LASER INTERFEROMETER GRAVITATIONAL WAVE OBSERVATORY
- LIGO -
CALIFORNIA INSTITUTE OF TECHNOLOGY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Specification **LIGO-E960099-B - E** 7-21-97

LIGO
RELIABILITY PROGRAM PLAN

LIGO Systems Engineering

This is an internal working note
of the LIGO Project.

California Institute of Technology
LIGO Project - MS 51-33
Pasadena CA 91125
Phone (818) 395-2129
Fax (818) 304-9834
E-mail: info@ligo.caltech.edu

Massachusetts Institute of Technology
LIGO Project - MS 20B-145
Cambridge, MA 01239
Phone (617) 253-4824
Fax (617) 253-7014
E-mail: info@ligo.mit.edu

WWW: http://www.ligo.caltech.edu/

1.0 INTRODUCTION 4

1.1 PURPOSE 4

1.2 SCOPE AND OBJECTIVES 4

1.3 ACRONYMS 5

2.0 APPLICABLE DOCUMENTS 6

3.0 RESPONSIBILITIES 7

3.1 STAFFING AND REPORTING 7

3.2 RELIABILITY PROGRAM DELIVERABLES 7

4.0 RELIABILITY ASSESSMENT 8

4.1 RELIABILITY AND AVAILABILITY PREDICTION 8

4.1.1 Reliability Modeling 8

4.1.2 Modes of Operation 9

4.1.3 System Reliability Requirements 10

4.1.4 Assumptions 10

4.1.5 Reliability Assessment 10

4.1.6 System Availability 12

4.1.7 Analysis Method and Recommendations 13

4.1.8 Availability In Terms of Reliability Growth Assessment 13

4.2 FAILURE MODES AND EFFECTS ANALYSIS 13

4.3 FAULT TREE ANALYSIS 14

5.0 SPARE PART PLANNING 14

6.0 REVIEW OF VENDOR AND TEST DOCUMENTATION 14

6.1 REVIEW OF QUALITY ASSURANCE, RELIABILITY, AND OTHER RELEVANT DOCUMENTATION 14

6.2 REVIEW AND ANALYSIS OF THE VENDOR AND IN-HOUSE DATA 14

7.0 RELIABILITY PROGRAM REVIEWS 15

8.0 LIGO RELIABILITY AND AVAILABILITY REPORT 15

9.0 SUBSYSTEM AVAILABILITY ALLOCATIONS 15

APPENDICES

Appendix A:	Reliability Definitions and Modeling	A-16
Appendix B:	Derivations For LIGO Reliability	B-20
Appendix C:	Failure Mode and Effects Analysis Worksheet	C-27
Appendix D:	Fault Tree Analysis	D-30
Appendix E:	Reliability and Availability Growth Assessment	E-33
Appendix F:	Fault Tree Diagrams Depicting Subsystem Availability Allocations	F-37

1.0 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to outline the reliability assurance plan for the Laser Interferometer Gravitational Wave Observatory (LIGO).

1.2 SCOPE AND OBJECTIVES

This document establishes the reliability assurance plan to be implemented during the design, development, and test of the LIGO system. With regards to design, the application of this plan is focused upon the Detector. The Detector is comprised of the Interferometer (IFO), the Control and Data System (CDS) and the Physics Environment Monitoring System (PEM). The reliability design focus is placed upon the Detector because it is a unique, state-of-the-art instrument with demanding Availability requirements. The facilities have been designed to industry standards with an emphasis on reliability and robustness. The objective of this document is to identify the reliability associated activities and tasks that will be necessary to accomplish the project goals with risks commensurate with the LIGO system. This includes the following:

a. Adequate consideration is given to reliability during the design and development of hardware.

b. Possible sources of unreliability are identified and, where possible, eliminated through the design verification process.

c. Hardware reliability activities are implemented in a timely manner consistent with project schedules.

d. Problems or failures that occur during testing or operation are thoroughly analyzed and corrective action is implemented to preclude possible recurrence.

This plan does not cover any influences or disturbances outside the control of the system itself or exceeding its design specifications. These include, but are not limited to:

a. Environmental extremes (storms, excessive ground motion, etc.)
Based upon the established design criteria, it is assumed that the influence of the environment on system availability will be negligible.

b. Interruption of site power

c. Loss of interferometer lock due to excessive transient disturbances (e.g. heavy machinery operation during future building expansion).

1.3 ACRONYMS

See Appendix A for additional reliability terms and definitions.

BT	Beam Tube
CDS	Control and Data System
CMN	Common
FMEA	Failure Modes and Effects Analysis
FMCS	Facilities Monitoring and Control System
FTA	Fault Tree Analysis
HVAC	Heating, Ventilation and Air Conditioning
IFO	Interferometer
IF2	Interferometer, 2 km long
IF4	Interferometer, 4 km long
LA	Louisiana site
LIGO	Laser Interferometer Gravitational Wave Observatory
MDT	Mean Down Time
MTBF	Mean Time Between Failure
PEM	Physics Environment Monitoring System
PWR	Electrical Power System
SRD	Science Requirements Document
VE	Vacuum Equipment
WA	Washington Site
4D	Detector, 4 km long
2D	Detector, 2 km long

2.0 APPLICABLE DOCUMENTS

The documents containing LIGO reliability requirements and guidelines, reliability modeling assessment, and prediction methods, and the software used in the LIGO reliability assurance program are listed in the tables below.

TABLE 2-1. Project Documents

LIGO-M950001	LIGO Project Management Plan
LIGO - E950018, dated 03/25/96	LIGO Science Requirements Document
LIGO-E950084, dated 10/27/94	LIGO System Specification

TABLE 2-2. Basic Reliability Standards and Handbooks

MIL-STD-785	Reliability Program for Systems and Equipment Development and Prediction
MIL-STD-756	Reliability Modeling and Prediction
MIL-STD-781D	Military Standard; Reliability Testing for Engineering Development, Qualification, and Production
MIL-HDBK-781	Military Handbook; Reliability Test Methods, Plans, and Environments for Engineering Development, Qualification, and Production
MIL-HDBK-189	Reliability Growth Management
MIL-STD-1629	Failure Mode Effects and Criticality Analysis
MIL-HDBK-217F	Reliability Prediction Database
NRPD-91	Non-Electronic Parts Reliability Data, 1991, Reliability Analysis Center
	Reliability Tool Kit: Commercial Practices Edition, Rome Laboratory and Reliability Analysis Center

TABLE 2-3. Reliability Software

RELEX FMECA	Used to perform Failure Modes and Effects Analyses
RELEX Reliability Prediction	Used in calculating failure rates for hardware items.
ITEM Faultree+	Used to perform fault tree analyses

3.0 RESPONSIBILITIES

The complete design, construction, and operation of LIGO is the responsibility of the staff at California Institute of Technology (Caltech) and the Massachusetts Institute of Technology (MIT) under the terms of a cooperative Agreement (No. PHY-9210038 dated May, 1992) with the National Science Foundation (NSF). These responsibilities include assuring adequate reliability of the LIGO system.

The reliability group is an integral part of the LIGO Project System Integration Group. The responsibility of the reliability group is to:

a. Contribute to the realization of LIGO reliability and availability goals by participating in LIGO design efforts and defining reliability requirements

b. Assess the reliability of LIGO systems, subsystems, and assemblies

c. Perform reliability tradeoffs to minimize risk

3.1 STAFFING AND REPORTING

The reliability group is composed of personnel from the Product Reliability Office of the Jet Propulsion Laboratory, California Institute of Technology. The group reports directly to the LIGO System Engineer or Deputy System Engineer, as well as to the Circuit and Product Reliability Group Supervisor and the Managers of the Offices of Reliability and Quality Assurance at the Jet Propulsion Laboratory.

3.2 RELIABILITY PROGRAM DELIVERABLES

Deliverables of the reliability program are as follows:

a. Reliability Program Plan

b. Preliminary Failure Mode Effects Analysis (FMEA) of the major subsystems and assemblies

c. Preliminary Fault Tree Analyses (FTA) of the critical parts of the major subsystems and assemblies

d. Preliminary reliability assessment and tradeoff of the LIGO critical subsystems and associated assemblies and components

e. Final analyses as in b through d

f. Component and/or assemblies logistic sparing plan

g. Final LIGO reliability and availability assessment report

4.0 RELIABILITY ASSESSMENT

LIGO system reliability will be assessed by means of :

- Reliability and Availability Prediction
- Failure Mode Effects Analysis
- Fault Tree Analysis

The RELEX software package will be used to perform the reliability/availability prediction, failure-mode-effects and fault tree analyses.

4.1 RELIABILITY AND AVAILABILITY PREDICTION

4.1.1 Reliability Modeling

The top level reliability block diagram of the LIGO system is shown in Figure 4.1.1. The LIGO system reliability block diagram is a series model which consists of a detector system, vacuum system, and facilities infrastructure. Failures of the support equipment, beam tube enclosure, and building structures have minimum effect on the overall LIGO system function and are excluded from the reliability model.

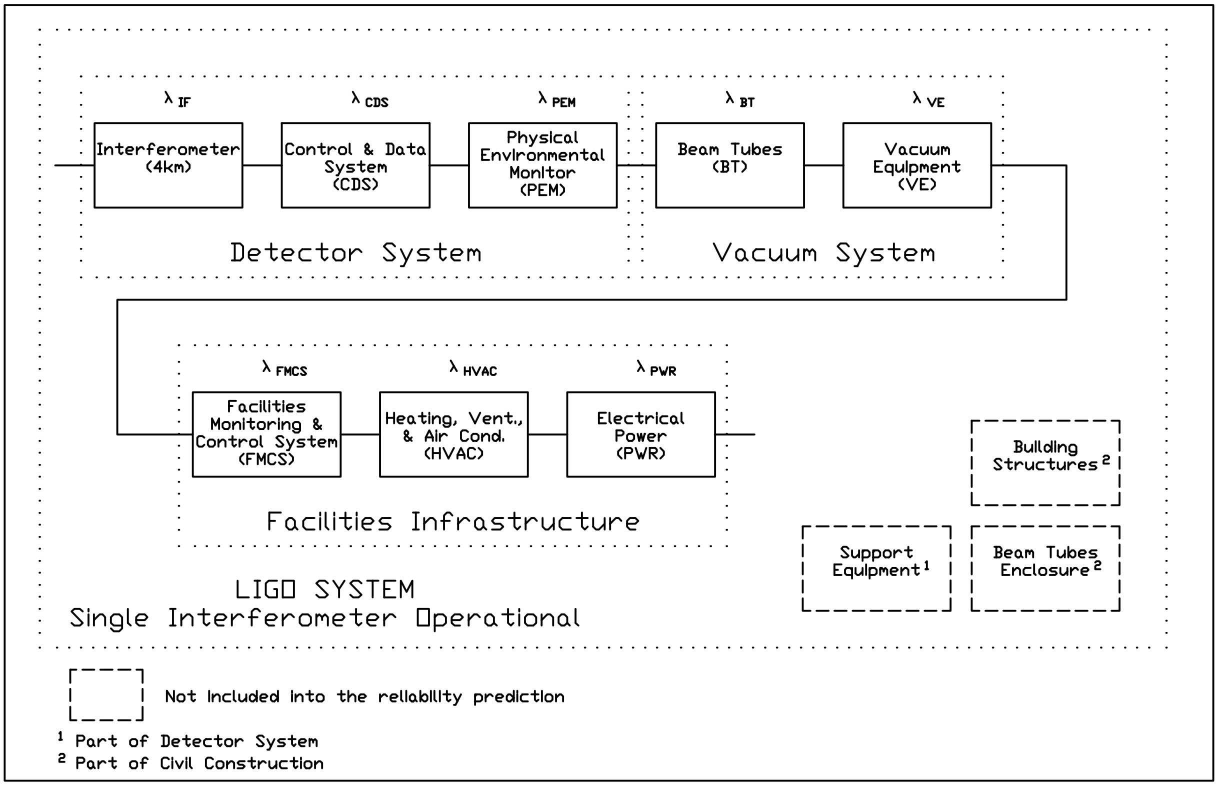

λ IF
λ CDS
λ PEM
λ BT
λ VE
Interferometer (4km)
Control & Data System (CDS)
Physical Environmental Monitor (PEM)
Beam Tubes (BT)
Vacuum Equipment (VE)
Detector System
Vacuum System
λ FMCS
λ HVAC
λ PWR
Facilities Monitoring & Control System (FMCS)
Heating, Vent., & Air Cond. (HVAC)
Electrical Power (PWR)
Facilities Infrastructure
Building Structures 2
Support Equipment 1
Beam Tubes Enclosure 2
LIGO SYSTEM
Single Interferometer Operational
Not included into the reliability prediction
1 Part of Detector System
2 Part of Civil Construction

Figure 4.1.1: LIGO Top Level Reliability Block Diagram

4.1.2 Modes of Operation

LIGO system is comprised of two remotely located observatory sites located at Hanford, Washington and at Livingston, Louisiana. The Washington site consists of two interferometers, 4km and 2km, and the Louisiana site consists of one 4km interferometer. Per the LIGO SRD, the LIGO system will operate in one of the following three modes:

a. Single Operations Mode (1X): At least one of three interferometers is operational (Reference Fig. 4.1.1)

b. Double Operations Mode (2X): At least two interferometers are operational. One of which must be the Louisiana interferometer.

c. Triple Operations Mode (3X): All three interferometers are operational

A Venn Diagram depicting the three operational modes is shown in Figure 4.1.2

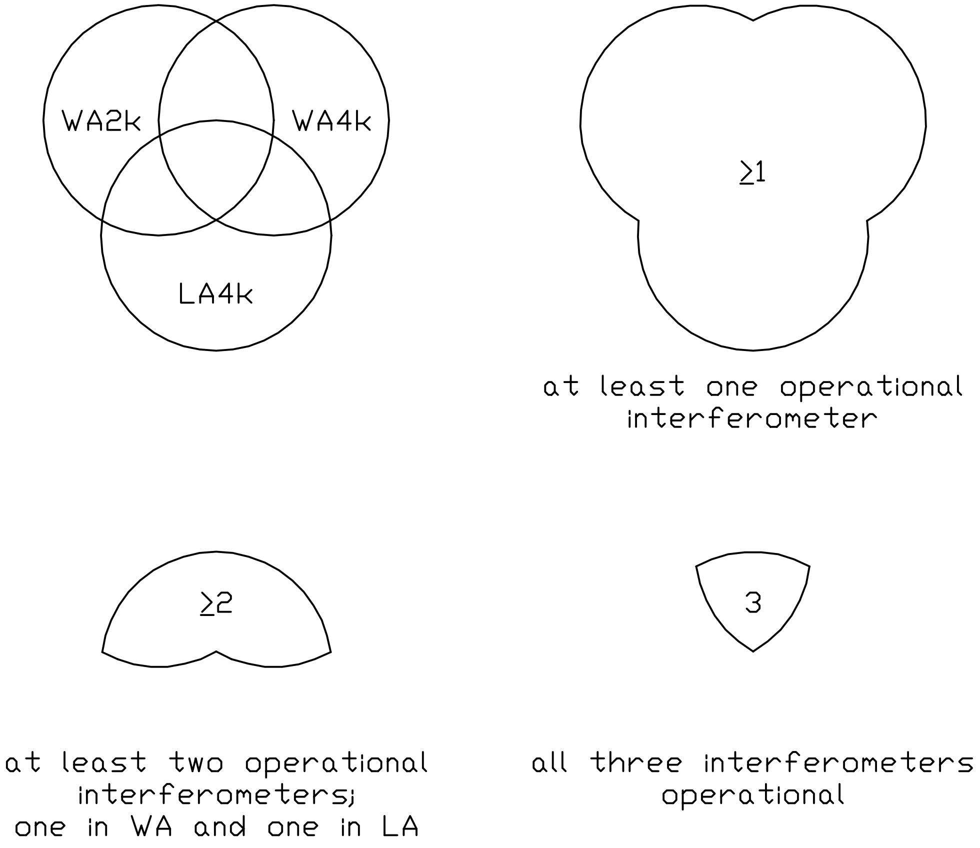

WA2k
WA4k
LA4k
≥1
at least one operational interferometer
≥2
3
at least two operational interferometers; one in WA and one in LA
all three interferometers operational

Figure 4.1.2: The Three Modes of LIGO Operation

4.1.3 System Reliability Requirements

LIGO top level system reliability requirements are summarized in Table 4.1.3

Table 4.1.3: LIGO System Reliability Requirements

Modes of Operation	**Availability per year, A**	**Minimum Continuous Operating Period, $MTBF_{min}$**	**Max System Failure Rate, λ_{max}[1] (failures/10^6 hrs)**
1X	90%	40 hrs	25,000
2X	85%	100 hrs	10,000
3X	75%	100 hrs	10,000

[1] $\lambda_{max}=1/MTBF_{min}$

4.1.4 Assumptions

Assumptions used for derivation of system availability equations:

- The 4km and 2km interferometers have similar failure rates (λ_{IF})
- The failure rates of other LIGO assemblies (CDS, PEM, BT and VE) in Washington are similar to the ones in Louisiana.
- Failure rates are for hardware failures. It is assumed that the software has been validated prior to commencement of operations. Therefore, software failures are excluded from the hardware reliability calculations. Software failures will be accounted for in the system availability calculations as a contributing factor to the system's Mean-Down-Time (MDT).
- The support equipment, beam tube enclosure, and building structures are excluded from the overall LIGO system reliability model.
- Based upon the established design criteria, it is assumed that the influence of the environment on system availability will be negligible.

4.1.5 Reliability Assessment

The LIGO Science Requirements Document, specifies an Availability, A(t), requirement for the LIGO System. Availability allows a trade-off between LIGO System reliability, R(t), and LIGO Mean Down Time (MDT). MDT includes unscheduled maintenance, scheduled maintenance and any logistics delays associated with either one. Since there is no specific requirement for R(t), the reliability for the three operational modes will be assessed using the constant failure rate model. The LIGO system reliability block diagrams (Figures B.2.1-B.2.3) and the derivation of the following reliability equations are presented in Appendix B. Reliability definition and general reliability modeling are discussed in Appendix A.

Assuming a constant failure rate, the reliability of individual LIGO assemblies (i.e., CDS, PEM, etc.) can be determined by:

$R_i(t) = e^{-(\lambda \cdot t)}$ where t = operation time

From the reliability block diagrams (Figure B.2.1 - B.2.3 in Appendix B), the reliability for the three LIGO operating modes can be mathematically represented as follows:

a. Reliability for 1X mode:

$$R_{1X}(t) = [R_{LA}(t) + R_{WA}(t) - (R_{LA}(t) \cdot R_{WA}(t))]$$

Where:

$$R_{LA}(t) = R_{IF}(t) \cdot R_{CDS}(t) \cdot R_{PEM}(t) \cdot R_{BT}(t) \cdot R_{VE}(t) \cdot R_{FMCS}(t) \cdot R_{HVAC}(t) \cdot R_{PWR}(t)$$

$$R_{WA}(t) = [R_{2D}(t) + R_{4D}(t) - (R_{2D}(t) \cdot R_{4D}(t))] \cdot R_{CMN}(t)$$

And:

$$R_{2D}(t) = R_{IF2K}(t) \cdot R_{CDS2K}(t) \cdot R_{PEM2K}(t) \cdot R_{VE2K}(t)$$

$$R_{4D}(t) = R_{IF4K}(t) \cdot R_{CDS4K}(t) \cdot R_{PEM4K}(t) \cdot R_{VE4K}(t)$$

$$R_{CMN}(t) = R_{CDSCMN}(t) \cdot R_{PEMCMN}(t) \cdot R_{BT}(t) \cdot R_{VECMN}(t) \cdot R_{FMCS}(t) \cdot R_{HVAC}(t) \cdot R_{PWR}(t)$$

Note: For the purposes of this plan, a general reliability model has been presented. The model will be refined during the course of the actual analyses as the LIGO design develops. Therefore, in the initial analysis, it will be assumed that, at the Washington Observatory, the PEM Systems associated with the 2 km interferometer and the 4 km interferometer will be common.

b. Reliability for 2X mode:

$$R_{2X}(t) = (R_{LA}(t) \cdot R_{WA}(t))$$

c. Reliability for 3X mode:

$$R_{3X}(t) = R_{IF2}(t) \cdot (R_{IF4}(t))^2 \cdot (R_{OpEquip}(t))^2$$

where:

$$R_{OpEquip}(t) = R_{CDS}(t) \cdot R_{PEM}(t) \cdot R_{BT}(t) \cdot R_{VE}(t) \cdot R_{FMCS}(t) \cdot R_{HVAC}(t) \cdot R_{PWR}(t)$$

4.1.6 System Availability

The availability of a system can be expressed in terms of failure rate, λ, and Mean Down Time, MDT:

$$A = \frac{MTBF}{MTBF + MDT} = \frac{1}{1 + \frac{MDT}{MTBF}} = \frac{1}{1 + \lambda \cdot MDT} \qquad \text{where}$$

the failure rate (λ) is related to Mean Time Between Failure (MTBF) by:

$$\lambda = \frac{1}{MTBF}$$

Hence, the system availability for the 1X, 2X, and 3X modes of operation are:

$$A_{1x} = \frac{1}{1 + \lambda_{1x} \cdot MDT_{1x}}$$

$$A_{2x} = \frac{1}{1 + \lambda_{2x} \cdot MDT_{2x}}$$

$$A_{3x} = \frac{1}{1 + \lambda_{3x} \cdot MDT_{3x}}$$

The 1X system failure rate, λ_{1x}, will be:

$$\lambda_{1x}(t) = \frac{-\ln(R_{1x}(t))}{t}$$

The 2X system failure rate, λ_{2x}, will be:

$$\lambda_{2x}(t) = \frac{-\ln(R_{2x}(t))}{t}$$

Since most assemblies within the system are in series for the 2X mode, with the exception of the redundant interferometers (Figure B.2.2), the system failure rate can be approximated by:

$$\lambda_{2x} \approx \frac{5}{3}\lambda_{IF} + 2\lambda_{OpEquip} \quad \text{where}$$

$$\lambda_{OpEquip} = \lambda_{CDS} + \lambda_{PEM} + \lambda_{BT} + \lambda_{VE} + \lambda_{FMCS} + \lambda_{HVAC} + \lambda_{PWR}$$

The 3X system failure rate, λ_{3x}, will be:

$$\lambda_{3x}(t) = \frac{-\ln(R_{3x}(t))}{t} \quad \text{or} \quad \lambda_{3x} = 3\lambda_{IF} + 2\lambda_{OpEquip}$$

4.1.7 Analysis Method and Recommendations

Assembly failure rates are predicted using vendor failure rate data, MIL-HDBK-217, NRPD-91 or engineering estimates at the component level. System failure rates for each operating mode, λ_{1x}, λ_{2x}, and λ_{3x} are calculated using system failure rate equations in section 4.1.6. The allowable Mean Down Time, MDT, is then determined from the availability equations in section 4.1.6 for each operational mode. The predicted system failure rates should be less than or equal to the maximum failure rates derived from the requirement ($\lambda_{max.}$ in Table 4.1.3).

From the reliability models shown in Figures B.2.1 to B.2.3 of Appendix B, the system failure rate should be lowest for the 1X mode with system redundancy and highest for the 3X mode with no redundancy. By definition, MTBF is inversely proportional to the system failure rate. Hence, the MTBF for the LIGO system should increase in the order of $MTBF_{3x}$<$MTBF_{2x}$< $MTBF_{1x}$.

For the same reason, to satisfy the availability requirement, the allowable MDT for the three operational modes will be $MDT_{1x} < MDT_{2x} < MDT_{3x.}$

4.1.8 Availability In Terms of Reliability Growth Assessment

The analysis presented in section 4.1.6 assumed a constant failure rate. In reality, during the course of operation, the LIGO system will undergo continuous failure corrections and will consider instrumentation upgrades as new technologies are developed. It can be expected that reliability growth, or degradation, may occur as a result of these failure corrections and/or instrumentation upgrades. Appendix E details an approach to predicting and tracking the reliability, and subsequent availability, growth during the course of these system design changes.

4.2 FAILURE MODES AND EFFECTS ANALYSIS

The Failure Mode and Effects Analysis (FMEA) is used to study the effects of single failure modes on subsystem and system operation and to classify each potential failure according to its severity. The FMEA will be performed in two steps:

1. Preliminary FMEA, concurrent with the subsystem preliminary design, updated as the design information becomes available
2. Final FMEA, when the design is near completion

FMEA will identify assemblies and components that constitute high risk for the system premature failure that may compromise achievement of the system availability goals. The analysis will be performed based on the guidelines of MIL-STD-1629A. The analysis will include the following items:

- Functional block diagrams of overall LIGO system and individual assemblies (i.e., Control Data System, Physics Environment Monitoring System, Beam Tube and Vacuum System)
- Functional descriptions for system and assemblies, including any design redundancy
- FMEA worksheets (See Appendix C)

4.3 FAULT TREE ANALYSIS

A Fault Tree Analysis (FTA) is a systematic, deductive methodology for defining a single specific undesirable event and determining all possible failures that could cause that event to occur. The undesired event, usually a critical system failure, constitutes the top event in a fault tree diagram. While the FMEA uses a bottoms up approach, the FTA uses a top down approach; the two techniques complement each other. For a system with little or no redundancy, an FMEA is probably the best approach, but for a complex system, with lots of back up, an FTA is usually recommended.

A fault tree will be prepared for the LIGO assemblies considered critical to the operability of a subsystem. Starting with the resultant event (a subsystem or assembly failure), a corresponding fault tree will be constructed to determine causes of the faults to the basic events. Based on the estimated failure rates of the basic event, the probability of the resultant event will be calculated. The will indicate whether or not there is a necessity for the design improvement. The results will be verified through Monte Carlo simulations contained in the RELEX software. Appendix D includes a description of symbols and procedures used for constructing fault trees.

5.0 SPARE PART PLANNING

Spare parts will be planned based on their determined failure frequency or the expected/calculated wearout. An important factor to be considered in the spare parts planning is the part market availability, the lead times and the part technology. It will also be necessary to plan for spare parts in the case of part obsolescence, even if the part failure rate is expected to be low.

Planning of the spare parts will start as the design of subsystems is finalized.

6.0 REVIEW OF VENDOR AND TEST DOCUMENTATION

6.1 REVIEW OF QUALITY ASSURANCE, RELIABILITY, AND OTHER RELEVANT DOCUMENTATION

Available vendor documentation will be examined for information relevant to reliability and availability estimation and assurance. Failure rate information, if available, will be verified and used for LIGO reliability and availability estimates.

6.2 REVIEW AND ANALYSIS OF THE VENDOR AND IN-HOUSE DATA

All available test records of components, assemblies and subsystems will be reviewed and analyzed to gain failure rate (λ) estimates, failure rate behavior (increase or decrease) or failure probability information. If available, the information from the test records will be used to estimate and verify LIGO assemblies and subsystems failure rates.

7.0 RELIABILITY PROGRAM REVIEWS

LIGO reliability personnel will participate in program reviews as deemed necessary by LIGO Management to collect pertinent program information and/or to present LIGO reliability issues.

8.0 LIGO RELIABILITY AND AVAILABILITY REPORT

After the completion of the LIGO design and integration, a formal report will be prepared on the LIGO system reliability and availability.

9.0 SUBSYSTEM AVAILABILITY ALLOCATIONS

The subsystem availability allocations are derived from the observatory availability requirement for the triple coincidence (3X) mode of operation. With respect to availability, the triple coincidence (3X) mode of operation represents the worst case operating scenario. The subsystem availability requirements are summarized in Table 9.0 and the respective fault tree diagrams are provided in Appendix F. The 4km interferometer and the 2km interferometer were assumed to be of equal complexity. Therefore, the subsystems at the Washington Observatory were assumed to be twice as complex as the respective subsystems at the Louisianna Observatory. As a result, the Washington Observatory subsystem MTBMCF values are half of the Louisianna Observatory subsystem MTBMCF values. The Beam Tube, Facilities Monitoring and Control System, Heating, Ventilation and Air Conditioning, and Electrical Power are exceptions to this rule. These four subsystems were considered to be of equal complexity at each observatory.

The Mean-Time-Between-Mission-Critical-Failure (MTBMCF) is the mean time between susbystem failures which would jeopardize the collection and validation of science data. The MTBMCF takes into consideration equipment redundancies which might be present within the subsystem.

Mean-Down-Time (MDT) is the total preventive and corrective maintenance time divided by the total number of preventive and corrective maintenance actions for a given subsystem. Logistic delays are included in the calculation of preventive and corrective maintenance times. The subsystem MDT requirements are based upon subsystem size, complexity, as well as the fact that some subsystems may require a bake-out following maintenance actions. The MDT requirement should be used as a guide in the development of on-site spares and maintenance support policies.

Availability is defined as the ability of an item, under the combined aspects of its reliability and maintenance, to perform its required function over a given period of time. Mathematically, Availability is approximated as:

$$A = \frac{MTBMCF}{MTBMCF + MDT}$$

Therefore, since availability allows for trade-offs between reliability (MTBMCF) and maintenance (MDT), the subsystem availability allocations are the design constraints which must be met in order to achieve the desired level of observatory availability.

TABLE 9-1. Subsystem Availability Allocations

SUBSYSTEM	*OBSERVATORY*					
	LOUISIANA			*WASHINGTON*		
	MTBMCF *(Op. Hours)*	*MDT* *(Hours)*	*A*	*MTBMCF* *(Op. Hours)*	*MDT* *(Hours)*	*A*
CDS C&M	17, 600	24	0.9986	8, 800	24	0.9973
CDS DAQ	17, 600	24	0.9986	8, 800	24	0.9973
CDS Infrastructure	17, 600	24	0.9986	8, 800	24	0.9973
VCMS	17, 600	24	0.9986	8, 800	24	0.9973
ASC	20, 000	72	0.9964	10, 000	72	0.9929
LSC	20, 000	72	0.9964	10, 000	72	0.9929
COC	26, 000	72	0.9972	13, 000	72	0.9945
COS	24, 000	72	0.9970	12, 000	72	0.9940
IOO	10, 000	72	0.9929	5, 000	72	0.9858
PSL	5, 000	72	0.9858	2, 500	72	0.9720
SEI	13, 000	72	0.9945	6, 500	72	0.9890
SUS	13, 000	72	0.9945	6, 500	72	0.9890
PEM	17, 600	24	0.9986	8, 800	24	0.9973
BT	35, 000	1, 460	0.9600	35, 000	1, 460	0.9600
FMCS	17, 600	24	0.9986	17, 600	24	0.9986
HVAC	17, 600	72	0.9959	17, 600	72	0.9959
ELEC. PWR.	8, 800	24	0.9973	8, 800	24	0.9973
VE	8, 800	72	0.9919	4, 400	72	0.9839

Appendix A

Reliability Definitions and Modeling

A.1.0 Reliability Definitions

A System operational availability

MTBF Mean Time Between Failures

MDT Mean Down Time consisting of:

MTTR Mean Time To Repair
This time is calculated based on the time required by an average skilled service engineer to diagnose the failure and restore the system to its normal operation condition, given that the required spare parts are immediately available.

LDT Logistic Delay Time
The administrative delay time, part delivery or procurement time, service request and schedule time, and time to prepare the diagnostic equipment.

MSMT Mean Schedule Maintenance Time
The mean time to perform a schedule system maintenance, not related to a failure occurrence.

λ Failure rate

R(t) Probability of success or system reliability

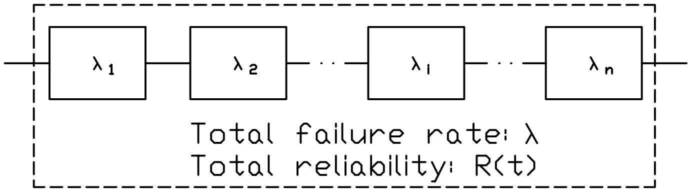
$\rho(t)$ System failure intensity (rate)

β Reliability growth rate

A.1.1 Reliability Modeling

The following reliability modeling equations will be used based upon the particular mode of operation.

a. Series configuration



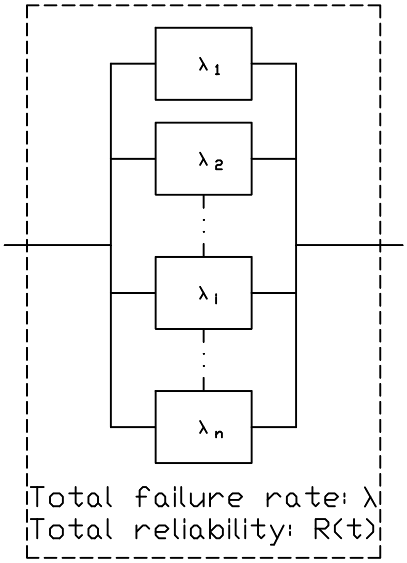
If constant failure rate assumed:

$$\lambda = \sum_{i=1}^{n} \lambda$$

$$R_i(t) = e^{-\lambda_i t}$$

$$R(t) = \prod_{i=1}^{n} R_i(t) = \prod_{i=1}^{n} e^{-\lambda_i t} = e^{-\left(\sum_{i=1}^{n} \lambda_i\right) t}$$

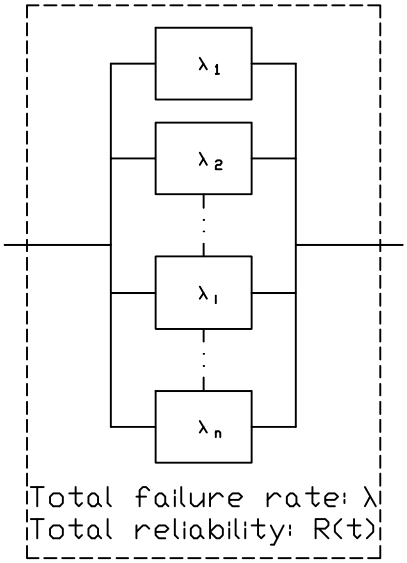
b. Parallel redundant configuration, different or identical units, at least one of the redundant units must be operational.



$$R(t) \ = \ 1 - \prod_{i\,=\,1}^{n} [1 - R_i(t)]$$

$$\lambda \ = \ \frac{1}{\int_0^\infty \left\{ 1 - \prod_{i\,=\,1}^{n} [1 - R_i(t)] \right\} dt}$$

c. Parallel configuration, identical units, m out of n available units must be operational



$$R(t) = 1 - \sum_{i=0}^{m-1} \frac{n!}{i! \cdot (n-i)!} \cdot [R_1(t)]^i \cdot [1 - R_1(t)]^{(n-i)}$$

$$R(t) = 1 - \sum_{i=0}^{m-1} \frac{n!}{i! \cdot (n-i)!} \cdot [e^{\lambda_1 \cdot t}]^i \cdot [1 - e^{\lambda_1 \cdot t}]^{(n-i)}$$

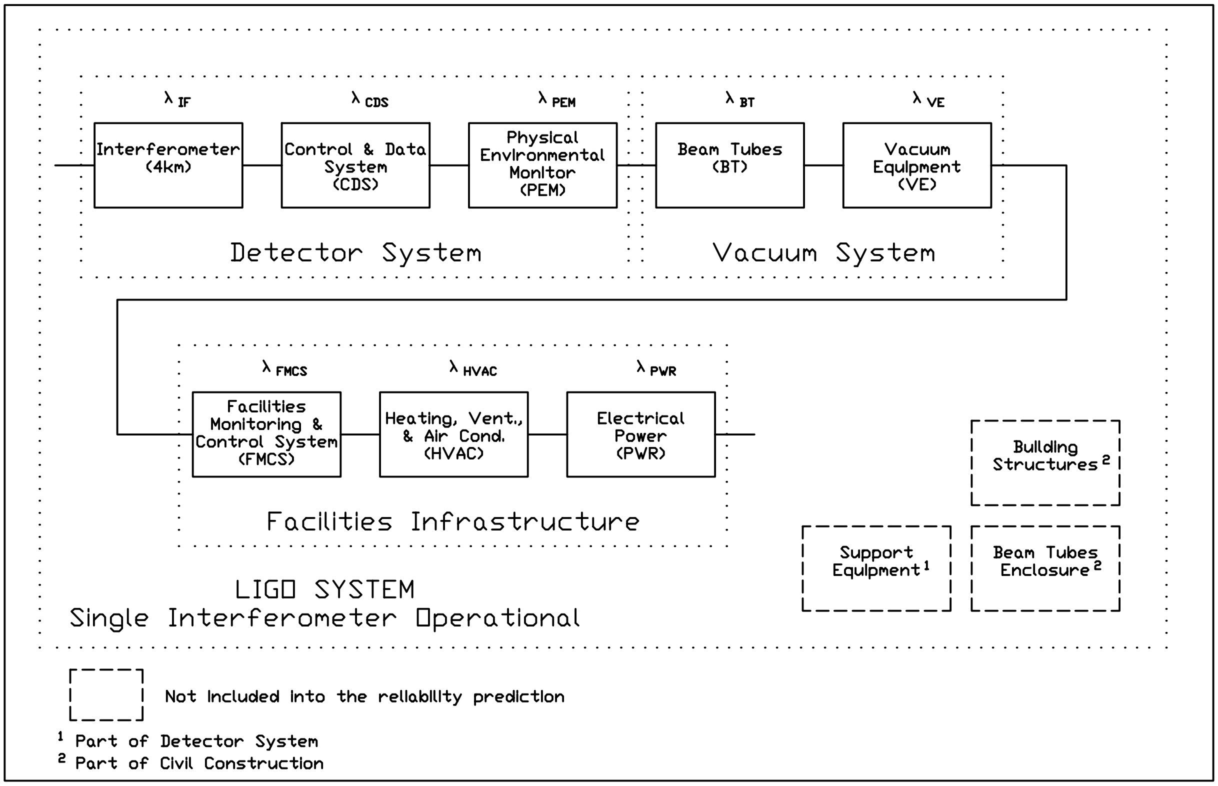
$$\lambda = \frac{\lambda_1}{\sum_{i=m}^{n} \frac{1}{i}}$$

Appendix B

Derivations for LIGO Reliability

B.1.0 LIGO System Reliability Modeling

The LIGO system mainly consists of a detector system, vacuum system, and a facilities infrastructure as shown in Figure B.1.1. The support equipment, beam tube enclosure and the building structures are assumed to have minimum contributions to the failure rate of the LIGO system and are excluded from the reliability prediction. The support equipment mainly consists of oscilloscopes and some non-essential mechanical parts. The beam tube enclosure, a concrete structure, and the building structures will have minimum effect on the failure of the LIGO operation.


λ IF
λ CDS
λ PEM
λ BT
λ VE
Interferometer (4km)
Control & Data System (CDS)
Physical Environmental Monitor (PEM)
Beam Tubes (BT)
Vacuum Equipment (VE)
Detector System
Vacuum System
λ FMCS
λ HVAC
λ PWR
Facilities Monitoring & Control System (FMCS)
Heating, Vent., & Air Cond. (HVAC)
Electrical Power (PWR)
Facilities Infrastructure
Building Structures 2
Support Equipment 1
Beam Tubes Enclosure 2
LIGO SYSTEM
Single Interferometer Operational
Not Included into the reliability prediction
1 Part of Detector System
2 Part of Civil Construction

[1] Part of Detector System

[2] Part of Civil Construction

Figure B.1.1: LIGO Top Level Reliability Block Diagram (Louisiana)

Figure B.1.1 above is a representation of the single LIGO system at Louisiana with the 4Km interferometer. The system at Washington consists of two interferometers, 2Km and 4Km, in addition to the other assemblies within the vacuum and detector systems. The system reliability block diagram for the Washington site can be modeled by two configurations as shown in Figures B.1.2 and B.1.3. Figure B.1.2 shows the reliability model with both interferometers required for the 3X mode. Figure B.1.3 shows the reliability model with 1 of the 2 interferometers required for the 2X and 1X modes as defined in section 4.1.2.

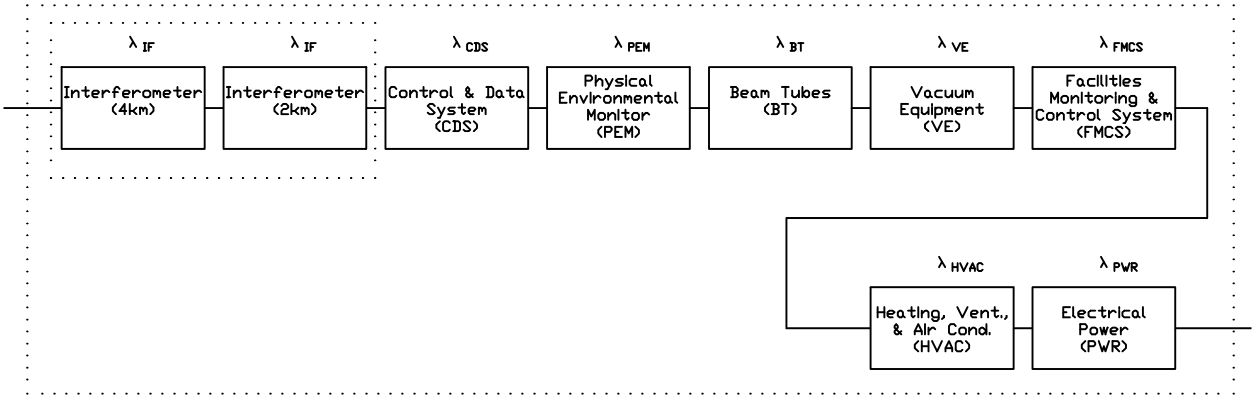

λ IF
λ IF
λ CDS
λ PEM
λ BT
λ VE
λ FMCS
Interferometer (4km)
Interferometer (2km)
Control & Data System (CDS)
Physical Environmental Monitor (PEM)
Beam Tubes (BT)
Vacuum Equipment (VE)
Facilities Monitoring & Control System (FMCS)
λ HVAC
λ PWR
Heating, Vent., & Air Cond. (HVAC)
Electrical Power (PWR)

Figure B.1.2: LIGO System Reliability Block Diagram at Washington
with both interferometers required

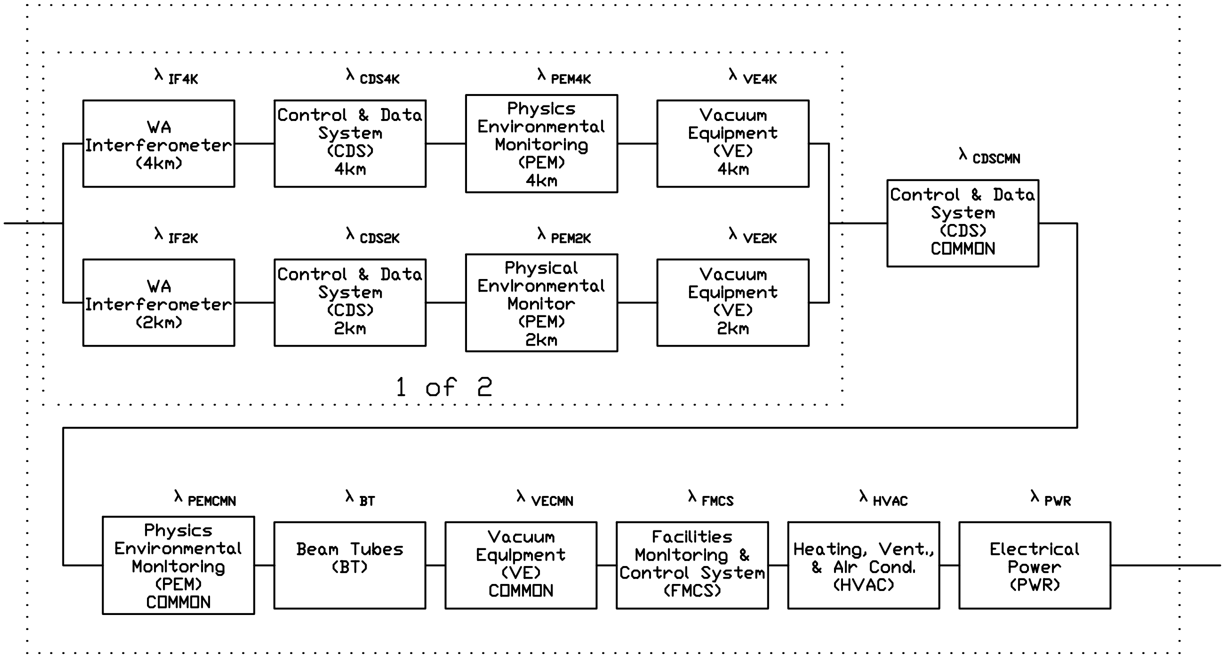

λ IF4K
λ CDS4K
λ PEM4K
λ VE4K
WA Interferometer (4km)
Control & Data System (CDS) 4km
Physics Environmental Monitoring (PEM) 4km
Vacuum Equipment (VE) 4km
λ CDSCMN
Control & Data System (CDS) COMMON
λ IF2K
λ CDS2K
λ PEM2K
λ VE2K
WA Interferometer (2km)
Control & Data System (CDS) 2km
Physical Environmental Monitor (PEM) 2km
Vacuum Equipment (VE) 2km
1 of 2
λ PEMCMN
λ BT
λ VECMN
λ FMCS
λ HVAC
λ PWR
Physics Environmental Monitoring (PEM) COMMON
Beam Tubes (BT)
Vacuum Equipment (VE) COMMON
Facilities Monitoring & Control System (FMCS)
Heating, Vent., & Air Cond. (HVAC)
Electrical Power (PWR)

Figure B.1.3: LIGO System Reliability Block Diagram at Washington
with 1 of 2 interferometers required

B.2.0 Reliability Modeling for 1X. 2X. and 3X Operating Modes:

Details for the modes of operation, system requirements, and assumptions are summarized in sections 4.1.2 to 4.1.4. The reliability block diagrams for three different modes of operations are presented as follows:

a. 1X Mode:

The 1X mode implies that at least one out of three available LIGO interferometers (2 in Washington and 1 in Louisiana) must be operational. The overall system reliability block diagram for the 1X mode is shown in Figure B.2.1

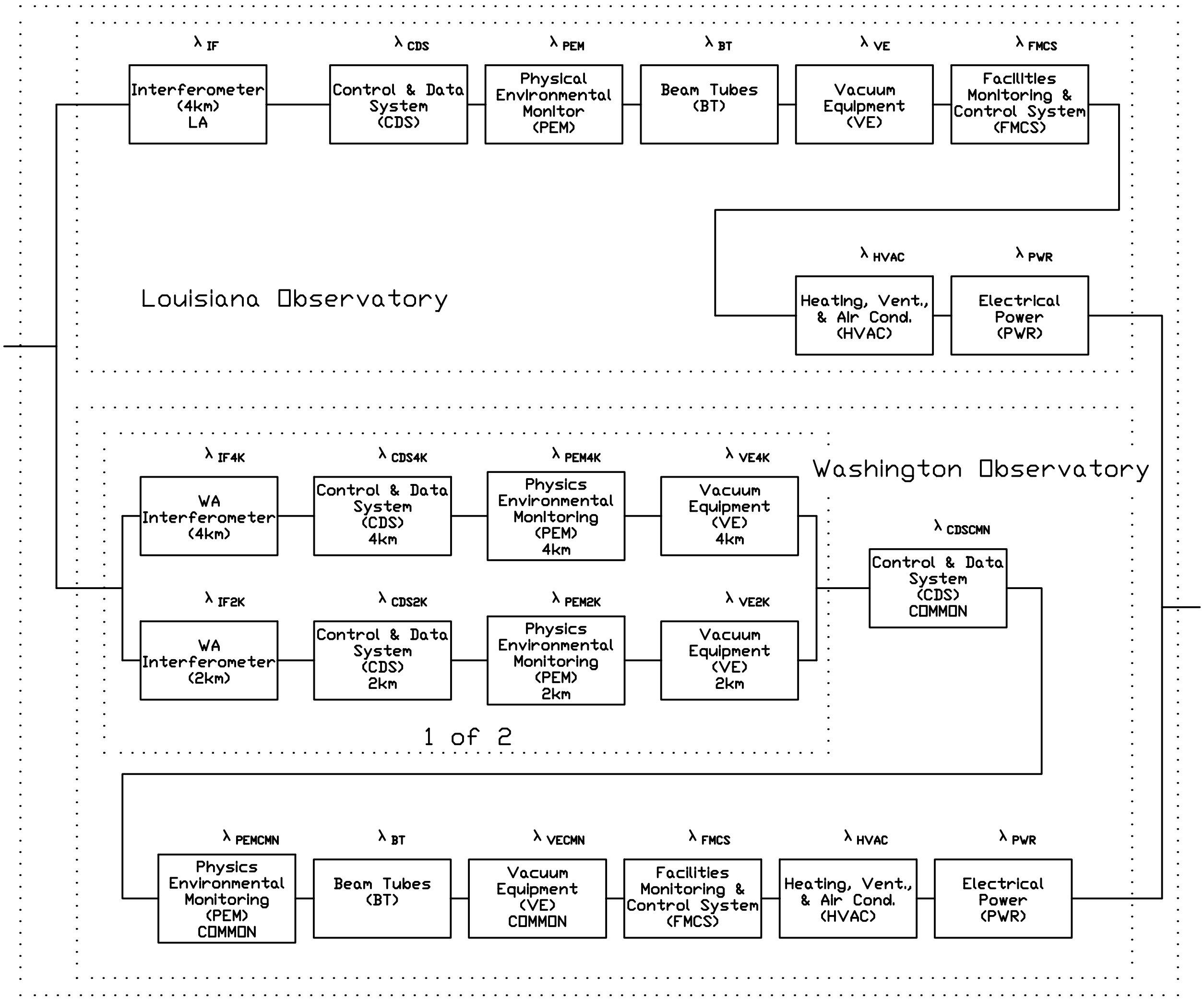

λ IF
Interferometer (4km) LA
λ CDS
Control & Data System (CDS)
λ PEM
Physical Environmental Monitor (PEM)
λ BT
Beam Tubes (BT)
λ VE
Vacuum Equipment (VE)
λ FMCS
Facilities Monitoring & Control System (FMCS)
λ HVAC
Heating, Vent., & Air Cond. (HVAC)
λ PWR
Electrical Power (PWR)
Louisiana Observatory
Washington Observatory
λ IF4K
WA Interferometer (4km)
λ CDS4K
Control & Data System (CDS) 4km
λ PEM4K
Physics Environmental Monitoring (PEM) 4km
λ VE4K
Vacuum Equipment (VE) 4km
λ IF2K
WA Interferometer (2km)
λ CDS2K
Control & Data System (CDS) 2km
λ PEM2K
Physics Environmental Monitoring (PEM) 2km
λ VE2K
Vacuum Equipment (VE) 2km
1 of 2
λ CDSCMN
Control & Data System (CDS) COMMON
λ PEMCMN
Physics Environmental Monitoring (PEM) COMMON
λ BT
Beam Tubes (BT)
λ VECMN
Vacuum Equipment (VE) COMMON
λ FMCS
Facilities Monitoring & Control System (FMCS)
λ HVAC
Heating, Vent., & Air Cond. (HVAC)
λ PWR
Electrical Power (PWR)

Figure B.2.1: 1X Configuration

Assuming a constant failure rate:

$R(t) = \exp(-\lambda \cdot t)$ where t = operation time

The mathematical model for LIGO 1X system reliability is:

$R_{1x}(t) = R_{LA}(t) + R_{WA}(t) - R_{LA}(t)R_{WA}(t)$ (B.2.1)

Therefore, the failure rate for the 1X mode is:

$$\lambda_{1X}(t) = \frac{-\ln(R_{1X}(t))}{t}$$

The reliability for the system at Louisiana, $R_{LA}(t)$, will be:

$$R_{LA}(t) = R_{IF}(t) \cdot R_{CDS}(t) \cdot R_{PEM}(t) \cdot R_{BT}(t) \cdot R_{VE}(t) \cdot R_{FCMS}(t) \cdot R_{HVAC}t \cdot R_{PWR}(t)$$

The reliability of the system at Washington, $R_{WA}(t)$, will be:

$$R_{WA}(t) = [R_{2D}(t) + R_{4D}(t) - R_{2D}(t) \cdot R_{4D}(t)] \cdot R_{CMN}(t)$$

Where:

$$R_{2D}(t) = R_{IF2K}(t) \cdot R_{CDS2K}(t) \cdot R_{PEM2K}(t) \cdot R_{VE2K}(t)$$

$$R_{4D}(t) = R_{IF4K}(t) \cdot R_{CDS4K}(t) \cdot R_{PEM4K}(t) \cdot R_{VE4K}(t)$$

$$R_{CMN}(t) = R_{CDSCMN}(t) \cdot R_{PEMCMN}(t) \cdot R_{BT}(t) \cdot R_{VECMN}(t) \cdot R_{FMCS}(t) \cdot R_{HVAC}(t) \cdot R_{PWR}(t)$$

b. 2X Mode:

The 2X mode of operation requires at least 2 of interferometers operational in coincidence, one at Louisiana and one at Washington. The overall system reliability block diagram for 2X mode can be represented as “1 out of 2” interferometer redundancy at the Washington observatory, as shown in Figure B.2.2.

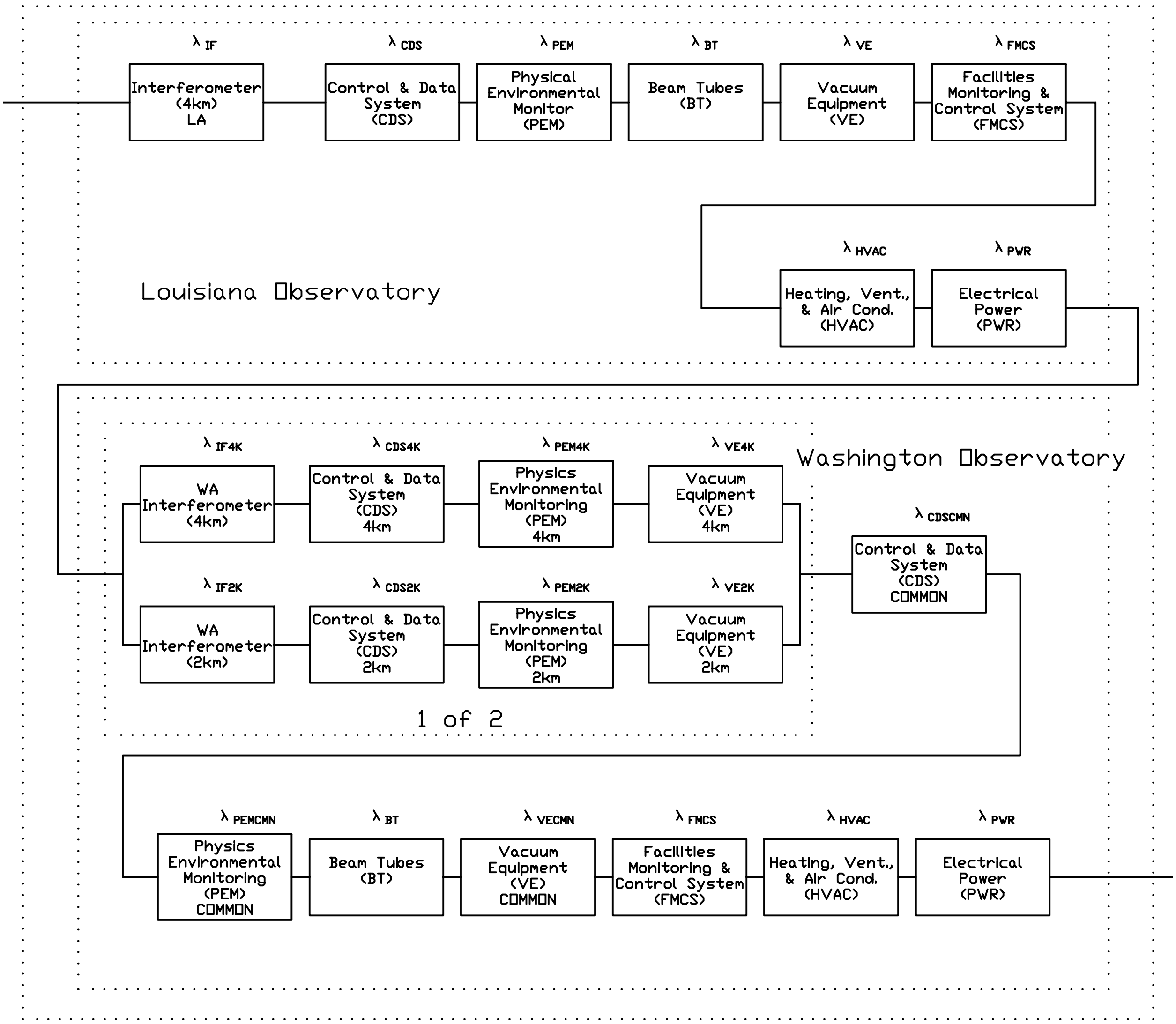

λ IF
Interferometer (4km) LA
λ CDS
Control & Data System (CDS)
λ PEM
Physical Environmental Monitor (PEM)
λ BT
Beam Tubes (BT)
λ VE
Vacuum Equipment (VE)
λ FMCS
Facilities Monitoring & Control System (FMCS)
λ HVAC
Heating, Vent., & Air Cond. (HVAC)
λ PWR
Electrical Power (PWR)
Louisiana Observatory
Washington Observatory
λ IF4K
WA Interferometer (4km)
λ CDS4K
Control & Data System (CDS) 4km
λ PEM4K
Physics Environmental Monitoring (PEM) 4km
λ VE4K
Vacuum Equipment (VE) 4km
λ IF2K
WA Interferometer (2km)
λ CDS2K
Control & Data System (CDS) 2km
λ PEM2K
Physics Environmental Monitoring (PEM) 2km
λ VE2K
Vacuum Equipment (VE) 2km
1 of 2
λ CDSCMN
Control & Data System (CDS) COMMON
λ PEMCMN
Physics Environmental Monitoring (PEM) COMMON
λ BT
Beam Tubes (BT)
λ VECMN
Vacuum Equipment (VE) COMMON
λ FMCS
Facilities Monitoring & Control System (FMCS)
λ HVAC
Heating, Vent., & Air Cond. (HVAC)
λ PWR
Electrical Power (PWR)

Figure B.2.2: 2X Configuration

The 2X reliability mathematical model will be:

$$R_{2x}(t) = R_{LA}(t) \cdot R_{WA}(t) \qquad \text{(B.2.2)}$$

Where:

$$R_{LA}(t) = R_{IF}(t) \cdot R_{CDS}(t) \cdot R_{PEM}(t) \cdot R_{BT}(t) \cdot R_{VE}(t) \cdot R_{FCMS}(t) \cdot R_{HVAC}t \cdot R_{PWR}(t)$$

$$R_{WA}(t) = [R_{2D}(t) + R_{4D}(t) - R_{2D}(t) \cdot R_{4D}(t)] \cdot R_{CMN}(t)$$

And:

$$R_{2D}(t) = R_{IF2K}(t) \cdot R_{CDS2K}(t) \cdot R_{PEM2K}(t) \cdot R_{VE2K}(t)$$

$$R_{2D}(t) = R_{IF4K}(t) \cdot R_{CDS4K}(t) \cdot R_{PEM4K}(t) \cdot R_{VE4K}(t)$$

$$R_{CMN}(t) = R_{CDSCMN}(t) \cdot R_{PEMCMN}(t) \cdot R_{BT}(t) \cdot R_{VECMN}(t) \cdot R_{FMCS}(t) \cdot R_{HVAC}(t) \cdot R_{PWR}(t)$$

The 2X system failure rate will be:

$$\lambda_{2X}(t) = \frac{\ln(R_{2X}(t))}{t}$$

Since most of items in this mode are in series with the exception of the redundant interferometers at Washington, the system failure rate for 2X can be approximated by:

$$\lambda_{OpEquip} = \lambda_{CDS} + \lambda_{PEM} + \lambda_{BT} + \lambda_{VE} + \lambda_{FMCS} + \lambda_{HVAC} + \lambda_{PWR}$$

$$\lambda_{2X} \approx \left[\frac{\lambda_{IF}}{\sum_{i=1}^{2} \frac{1}{i}} + \lambda_{IF} \right] + 2\lambda_{OpEquip} \approx \left[\frac{\lambda_{IF}}{\frac{1}{1} + \frac{1}{2}} + \lambda_{IF} \right] + 2\lambda_{OpEquip} \approx \frac{5}{3}\lambda_{IF} + 2\lambda_{OpEquip}$$

c. 3X Mode:

The 3X mode requires simultaneous operation of all three LIGO interferometers. A reliability block diagram of the 3X mode is shown in Figure B.2.3

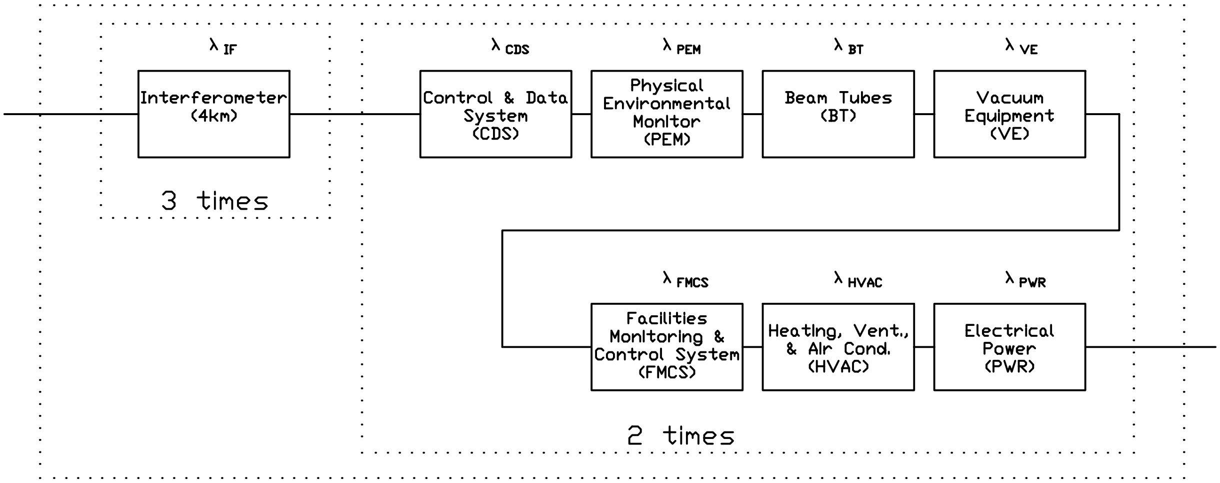

λ IF
Interferometer (4km)
3 times
λ CDS
Control & Data System (CDS)
λ PEM
Physical Environmental Monitor (PEM)
λ BT
Beam Tubes (BT)
λ VE
Vacuum Equipment (VE)
λ FMCS
Facilities Monitoring & Control System (FMCS)
λ HVAC
Heating, Vent., & Air Cond. (HVAC)
λ PWR
Electrical Power (PWR)
2 times

Figure B.2.3: 3X Configuration

The reliability for the 3X mode of operation will be:

$$(R_{3X}(t) = (R_{IF}(t))^3) \cdot (R_{OpEquip}(t))^2 \qquad \text{(B.2.3)}$$

The system failure rate for the 3X mode:

$$\lambda_{3X}(t) = \frac{-\ln(R_{3X}(t))}{t}$$

Since all the assemblies in the 3X mode are in series, the 3X system failure rate can be simplified to:

$$\lambda_{3X} = \sum_{i=1}^{3} \lambda_{IF} + 2\lambda_{OpEquip} = 3\lambda_{IF} + 2\lambda_{OpEquip}$$

Appendix C

Failure Mode Effects and Analysis Worksheet

Table C shows the format for FMEA worksheet per Task 101 of MIL-STD-1629A with minor modifications. The changes are deletion of mission phase/operational mode and addition of probability of failure occurrence.

The following is a more detailed description of the headers in the FMEA worksheet:

- I.D. No. - An identification number is assigned for traceability purposes.
- Failure Mode - Identifies the failed item within the system being analyzed.
- Failure cause - Identifies the most probable cause associated with the postulated failure mode.
- Failure effect - The consequences of each assumed failure mode on operation, function or status. Failure effects may consider the system functional objectives, maintenance requirements and personnel and system safety. The failure may impact several indenture levels in addition to the indenture level under analysis. Therefore, “local” and “system” effects need to be evaluated.
- Failure detection method - A description of the methods by which occurrence of the failure mode is detected by the operator. The failure detection means, such as visual or audible warning devices, automatic sensing devices, sensing instrumentation, or none should be identified.
- Compensation provisions - either design provisions or operator actions, which circumvent the effect of the failure should be identified.

  Design compensating provision include:

  - Redundant items that allow continued and safe operation.
  - Safety or relief devices such as monitoring or alarm provision which permit effective operation or limits damage.
  - Alternative modes of operation such as backup or standby items or systems.

  Compensating provisions requiring operator action:

  - The compensating provision that satisfies the indications observed by an operator when the failure occurs.

- Severity - A severity classification is assigned to each failure mode according to the failure effect. Severity classification categories consistent with MIL-STD-882 are defined as follows:

Category	Classification	Failure Description
I	Catastrophic	Failures causing death or system loss
II	Critical	Failures causing major system damage
III	Marginal	Failures causing system degradation
IV	Minor	Failures that do not cause degradation of system, but has a hindering or nuisance effect

- Remarks - Any pertinent remarks pertaining to and clarifying any other column in the worksheet should be noted.

SAMPLE

Relex FMECA | LIGO Failure Modes and Effects Analysis | Page: 1

File Name: VCMS.FMEA | Date: November 8, 1996

Description: VCMS

I.D. No.	Failure Mode	Failure Cause	Local Effect	End Effect	Method of Detection	Compensating Provisions	Severity	Remarks
1.01	CDS Infrastructure fails	Break in connection between CDS and VCMS	Loss of vacuum monitoring in area(s) disconnected from CDS, vacuum control would remain at its last state	None. No effect on the ability to detect gravity waves	Visual Alarm at Operator's Console in Facility Control Room	None	IV. Minor	
2.01	Transition Module fails	Electronic failure	Loss of vacuum monitoring in area(s) disconnected from CDS, vacuum control would remain at its last state	None. No effect on the ability to detect gravity waves	Visual Alarm at Operator's Console in Facility Control Room	None	IV. Minor	
3.01	Microprocessor Module fails	Electronic failure / Software Lock-up	Loss of remote monitoring of LN2 Level	None. No effect on the ability to detect gravity waves	Visual Alarm at Operator's Console in Facility Control Room	None	IV. Minor	

Appendix D

Fault Tree Analysis

D.1 Fault Tree Symbols

Standard symbols are used in constructing an FTA to describe events and logical connections. These are shown in Table D.1.

Table D.1: Fault Tree Symbols

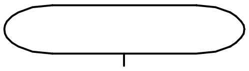
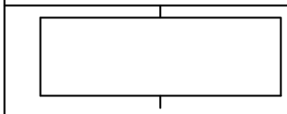
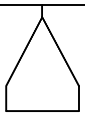
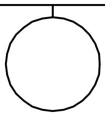
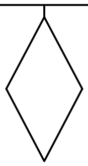
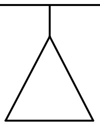
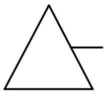
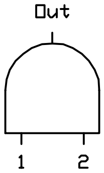
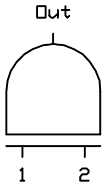
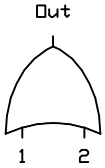
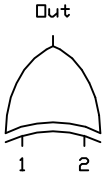
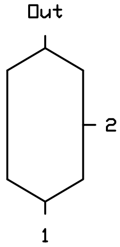
Symbol/Name	Description
 Ellipse	Top Event: Contains description of the system-level fault or the undesired event. Input to the ellipse is from a logic gate.
 Rectangle	Fault Event: Contains description of a lower-level fault. Fault events receive inputs from and provide outputs to a logic gate.
 House	Input Event: Contains a normal system operating input which has the capability of causing a fault to occur. The input event is used as an input to the logic gate.
 Circle	Basic Event: Contains a failure at the lowest level of examination which has the capability of causing a fault to occur. The basic event is used as an input to a logic gate.
 Diamond	Undeveloped Event: Contains a failure at the lowest level of examination which can be expanded into a seperate fault tree. The undeveloped event is used as an input to a logic gate.
Transfer In  Triangle Transfer Out  Triangle	Transfer Function: Signifies a connection between two or more selections of the fault tree to prevent duplicating sub-branches at multiple tree locations or to signify a location on a seperate sheet of the same fault tree.
	And Gate: Output is to any fault event block or Transfer Out function. Inputs are from any fault event block or Transfer In Function. Output occurs only if all inputs exist.

Table D.1: Fault Tree Symbols (Continued)

Symbol/Name	Description
	Ordered AND Gate: Output is to any fault event block or Transfer Out function. Inputs are from any fault event block or Transfer In function. Output occurs only if all inputs exist and the inputs occur in a specific order.
	OR Gate: Output is to any fault event block or Transfer Out function. Inputs are from any fault event block or Transfer In function. Output occurs only if one or more of the input events occur.
	Exclusive OR Gate: Output is to any fault event block or Transfer Out function. Inputs are from any fault eventblock or Transfer In function. Output occurs only if one, and only one, of the input events occur.
	Inhibit Gate: Output is to any fault block or Transfer Out function. Inputs are from any fault event block or Transfer In function. One input is a lower fault event and the other input is a conditional qualifier.

D.2 Procedures for Fault Tree Construction

Following are steps for constructing a fault tree:

- Define the undesired events (major) faults. Faults that can result in :
  - Complete system failure
  - Degradation of system performance
  - Failure of a backup system
  - Undetected failure
  - Safety hazards.
- Define whether the faults are operational faults or component faults.
  - Operational faults occur when a component is operating as intended, but at an inappropriate time.
  - Components faults occur when a component fails in its intended or non-intended environment.
- Define the types of failures. Identify whether the failure is due to component failures, environmental failures, human failures or software failures
- Define the level(s) of analysis. The fault tree can be decomposed into 3 levels to simplify the process:
  - Level I - the highest level to be analyzed. Define the level I failure causes and effects .
  - Level II - the system is divided into functional blocks which reflect the level I failure causes. These causes are expanded to determine their contribution to the failure effects.
  - Basic Event Level - the lowest level. It is the level at which the failure occurs, and can be further analyzed to distinguish between the failure causes, modes & mechanisms.

Appendix E

Reliability and Availability Growth Assessment

E.1.0 Availability in Terms of Reliability Growth Assessment

A constant failure rate was assumed for the analysis presented in section 4.1.6. In actuality, the LIGO system will undergo continuous failure corrections and will consider new technology upgrades of instrumentation after five years of operation. When addressing reliability growth, it is necessary to consider the intensity function, ρ(t), from MIL-HDBK-189:

$$\rho(t) = \lambda \cdot \beta \cdot t^{\beta - 1}$$

Within the intensity function, λ is considered a scale parameter because it depends upon the measurement units chosen for t. β is important because it characterizes the shape of the graph of the intensity function. If β is equal to 1, the intensity function is constant. In that case the reliability of the system is not changing since the times between successive failures are independent identically distributed random variables with an exponential distribution and a mean of λ^{-1}. If β does not equal 1, the times between successive failures are not identically distributed and don not have exponential distributions. For a development project during which the system reliability improves, the shape parameter, β, is less than one. In this case, the expected number of failures in an interval of fixed length decreases as its starting point increases. In a project wherein new and unproven technologies are continually being inserted resulting in reliability degradation, β is greater than 1. This indicates that the number failures expected during a fixed time interval is increasing with time.

Therefore, the system availability can be expressed in terms of the following reliability growth equation:

$$A = \frac{1}{1 + MDT \cdot \rho(t)} = \frac{1}{1 + MDT \cdot (\lambda \cdot \beta \cdot t^{\beta - 1})}$$

where λ varies as a function of time as defined by the failure intensity, ρ(t) in MIL-HDBK-189. The shape parameter "β" is equal to one for a constant intensity function (no part replacement or maintenance work after system installation). rate It is less than one if the system reliability improves during process development and greater than one if improper design changes occur.

. As an example, let:

β = 0.9 (assuming the LIGO system improves with failure correction and part upgrade)

β = 1.0 (constant failure rate)

MDT_{3x} = 33 hours

Failure, $\lambda_{3x} = 10{,}000 \times 10^{-6}$ failures/hr

The 3X system availability can be calculated using the A_{3x} equation in section 4.1.6 and plotted vs. a LIGO operational time of 5 years. Figure 4.1.8 indicates that the availability improves (grows) with time for β = 0.9 (especially within the first year) due to the fact that faults have been corrected and inferior parts have been upgraded with better parts.

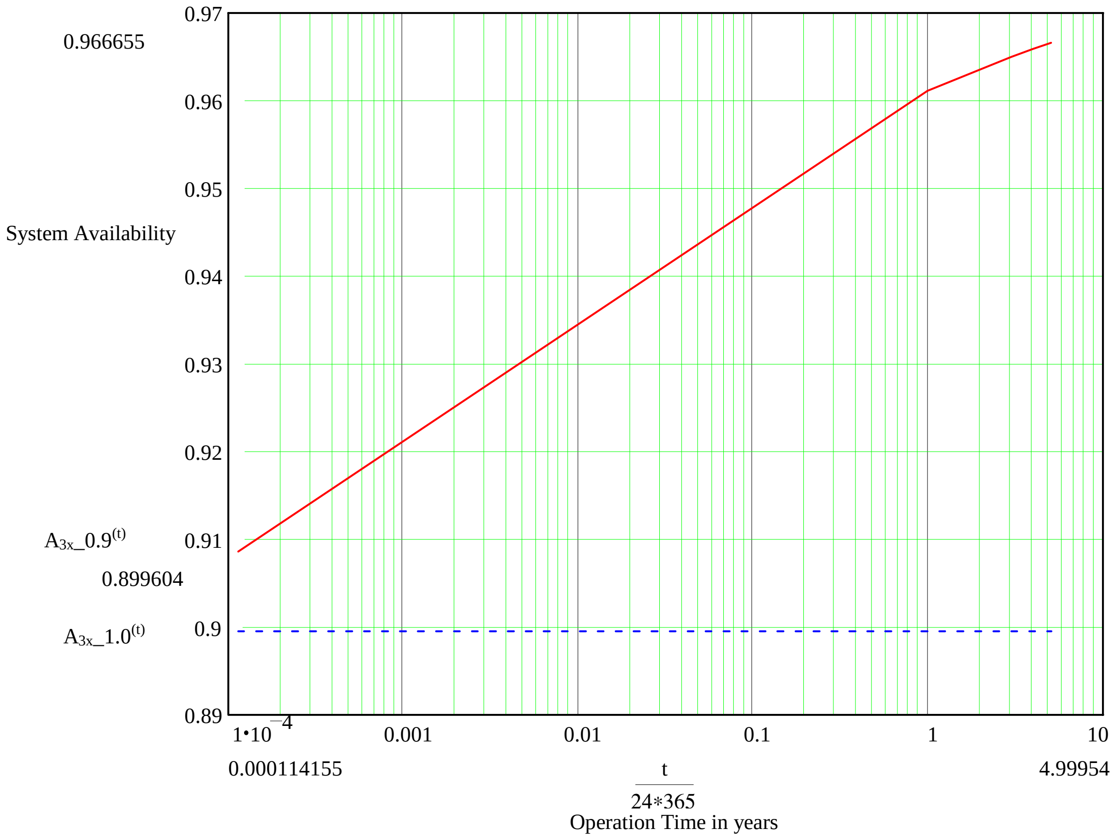


Figure 4.1.8: Example for LIGO Initial System Projected Availability

The plan, therefore, is to estimate system availability based on the conservative constant failure rate method shown in section 4.1.6. Then a plot of availability vs. time can be created using the reliability growth method discussed in this section to predict its actual improvement. A realistic value for β can be derived if failure data for the system is available (See E.2 below for a sample derivation). Otherwise, a conservative factor, such as 0.9, will be used to show the system with slight improvement with part replacement and maintenance plan.

E.2.0   Reliability Growth Assessment: Derivation of β For The Intensity Function

MIL-HDBK-189 defines the intensity function as:

$$\rho(t) = \lambda \cdot \beta \cdot t^{\beta - 1}$$

where the shape parameter, β =1 for constant system reliability

β <1 if system reliability improves with time

β >1 if system reliability degrades with time β can be derived by using the point estimation equation:

$$\beta = \frac{N}{N \ln T - \sum_{i=1}^{N} \ln X_i}$$

where N = total number of failures

X = successive failure time

T = total cumulative time

A sample calculation for β from MIL-HDBK-189 is presented as follows:

Two prototypes of mechanical system are tested concurrently with the incorporation of design changes. The first system runs 132.4 hours, and the second runs 167.6 hours. The time on each system and cumulative test time at each failure rate are listed below. An asterisk denotes the failed system.

N	#1 (hours)	#2 (hours)	Cumulative (hours)
1	2.6*	0	2.6
2	16.5*	0	16.5
3	16.5*	0	16.5
4	17.0*	0	17.0
5	20.5	0.9*	21.4
6	25.3	3.8*	29.1
7	28.7	4.6*	33.3
8	41.8*	14.7*	56.5
9	45.5*	17.6	63.1
10	48.6	22.0	70.6
11	49.6	23.4*	73.0
12	51.4*	26.3	77.7
13	58.2*	35.7	93.9
14	59.0	36.5*	95.5
15	60.5	37.6*	98.1
16	61.9*	39.1	101.1
17	76.6*	55.4	132.0
18	81.1	61.1*	142.2
19	84.1*	63.6	147.7
20	84.7*	64.3	149.0
21	94.6*	72.6	167.2
22	104.8	85.9*	190.7
23	105.9	87.1*	193.0
24	108.8*	89.9	198.7
25	132.4	119.5*	251.9
26	132.4	150.1*	282.9
27	132.4	153.7*	286.1
End	132.4	167.6	300.0

The point estimate of β is thus:

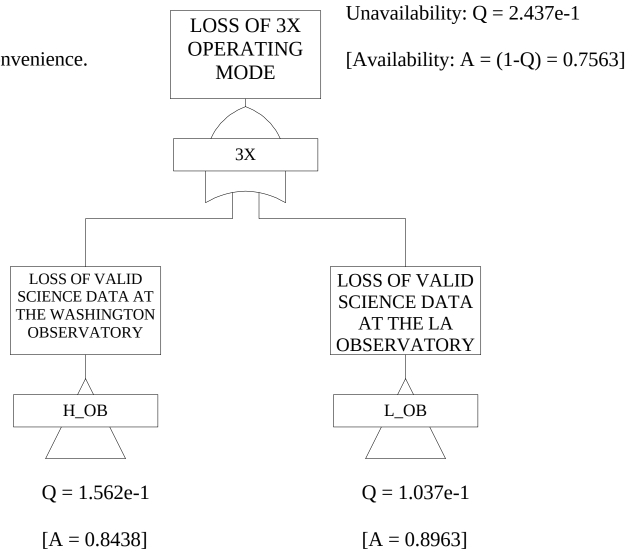
$$\hat{\beta} = \frac{27}{27 \ln 300 - (\ln 2.6 + \ln 16.5 + \ldots + \ln 286.1)} = 0.716$$

APPENDIX F

Fault Tree Diagrams Depicting Subsystem Availability Allocations

NOTES:

1. Diagram logic depicts Unavailability, Q.
Availability, A, values are shown in brackets for the reader's convenience.

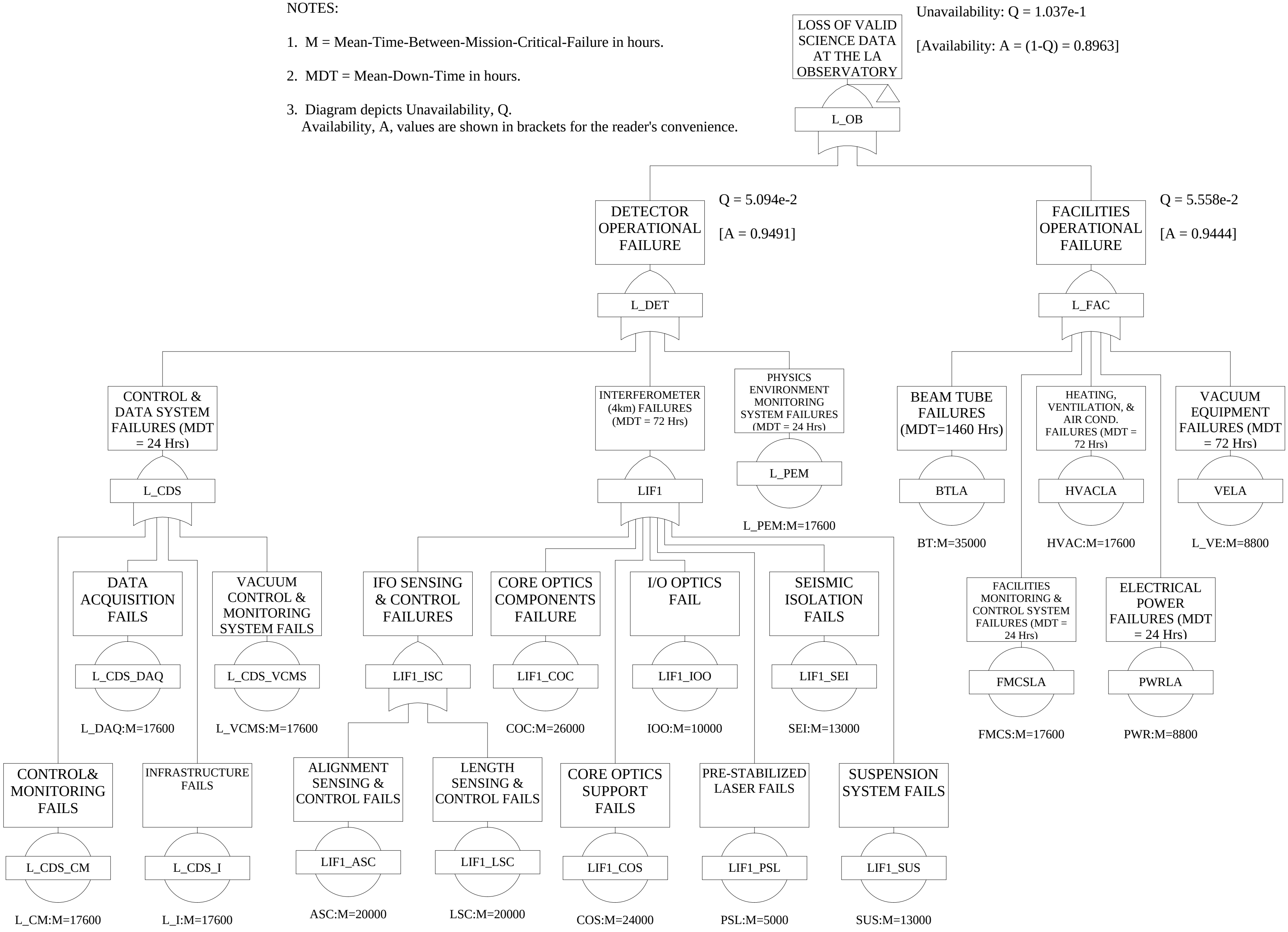

LOSS OF 3X OPERATING MODE
Unavailability: Q = 2.437e-1
[Availability: A = (1-Q) = 0.7563]
3X
LOSS OF VALID SCIENCE DATA AT THE WASHINGTON OBSERVATORY
H_OB
Q = 1.562e-1
[A = 0.8438]
LOSS OF VALID SCIENCE DATA AT THE LA OBSERVATORY
L_OB
Q = 1.037e-1
[A = 0.8963]

NOTES:

1. M = Mean-Time-Between-Mission-Critical-Failure in hours.

2. MDT = Mean-Down-Time in hours.

3. Diagram depicts Unavailability, Q.
Availability, A, values are shown in brackets for the reader's convenience.

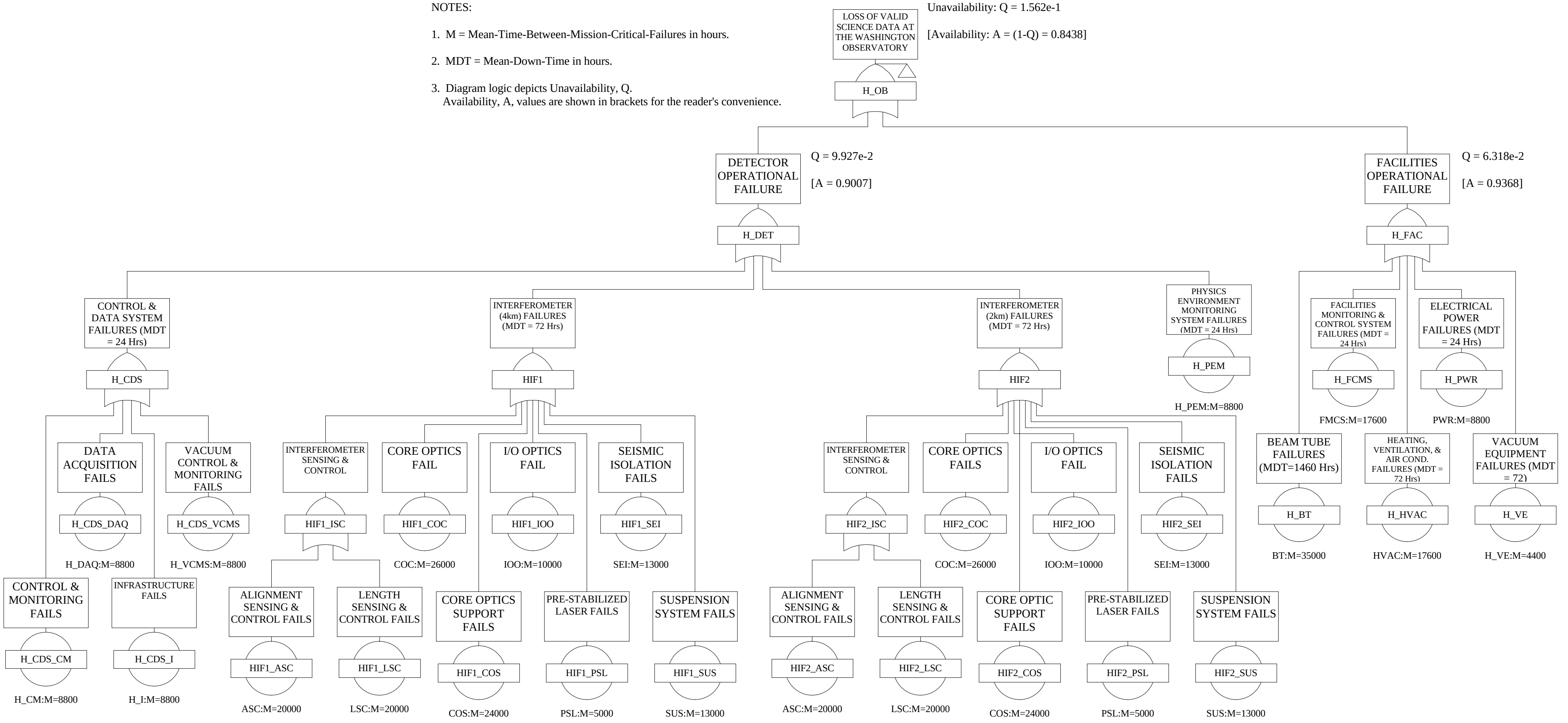

LOSS OF VALID SCIENCE DATA AT THE LA OBSERVATORY
L_OB
Unavailability: Q = 1.037e-1
[Availability: A = (1-Q) = 0.8963]
DETECTOR OPERATIONAL FAILURE
Q = 5.094e-2
[A = 0.9491]
L_DET
FACILITIES OPERATIONAL FAILURE
Q = 5.558e-2
[A = 0.9444]
L_FAC
CONTROL & DATA SYSTEM FAILURES (MDT = 24 Hrs)
L_CDS
INTERFEROMETER (4km) FAILURES (MDT = 72 Hrs)
LIF1
PHYSICS ENVIRONMENT MONITORING SYSTEM FAILURES (MDT = 24 Hrs)
L_PEM
L_PEM:M=17600
BEAM TUBE FAILURES (MDT=1460 Hrs)
BTLA
BT:M=35000
HEATING, VENTILATION, & AIR COND. FAILURES (MDT = 72 Hrs)
HVACLA
HVAC:M=17600
VACUUM EQUIPMENT FAILURES (MDT = 72 Hrs)
VELA
L_VE:M=8800
DATA ACQUISITION FAILS
L_CDS_DAQ
L_DAQ:M=17600
VACUUM CONTROL & MONITORING SYSTEM FAILS
L_CDS_VCMS
L_VCMS:M=17600
IFO SENSING & CONTROL FAILURES
LIF1_ISC
CORE OPTICS COMPONENTS FAILURE
LIF1_COC
COC:M=26000
I/O OPTICS FAIL
LIF1_IOO
IOO:M=10000
SEISMIC ISOLATION FAILS
LIF1_SEI
SEI:M=13000
FACILITIES MONITORING & CONTROL SYSTEM FAILURES (MDT = 24 Hrs)
FMCSLA
FMCS:M=17600
ELECTRICAL POWER FAILURES (MDT = 24 Hrs)
PWRLA
PWR:M=8800
CONTROL& MONITORING FAILS
L_CDS_CM
L_CM:M=17600
INFRASTRUCTURE FAILS
L_CDS_I
L_I:M=17600
ALIGNMENT SENSING & CONTROL FAILS
LIF1_ASC
ASC:M=20000
LENGTH SENSING & CONTROL FAILS
LIF1_LSC
LSC:M=20000
CORE OPTICS SUPPORT FAILS
LIF1_COS
COS:M=24000
PRE-STABILIZED LASER FAILS
LIF1_PSL
PSL:M=5000
SUSPENSION SYSTEM FAILS
LIF1_SUS
SUS:M=13000

NOTES:

1. M = Mean-Time-Between-Mission-Critical-Failures in hours.

2. MDT = Mean-Down-Time in hours.

3. Diagram logic depicts Unavailability, Q.
Availability, A, values are shown in brackets for the reader's convenience.


LOSS OF VALID SCIENCE DATA AT THE WASHINGTON OBSERVATORY
H_OB
Unavailability: Q = 1.562e-1
[Availability: A = (1-Q) = 0.8438]
DETECTOR OPERATIONAL FAILURE
H_DET
Q = 9.927e-2
[A = 0.9007]
FACILITIES OPERATIONAL FAILURE
H_FAC
Q = 6.318e-2
[A = 0.9368]
CONTROL & DATA SYSTEM FAILURES (MDT = 24 Hrs)
H_CDS
INTERFEROMETER (4km) FAILURES (MDT = 72 Hrs)
HIF1
INTERFEROMETER (2km) FAILURES (MDT = 72 Hrs)
HIF2
PHYSICS ENVIRONMENT MONITORING SYSTEM FAILURES (MDT = 24 Hrs)
H_PEM
H_PEM:M=8800
FACILITIES MONITORING & CONTROL SYSTEM FAILURES (MDT = 24 Hrs)
H_FCMS
FMCS:M=17600
ELECTRICAL POWER FAILURES (MDT = 24 Hrs)
H_PWR
PWR:M=8800
BEAM TUBE FAILURES (MDT=1460 Hrs)
H_BT
BT:M=35000
HEATING, VENTILATION, & AIR COND. FAILURES (MDT = 72 Hrs)
H_HVAC
HVAC:M=17600
VACUUM EQUIPMENT FAILURES (MDT = 72)
H_VE
H_VE:M=4400
DATA ACQUISITION FAILS
H_CDS_DAQ
H_DAQ:M=8800
VACUUM CONTROL & MONITORING FAILS
H_CDS_VCMS
H_VCMS:M=8800
CONTROL & MONITORING FAILS
H_CDS_CM
H_CM:M=8800
INFRASTRUCTURE FAILS
H_CDS_I
H_I:M=8800
INTERFEROMETER SENSING & CONTROL
HIF1_ISC
CORE OPTICS FAIL
HIF1_COC
COC:M=26000
I/O OPTICS FAIL
HIF1_IOO
IOO:M=10000
SEISMIC ISOLATION FAILS
HIF1_SEI
SEI:M=13000
ALIGNMENT SENSING & CONTROL FAILS
HIF1_ASC
ASC:M=20000
LENGTH SENSING & CONTROL FAILS
HIF1_LSC
LSC:M=20000
CORE OPTICS SUPPORT FAILS
HIF1_COS
COS:M=24000
PRE-STABILIZED LASER FAILS
HIF1_PSL
PSL:M=5000
SUSPENSION SYSTEM FAILS
HIF1_SUS
SUS:M=13000
INTERFEROMETER SENSING & CONTROL
HIF2_ISC
CORE OPTICS FAILS
HIF2_COC
COC:M=26000
I/O OPTICS FAIL
HIF2_IOO
IOO:M=10000
SEISMIC ISOLATION FAILS
HIF2_SEI
SEI:M=13000
ALIGNMENT SENSING & CONTROL FAILS
HIF2_ASC
ASC:M=20000
LENGTH SENSING & CONTROL FAILS
HIF2_LSC
LSC:M=20000
CORE OPTIC SUPPORT FAILS
HIF2_COS
COS:M=24000
PRE-STABILIZED LASER FAILS
HIF2_PSL
PSL:M=5000
SUSPENSION SYSTEM FAILS
HIF2_SUS
SUS:M=13000