2009 ARS, North America, San Diego

Track 2, Session 11

Begins at 10:30 to 11:30 AM, Thursday, June 11, 2009

Current Time
5/22/2009

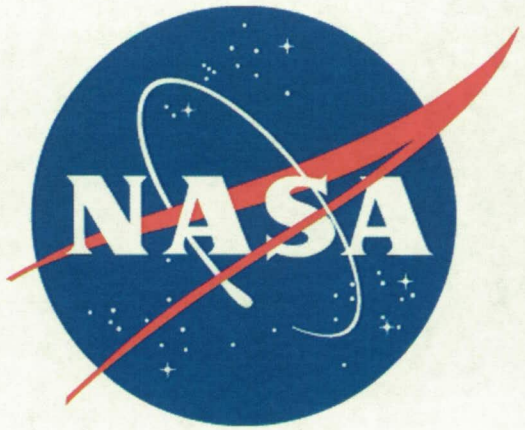
The Application of a Residual Risk Evaluation Technique Used for Expendable Launch Vehicles

John A. Latimer

Senior Systems Reliability Engineer

SAIC/NASA KSC

SAIC®
From Science to Solutions



Agenda

• Introduction	3 min
• RRET Overview	5 min
• RRET Implementation Process	15 min
• Example	20 min
• Summary	7 min
• Questions	10 min

- Attachments
  - Definitions
  - Acronyms

Introduction *(1 of 3)*

Author/Presenter: John A. Latimer

- Senior System Reliability Engineer
- Over 33 Years Experience in Systems Engineering and Risk Management
  - Concept Formulation
  - Development
  - Test
  - Production
- Employed at Science Applications International Corporation (SAIC) for Over 22 Years
- Currently Working the National Aeronautics and Space Administration (NASA) Expendable Launch Vehicle (ELV) Contract at Kennedy Space Center (KSC)

Introduction *(2 of 3)*

Presentation Material :

- Residual Risk Evaluation Technique (RRET)
  - RRET Was Developed by KSC's Safety and Mission Assurance (SMA) Launch Services Division to Provide System Reliability Input to the Decision Makers for ELV's Readiness Reviews and Other Major Life Cycle Milestones
    - RRET Determines the Impact of Residual Risks on the System Baseline Reliability Throughout the ELV's Life Cycle Mission
  - RRET Met the Approval of the Office of Safety and Mission Assurance (OSMA) at NASA Headquarters

Introduction *(3 of 3)*

ELV's Risk Management:

- A Continuous Risk Management Plan (RMP) Is Being Implemented for Each ELV Mission
  - LSP-PLIN-353-01," Launch Services Program Risk Management Plan"
    - o The RMP Is Based on NASA Requirements and Guidelines
      - – NPR 8000.4, "Risk Management Procedural Requirements"
      - – NPD 8700.1C, "NASA Policy For Safety And Mission Success"
    - o The RMP Includes a Controlled, Logical, Management Procedure for Identifying, Assessing, and Reporting Potential Technical Risks
    - o SMA Performs Reliability Analysis as One of Many Independent Mission Assurance Tasks to Maximize Mission Success for Each ELV Mission

RRET Overview

RRET:

- A Simplistic, Cost Effective Residual Risk Evaluation Technique
  - It Provides Quantifiable Insight Into the Severity of the Residual Risks Impact on a System Baseline Reliability
    - The System Reliability Impact Indicator Provides a Quantitative Measure of the Reduction in the System Baseline Reliability Due to the Identified Residual Risks
- Proven Methodology
  - Risk Management
    - NASA: Risk Management Procedural Requirements
  - Fault Tree Analysis (Probability of Failure - P_F)
    - NASA: Fault Tree Handbook with Aerospace Application
  - Reliability Prediction (Probability Of Success – R)
    - NASA: System Engineering Toolbox for Design-Oriented Engineers

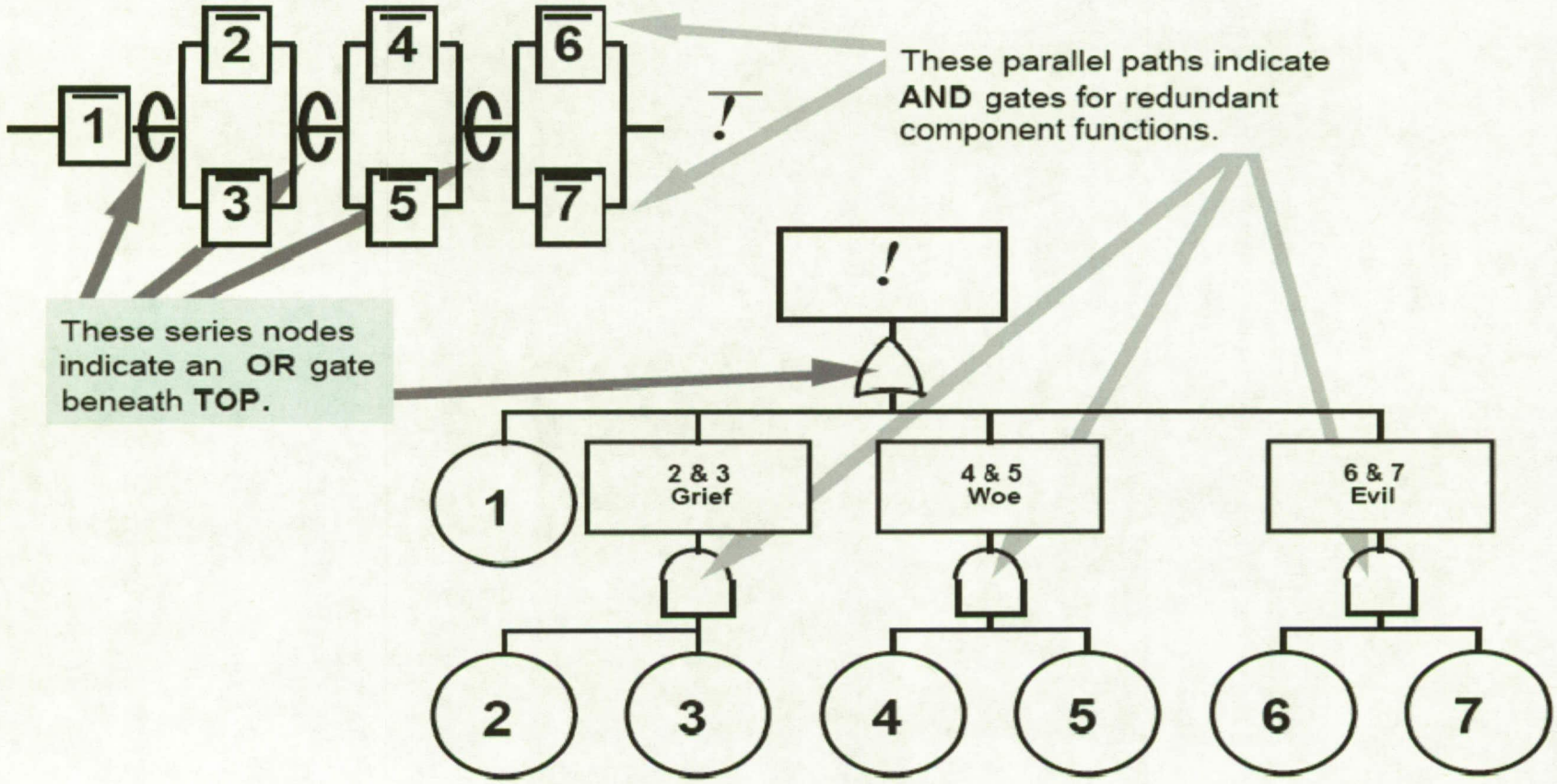
RRET Implementation Process *(1 of 6)*

The RRET Implementation Process Involves 5 Steps:

- Step 1: Generation of System Baseline Reliability (R_{SBR}) Prediction [3]
  - RRET Uses Standard Industry Procedure (MIL HDBK 338)
    - o Define the Configuration for Which the Prediction Is Applicable
    - o Define the Service Use (Life Cycle)
    - o Define and Generate the Item Reliability Block Diagrams
    - o Define the Mathematical Models for Computing Item Reliability
    - o Define the Parts of the Item
    - o Define the Environmental Profile and Expected Conditions
    - o Define the Stress Conditions
    - o Define the Failure Distribution
    - o Define the Failure Rates
    - o Compute the Item Reliability

RRET Implementation Process *(2 of 6)*

- Step 2: Transformation of the RBD Model to a Fault Tree Model [8]
  - Fault Tree Generation



RRET Implementation Process *(3 of 6)*

- Step 2: Transformation of the RBD Model to a Fault Tree Model *(Continued)*
  - Calculate the Corresponding Failure Probabilities
    - Perform Analyses Per Fault Tree Software Package
      - System Failure Probability ($P_F = 1 - R$)

RRET Implementation Process *(4 of 6)*

- Step 3: Determination of Failure Probabilities for Residual Risks and Uncertainty Events [3]
  - Residual Risks Sources
    - Manufacturer's
    - MIL-Standards
    - Historical Data (Similarity Theory)
    - Simulation Data
    - Test Data
    - Industry Standards
    - Delphi Technique
  - Mitigation Plan Uncertainty Events Source
    - Delphi Technique

RRET Implementation Process *(5 of 6)*

- Step 4: Generation of Residual Risks Fault Tree [2]
  - Construct Fault Tree Using Software Package
    - o Integrate Residual Risks and Mitigation Plan Uncertainty Events Into the Baseline Fault Tree
      - – Residual Risks and Designated Mitigation Plan Uncertainty Events Are Propagated Through an AND Gate
    - o Determine System Failure Probability (P_{SRRF})

RRET Implementation Process *(6 of 6)*

- Step 5: Determination of Residual Risk Indicator
  - Calculate the System Residual Risk Reliability (R_{SRRR}) Parameter
    - $R_{SRRR} = 1 - P_{SRRF}$
  - Derive the Residual Risk Indicator
    - Indicator = $R_{SBR} - R_{SRRR}$

2009 ARS, North America, San Diego

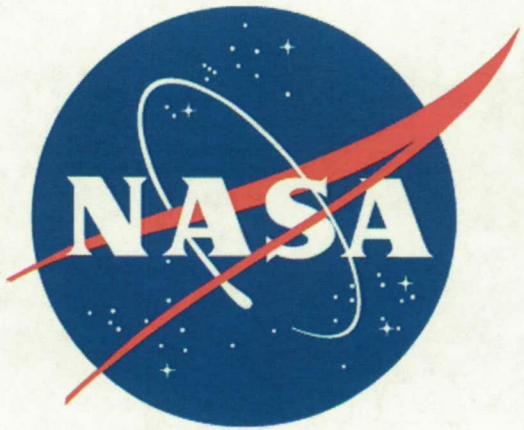
Track 2, Session 11

Begins at 10:30 to 11:30 AM, Thursday, June 11, 2009

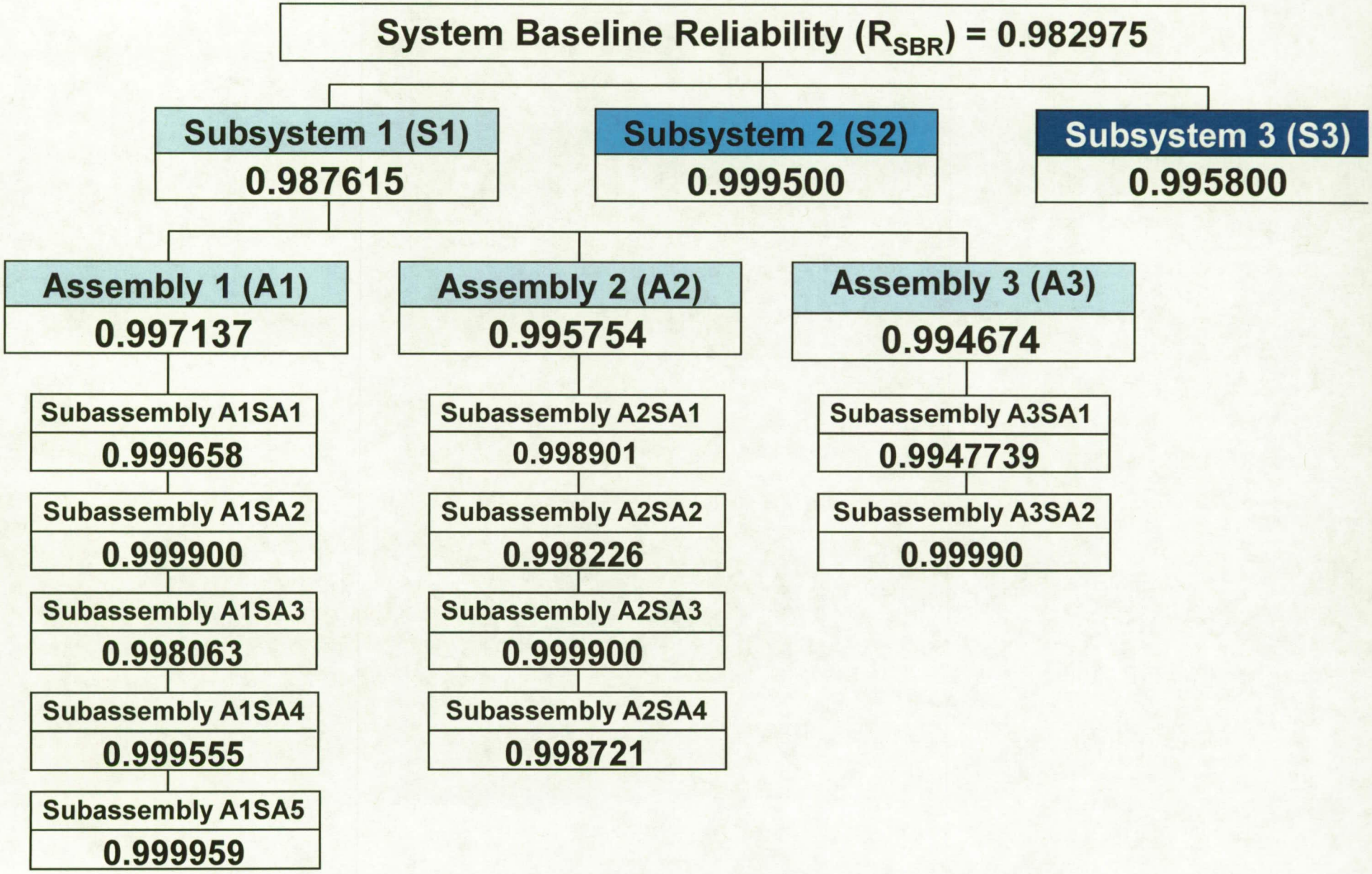
Current Time
5/22/2009

RRET
Example

SAIC®
From Science to Solutions



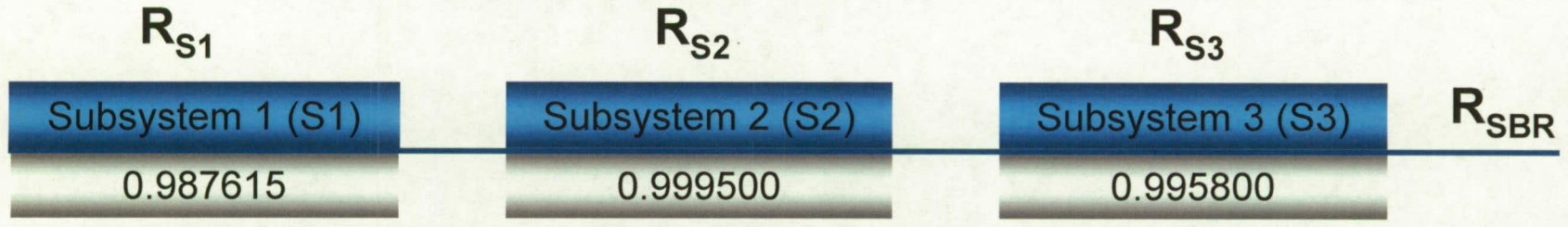
Step 1: Generation of System Baseline Reliability Prediction, R_{SBR} *(1 of 2)*



Step 1: Generation of System Baseline Reliability Prediction, R_{SBR} *(2 of 2)*

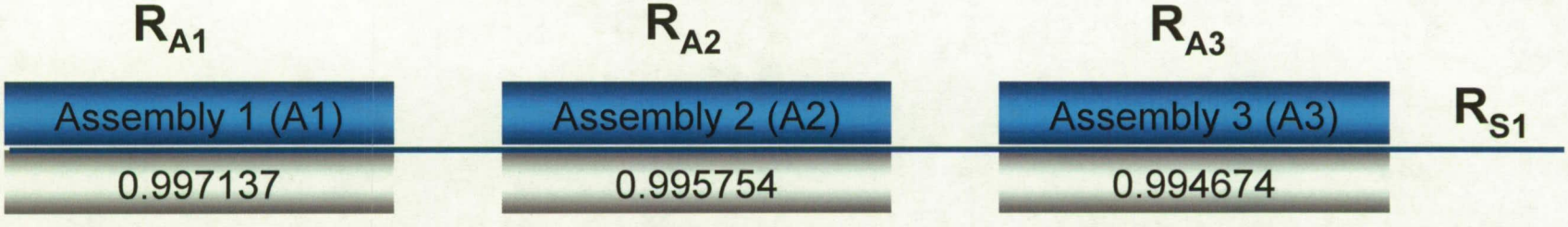
Reliability Block Diagram Model:

System Baseline Reliability (R_{SBR}) = R_{S1}* R_{S2}* R_{S3}= 0 .982975



System Level Baseline Reliability (R_{SBR})

R_{S1} = R_{A1}* R_{A2}* R_{A3}= 0.987615

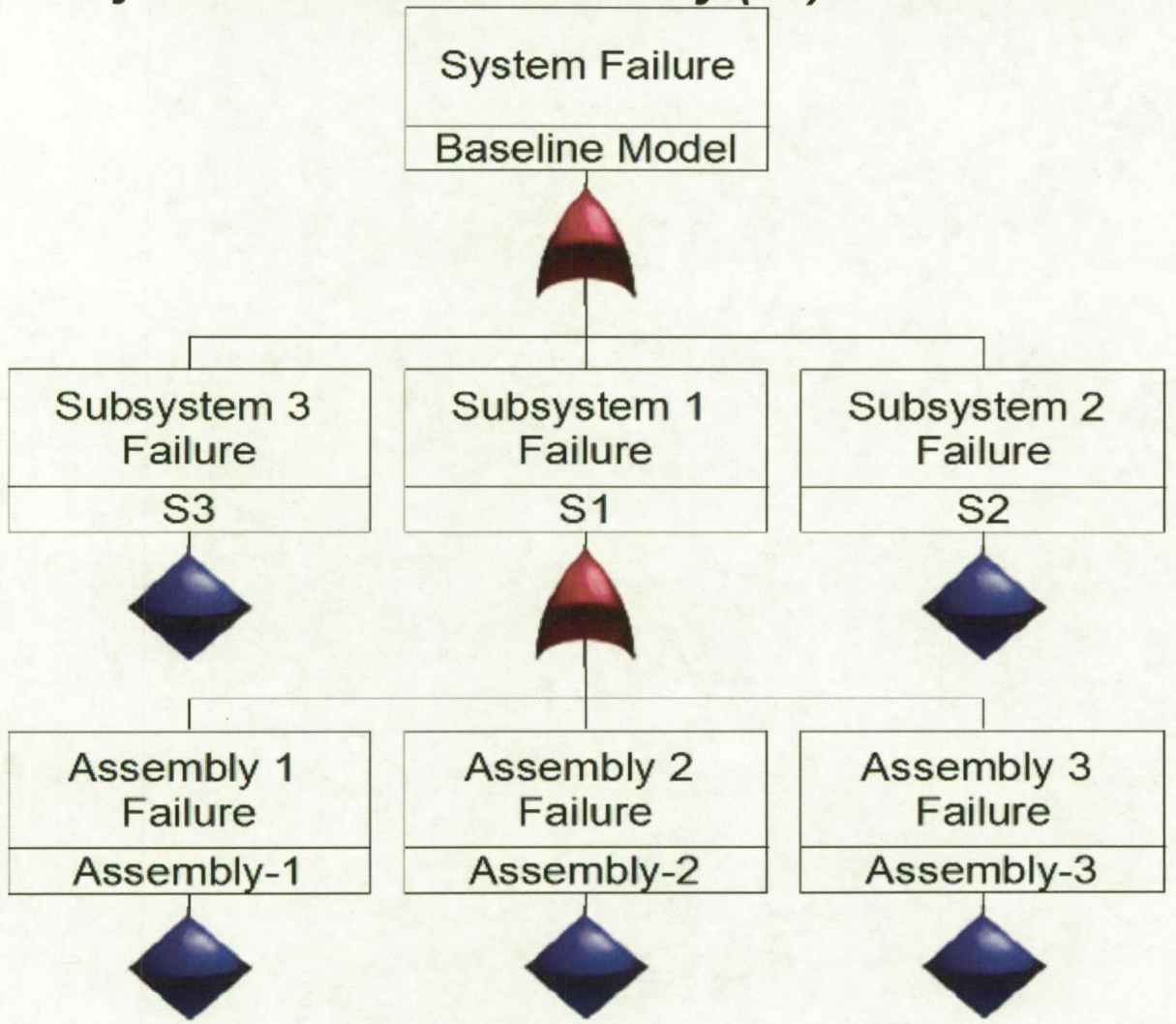


Subsystem Level Reliability (R_{S1})

Step 2: Transformation of the RBD Model to a Fault Tree Model

Fault Tree Diagram

System Failure Probability (P_F) = 0.017025



Step 3: Determination of Failure Probabilities for Residual Risks and Uncertainty Events

Residual Risk	Failure Probability	Data Source	Affected Subassembly
Risk Item 1	≈ 1.760E-03	Historical Data and Manufacturer	A1SA1
Risk Item 2	≈ 2.000E-04	Manufacturer and Test Data	A1SA1
Risk Item 3	≈ 1.937387E-03	Historical Data and Test Data	A1SA3
Risk Item 4	≈ 4.2710E-03	Mil-Standard and Historical Data	A2SA2
Risk Item 5	≈ 1.990E-05	Test Data	A2SA4

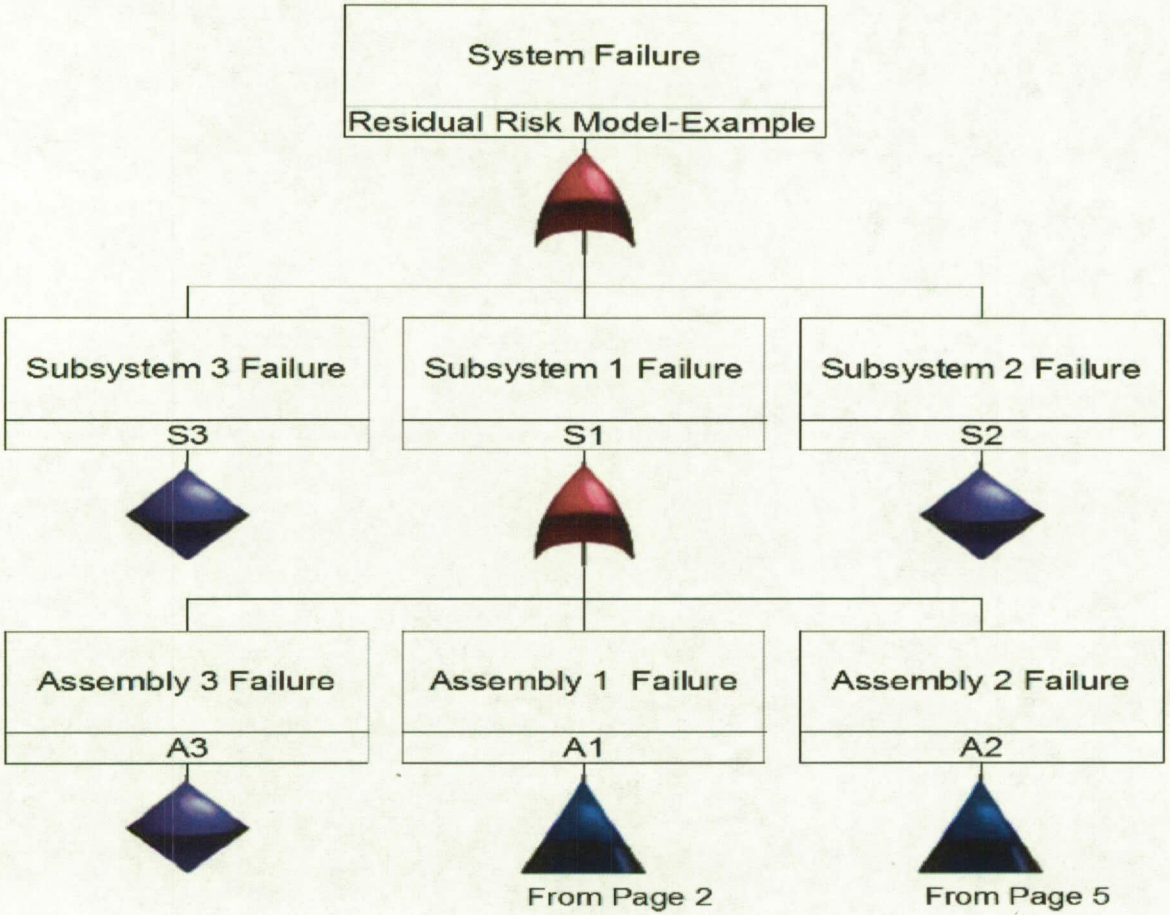
*To Simplify the Example, a Failure Probability Of .1 Was Used for the Mitigation Uncertainty Events… Delphi Technique

Step 4: Generation of Residual Risks Fault Tree *(1 of 6)*

Fault Tree Diagram (continued)

System Failure Probability (P_{SRRF}) = 0.017829

File Name: Applied Reliability Symposium -2009



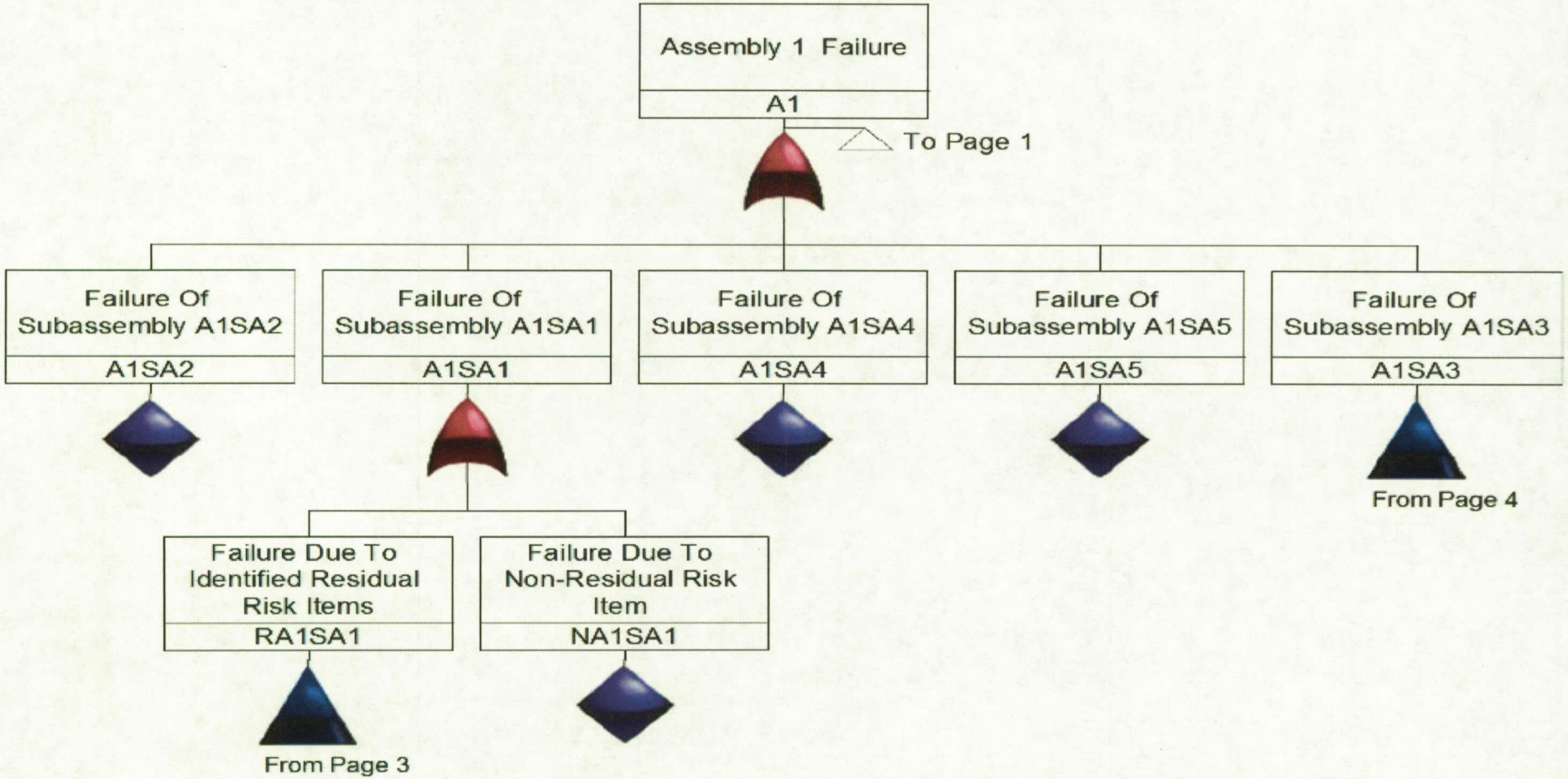
Page #: 1 of 6

Print Date: 4/7/2009

Step 4: Generation of a Residual Risk Fault Tree *(2 of 6)*

Fault Tree Diagram (continued)

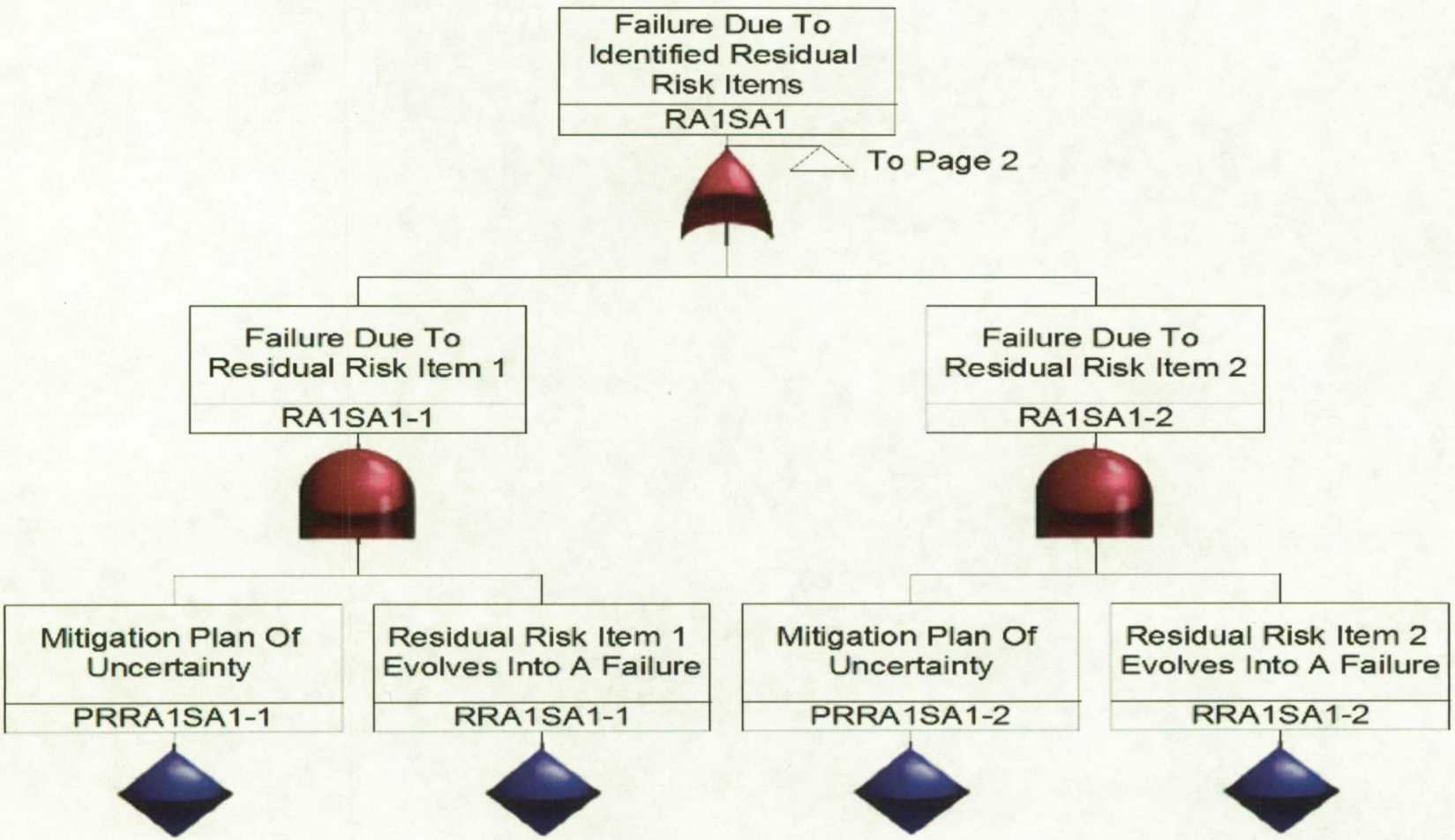
File Name: Applied Reliability Symposium -2009



Step 4: Generation of a Residual Risk Fault Tree *(3 of 6)*

Fault Tree Diagram (continued)

File Name: Applied Reliability Symposium -2009



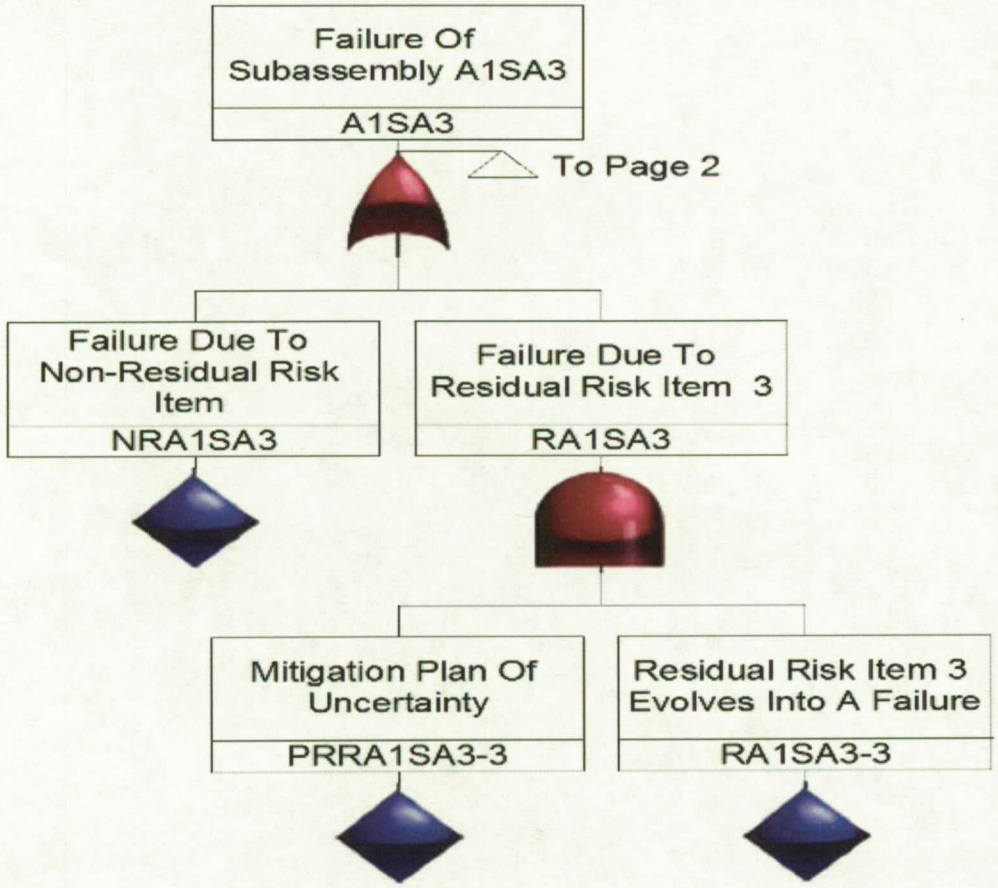
Page #: 3 of 6

Print Date: 4/7/2009

Step 4: Generation of a Residual Risk Fault Tree *(4 of 6)*

Fault Tree Diagram (continued)

File Name: Applied Reliability Symposium -2009



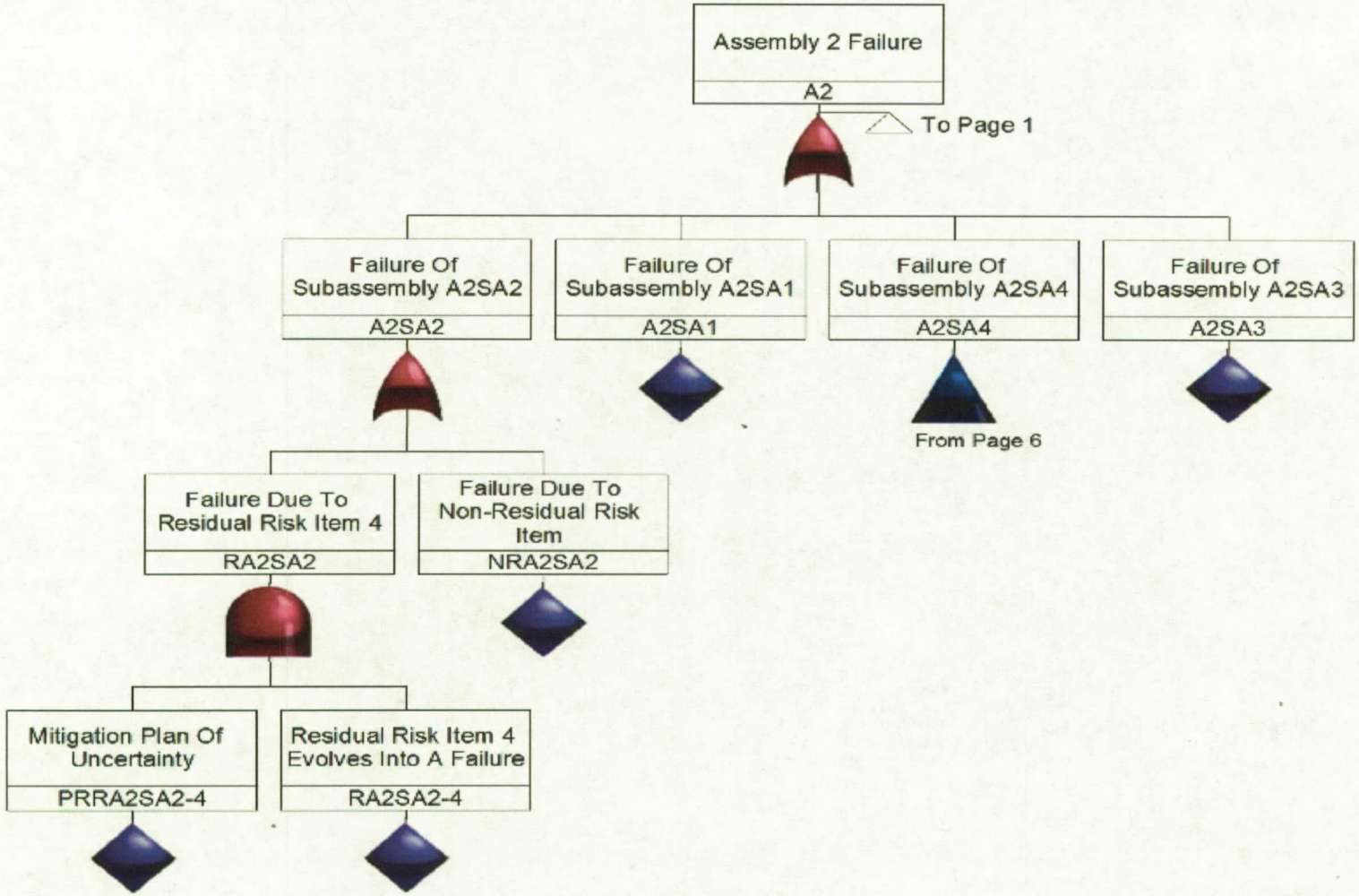
Page #: 4 of 6

Print Date: 4/7/2009

Step 4: Generation of a Residual Risk Fault Tree *(5 of 6)*

Fault Tree Diagram (continued)

File Name: Applied Reliability Symposium -2009

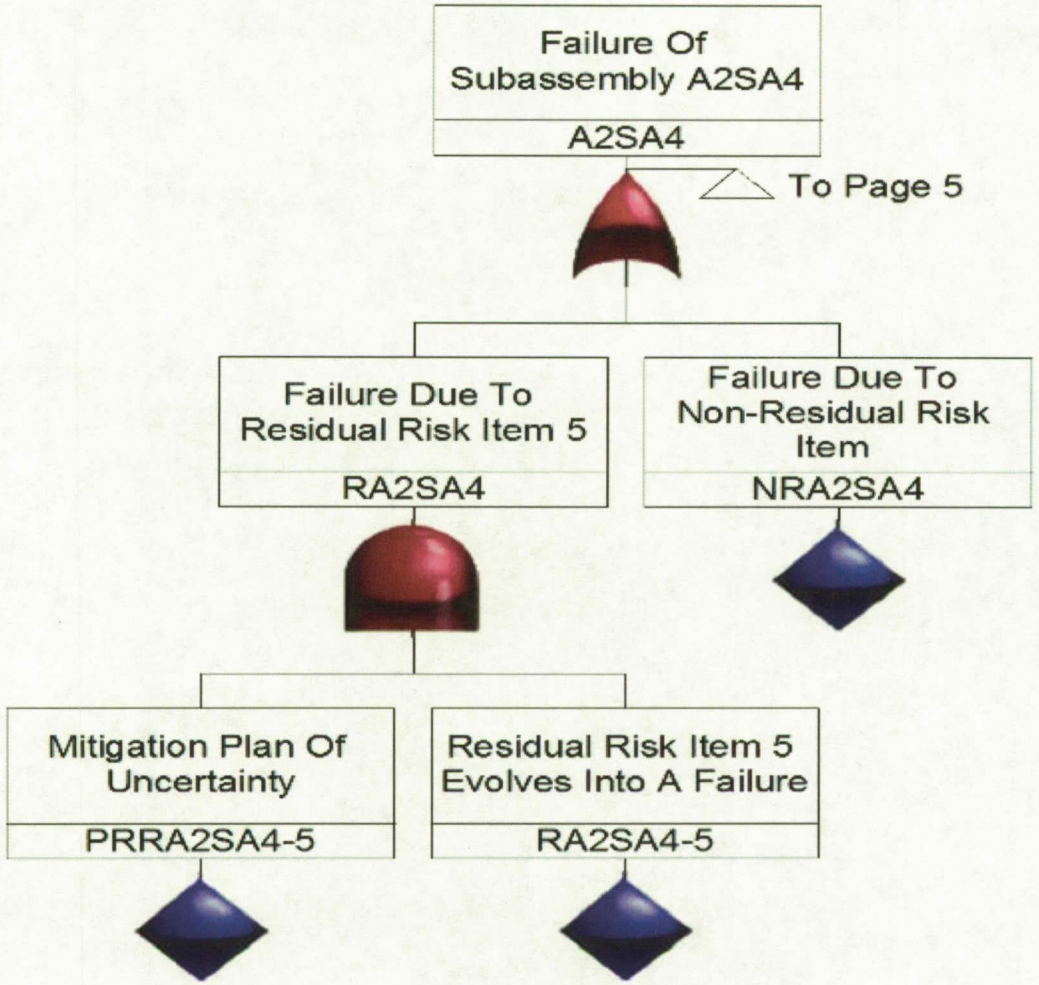


Print Date: 4/7/2009

Step 4: Generation of a Residual Risk Fault Tree *(6 of 6)*

Fault Tree Diagram (continued)

File Name: Applied Reliability Symposium -2009



Step 5: Determination of Residual Risk Indicator

- Calculate the System Residual Risk Reliability (R_{SRRR}) Parameter
  - $R_{SRRR} = 1 - P_{SRRF} = 0.982171$
- Derive the Residual Risk Indicator
  - Indicator = $R_{SBR} - R_{SRRR}$ = 0.982975 - 0.982171 = 0.000804

Summary

- KSC's S&MA Launch Services Division Developed a Residual Risk Evaluation Technique for Reliability Insight
  - It Is a Simplistic, Cost Effective Technique That Provides Decision Makers a Quantifiable Insight into the Severity of the Cumulative Residual Risks Impact Associated with any System.
  - The Quantifiable Insight Is Determined by Using the Proven Methodology
    - o Risk Management
    - o Reliability Prediction
    - o Fault Tree Analysis
  - RRET Calculates the Reduction In System Baseline Reliability Due to Identified Residual Risks.
- A Simple System Was Provided As an Example to Show RRET's Application
- RRET Can Be Adapted to a Wide Variety of Complex Systems, Processes, and Facilities

Where to Get More Information

- **6.0 References**

[1] NPR 8000.4, "Risk Management Procedural Requirements," 2/1/07

[2] Vesely, W.E., et al, "Fault Tree Handbook with Aerospace Applications," Prepared for NASA Office of Safety and Mission Assurance, NASA Headquarters, Washington, DC 20546, August 2002

[3] MIL Handbook 338, "Electronic Reliability Design Handbook," 10/1/1998

[4] LSP-PLIN-353-01, "Launch Services Program Risk Management Plan," 4/29/05

[5] NPD 8700.1C, "NASA Policy for Safety and Mission Success," 10/13/2002

[6] 2008 Space Systems Engineering and Risk Management Symposium Paper, "A Residual Risk Evaluation Technique Used For Expendable Launch Vehicles", 2/28/2008

[7] KTI-3643, "Launch Services Division Safety and Mission Assurance Operating Plan,"10/17/2007

[8] NASA Reference Publication 1358, "System Engineering Toolbox for Design-Oriented Engineers," December 1994

John A. Latimer

- **John A. Latimer** is currently a Senior System Lead Reliability Engineer at Science Applications International Corporation (SAIC) working on the NASA Expendable Launch Vehicle Contract. He has over 33 years experience in Systems Engineering and Risk Management with expertise in the Specialty System Engineering areas of Reliability, Maintainability, and Availability (RMA). His experience encompasses concept formulation, development, integration, test, production, and fielding of military and commercial systems.
- Education/Contact Information:
  - Mr. Latimer received his BS and MS degrees in Electrical Engineering from Tennessee State University and Stanford University, respectfully
  - E-mail Address: John.A.Latimer@nasa.gov or Latimerj@saic.com
  - Address: Mailcode Analex-3, Kennedy Space Center, FL 32899
  - Phone Number: 321-867-8719

Questions

Thank You for Your Attention

Do You Have Any Questions?

ATTACHMENTS

Attachment1:Definitions *(1 of 2)*

- **Assembly** is an item composed of any number of parts or subassemblies, joined together to perform a specific function, which can be disassembled without destruction.
- **Assessment** is an evaluation or appraisal of the state of a system, program/ project or a portion of a program/project.
- **Delphi Technique** is an iterative process that results in a consensus by a group of experts.
- **Fault Tree Analysis** is a deductive system reliability tool which provides both qualitative and quantitative measures of the probability of failure. It estimates the probability that a top level event will occur, systematically identifies all possible causes leading to the top event, and documents the analytic process to provide a baseline for future studies of alternative designs.
- **Human Error Risk Assessment** is a process that identifies risks to designs, equipment, procedures, and tasks as a result of human error.
- **Mission Reliability** is the measure of the ability of an item to perform its required function for the duration of a specified mission profile. Mission reliability defines the probability that the system will not fail to complete the mission, considering all possible redundant modes of operation.

Attachment1:Definitions *(2 of 2)*

- **Reliability Prediction** is a forecast of the reliability of a system or system element, postulated on analysis, past experience, and tests.
- **Residue Risk** is the risk that remain after risk management options have been identified and the required mitigation plans implemented properly.
- **Risk** is a combination of the likelihood of an undesirable event occurring and the severity of the consequences of the occurrence.
- **Risk Assessment, Quantitative** is the process of assigning proportional numerical quantities to both the likelihood and the adverse consequences of risk items.
- **Risk Management** is an organized means of controlling the risk on a program.
- **Risk Mitigation** is the process of reducing either the likelihood or the severity of a risk because the benefits from assuming the risk do not outweigh the perceived risk.
- **Subsystem** is a grouping of items satisfying a logical group of functions within a system.
- **System** is an integrated aggregation of end items, interfaces, and support functions designed to fulfill a specific mission requirement. A system may include equipment, trained personnel, facilities, data and procedures, and software. For program/project purposes, a system is typically defined as the highest level of hardware organization composed of multiple subsystems.

Attachment 2:Acronyms *(1 of 1)*

- **ELV** - Expendable Launch Vehicle
- **FTA** - Fault Tree Analysis
- **FT** - Fault Tree
- **KSC** - Kennedy Space Center
- **OSMA** - Office of Safety and Mission Assurance
- **P_F** - Probability of Failure
- **P_S** - Probability of Success
- **RBD** - Reliability Block Diagram
- **NASA** - National Aeronautics and Space Administration
- **NPD** - NASA Policy Directive
- **NPG** - NASA Procedures and Guidelines
- **R_{SBR}** - System Baseline Reliability
- **R_{SRRR}** - System Residual Risk Reliability
- **RMP** - Risk Management Program
- **RRET** - Residual Risk Evaluation Technique
- **SMA** - Safety And Mission Assurance

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
11-06-2009	Applied Reliability Symposium Presentation	Nov. 2008 - Jan. 2009

4. TITLE AND SUBTITLE

The Application of a Residual Risk Evaluation Technique Used for Expendable Launch Vehicles

5a. CONTRACT NUMBER

NAS10-02026

5b. GRANT NUMBER

N/A

5c. PROGRAM ELEMENT NUMBER

N/A

6. AUTHOR(S)

John A. Latimer

5d. PROJECT NUMBER

N/A

5e. TASK NUMBER

N/A

5f. WORK UNIT NUMBER

N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

KSC' s Safety and Mission Assurance Launch Service Division (SA-D) \ SAIC
Kennedy Space Center, FL 32899

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

KSC' s Safety and Mission Assurance Launch Service Division (SA-D)
Kennedy Space Center, FL 32899

10. SPONSOR/MONITOR'S ACRONYM(S)

SA-D

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified - Public Dissemination

13. SUPPLEMENTARY NOTES

N/A

14. ABSTRACT

This presentation provides a Residual Risk Evaluation Technique (RRET) developed by Kennedy Space Center (KSC) Safety and Mission Assurance (S&MA) Launch Services Division. This technique is one of many procedures used by S&MA at KSC to evaluate residual risks for each Expendable Launch Vehicle (ELV) mission. RRET is a straight forward technique that incorporates the proven methodology of risk management, fault tree analysis, and reliability prediction. RRET derives a system reliability impact indicator from the system baseline reliability and the system residual risk reliability values. The system reliability impact indicator provides a quantitative measure of the reduction in the system baseline reliability due to the identified residual risks associated with the designated ELV mission. An example is discussed to provide insight into the application of RRET.

15. SUBJECT TERMS

Residual Risk, Risk Management, Fault Tree Analysis, and Reliability Prediction

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			John A. Latimer
U	U	U	UU	32	19b. TELEPHONE NUMBER *(Include area code)* 321-867-8719