"Pitfalls and Precautions when using Predicted Failure Data for Quantitative Analysis of Safety Risk in Human Rated Launch Vehicles

8th IAASS Conference
Safety First
Safety for All
Melbourne - FL
May 18-20, 2016

Glen (Spencer) Hatfield, Bastion Technologies Inc.
Frank Hark, Bastion Technologies Inc.
James Stott, PhD NASA

NASA Marshall Space Flight Center (MSFC)

Objective

To support risk-informed decision making by understanding the issues involved when assessing risk by:

- Correctly Assessing Risk
  - Identifying areas of concern in Design and Development of Complex Launch Vehicles
  - Improving accuracy of risk values in the decision making process
  - Providing justification for redesign of a system when risk is too great
- Validating Data Sources
  - Identify issues relative to predicted and demonstrated data sources
  - Evaluate the use of epistemic error factors for predicted data
  - Calculate error factors for demonstrated data
- Performing Comparison of Risk Model Results
  - Compare Predicted vs. Demonstrated data in risk models
  - Comparison of uncertainty utilizing epistemic values vs. calculated values
- Identify Pitfalls and Precautions of using predicted failure data vs. demonstrated data when making the decision to accept risk.

Model Parameters

- Model Development
  - Two models were developed for comparison utilizing the same components
  - Each model represents a theroetical circuit which requires a two of two output for circuit functionality to be achieved
  - Each of the models were run independantly in SAPHRE 8
  - Each model was then subjected to 50,000 Monte Carlo trials with identical seed values
  - Data Correlation for each type of component was performed in SAPHRE 8
  - Predicted failure data model uses data derived from MIL-HDBK-217F (point estimates)
  - Demonstrated failure data model uses data obtained from Quanterion Automated Databook version 4.2.1 (EPRD-2014) (mean values from data sets)
  - Calculation of risk and uncertainty for each model type
    - Predicted failure data uses epistemic uncertainty (Error Factor) values

Epistemic Data Source Classification Approach			
Source	Source Description	Source Application	Error Factor
New Hardware	MIL-HDBK-217F	Same Component	8
		Like Component	9

- Demonstrated data use the following formula for uncertainty (Error Factor)

$$EF = e^{1.645}\sqrt{\ln(1 + (\sigma_{ln}/\mu_{ln})^2)}$$

Predicted Component Models

- Component Models
  - MIL-HDBK-217F Model - uses stress method, Quality factors are those of the highest level for the specific part analyzed. Temperatures, where applicable, are baselined at 130 deg. C, stress loads, where applicable, are between 90 and 100%. Environment is Airborne Uninhabited Fighter (AUF). Example calculations are seen below.

CMOS Digital Gate Array $\lambda P = (C1\pi T + C2\pi E)\pi Q\ \pi L$		
C_1	0.02	101 to 1000 gates
π_T	1.1	130 deg. C
C_2	0.0096	Glass Seal DIP 24 pins
π_E	8	AUF
π_Q	0.25	Class S
π_L	1	Learn. Factor > 2 yrs
FPMH	0.0247	
FR/hr	**2.47E-08**	
MTTF	40,485,830	

Capacitor - CCR $\lambda p = \lambda b\ \pi T\ \pi C\ \pi V\ \pi SR\ \pi Q\ \pi E$		
λ_B	0.0099	CCR
π_T	35	130c
π_C	0.66	0.01µf
π_V	2	0.6
π_{SR}	1	N/A
π_Q	0.001	D
π_E	30	AUF
FPMH	0.0137214	
FR/Hr	**1.37E-08**	
MTTF	72,878,861	

All Components	Failure Rate	MTTF
Digital Gate Array	2.47e-8	40,485,830
Diode (LF)	4.25e-7	2,350,012
Transistor	3.53e-7	2,829,562
Resistors (RCR)	1.42e-7	7,058,767
Capacitors (CCR)	1.37e-8	72,878,861

Demonstrated Component Models

- Component Models
  - Demonstrated Model - This approach quantifies failure rates by using same components taken from the Quanterion Automated Databook using EPRD-2014, NPRD-2016, and where applicable FMD-2016. The same components used in the predicted model are selected where several years of failure data was found. Adjustments for varying environments were adjusted to the AUF environment by using MIL-HDBK-338 adjustment factors. The mean values and standard deviations were calculated. Error factors were then calculated for each component type. An example calculation is seen below.

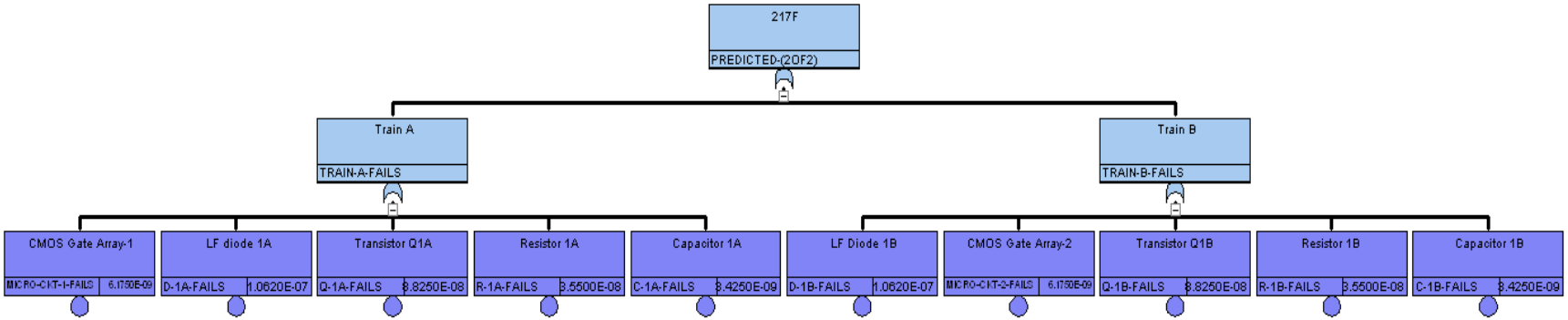
Micro Circuit (Digital Gate Array) Class S				
338 Conversions (AUC-AUF)				
FPMH	Failure Rate/Hr.	MTBF	MTBF Conversion	Converted Failure Rate/Hr.
1.87	1.87E-06	534759	320856	3.12E-06
1.73	1.73E-06	578035	346821	2.88E-06
1.57	1.57E-06	636943	382166	2.61E-06
1.44	1.44E-06	694444	416667	2.40E-06
1.56	1.56E-06	641026	384615	2.60E-06
1.66	1.66E-06	602410	361446	2.76E-06
1.83	1.83E-06	546448	327869	3.05E-06
1.88	1.88E-06	531915	319149	3.13E-06
1.99	1.99E-06	502513	301508	3.31E-06
2.04	2.04E-06	490196	294118	3.40E-06

MEAN	STD DEV	EF
2.93E-06	3.29E-07	4.61

Component Types	MEAN	STD DEV	EF
Digital Gate Array	2.93E-06	3.29E-07	4.61
Diodes	2.45E-06	1.44E-06	4.10
Transistor	9.38E-07	5.37E-07	4.09
Resistor	2.77E-06	2.52E-07	4.67
Capacitor	1.07E-06	1.14E-06	3.91

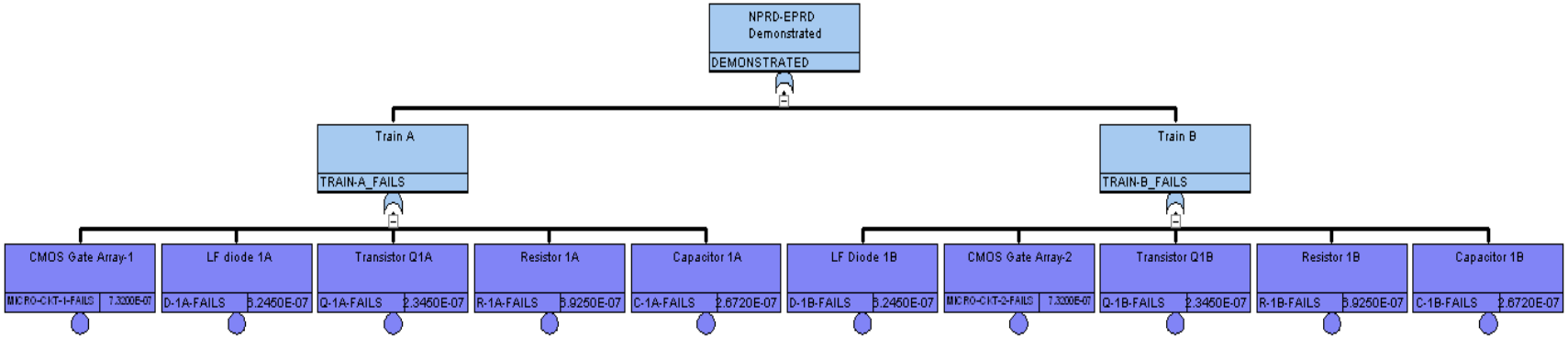
Predicted Circuit Model

- Predicted Circuit Model
  - Predicted Circuit Model - This approach quantifies the model by utilizing the MIL-HDBK-217F component calculations for each part as decribed in the component models slides. The fault tree was then constructed to represent a two of two scenario. Each of the models were set up the same and solved for a mission time of 15 minutes. Epistemic error factor of 8 was used in the model based on the values seen in the chart in slide3.



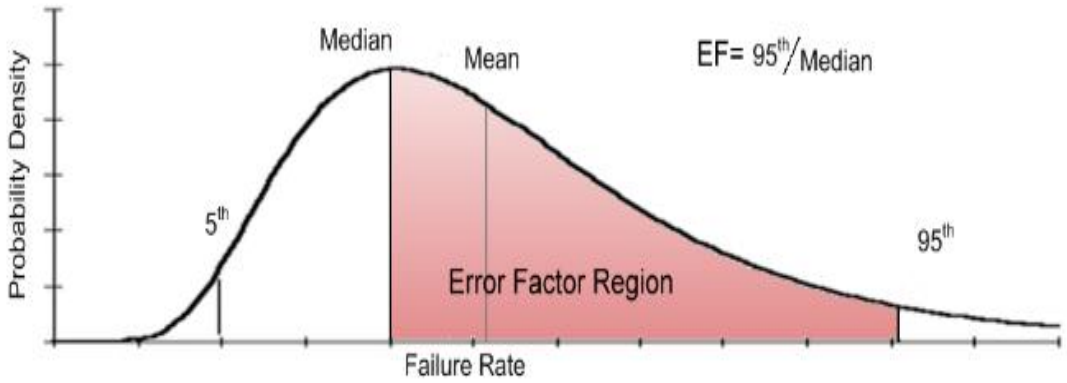
Demonstrated Circuit Model

- Demonstrated Circuit Model
  - Demonstrated Circuit Model - This approach quantifies failure rates by using same components taken from the Quanterion Automated Databook using EPRD-2014, NPRD-2016, and where applicable FMD-2016. The same components are used in the predicted model and were selected where several years of failure data was found. Adjustments for varying environments were made to adjust to the AUF environment by using MIL-HDBK-338 adjustment factors. The mean values and standard deviations were calculated. Error factors were then calculated for each component type.



System Uncertainty

- Uncertainty Types
  - Aleatory (Inherent characteristic of the system)
  - Epistemic (lack of knowledge)
- Parameter uncertainty is measured by the spread of the distribution, which can be expressed as the bounds (e.g. 5th and 95th percentiles) of the probability distribution
- Failure rates are often modeled by the lognormal distribution
  - Quantitatively, the error factor (EF) is a measure of the spread of uncertainty for the lognormal about the Median
  - EF = 95th/Median
  - System Uncertainties were modeled post processing by the method below



Lognormal Probability Density Function

Applicability of Data

- Newly designed Launch vehicles are comprised of heritage, Commercial Off the shelf, Modified Off the shelf, and newly designed components.
- Due to cost and time constraints many programs allow the use of predicted failure data in determining if requirements have been met.
  - Predicted data is often overly optimistic in the values calculated
  - Predicted data does not take into account manufacturing, assembly, installation and operational considerations, which are often the primary factors in determining the reliability of a component or circuit
  - Reliability models are often developed from data from multiple sources:
    - Component databases (NPRD, EPRD, NUCLARR, etc.)
    - Aerospace historical data
    - Other industry historical data
    - Piece part count or Stress method (MIL-HDBK-217F)
    - Engineering judgment

Results

- The table below demonstrates the difference between the predicted models mean values (i.e. risk) and the uncertainty about the distribution of each model type.
  - Predicted risk is 11 times less that that of the demonstrated
  - System uncertainty of the predicted is two times greater than that of the demonstrated systems uncertainty
  - Risk assessments may be inacurate
  - Aggregate risk may be greater than the actual risk due to a skewing of multiple risk sources
  - Reliability models may misrepresent the actual risk due to mixed failure data

Model Type	Risk (1/N)	System Uncertainty
Predicted	1/2,111,041	4.08
Demonstrated	1/196,657	2.3

- When assessing Risk one must take into consideration the factors which may be providing an inaccurate representation of the risk, which is now assumed due to incomplete data , mixed models, as well as overly optimistic failure data.
  - Risk assessments may be inacurate
  - Aggregate risk may be greater than the actual risk due to a skewing of multiple risk sources
  - Reliability models may misrepresent the actual risk due to mixed failure data

Conclusion

- Using predicted failure data may provide incorrect data, which may misrepresent the actual risk.
  - Data is overly optimistic
  - Data does not take into account manufacturing, assembly, quality processes, and operations
  - How applicable is the data
  - Applicability is a source of uncertainty
  - Epistemic Uncertainty is usually as uncertain as the predicted data
  - Data may mislead managers into accepting an unknown level of risk

- Using demonstrated failure data will provide a reasonable results and may be more representative of actual risk.
  - More time and effort are required to seek out and find applicable data
  - Environments must be evaluated and adjusted to the appropriate value
  - Equal quality of components must be used in assessing risk
  - Failure databases are difficult to find and validate
  - The source of data must be documented for traceability

Summary

- System design is constrained by Safety, Reliability, and Quality requirements as well as design standards. The purpose being to assure safety, which is generally related to quality of product, design, and testing.

- These bounds are where the risks lie, and must be fully recognized, understood, minimized, and eventually accepted or redesigned to a level, which then meets acceptable risk.

- The bounds over time become eroded by the acceptance of risk, and at some time, the aggregate risks may well exceed these bounds.

- This may result in a falsely perceived level of confidence, and allow a project to proceed to a state of potential disaster, which may result in a loss of life and physical property.

Questions?

POC: Glen (Spencer) Hatfield

Glen.S.Hatfield@nasa.gov

256-544-5874

Backup Charts

MIL-HDBK-217F Predictions

Resistors - RCR Fixed Composition ER λp=λbπT πP πS πQ πE		
λ_B	0.0017	RCR Fixed
π_T	7.6	130c (col1)
π_P	2.5	10W
π_S	3.4	0.9
π_Q	0.03	S
π_E	43	AUF
FPMH	0.1416678	
FR/Hr	**1.42E-07**	
MTTF	7,058,767	

Diodes (Low freq) λP= λB πT πS πC πQ πE		
λ_B	0.0034	GP analog
π_T	5.4	130C
π_S	0.77	.8<Vs<=.9
π_C	1	metal bond
π_Q	0.7	JANTXV
π_E	43	AUF
FPMH	0.42552972	
FR/Hr	**4.25E-07**	
MTTF	2,350,012	

Transistors LF, BIPOLAR λp=λb πT πA πR πS πQ πE		
λ_B	0.00074	NPN/PNP
π_T	6.3	130c
π_A	1.5	Linear Amp
π_R	2.3	10W
π_S	0.73	0.8<Vs≤0.9
π_Q	0.7	JANTXV
π_E	43	AUF
FPMH	0.353411535	
FR/Hr	**3.53E-07**	
MTTF	2,829,562	

Backup Charts (Contd.)

EPRD/NPRD Demonstrated

Diodes (Low Frequency) JANTXV					
MIL HDBK-338 Conversions (AUC-AUF)					
FPMH	Environment	Failure Rate/Hr.	MTBF	MTBF Conversion	Converted Failure Rate/Hr.
2.86	auf	2.86E-06	349650	349650	2.86E-06
2.6	auc	2.60E-06	384615	230769	4.33E-06
0.6	auc	6.00E-07	1666667	1000000	1.00E-06
1.8	auf	1.80E-06	555556	555556	1.80E-06

Mean	STD DEV	EF
2.49E-06	1.44E-06	4.10

Transistors (Bipolar) JANTXV					
MIL HDBK-338 Conversions (AIF-AUF)					
FPMH	Environment	Failure Rate/Hr.	MTBF	MTBF Conversion	Converted Failure Rate/Hr.
0.71	aif	7.10E-07	1408451	563380	1.77E-06
0.99	auf	9.90E-07	1010101	1010101	9.90E-07
0.87	auf	8.70E-07	1149425	1149425	8.70E-07
0.46	auc	4.60E-07	2173913	1304348	7.66E-07
0.29	auf	2.90E-07	3448276	3448276	2.90E-07

Mean	STD DEV	EF
9.38E-07	5.37E-07	4.09

Resistor (RCR) Class S					
MIL HDBK-338 Conversions (ARW-AUF)					
FPMH	Environment	Failure Rate/Hr.	MTBF	MTBF Conversion	Converted Failure Rate/Hr.
0.539	arw	5.39E-07	1855288	371058	2.6950E-06
0.531	arw	5.31E-07	1883239	376648	2.6550E-06
0.560	arw	5.60E-07	1785714	357143	2.8000E-06
0.527	arw	5.27E-07	1897533	379507	2.6350E-06
0.539	arw	5.39E-07	1855288	371058	2.6950E-06
0.581	arw	5.81E-07	1721170	344234	2.9050E-06
0.677	arw	6.77E-07	1477105	295421	3.3850E-06

Mean	STD DEV	EF
2.77E-06	2.52E-07	4.67

Capacitor CCR Class D					
MIL HDBK-338 Conversions (GB-AUF)					
FPMH	Environment	Failure Rate/Hr.	MTBF	MTBF Conversion	Converted Failure Rate/Hr.
0.109	auf	1.09E-07	9174312	9174312	1.0900E-07
2.41	auf	2.41E-06	414937.8	414938	2.4100E-06
0.164	gb	1.64E-07	6097561	609756	1.6400E-06
0.012	gb	1.20E-08	83333333	8333333	1.2000E-07

Mean	STD DEV	EF
1.07E-06	1.15E-06	3.91

Data Source Application Classification

Note: This table is intended to be used for point estimates that lack distribution data. Use the distribution for uncertainty if it is known

Source	Category	Source Descrption	Source Application	Source Application Error Factor
Legacy Hardware	A	Other Launch Vehicle Data (Most Applicable)	Same component	3
			Like component	4
	B	Aerospace Data	Same component	5
			Like component	6
	C	Other Industry Data	Same component	6
			Like component	7
New Hardware	D	MIL-HDBK-217F Methods	Same component	8
			Like component	9
	E	Non-expert Engineering Judgment (Least Applicable)	Documented Process	10
			Undocumented Process	15