LCC-0084
July 2002

Linear Collider Collaboration Tech Notes

A Comment on Machine Reliability and Availability

Raymond S. Larsen

Stanford Linear Accelerator Center
Stanford University
Menlo Park, California

Abstract: There appears to be continuing confusion in the community between the terms *reliability* and *availability*. The following is a comment on the salient points, none of which are particularly new to NLC discussions of the past 2-3 years, but which will soon require serious further study because of potential impact on overall system engineering manpower, costs and schedules.

LCC-0084

A Comment on Machine Reliability and Availability

R.S. Larsen
Stanford Linear Accelerator Center
February 15, 2002

The just concluded LC02 discussions on machine reliability were very interesting but due to lack of time, were left in a somewhat defocused state. There appears to be continuing confusion in the community between the terms *reliability* and *availability*, and several other aspects that did not get discussed for lack of time. The following is a comment on the salient points, none of which are particularly new to NLC discussions of the past 2-3 years, but which will soon require serious further study because of potential impact on overall system engineering manpower, costs and schedules.

1. Availability vs. Reliability

The primary measure of our ability to run a 1 TeV LC with high efficiency is *availability*. As modern accelerators have proven, availability can be high even though the *reliability* of any given system is low enough that were it the measure of our ability to operate the machine, it would never be able to run. The relationship of these parameters is made clear in a formal reliability model of the machine. Z. Wilson[1,2] has studied a reliability model of the NLC in which availability, reliability and Mean Time to Repair (MTTR) of various subsystems were related to a calculation of total machine availability.

High *availability* is achieved by recognizing the failure modes of systems and designing schemes to render them as invisible as possible to the total system, so the system itself "takes a licking but keeps on ticking" like a Timex watch. Methods are obvious to us all:

- Build extra RF power stations that run all the time in standby mode and can be brought on line between pulses when one unit hiccups.
- Make redundant modular electronics systems such that the loss of a single channel of monitoring or control can be worked around.
- Design power devices to be modular and redundant so they can run when a section fails, and the failed section can be replaced without interruption to operations.

By addressing each subsystem at the design level to enable these kinds of strategies, a high level of *availability* of a total LC can be achieved. Obviously there is an engineering discipline required, an engineering cost and an implementation cost. This cost is normally buried in new designs and not called out separately.

2. Reliability and FMEA

Each subsystem of the total accelerator must strive for *reliability*, but there is a cost in engineering for high inherent reliability. In practice *subsystem reliability* is limited by inherent reliabilities of connectors, PC board technology, power device technology, integrated circuit reliability, packaged power supplies, fans, plumbing, mechanical joints

and welds, and so on. Sometimes we experience basic problems with something like a standard connector or cable and have to invent new, custom designs to achieve the reliability we need. Examples were mentioned in the talks.

The tool called FMEA, *Failure Modes and Effects Analysis,* is valuable for examining the weak points of a design and addressing them with engineering solutions. FMEA can be applied to a circuit or to a large system. Companies that make thousands or millions of products that get shipped everywhere around the world, or that have production lines where there is a large payoff to improving yield, rely heavily on this tool. NLC has experimented with FMEA but now it is on the back burner, because in the R&D stage there is insufficient time and funding to impose it. However, for the real machine design, it would be foolish to ignore FMEA for those high volume parts that permeate many subsystems: 30,000 vacuum pumps and drivers, 10,000 movers (maybe more with adjustable permanent magnets), 10,000 BPMs. 30,000 IGBT drivers and boards etc. The investment required is primarily in engineering, and companies that use FMEA report that it adds about 40% to the normal engineering and design bill. FMEA principles are normally used in all designs but formally applied FMEA is useful and necessary in cases where there is a big potential payoff in an improved design, where some areas of payoff are much richer than others. SLAC has successfully used the technique to design a new magnet system, and a prototype magnet has been built.[1] FMEA is also useful as a discipline to look critically at specialized low volume systems (as opposed to devices) such as Machine Protection.

3. Engineering and Cost Considerations

Subsystems and the total system must be engineered for both *availability* and *reliability,* within the reasonable cost constraints that are imposed on every system. Life-cycle costs should be considered. A machine with poor reliability will have a proportionately higher maintenance cost for the life of the machine. In these days of very high capital cost projects, with long gestation and build cycles, a fast ramp-up to design and commissioning is paramount, and that argues for more engineering up front to achieve both reliability and availability. We should try to identify explicitly the areas where increased design cycles, and costs, are required to engineer reliability into devices; and we should specifically call out in each area where we need to add cost for redundancy that is designed to increase machine availability. The most obvious example is in modulators and RF stations.

4. Redundancy and Safety

In areas such as safety systems, redundancy is added not to improve availability but to improve either machine or personnel safety. These costs are viewed as part of the basic

[1] *A Novel Approach To Increasing The Reliability Of Accelerator Magnets,* Paul Bellomo, Carl E. Rago, Cherrill M. Spencer, Zane J. Wilson (SLAC). SLAC-PUB-8254, Feb 2000. 5pp. Presented at 16th International Conference on Magnet Technology (MT-16 1999), Tallahassee, Florida, 29 Sep -1 Oct 1999. Published in IEEE Trans.Appl.Supercond.10: 284-287,2000

system design, rather than as costs added to improve availability, so do not pose an extra cost burden per se.

5. Additional Diagnostics to Improve Availability

Improved diagnostics will enable more rapid identification and repair of problems and even prediction of the onset of problems before they interrupt operations. This topic, however, has not progressed to a serious study. Obviously, adding more diagnostics than we normally include will add both engineering and a capital cost. To quantify this, we need to make case studies. Modulators, low and high level RF, machine protection and personnel protection would be excellent candidates. Besides the subsystem hardware implementation, the overall software engineering effort needed to support the added diagnostics modes needs analysis.

6. Summary

Availability is the key parameter to keep in view when discussing related topics of inherent reliability, engineering for improved reliability with FMEA, redundancy, and added engineering costs of related hardware and software. The relationships and cost tradeoffs between reliability and availability can be studied using a formal model. Reliability can be improved by the engineering discipline called FMEA, and advocates integrate the discipline into the design process. The cost of adding FMEA into the engineering cycle of a commercial product is estimated at about 40%. For a large system of many subsystems such as a next-generation LC, the cost may be higher or lower, depending on how extensively the discipline is applied. In addition, FMEA-like disciplines are applied to software design where the cost of a failure can be enormous, such as in spacecraft. Machine Protection would be one area where robustness of software and hardware design will be well worth an extra investment. Finally, MTTR is inversely related to availability, so that diagnostics, redundancy and design for ease in maintenance and prediction of impending failure, all aimed at reducing MTTR, can significantly improve machine availability.