# QUANTITATIVE FAULT TREE ANALYSIS OF THE BEAM PERMIT SYSTEM ELEMENTS OF RELATIVISTIC HEAVY ION COLLIDER (RHIC) AT BNL*

P. Chitnis#, T.G. Robertazzi, Stony Brook University, Stony Brook, NY 11790, U.S.A.
K.A. Brown, C. Theisen, Brookhaven National Laboratory, Upton, NY 11973, U.S.A.

*Abstract*

The RHIC Beam Permit System (BPS) plays a key role in safeguarding against the anomalies developing in the collider during a run. The BPS collects RHIC subsystem statuses to allow the beam entry and its existence in the machine. The building blocks of BPS are Permit Module (PM) and Abort Kicker Module (AKM), which incorporate various electronic boards based on VME specification. This paper presents a quantitative Fault Tree Analysis (FTA) of the PM and AKM, yielding the failure rates of three top failures that are potential enough to cause a significant downtime of the machine. The FTA helps tracing down the top failure of the module to a component level failure (such as an IC or resistor). The fault trees are constructed for all module variants and are probabilistically evaluated using an analytical solution approach. The component failure rates are calculated using manufacturer datasheets and MIL-HDBK-217F. The apportionment of failure modes for components is calculated using FMD-97. The aim of this work is to understand the importance of individual components of the RHIC BPS regarding its reliable operation, and evaluate their impact on the operation of BPS.

## INTRODUCTION

The Beam Permit System [1] is a centralized safety system that inspects the conditions prevailing in RHIC support systems, and acts appropriately to bring the machine to a safe state. To ensure equipment and personnel safety at all the times, it is very important that the BPS is highly reliable. The aim of this analysis is to calculate the failure rate of adverse failures occurring in PM and AKM. The analysis also provides a quantitative comparison of basic component failure rates and identifies the failure prone components.

## BEAM PERMIT SYSTEM MODULES

The BPS consists of 37 modules that are dispersed around RHIC ring and are broadly divided in two categories. The first 33 of them are the PMs and the last 4 are AKMs. The PMs are connected to each other through three 10 MHz carrier links: the permit link, the blue link and the yellow link. The permit link passes the beam dump signal and the blue & yellow links pass the magnet power dump signal. The AKM only connects to the permit link. The PM concentrates health inputs from various local support systems and has in-built intelligence to take decisions regarding safety. The health of the connected support systems is reported to other modules by maintaining the carrier outputs. The health inputs are called Permit Inputs and Quench Inputs. Taken together with the carrier inputs from previous PM, any input signal failure will cause its carrier output to terminate. The carrier failure ultimately reaches the AKMs. The AKMs have the permit carrier input, but no health inputs from support systems. They however have the carrier output and the beam dump output. If AKMs see a carrier failure, they wait for the beam abort gap, and then synchronize their dump output signal with the gap. If they don't see the gap, the dump signal is sent asynchronously.

A support system fault kills the permit input and permit link. A magnet quench fault kills the quench input, permit link, blue link and yellow link.

### *Failure Modes*

The PM and AKM themselves can malfunction which can be potentially detrimental to RHIC. Three such catastrophic failures are analyzed in this paper. The PM can fail in three modes, namely a False Beam Abort (FB), a False Quench (FQ) and a Blind (B).

- 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 AKM can fail in three modes, namely a False Beam Abort (FB), a Blind (B) and a Dirty Dump (DD).

- 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.

Table 1 shows the BPS module variants with their allowed modes of failure.

### *Modules' Structure*

Figure 1 shows the general structure of a PM [2]. It consists of various boards as shown. The thin arrows are the carrier signals, the broad arrows being the permit & quench inputs. The F/O-P, F/O-BY are the fiber optic cables along with connectors, for permit, blue and yellow carriers. The SMRX / SMTX is a single mode fiber optic

*Work performed under Contract Number DE-AC02-98CH10886 with the auspices of the US Department of Energy

#prachi.chitnis@stonybrook.edu

ISBN 978-3-95450-139-7

Table 1: BPS Modules

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

receiver / transmitter board that converts optical to TTL / TTL to optical signals. At some locations, SMTX is replaced by MMTX which is a multimode transmitter board. The V120 is the backbone of the PM that houses the intelligence to take decision for dropping carriers. T120 is the transition board for V120. PMIO is the interface between support systems and the PM. The V120, T120 and PMIO configurations decide the PM variant.

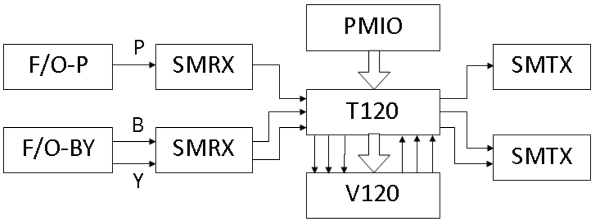

Figure 1: The permit module.

The module variants differ in minor functions and number of boards. The PM:M is the carrier signal generator. Slave modules just pass the carrier around. A PM:SQ has all the three carriers passing through. A PM:SNQ on the contrary just has the permit carrier passing through. Consequently PM:SNQ has only one set of the SMRX, SMTX boards and fiber cables. The PM:S does not have the PMIO board. Number of SMRX, SMTX and optical fibers depends on whether the carriers are passed through optical fibers or copper cables.

The AKM has only one board called V125. Upon seeing permit carrier failure, it waits for the abort gap and sends out the dump signals so that the beam is steered into the dump during the abort gap.

## CONCEPTUALIZATION

### *Fault Tree Analysis*

Fault Tree Analysis [3] [4] is a deductive method that aims at resolving an undesired event into its causes. It involves the translation of a physical system into a structured logic diagram, in which certain specified causes lead to one specified event of interest, called the TOP event. The TOP events are generally catastrophic system states that can result from sub-system faults. The event is then resolved into its immediate, necessary and sufficient causal events, and related by appropriate AND and OR logic. The process is followed until the elementary causes are identified. FTA exhaustively identifies causes of a failure and quantifies the failure probability and contributors. It is used to assess a proposed design for its reliability or safety.

### *Exponential Distribution*

The exponential distribution [5] plays a pivotal role in reliability and lifetime modelling because it is the only continuous distribution with constant failure rate and has a memory-less property. The intrinsic failure zone of the Bathtub curve [6] has a constant failure rate, and is often used to model the lifetime of electronic components that typically do not wear out until long after the expected life of the system. This zone signifies that a component that has not failed is as good as a new component. The effect of aging actually starts in the wear-out zone, which is far beyond the considered life of the system.

$f(t) = \lambda e^{-\lambda t}$; *failure probability density function*

$h(t) = \lambda$; *failure rate function*

$F(t) = 1 - e^{-\lambda t}$; *failure distribution function*

$S(t) = e^{-\lambda t}$; *reliability/survival function*

### *Quantitative FTA [7]*

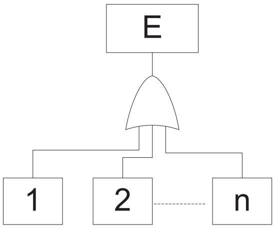

Figure 2: Fault tree example.

Figure 2 shows a fault tree with a higher event *E* resolved into *n* basic events, which are statistically independent and exponentially distributed. The OR gate logically represents a series system i.e. the output fails if any input fails. So the reliability function of *E* is:

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

And the failure rate of *E* is

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

Since there are no redundant components that have to fail at the same time to cause a higher-level failure, this analysis has fault trees that only contain OR gates. In this case, the TOP failure will be exponential if all individual component failures are exponential. Common cause failures [7] are not considered in this analysis thus making all the elementary failures statistically independent. They will be evaluated later in the project.

## FAULT TREE ANALYSIS

Fault trees have been constructed for the variants of PM and AKM for their earlier discussed failure modes of FB, FQ, B, and DD. These are the TOP failures. The levels of hierarchy in trees represent various stages of detail and the number of levels depends upon the constituent boards and their complexity. At the board level, the circuit is divided into signal paths through which particular inputs and outputs relate to a TOP failure. There are some paths which are common to multiple TOP failures. In such a case, the failure rates are divided among them. As all the trees are composed only of OR gates, the TOP failure rate is a summation of the involved basic component failure rates (see Eq. 1).

While FTA is very good at showing how resistant a system is to multiple initiating faults, it is not good at finding all possible initiating faults. To ensure this, a lowest level FMEA (Failure Mode and Effect Analysis) is performed. FMEA is an inductive approach in which individual failure modes of a component are considered, and possible progressions to a system level fault are identified. Here, a single level FMEA is done for all the board components, which defines the immediate consequence of each of their failure mode. This ensures that none of the failure mode of a component is left unexamined. An FMES (Failure Mode Effect Summary) is then prepared which serves as an interface between FTA and FMEA.

### *Component Failure Rate Prediction*

The exponential failure rates for basic component failures are obtained from various sources. The failure rates for the newer components are obtained from the manufacturer datasheets. For older components, MIL-HDBK-217F [8] is used. It is a military standard that provides failure rate data for many military and commercial electronic components. It is the most widely known and used reliability prediction handbook. The failure rate is calculated by using the “Part Stress Analysis” method which takes into account the actual operating conditions such as environment, temperature, voltage, current and applied power levels. An environmental factor of $G_b$ and an ambient temperature of 30°C are used throughout. For some of the fiber optic components, the SR-332 [9] is used. All the failure rates are calculated for a 60% confidence interval.

### *Component Failure Modes Prediction*

Quantification for the relative probability of occurrence for each potential failure mode for a component is essential to perform an FTA or FMEA. The FMD-97 [10] provides a cumulative compendium of failure mode data, which lists the apportionments of all tested failure modes. It can be used to apportion a component’s failure rate into its modal elements, by multiplying the failure rate to the given failure mode percentage. The normalized distribution data from FMD-97 is used here, which excludes the non-inherent failures like workmanship errors and externally induced errors. Failure mode apportionments for a few components were made available by the manufacturer. The usual failure modes for electronic components are open circuit, short circuit, leakage, functional failure, drift, cracks, voids etc. [10]

### *Component Contribution to FTA*

After preparing FMES, only those component failure modes are passed to FTA that contribute to TOP fail-ures. These components (or failure modes) are active for real-time BPS actions (decision to drop carriers). They can be broadly classified into logical devices, terminations, voltage regulation, drivers, receivers, buffers, isolators, PLLs, connectors etc.

Some components are common to all the carrier paths. A malfunction here will affect all the three carriers causing an FQ. If the common circuit is in PM:SNQ, then it will cause an FB. The component is ignored if it is: active only during initialization, active only after beam-abort, used for diagnostics (LEDs, testing ports), has a zero failure rate or inactive in a certain board variant. A failure mode is ignored if: it has an unknown consequence, is a early life failure mode or is a parametric failure.

## RESULTS

Figures 3, 4 and 5 show the logarithmic bar charts of TOP failure rates of PMs and AKM for their variants. The horizontal axis shows the location indices of modules in the ring. The vertical axis shows the failure rate expressed in terms of FIT [11] that is equal to the number of failures expected per billion device-hours of operation.

### *Discussion*

The failure rates for PM are shown for TOP failure modes as FB, FQ and B. In Fig. 3, the $0^{th}$ module is PM:M and all other are PM:SQ. False failures are failsafe conditions that impart downtime to restart the machine. The false failure rates $\lambda_{FQ}$ and $\lambda_{FB}$ are mainly contributed by the fiber optic elements like cables, connectors, receivers and transmitters, which have failure rates on the order of $10^2$ FITs. Among the three, the $\lambda_{FQ}$ is highest of all as it has fiber optic elements for two links, blue and yellow. Here the $\lambda_{FB}$ is approximately half of the $\lambda_{FQ}$ because it has fiber optic elements for permit link only. The $\lambda_{FB}$ for PM:M is very low as does not have any fiber optic elements connected. Blind failure is a fatal failure that can cause serious damage to equipment and personnel. The $\lambda_B$ is about an order of magnitude less than other two, and is essentially contributed by the optocoupler malfunction in V120 board. The optocouplers

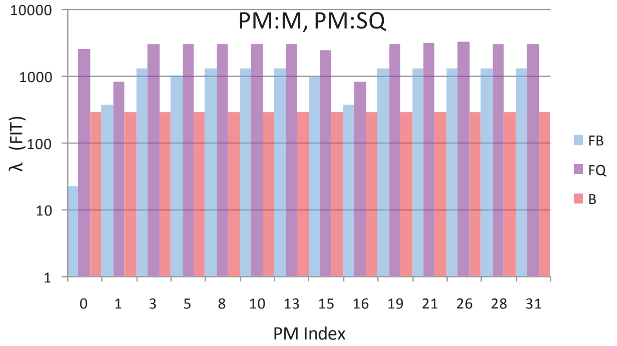

Figure 3: PM:M and PM:SQ.

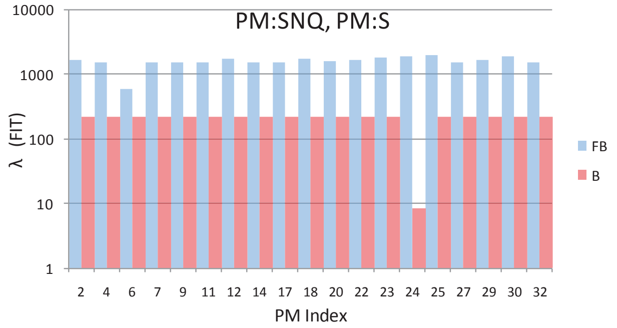

Figure 4: PM:SNQ and PM:S.

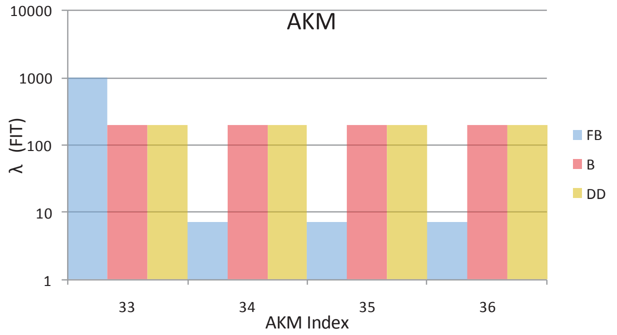

Figure 5: Abort kicker modules.

isolate the permit and quench input signals from power ground.

In Fig. 4, the 24th module is PM:S and all other are PM:SNQ. As seen, there is no FQ mode here because there are no quench inputs or blue/yellow carriers connected. The $\lambda_{FB}$ is higher than in Fig. 3 which represents that the fault in common circuits for carriers will cause an FB rather than an FQ. The $\lambda_B$ is slightly lower than that in Fig. 3, as quench inputs are absent and corresponding optocouplers are ignored for the analysis.

The failure rates for AKM are shown for TOP failure modes as FB, B and DD in Fig. 5. The $\lambda_{FB}$ is very small for all modules except the 33rd as it has fiber-optic elements connected. The $\lambda_B$ is almost equal to that of PMs, and is largely contributed by oscillator malfunction and power failures on-board. The $\lambda_{DD}$ is also similar to the $\lambda_B$, largely contributed by oscillator malfunction and power failures on-board. The DD failure increases the residual radiation in the machine somewhat, but is less critical than a false or blind failure.

## CONCLUSION

The MIL-HDBK-217F is fairly conservative in its approach as its failure rates are considerably higher than manufacturer supplied failure rates. The first priority is given to the manufacturer's data as it is up-to-date. For components not supplied with manufacturer's data, MIL-HDBK approach is beneficial from a safety analysis point of view.

This work elucidates the impact of individual component reliability on the reliability of the entire module. The maximum values of $\lambda_{FB}$, $\lambda_{FQ}$, $\lambda_B$ and $\lambda_{DD}$ are 1987, 3332, 290 and 195 FITs. The corresponding MTTFs are 57, 34, 393 and 585 years. On an individual basis, these values are substantially greater than the 20 years life of RHIC. But due to multiple modules and their operation dynamics, a system failure can occur within the 20 years range. This evaluation is done through a Monte Carlo simulation of the BPS [12]. The $\lambda_{FB}$, $\lambda_{FQ}$ and $\lambda_B$ for the PMs and the $\lambda_{FB}$, $\lambda_B$ and $\lambda_{DD}$ for AKM calculated here are used as the inputs for the simulation. An overall impact of these numbers on the BPS performance is evaluated there.

## REFERENCES

[1] C.R. Conkling, "RHIC Beam Permit and Quench Detection Communication System", PAC 1997.

[2] RHIC Electrical Drawings, *Internal Documentation,* Brookhaven National Laboratory, NY.

[3] W.S. Lee et al., "Fault Tree Analysis, Methods and Applications – A Review", IEEE transactions on Reliability, Vol. R-34, No. 3, 1985.

[4] W. Vesely, *Fault Tree Handbook with Aerospace Applications*, v1.1, NASA Publication, Aug. 2002.

[5] L. M. Leemis, *Reliability, Probabilistic Models and Statistical Methods*, 2nd ed., 2009, Pg. 96-104.

[6] Minitab Technical Support Document, *Distribution Models for Reliability Data*, Knowledgebase ID 2716.

[7] B.S. Dhillon et al., *Engineering Reliability - New Techniques and Applications*, 1981.

[8] MIL-HDBK-217F, *Military Handbook-Reliability Prediction of Electronic Equipment*, Department of Defense, 1995.

[9] Telcordia SR-332, *Reliability Prediction Procedure for Electronic Equipment*, Issue 1, 2001.

[10] FMD-97, *Failure Mode / Mechanism Distribution*, 1997, Reliability Analysis Center, Rome, NY.

[11] JESD85, *JEDEC Standard - Methods for Calculating Failure Rates in Units of FITS*, JEDEC Solid State Technology Association, July 2001.

[12] P. Chitnis et al., MOPPC075, ICALEPCS 2013.