A Monte Carlo simulation approach to the reliability modeling of the beam permit system 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
Brookhaven National Laboratory, Upton, NY 11973, U.S.A.

Collider-Accelerator Department
Brookhaven National Laboratory

U.S. Department of Energy
DOE Office of Science

DISCLAIMER

A MONTE CARLO SIMULATION APPROACH TO THE RELIABILITY MODELING OF THE BEAM PERMIT SYSTEM 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, Brookhaven National Laboratory, Upton, NY 11973, U.S.A.

Abstract

The RHIC Beam Permit System (BPS) monitors the health of RHIC subsystems and takes active decisions regarding beam-abort and magnet power dump, upon a subsystem fault. The reliability of BPS directly impacts the RHIC downtime, and hence its availability. This work assesses the probability of BPS failures that could lead to substantial downtime. A fail-safe condition imparts downtime to restart the machine, while a failure to respond to an actual fault can cause potential machine damage and impose significant downtime. This paper illustrates a modular multistate reliability model of the BPS, with modules having exponential lifetime distributions. The model is based on the Competing Risks Theory with Crude Lifetimes, where multiple failure modes compete against each other to cause a final failure, and simultaneously influence each other. It is also dynamic in nature as the number of modules varies based on the fault trigger location. The model is implemented as a Monte Carlo simulation in Java, and analytically validated. The eRHIC BPS will be an extension of RHIC BPS. This analysis will facilitate building a knowledge base rendering intelligent decision support for eRHIC BPS design.

INTRODUCTION

The peak energy stored in RHIC (Relativistic Heavy Ion Collider at BNL) in the form of beams and magnet current is about 72 MJ [1]. BPS is an important element of the machine protection system and consistently observes the health of RHIC support systems like power supplies, cryogenics, beam loss monitors, access controls, quench detection, vacuum etc. Upon sensing an anomaly, it is responsible for taking action for the safe disposal of this energy [2].

The BPS protects equipment and personnel from dangerous fault consequences. The reliability of BPS thus directly impacts the reliability of RHIC. Hence, there is an inherent need for high reliability of a safety critical system like BPS. The aim of this work is to calculate the probability of dangerous failures, which can lead to significant downtime of the collider.

RHIC BEAM PERMIT SYSTEM

The basic unit of BPS is a Permit Module (PM). There are 33 PMs located around the ring at equipment locations. They are connected by three fiberoptic links

called the Permit Carrier Link, Blue Carrier Link and Yellow Carrier link. These links carry 10 MHz signals whose presence allows the beam in the ring. Support systems report their status to BPS through "Input triggers" called Permit Inputs (PI) and Quench Inputs (QI). If any support system PI fails, the permit carrier terminates, initiating a beam dump. If QI fails, then the blue and yellow carriers also terminate, initiating magnet power dump in blue and yellow ring magnets. The carrier failure propagates around the ring to inform other PMs about the occurrence of a fault.

Other than PMs, BPS also has 4 Abort Kicker Modules (AKM) that see the permit carrier failure and send the beam dump signals to Beam Abort System. The magnet dump is initiated by terminating the power supply interlocks at individual PM location. The table shows the variants of the modules in BPS.

Table 1: BPS Modules

Modules	Number
Permit Module: Master (PM:M)	1
Permit Module: Slave with Quench detection inputs (PM:SQ)	13
Permit Module: Slave with No Quench detection inputs (PM:SNQ)	18
Permit Module: Slave without any support system input (PM:S)	1
Abort Kicker Module (AKM)	4

RELIABILITY THEORY

Reliability [3] is the probability that a system will perform a required function under stated conditions for a specified period of time. The variable of interest is the system lifetime, which depends upon its components' lifetimes. The lifetimes are related to the Hazard Rate/Failure Rate, which represents number of failures per unit time. The Bathtub curve [4] is generally used to model the lifetimes. The intrinsic failure period has a constant hazard function, which is used to model lifetimes of electronic components [5] that have a relatively longer intrinsic failure period. The constant hazard rate period has an exponential failure probability distribution function and has a peculiar property of being memory-less. It implies that a used item that is functioning has the same failure distribution as a new item. The effect of

aging starts in the wear-out period, which is far from the expected life of the system.

Figure 1 shows the failure probability density function f(t), the cumulative failure distribution function F(t), the Survival function S(t) and the hazard function h(t) which is equal to a constant λ. All the BPS module lifetimes are found to be exponentially distributed [6].
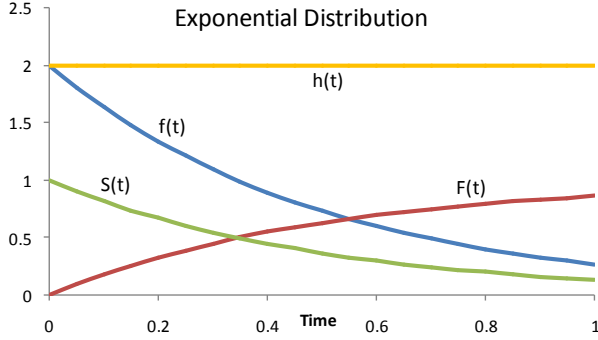

Figure 1: Exponential distribution for λ = 2

$$f(t) = \lambda e^{-\lambda t}, \qquad h(t) = \lambda$$
$$F(t) = 1 - e^{-\lambda t}, \quad S(t) = e^{-\lambda t}$$

Failure Modes

The state of BPS at any given time depends upon the state of its components i.e. PMs and AKMs. The PM can fail in three states namely a False Beam Abort (FB), a False Quench (FQ) and a Blind (B), which have three independent failure rates as λ_{FB}, λ_{FQ} and λ_B. The AKM can fail in three states namely a False Beam Abort (FB), Blind (B) and Dirty Dump (DD), which have three independent failure rates as λ_{FB}, λ_B and λ_{DD}. Detailed description of these modes is found here [6].

Figure 2 shows the Markov state diagrams [7] for PM, AKM and input triggers. The input triggers PI and QI are modeled as Poisson variable. Their time of arrival is also exponentially distributed.
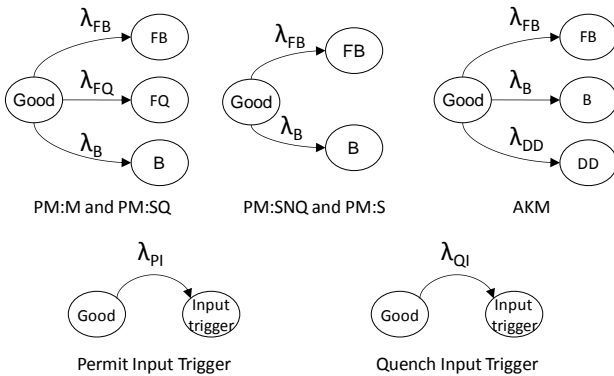

Figure 2: Markov diagrams for BPS modules

Depending on above module states, the BPS can have the following system states in whole:

- **System No Dump:** No trigger arrives that demands the action of BPS
- **System Good Dump:** Input trigger arrives at a module, and causes a beam dump and/or magnet power dump.
- **System False Beam Abort Failure:** False trigger generated within a module causes the beam dump.
- **System False Quench Failure:** False trigger generated within a module causes beam dump and magnet power dump.
- **System Blind Failure:** Any trigger is blocked in its way, which results in ignored beam dump (and magnet power dump).
- **System Dirty Dump Failure:** Input trigger arrives at a module and causes a beam dump and/or magnet power dump, but signal is not synchronized with the abort gap and sweeps the beam across the dump.

Significant downtimes are imposed by the System False and System Blind failures. The false failure is a fail-safe condition that furnishes a downtime to power-up and re-initialize BPS, power supplies, beam abort system etc. The blind failure represents a failure to respond to an emergency. It is in fact far more dangerous than the false failure as it can actually cause damage to the RHIC sub-systems, inflicting downtime of several months. The System Dirty Dump increases the radiation levels inside the machine. All these failures affect the reliability and availability of RHIC.

Competing Risks with Crude Lifetimes

In Competing Risks theory [8], several causes of failure or risks compete for the lifetime of an item. The observed outcome comprises *T*, the time of failure and *C*, the mode of failure. Thus the basic probability framework here is a Bivariate Distribution, where *T* is a continuous random variable and *C* is a discrete random variable. Here *T* can assume continuous values between *[0, ∞)* and *C* assumes discrete values as *{1, 2... k}*

While considering Crude Lifetimes, each risk is viewed in the presence of all other risks. The lifetimes are analyzed as if all risks are simultaneously acting on the item under examination. A Net Lifetime approach has been previously used [9] for Monte Carlo simulation where all the risks are viewed individually.

The BPS modules are subjected to *j = {1, 2... k}* risks. The hazard rate for *j*th risk if viewed individually is λ_j. *T* is the time of failure and *t* is the time of observation. The crude probability distribution function of risk *j* is given by

$$F_j(t) = P[0 < Tj < t, Tj < Ti \ \forall \ i \neq j | T > 0]$$

For exponentially distributed *T*:

$$F_j(t) = \frac{\lambda_j}{\sum_i^k \lambda_i} \left(1 - e^{-(\sum_i^k \lambda_i)t} \right); j = 1, 2.., k$$

(1)

The probability of failure from risk j is given by

$$\pi_j = \lim_{t \to \infty} F_j(t) = \frac{\lambda_j}{\sum_i^k \lambda_i} \; ;$$

$$\sum_j^k \pi_j = 1$$

The overall survival function $S_T(t)$ is the probability distribution of survival from all the k risks given by

$$S_T(t) = e^{-(\sum_i^k \lambda_i)t}$$

For permit modules, j is {FB, FQ, B} for PM:M and PM:SQ, and is {FB, B} for PM:SNQ and PM:S. For abort kicker modules j is {FB, B, DD}. For input triggers, $F_j(t)$ can be viewed as probability of trigger arrival with j equal to {PI} for permit input trigger and equal to {QI} for quench input trigger.

BPS MODEL

A Monte Carlo simulation has been implemented to calculate the probabilities of occurrence of system states as described earlier. As opposed to the circular configuration BPS, the Monte Carlo model is cut-out to a linear configuration, starting from the PM:M to the last AKM. There are two types of states of a module: active and passive. The "false" and "input arrival" are active states that upon inception propagate carrier failure in BPS, and are considered as triggers. The "good" and "blind" states are passive states, which do not propagate any carrier failure, and the module waits in that state.

Smirnov Transform

A two-dimensional random variable has to be generated for simulating a bivariate distribution of T. Smirnov transform [10] states that if U_1 is a uniformly distributed random number, and T has a cumulative distribution function F, then the random variable $F^{-1}(U_1)$ also has a cumulative distribution function equal to F. Thus T can be generated as $T = F^{-1}(U_1)$ by using computer generated pseudo-random number. From Eq. 1, the continuous random variable T of the bivariate distribution is

$$T = \frac{-1}{\sum_j^k \lambda_j} \; ln\, U_1 \qquad (2)$$

The discrete random variable C that represents the cause of failure due to risk j, is generated by using the following equation with another pseudo-random number U_2

$$C = \begin{cases} 1, & 0 \le U_2 \le \pi_1 \\ 2, & \pi_1 < U_2 \le \pi_1 + \pi_2 \\ ... \\ k, & \pi_1 + .. \pi_{k-1} < U_2 \le 1 \end{cases} \qquad (3)$$

Eq. 2 and Eq. 3 together generate the bivariate distribution of module lifetime.

Simulation Flow

The simulation has individual competing risks models for all the BPS modules. Each iteration starts with generating exponentially distributed random lifetimes per Eq. 2 and Eq. 3, and the time and mode of failure for each module are recorded. The maximum observation time of simulation is 6 hrs, equal to the average store length of RHIC. Thus, all times of failure larger than this are rejected. The arrival of the first trigger (either an input or false) freezes the system state, and BPS operation is emulated to find the overall system state. The iterations are repeated until the failure probabilities are constant upto 4 decimal places. The system state is reset after every iteration.

The model is dynamic in nature, i.e., the number of components varies according to the location of trigger. The components before the trigger location are removed from the model.

The simulation is started with the assumption that the system is initialized and beam is established. The simulation stops at the arrival of a trigger. The values of λ for different modules are calculated by Fault Tree Analysis [6]. The input trigger rates are calculated from the RHIC historical operational data.

Special Cases

There can be some special cases where the simulation has to be designed specifically to address those issues. For instance, the PM:SNQs do not have the blue and yellow links connected to them. Thus if there is a PM:SNQ between two PM:SQs, two paths exist between the PM:SQs. One is through the permit link & PM:SNQ, another one through the blue and yellow link. If this PM:SNQ goes blind, the carrier failure is still propagated through the blue & yellow links.

In another case, one module can attain only one failure state. After acquiring a state, transition to other state is not possible. However, there can be multiple failed modules in the system at any given time. The false failure propagation can be hindered by a module sitting in blind state. This case is counted in system blind failure. More than one trigger can occur at an instant. In such case, the trigger nearest to the AKMs is considered. There can be blind modules in the system, but the run ends without the arrival of a trigger. This case is counted in no dumps.

Furthermore, consider next two cases. First: due to multiple blind AKMs, only one of the blue or yellow beams is aborted. This case is called a partial dump. Second: power supply interlock failure mode of PM, where the beam is maintained but magnet power is

dumped. These two cases eventually result in false failures due to beam loss. For now, they are counted in false failure but will be evaluated separately later.

RESULTS

Figure 3 shows the pie chart for the probability of BPS operational scenarios expressed as a percentage of total dumps. As seen, a very small percentage of total failures occur in the system. The failures are further expanded in the second pie to show their relative sizes.

Discussion

On an average, the beam operation per year is 165.6 days, calculated from historical data. In the model, each run lasts for an average of 3.5 hrs. This gives the number of runs per year as 1135. According to the pie chart, the
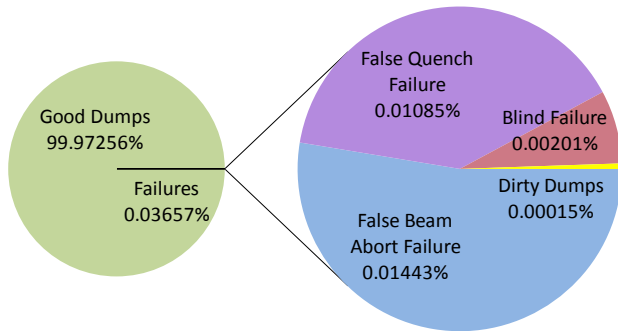

Figure 3: Probability of BPS operational scenarios

MTTF of false beam abort failure, false quench failure, blind failure and dirty dump are 7.2, 9.5, 51.2 and 672 years respectively. The 20-year operational life of RHIC is quite lower than the blind failure MTTF, and so is the risk of a fatal failure. The false failure numbers here are acceptable, as they are failsafe and impose downtime to restart the machine. It is to be noted that the system failures calculated here are induced only due to BPS failures. There might be other segments of RHIC that can cause a False or Blind failure.

The size of the pie sectors for failures depends on the magnitude of failure rates as well as the number of modules generating that failure. As seen here [6], the λ_{FQ} is generally much higher than the λ_{FB}, but due to large number of modules generating FB than FQ, the sector for false beam abort failure is bigger than false quench failure.

An analytical model is also developed for BPS, which evaluates the probabilities of the system failure mathematically. The analytical model description is beyond the scope of this paper.

During a quench triggering scenario, all the three carriers have to be dropped down. As discussed in one of the special cases, if PM:SNQ residing between two PM:SQs goes blind, there still exists a path that can propagate the failure. Due to this alternate path, the PM:SNQ is bypassed. However, if PM:SQ is blind, the

propagation of carrier failure is definitely hindered. Thus, the SQs have a higher structural importance than the SNQs. The analytical model quantifies the structural importance of individual modules.

CONCLUSION

The analysis yields the probabilities of dangerous failures that exist in the system. There is an upcoming extension of RHIC, called eRHIC (e stands for electron) [11], which will have an additional electron ring. Thus, RHIC BPS will be an integral part of the eRHIC BPS. Also, a new BPS section for the electron ring will be designed. This work formulates the possibilities of dangerous failures that adversely affect the machine downtime, based on the current design of BPS. It also illustrates the impact of BPS design aspects like module reliability and their organization on the system reliability. This will help rendering intelligent decision support towards recommendation for eRHIC BPS design [12].

REFERENCES

[1] Lessons Learned: Proactive Review of Large Hadron Collider (LHC) Magnet Over-Pressurization Event Leads to Improved Safety at BNL (SBMS) Dec 14, 2009.

[2] C.R. Conkling, "RHIC Beam Permit and Quench Detection Communication System", Proceedings of the Particle Accelerator Conference, 1997

[3] L. M. Leemis, *Reliability, Probabilistic Models and Statistical Methods*, 2nd edition, 2009

[4] R. Billington et al., *Reliability Evaluation of Engineering Systems*, 2nd ed., 1992

[5] Minitab Technical Support Document, Distribution Models for Reliability Data, Knowledgebase ID 2716

[6] P. Chitnis et al., MOPPC076, these proceedings

[7] T.G. Robertazzi, *Computer Networks and Systems: Queueing Theory and Performance Evaluation*, 3rd edition, 2000

[8] M.J. Crowder, *Classical Competing Risks*, 2001

[9] S. Wagner, "LHC Machine Protection System: Method for Balancing Machine Safety and Beam Availability", CERN-THESIS-2010-215

[10] http://www.princeton.edu/~achaney/tmve/ wiki100k/docs/Inverse_transform_sampling.html

[11] K.A. Brown et al., MOMIB03, these proceedings

[12] K.A. Brown et al., TUCOCA03, these proceedings