# Reliability, Maintainability, & Availability

## Consideration to Ensure Mission Success

**Amanda M Gillespie, ASQ CRE**, Solutions Architect, Logistics & Supply Chain Service Line
March 1, 2014

SAIC®

# Contents


- Background
  - What is RMA?
  - RMA Analysis Purpose
  - RMA Design Life Analysis Process
- SAIC RMA: Solution to a Challenge
- SAIC RMA
  - Requirement Development
  - Allocation
- SAIC RMA Analysis of Systems
- Other RMA Analyses
- Summary

# What is RMA?

- RMA is the acronym for Reliability, Maintainability, and Availability
  - Reliability (R)
    - *The probability (likelihood) that a component or system will perform its intended function with no failures for a given period of time (mission time) when used under specific operating conditions (test environment or operating environment)*
  - Maintainability (M)
    - *The probability a failed item will be restored or repaired to a specified condition within a given period of time*
  - Availability (A)
    - *The probability that a repairable system will perform its intended function at a given point in time or over a specified period of time when operated and maintained in a prescribed manner. Thus , availability is a function of reliability and maintainability*

$$f(R,M) = A$$

# RMA Analysis Purpose

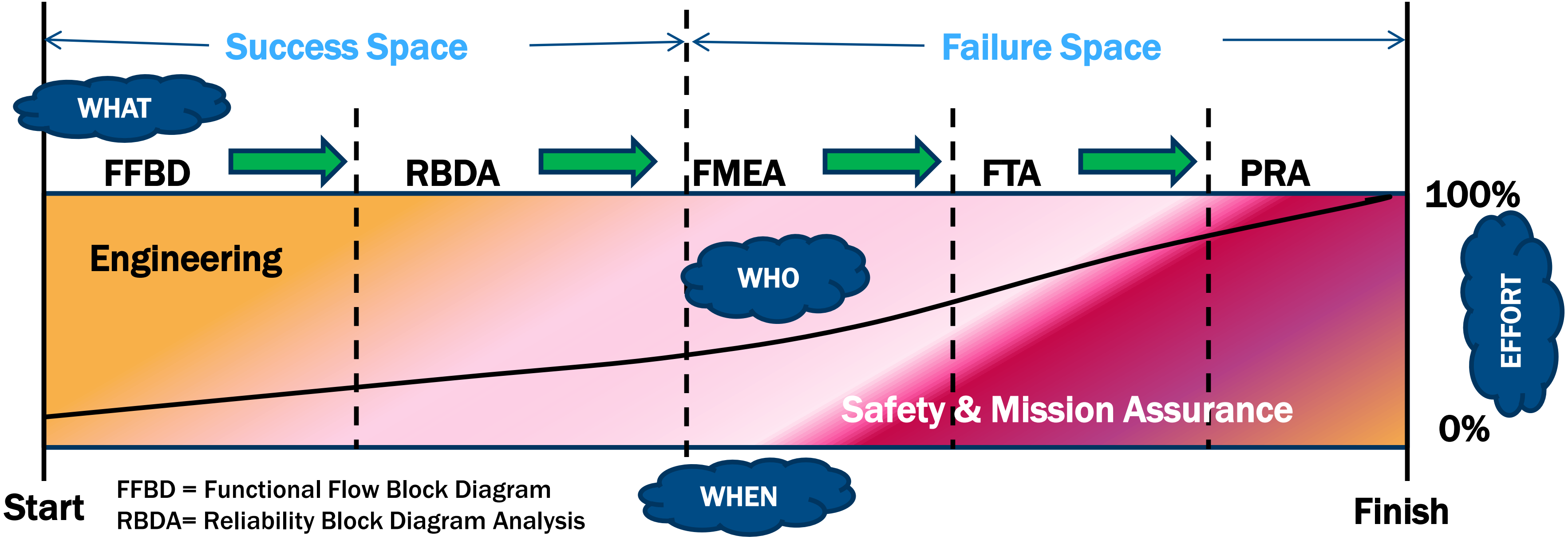
- To reduce lifecycle cost by:
  - *Efficiently and effectively identifying limitations within a system that may cause a failure before the intended lifetime*
  - *Identify unreliable systems that may pose a safety or health hazard*
  - *Providing specific reliability requirements for component procurement*
  - *To identify wasted efforts and hardware that were intended to improve Availability, but are providing little value*
- To study, characterize, measure, and analyze the failure and repair of systems in order to:
  - *Improve their operational use by increasing their design life*
  - *Eliminate or reduce the likelihood of failures and safety risks*
  - *Reduce downtime (maintenance), thereby increasing available operating time*



SAIC®

# RMA Design Life Analysis Process

- Ideally, the Reliability Engineering process looks like this:




FFBD = Functional Flow Block Diagram
RBDA= Reliability Block Diagram Analysis
FMEA= Failure Mode & Effects Analysis
FTA = Fault Tree Analysis
PRA= Probabilistic Risk Assessment

# SAIC RMA: Solution to a Challenge

- KSC GSDO Program needs to deliver high launch probability
  - Lunar missions and beyond require multiple launches and payloads to achieve mission goals
  - Commercial, DoD, and NASA customers will desire high availability from Ground Systems for launch support
  - The cost of each launch "scrub" is severe
    - De-tanking vehicles, re-synchronizing orbits, rescheduling Range conflicts, resting crew, etc
    - If a ground systems cause this scrub (*when the vehicle was otherwise "Available"*), then the community's penalty is even more severe
- High Probability of Successful launch is needed; however, challenges were faced:
  - KSC Ground Systems delivered 88% probability of launch during Space Shuttle Program (SSP) for any given launch countdown
  - KSC Ground Systems Constellation Program (CxP) requirement was 99% probability of launch for the last 10 hours of launch countdown
  - GSDO Program requirement is 98% Inherent Launch Availability for any given launch countdown



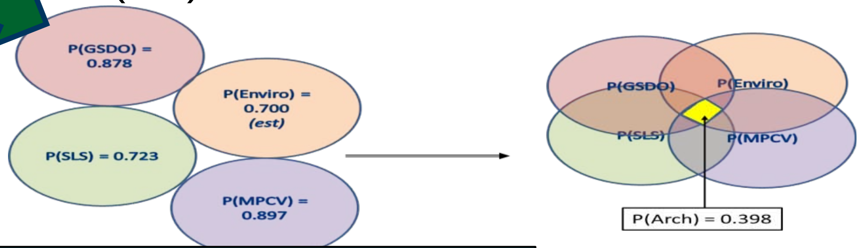
SAIC

# SAIC RMA: Solution to a Challenge

- **Risk Factors for GSDO:**

| GSDO |
| --- |
| Ground Systems |
| Human Errors |
| Range Conflicts |
| Range Systems |
| Range Intrusions |
| Hurricanes |

- **Risks for launch probability:**
  - GSDO
  - Space Launch System (SLS) – the Launch Vehicle
  - Orion Multi-Purpose Crewed Vehicle (MPCV)
  - Environments – Launch Weather (Wx), Abort Wx, Sea State



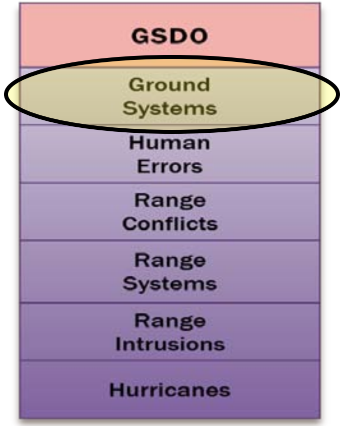

**Example of Probability of Architecture on Any Given Launch Attempt***
**Does not necessarily represent actual risk probabilities.*

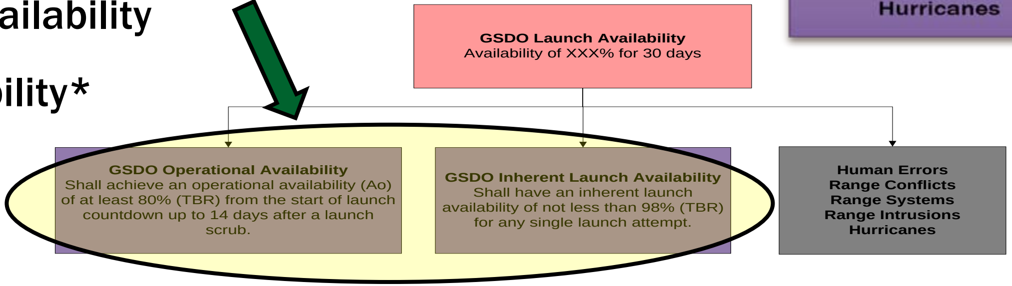


SAIC®

# SAIC RMA: Requirement Development

- Needed to put requirements in place to minimize risks to successful launch support
  - Only could control risks to Ground Systems design and upgrades
  - Allocated Availability requirements to ground systems
    - Inherent Launch Availability
    - Operational Availability*



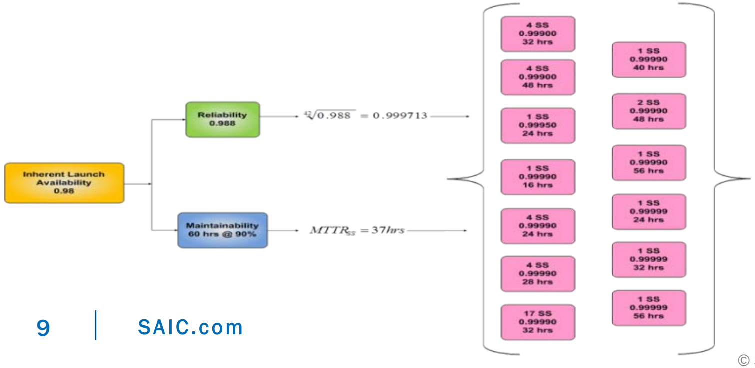

***Operational availability cannot be controlled by system design, but Inherent Availability can***

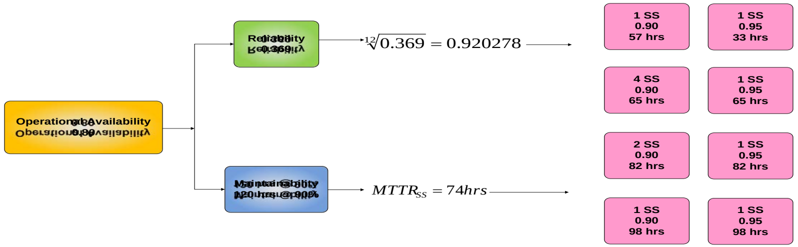


SAIC

# SAIC RMA: Requirement Allocation

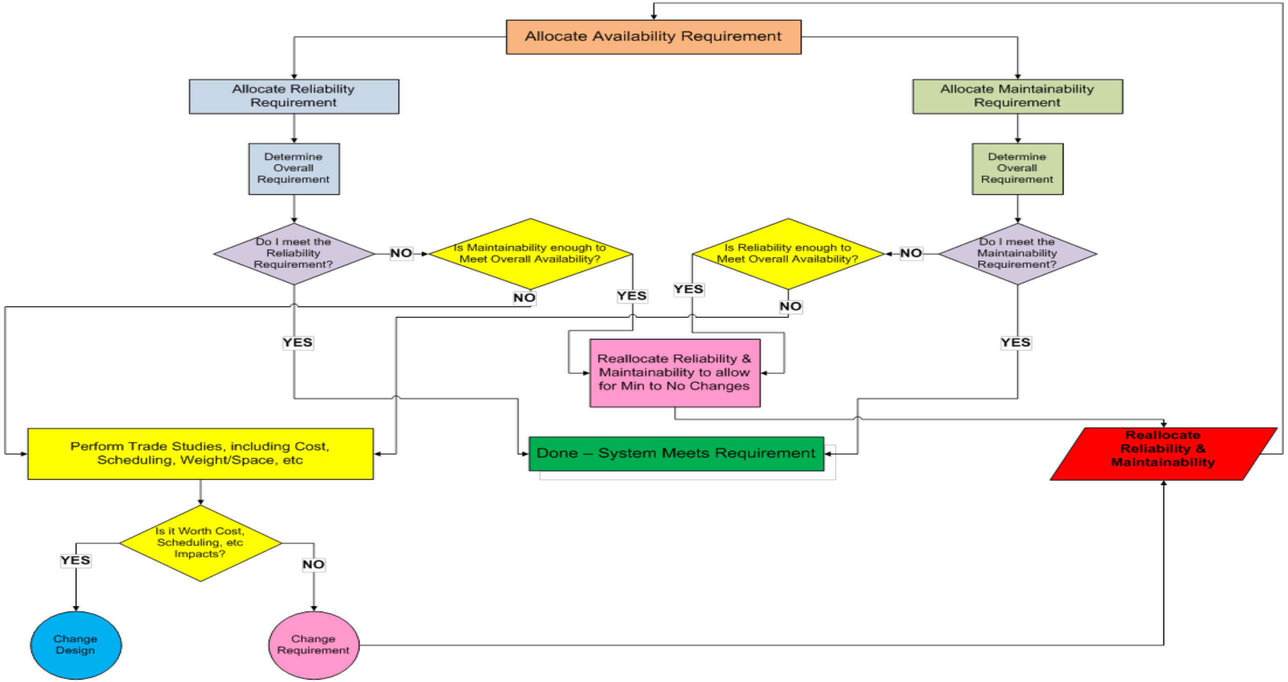
- Reliability allocations made via improved Reliability Apportionment Method
  - *Accounts for knowledge of ground system performance, design, and use*
- Maintainability allocations made via an improved MIL-HDBK-470A method
  - *Accounts for knowledge of ground system design, fault isolation techniques, and maintenance design characteristics, i.e., accessibility on the pad*



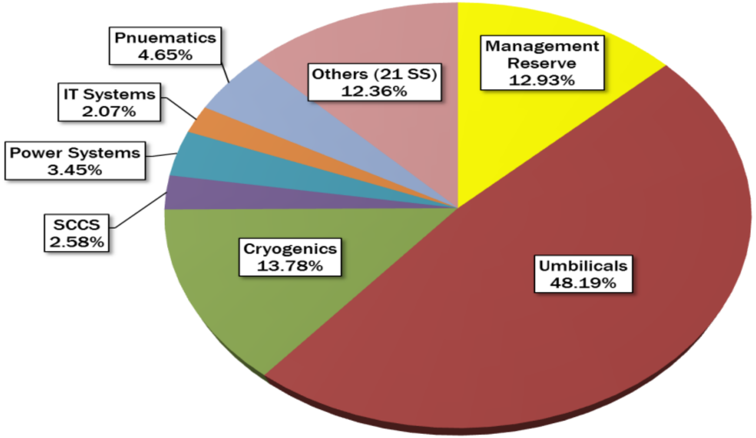
# SAIC RMA: Requirement Allocation

- Allocation is an iterative process
  - As designs are analyzed, allocations may need to be adjusted



# SAIC RMA: Requirement Allocation

- "Management reserve" is built into each RMA requirement allowing for room for growth in GSDO subsystems
  - Fraction of the overall requirement is unallocated
  - If the cost for an availability improvement in a subsystem design outweighs the benefit in increased GSDO launch availability, there is enough management reserve to leave the design as-is, in most cases




- The RMA analyses are completed during the design and upgrade schedules
  - RMA analysis is a required product for design milestones (30/60/90 or 45/90)
  - RMA analyses are performed as requested to assist in trade studies



SAIC

# SAIC RMA Analysis of Systems

1) Develop Component List from Subsystem Drawings

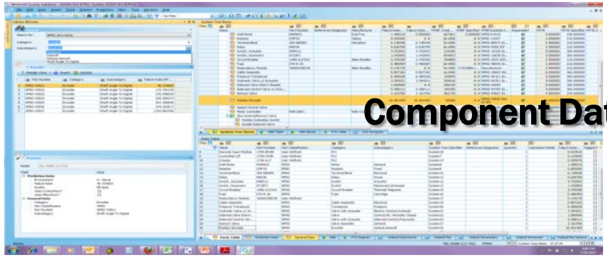
2) Develop Reliability Block Diagram (RBD) from Subsystem Drawings

3) Determine Reliability, Maintainability, and Availability from RBD

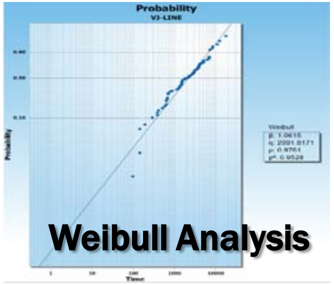
4) Determine Cut Sets from RBD

5) Determine Importance Measures from Cut Sets

6) Report Results and Recommendations in Subsystem RMA Reports



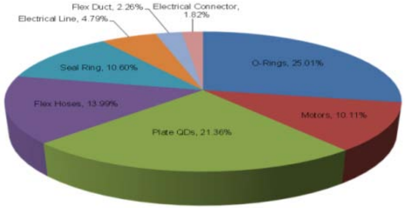
**Component Data**



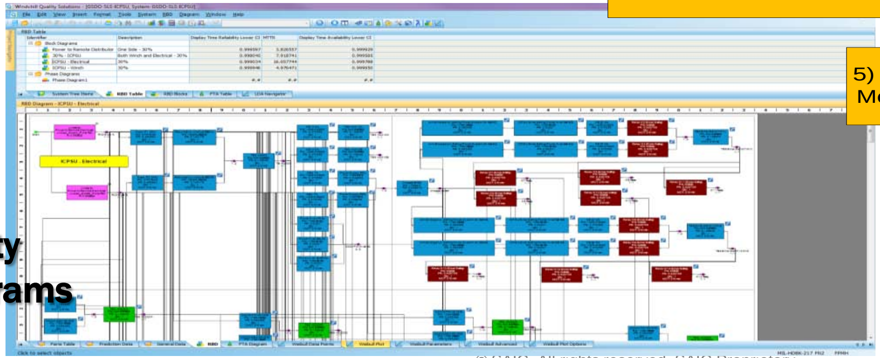

**Weibull Analysis**

| CUM UNAVAIL % | UNAVAIL % | UNAVAIL | Component Failure | Component Failure |
|---|---|---|---|---|
| 5.92% | 5.92% | 0.000146 | ICPSU Position Encoder 1 | |
| 11.83% | 5.92% | 0.000146 | ICPSU Position Encoder 3 | |
| 13.13% | 1.30% | 3.22E-05 | 4000 PSI Hydraulic Supply Pressure Xducer (36583MT-1) | |
| 14.22% | 1.08% | 2.68E-05 | 2200 PSI GN2 Supply Valve (36583A12) | |
| 15.17% | 0.95% | 2.36E-05 | Fully Extend Switch (36596) | |
| 15.97% | 0.80% | 1.97E-05 | Slow Extend/Retrack Valve (36583A9) | |
| 16.67% | 0.70% | 1.72742E-05 | CB (GSP to RIO) 50A - Side A | CB (GSP to RIO) 50A - Side B |
| 17.37% | 0.70% | 1.72742E-05 | CB (GSP to RIO) 50A - Side A | Circuit Breaker (CB) 2A - Side B |
| 18.07% | 0.70% | 1.72742E-05 | CB (GSP to RIO) 50A - Side A | Circuit Breaker (CB) to TB - Side B |
| 18.77% | 0.70% | 1.72742E-05 | CB (GSP to RIO) 50A - Side A | Circuit Breaker to Chassis - Side B |
| 19.47% | 0.70% | 1.72742E-05 | CB (GSP to RIO) 50A - Side A | Circuit Breaker to Ind & Enable - Side B |
| 20.17% | 0.70% | 1.72742E-05 | Circuit Breaker (CB) 2A - Side A | CB (GSP to RIO) 50A - Side B |
| 20.87% | 0.70% | 1.72742E-05 | Circuit Breaker (CB) 2A - Side A | Circuit Breaker (CB) 2A - Side B |

**Cut Set Analysis**




**Importance Measures**



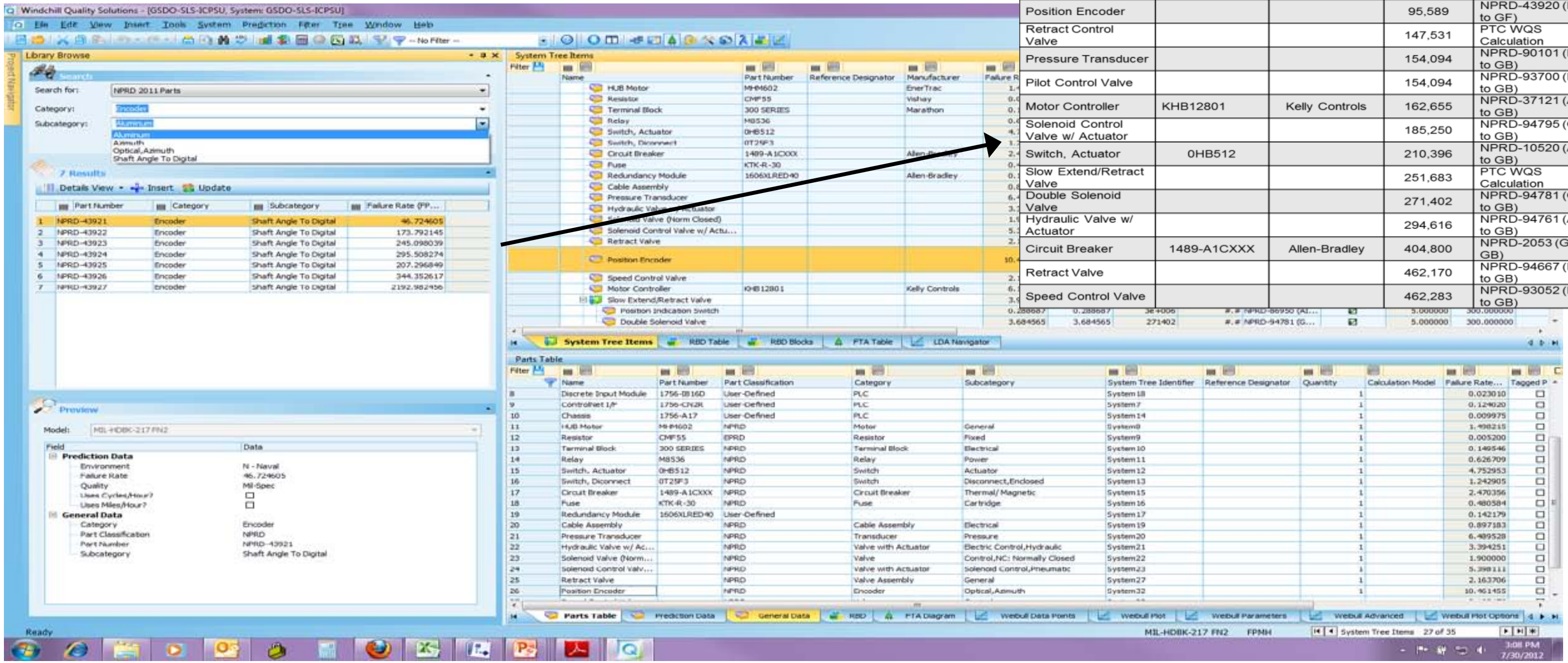
**Reliability Block Diagrams**



SAIC®

# SAIC RMA Analysis of Systems

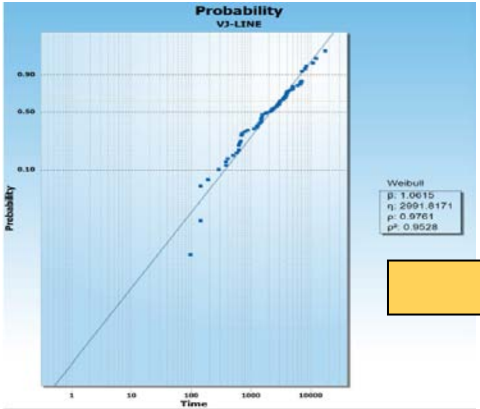
- Example of component data using COTS software: PTC Windchill Quality Solutions (WQS)

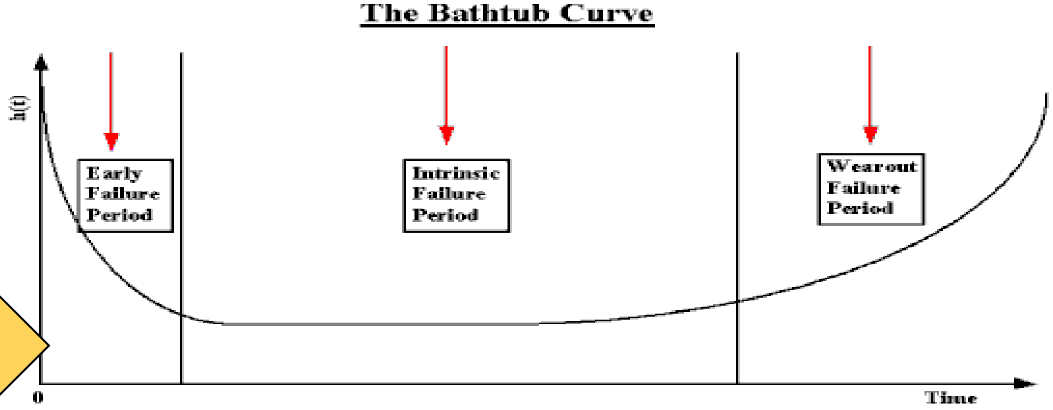



| Item Name | Part Number | Manufacturer (if known) | MTBF (hrs) | MTBF Source | MTTR (hrs) | MTTR Source |
|---|---|---|---|---|---|---|
| Position Encoder | | | 95,589 | NPRD-43920 (NU to GF) | 20 | Engineering Estimate |
| Retract Control Valve | | | 147,531 | PTC WQS Calculation | 5 | Engineering Estimate |
| Pressure Transducer | | | 154,094 | NPRD-90101 (NU to GB) | 5 | Engineering Estimate |
| Pilot Control Valve | | | 154,094 | NPRD-93700 (NU to GB) | 5 | Engineering Estimate |
| Motor Controller | KHB12801 | Kelly Controls | 162,655 | NPRD-37121 (AUF to GB) | 6 | Engineering Estimate |
| Solenoid Control Valve w/ Actuator | | | 185,250 | NPRD-94795 (GF to GB) | 5 | Engineering Estimate |
| Switch, Actuator | 0HB512 | | 210,396 | NPRD-10520 (AUG to GB) | 5 | Engineering Estimate |
| Slow Extend/Retract Valve | | | 251,683 | PTC WQS Calculation | 5 | Engineering Estimate |
| Double Solenoid Valve | | | 271,402 | NPRD-94781 (GM to GB) | 5 | Engineering Estimate |
| Hydraulic Valve w/ Actuator | | | 294,616 | NPRD-94761 (AUF to GB) | 5 | Engineering Estimate |
| Circuit Breaker | 1489-A1CXXX | Allen-Bradley | 404,800 | NPRD-2053 (GM to GB) | 3.5 | PTC WQS Estimate |
| Retract Valve | | | 462,170 | NPRD-94667 (NU to GB) | 4.5 | Engineering Estimate |
| Speed Control Valve | | | 462,283 | NPRD-93052 (NU to GB) | 5 | Engineering Estimate |

# SAIC RMA Analysis of Systems

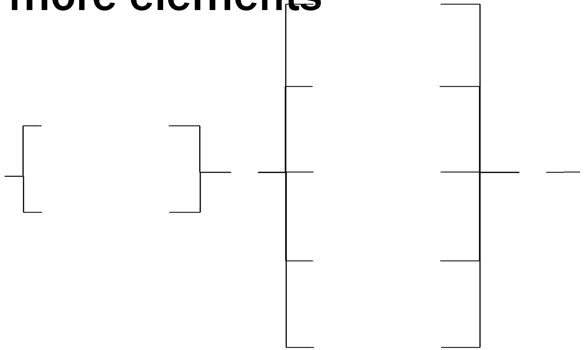
- Analysis of components will sometimes include Weibull analysis to attempt to determine what type of failures are experienced
  - Used for similar components
  - Used for heritage subsystems to characterize failure types seen:
    - Early failures (burn-in)
    - Useful Life (random failures)



# SAIC RMA Analysis of Systems

- Reliability Block Diagram (RBD) Analysis (RBDA):
  - Predicts reliability (uptime), maintainability (downtime), and availability (mission readiness being a function of uptime and downtime)
  - The RBDA method is used to estimate and analyze the reliability and availability for the systems containing at least two or more elements
    - RBDA is a “top-down” method in success space
    - Analyzes Reliability (and Availability) relationships
  - Quantitative

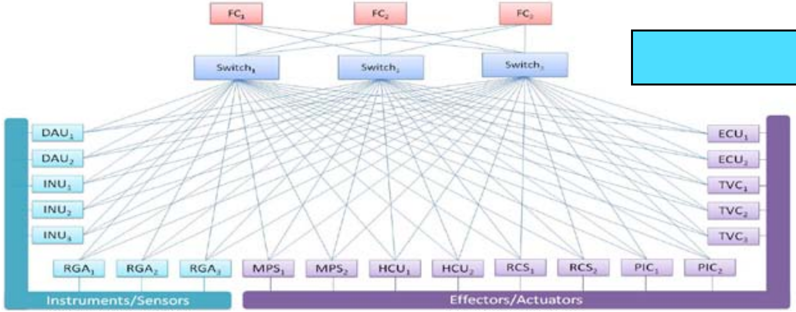


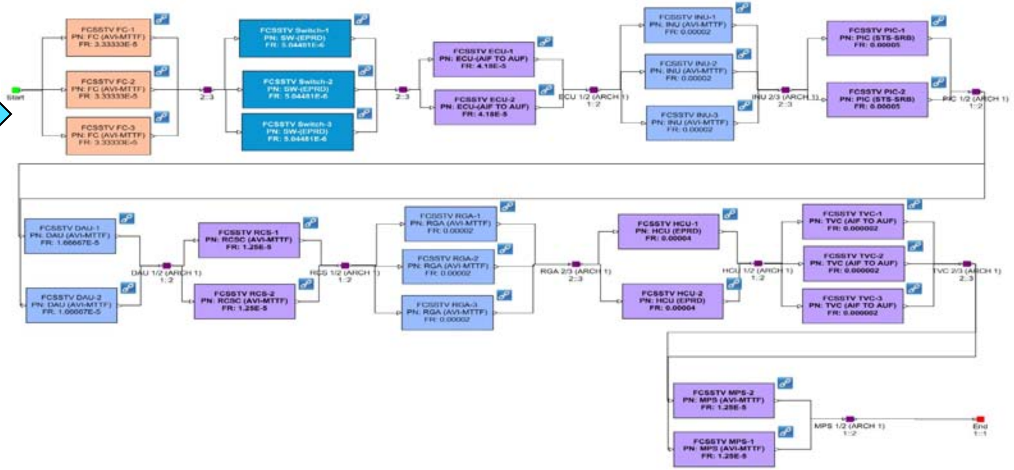


SAIC

# SAIC RMA Analysis of Systems

- RMA Team converts each drawing (mechanical and electrical) into a Reliability Block Diagram (RBD)
  - Verify accuracy and understanding of the components and their connections with the design team



# SAIC RMA Analysis of Systems

- RMA team determines the RMA of the subsystem by using both analytical and Monte-Carlo simulation calculations with at least 1,000,000 iterations.

**RMA Requirements**

| Reliability (for 24 hrs) | Maintainability (hrs) | Availability ($A_{inh}$) |
|---|---|---|
| 0.99900 | 48 | 0.998017 |

**Simulation Results**

| Reliability (for 24 hrs) | Maintainability (hrs) | Availability ($A_{inh}$) |
|---|---|---|
| 0.998448 | 12.59 | 0.999529 |

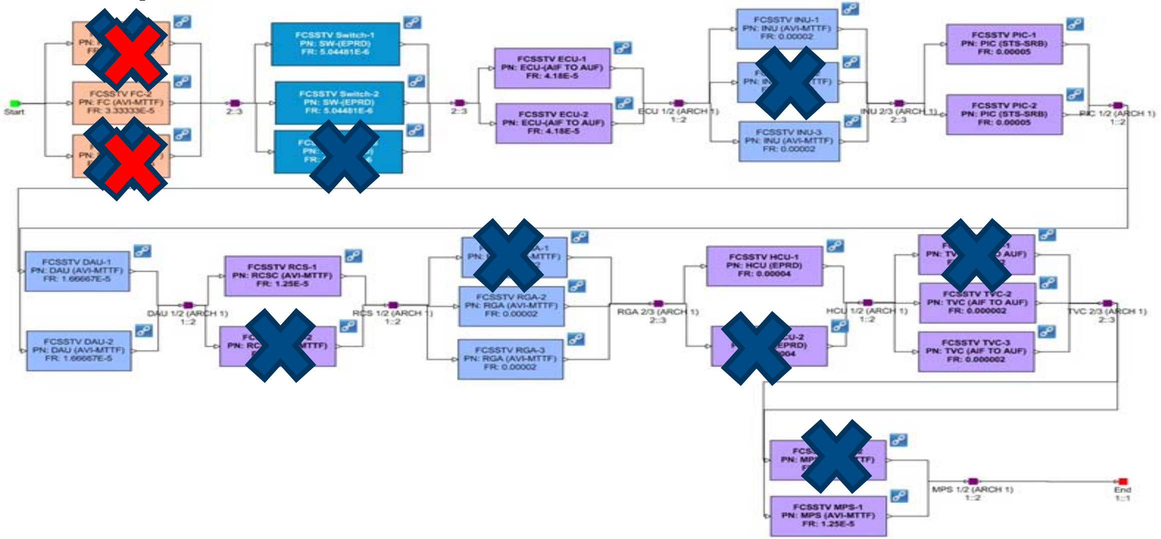
| Random Seed | Reliability | | | Failures per Million | MTTR (hrs) | Availability | | |
|---|---|---|---|---|---|---|---|---|
| | Lower Bound | Point Estimate | Upper Bound | | | Lower Bound | Point Estimate | Upper Bound |
| 1 | 0.998564 | 0.998636 | 0.998708 | 54.07 | 12.59 | 0.999521 | 0.999562 | 0.999603 |
| 10 | 0.998448 | 0.998523 | 0.998598 | 67.10 | 12.61 | 0.999439 | 0.999484 | 0.999529 |
| 100 | 0.998557 | 0.998630 | 0.998703 | 58.08 | 12.63 | 0.999520 | 0.999561 | 0.999602 |



SAIC

# SAIC RMA Analysis of Systems

- RMA Team performs Cut Set Analysis (CSA)
  - Provides clear indication of where most likely failure paths would be depending on the accuracy of the RBD and the accuracy of the failure data of the components

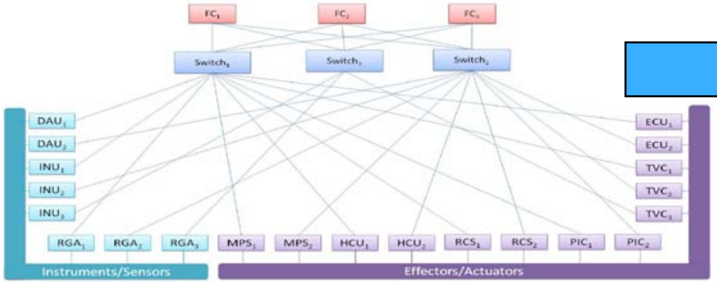


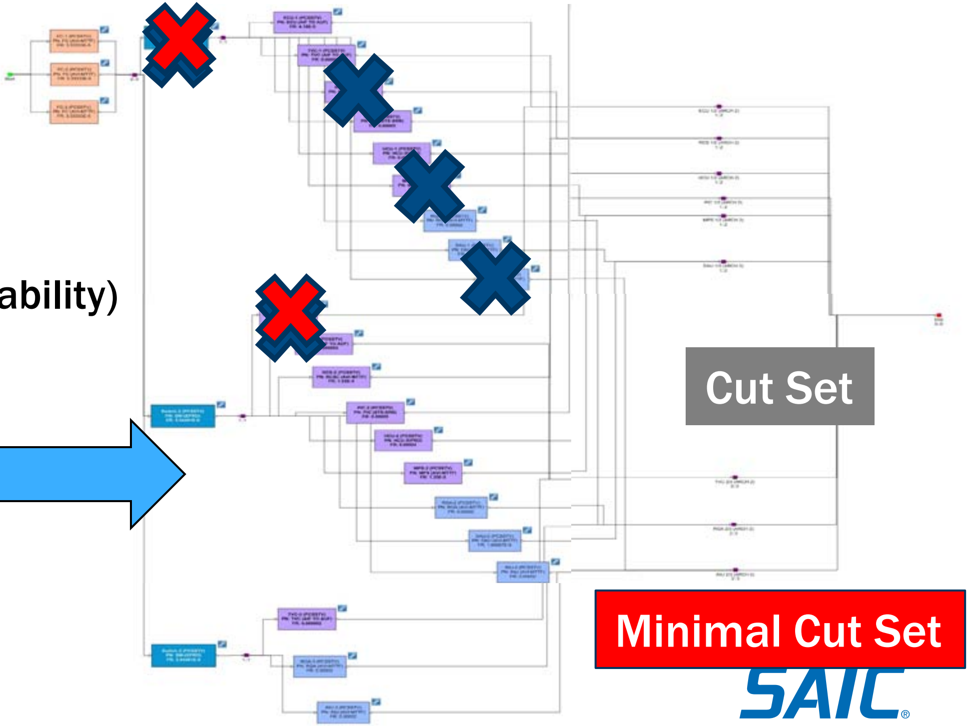

Cut Set

Minimal Cut Set

# SAIC RMA Analysis of Systems

- Enables the design team to focus on either:
  - Improving the design to correct the high failure nodes (improving reliability), or
  - Ensuring that the component is able to be repaired to an operational state as quickly as possible (improving maintainability)






SAIC

# SAIC RMA Analysis of Systems

- **Example of Cut Set Data**

| CUM UNAVAIL % | UNAVAIL % | UNAVAIL | Component Failure | Component Failure |
|---|---|---|---|---|
| 5.92% | 5.92% | 0.000146 | ICPSU Position Encoder 1 | |
| 11.83% | 5.92% | 0.000146 | ICPSU Position Encoder 3 | |
| 13.13% | 1.30% | 3.22E-05 | 4000 PSI Hydraulic Supply Pressure Xducer (36583MT-1) | |
| 14.22% | 1.08% | 2.68E-05 | 2200 PSI GN2 Supply Valve (36583A12) | |
| 15.17% | 0.95% | 2.36E-05 | Fully Extend Switch (36596) | |
| 15.97% | 0.80% | 1.97E-05 | Slow Extend/Retrack Valve (36583A9) | |
| 16.67% | 0.70% | 1.72742E-05 | CB (GSP to RIO) 50A - Side A | CB (GSP to RIO) 50A - Side B |
| 17.37% | 0.70% | 1.72742E-05 | CB (GSP to RIO) 50A - Side A | Circuit Breaker (CB) 2A - Side B |
| 18.07% | 0.70% | 1.72742E-05 | CB (GSP to RIO) 50A - Side A | Circuit Breaker (CB) to TB - Side B |
| 18.77% | 0.70% | 1.72742E-05 | CB (GSP to RIO) 50A - Side A | Circuit Breaker to Chassis - Side B |
| 19.47% | 0.70% | 1.72742E-05 | CB (GSP to RIO) 50A - Side A | Circuit Breaker to Ind & Enable - Side B |
| 20.17% | 0.70% | 1.72742E-05 | Circuit Breaker (CB) 2A - Side A | CB (GSP to RIO) 50A - Side B |
| 20.87% | 0.70% | 1.72742E-05 | Circuit Breaker (CB) 2A - Side A | Circuit Breaker (CB) 2A - Side B |

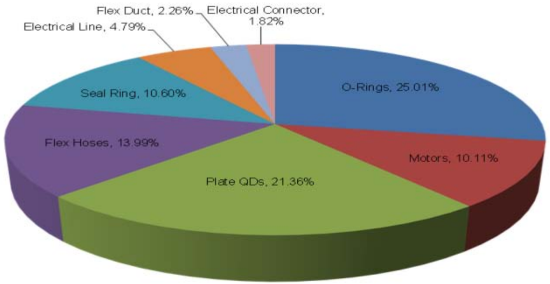


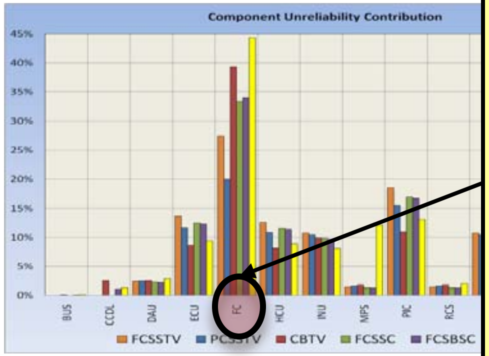
SAIC®

# SAIC RMA Analysis of Systems

- SAIC RMA Team performs Importance Measure Analysis (IMA)
  - Assesses the importance of the components in the subsystem or the sensitivity of the subsystem RMA to changes in the components' failure rates
  - Quantify the criticality of a particular component within a system design.

- This unique method described in paper written by RMA team, entitled, "*Comparison Modeling of System Reliability for Future NASA projects*" and presented at International Reliability and Maintainability Symposium (RAMS) in January 2012




1. Ensure this component/LRU is on hand in order to repair and/or replace when failed.
2. Ensure personnel are trained in procedures for repair and/or replace.
3. Ensure procedures are optimized for repair and/or replace.

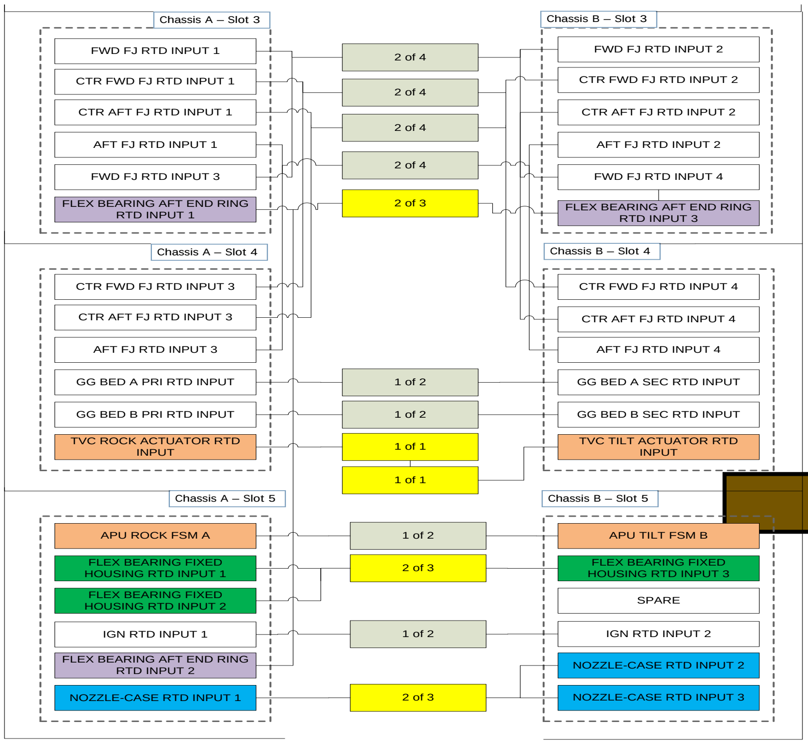
# SAIC RMA Analysis of Systems

- SAIC RMA Team reports results and recommendations in Subsystem RMA reports
  - Example recommendations for RMA improvement:
    - Have redundant components on separate busses
      - Improved availability by an order of magnitude (0.995 to 0.9994)
    - Move control and monitoring to different Programmable Logic Controller (PLC)
      - Had redundant monitoring on same PLC (*see next page*)
      - Improved availability by three orders of magnitude (0.9993 to 0.999999)
  - Example recommendations for trades:
    - Tertiary power system provides little to no improvement in availability (0.999995 to 0.999996); does not justify additional weight, space, and cost
    - Avionics architectures: triplex voter improves availability, however, self-checking pair does not

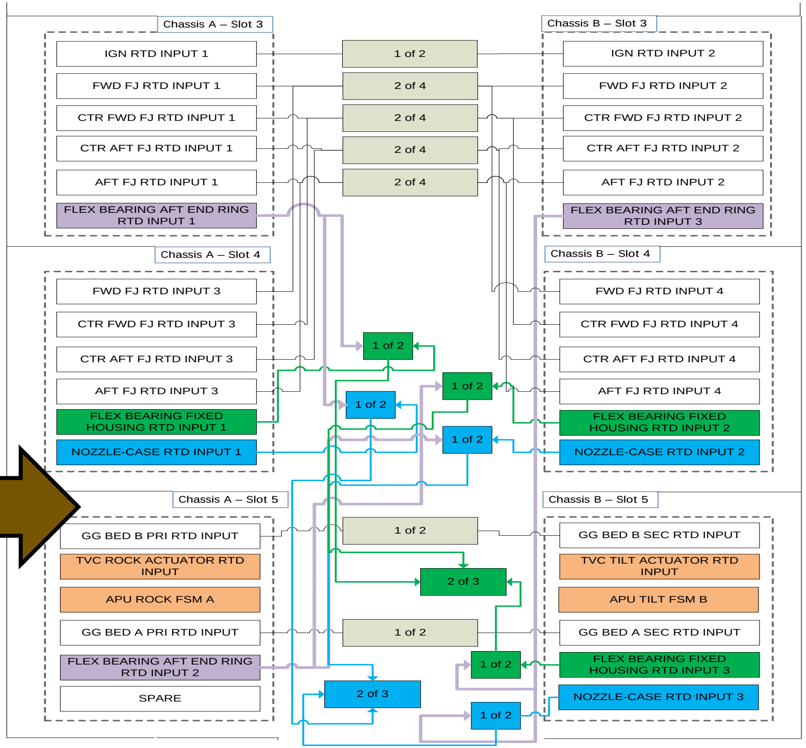



SAIC

# SAIC RMA Analysis of Systems



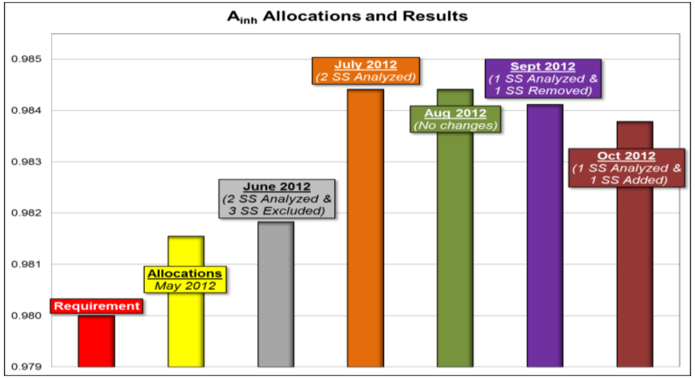

**R(10) = 0.999300**

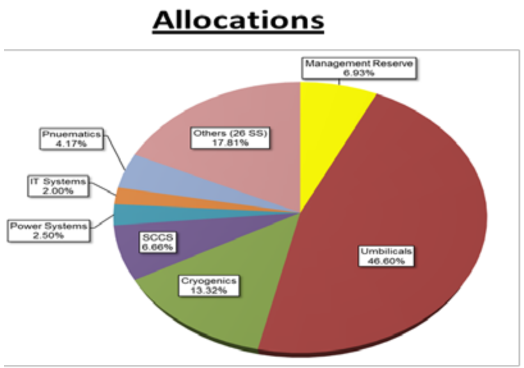


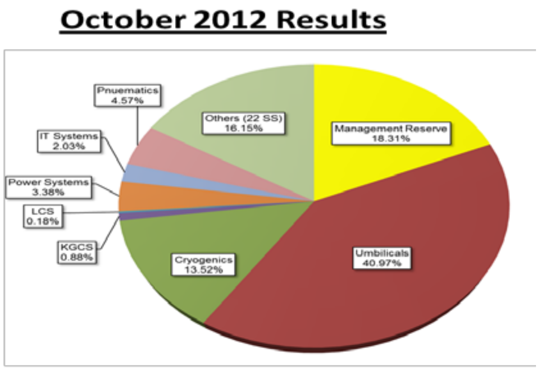

**R(10) = 0.999999**

# SAIC RMA Analysis of Systems

- Effectively monitoring and tracking RMA analysis results for management
  - Management informed of risk to achieving requirements almost immediately
- RMA tracking & reporting methodology effective and efficient in communicating recommendations for RMA improvements
  - Can quantify RMA improvements versus cost, scheduling, weight, space impacts



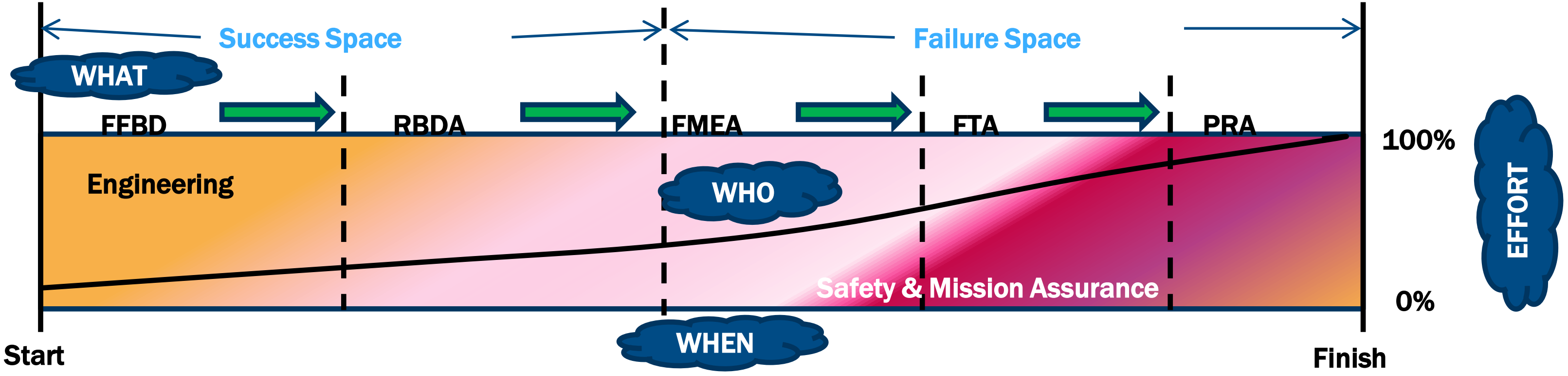



SAIC

# Other Reliability Engineering Analyses

# Other RMA Analyses

- Failure Modes & Effects Analysis (FMEA)
- Fault Tree Analysis (FTA)
- Probabilistic Risk Assessment (PRA)
- Historical Component Failure Rate Determination
- Component Burn-in and Test Time Requirements






SAIC

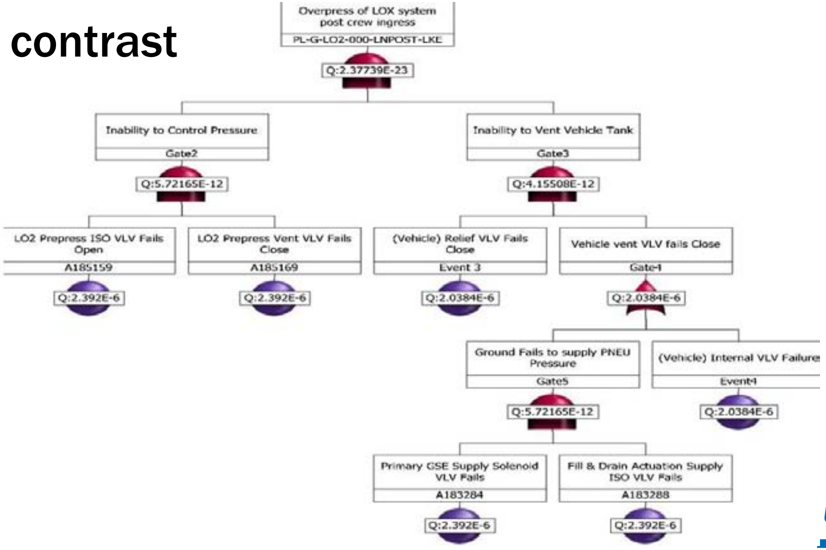
# Failure Modes and Effects Analysis (FMEA)

- Inductive (bottom-up) method where a table that describes the way or modes in which each system component can fail and assess the consequences of each of these failures is generated
- Determines hardware criticality
- Identifies the potential for single point failures
- Identifies areas where the design does not meet the failure tolerance requirements
- Changed from qualitative to quantitative by assigning values to:
  1. Probability of the failure occurring,
  2. Severity of the effect of the failure on the operation of the systems,
  3. Probability that the system controls will detect and eliminate the failure before the design is complete.
  - The product of all three values is the risk priority number (rpn)

| Rating | Description | Criteria |
|---|---|---|
| 1 | Very Low or None | Minor nuisance |
| 2 | Low or Minor | Product operable at reduced performance |
| 3 | Moderate or Significant | Gradual performance degradation |
| 4 | High | Loss of function |
| 5 | Very High or Catastrophic | Safety-related catastrophic failures |

# Fault Tree Analysis (FTA)

- Deductive (top-down) method that generates a symbolic logic model that traces and analyzes the failure paths from a predetermined, undesirable condition or event (called the top event) of a system to the failures or faults
- Can be qualitative or quantitative – *we do quantitative*
- FTA is an event-oriented analysis in contrast to the RBD, which is a structural-oriented analysis



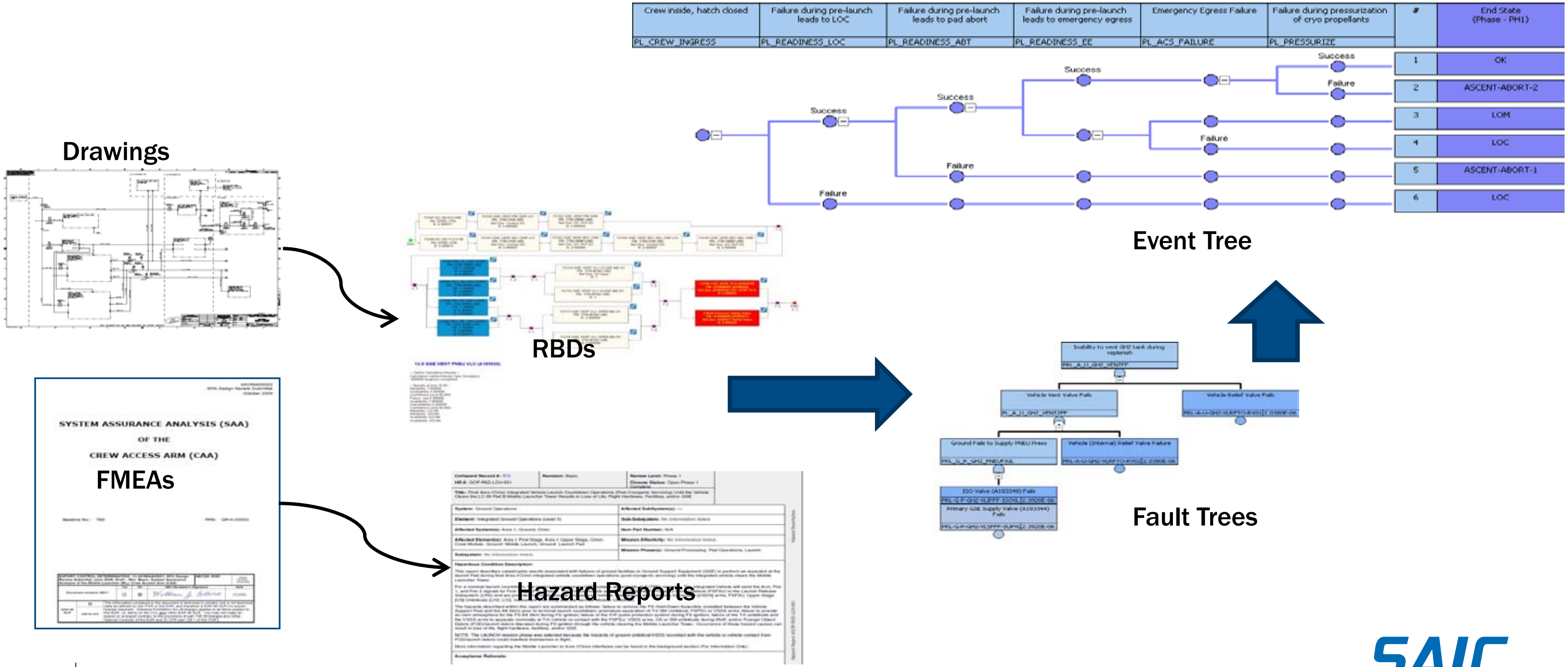
# Probabilistic Risk Assessment (PRA)

- Systematic and comprehensive methodology to evaluate risks associated with a complex system
- Risk in PRA is defined as scenarios, associated frequencies, and associated consequences
  - Risk management involves prevention of adverse scenarios and promotion of favorable scenarios
  - NASA uses Risk metrics of probability of loss of vehicle, mission failure, etc
- Goal is to describe how the system and its elements respond to an undesired initiating event, such as lightening or fire
- Quantitative
  - Magnitude of the possible adverse consequence
  - Probability of the occurrence of each consequence
- Include:
  - Human Reliability Analysis (HRA)
  - Common-Cause-Failure Analysis (CCF)

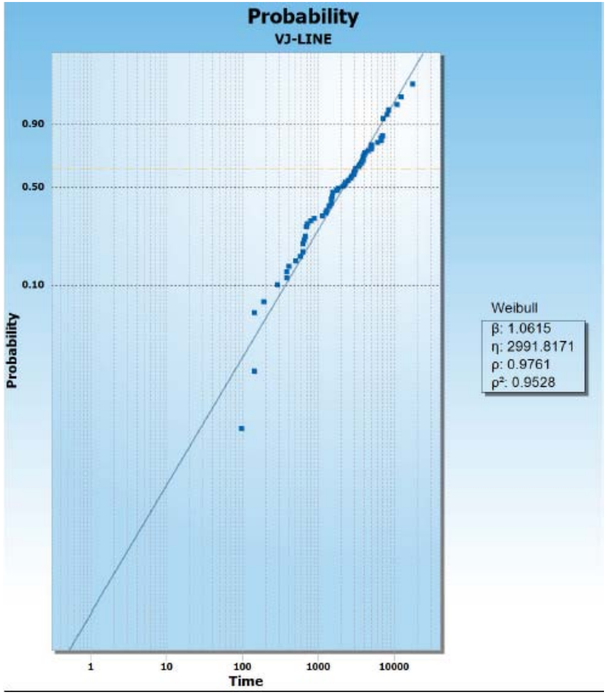


SAIC

# Probabilistic Risk Assessment (PRA)



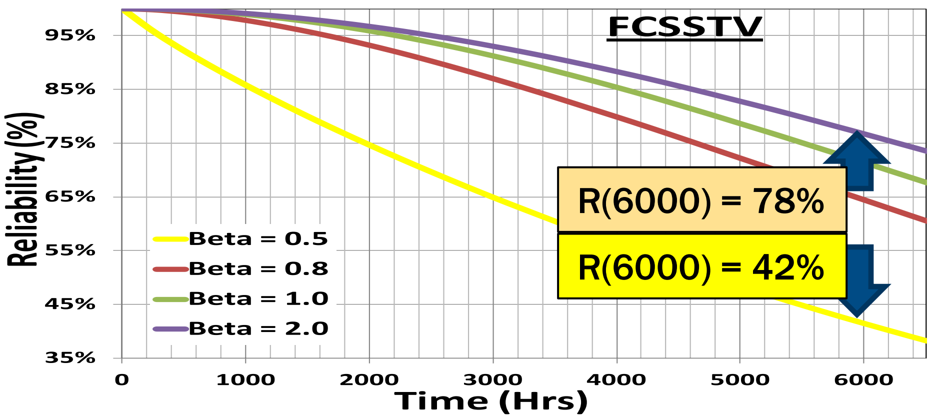
# Historical Component Failure Rate Determination




- **Using 442 PRACA records:**
  - Input into Weibull Analysis
  - Results:
    - It is in its useful life cycle, with random failures
    - β=1.0615
    - MTBF = 2991 hrs
  - Assumptions
    - Repair Time: 223 hrs
    - Inspection Time: 8 hrs
  - Maintainability
    - Maximum Availability = 87%
    - Inspection Time = 220 hrs

# Component Burn-in & Test Time Requirements

- RMA Analysis can determine product testing parameters
  - Reliability life testing can quantify reliability or safety goals
  - Burn-in test times can determine constant failure rates
  - Can determine acceptance test parameters
- The Weibull shape parameter (β) corresponds to the different failure modes for components
  - Infant mortality when β is less than 1
  - Random defects when β is equal to 1
  - Wear-out when β is greater than 1
- The results of system reliability analysis can be misleading if components are not properly up-screened (burned-in) or used under a certain bias condition where different failure modes may occur



# Why Have RMA Analysis in Design Process?

- RMA Analysis provides quantitative results, which can be used to justify component replacement, system upgrades, cost effectiveness of "abandon in place" concepts for systems, etc
- SAIC RMA process allows for verification and traceability of RMA requirements
- SAIC RMA Analysis encompasses entire design life cycle
  - *RBDA*
  - *FMEA*
  - *FTA*
  - *PRA*
- RMA Analysis can be used to optimize timeline and launch availability results
  - *Provide MTBF, failure distribution, MTTR, and repair probability to Ground System hardware and software*
- RMA Analysis can be used to optimize Logistics considerations
  - *Spare parts need*
  - *Logistic Facility space*
  - *Preventative Maintenance requirements*
  - *Maintenance Personnel Requirements*



SAIC®

# SAIC RMA Analysis Papers

- SAIC RMA Team Papers Published:
  - *"Allocating Reliability & Maintainability Goals to NASA Ground Systems,"* Reliability, Availability, and Maintainability Symposium (RAMS) 2013 Conference, Orlando, FL, 2013.
  - *"Determining Component Probability from Problem Report Data Used in Ground Systems for Manned Space Flight,"* Reliability, Availability, and Maintainability Symposium (RAMS) 2013 Conference, Orlando, FL, 2013.
  - *"On Component Reliability and System Reliability for Space Missions*," IEEE International Reliability Physics Symposium (IRPS) 2012, Anaheim, CA, 2012
  - *"Comparison Modeling of System Reliability for Future NASA Projects*," Reliability, Availability, and Maintainability Symposium (RAMS) 2012 Conference, Reno, NV, 2012.
  - *"Constellation Ground Systems Launch Availability Analysis: Enhancing Highly Reliable Launch Systems Design*," American Institute of Aeronautics and Astronautics (AIAA) 2010-2180, SpaceOps 2010 Conference, Huntsville, Alabama, 2010.



SAIC®

# Thank You

**Amanda M. Gillespie**, ASQ CRE, Solutions Architect

Logistics & Supply Chain Service Line

Tel: 312.758.6203 | Email: amanda.m.gillespie@saic.com

**Visit us at saic.com**

# Acronym & Abbreviation List

| | |
|---|---|
| $A_i$ | Inherent Availability |
| $A_o$ | Operational Availability |
| ASQ | American Society for Quality |
| CRE | Certified Reliability Engineer |
| CSA | Cut Set Analysis |
| CxP | Constellation Program |
| DoD | Department of Defense |
| FFBD | Functional Flow Block Diagram |
| FMEA | Failure Mode & Effects Analysis |
| FTA | Fault Tree Analysis |
| GSDO | Ground Systems Development and Operations |
| IMA | Importance Measure Analysis |
| KSC | Kennedy Space Center |

| | |
|---|---|
| KSC-NE | KSC Design Engineering |
| MPCV | Multi-Purpose Crewed Vehicle |
| MTBF | Mean Time Between Failures |
| MTTR | Mean Time to Repair |
| NASA | National Aeronautics and Space Administration |
| PLC | Programmable Logic Controller |
| PRA | Probabilistic Risk Assessment |
| PTC | Parametric Technology Corporation |
| R&M | Reliability & Maintainability |
| RAMS | Reliability and Maintainability Symposium |
| RBD | Reliability Block Diagram |
| RBDA | Reliability Block Diagram Analysis |
| RMA | Reliability, Maintainability, and Availability |

# Acronym & Abbreviation List

| | |
|---|---|
| SAIC | Science Applications International Corporation |
| SLS | Space Launch System |
| SSP | Space Shuttle Program |
| WQS | Windchill Quality Solutions |
| Wx | Weather |