RELIABILITY AND AVAILABILITY MODELLING FOR ACCELERATOR DRIVEN FACILITIES

O. Rey Orozko, E. Bargalló, A. Nordt, ESS, Lund, Sweden
A. Apollonio, R. Schmidt, CERN, Geneva, Switzerland

Abstract

Accelerator driven facilities are and will have to be designed to a very high level of reliability and beam availability to meet expectations of the users and experiments. In order to fulfil these demanding requirements on reliability and overall beam availability, statistical models have been developed. We compare different statistical reliability models as well as tools in terms of their performance, capacity and user-friendliness. In addition we also benchmarked some of the existing models. We will present in detail a tool being used for LHC and LINAC4, which is based on the commercially available software package Isograph, and a tool using Excel Visual Basics for Applications.

INTRODUCTION

Reliability and availability studies are becoming of crucial importance in the domain of particle accelerators and accelerator driven facilities. The increasing complexity of systems but also cost driven prioritization approaches and the interest in pushing performance towards the currently known limits, and even beyond, makes such studies necessary to guide physicists and engineers in the design of more performing systems in terms of reliability and maintainability and still low cost.

In particular, user needs are very demanding in terms of reliability and availability for neutron sources and synchrotron light sources. Users usually ask for a continuous and reliable beam. Requirements are specified in terms of maximum downtime of the accelerator or facility and in terms of acceptable beam performance degradation during experiments. These requirements need then accurate studies to be validated already in the design phase, eventually driving changes in the system design in case major limitations to the global availability of the facility are identified.

AVAILABILITY AND RELIABILITY MODELLING

Isograph

Isograph [1] is a commercial tool currently used at CERN for various reliability and availability calculations. The use of such software is relatively straight-forward for people already used to dependability [2] studies, but requires some time to fully exploit all its capabilities. It is composed of two separate workbenches, namely the Reliability workbench and the Availability workbench. The first one allows performing several reliability-related analyses, depending on the licensed packages, while the second focuses on the simulation of systems availability.

A Prediction package allows for the calculation of component failure rates, according to different existing standards (e.g. MIL-217). The Failure Mode Effect and Criticality Analyses (FMECA) package allows building a structured system failure analysis. The Event tree package offers the possibility of performing Event-tree analyses to evaluate the consequences of an initiating event on the system. The Markov package is of particular interest when dealing with systems whose components exhibit strong dependencies.

The Reliability Block Diagrams (RBD) and Fault Trees (FT) allow estimating the reliability of complex systems, for which basic failure modes need to be defined. A RBD is made of blocks and nodes connected together in parallel or series. A voting strategy can be defined for parallel cases. In FTs, the same structure can be reproduced by means of logical gates (AND, OR, etc). The two approaches are fully equivalent and the more convenient visualization can be chosen in Isograph, depending on the application. Different distributions (e.g. Poisson, Weibull, Lognormal…) and standards (e.g. IEC 61508) can be selected while defining failure modes.

The Weibull package is capable of assigning failure distributions to historical data; these can be used to perform simulations to reproduce the system behaviour in case of failures. In the Availability Workbench, a system can be again modelled with RBDs or FTs. The blocks in a RBD can be used to model component failures, as well as other events, such as operational decisions influencing the availability of the system. For component failure, several maintenance strategies can be selected with many detailed options, as will be shown in this paper. Once all parameters for faults and repairs are defined, simulations over a given observation time can be performed. Simulation results are presented in terms of mean unavailability, number of outages and mean repair times at the system or the sub-systems level. An analysis of costs of components, spares and personnel can also be executed with this workbench. For the simulation results there's the possibility of following the sequence of the simulated failure events and repair actions by a so-called 'simulation watch'. The latter is very useful to check the consistency of maintenance tasks and identify errors in the RBD or FT model.

Excel-based Model

The statistical model implemented in Excel Visual Basics for Applications (vba) was used at the ESS as a tool for preliminary reliability analysis for the accelerator. Excel was used as it is a program accessible for all users and no experience with dependability analyses is needed to use it.

ISBN 978-3-95450-132-8

When defining a system availability model it is important to identify its sub-systems, the corresponding individual availabilities and the logical manner in which these units are connected. Sometimes, dependability experts and the experts in charge of the design of a given system do not have regular contacts. Therefore, an excel based tool represents a good choice for interfacing the two parts and to obtain preliminary estimates of systems availability. Moreover, experts could use this preliminary analysis as a starting point for more sophisticated analyses.

The statistical model is based on common reliability and availability formulas combined following the rules of probability theory. The assumption is that the failure rate of the system follows an exponential distribution and that after a number of independent trials, the probability of failure follows a Bernoulli trial. There is the possibility to add the number of failures that could be anticipated and the different repair times. The MTTR takes into account the time to repair, restart, staffing and radio-protection measures after a failure. MTTR inputs also include the possibility to add the average time needed for administrative and logistics. Three repair strategies are defined in the model and also, three redundancy models. The model does not consider any maintenance strategies and does not take into account the cost of maintenance.

RiskSpectrum

RiskSpectrum PSA Professional is a widely used commercial software in reliability engineering, especially in the nuclear power plants industry, where it is used to develop probabilistic safety assessment (PSA) analyses. It has been used in accelerator reliability studies [3][4] because it is a verified software and because is widely used by reliability engineers.

This software is based on fault tree and event tree analyses through quick and powerful analytical calculation methods that assess time-dependent unavailability stabilization, sensibility analyses, parametric studies and uncertainties quantification among others.

Its analytical basis and its risk assessment focus make it difficult to analyse complex availability models. However, for reliability analyses and for simple availability calculations, the results are exhaustive.

AvailSim

AvailSim is a Matlab® Monte Carlo software developed for the International Linear Collider (ILC) [5] that simulates the availability and beam parameters of an accelerator. It simulates the continuous failure of components during the operation and the effect those events have on the accelerator performance. It allows flexible configuration of maintenance management, manpower requirements and operational parameters among others.

Some features of this software are: several ways problems can degrade performance, different kinds of maintenance (vault access required or not, hot swappable or not), turn-on recovery time (depending on failure, location and time expended), human resources management, and maintenance procedures customization (component priorities, kludges, wait until next scheduled maintenance period, etc.)

AvailSim has been used in the analysis of other accelerators such as IFMIF, for which some modifications and improvements where included in the software [6]. Both versions of the software are publicly available in [7].

EXAMPLES OF AVAILABILITY MODELLING

In order to benchmark the modelling approaches presented in this paper, four examples were considered and results compared for the corresponding models built in Isograph and in the Excel-based tool. Different failure modes and repair strategies are considered throughout the examples. Model inputs are expressed in terms of MTTF and MTTR, but several options for corrective maintenance can be chosen.

Table 1: RF System Parameters

RF System	MTBF	MTTR	Redundancy type	Repair
Modulator	$5*10^4$	4 h	Spare operational	On-line
LLRF	10^5	2 h	-	-
Klystron	$6*10^4$	5 h	-	-
Cavity	10^8	1800 h	-	-
Vacuum	$2.5*10^4$	6 h	Spare operational	Off-line

In the first case, a system made of two components is modelled (1). Both components are needed for the system to work correctly, therefore the corresponding RBD consists in a series connection of the two blocks. This is a very common situation when redundancy is not exploited and could represent the necessity of having a klystron and a vacuum system in order to operate a cavity. When one of these two systems fails, a corrective action needs to be taken to recover operating conditions.

In the second case (2), the system is made of two redundant components. During normal operation both components supply a necessary function for the system. If one of the two fails, the remaining one takes over the full system functionality, while the other is being repaired ('on-line maintenance'). This could be the case of redundant power supplies, placed in an accessible location of the facility that allows performing the corrective maintenance without stopping operation.

In the third example (3) a redundant system made of two components is again considered, but with a different type of corrective maintenance: when one of the two components fails, it is not immediately repaired, but maintenance is performed only when both components fail ('off-line maintenance'). This could be the case of two vacuum pumps located in an un-accessible location (e.g. a tunnel) during operation and that would only be replaced in case of a complete system failure or in an scheduled maintenance period.

As a fourth example (4), a simplified model of an RF system is proposed, based on the concepts explained with the first three examples. The model is composed of 4 systems in series, namely Low Level RF (LLRF), a powering system, an RF cavity and a vacuum system. The powering system is composed of two redundant modulators, for which 'on-line maintenance' is chosen. The vacuum system is composed of two pumps, for which 'off-line maintenance' is considered instead. RF system parameters are shown in Table 1.

The results provided by the two models are consistent across all the four examples, with relative errors in the order of 10^{-4}. With increasing model complexity, an increase of the relative error can be observed in the results.

COMPARISON OF MODELLING TOOLS

Several modelling tools have been used for past dependability studies in different accelerator facilities. In this paragraph an overview on the main features and capabilities of software tools for dependability studies is given and the main features are summarized in Table 2.

The first factor that differentiates softwares is whether they are commercially available or custom developed. This has in turn an influence on several other aspects of modelling. Commercial softwares are reliable sources for modelling, as they are tested and debugged by the developers. They normally provide a wide range of possibilities for several types of analyses (FMECA, Fault-trees, RBDs, etc.) and many options to be selected. On the other hand, given the variety of domains to which such studies are applied, it is possible that particular aspects of some applications could be difficult to take into account. Accelerators are a relatively small example of an application in which dependability studies are performed and the intrinsic nature of accelerators operation and beam-related quantities must be treated with a dedicated approach. Defining degradation of operating conditions and establishing a classification of events importance for a given observable (luminosity, neutron flux, etc.) are some typical examples of this. Some custom tools could be developed in order to make such analyses possible. At the same time custom tools are more critical to test and debug, therefore results need more careful validations.

Another main distinction between softwares can be made based on the calculation methods. Analytical methods have the advantage of making precise assessments of dependability figures, in a very reduced time scale. Nevertheless they are limited to a subset of cases where analytical solutions to the models exist, practically reducing their application to relatively simple cases. Complex cases can be more easily addressed with statistical simulation tools, which do not need an analytical solution to exist to calculate the dependability figures. The solution is an approximation derived by simulating the behaviour of the system according to the input parameters and averaging the results over the number of simulation runs. This approach is intrinsically slower, as simulations of complex systems can take a significant time, but is capable of dealing with increasing system complexity.

For what concerns the users of the tools, a previous knowledge on dependability analyses is required for the use of commercial softwares. Documentation and help functionalities let the user learn the software features over time, but a non-negligible effort has to be put into implementing particular domain-dependent aspects. Software support services can also help solving open issues. Custom tools instead can be tailored to user needs and result being more user-friendly, but a lot of effort has to be put in the documentation part for long-term maintainability.

Table 2: Comparison of Software Features

Features-Tools	Isograph	Excel	AvailSim	Risk-Spectrum
Commercial	CO	CU	CU	CO
Analytical or simulated	A&S	A	S	A
User-friendly	Medium	High	Low	Medium
Beam degradation	Yes	No	Yes	No
Events importance	Yes	No	Possible	Yes

CONCLUSIONS

Four softwares have been considered in this paper and the corresponding characteristics/capabilities are shown in Table 2. Depending on the application and the scope of the analysis, different solutions can be considered: for fast calculations and estimates of figures for simple systems, custom analytical calculations could be considered. In more complex systems, a simulation-based approach could be more valuable, especially when dealing with resources management and optimization.

REFERENCES

[1] Isograph, www.isograph.com
[2] E. Blanco, S. Karstensen, T. Ladzinski, J. Lindkvist, T. Lensch, A. Marqueta, D. McGinnis, A. Nordt, et al., Workshop on PLC Based Interlock Systems for Accelerators and Other Large Research Installations, ESS Accelerator Division. (2013).
[3] E. Bargallo, G. Martinez, J.M. Arroyo, J. Abal, P. Beauvais, F. Orsini, et al., RAMI analyses of the IFMIF accelerator facility and first availability allocation between systems, Fusion Eng. Des. (2012).

[4] A.E. Pitigoi, P.F. Ramos, E. Agrupados, E.A. Ea, Modeling high-power accelerators reliability - Reliability model of SNS linac (SNS-ORNL); Reliability modelling for MAX linac (MYRRHA project), (2011).
[5] T. Himel, J. Nelson, N. Phinney, M. Park, M. Ross, Availability and reliability issues for ILC, IEEE Part. Accel. Conf. (2007).
[6] E. Bargalló, P.J. Sureda, J.M. Arroyo, J. Abal, A. De Blas, J. Dies, et al., Availability simulation software adaptation to the IFMIF accelerator facility RAMI analyses, Fusion Eng. Des. (2014).
[7] https://ess-ics.atlassian.net/wiki/x/LoGh.

ISBN 978-3-95450-132-8