



BNL-82320-2009-CP

***Designing and Running for High Accelerator
Availability***

F. Willeke

Brookhaven National Laboratory, Upton, NY 11973-5000, USA

*Presented at the PAC09 Conference
Vancouver, Canada*

May 4 – 8, 2009

National Synchrotron Light Source II Project

Brookhaven National Laboratory

P.O. Box 5000
Upton, NY 11973-5000
www.bnl.gov

Notice: This manuscript has been authored by employees of Brookhaven Science Associates, LLC under Contract No. DE-AC02-98CH10886 with the U.S. Department of Energy. The publisher by accepting the manuscript for publication acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.

This preprint is intended for publication in a journal or proceedings. Since changes may be made before publication, it may not be cited or reproduced without the author's permission.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Designing and Running for High Accelerator Availability

F. Willeke, Brookhaven National Laboratory, Upton, 11973, NY, USA

Abstract

The report provides an overview and examples of high availability design considerations and operational aspects making references to some of the available methods to assess and improve on accelerator reliability.

INTRODUCTION

When the HERA electron-positron collider was proposed in 1981 [1], no goal for integrated luminosity was specified and high availability was not addressed. Like other accelerators for high energy physics it was designed and optimized for larger cm-energy for an affordable price thereby compromising operational efficiency. Efficient data collection over long periods was a secondary concern. When new frontiers in beam energy could not be reached easily, particle factories with large luminosity for precision measurements were proposed. Integrated luminosity and efficient operating then became a much more important issue. At the same time, dedicated synchrotron light sources were built. Their large and diverse user community consist of small research teams each of which occupies only one of many beam lines for a small fraction of the run time. Beam time needs to be scheduled well in advance and the multitude of users leaves little flexibility for change of plans. Thus very reliable and predictable accelerator operation is required. Accelerators are also increasingly frequently used for medical therapy which imposes a new level of availability and reliability requirements. The attention paid to reliability and availability issues of accelerator has increased ever since which is underlined by the fact that a first international workshop on accelerator reliability and availability [2] was held in 2001 which was followed by a 2nd workshop in January 2009 at Vancouver [3].

The operational efficiency of accelerators is usually low after start-up and the failure rate is large. The reasons are imperfections in manufacturing, inexperience in operations, and recoverable design flaws. An important factor to minimize this burn-in is thus quality assurance and control during system design and manufacture. After some time the failure rate stabilizes and settles to nearly constant values. When the system components will reach the end of their life cycle, failure rates will increase which will accelerate until the system is non-functional. Regular maintenance, good monitoring and a strategy to replace components and modernize and refurbish the system are the important factors of this part of the life cycle.

The issues of the early and late parts of the accelerator lifecycle are diverse and interesting and deserve to be discussed comprehensively. This report, however, will concentrate on issues that govern the center part of the

lifecycle which exhibits a flat failure rate. Two aspects of operational efficiency will be distinguished: the influence of design choices and the way the system is operated.

AVAILABILITY MODELING

High operational efficiency of accelerators requires continuous improvement. Modelling assists the improvement cycle of failure analysis, proposing improvements, and predicting improved performance before implementation. Basic definitions and relationships will be developed below.

A simple model considers failures as statistical events occurring independently of other failures and of failure history. While this model is imperfect, conventional wisdom is that it can provide results to understand and predict real failures in real technical systems. Prediction of absolute reliability might suffer from the principal shortcomings, but statistical modelling is helpful to compare alternative designs and competing operational strategies. In this sense, modelling is used for a quantitative analysis of observed performance and the results can be extrapolated for new or improved systems. In particular modelling is expected to provide information on critical subsystems and vulnerabilities.

The mean time between failures, MTBF refers to systems which continue to function after repair (non-repairable systems are characterized by a mean time to failure, MTTF). The mean time to repair (MTTR) includes the time needed for trouble shooting, to provide access to the faulty element, for actual repair, and to re-establish stable operation.

Accelerators are composed of subsystems with identical components. The rate of failure $\lambda(t)$ is the probability of failure of a component per unit time. It is closely connected to the MTBF and related properties such as the probability for surviving a certain time t , $S(t)$ and the probability for failure within that time, $F(t)$ via the failure probability density function $f(t)$. The probability $p = \lambda \cdot \Delta t$ ($0 < p < 1$) that a component fails within any small interval of time Δt is assumed independent from possible failures at other times. For constant λ , the probability for failure at a certain time $t = n\Delta t$ is $f_n = (1-p)^{n-1}p$. Then the MTBF, the expectation value of the time until a failure occurs, is $\sum_n((n\Delta t)(1-\lambda\Delta t)^{n-1}(\lambda\Delta t)) = \lambda^{-1}$. For a system with N identical components, each of them having a probability of p to fail within Δt , the most likely number of failures within Δt is $P_{n,N} = \sum_n(n \cdot c_{Nn} \cdot (1-p)^{N-n} \cdot p^n) = N \cdot p$ (c_{Nn}

*Work supported by DOE contract DE-AC02-98CH10886

binomial coefficient) so that the system MTBF is

$$MTBF = (N\lambda)^{-1}. \quad (1)$$

The consequence of this simple expression is that the reliability of the components must scale linearly with the system size in order to maintain operational efficiency. In general, the failure rate cannot be assumed constant. The probability per unit time that the system survives for $n-1$ time intervals of length Δt and fails in the n -th one is

$$f_n = \prod_{i=1}^{n-1} (1 - \lambda_i \cdot \Delta t) \cdot \lambda_n = \lambda_n \cdot \exp\left(\sum_{i=1}^{n-1} (1 - \lambda_i \cdot \Delta t)\right) \quad (2)$$

which, in the limit of infinitesimally small Δt becomes the continuous probability density function $f(t)$

$$f(t) = \lambda(t) \cdot \exp\left(-\int_0^t d\tau \cdot \lambda(\tau)\right). \quad (3)$$

The probability for failure within a time t is called failure function

$$F(t) = \int_0^t f(\tau) \cdot d\tau = 1 - \exp\left(-\int_0^t d\tau \cdot \lambda(\tau)\right) \quad (4)$$

and its complement is the survival function given by

$$S(t) = 1 - F(t) = \exp\left(-\int_0^t d\tau \cdot \lambda(\tau)\right). \quad (5)$$

The more general expression for MTBF is

$$MTBF = \int_0^{\infty} dt \cdot t \cdot f(t) = \int_0^{\infty} dt \cdot S(t). \quad (6)$$

Parameterizations of the failure rate need to be matched to the use case. In the simplest case where $\lambda(t)$ is constant, the failure probability densities function is exponential

$$F(t) = 1 - \exp(-\lambda \cdot t) \Leftrightarrow f(t) = \lambda \cdot \exp(-\lambda \cdot t) \quad (7)$$

and $MTBF$ is λ^{-1} . If the availability analysis covers more complex situations such as varying hazards (due to reduction of infant mortality, improvements, ageing, refurbishments, replacement, active/inactive periods, enhanced failure rates after turn on, influence of internal factors like temperature, humidity, varying degree of human intervention, time dependent distortions of the mains and other deterministic factors), the use of a more complex model will provide more accurate analysis and performance predictions. The analysis based on constant failure rate may lead to significant underestimation of the failure rate and overestimate of predicted performance. A powerful parameterization of the failure rate is the Weibull parameterization, a two-parameter function which can be adapted to a wide range of failure scenarios,

$$\lambda(t) = \frac{a}{b} \left(\frac{t}{b}\right)^{a-1} \Rightarrow S(t) = \exp\left[-\left(\frac{t}{b}\right)^a\right] \quad (8)$$

$$\Rightarrow MTBF = b \cdot \Gamma\left(1 + \frac{1}{a}\right)$$

(Γ is the gamma function). The parameters a and b can be chosen such as to describe a decreasing, increasing or

constant failure rate which leads to a more meaningful analysis of observed availability data.

Operational efficiency may be measured by availability, defined as the time the accelerator functions normally for user operations divided by the time scheduled for this purpose. In case failures are rare ($N \cdot \lambda \cdot MTTR \ll 1$), the availability of a single component may be defined as

$$A = 1 - MTTR / (MTBF + MTTR) \quad (9)$$

and the availability of a system with N subsystems is

$$A = \prod_{i=1}^N \left[1 - \frac{MTTR_i}{MTTR_i + MTTF_i}\right]. \quad (10)$$

In case the system performance reduction D_i due to a component failure is only partial, the system might continue to operate until the next opportunity for repair. The decision of either to continue or to interrupt operation depends on safety considerations, repair opportunity due to scheduled maintenance, availability of spares, performance reduction of other subsystems and the ability to repair. Assuming that all failures can be repaired during regularly scheduled maintenance with a period of ΔT , the availability of a partially impaired system is described by

$$A = \prod_{i=1}^N (1 - 0.5 \cdot \Delta T \cdot D_i / MTBF_i). \quad (11)$$

Depending on the tolerance for degraded performance, the system availability is somewhere in between the results of these two scenarios.

AVAILABILITY SIMULATIONS

The shortcoming of analytical models of the failure rate to describe the full complexity accelerators with complicated operating scenarios are overcome by Monte Carlo simulations which allow testing strategies in dealing with failures as well investigating systematic effects on the failure rate. The simulation may include: rational decision making on whether to continue running with reduced performance until there is an opportunity for repair or immediate repair, saving time by parasitic accelerator studies during reduced performance thereby reducing the scheduled time of non-availability, enhanced failure rate in a second system due to modification of operational parameters implied by operating with a failure in a first, controlling the number of in situ-repair activities in the same locations, enhanced failure rates for a certain period after recovery from the downtime, enhanced failure rate due to maintenance and trouble shooting activities, and start-up period to ramp up performance to steady state level. Simulations also allow taking into account the effects of preventive maintenance, regularly scheduled maintenance, replacement strategies, and impact of limited accessibility of the components for repair.

Such a simulation has been set up for an ILC scenario to study vulnerabilities and identify systems which need upgraded reliability as well as to study the impact of providing access to the accelerator via a service tunnel. Details are provided in reference [4].

A simulation procedure has been developed to assess NSLS-II availability which handles most effects mentioned above. Most critical subsystems are the power supplies and site main power. Power supply reliability is specially addressed for NSLS-II. The tool also allows testing different operation strategies. An example which has been studied is: “What is the optimum performance reduction due to failures which can be tolerated to keep the accelerator running?” Performance is parameterized by beam current/effective beam size. A critical parameter is the minimum intervention time of 4h. The result is that best performance is always obtained if no or little performance reduction is tolerated. Only a minor advantage in availability, thus schedule safety, can be achieved on the expense that the overall performance is reduced to less than 80% (See figure 1).

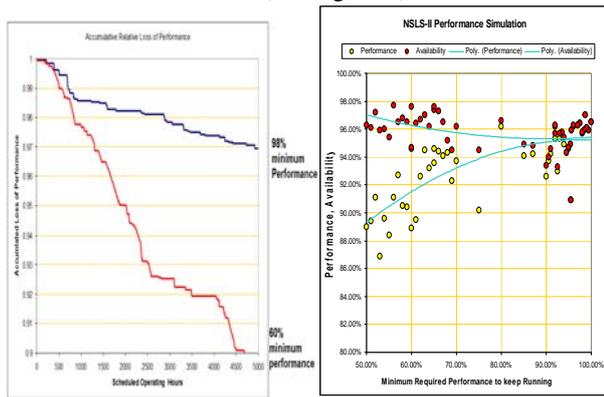


Figure 1: NSLS-II Performance Simulation for 2 modes of operation: Interrupt operation if performance falls below 98% (blue) or below 70% (red), left figure. Performance, availability versus minimum required performance to run, right figure.

HIGH AVAILABILITY DESIGN

Many aspect of accelerator design impact the system availability. Designers are forced to compromise between performance goals, affordable cost and optimum design for availability. The overall complexity of a facility usually is dictated by the primary design goals and cannot be compromised. This, besides facility size is a main reason why availabilities in the order of >95% can be achieved for synchrotron light sources while in colliders for particle physics where two particle beams must be accelerated in a complex high energy acceleration chain achieve rarely better availabilities than 75%.

Compromise to save cost and to assure performance is unavoidable but the design should avoid accumulation of

design weakness. For example a slow injector should be mitigated by transfer lines with excellent diagnostics.

Which global design features affect operational efficiency? Compact versus modular design approaches is discussed. A compact solution is expected to fail less frequently as it will minimize the number of active components but is more likely to constitute a single point failure. A modular design will fail more often for the opposite reason, but the impact of a failure might be less severe. A combination of the two approaches may accumulate the disadvantages. Consider for example a large DC power supply which feeds a large number of small switched mode supplies. The numerous individual switched mode supplies will fail relatively often. Each failure of the daughter supply will trip the mother supply and will cause a major failure which not only trips the beam more likely but requires much longer recovery. Thus, individual independent supplies are expected to be more reliable. The NSLS-II approach [7] is to provide a single small DC supply for each switched mode supply. There is a solution which avoids the dilemma: A switched mode power supply with parallel power modules that provide N+1 redundancy with a redundant embedded digital controller has been developed at SLAC [5] which recognizes a fault condition and isolates the supply from the mother via fast FET switches (figure 2 shows the block diagram).

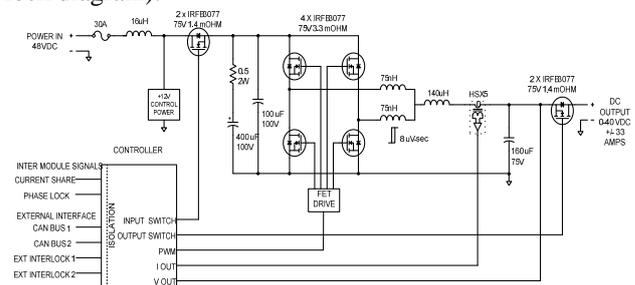


Figure 2: High Availability switched mode power supply block diagram with FET isolating switches

A fail safe design approach is mandatory especially for high power components. A number of technical interlocks based on measurements at a number of control points protect the device from self destruction. Especially the during start-up phase, technical interlock safety thresholds need to be set conservatively low. This however increases the trip-rate of the devices. In order to be able to adapt the trip-threshold to the increasing confidence and control as operation matures, flexible trip-thresholds are desirable for high availability. These need to be included into the early design phase including consideration for safely managing the trip-thresholds.

There are technical approaches which are intrinsically error prone. This is the case wherever water cooling is used on or near electrical devices. Water cooling is in particular cumbersome if rubber hoses are used in the cooling system. But also soldered and braised connections are frequent sources of leaks which can cause shorts,

corrode contacts, destroy electronics and monitoring devices. While water cooling of magnet coils can hardly be avoided, one can try to avoid water cooling with power supplies. An example is the NSLS-II approach [6] which uses a closed air-cooled rack system with an air-to-chilled water heat exchanger system (see figure 3). Analogue cable connections are a weak point in each technical installation and should be avoided wherever digital signal transmission is possible.

The control of environmental factors such as dust, humidity and external temperature changes is a key issue in the reliability and availability of all electronic and electric devices. The NSLS-II rack-system also allows controlling other relevant environmental parameters such as ambient temperature change and change of humidity and mechanical vibrations.



Figure 3: NSLS-II Power closed supply rack with air-cooling and air-to-chilled-water heat exchanger.

Build-in technical margins are a well known and proven method of controlling failure rates (see for example [7]). This is observed for many high power systems such as power supplies and RF power sources. The mechanism related to temperature changes in operation and the corresponding change in mechanical forces and stresses. The HERA electron beam current before 1997 was limited to about 35mA mainly due to frequent RF trips. When another 1.5MW RF transmitter station provided additional RF power margin of 14% after 1997, the beam current could be raised routinely above 45mA. There is, however, a large uncertainty about the gain of reliability due to overrating the device which makes a rational cost-benefit analysis quite difficult.

Repair friendly design will speed up repair by not required experts and by minimizing the work with disconnections and connections. Obviously the modularity of the design is an important aspect. An example for a repair-friendly design is the docking station for the XFEL power supply rack with five switched mode power supplies [8] which allows exchanging a modulator with minimum intervention (see figure 4).



Figure 4: XFEL Power Supply Rack Docking Station for fast installation/replacement of entire rack

The use of hot spares and build in redundancy improves reliability by reducing the impact of a failure. Repair and recovery times can be minimized, or, in case there is automatic switching to the hot spare has hardly any impact on operations. The disadvantage is that it is very expensive when considering large series of components. An example is the switched mode power supply with parallel and redundant switching modules developed at DESY for TESLA and XFEL [8]. The current is automatically redistributed over the intact switching units in case of failure. The defect switching module can be exchanged while the power supply is in operation (see figure 5).

Access to the components is an important design consideration relevant for quick recovery from a failure. This includes the accessibility to perform measurements and inspection, in-situ repairs and replacements. The impact of design choices on accessibility is ideally assessed during the design phase including detailed failure and recovery scenarios. It is often not feasible to recover from missed opportunities in design phase. In the category of minimizing the impact of a failure is build-in diagnostics. This diagnostics can be used for trouble shooting but is also useful for continuous monitoring and failure prevention (see below).

HIGH AVAILABILITY OPERATIONS

While many reasons for inefficiency are a consequence of design decisions, the way a facility is operated has a large impact on availability. A very important principle is continuous improvement which will continuously reduce the failure rates and has the potential of extending the useful life of the facility and its components significantly.

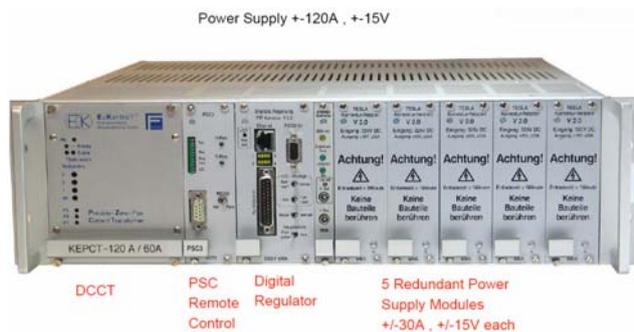


Figure 5: Modular switched mode power supply developed for TESLA and XFEL (see ref [8]).

The quest of interrupting operations for regular maintenance instead keep the facility running until a necessary repair will require a break is an on-going debate. On one hand, it is well proven that the temperature changes when turning off/on components will lead to increased initial failure rate. In HERA for example, the extra time to trouble shoot and repair failing components after each of the monthly regular maintenance day amounted to 4 h on average. On the other hand, regularly scheduled maintenance provides opportunity for repairs without affecting availability. When regular and preventive maintenance of the HERA power supply system was introduced in 2003, where routinely all water cooling connections, mechanical supports, clamping and bolted connections were checked and fixed, the meantime between failure of the large thyristor power supplies went from 20000h to >100000h. Preventive maintenance is of mandatory for all rotary equipment like pumps, compressors, and fans. Fan systems, while playing a major role in maintaining proper functioning have a high failure rate. Regular refurbishment of these consumable-like low cost items such as fans, water-hoses, fuses etc is recommendable. In order to do this in a rational way compromising between cost and availability, the mean residual lifetime (*MRL*) should be considered. Has the failure function $\lambda(t)$ thus $S(t)$ for a component known, the mean residual lifetime can be evaluated at any point t in time using the relationship

$$MRL = \frac{1}{S(t)} \cdot \int_0^{\infty} dt' S(t+t') \quad (12)$$

where the component has been functioning for a time t without failure. *MRL* will provide guidance for replacement before the components fail. It should be pointed out, that if a constant failure rate λ is assumed, the result will always be λ^{-1} . Thus a more sophisticated model such as the Weibull parameterization should be used for analysis. It is not advisable to use this method for decisions on replacing more costly devices like thyratrons, ignitrons, thyristors, or RF power tubes. However some of these components reveal performance

degradation prior to failure. Thyratrons for example are known to become resistive at the end of the lifecycle which requires increasing the set-points of kickers and septa pulsers. If this is carefully monitored the onset of failures can be detected and opportunities to fix before failure can be identified.

Continuous improvement by monitoring, analysis and corrective actions is a key issue in achieving good performance. Comprehensive logging of time stamped data from all hardware systems is an important ingredient. Root cause analysis is essential not only to prevent serious failures from repeating but to eliminate entire failure classes. Another issue is efficient recovery from failure. Transient recording, integrating asset managing into the operational data base are supporting fast trouble shooting and repair.

This report should not end without mentioning the importance the human factor for the operational efficiency of a facility. Is the operation process sufficiently complex human errors are a factor to be taken into account. Operator training and qualifications are important but not efficient. Operational software should be carefully designed to support the operators in not making mistakes. Once a failure has happened, availability of experts is essential in speeding up trouble shooting and repair thereby minimising lost time. Remote access to the components should be seriously considered despite the challenges of cyber security. Last but not least, it should be pointed out that ownership of operations and operational results by the entire technical and scientific staff cannot be overemphasized in the successful high efficient operation of an accelerator facility.

REFERENCES

- [1] HERA proposal, HERA 81-10, DESY 1981
- [2] <http://www.esrf.eu/Accelerators/Conferences/ARW>
- [3] <http://www.triumf.info/hosted/ARW/index.htm>
- [4] T. Himel et al, PAC 2007, WEYAB02
- [5] P. Bellomo[#], D. MacNair, <http://indico.triumf.ca/contributionDisplay.py?contribId=5&sessionId=7&confId=749>, Vancouver 2009
- [6] H. Calleja et al; PESC 2007, p 1522
- [7] NLSLII TDR, <http://www.bnl.gov/nsls2/project/TDR/>
- [8] J. Eckoldt, http://adweb.desy.de/mpy/Groemitz_MiniWorkshop2005/