Element(s)	3	F[illegible]e t[illegible] [illegible]O/MIO [illegible]al L[illegible] [illegible]e Post FRR issue LOC violation	3	[illegible]os[illegible] in[illegible]intenance or production [illegible]ability (expertise, spares, vendors, etc.) impacting Non-Critical Element(s) 10% to 20% increase in maintenance time for all Non-Critical Element(s)	3	Greater than 7-day slip in a SSP/ISS Freeze Point or milestone ISS hardware/software delivery date not met for onorbit needs	3	Recovery costs between $1M and $5M
2	**Low** Multiple occurrences unlikely May not be able to prevent; alternatives have been defined		2	Medical treatment injury Significant damage to Essential Element(s) Loss of ISS system redundancy or functionality OSHA: De minimis violation EPA: Minor violation	2	Delay of MIO Failure to meet DTO/DSO Degradation of science Operational readiness impacts prior to FRR	2	Temporary loss/reduction in maintenance or production capability (expertise, spares, vendors, etc.) impacting Non-Critical Element(s) <10% increase in maintenance time for Critical or Essential Element(s)	2	Less than 7-day slip in an SSP/ISS Freeze Point or milestone	2	Recovery costs between $.5M and $1M Recovery costs below $.5M, which cannot be absorbed
1	**Remote** Unlikely to occur. Occurrence is far outside the operational envelope, and robust hardware and operational constraints exist		1	First aid injury Significant damage to Non-critical Element(s) Any decrease in reliability for Non-Critical Element(s)	1	Conditions which may have minor impacts to mission planning, training, or hardware processing	1	<10% increase in maintenance time or procurement lead time for Non-Critical Element(s)	1	Minor operational slips	1	Recovery costs below $.5M, which can be absorbed

Example

Use this Scorecard to assess SFOC (SSP/ISS) program risk:

1. What can go wrong? Identify risks to achieving safety, mission success, schedule, and supportability. Determine what it would cost to recover from the risk, if the risk were to occur.
2. Conduct quantitative/qualitative analysis. Gather requirements, problem data, trends, hazards, etc. Assess safety.
3. How likely is it to occur? Locate the most reasonable likelihood description, assuming that no action is taken to prevent the undesirable event. There is only one likelihood for each risk scenario, even if there are multiple consequences.
4. What are the impacts? Locate all applicable consequence descriptions. All five consequences categories may be applicable.
5. Compute the risk score. R = L x C. Multiply the single likelihood score by each of the consequence scores (up to five). Plot on matrix.
6. Plot the risk scores. Select the greatest risk level for this scenario, in terms of Green, Yellow, Red, based on its placement on the matrix.

LIKELIHOOD					
5	🟩	🟨	🟥	🟥	🟥
4	🟩	🟨	🟨	🟥	🟥
3	🟩	🟨	🟨	🟨	🟥
2	🟩	🟩	🟩	🟨	🟨
1	🟩	🟩	🟩	🟩	🟨
	1	2	3	4	5
	CONSEQUENCES				

Note (1):
Safety is always first and foremost.

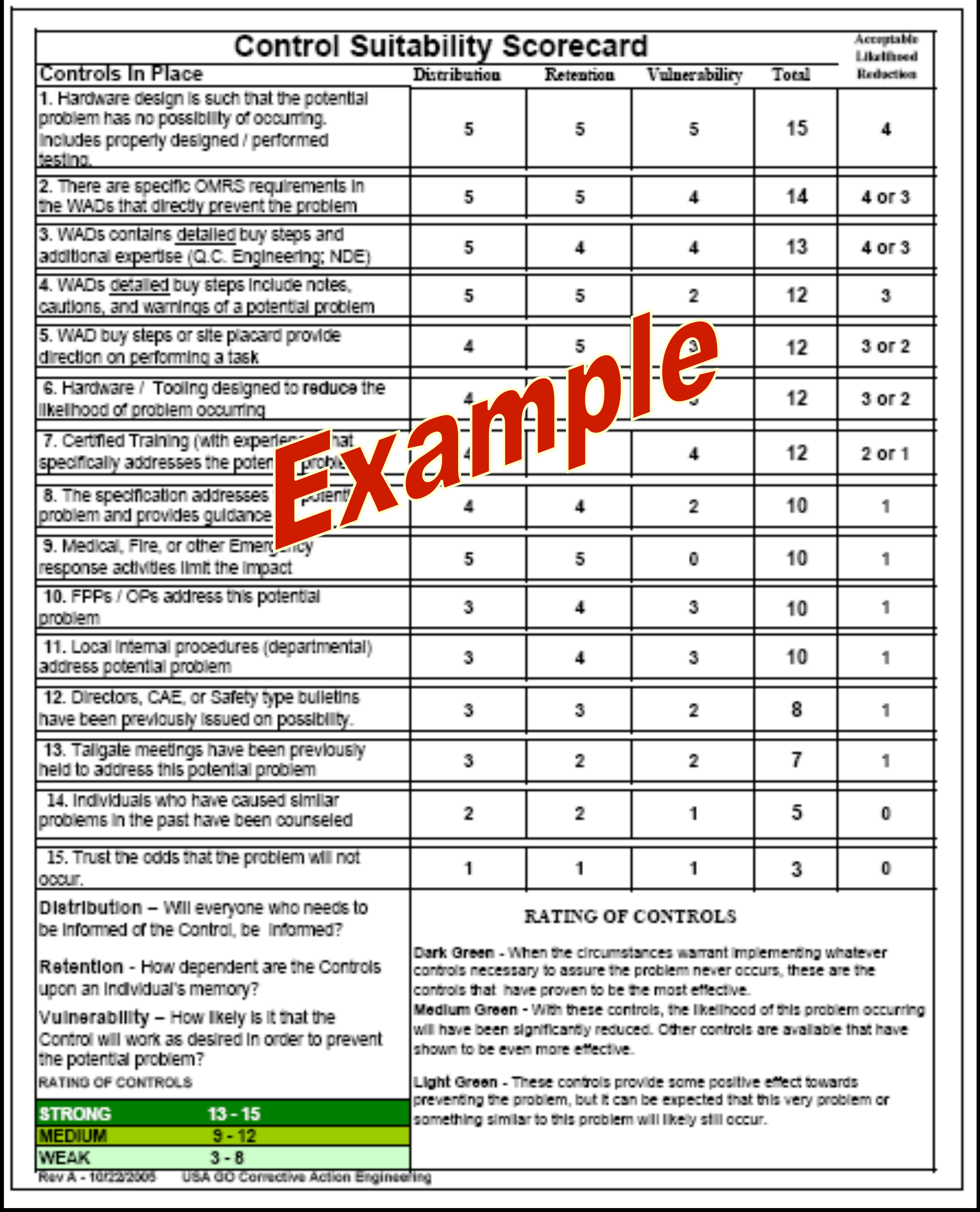
United Space Alliance

02/01/2004 SFOC PRB CR-U500342

SSP - Quality Lessons Learned

Hierarchy of Controls

- Distribution
  - Has everyone who could influence the outcome or objective been informed of the control?
- Retention
  - For those needing to take action, how much of what is expected to be done up to their memory versus what is clearly provided to them at the time those actions are to be taken?
- Vulnerability
  - Does everyone have a clear understanding of what is expected? Is that expectation enforced by management? Is that expectation within the cultural norm?



Control Suitability Scorecard

Controls In Place	Distribution	Retention	Vulnerability	Total	Acceptable Likelihood Reduction
1. Hardware design is such that the potential problem has no possibility of occurring. Includes properly designed / performed testing.	5	5	5	15	4
2. There are specific OMRS requirements in the WADs that directly prevent the problem	5	5	4	14	4 or 3
3. WADs contains detailed buy steps and additional expertise (Q.C. Engineering; NDE)	5	4	4	13	4 or 3
4. WADs detailed buy steps include notes, cautions, and warnings of a potential problem	5	5	2	12	3
5. WAD buy steps or site placard provide direction on performing a task	4	5	3	12	3 or 2
6. Hardware / Tooling designed to reduce the likelihood of problem occurring	4	[illegible]	[illegible]	12	3 or 2
7. Certified Training (with experien[illegible] that specifically addresses the poten[illegible] proble[illegible]	4	[illegible]	4	12	2 or 1
8. The specification addresses [illegible] potenti[illegible] problem and provides guidance [illegible]	4	4	2	10	1
9. Medical, Fire, or other Emerg[illegible]ncy response activities limit the impact	5	5	0	10	1
10. FPPs / OPs address this potential problem	3	4	3	10	1
11. Local internal procedures (departmental) address potential problem	3	4	3	10	1
12. Directors, CAE, or Safety type bulletins have been previously issued on possibility.	3	3	2	8	1
13. Tailgate meetings have been previously held to address this potential problem	3	2	2	7	1
14. Individuals who have caused similar problems in the past have been counseled	2	2	1	5	0
15. Trust the odds that the problem will not occur.	1	1	1	3	0

Distribution – Will everyone who needs to be informed of the Control, be informed?

Retention - How dependent are the Controls upon an individual's memory?

Vulnerability – How likely is it that the Control will work as desired in order to prevent the potential problem?

RATING OF CONTROLS

STRONG	13 - 15
MEDIUM	9 - 12
WEAK	3 - 8

RATING OF CONTROLS

Dark Green - When the circumstances warrant implementing whatever controls necessary to assure the problem never occurs, these are the controls that have proven to be the most effective.

Medium Green - With these controls, the likelihood of this problem occurring will have been significantly reduced. Other controls are available that have shown to be even more effective.

Light Green - These controls provide some positive effect towards preventing the problem, but it can be expected that this very problem or something similar to this problem will likely still occur.

Rev A - 10/22/2005 USA GO Corrective Action Engineering

Example

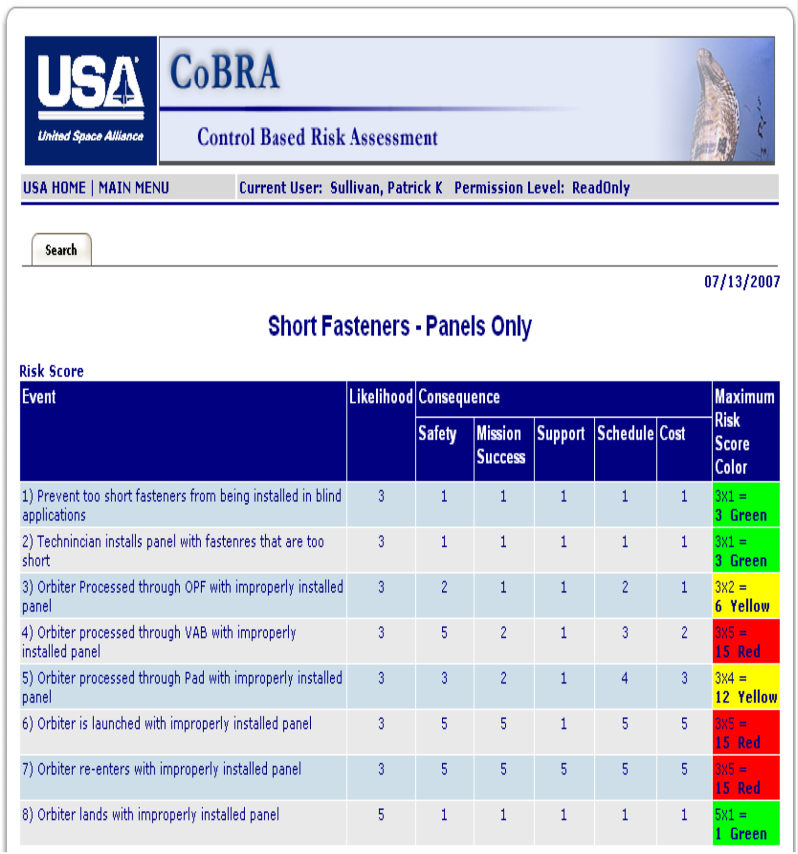
SSP - Quality Lessons Learned

- DATOM Analysis evaluates a process based on five key attributes to determine if a process is capable and repeatable
  - Define
    - States the actions to be performed so it cannot be misunderstood or interpreted in more than one way
  - Assign
    - Specifies a single person or organization responsible for ensuring the success of the actions
  - Train
    - Identifies the necessary skills/knowledge/experience required to perform the actions
  - Organize
    - Provides the necessary environment and tools that facilitate successful performance of the actions
  - Monitor
    - Monitors, Measures and Manages the actions performed

SSP - Quality Lessons Learned

Control Based Risk Assessment CoBRA

- Determines the likelihood of an unwanted event by analyzing the controls designed to prevent or mitigate consequences
  - Bases risk assessment on facts not intuition
  - Does NOT depend on the probability of the occurrence
  - Evaluates risk over the entire life of the process
- Assists in determining best process enhancements and precludes the use of ineffective corrective actions
- Bridges communication between technical employees and management



Current User: Sullivan, Patrick K Permission Level: ReadOnly

07/13/2007

Short Fasteners - Panels Only

Risk Score

Event	Likelihood	Consequence					Maximum Risk Score Color
		Safety	Mission Success	Support	Schedule	Cost	
1) Prevent too short fasteners from being installed in blind applications	3	1	1	1	1	1	3X1 = 3 Green
2) Technincian installs panel with fastenres that are too short	3	1	1	1	1	1	3X1 = 3 Green
3) Orbiter Processed through OPF with improperly installed panel	3	2	1	1	2	1	3X2 = 6 Yellow
4) Orbiter processed through VAB with improperly installed panel	3	5	2	1	3	2	3X5 = 15 Red
5) Orbiter processed through Pad with improperly installed panel	3	3	2	1	4	3	3X4 = 12 Yellow
6) Orbiter is launched with improperly installed panel	3	5	5	1	5	5	3X5 = 15 Red
7) Orbiter re-enters with improperly installed panel	3	5	5	5	5	5	3X5 = 15 Red
8) Orbiter lands with improperly installed panel	5	1	1	1	1	1	5X1 = 1 Green

SSP - Quality Lessons Learned

- Conclusion
  - People Make Mistakes
  - Risk Management is an aggregate of activities designed to reduce the likelihood of an unwanted event from occurring
  - Risk Based Quality is the design and use of behavioral controls to reduce the likelihood of human error resulting in a negative consequence