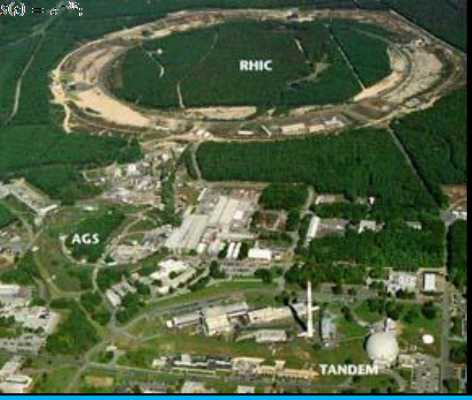


Quantitative fault tree analysis of the beam permit system elements of RHIC at BNL

Prachi Chitnis†, Kevin A. Brown‡, Thomas G. Robertazzi† and Charles Theisen‡
†Stony Brook University, NY, ‡Brookhaven National Laboratory, NY

Objective

To find hazard rates for adverse failures occurring in beam permit system modules

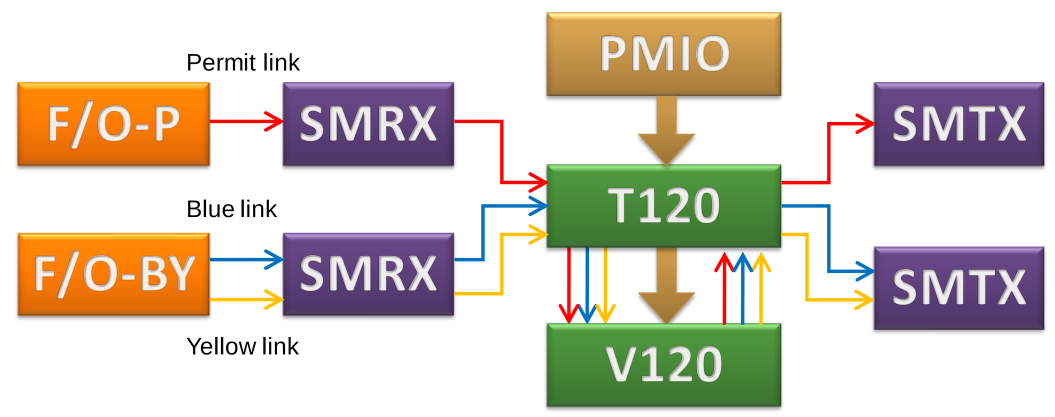
Introduction

- Beam permit system is a centralized safety system that ensures the equipment and personnel safety at all the times
- This work calculates the failure rate of adverse failures occurring in BPS modules
- Also provides a quantitative comparison of basic component failure rates and identifies the failure prone components

BPS modules

- BPS consists of 37 modules that can be put in two major categories: Permit Modules (PM) and Abort Kicker Modules (AKM)
- PM concentrates the health inputs from RHIC support systems and takes decision regarding system safety
- AKM upon seeing a failure, waits for the beam abort gap and sends dump signals to kicker magnets to dump the beams

Type of Modules	Number	Mode
PM: Master (PM:M)	1	FB,FQ,B
PM: Slave with Quench detection inputs (PM:SQ)	13	FB,FQ,B
PM: Slave with No Quench detection inputs (PM:SNQ)	18	FB,B
PM: Slave w/o any support system input (PM:S)	1	FB,B
Abort Kicker Module (AKM)	4	FB,B,DD



Permit module

Abort kicker module

- F/O-P, F/O-BY: Fiber optic cables with connectors
- SMRX/SMTX : Single mode fiber optic receiver / transmitter
- V120: Takes decision to drop carriers
- T120: Transition board for V120
- PMIO: Interface between support systems and PM
- V125: Synchronize dump signals with abort gap

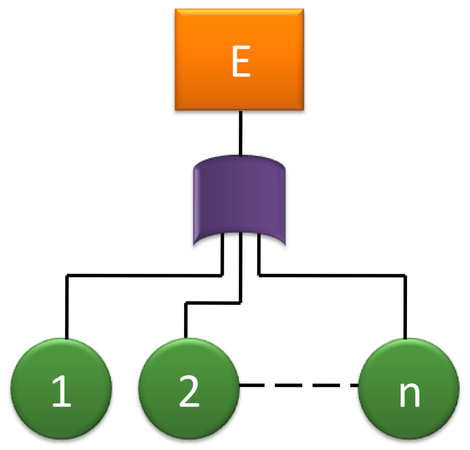
Fault tree analysis

Quantitative FTA

- Fault Tree Analysis[1] is a deductive approach that translates a physical system into a structured logic diagram and resolves an undesired event into its causes.
- The exponential distribution is used to model the lifetime of electronic components, and has a reliability function equal to:

$$S(t) = e^{-\lambda t}$$

Below is a Fault Tree[2] with a higher level event E resolved into n basic events, which are independent and exponentially distributed.



Represented as a series system, the reliability function of E:

$$S_E(t) = \prod_{i=1}^{n} S_i(t) = \prod_{i=1}^{n} e^{-\lambda_i t}$$

The failure rate function of E:

$$\lambda_E = \sum_{i=1}^{n} \lambda_i$$

No redundant components in system makes all the top level failure rates for modules as exponential.

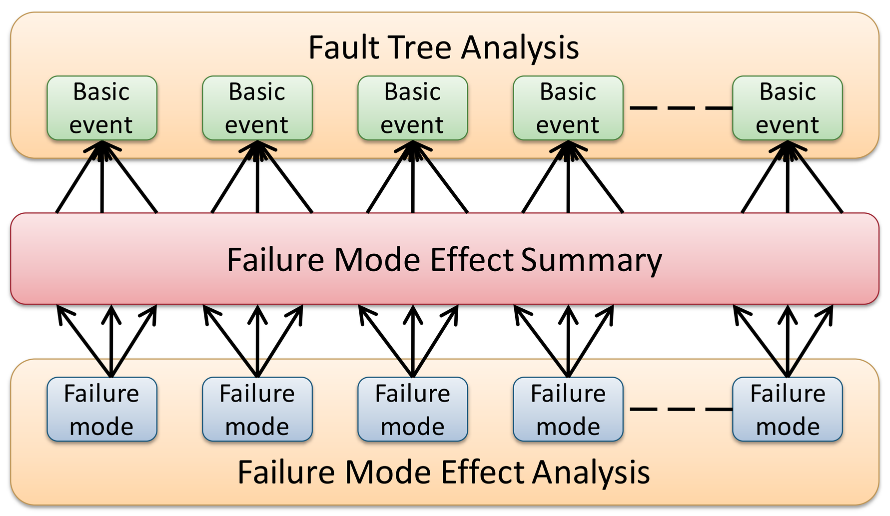
The analysis

The top failure modes of PM are:

FB	An input signal path fails within PM that terminates its permit carrier output
FQ	An input signal path fails within PM that terminates its permit, blue & yellow carrier outputs
B	PM ignores any input failure and maintains its carrier outputs

The top failure modes of AKM are:

FB	An input signal path fails within AKM that terminates its permit carrier output and generates beam dump signal
B	AKM sees the carrier failure but cannot generate the beam dump signal
DD	AKM cannot synchronize the dump signal with the abort gap, and beam is swept across the beam dump



The analysis (continued)

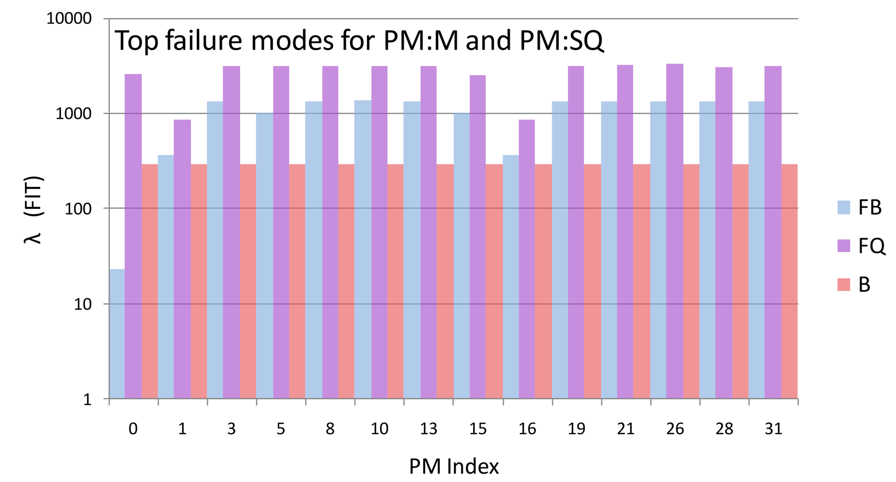
- Levels of hierarchy in tree represent stages of detail
- Number of levels depends on the constituent boards' complexity.
- At board level, the circuit is divided into signal paths relating inputs and outputs of a top level failure
- Failure rates are divided for common paths of failures

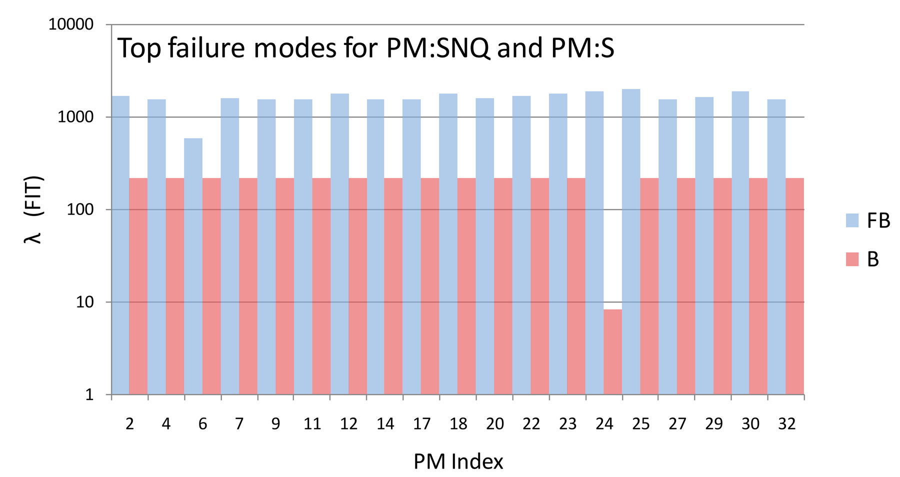
Component failure rate prediction: The exponential failure rates are obtained from manufacturer for newer components and from MIL-HDBK-217F[3] for older components. Environmental factor of G_b, amb-ient temperature of 30°C and a 60% confidence interval is used.

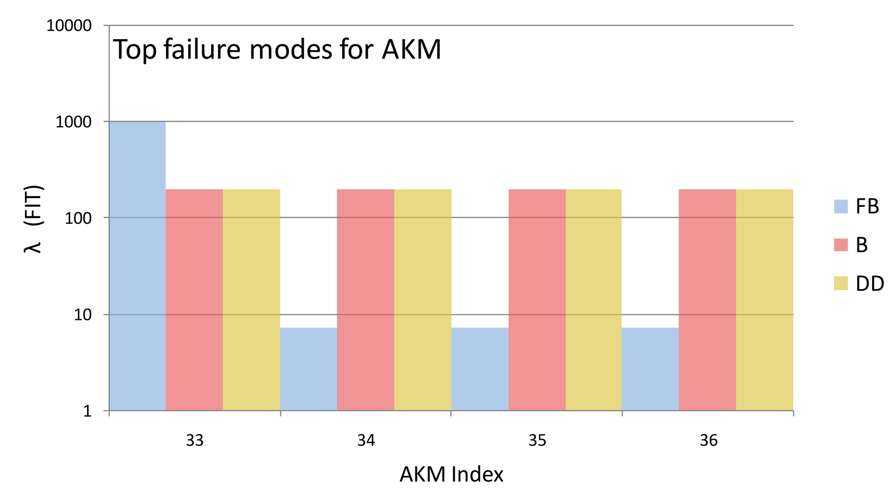
Component failure mode prediction: The failure rate is further divided into failure mode rates through apportionments given by FMD-97[4]. The normalized distribution data is used, which excludes non inherent failures.

Component contribution: A component common to all the signal paths will cause an FQ in PM:SQ and FB in PM:SNQ. Component is ignor-ed if: active at initialization or beam-abort, diagnostics, having zero failure rate, inactive in a variant. Failure mode is ignored if: unknown consequence, early life failure mode or parametric failure.

Results







Shown are the logarithmic bar charts for modules with y-axis showing calculated failure rates in FIT (Failure In Time) and x-axis showing the module indices.

Discussion

PM:M (0th) and PM:SQ

- λ_{FQ} and λ_{FB} are largely contributed by the fiber optic elements having failure rates of the order of 10^2 FIT.
- λ_{FQ} is highest: having optical elements for both blue and yellow link
- λ_{FB} is almost half of λ_{FQ}: having optical elements for permit link only
- λ_{FB} for PM:M is very low: absence of optical elements
- λ_B is an order less than other two, contributed by the optocoupler malfunction in V120 board

PM:SNQ and PM:S (24th)

- No FQ mode: no quench inputs or blue/yellow carriers
- λ_{FB} is higher than PM:SQ : fault in common circuits causes an FB rather than an FQ
- λ_B is slightly lower than PM:SQ: no quench inputs and correspon-ding elements

AKM

- λ_{FB} is very small for all modules except the 33rd : optical elements
- λ_B is almost equal to PM: largely contributed by oscillator malfunc-tion and power failures on-board
- λ_{DD} like λ_B: largely contributed by oscillator malfunction and power failures on-board

Conclusion

The MIL-HDBK-217F is fairly conservative in its approach which is suitable for safety analysis of components that are not supplied with data from manufacturer. The maximum values of λ_{FB}, λ_{FQ}, λ_B and λ_{DD} are 1987, 3332, 290 and 195 FIT. The corresponding MTTFs are 57, 34, 393 and 585 years. Due to multiple modules and their operation dynamics, a system failure can occur in RHIC operational life of 20 years. This evaluation is done through a Monte Carlo simulation of the BPS[5].

Acknowledgement

The authors would like to thank R. Schoenfeld and W. Jappe for doing rigorous tests to find the operating parameters of components on various boards.

References

1. W. Vesely, *Fault Tree Handbook with Aerospace Applications*, v1.1, NASA Publication, Aug. 2002
2. B.S. Dhillon et al., *Engineering Reliability - New Techniques and Applications*, 1981
3. MIL-HDBK-217F, *Military Handbook-Reliability Prediction of Electronic Equipment*, Department of Defense, 1995
4. FMD-97, *Failure Mode / Mechanism Distribution*, 1997, Reliability Analysis Center, Rome, NY
5. P. Chitnis et al., MOPPC075, these proceedings

Footnotes

- Work supported by Brookhaven Science Associates, LLC, under Contract Number DE-AC02-98CH10886 with the US Department of Energy
- Contact info: prachi.chitnis@stonybrook.edu