D-14764

METHODOLOGY & CRITERIA for RISK ASSESSMENT of COMMERCIAL OFF-THE-SHELF (COTS) PARTS

MAY 5, 1997

MIKE SANDOR

OFFICE 507 ELECTRONIC PARTS ENGINEERING

JET PROPULSION LABORATORY
CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA

FORWARD

The activities described in this report were performed by the Jet Propulsion Laboratory, California Institute of Technology, and were sponsored by the National Aeronautics and Space Administration, Office of Safety and Mission Assurance, Washington, DC. The work herein was accomplished under NASA RTOP No. UPN 323-79-2F and the JPL Technical Infrastructure Program.

The author wishes to acknowledge the following for their special contributions to this work:

S. Agarwal
E. Cuddihy
J. Okuno
D. N. Nguyen
E. Grigorian

ABSTRACT

System and subsystem engineering within the aerospace and commercial industries are using risk and decision analysis in conjunction with trade study processes to aide in reducing spacecraft system cost, assessing Commercial Off-The-Shelf (COTS) component reliability, selecting among competing technologies, and weighing the benefits of cost and risk of implementing candidate technologies and components. These methods have been successful at the system and subsystem levels. These methods are also useful for a parts engineer who must continually evaluate COTS part candidates where little or no information is known. A set of criteria for part evaluation and review would be valuable to a parts engineer that would help in performing a risk assessment and in making the final decision as to whether a COTS part can be used in a given application or not. The work herein lists criteria developed and demonstrates how risk assessment and decision making were used for assigning a risk classification to a Commercial Flash Memory electronic part. Various references materials in risk management and decision making including the work by Dr. Michael A. Greenfield at NASA Headquarters were helpful in implementing risk and decision making techniques.

CONTENTS

SECTION

1.0 BACKGROUND

2.0 INTRODUCTION TO RISK MANAGEMENT AND DECISION MAKING

3.0 PRELIMINARY STEP TAKEN TOWARD COTS EVALUATIONS

4.0 EVALUATION CRITERIA DEFINED

5.0 RESULTS APPLIED

6.0 SUMMARY OF RESULTS

APPENDIX A
Risk Management " Risk as a Resource" Presentation to JPL, Dr. Michael A. Greenfield, Deputy Associate Administrator, Office of Safety and Mission Assurance, NASA Headquarters, February 26, 1997

APPENDIX B
Risk Analysis References courtesy of the University of Guelph

---

References:

1. Part Construction Analysis for Intel Part No. DA28F016SV in Plastic Package, Report No. 1, Jet Propulsion Laboratory, Electronic Parts Engineering Office, Oct. 17, 1996
2. Part & Package Construction Analysis for Intel Part No. DA28F016SV in Plastic Package, Report No. 2, Jet Propulsion Laboratory, Electronic Parts Engineering Office, Oct. 25, 1996
3. Electrical Test Performance for Intel Part No. DA28F016SV in Plastic Package Under Extended Hot & Cold Temperature Ranges, Jet Propulsion Laboratory, Electronic Parts Engineering Office, Oct. 17, 1996
4. Burn-In Results for Intel Part No. DA28F016SV in Plastic Package, Jet Propulsion Laboratory, Electronic Parts Engineering Office, Jan. 20, 1997
5. Chemical Analysis and Outgassing of Plastic Packaged Parts, Jet Propulsion Laboratory, Electronic Parts Engineering Office, April 22, 1997
6. Intel Flash Memory Data Sheet

1.0 BACKGROUND

1.1 THE NEED FOR ASSIGNING RISK LEVEL WITH LITTLE DATA AVAILABLE

The next generation of spacecraft has the formidable challenge to revolutionize spacecraft design and construction. Specific objectives include affordability, significant reduction in mass and volume, and high integration of on-board operations using ultra micro miniaturization of electronics and complex computing functions offered with commercial off-the-shelf (COTS) parts and technologies. Determining what parts and technologies can accommodate this end is no easy task. Informed planning and risk management are essential to building a reliable spacecraft. Any unknown risk associated with using advanced electronic technologies and COTS parts can result in a significantly degraded or even catastrophic mission. To mitigate such events in the past, developers and designers, with the help of the parts engineer, have taken conservative measures to purchase the best available and qualified parts. This was accomplished by putting the parts through elaborate tests and screens to separate out parts that may jeopardize long term reliability. These options are still available and can be used today. However these options are becoming less the norm and more emphasis is being put on choosing reliable parts without the high cost of testing, elaborate screening, and qualifications. There is now a need to make risk assessments based on what information or data exists, without a formal qualification, and little additional testing if any. This is the challenge.

2.0 INTRODUCTION

2.1 RISK MANAGEMENT

Risk management comes under the general field of management and can be considered as a special field. "Management" may be defined as the process of planning, organizing, leading, and controlling the resources and activities of an organization in order to fulfill its objectives most cost-effectively. Risk management is devoted to minimizing the adverse effects of accidental loss on the organization. For the parts engineer risk management is devoted to minimizing or preventing the loss or malfunction of a spacecraft due to a faulty part. In a general sense part risk management is a process that includes planning, organizing, leading, and controlling the activities of part evaluation and selection. Part risk management can also be defined in terms of a decision making process. Five steps in this decision making process are 1) identifying exposures of part failures that may interfere with the spacecraft objectives, 2) examining feasible alternatives for dealing with these exposures, 3) selecting a risk management technique, 4) implementing the chosen technique, and 5) validating the results of the chosen technique. The point here is that there are two aspects to risk management. One aspect emphasizes the management aspect and the other is the decisional aspect.

2.2 DECISION MAKING

Decision making is the result of very small incremental gains in the understanding of decision making processes and human thought, and the application of technology tools to support the process. In the absence of predictive information, decision is process of guessing the future consequences of impending choice. Human decision makers have traditionally looked for support for their decisions. Support can from may sources such as quantitative data, analysis, advice from a consultant, or even ones horoscope. However there are some good principles to follow in the decision process such as proceed slowly, consider the alternatives, identify the risks, and build a contingency plan before choosing a course of action. It is better to generate creative choices and then systematically them rather than to guess. A key step in the decision process is to point out information gaps that must be filled before a decision can be made. Modern decision making has now advanced to where computers make decisions or choose a course of action based on algorithms, weighting factors, and information, analysis, and data that is fed in to the computer. The methodology envisioned for this RTOP in deciding COTS acceptability was more along the following path:

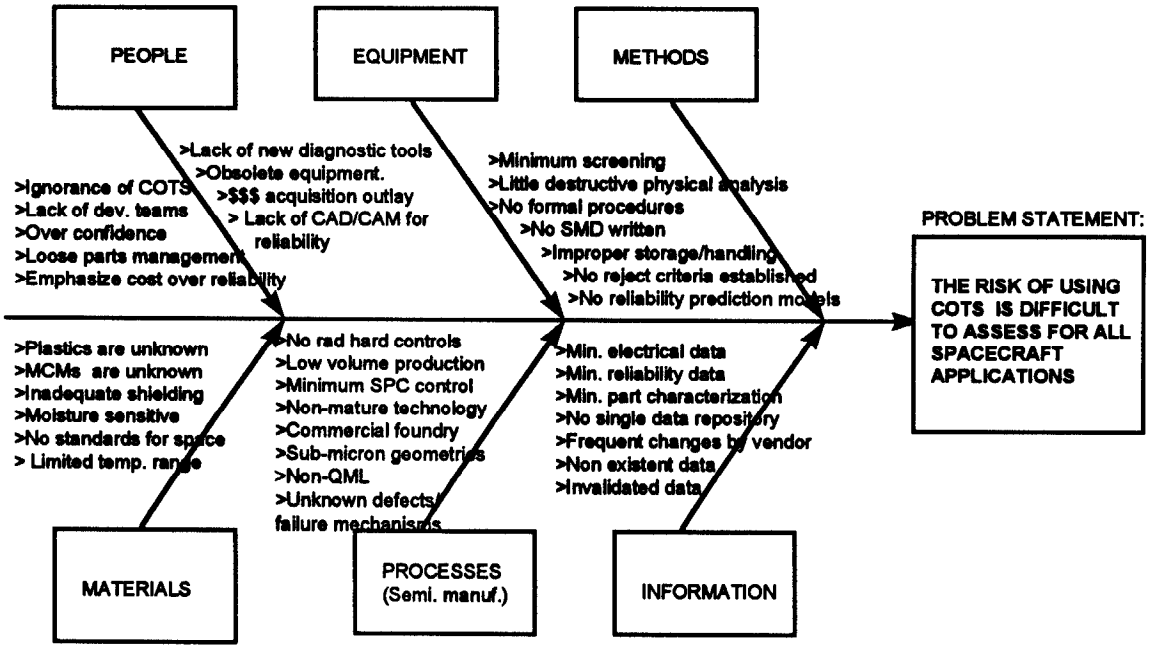
1. Define the problem
2. Formulate decision objective
3. Generate the criteria
4. Gather the data
5. Evaluate the data against the criteria
6. Make a risk assessment for each criteria based on mitigation options
7. Assign a risk level

3.0 PRELIMINARY STEPS TAKEN TOWARD COTS EVALUATIONS

There were many attempts to try and understand the issue of COTS parts and their future acceptance in aerospace hardware. One of the first issues to understand was an acceptable definition of what COTS parts are. One definition says Commercial Off-The-Shelf parts include all commercial/industrial grade parts such as Plastic Encapsulated Microcircuits (PEMS), Ceramic parts, Known-Good-Die (KGD), and Multi Chip Modules (MCM). COTS are typically manufactured in high volume production lines and have the lowest unit cost compared to military, high reliability, or radiation hardened produced parts, Quality, Reliability, Performance, and Vendor's Liability can vary significantly from vendor to vendor. Another short definition for COTS is "Check On The Supplier" inferring that COTS parts are risky and little is known about them or their source.

Because it is commonly believed that COTS parts are risky to use, a fishbone diagram was developed to define this problem. In the Diagram shown on the following page the casual determinants were defined: People, Equipment, Methods, Materials, Processes, and Information. Within each of these generic casual determinants specific causes for why COTS parts are risky were identified.

Office of Electronic Parts Engineering



Causal Fishbone Diagram 1

From the above results it was apparent that there was too many causal effects to address in order to minimize risk of using COTS parts. Another attempt was taken to identify more explicitly what factors must be understood in order to eliminate any risk and insure the best available COTS parts would be used in system hardware. Chart 1 on the next page identified six factors for which if all information was known would achieve > 95% success in reliability and performance with COTS.

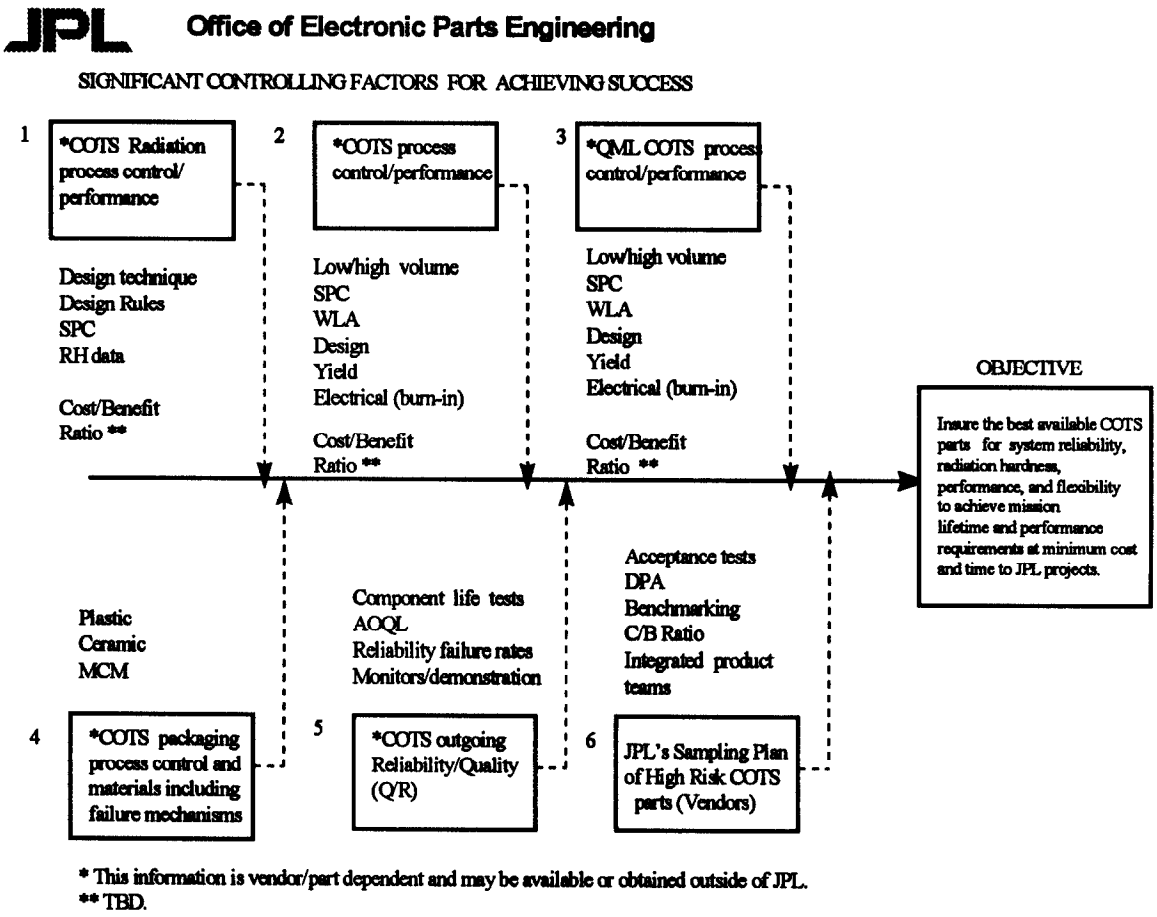


CHART 1

The next step in the process was to determine what actions could be taken for each of the subcauses that lead to COTS being risky and list what actions could be taken. The following table lists possible actions and ranks them according to doable, cost of implementing the action, time to complete the action, and their impact to resolving the problem statement. From this table and the ranking, it was decided that obtaining all existing information and data on COTS parts was most doable, very cost effective, could be achieved within the time guidelines and would have the best impact on reducing risk of COTS. All categories were ranked according to total score with the lowest score being the most favorable solution and the logical place to start.

Category	CAUSE	SubCauses	Possible Actions	Strong =1 Medium =3 Weak =9 Doable	High =9 Medium =3 Low =1 Cost	FY96 =1 FY97 =3 FY98 =9 Time	High =1 Medium =3 Low =9 Impat	Total
(People)	User Over/under confidence in COTS	Ignorance of COTS Q&R	Collect information; Self-education of staff and JPL users	1	1	1	1	4
(People)	User Misapplied	Lack of characterization data for space environment	Educate & warn users of 'traps' and pitfalls	3	1	1	3	8
(Methods)	Design Flow	Device may not have sufficient EOS/ESD protection built into its design	Inform users; suggest board level implementation techniques; impose strict handling criteria	3	1	1	3	8
(Materials)	PEMs Packaging Related Concerns	Thermomechanical shear stress related failures when exposed to temp cycling	Determine application true temperature extremes; Eliminate unnecessary temp. cycles	3	1	1	3	8
(Materials)	PEMs Packaging Related Concerns	Moisture contamination due to nonhermetic sealing	For moisture, do bakeout & place strict parts handling controls thereafter	1	3	1	3	8
(Machines)	Vendor's Inspection Equipment	Inadequate tools in use due to emphasis on cost over quality & reliability	If risk verified, institute in-house inspections on a sample basis	1	3	3	3	10
(Methods)	Fab Processes	Process not designed to be rad hard (latchup & total dose)	Not much for latchup; possible shielding options	3	3	3	1	10
(Methods)	Fab Processes	Inadequate quality controls at some vendors	If risk verified, institute in-house inspections on a sample basis	3	3	3	1	10
(People)	User Over/under confidence in COTS	Incorrect generalization of COTS performance based on track record of other COTS parts/vendors	Avoid generalizing; educate user community	1	1	1	9	12
(Methods)	Design Flow	Device may not have incorporated Design for Test practices (resulting in low fault coverage)	Add test vectors to increase fault coverage & test	3	3	3	3	12
(Methods)	Test	Insufficient environmental (radiation, hi/low	Conduct tests	1	9	1	1	12

		environmental (radiation, hi/low temp, humidity) testing						
(Methods)	Test	Insufficient mechanical (shock/vibration, Seal) testing	Conduct tests	1	9	1	1	12
(Methods)	Test	Insufficient electrical (functional, parametric, burn-in/life-test) testing	Conduct tests	1	9	1	1	12
(Methods)	Design Flow	Device may not have SEU hardened design	Inform users; suggest system level mitigation & implementation of fault tolerance techniques	3	1	1	9	14
(Methods)	Design Flow	Device may not have incorporated conservative design rules or Design for Reliability	Suggest implementation of redundancy/fault tolerance techniques; look for alternate devices	3	1	1	9	14
(Materials)	PEMs Packaging Related Concerns	Radiation effects on plastic materials are unknown	Study effects by conducting tests	3	9	1	1	14
(Materials)	PEMs Packaging Related Concerns	Impurities contamination due to nonhermetic sealing	Test for effects from existing contamination; Place strict parts handling controls to limit further contamination	3	3	1	9	16
(Methods)	Fab Processes	Inadequate process monitoring controls in place to monitor reliability at some vendors	Establish quality level by performing QCI & DPA type tests	3	9	3	1	16
(Methods)	Fab Processes	Inadequate process data collected from a new process to consider the process "qualified", at some vendors	Wait for process to mature OR put parts on test to collect data	3	9	3	1	16
(Methods)	Fab Processes	Inadequate/nonexistant reliability test structure data at some vendors	Fab test structures and test	3	9	3	1	16
(Methods)	Fab Processes	No rad controls exercised in fab even if process is randomly rad tolerant	Perform lot-specific radiation testing	3	9	3	3	18

(Machines)	Vendor's CAE Tools	Inadequate design tools in place to do Design for Reliability & Test, due to emphasis on cost over Q & R	Not much	9	9	9	9	36

Sorted by Ascending order in the following categories:
Total Score, Cost, and Time

Notes: 1. Doable: This implies that a solution to a particular cause can be partially or totally implemented..

2. Cost: The cost is the relative cost to accomplish a solution compared to all other possible solutions.

3. Time: This is a forecast to implement a partial or total solution by FY.

4. Impact: This indicates the affect a solution would have on correcting the problem statement.

(The lower the sum the more favorable is the acceptance of a solution.)

4.0 EVALUATION CRITERIA DEFINED

Because of the emphasis by JPL to deliver future spacecraft using a better, faster, cheaper approach, it was necessary to look at evaluating and using COTS parts in the same light. The action study completed above showed that if one could get all the information and data needed from a parts vendor and not perform any special testing the better, faster, cheaper objective would be satisfied. Therefore a set of performance criteria was developed with indicators. The indicators were chosen as a minimum set upon which risk assessment could be ascertained as to whether a COTS part was acceptable for a given application or requirement. However another set of decision criteria was deemed necessary whereby JPL could perform testing and data to augment what data the vendor could or could not provide. Early on it was believed that all data and information requested of a vendor would not be available. The premise was to obtain as much available information as possible and quickly. The following criteria was developed and the rationale behind some of the information indicators.

Vendor Criteria

1. Vendor Generic Information - Establish a vendor contact from whom you can obtain information from as needed and determine if a cooperative relationship can develop. Determine if the vendor is a QML supplier for the parts to be evaluated.
2. Generic Part Information - Obtain part information such as description, part number, cost, quality level and whether it is fully in production and available.

3. Process/Technology Information - Determine the technology used to fabricate the parts, where the process is done, and what controls are in place such as SPC and test structures.
4. Design Technology Information - Determine how current is the vendor's design tools to enhance reliability, performance, testing, and modeling.
5. Reliability Assurance/Data Information - Obtain all the vendor's reliability data generic and specific to the part type under evaluation.
6. Quality Assurance/Data Information - Obtain all the vendor's quality data that would demonstrate his out going quality and part workmanship.
7. Test Information - Determine the completeness of testing parts at temperature, parameters specified on the data sheet, and where the testing is done.
8. Screening/Data Information - Obtain vendor's data on 100% lot screening was performed for temperature cycling, electrical, power cycling, and burn-in.
9. Part Performance/Data Information - Obtain vendor's part data from characterization and qualification for speed, ESD, latch-up, and power.
10. Package/Data Information - Obtain plastic encapsulated package data for steam autoclave, temperature cycling, humidity, Tg, and molding compound.
11. Radiation Performance/Data Information - Obtain vendor's data for low dose effects, high dose rate effects, SEE, latch-up and recent process improvements.
12. KGD Data Information - Obtain flows and determine availability of die to flows.

JPL Criteria for Augmentation

13. Chip Overview Information - Determine if there are any obvious anomalies with the die for defects, foreign material, correct revision and mask stepping.
14. Package DPA Information - Obtain wire pull strength, dye penetrant, package weight, glass transition, outgassing, and possibly C-Sam data.
15. Chip DPA Information - Obtain cross section data for metallization, oxide, via and contacts, passivation, polysilicon.
16. Test/Burn-in Information - Obtain test data at device operating temperatures.

Using the above agreed upon criteria, a working and interactive template was developed in Excel format that would facilitate entering information and data as it was obtained. The template format also allowed adding, modifying, or removing risk indicators as necessary. This would accommodate a better fit to different part types, and or project needs. The template is designed to be flexible and without restriction when gathering information for evaluation. The following example was used for evaluating a commercial Flash Memory part. The example shows that all information is not available but important information was still obtained that led to some risk analysis, decision making, and acceptance of the part .

5.0 RESULTS APPLIED

5.0 Results Applied

RISK ASSESSMENT AND CRITERIA FOR FLASH MEMORY

THIS TEMPLATE IS UPDATED AS NEW INFORMATION IS AVAILABLE.

JET PROPULSION LABORATORY COTS PART EVALUATION
by Electronic Parts Engineering Office 507

Note: Any small red square symbol indicates there is a note attached to that cell.

For Vendor Input

Vendor:	INTEL CORPORATION
Contact:	Anna Spaanem
Part Number Evaluated:	DA28F016SV, (1M x 16), (2M x 8)
Part Function:	CMOS NONVOLATILE FLASH MEMORY

List of criteria used for COTS	Current Status
1. Vendor	Information Complete
2. Part	Information Complete
3. Process Technology	Partial Information Received
4. Design	No Information Available
5. Reliability Assurance	Partial Information Received
6. Quality Assurance	No Information Available
7. Testing	No Information Available
8. Screening	No Information Available
9. Performance	Partial Information Received
10. Package	Partial Information Received
11. JPL Radiation	Partial Information Received
12. Known Good Die	N/A
13. JPL Chip Overview	Information Complete
14. JPL DPA (Package)	Information Complete
15. JPL DPA (Die Cross Section)	Information Complete
7a. JPL Testing/Burn-In	Information Complete

List of criteria	JPL's Evaluation
1.Vendor	Accept
2. Part	Accept
3.Process Technology	Warning
4. Design	Unknown
5. Reliability Assurance	Warning
6. Quality Assurance	Accept
7. Testing	Unknown
8. Screening	Unknown
9. Performance	Accept
10. Package	Warning
11. JPL Radiation	Warning
12. Known Good Die	N/A
13. JPL Chip Overview	Accept
14. JPL DPA (Package)	Accept
15. JPL DPA (Die Cross	Waived
7a. JPL Testing/Burn-In	Warning

Space Application Risk Level Assigned:

Medium / High

Class Payload:

Class C / Class D

Primary Risk Driver(s):

A. Radiation Performance

Mitigation action:

1. Explore Techniques

B. Infant Mortality

Mitigation action:

1. Perform Burn-in
2. Insure adequacy of BI circuit

Secondary Risk Driver(s):

A. Plastic SMT Part

Mitigation action:

1. Package Bakeout
2. Solder Thermal Profile

1. Manufacturer's (Vendor) Generic Information:

	Vendor's Data	Information Received ->
Manfacturer' Name:	Intel Corporation	X
City:	Folsom	X
State:	CA	X
Country:	US	X
Marketing Contact:	Anna Spaanem	X
Phone:	Call 800-628-8686 (refer to case	X
Fax:	NA	X
Application Engr.	Davinder Singh	X
Phone:	(916) 356-0217	X
Fax:	(916) 356-2892	X
QML Status:	Full QML Certification/Qualification (Class Q) including Plastics. Company contact: Carolyn Moen (602) 554-8450.	X

Insert Code
X = Yes
Y = Not required
Z = Requested
NA = Not Available
TBD = To Be Determined
NAATT = Not Available At This Time
N / A = Non Applicable

2. Generic Part Information:

	Vendor's Data	Information Received
Part Number:	DA28FO16SV	X
Part Description	16-MBIT (1 MBIT x16, 2 MBIT x 8)	X
Part Name:	FlashFile™ Memory	X
Technology Status:	Production	X
Part Availability:	Now	X

Data Sheet (Spec):	Advance Information	X
Quality Level Offered :	Commercial & Extended Temperature	X
Unit Cost:	$67.00	X
Packages Offered:	56-Lead, TSOP; 56-Lead, SSOP	X

3. Process / Technology:

	Vendor's Data	Information Received	*For JPL Use Only (Quality/Risk Evaluation)* Unknown	Low	High	Waived	Accept
Wafer Fab Technology:	0.6 um ETOX™ IV process 627	X					Accept
Process Location:	Intel Fab 7 (Albuquerque, NM)	X					Accept
Process Qualified:	Level III Quality/Reliability	X					Accept
Rad Hard/Rad Tolerant/Non-Rad Hard:	Non Rad Hard	X			High		
Reliability Test Structure Data Available:			X				
SPC Process Monitor Data Available:			X				
EPI or non EPI Process:	EPI	X					Accept
Assembly Location:	Philippines	X					Accept

For JPL Use Only
Risk analysis:

Any commercial non rad hard device that is used in a space application must be tested for RH characteristics.

4. Design Technology:

	Vendor's Data	Information Received	*For JPL Use Only (Quality/Risk Evaluation)* Unknown	Low	High	Waived	Accept
****EDA tools used for EM:**			X				
****EDA tools used for ESD:**			X				
****EDA tools used for EOS:**			X				
****EDA tools used for Latchup:**			X				
****EDA tools used for Antenna:**			X				
****Spice tools used for Hot Electrons:**			X				
SEE Hardened Design:			X				
EDA tools used for fault coverage:			X				
BIST capability on chip:			X				
IDDQ capability on chip:			X				

For JPL Use Only
Risk analysis:

No information is available at this time.

Note: **These are critical design-for-reliability issues for Deep Submicron technologies.

5. Reliability Assurance/Data:

	Vendor's Data	Information Received	*For JPL Use Only (Quality/Risk Evaluation)* Unknown	Low	High	Waived	Accept
Infant Mortality Evaluation (IME):	Ten lots were tested at 6.5v and 125C. Results are 0/2002 after 48 hrs. and 0/2002 after 168 hrs.Intel Report 12/29/95.	X					Accept
Dynamic Lifetest:	Four lots were tested at 6.5V and 125C. Results are 0/249 after 500 hrs. and 2/249 after 1000 hrs. 2 rejs are lccs due to gate oxide breakdown. Intel Report 12/29/95.	X			Burn-In Required		
64K Program Erase Cycle:	Four lots were tested at 0C at 100cyc.; 1K cyc.; 5K.; 10K.; and 50K. Results are 1/530 at 15,010 cycles. There were no additional failures when tested at 70C. Intel Report 12/29/95.	X		Low risk (1 failure out of 50K cyc.)			
Uncycled High Temperature Storage:	Four lots were tested at 140C at 48 hrs.; 168 hrs.; 500 hrs.; and 1000 hrs. Results are 0/180. Intel Report 12/29/95.	X					Accept
Endurance:	TBD						
Data Retention:	TBD						
Post Program/Erase Cycled High Temp. Storage:	Four lots were tested at 140C at 48 hrs.; 168 hrs.; 500 hrs.; and 1000 hrs. Results are 17/4160 after 10K cyc.; 6/520 after 50K cyc.; and 63/1560 after 100K cyc.All rejects were due to single bit charge loss. Intel Report 12/29/95.	X			High risk (multiple failures)		

For JPL Use Only
Risk analysis:

For high reliability applications a dynamic burn-in and post program/erase cycle temperature storage qualification is recommended.

6. Quality Assurance/Data:

	Vendor's Data	Information Received	For JPL Use Only (Quality/Risk Evaluation) Unknown	Low	High	Waived	Accept
Destructive Physical Analysis (DPA) Results:	Part and package analysis completed. See JPL and DPA Labs Reports dated 10/17/96.	X					Accept
Average Outgoing Quality Level defect rate:			X				
Chip Layout provided:			X				
Die Cross Sections provided:			X				

For JPL Use Only Risk analysis:

No risk is evident based on two independent DPA reports.

7. Testing:

	Vendor's Data	Information Received	For JPL Use Only (Quality/Risk Evaluation) Unknown	Low	High	Waived	Accept
No. of Data Sheet Parameters tested @ 25C:			X				
No.of Parameters tested @ Upper/Lower Temp. Limits:			X				
% Bench Testing:			X				
% ATE Testing:			X				
Part Characterization data provided :			X				
In-House or Off Shore Testing:			X				

For JPL Use Only Risk analysis:

No information is available at this time.

8. Screening/Data:

	Vendor's Data	Information Received	For JPL Use Only (Quality/Risk Evaluation) Unknown	Low	High	Waived	Accept
Manufacturing Yields:			X				
Test Temperature(s) :			X				
Temperature Cycling:			X				
Thermal Shock:			X				
Humidity:			X				
Shock/Vibration:			X				
Mechanical:			X				
Electrical:			X				
Power Cycling:			X				
Burn-In (Static vs Dynamic):			X				

For JPL Use Only Risk analysis:

No information is available at this time.

9. Part Performance/Data:

	Vendor's Data	Information Received	For JPL Use Only (Quality/Risk Evaluation) Unknown	Low	High	Waived	Accept
Minimum Frequency:							
Maximum Power Dissipation:							
Temperature Range:	Commercial: 0C to 70C	X					Accept
Vcc Operating:	3.3V or 5V	X					Accept
ESD Sensitivity Rating:	Three lots were tested to the Human Body Model at 2000V for I/O, Vcc, Vccq, Vss, and Vssq. Results were 0/9 for each test. For lots were tested to the Charged Device Model at 500V. Results were 0/11. Intel Report 12/29.95.	X					Accept
Electrical Latch-Up Rating:	Six lots were tested for Vcc, Vpp, and I/O latchup at 25C, 0C, and 125C. Results were 0/57 for all three temperatures. Intel Report 12/29/95.	X					Accept
APS Active Current:	1 mA Typical Icc in Static Mode at 5V; 3.0 mA at 3.3V	X					Accept
CMOS Standby Current:	70 uA at 5V	X					Accept
Access Time:	65ns Max at 5V; 75ns at 3.3V	X					Accept
Write Cycle Time:	75 ns min (3.3V); 65 ns min (5.0v)	X					Accept

For JPL Use Only Risk analysis:

No risk is evident with the part performance indicators.

10. Package/Data:

	Vendor's Data	Information Received	For JPL Use Only (Quality/Risk Evaluation) Unknown	Low	High	Waived	Accept	For JPL Use Only Risk analysis:
Steam Autoclave (PEMS):	Six lots of the TSOP were tested at 121C and 2 stmospheres. Results were 0/53 at 48 hrs and 0/53 at 168 hrs. Three lots of the SSOP were also tested. Results were 0/18 at 48 hrs and 0/18 at 168 hrs. Intel Report 12/29/95.	X					**Accept**	To reduce risk of popcorning, the SSOP package should be baked prior to SMT or vapor flow assembly.
Temperature Cycling (PEMs):	Three lots were tested at -65C to 150C. Results were 0/37 for precondition; 0/37 at 200 cyc.; 0/37 at 500 cyc.; and 0/37 at 1K cyc. Intel Report 12/29/95.	X					**Accept**	
Radiation Effects (PEMs):								
Temperature Humidity (85/85L (PEMs):	Three lots of TSOP were tested at 85C ambient and 85% relative humidity. Results are 0/40 at precondition; 0/40 at 168 hrs; 0/40 at 500 hrs; and 0/40 at 1K hrs. Intel Report 12/29/95.	X					**Accept**	
Popcorning>215C-JEDEC Level classification (PEMs):	Moisture Absorption tested for JPL & reached 80% saturation within 24 hrs at 85/85. Baking recommended prior to surface mount assembly. e.g. 24hrs @ 125C.	X			**Moisture sensitive package-Shipped as Level 5 (24 hrs max out of drypack)**			
Surface Mount Part >44 pins (PEMs):	Popcorning not tested.		X					
Glass Transistion Temperature (PEMs):	Tg Tested at 165C	X					**Accept**	
Alpha Particle Emission (PEMs):			X					
Epoxy Molding Compound (EMC) Grade:	Test by FTIR as glass filled epoxy.	X					**Accept**	
Stress Buffers Coatings (PEMS):			X					

Beware: Currently there is no one standard for PEMs (commercial / industrial grade) microcircuit quality.

11. Radiation Performance/Data:

	JPL Data	Information Received	For JPL Use Only (Quality/Risk Evaluation) Unknown	Low	High	Medium	Accept	For JPL Use Only Risk analysis:
Low dose rates effects (Bipolar & Bi-CMOS):	N/A	X						Part is usable for TID <10Krads.
High Dose Rates:	Tested at 25rads(Si) per sec.	X			**High**			
****Single Event Dielectric Rupture(SEDR):**			X					
Rad Results:								
****LET Latchup:**	One device was tested (28FO16SV-70 S/N 2225) with 1960 Mev Xe (LET=44 MeV/(mg/cm2) and 600 Mev Ar (LET=7.4 MeV/(mg/cm2). One or two latchups were observed for Xe at 0 degrees angle with 5x10-6 Xe ions/cm2. The latchup threshold LET is ~ 44 MeV/(mg/cm2)	X	**Latchup currents ranged between 52 mA and 123 ma, compared to nominal currents of 6 mA.**			**Medium**		Waiver required for SEU.
RH Process Improvements:	N/A	X						
SEU:	Test in progress							

****These are critical issues for Deep Submicron technologies.**

12. Known Good Die:

	Vendor's Data	Information Received	For JPL Use Only (Quality/Risk Evaluation) Unknown	Low	High	Waived	Accept
See KGD Manufacturers:		N/A					
See KGD Criteria:		N/A					
See KGD Products:		N/A					

For JPL Use Only Risk analysis:

N/A

13. JPL Chip Overview Results:
(See Report "FA6745.pdf")

	JPL's Data	Information Completed	For JPL Use Only (Quality/Risk Evaluation) Unknown	Low	High	Waived	Accept
External Visual Anomalies:	Pass	X					Accept
Die Name:						Waived	
Die Revision:						Waived	
Internal Visual Foreign Material:	Pass	X					Accept

For JPL Use Only Risk analysis:

No risk is evident based on die examination.

14. JPL DPA (Package) Results:
(See Report "FA6745.pdf")

	JPL's Data	Information Completed	For JPL Use Only (Quality/Risk Evaluation) Unknown	Low	High	Waived	Accept
Wirebond Pull:	13.0 to 17.8 grams force	X					Accept
Die Shear:	Test was not performed		X			Waived	
Bondpad:	Au Ball placement passes at all pads	X					Accept
X-Ray:	Pass	X					Accept
Dye Penetrant:	Pass	X					Accept
Package Weight:	0.95 grams average	X					Accept
Glass Tansistion Temperature:	165 C	X					Accept
Volatile Organic Compounds (outgassing):	TML=0.19% avg (spec=1.0%); CVCM=0.06% avg (spec=0.1%)	X					Accept
Scanning Acoustic Microscopy:	Pass	X					Accept

For JPL Use Only Risk analysis:

No risk is evident with the 56 lead SSPO package. All indicators show the package process and assembly to be in control.

15. JPL DPA (Die Cross Section) Results:
(See Report "FA6745.pdf")

	JPL's Data	Information Completed	For JPL Use Only (Quality/Risk Evaluation) Unknown	Low	High	Waived	Accept
SEM Examination of Metalization:	Excellent step coverage	X					Accept
SEM Examination of Oxide:	Excellent	X					Accept
SEM Examination of Via and Contacts:	Excellent	X					Accept
SEM Examination of Passivation:	Excellent	X					Accept
SEM Examination of Polysilicon:	Metal layer over poly 2 select lines shows some evidence of thinning.	X	The reliability impact is not understood			Waived	

For JPL Use Only Risk analysis:

No risk is evident based on SEM examination of die topography and cross sections. Process is in good control.

7a. JPL Test/Burn-In Results:

(See Test Data Reports)	*JPL's Data*	Information Completed	*For JPL Use Only (Quality/Risk Evaluation)* Unknown	Low	High	Waived	Accept	For Use Only Risk analysis:
25C Testing:	33/33 passed	X					**Accept**	Risk of using this commercial part beyond its recommended operating temperature range will cause failures. Part can be pattern sensitive during screening.
70C (max rated temp.) Testing:	5/5 passed	X					**Accept**	
100C Testing:	5/5 passed	X					**Accept**	
125C (extended temp.) Testing:	2/5 failed funnctional checkerboard and inverse pattern @ 110C; 3 passed @ 125C.	X			**Screening is required to insure operation beyond 70C.**			
-55C (extended temp.) Testing:	5/5 failed diagonal and inverse pattern test and TGLQV3V.	X			**Screening is required to insure operation below 0C.**			
0C (low rated temp.) Testing:	5/5 passed						**Accept**	
125C DYNAMIC BURN-IN FOR 336 HRS:	1/7 failed Vcc Deep Power Down (ICCD) @ Vdd=3.3V	X			**Burn is required**			500 hr min. dynamic burn-in is recommended for high reliability applications.
Static Burn-in:	N/A							

End of Data

6.0 SUMMARY OF RESULTS

METHODOLOGY

The objective of this work was to develop a methodology and decision criteria to evaluate and select COTS parts that:

- Minimized the cost to the users by using available data
- Established COTS criteria for Space Applications
- Minimized risk to users of COTS parts
- Allowed trade-off assessments with radiation hardened parts
- Provided quality service and value to the customer
- Stimulated gaining new knowledge and experience with COTS
- Provided for dissemination of the knowledge and experience gained

Much of what has been accomplished to develop a methodology has been by reviewing what others were implementing to make COTS acceptable in the consumer market and in the aerospace world. Many approaches and methodologies are being used, some being very complex and others are simplistic. The methodology used by JPL focused on more objective risk assessment and analysis. Criteria were developed to make decisions, retain flexibility, and capitalize on available information and data. What has been learned is that it is difficult to obtain information from the vendors directly. In many cases vendors often want you to go to their representatives for information. When they in turn cannot provide the information requested they send you back to the vendor. With the new automatic phone answering systems where vendors are giving options by punching in numbers, one is not able to talk to a person directly. Once you get around this system there is usually some success in getting some of the data and information you request. Using the vendors Web page also is of some help but if one is looking for reliability and quality data the Web pages fall short especially on new products. Therefore trying to use all available information to make risk assessments and keep the cost down can take more time that a project schedule has planned for. However some good information can be gotten without expensive tests. One way to expedite the process is to limit the criteria you are going to evaluate and concentrate on the sensitive or critical items to mission success.

The COTS criteria used in this work was not constrained. They were chosen to be comprehensive in order to see how much information one could obtain from the vendor in a reasonable time and how much value it had in making risk assessments and analysis. In the example of the Flash Memory only three of the twelve criteria defined as vendor inputs failed to produce any real information. However it is not surprising since much of this information is considered propriety by some vendors. In other cases vendors will share this information provided you are a large volume customer of theirs. For aerospace customers this will always be a challenge. The five criteria used for JPL inputs were selected to fill the gaps when vendor information or data was not readily available. Because of this there was more cost added to the process but if it is necessary to make a good risk assessment then it must be done. The parts engineer must decide what makes good sense in light of

mission requirements and making the right decisions to minimize risk. For the Flash Memory example the evaluation and risk assessment is still on going.

In order to minimize or eliminate risk concerns for COTS parts it is important to identify which indicators within established criteria must be evaluated on recent factual data. For the flash memory example moisture absorption and desorption data for the SSOP plastic package were tagged as very important data. Another important indicator for plastic packages is outgassing. For infant mortality projections, dynamic burn-in data was tagged as very important. These concerns led to developing a plan to acquire the data in real time. The data and results obtained for these indicators is included in the flash memory risk assessment template. The outgassing and burn-in work has been completed and reviewed. The outgassing data showed no evidence for concern but the dynamic burn-in data did. One burn-in failure found by JPL testing was in agreement with data reported by the vendor in 1995. Therefore infant mortality was labeled as a primary risk driver. The early work done by JPL on plastic moisture absorption has led to further work which now includes moisture desorption. This new work is evaluating different plastic package configurations. It is not complete and some preliminary observations found are not understood. Therefore risk assessment for plastic moisture concerns cannot be made at this time. Radiation performance data has been difficult to complete because of conflicting and strange results obtained for the flash memory tested. When evaluating COTS parts this is often the case. Radiation testing is continuing in a consistent and precise manner to resolve all anomalies found. Risk assessment is still under evaluation for all the radiation indicators except one. Total ionizing dose (TID) test results in a plastic package indicate the flash memory part is limited to $\leq$ 10Krads.

One general conclusion is evident. The time it takes to properly evaluate a COTS part is too often underestimated and forcing a rush to judgment on its acceptability will likely lead to problems later on.

Performing trade-off studies of COTS parts with radiation hardened high reliability parts was one of the objectives for the methodology development. Trade-off studies and analysis gives the parts engineer options to consider in reliability, performance, and cost factors. Selection of a part is then determined based on options that best meet requirements, risks allowed and cost constraints. For the COTS flash memory example a trade-off study is not possible since there are no vendors who manufacture a radiation hardened high reliability part. Therefore any trade-off studies would have to be done on similar non rad hard COTS parts. Some of this work is underway.

The methodology undertaken to evaluate the COTS flash memory was designed as a structured risk management approach. The process followed concurrent engineering methodology with risk drivers identified and whereby risk predictions could then be made based on real time data. The flash memory example demonstrated that this approach does provide value and quality to the customer. COTS parts must be considered high risk until proven or shown otherwise. Since little is known about their behavior in *deep space* applications, caution and discretion must be adhered to during a project part evaluation phase.

Using and applying COTS parts and technologies in Space Applications without risk requires having extensive knowledge and experience with a part. Gaining the knowledge and experience takes time, commitment, and perseverance. The cost of obtaining these may not always be justified and must be evaluated against the risk of failure. The methodology followed in the Flash Memory example attempted to contain the cost of evaluation. However when nothing is known and there is no previous experience to rely on it can be expected that cost will exceed initial projections. If the information and data obtained have shown that they have led to good risk assessment and decision making that will prevent a major mistake in choosing a COTS part , then cost will be supported by project planners. The Flash Memory example has definitely stimulated some new directions to pursue not only for Flash Memories but for other COTS part types. The real test for the knowledge gained and how it was evaluated is when the part is flown in a Space Application and performs flawlessly over the life of the mission. At this time experience in real time has been gained. There will be some future failures attributed to lack of knowledge and maybe lack of testing. Making a decision between having more knowledge and working with limited knowledge is what the parts engineer must evaluate in a high risk environment.

The information, knowledge, and experience gained with COTS parts is being shared through JPL's Parts Information Program (PIP), Conference Papers, The NASA EEE Parts Program, COTS data base, JPL Technical Infrastructure Program, NASA Flight Readiness Technology Assessment RTOP, and direct communication with design engineers working on various NASA projects.

APPENDIX A

Risk Management
"Risk as a Resource"

Presented to
Jet Propulsion Laboratory
February 26, 1997

Dr. Michael A. Greenfield
Deputy Associate Administrator
Office of Safety and Mission Assurance

Topics

- → Risk Management - New Requirements in NHB 7120.5A
- → Our New Environment - "Better, Faster, Cheaper"
- → A New Way: Risk as a Resource (Knowledge-Based, Not Rule-Based)
- → The Role of Safety and Mission Assurance in Understanding Risk

Risk Management is an Integral Part of Project Management

- → The Consequence of Risk Is Very Broad: Performance Reduction, Cost Increase and Schedule Delays, Mission Failure, Property Damage, Loss of Life or Injury
- → The Objective of Risk Management Is to Keep All Risks Within the Defined and Accepted Boundaries
- → Risk Management Is Not New At NASA, But Must Be Changed to Be More a Part of an Upfront Concurrent Engineering Process

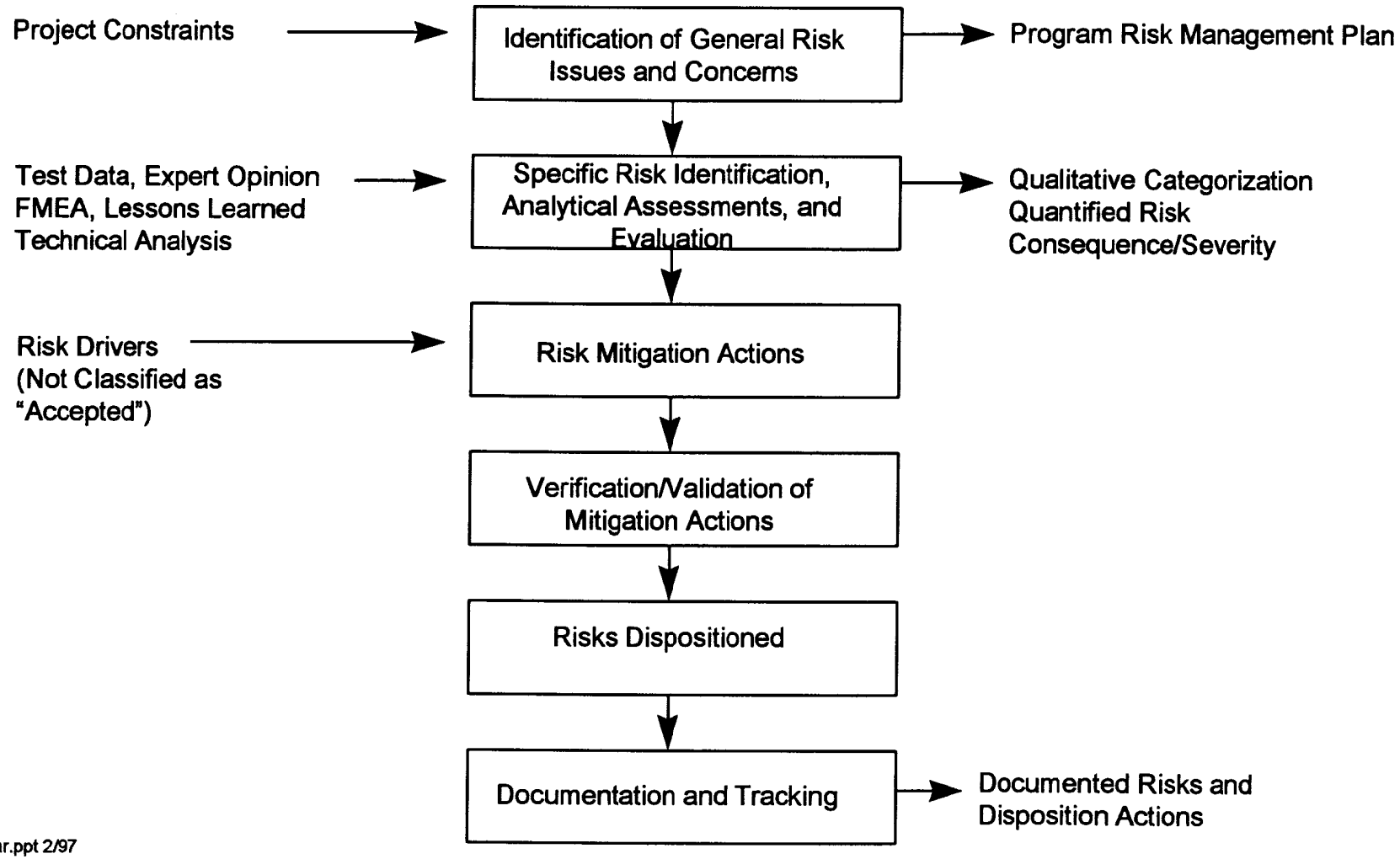
Definition of Risk and Risk Drivers (NHB 7120.5A)

- → Risk to Mission Success Is the Probability (Qualitative or Quantitative) That a Program/Project Will Experience Undesired Consequences Such As:
  - → Failure to Achieve Technological or Scientific Objective
  - → Cost Overrun
  - → Schedule Slippage
  - → Safety Mishaps
- → Primary Risk Drivers are Those Undesirable Events Whose Probability Is More Likely Than "Remote" and Whose Consequences Could Pose a Significant Threat to Mission Success

Revised NASA Program/Project Management Handbook (NHB 7120.5A)

- → The New Handbook Is Divided Into Four Program Life Cycle Parts
  - → Formulation
  - → Approval
  - → Implementation
  - → Evaluation
- → It Stresses Risk Management As an Integral Part of Project Management
- → The Formulation Section Requires a Risk Management Plan to Be Developed by End of Phase B
- → The Implementation Section Defines a Risk Management/Risk Assessment Process
- → All Risk Drivers Must Be Dispositioned Before Flight

Risk Management Process



Analysis of Program/Project Constraints

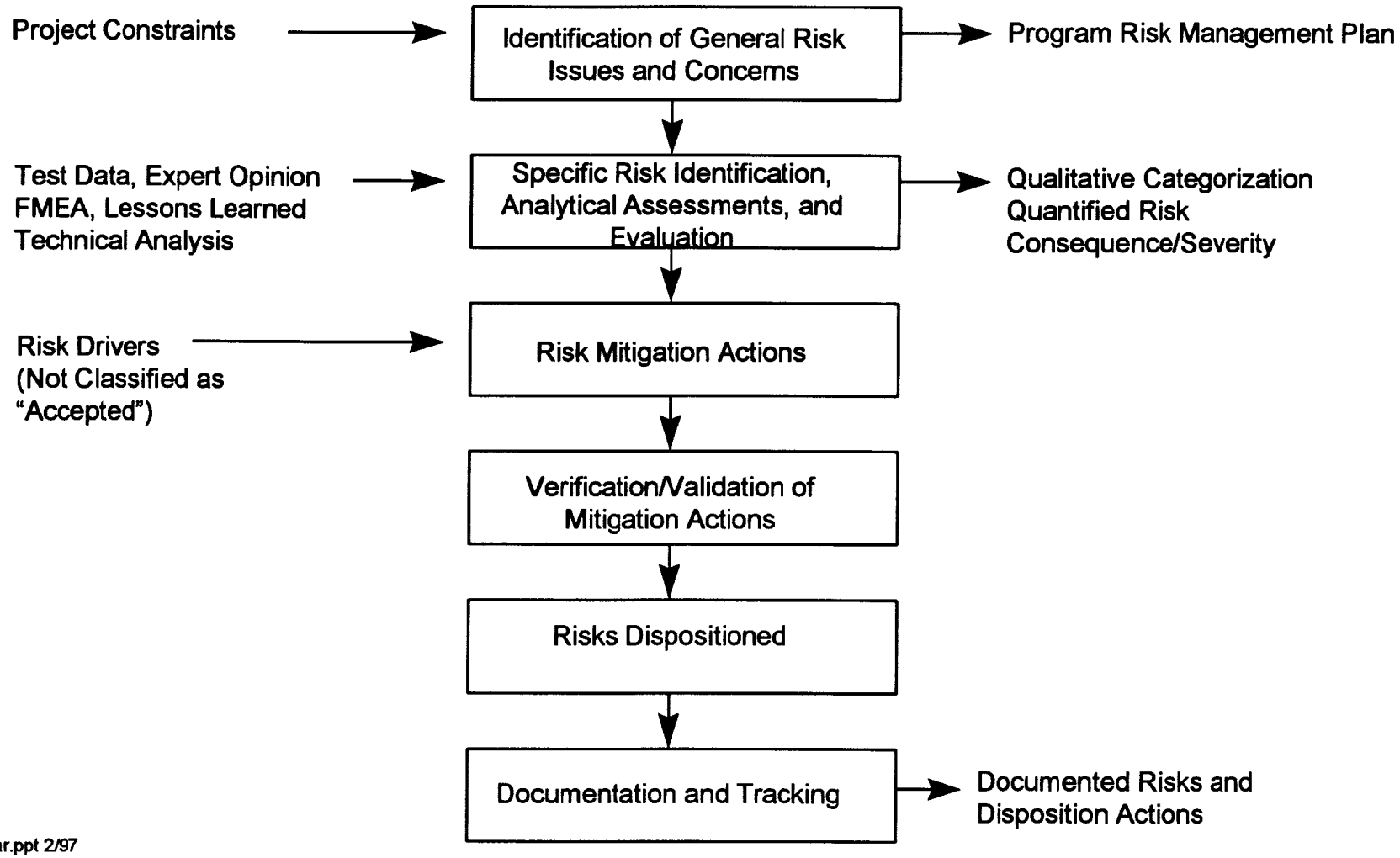
→ Examples of Program/Project Constraints Include:

- → Mission Success Criteria (Primary and Secondary)
- → Development Schedule
- → Budget Limits
- → Launch Window and Launch Vehicle Availability
- → International Partner Participation
- → Human Space Flight Safety Issues
- → "Fail Ops/Fail Safe" Requirements
- → Technology Readiness
- → Oversight Requirements
- → Amount and Type of Testing

Risk Management Requirements Risk Plan

- → A Completed Risk Plan Is Required at the End of Phase B. It Must Include:
  - → Risk Management Responsibilities, Resources, Schedules, and Milestones
  - → Methodologies, Processes, and Tools to Be Used for Risk Identification, Risk Analysis, Assessment, and Mitigation
  - → Criteria for Categorizing or Ranking Risks According to Probability and Consequences
  - → Role of Decision-Making, Formal Reviews, and Status Reporting With Respect to Risk Management
  - → Documentation Requirements for Risk Management Products and Actions

Risk Management Process



Risk Management Requirements: Primary Risk Driver Analysis

- For Each Primary Risk Driver, the Program Shall Document:
  - Description of the Risk Driver Including Primary Causes and Contributors to the Risk
  - Estimate of the Probability (Qualitative or Quantitative) of Occurrence Together With the Uncertainty of the Estimate
  - Primary Consequences Should the Undesired Event Occur
  - Significant Cost Impacts Given Its Occurrence
  - Significant Schedule Impacts Given Its Occurrence
  - Potential Mitigation Measures
  - Implemented Mitigation Measures, If Any

Risk Management Requirement: Risk Control

- All Primary Risk Drivers Must Be Adequately Resolved. A Risk Driver Will Be Considered "Controlled" or "Retired" When Any One of the Following Conditions Are Satisfied:
  - Risk Mitigation Options That Reduce the Probability of Occurrence to "Remote" Have Been Planned and Will Be Implemented
  - All Reasonable Mitigation Options (Within Cost, Schedule, and Technical Constraints) Have Been Instituted, and the Risk Driver Has Been Judged to Be "Accepted" by a PMC
  - Reserve Funds Are Available to Recover From Cost, Schedule, and Technical Impact Should the Risk Actually Occur

Risk Management in Today's "Better, Faster, Cheaper" Environment

The Past and the Future

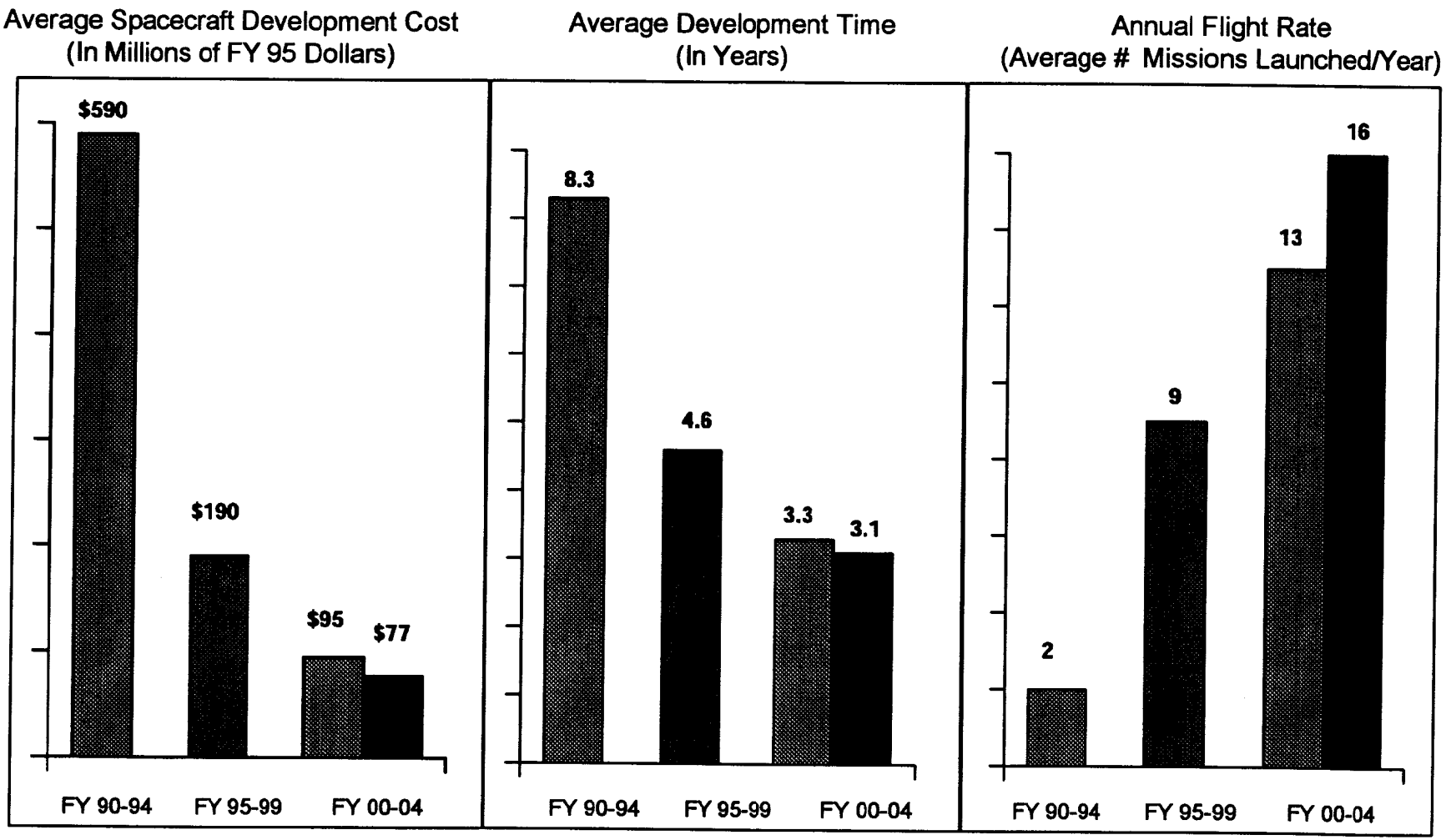
- → Past
  - → Large NASA Budget
    - → Few and Large S/C
    - → Big Budgets for S/C
    - → Risk Adverse
    - → Extensive Tests/Analysis

  } Some Large Successes - Few Failures

- → Today
  - → Shrinking NASA Budget
    - → Many Small S/C
    - → Small Budgets for S/C
    - → Risk Managed
    - → Value Based Tests/Analysis

  } Many Small Successes - Some Failures

Total NASA Earth and Space Science Better, Faster, Cheaper*



magrar.ppt 2/97
2/25/97, 11:10 (14)

* From NASA FY 1998 Budget Request Briefing (Feb. 6, 1997)

Success - What is It?

→ Monumental Success - or - Monumental Failure

Mission - One Large Expensive S/C (e.g., 1 S/C for 1 Billion with R(t) = 0.99)

<u>Expectation = 1 Success</u>

Or

→ Many Successes - And - Some Failure

Mission - Array of S/C to Accomplish the Mission (e.g., 10 S/C for 1 Billion with R(t) = 0.8)

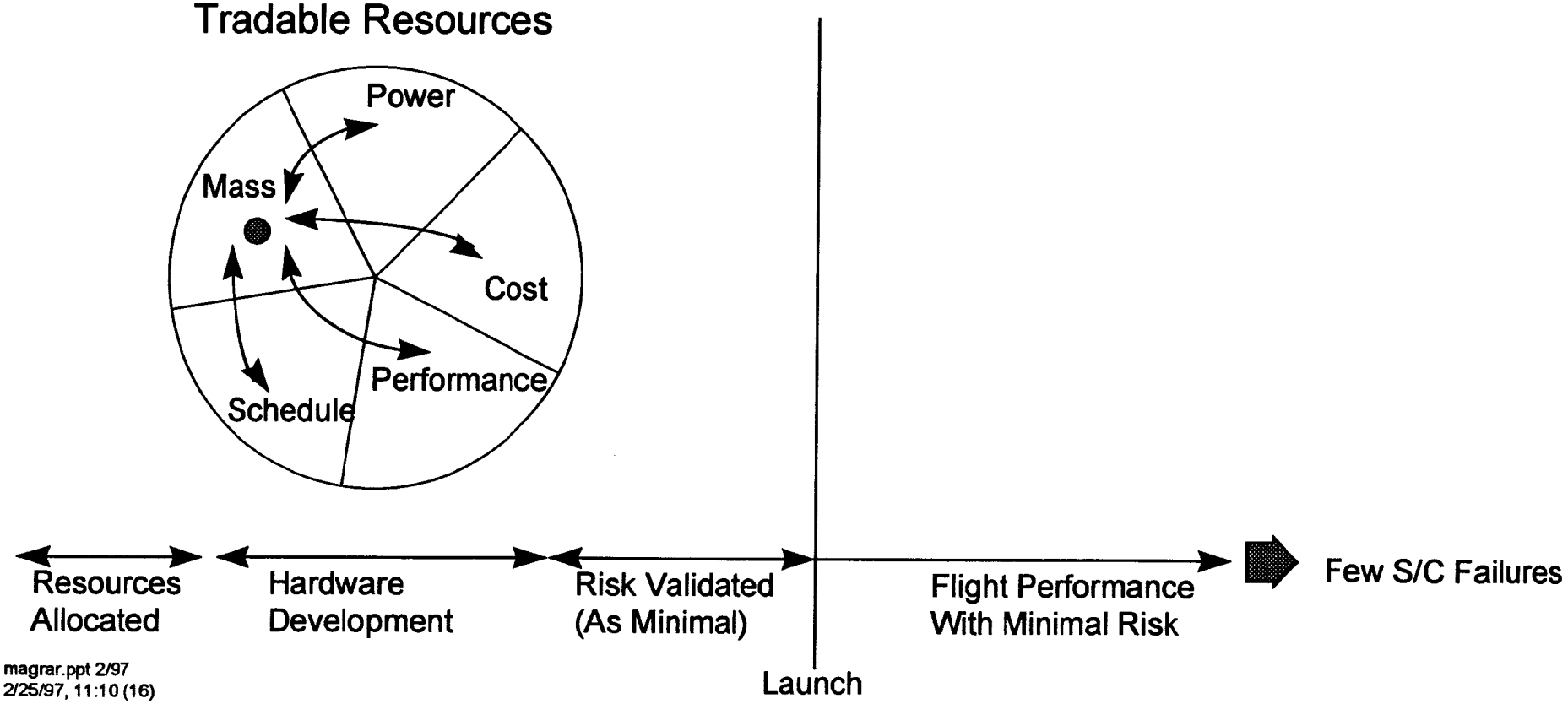
<u>Expectation = 8 Successes</u>

Key - Manage Risk to Avoid Systematic Common Mode Failures

Risk as a Consequence

Historically → Risk to Be Minimized (Avoided)
→ Residual Risk Is A Consequence of Deficiency in Tradable Resources

Tradable Resources



Characterization, Mission Success and SRM&QA Cost Guidelines for Class A-D Payloads

Classification	Class A	Class B	Class C	Class D
Characterization	High Priority, Minimum Risk	High Priority, Medium Risk	Medium Priority, Medium/High Risk	High Risk, Minimum Cost
Typical Factors Used to Determine Payload Classifications:	High National Prestige; Long Hardware Life Required; High Complexity; Highest Cost; Long Program Duration; Critical Launch Constraints; Retrieval/Reflight or in-Flight Maintenance to Recover From Problems Is Not Feasible.	High National Prestige; Medium Hardware Life Required; High to Medium Complexity; High Cost; Medium Program Duration; Some Launch Constraints; Retrieval/Reflight or in-Flight Maintenance to Recover From Problems Is Difficult or Not Feasible.	Moderate National Prestige; Short Hardware Life Required; Medium to Low Complexity; Medium Cost; Short Program Duration; Few Launch Constraints; Retrieval/Reflight or in-Flight Maintenance to Recover From Problems May Be Feasible.	Little National Prestige; Short Hardware Life Required; Low Complexity; Low Cost; Short Program Duration; Non-Critical Launch Time/Orbit; Reflyable or Economically Replaceable; In-Flight Maintenance May Be Feasible.
Achievement of Mission Success Criteria:	All Affordable Programmatic and Other Measures Are Taken to Achieve Minimum Risk. The Highest Practical Product Assurance Standards Are Utilized.	Compromises Are Used to Permit Somewhat Reduced Costs While Maintaining a Low Risk to the Overall Mission Success and a Medium Risk of Achieving Only Partial Success. Stringent Product Assurance Standards Are Utilized.	Moderate Risks of Not Achieving Mission Success Are Accepted to Permit Significant Cost Savings. Reduced Product Assurance Requirements Are Allowed.	Significant Risk of Not Achieving Mission Success Is Accepted to Permit Minimum Costs. Minimal Product Assurance Requirements Are Allowed.
Estimated Relative SRM&QA Cost Factors:	1.0	0.7 X Class A	0.4 X Class A	0.1 X Class A

Notes: 1. There Are Wide Variations in the Methods for Specifying and Accounting for "SRM&QA Costs". For Class A Programs, These Costs Are Typically in the Range of 10-15% of the Total Program Cost. The Relative SRM&QA Cost Factors Specified Here Are Intended to Require Substantive Differences in the SRM&QA Programs (and the Associated Costs) for the Various Program Classifications in Order to Establish a Meaningful Ladder of Cost/Risk Levels.

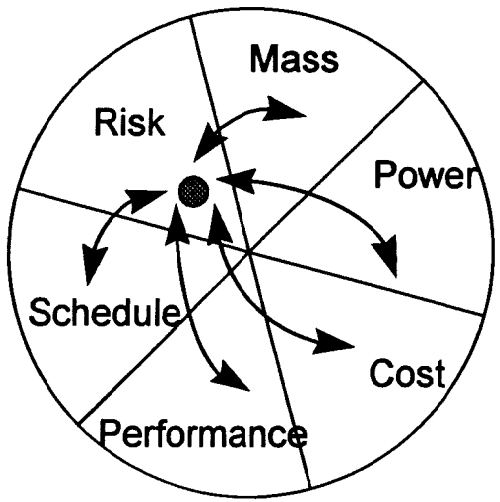
RuleBase

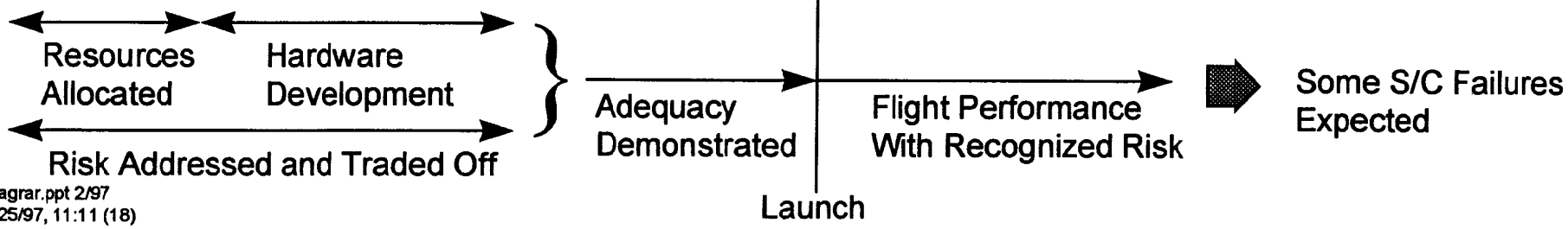
Attachment A - NMI 8010.1A

Risk as a Resource

A New Paradigm → Risk to Be Identified, Planned, and Accepted
→ Risk Understood and Traded as a Resource

Tradable Resources

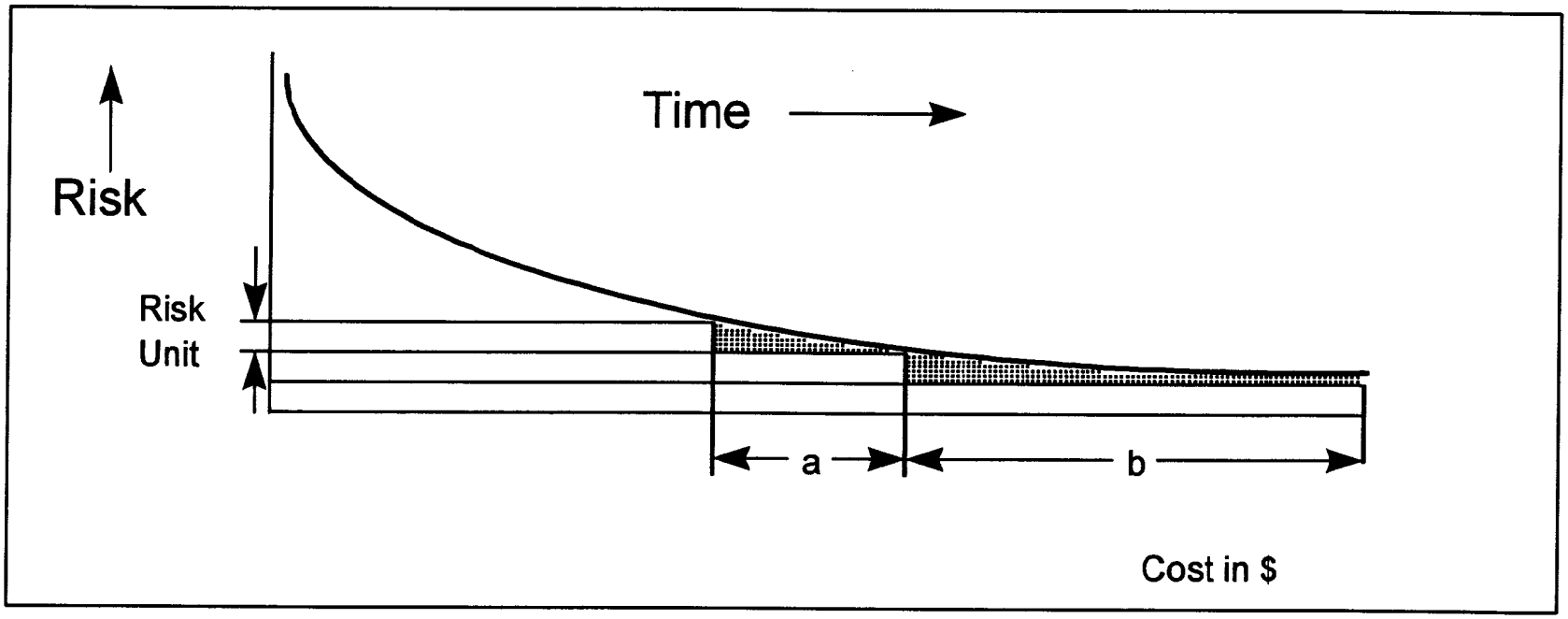




Reducing the Cost of Risk

<u>Marginal Cost of Risk</u>

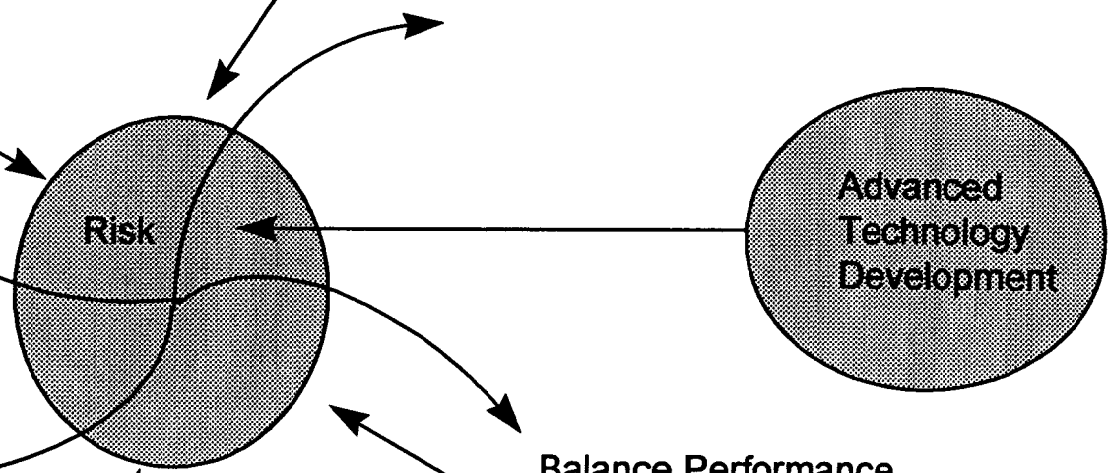
→ When the Cost Per Unit of Risk Reduction Increases Significantly -- STOP



Risk as a Resource
Tradeoffs & Advanced Technology

Reduce Cost
- Shorten Schedule
- Reduce Complexity
- Reduce Testing
- Reduce Analysis
- Buy Adequate, Not Optimum
- Reduce Ops. Complexity

Shorten Schedule
- Limit Development
- Shorten Testing
- Reduce Evaluation
- Fly Available Proven Hardware

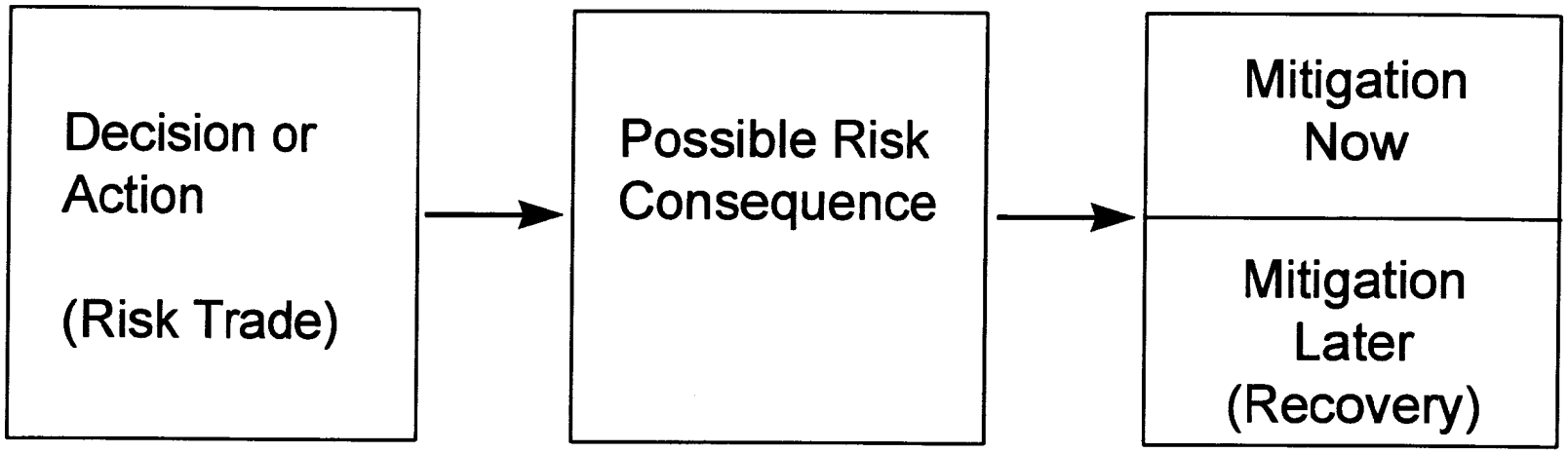


Lower Power Demand
- Low Pwr. Elect.
- Widen Temp. Control Range
- Power Share

Reduce Mass
- Miniaturize Electronics
- Reduce Volume
- Increase Density
- Reduce Cabling
- Stack Components
- Reduce I^2R Heating

Balance Performance
- Do What is Needed, Not Everything Possible
- Design Mission to Match Performance Available

Risk As A Resource Process



A Strategy to Recover From the Occurrence of a Risk Driver Must Be Determined Upfront and Considered Throughout the Risk Trade Process

Risk as a Resource Tradeoff Examples

- → Technology Utilization
- → Redundancy or Single String
- → Class of EEE Parts
- → Dynamics Validation
- → EMI Validation

Risk as a Resource
Technology Utilization Trades

Possible Risk Consequence

Function	Risk Trade Space	System Development	Resource	Flight	Attributes
Technology Utilization	Advanced Technology*	• Technology Readiness Uncertainty • Greater (Imbedded) Functional Complexity • Interface Uncertainty	• Development Costs • Possible Redesigns Late in Lifecycle • Backup Design Cost • Technology Readiness Schedule • Qualification Complexity Cost	• Unknown Failures • Untried Recovery	• Quantum Resource/Performance Improvement • Less Hardware and Less Integration Complexity • Greater Reliability Potential
	Or				
	Existing Technology**	• Constraints on Other Subsystems • Resource Compromise Induced Failures • Heritage Traps	• Mass • Power • Test Facility Cost and Schedule Logistics	• Work Around Complexity	• Qualified and Flight Proven; Heritage • Availability • Confidence in Established Reliability

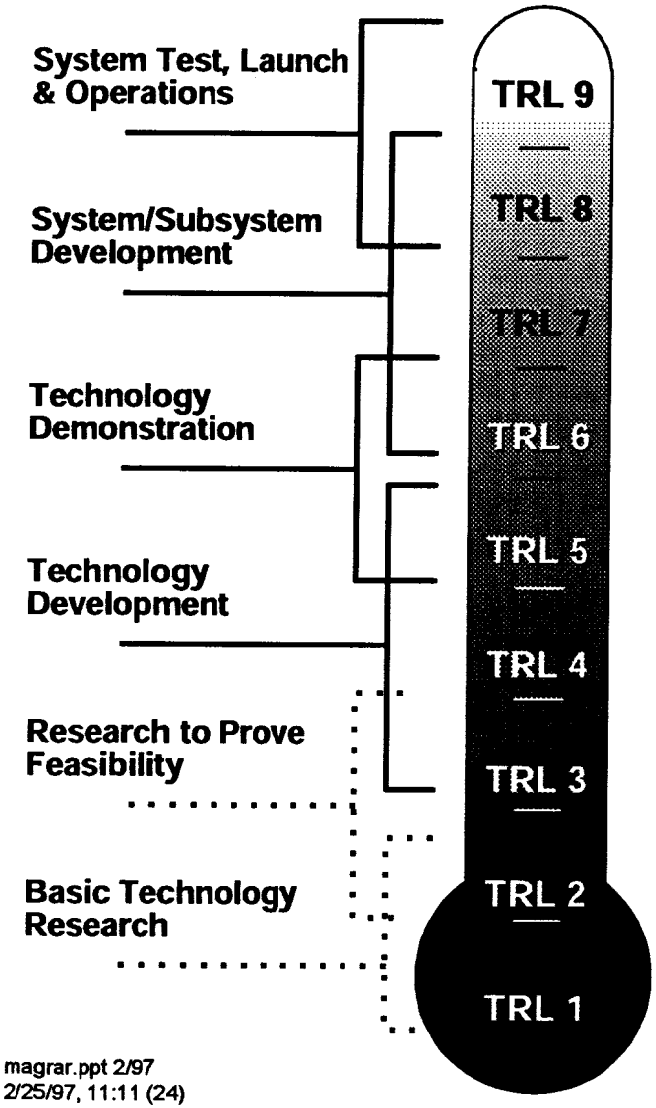
* Greater Success Risk for Significant Resource Advantage

** Greater Resource Demand for More Confidence in Reliability

SMA Role

- Technology Readiness Assessment
- Reliability Estimates
- Co-participation in Qualification Plans
- Risk Assessments and Risk Management Support

Technology Readiness Levels (TRLs)



Actual System "Flight Proven" Through Successful Mission Operations

Actual System Completed and "Flight Qualified" Through Test and Demonstration (Ground or Flight)

System Prototype Demonstration in a Space Environment

System/Subsystem Model or Prototype Demonstration in a Relevant Environment (Ground or Space)

Component and/or Breadboard Validation in Relevant Environment

Component and/or Breadboard Validation in Laboratory Environment

Analytical and Experimental Critical Function and/or Characteristic Proof-of-Concept

Technology Concept and/or Application Formulated

Basic Principles Observed and Reported

Risk as a Resource
Redundancy or Single String

Possible Risk Consequence

Function	Risk Trade Space	System Development	Resource	Flight	Advantage
System Design	Redundancy (Block & Functional)	• Complexity Due to Cross Strapping	• Cost • Schedule • Mass • Pwr		• Lowest Flight Performance Risk • Supports Long Life Missions • Compatible With Continuous Ground Test During Sys. Dev.
Or	Selected Redundancy in Critical Subsystems	• Possible Consequences Associated with Both	• Cost • Schedule • Mass • Pwr	• Possible Consequences Associated with Both	• Combination = f(Degree)
Or	Single String	• One Failure May Be Fatal • Poor Quality May Be Fatal • Hardware Glitch Interrupts Ground Testing		• Higher Risk If Complicated Operations	• Most Cost Effective • Fits With Economical Multi-Launch Missions • Fast Development

SMA Role

- Probabilistic Trade Analysis in the Trade Space
- Redundancy Switching Analysis
- Failure Mode Analysis
- Flight Performance Histories
- Lifetime Projections

Risk as a Resource
Class of EEE Parts

Possible Risk Consequence

Function	Risk Trade Space	System Development	Resource	Flight	Advantage
EEE Parts Quality	Class "S"/ Grade 1	• Availability Poor • Long Lead Time • Mass and Volume Higher	• Cost • Schedule • Procurement		• Lowest Risk if Used • Fits Long Life • More Resistant to SEE
Or					
	Class B	• No Heritage • Lot Variations Means Variable Radiation Tolerance	Many of same issues as Class "S" But with Less Flight Risk than "COTS"		• Moderate Cost • Higher Performance Expectation than "COTS
Or					
	Commercial Off-the-Shelf (COTS)	• Quality Control at Parts Vendors • Post Procurement Screening & Burn in May Find Inadequacies	• Schedule (Test Operations)	• Performance • Lifetime • Incidence of "Maverick" is Higher	• Readily Available • Cheap • Fits Short Duration Missions with Multiple Launches

SMA Role

- Procurement Specifications
- Vendor Qualification
- Upgrading Process Definition
- Parts Testing Program
- Residual Parts Risk Assessment

Risk as a Resource
Dynamics Validation

Possible Risk Consequence

Function	Risk Trade Space	System Development	Resource	Flight	Advantage
Dynamics Validation	Analysis & Test	• Conflict Resolution Between Analysis & Test Results	• Cost • Schedule • Mass		• Most Reliable Design
	Or Analysis Only	• Adequacy Not Demonstrated	• Mass	• Considerable Performance Risk	• No Prelaunch Hardware Degradation
	Or Test Only	• Later Problem Discovery • Rework	• Mass • Cost/Schedule if Design Poor		• Simple (Design to Pass Test) • Cheap & Fast

SMA Role

- Test Requirement Definition
- Analysis Verification
- Test Oversight
- Residual Risk Assessment

Risk as a Resource
EMI Validation

Function	Risk Trade Space	Possible Risk Consequence: System Development	Possible Risk Consequence: Resource	Possible Risk Consequence: Flight	Advantage
EMI Validation Testing	Unit & Systems Testing		• Cost • Schedule		• Early and Thorough Problem Resolution • Lowest Flight Risk
Or	System Testing Only	• Rework Late in Schedule • Constrained Solutions - Mostly Shielding	• Mass		• Lowest Cost • Most Efficient Schedule

SMA Role

- Requirement Establishment to Consider Risk Consequences
- Mitigation Strategy Development
- Problem/Corrective Action Assessment
- Definition of Residual Risk

Summary

- → We Work in a High Risk Environment
- → A Structured Risk Management Approach Is Critical to A Successful Project--This Is Nothing New
- → Risk Policy Must Be An Integral Part of the Program As Part of a Concurrent Engineering Process; Risk and Risk Drivers Must Be Monitored Throughout the Program
- → Risk May Also Be Managed As A Resource; the New Way of Managing Better, Faster, Cheaper Programs Encompasses Up-Front, Knowledge-Based Risk Trades
- → Risk Management Is a Smart Thing to Do; It Is Also Required (NHB 7120.5A)

APPENDIX B

Risk Analysis

Table of Contents

1. Introduction
2. Risk Identification
   1. Project Risks
   2. Technical Risks
   3. Business Risks
3. Sample Risk Item Checklist
4. Risk Projection (Estimation)
5. Risk Assessment
   1. Risk Referent Level
   2. Risk Assessment Checklist
   3. Risk Evaluation Outcomes

Links to CMU's Software Engineering Institute

- **What is Risk Management?**
- **Software Risk Management**
- **Risk Program Slide Overview Index**
- **Continuous Risk Management Definition**
- **Risk Cost Model**
- **Software Development Risk: Opportunity, Not Problem**
- **Software Risk Management, SW-CMM v2.0 Draft A**

Return to Table of Contents for the Course Notes

Introduction

1. Risk is concerned with the **future**
   - what might cause a software project to go awry
2. Risk is concerned with **change**

2. Risk is concerned with **change**
   - changes in requirements, development technologies, target computerss
3. Risk is concerned with **choices**
   - what methods and tools to use, how many people to involve

For an event, action or object to be considered a risk there must be:

1. A loss associated with it.
2. Uncertainty or chance involved.
3. Some choice involved.

Risk analysis is composed of **four** distinct activities:

1. risk identification
2. risk projection
3. risk assessment
4. risk management

Risk Identification

Risks can be categorized at a macroscopic level as:

1. Project risks
2. Technical risks
3. Business risks

Project Risks

- Potential budgetary, schedule, personnel, resources, customer and requirements problems and impact.
- Project complexity, size and structure are determining factors.

Technical Risks

- Potential design, implementation, interfacing, verification and maintenance problems.
- Specification ambiguity, technical uncertainty, technical obsolescence and ``leading edge'' technology.

obsolescence and ``leading edge'' technology.

Business Risks

- The most insidious!

1. Market Risk
   - building a product that no one really wants.
2. Product Risk 1
   - building a product that no longer fits into the overall product strategy for the company.
3. Product Risk 2
   - building a product that the sales force doesn't understand how to sell.
4. Management Risk
   - losing the support of senior management due to a change in focus or people.
5. Budget Risk
   - losing budgetary or personnel committment.

Sample Risk Item Checklist

- Use of a set of questions to help the project planner to understand the project or technical risks.
- Risk item checklist for staffing risk:
  1. Are the best people available?
  2. Are enough (too many) people available?
  3. Do the people have the right combination of skills?
  4. Have staff members received the necessary training?
  5. Is the staff committed for the entire project duration?
  6. Will some staff members only be part time?
  7. Will staff turnover be low enough for continuity?

Risk Projection (Estimation)

Attempts to rate each risk in two ways:

1. **Likelihood** that the risk is real.

2. **Consequences** of the problems associated with the risk, should it occur.

Four risk projection activities:

1. Establishing a scale that reflects the perceived likelihood of a risk.
   - boolean, qualitative, quantitative
2. Delineating the consequences of a risk.
3. Establishing the impact of the risk on the project and the product.
4. Noting the overall accuracy of the risk projection.

Risks are weighted by perceived impact and then prioritized. Three factors affect impact:

1. The **nature** of the risk indicates the problems that are likely if it occurs.
2. The **scope** of a risk combines its severity with its overall distribution.
3. The **timing** of a risk determines when and for how long the impact will be felt.

The importance of risk impact and probability is linked to their effect on management concerns.

```
IF      risk_factor = high_impact        AND
        probability_of_occurence = low
THEN    management_concern = not significant

IF      risk_factor = high_impact        AND
        probability_of_occurence = moderate to high
THEN    management_concern = risk analysis activity

IF      risk_factor = low_impact         AND
        probability_of_occurence = high
THEN    management_concern = risk analysis activity
```

Risk Assessment

- Risks can be represented as a set of triples of the form: *[r,l,x]*

where
- *r* is risk
- *l* is the likelihood (probability) of the risk
- *x* is the impact of the risk.

- During risk assessment the following actions occur:
  1. An examination of the accuracy of the estimates made during risk projection.
  2. A prioritization of the risks that have been uncovered.
  3. A preliminary examination of the ways to control and/or avert likely risks.

Risk Referent Level

- At a certain level of risk, or a combination of risks, a project will have to be terminated.
- A **risk referent level** has a single point, called the **referent** or **break point**, at which time the decision to proceed or terminate are equally acceptable.
- Cost, schedule and performance represent three typical risk referent levels.

Risk Assessment Checklist

1. Define the risk referent levels for the project.
   - Referents are stated as a probability of failure or the probability of success level for each individual risk or the system as a whole.
   - A value should be agreed upon where it is decided that a project should not continue.
   - The system risk referent can be:
     1. an aggregate of individual risks, or
     2. one or more prioritized high impact risks
2. Attempt to develop a relationship between each *[r,l,x]* and each of the referent levels.
3. Predict the set of referent points that define a region of termination, bounded by a curve or areas of uncertainty.
4. Try to predict how compound combinations of risks will affect a referent level.

Risk Evaluation Outcomes

Comparing the evaluated risk against its risk referent has three possible outcomes:

1. Acceptable
   - the evaluated risk is less than the referent.
2. Impossible
   - the evaluated risk is much greater than the referent.
3. Infeasible
   - the evaluated risk is greater than, but almost equal to, the referent.

- If the **system** risk is **acceptable** then
  - proceed to evaluate individual risks
- If the **system** risk is **impossible** then
  - determine if the project should continue.
  - if the project continues
    - replan to avert the identified risks
    - repeat risk analysis.
- If the **system** risk is **infeasible** then
  - determine if the project should continue.
  - if the project continues
    - replan to avert the identified risks OR
    - continue with the plan but apply risk aversion strategies.
- After system-wide evaluation, the individual risks should be completed and evaluated in the same way as the system risk.