Proposal to use Failure Prediction as a Means of Meeting Availability Requirements at the SSC

Surajit Sarkar, William Merz, Frank Meyer.
Superconducting Super Collider Laboratory*
2550 Beckleymeade Avenue, Dallas, Texas, 75237

Abstract

The SSC is a complex of six accelerators with a large number of components and high availability requirements. In a number of accelerator subsystems, for example the Collider Correction Magnet Power Supplies, availability requirements cannot be met with non-redundant architectures. Cost and practicality considerations preclude the use of multiply redundant architectures as viable options. The possible use of failure prediction as a means of meeting the high availability requirements of the Collider Corrector Power Supply subsystem is described and the implications on the SSC Central Control System is discussed.

I. INTRODUCTION

The SSC complex of six accelerators is currently estimated to have about 540,000 control and monitor points[1]. The large number of control and monitor points reflects the number of devices and components which are involved in the proper operation of these accelerators. The availability requirements placed on these accelerators and therefore on the devices and components is high. For example the required Collider availability of 0.80 translates to an availability requirement of 0.997 for the Collider correction magnet power supply system. Comparable availability figures have been achieved at Fermilab, a complex of accelerators the largest of which is about one tenth the size of one of the two SSC collider rings, however, only after many years of operation.

For a system consisting of a network of components the system reliability is evaluated by applying well known combinatorial rules as determined by network topology and by the individual component reliabilities[2]. Very roughly, the Mean Time Between Failure, $MTBF_s$ of a system 's', with 'n' identical components having component $MTBF_c$ is given by $MTBF_s = MTBF_c / n$. The MTBF decreases (or the system failure rate increases) in proportion to the number of components. The standard approaches to improving the system reliability are: (1)to increase the component reliability or (2)to favorably alter the system / sub-system topology by adding redundancy to (weak or) less reliable links.

The problem arises in systems with a large number of components. For such systems it may not be possible to increase component reliability to meet the availability requirements. The avenues of using redundant architectures may not be cost effective and those of using multiply redundant architectures may not be practical. This problem is aggravated as the numbers increase.

Two examples related to the Collider correction magnet power supply operation are the Collider correction magnet power supply system and the power supply controller to power supply fibre optic link components.

*Operated by the Universities Research Association, Inc., for the U.S. Department of Energy under Contract No. DE-AC02-89ER40486.

Even with singly redundant architectures[3] achieving a Collider correction magnet power supply system MTBF of ten days (or one run period) requires an increase of component power supply MTBF from the current industry standards, in the range of 50,000-100,000 hours to a figure somewhat greater than 1 million hours MTBF - a ten to twenty fold increase.

Using selected devices for the power supply controller fibre-optic links, with component typical MTBF in the range of about 4 million hours, the 24,000 optical transmitters and receivers to be used in the SSC correction, 'DC', and ring magnet power supply controllers will have a combined MTBF of 6.5 days. This is less than the ten day running period.

From the above two examples it becomes clear that for systems with a large number of components increasing the MTBF of well designed sub-systems or good components, which may already be state-of-the-art limited, becomes increasingly difficult to the point of requiring the achievement of unattainable MTBFs.

MTBF gains for redundant systems do not scale directly as the number of systems when repair is constrained to scheduled maintenance periods. They are further degraded due to the additional components and methods required to switch over to the non failed system. Buying more reliable components, using redundancy and component derating as means of increasing system MTBF have cost implications which may pose limitation on system design for reliability. For example the 'reliability allowance' included in cost estimates for the collider corrector power supply systems do not allow redundancy and power supply controller costs have been estimated using commercial not high reliability components.

While cold spares may reduce the mean time to repair a sub-system and consequently increase system availability it cannot compensate for the lost time required to reach the given operational state aborted by the particular failure.

The MTBF is a statistical figure. By definition for a constant failure rate, ie. an exponential distribution of failures, the probability of surviving one MTBF without failure is 37%. For a system MTBF of one run period, most failures will happen before this time interrupting a run. User frustration will likely scale as the frequency of stopped runs.

From the above arguments we conclude that: *'what is required is failure free system operation for the duration of each run and not a high over all system MTBF'* - with a failure being defined as anything that causes beam quality degradation sufficient to require a dump.

II. FAILURE PREDICTION

The method proposed here to address the above requirement is the use of 'quantitative' prediction of failures. The assumptions are that we have a scheduled 4 day shutdown following a ten day run period. If all failures can be anticipated and taken care of during the scheduled shutdown,

unscheduled downtime is nil. The effective system uptime is 100% or equivalent to a system with an infinite MTBF.

Our premise here is that if some of the failure modes of a component are not instantaneous, but rather are a result of the progression of degradation of some parameter(s), then it should be possible to monitor those parameters and from the progression of monitored states predict, with some associated probability, that a piece of equipment is going to fail within a certain time period.

Failure modes with the highest frequency can be identified and the characterized such that one can predict component failure to some required degree of temporal accuracy. Such components can then be replaced during a shutdown period or scheduled maintenance so as not to contribute to system down-time figures. Components known to be partially marginal (or those for which, the temporal bracketing achievable is known to be less accurate) may be removed from critical subsystems and placed into operation in the less critical or easily accessible areas which incur a smaller Mean Time to Repair (MTTR) or system down-time per failure.

In searching the literature we find that the idea of being able to detect failures exists in the industry, though somewhat qualitatively, under the name of Condition Monitoring. What is proposed here is an extension of these basic principles to add a temporal domain to the analyzed data so as to allow us to bracket the failure to some predetermined window of time in which failures will happen with some given probability. This probability multiplied by the cost of such a failure (in terms of lost beam production) gives us a factor determining the urgency, or the requirement to replace, given the cost of reaching that stage of operations. The probability of failure, the cost to reach that stage in operations and the cost of potential loss of operation as a function of stage of operation are all continuously changing variables and need to be dynamically evaluated against the real cost of component replacement.

The idea proposed here is generally applicable to large systems. Conveniently failure prediction becomes useful for systems where it becomes necessary to use or rely on such methods: those with a large number of components. Systems with large numbers of similar components require less running hours to gather the statistical data needed to characterize the failure modes. Failure modes with the highest frequency - those that can cause the most operational grief - provide data (and so can be characterized) quicker. This proposal can be extended to the not so large systems, which however have critical mission requirements, as described in section V.

A. Implementation

In practice a combination of methods will have to be used. In any system routine Failure Modes and Effects Analysis (FMEA) will identify the critical areas and actions required to mitigate them. Quantitative failure prediction is proposed to be used as an adjunct to the above procedures, in cases where requirements cannot be met by such methods alone, in cases where exceptional availability is required during run periods, or in mission critical systems where even single failures cannot be tolerated and cost is not a constraining factor.

For each system it is necessary to determine what fraction of components can fail before system operation is affected. For the 'DC' and corrector power supply to controller fibre-optic links, failures do not affect the operation of the 'DC' PS operation as long as no beamline energy or steering changes are required. Injector and possibly collider corrector failures during the 20 hour collider flat-top may also be tolerable. The effect of single point failures[5] and the possibility of compensation using adjacent (sets of) correctors[4] is being explored. In the case of the controller to power supply fibre-optic links implementation of failure prediction using parasitic trending of link Bit Error Rates is being explored - system cost here is the specification of appropriate link protocol[6].

The practical implementation of these techniques must proceed in the stages. Initial task will be the identification of failure modes followed by the implementation in stages of condition monitoring, qualitative and quantitative failure prediction, to the generation of dynamically evaluated component replacement cost factor projected as a function of time, for particular failure modes with operator prompting programs being implemented later.

III. METHODS

The parameters used as indicators of failure may be analog, digital or complex types derived by processing other parameters as described below.

A. Analog Parameters

Typical analog parameters envisaged for example in a power converter was h_{FE} of pass transistors in regulator banks. At a recent conference it was confirmed that this is indeed a parameter which showed degradation in failing power converter amplifier pass banks[7]. In switched mode power converters for example the occurrence of spikes have been seen as precursors to failure[8] although they have not been used in the manner proposed here of characterization and failure prediction.

B. Digital Parameters

Some of the parameters may be digital signals say from relay contact closures, logic signals or composite digital signals from interlock processing equipment.

It may seem that digital signal failures are not predictable or are sudden. Looking more closely for example a relay may have some contact bounce associated with closure. It is possible to characterize this bounce and see if this changes with time - or as a function of other factors such as operating current or ambient temperature.

Discreet logic signals are digital only in that a categorization has been imposed on analog characteristics: for example for TTL signals a logic level of 0 encompasses 0-0.4V and some associated node currents. Logic state transitions are digital (only) above a range of time granularity. Variations in any of these parameters can be used for failure mode identification. Examples are given in reference[9].

C. Complex Parameter Types

Adding a level of complexity one could explore the behaviour 'surface' (along the lines of control surface for a dynamical control system) of multi-parameter failure modes, such as ambient temperature and operating current versus the contact bounce, and contact opening time versus the bounce for a relay. A fraction of such failure data may be non-stationary and may require specialized techniques[10] for processing. The caveat of course is that this must be only for systems where this is indeed of sufficient importance - how ever in

such large systems and where other restrictions do not hinder this may be a possible technique to consider. The plotting of behaviour surfaces for visual feature detection or the use of Neural nets for feature extraction may be required. With the perfection of these techniques relatively inexpensive integrated hardware to carry out these functions could be developed and the evaluation and implementation of complex processing functions could be easier. The use of Fuzzy logic to implement estimation algorithms on the extracted features and implement decision trees to inform Central controls of impending failures or of required actions such as abort or change particular component within predicted time are all possible. The use of built in test vectors in front end electronics allows the possibility in controls electronics of predicting chain failures which may not become critical before a certain time.

IV. CONSEQUENCES OR REQUIREMENTS FOR THE CONTROL SYSTEM

To implement Quantitative Failure Prediction (QFP) the Global Accelerator Control System (GACS) must allow for the collection and analysis of requisite data - the characteristics of both of which are not fully defined at this stage. Data for QFP will have to be collected either 'passively' from accelerator sub-system and component data monitored routinely, or 'actively', where the data collection process requires the modification of mode of operation of the sub-system or device under test from the normal accelerator operation modes, between acceleration cycles. The monitoring of specific controls equipment, the use of specialized techniques such as statistical or syntactic pattern recognition[11] techniques and the possible use of neural nets[12] and fuzzy logic in decision processes and their impact on the GACS processing hardware, controls software and the effects (of additional hardware and system software) on system reliability all need to be addressed. The addition of processing capacity at the 'rear-end' or Main Control Room computers is relatively easy. Number of component systems are relatively small and good accessability guarantees a small mean time to *replace*. Capacity additions to the GACS communications are also relatively easy but are not expected to be required.

Typically Front End Electronics components and sub-systems have the largest numbers and are most difficult to change or upgrade later in the implementation cycle and must be appropriately designed. Changes have ripple effects on downstream equipment such as sensors and controllers. Reliability of front end electronics needs to be considered in detail. The use of front end equipment buses with the capability to isolate failed cards and with kernels which allow dynamic task allocation between crate level processors allows the problem at the equipment crate level to be mitigated. The problem of failures at the front end electronics signal conditioning and interface level can not be addressed by the methods used above and a possible solution is QFP. With time as such methods are frequently used library of standard techniques will be developed which can be reused with relatively lower cost and effort impact.

V. DISCUSSION

A. *Status*

Few systems are currently being analyzed with reference to controls requirements for failure detection or prediction. The redeeming factor is that at present only systems having relatively small number of components are being interfaced to the GACS. However, the definition of techniques required for failure prediction, from this stage would have allowed all systems to be similar with the attendant benefits of inventory reduction and maintenance streamlining.

For the 'DC', correction and pulsed power supply controls we are considering these options when feasible within limited available effort.

B. *Cost Implications*

The use of high reliability components and testing methods increases the cost of systems conservatively by a factor of 10 times for initial purchases and all future replacements. If the use of failure prediction allows the use of relatively inexpensive components then there can be definite long term cost gains associated with the use of such techniques.

The initial cost of implementation of failure prediction is in the systems analysis effort and currently in the development of implementation techniques. Only the hooks required for the specialized data acquisition hardware and software needs to be provided initially with modules being populated or incorporated as required. For the 'DC' and corrector power supply controllers the additional costs for hardware were found to be negligible.

C. *General*

Quantitative failure prediction can be useful for mission critical systems such as space flight were even single 'unprotected' failures can be critical. In case of not so large systems, data required for failure characterization can be acquired by using an extended set of components during the system design and commissioning periods - assuming that cost is not a constraining factor.

System availability requirement allocations may require a re-evaluation based on the modified system properties with the incorporation of failure prediction.

VI. REFERENCES

[1] 'SSC Global Accelerator Control System Preliminary Design Requirements Review', SSC Internal Documents, September 9th, 1992.
[2] 'Electronic Reliability Design Handbook', Military Handbook, MIL-HDBK-338-IA, vol.I, October 1988.
[3] F. Meyer, 'Impact of Reliability Requirements for the Collider Correction Power Systems', SSC internal note, May 5th, 1992.
[4] S. Sarkar, 'Compensation for Failed Collider Correctors', SSC internal note, December 9th, 1992.
[5] G. Bourianoff, 'Accelerator Simulation activities at the SSCL', SSC laboratory publication number SSCL-N-811, January, 1993.
[6] S. Sarkar *et al*, 'Controls Interface Protocols for the SSC Correction and 'DC' Magnet Power Supplies' These proceedings.
[7] M. Fatizadeh, private communication, Panel Discussions on Power Supply Controls, IEEE Nuclear Science Symposium, Orlando, FL, October, 1992.
[8] H. Isch, private communication, Panel Discussions on Power Supply Controls, IEEE Nuclear Science Symposium, Orlando, FL, October, 1992.
[9] K. Liu, J. Gertler, 'Monitoring the Condition of Feedback Control Systems', Proceedings IEEE International Symposium on Intelligent Control, p-51, Arlington, VA, August, 1988.
[10] A. Moore, S. McLaughlin, 'Spectral Estimation of Nonstationary Time Series', Proceedings 6th International Conference on Digital Processing of Signals in Communications, Loughborough, UK, p-36, September, 1991.
[11] R.J. Hamilton *et al*, 'Syntactic Techniques for Pattern Recognition on Sampled Data Systems', IEE Proceedings on Computers and Digital Techniques, p-156, Vol.139, No. 2, March, 1992.
[12] M. Chow *et al*, 'A neural Network Approach to Real-Time Condition Monitoring of Induction Monitors', IEEE Transactions on Industrial Electronics, p-448, Vol. 38, No. 6, December, 1991.