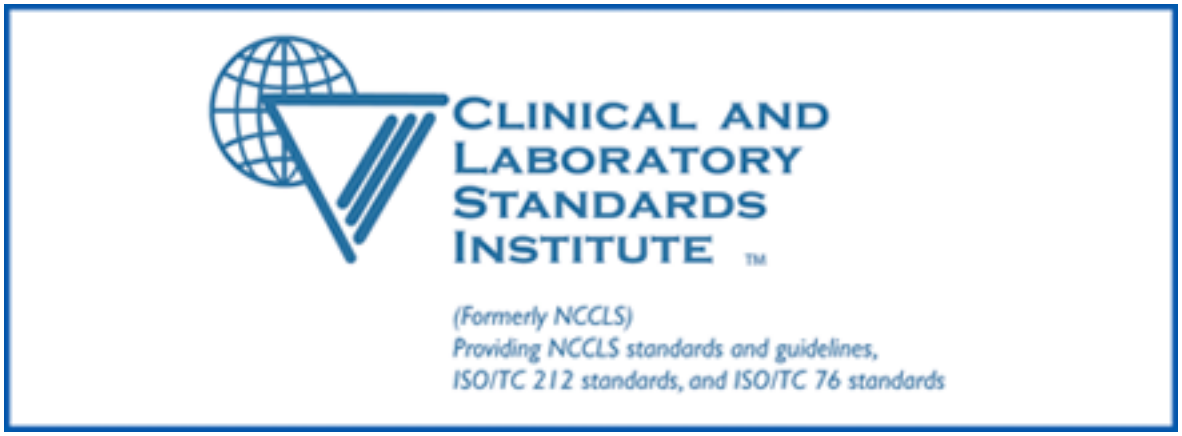
LIS6-A
Vol. 23 No. 12
Formerly ASTM E1246-01

Standard Practice for Reporting Reliability of Clinical Laboratory Information Systems



This document describes a system for collecting data, maintaining records, and reporting on the reliability of operating clinical laboratory computer systems.

NCCLS

NCCLS...

Serving the World's Medical Science Community Through Voluntary Consensus

NCCLS is an international, interdisciplinary, nonprofit, standards-developing, and educational organization that promotes the development and use of voluntary consensus standards and guidelines within the healthcare community. It is recognized worldwide for the application of its unique consensus process in the development of standards and guidelines for patient testing and related healthcare issues. NCCLS is based on the principle that consensus is an effective and cost-effective way to improve patient testing and healthcare services.

In addition to developing and promoting the use of voluntary consensus standards and guidelines, NCCLS provides an open and unbiased forum to address critical issues affecting the quality of patient testing and health care.

PUBLICATIONS

An NCCLS document is published as a standard, guideline, or committee report.

Standard A document developed through the consensus process that clearly identifies specific, essential requirements for materials, methods, or practices for use in an unmodified form. A standard may, in addition, contain discretionary elements, which are clearly identified.

Guideline A document developed through the consensus process describing criteria for a general operating practice, procedure, or material for voluntary use. A guideline may be used as written or modified by the user to fit specific needs.

Report A document that has not been subjected to consensus review and is released by the Board of Directors.

CONSENSUS PROCESS

The NCCLS voluntary consensus process is a protocol establishing formal criteria for:

- the authorization of a project
- the development and open review of documents
- the revision of documents in response to comments by users
- the acceptance of a document as a consensus standard or guideline.

Most NCCLS documents are subject to two levels of consensus—"proposed" and "approved." Depending on the need for field evaluation or data collection, documents may also be made available for review at an intermediate (i.e., "tentative") consensus level.

Proposed An NCCLS consensus document undergoes the first stage of review by the healthcare community as a proposed standard or guideline. The document should receive a wide and thorough technical review, including an overall review of its scope, approach, and utility, and a line-by-line review of its technical and editorial content.

Tentative A tentative standard or guideline is made available for review and comment only when a recommended method has a well-defined need for a field evaluation or when a recommended protocol requires that specific data be collected. It should be reviewed to ensure its utility.

Approved An approved standard or guideline has achieved consensus within the healthcare community. It should be reviewed to assess the utility of the final document, to ensure attainment of consensus (i.e., that comments on earlier versions have been satisfactorily addressed), and to identify the need for additional consensus documents.

NCCLS standards and guidelines represent a consensus opinion on good practices and reflect the substantial agreement by materially affected, competent, and interested parties obtained by following NCCLS's established consensus procedures. Provisions in NCCLS standards and guidelines may be more or less stringent than applicable regulations. Consequently, conformance to this voluntary consensus document does not relieve the user of responsibility for compliance with applicable regulations.

COMMENTS

The comments of users are essential to the consensus process. Anyone may submit a comment, and all comments are addressed, according to the consensus process, by the NCCLS committee that wrote the document. All comments, including those that result in a change to the document when published at the next consensus level and those that do not result in a change, are responded to by the committee in an appendix to the document. Readers are strongly encouraged to comment in any form and at any time on any NCCLS document. Address comments to the NCCLS Executive Offices, 940 West Valley Road, Suite 1400, Wayne, PA 19087, USA.

VOLUNTEER PARTICIPATION

Healthcare professionals in all specialties are urged to volunteer for participation in NCCLS projects. Please contact the NCCLS Executive Offices for additional information on committee participation.

Preface

In 2001, ASTM Committee E31 decided to restructure its operations, with the intent of focusing on standards-development issues such as security, privacy, and the electronic health record. Part of the reorganization plan was to explore the option of transferring responsibility for nine E31.13 standards to NCCLS.

The NCCLS Area Committee on Automation and Informatics, at its meeting in April 2002, reached a positive assessment of the value of the ASTM standards and encouraged the NCCLS Executive Offices staff to pursue negotiations with ASTM on transferring these standards to NCCLS.

Following this transfer, these nine standards (formerly ASTM E792; E1029; E1238; E1246; E1381; E1394; E1466; E1639; and E2118) have been redesignated as NCCLS standards LIS1 through LIS9.

The Area Committee on Automation and Informatics has assumed responsibility for maintaining the documents and will revise or update each document in accord with NCCLS Administrative Procedures.

This document is the equivalent of ASTM E1246 but has been redesignated and is now maintained by NCCLS. This document has been approved as an American National Standard (ANSI/ASTM E1246-01).

Suggested Citation

(NCCLS. *Standard Practice for Reporting Reliability of Clinical Laboratory Information Systems*. NCCLS document LIS6-A [ISBN 1-56238-494-5]. NCCLS, 940 West Valley Road, Suite 1400, Wayne, Pennsylvania 19087-1898 USA, 2003.)

Published
April 2003

ISBN 1-56238-494-5
ISSN 0273-3099

Standard Practice for
Reporting Reliability of Clinical Laboratory Information Systems

1. Scope

1.1 This practice describes a system for collecting data, maintaining records, and reporting on the reliability of operating clinical laboratory computer systems.[1] The reliability measure will be achieved by documenting the number, severity, cause, impact, and duration of the failures that a system experiences. This practice can be implemented with paper forms or computer records. The type of computer systems under consideration are those designed to assist the overall workflow of the laboratory, and generally include some or all of the functions of patient biographical data, test ordering, draw list printing, specimen check-in, workstation work list printing, test result entry, result verification, patient report printing, data archiving, quality control, and management report printing. This practice is applicable to all types of clinical laboratories, including major medical centers, teaching hospitals, community hospitals, referral clinics, emergency centers, health care maintenance organizations, specialty institutions, commercial laboratories, and private practices. The significance of portions of the reliability measure may be different in the different settings, but the measurement procedure is the same. This practice is not intended for computers inside instruments or for those systems designed to support a single workstation, although portions of this practice may be applicable.

1.2 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety and health practices and determine the applicability of regulatory limitations prior to use.*

2. Referenced Documents

2.1 *ASTM Standards:*

E 1239 Guide for Description of Reservation/Registration-Admission, Discharge, Transfer (R-ADT) Systems for Electronic Health Record (EHR) Systems[2]

E 1715 Practice for Object-Oriented Model for Registration, Admitting, Discharge and Transfer (RADT) Functions in Computer-based Patient Record Systems[2]

2.2 *ISO Standards:*

ISO IS 12207 Information Technology-Software Life Cycle Processes

ISO CD3 15288 System Life Cycle Processes

3. Significance and Use

3.1 *Use*—This practice is intended to be used by laboratory personnel on a regular ongoing basis. It is primarily intended for laboratory management to keep records on a system in regular operation. The information produced by this practice will also be useful to regulatory agencies, professional review groups, system maintainers, system manufacturers, and others who may be contemplating purchase of a similar system. It is expected that the reports produced by this standard practice will be saved as a part of the life cycle records for the system. This practice is one part of the activities of a system life cycle (see IS 12207 and CD3 15288) and in particular its operation and maintenance processes. A key part of system maintenance is documentation of defects and their effect upon the enterprise operations. This practice addresses ways to make use of the recordkeeping needed to manage system maintenance.

3.1.1 This practice is not intended for those systems or parts of systems that are still in development or testing, and any failures caused by such testing shall not be included in the statistics.

3.1.2 This practice is not intended to cover problems due to system designs that do not meet user needs, either at the time of acceptance or because user needs have changed over time. It is expected that such immediate or potential problems will be identified and solved during verification, validation, and acceptance phases of the project (see CD3 15288).

3.1.3 If this practice is referenced in a contract, it shall be referred to as the "Standard Practice for Reporting Reliability of Clinical Laboratory Computer Systems." Vendors agreeing to supply reliability reports in accord with this standard practice shall meet all the requirements described herein, or shall provide a list of exceptions or alterations that is acceptable to the managers of the computer system, along with an explanation of how the purpose and integrity of this standard practice is maintained.

[1] Prepared in cooperation with the College of American Pathologists.

[2] *Annual Book of ASTM Standards*, Vol 14.01.

3.2 *Significance*—There are several advantages to the widespread adoption of a common practice for reporting clinical laboratory computer system reliability.

3.2.1 *Comparison of Different Systems*—A practice for reporting system reliability will permit comparison of systems offered by different vendors. When each vendor and each laboratory choose to define downtime differently and to follow different procedures for keeping reliability information, there is no easy way to compare the reliability of different systems. A commonly adopted reliability measure will allow:

3.2.1.1 Prospective buyers to compare reliability of different systems as a part of their selection process.

3.2.1.2 Prospective buyers to realistically determine for the systems under consideration the amount of redundancy, spare parts, and service support they would need to satisfy the reliability requirements of their particular operations.

3.2.1.3 Vendors to evaluate their product against the competition and to identify and correct areas that need improvement.

3.2.1.4 Vendor sales people to accurately represent the reliability of their product to prospective customers.

3.2.2 *System Purchase*—Demonstrated system reliability over an initial trial period is often included as one of the acceptance criteria items during purchase contract negotiations. Availability of a standard practice for reporting reliability will clarify that part of the contract and simplify that portion of the negotiations (LIS3).

3.2.3 *System Life Cycle*—All laboratories need to maintain records on system reliability and to periodically make reports on that reliability to institution administrators and outside reviewers (LIS4) as part of the operation and maintenance processes and laboratory management. A standard practice for reporting reliability of the information system offers the laboratory the following advantages:

3.2.3.1 It reduces the planning effort needed to devise a separate reliability reporting scheme at each institution.

3.2.3.2 It results in a more uniform level of quality in the reliability reporting procedures used from institution to institution.

3.2.3.3 It provides the laboratory with an accepted tool to answer critics of information system reliability, both from the administration and from the users of the laboratory services.

3.2.3.4 It permits creation of an accepted definition of the time when repair or other remedial action is needed. When reliability drops below a specified level, then redesign, replacement of older components, retraining of users or repair people, or other corrective action is indicated. If such a definition becomes widely accepted, the laboratory will have less difficulty convincing administrators to allocate funds for upgrade or convincing vendors to undertake the repairs.

3.2.4 *Reliability Standards and Reviews*—A standard measure of reliability makes it possible to determine national levels of normal or typical reliability of clinical laboratory information systems. This has several advantages:

3.2.4.1 Individual institutions may compare themselves against those standards to decide when to modify the system or alter the operating procedures.

3.2.4.2 Regulatory or professional review groups can use this information as a part of their evaluation.

3.2.4.3 Once national levels of reliability are determined, the medical laboratory community in cooperation with the suppliers can evaluate the average reliability of system components in the field and determine if it should be improved. If so, the data collected might help identify the areas of reliability that are most in need of improvement.

4. Downtime and Intermediate Events

4.1 In order to provide an operational definition of downtime, it is helpful to identify some individual events within a typical failure incident. Each of these events shall be assigned a time and date. The downtime, or time a system is inoperative in any way due to a failure, is defined as the interval from “failure occurrence” (see 4.2) to “resumption of normal operations” (see 4.11). Intermediate milestones make it possible to evaluate the quality of service and identify areas where improved service procedures are needed. The interval from “failure occurrence” (4.2) to “initial service contact” (4.4) is the time the end-user needed to recognize and act on the problem. From there to “start of diagnosis/repair” (4.8) is the service vendor response time. From “start of diagnosis/repair” to "completion of validation” (4.9) is the repair time. The interval from “completion of validation” to “resumption of normal operations” (4.11) is the time needed to recover the system.

4.2 *failure occurrence*—the time and date when the failure occurred marks the beginning of a failure incident. Sometimes the exact time of the failure can only be estimated.

4.3 *failure discovery*—often immediately, but perhaps some time after the failure happened, an operator becomes aware that a problem has developed. “Failure discovery” is the time and date when the system operator determines that there is a failure.

4.4 *failure documented*—the “failure documented” step is the time and date when basic information about the failure occurrence and associated information is recovered in a form useful to communicating to the support or service person. See Fig. 1.

4.5 *initial service contact*—the time and date when the system operator first attempts to secure the assistance of an appropriate service person is the "initial service contact" time. Several initial service contact times may be identified if maintenance is provided in layers. For example, there may be an in-house person who provides low- or intermediate-level service who is contacted first. If that person determines that the problem requires it, the system vendor or outside maintenance organization is subsequently contacted.

4.6 *end of service contact*—the time and date when the provider of service acknowledges a request for repair is the next milestone. This may be considerably later than the initial service contact if busy telephones, answering services, or other communication problems are encountered. There may be more than one end of service contact time if maintenance is provided in layers.

4.7 *initial service response*—the time and date when an authorized service representative of the hardware/software maintenance provider contacts the user regarding the problem. This is the time when the nature of the problem is first discussed with a service person. It may or may not coincide with end of service contact (4.6).

4.8 *start of diagnosis/repair*—after being made aware of the problem, there will be a time and date when the service provider commences the evaluation of the reported failure and begins the diagnosis and repair.

4.9 *end of diagnosis/repair*—the next milestone is the time and date when the service provider reports to the user that the problem has been repaired. In the case of layered service, this may be the time when an in-house group reports that the problem requires the attention of an external service provider. In this case, there may be more than one pair of start and end times (4.8 and 4.9) for diagnosis and repair.

4.10 *completion of validation*—the next time and date identified is when diagnostic routines or application programs indicate that the problem has been corrected. This milestone represents the time at which all functions have been restored and validated. There still may be additional effort required of the user to restore and validate data that may have been lost or corrupted because of the failure.

4.11 *restart of operations*—when the user is able to exercise all previously disabled functions and execute application-dependent backup procedures. For some systems, this may mean reloading the backup database and reapplying records from the transaction log to the database. In other cases, the transactions lost since the last backup may be reentered manually.

4.12 *resumption of normal operations*—the failure event is over at the time and date when all normally scheduled tasks can be executed in their regular time frame. If the failure event was of long duration, it may require many hours from the "restart of operations" until database recovery is complete and normal operation is possible.

5. Classification of Failures

5.1 In the measurement of computer system reliability, it is important to recognize that some failures are more serious than others. Some failures only degrade performance or affect only a noncritical function, and do not require the laboratory to seek alternative methods to continue to accept test orders and turn out results. To achieve the objectives in Section 4, it is desirable to account for the more serious and the less serious failures separately. In this way, the standard reliability statistics can more properly reflect the impact of failures on the operation of the laboratory, which is the important objective of a standard measure of reliability. In this section, failures are classified into several types depending on whether they involve loss of primary function, secondary function, or redundancy.

5.2 *Primary Functions*—The primary purpose of a clinical laboratory system is to enhance patient care by providing measurement information about patients' health conditions, including clinical decision support. It can do this by keeping records, assisting laboratory workflow, and improving communications by maintaining continuing information flow from the laboratory to the practitioner in all settings of care. A primary function is therefore any function directly related to providing patient care. Primary functions include:

5.2.1 Patient registration,
5.2.2 Test ordering,
5.2.3 Specimen collection,
5.2.4 Work list generation,
5.2.5 Result acquisition,
5.2.6 Result verification, including any quality control reports needed to help verify patient results,
5.2.7 Patient result reporting and posting,
5.2.8 Charge capture, but not charge reporting,
5.2.9 Inventory functions in blood bank,
5.2.10 Word processing functions in anatomical pathology,
5.2.11 Supply chain management,
5.2.12 Human resource management, and
5.2.13 Transaction logs or audit trails that backup the changes made to the database.

5.3 *Secondary Functions*—Secondary functions consist of all other activities. In most institutions, these functions are important, but will not impact the patient care system as much if they are impaired or delayed. They include:

5.3.1 All patient reports other than test results, such as a census reports.

5.3.2 Quality control reports performed after the patient results are reported.

5.3.3 Charge reporting.

5.3.4 Management reports, such as turnaround times, loads by workstation, personnel scheduling, etc.

5.3.5 System customization and parameter selection, such as setting normal values for tests, adding new tests, changing the list of authorized system users, etc.

5.3.6 Patient discharge (see Guide E 1239 and Practice E 1715).

5.3.7 Archive operations, including both filing current records to archive and retrieving old records for examination.

5.4 *Failure Categories*—When a failure happens, it shall be classified into one of the following categories. The categories are listed in order of severity, and a failure incident shall be classed by the most severe category in which it fits. See also 7.2 which condenses these categories for tabulation purposes.

5.4.1 Total loss of all functions.

5.4.2 *Loss of Primary Function*—One or more of the functions described above as primary cannot be used at all, or it produces incorrect results.

5.4.3 *Impaired Primary Function*—Operation of one of the primary functions is restricted, but can still be performed. For example, the electronic posting of test results to an Electronic Health Record is degraded or interrupted; also a high speed printer normally used to print patient test results may have failed, and so result reporting is instead carried out with a lower speed printer. Reports are delivered to the care settings late. This counts as an impaired primary function.

5.4.4 *Loss of Secondary Function*—One or more secondary function cannot be used at all, or it produces incorrect results.

5.4.5 Impaired secondary function.

5.4.6 *Loss of Redundancy*—Some systems have redundant components and they can continue to function even if some parts have failed. If such a failure does not cause an impaired primary or secondary function, it is classed as a loss of redundancy. This category is created for those systems that have multiple processors, maintain duplicate databases on different disk drives, or incorporate other such backup schemes to reduce the possibility there will be an interruption of service. It also includes loss of a peripheral device where there are others capable of performing the same task. Examples are small printers, terminals, bar code readers, and the like.

6. Failure Reports

6.1 A report shall be prepared for every separately identified failure. This report may consist of paper records or may be kept as a computer file with suitable programs for entry, correction, and retrieval. When records are kept in a computer, they shall be periodically backed up and archived so as to maintain their integrity in the event of a computer failure. An example failure report form for paper records is shown in Fig. 1. Appendix X1 gives a logical structure of a persistent data structure that is implementation-independent and could be implemented in several ways. It contains the same information given in Fig. 1 and discussed in 6.2. Each failure report shall contain the following information:

6.2 *Heading*—The report heading shall contain the following general information:

6.2.1 The report name, such as “Failure Report."

6.2.2 The name of the enterprise, hospital, company, or institution.

6.2.3 The name of the laboratory computer system to which the report applies.

6.2.4 The name of the person responsible for preparing the report.

6.2.5 The job title of the person preparing the report.

6.3 *Failure Category*—The failure shall be classified into one of the categories of total loss of all function, loss of primary function, impaired primary function, loss of secondary function, impaired secondary function, and loss of redundancy. See 5.3.1 to 5.3.7. This may be shown as six labeled boxes, one of which is to be checked or used as a term noting the category.

6.4 Time and date history of the failure.

6.4.1 The time and date for the eleven important milestones described in Section 4 shall be recorded. See 4.1 to 4.12. In many failure episodes, some of these milestones occur at the same time. If so, the subsequent responses may be entered as ditto marks.

6.4.2 A separate space shall be used to compute the total duration of the failure rounded to the nearest 0.1 h. Determine this time as the difference between the time of “resumption of normal operations” (4.12) and “failure occurrence" (4.2).

6.4.3 Optionally, other subtotals may be calculated, such as user action time, vendor response time, repair time, and recovery time. These may be useful for local management purposes.

6.5 Individual responsible for the repair. If more than one, it is sufficient to record the name of the senior person on the scene responsible for the service task group. The following should be recorded:

6.5.1 Name of the responsible service person.

6.5.2 Job title of this individual.

6.5.3 Employer or affiliation of the service person.

6.6 *Symptoms of the Problem*—The symptoms of the failure shall be recorded in sufficient detail to fully document the incident. It is also desirable to record the symptoms so that a similar problem in the future can be recognized and repaired more quickly. If a review of the failure reports indicates a reoccurring problem, then redesign of the system, replacement of a major component, a change in the building environment, or a modification of the operating procedures may be indicated.

6.7 *Repairs Made*—The nature of the repairs that have been made shall be recorded. This shall include an indication of the likely cause of the problem, and which components were replaced, fixed, changed, or adjusted.

6.8 *Probable Cause*—The most likely cause of the failure shall be determined and assigned to one of the following 4 categories. If the cause can be attributed to more than one category, choose the one deemed to be most responsible. The categories are:

6.8.1 *Hardware Failure*—This will be the usual category when replacement of a hardware component is able to fix the problem and it is determined that the component was not abused.

6.8.2 *Software Failure*—If revised software is needed to correct the difficulty, the failure is classified as a software failure.

6.8.3 *User/Site Problems*—If the problem can be traced to a failure of the air conditioning, electric power system, or other environmental conditions, count the failure in this category. Include here all problems that are caused by user errors and failures to follow operating and maintenance procedures. For tabulation purposes, all failures due to the way the system was operated are counted here. If more detailed accounting is desired, the actual cause of the failure is described in 6.6 and can be used for additional optional summaries. Note that excessive failures due to operator errors may indicate a system design that has insufficient protection against common mistakes.

6.8.4 *Unknown/Miscellaneous*—Use this last category for those failures where the cause cannot be determined or the reason does not fall into one of the above categories.

6.9 *Comments*—A space for general comments shall be provided. Any special circumstances or occurrences can be recorded in this space.

6.10 *Exceptions*—When the reliability records are not being kept in a computer file, and if the maintenance vendor has a suitable report with a different format, it is acceptable to attach a copy of the vendor's report to replace those items described above, but only where the information would be the same. Acceptability of a repair vendor report shall be verified by the system managers.

7. Reliability Report

7.1 A standard reliability report is defined in this section. It is useful for regular system records, for reports to administrators, when questions of computer system reliability arise, when hosting site visits, during reviews by professional groups, and for any required reports to regulatory agencies.

7.2 Timetable.

7.2.1 The reliability report shall be prepared at the beginning of each time period, for example, a month, and it shall include a summary of all failure events that were solved during the previous month. If a failure event crosses a time period boundary, it is counted only in the month in which it ends.

7.2.2 In addition, a yearly report shall be prepared at the beginning of each year. It shall be a cumulative summary of the monthly reports of the preceding year.

7.3 The reliability report will separate failures into two categories on the basis of their impact on the operation of the laboratory. This is a condensation of the six failure categories used in individual incident reports (see 6.2). It allows the more serious and less serious failures to be treated separately, but avoids the confusion of having six different summary tables of the type described below. It is a compromise between conciseness and specificity for the reliability summary report.

7.3.1 Level 1 failures include Total Loss of System and Loss of a Primary Function. This level includes failures that meet the definitions of 5.2.1 to 5.2.13.

7.3.2 Level 2 failures include the categories of failure defined by 5.3.1–5.3.7.

7.4 Failures will also be classified by their duration. In most hospitals, the longer a failure lasts, the bigger it's impact on operation of the laboratory. Use the total failure duration as defined and calculated in 6.4.2 to determine

how to classify each failure incident. The following time intervals are defined for purposes of summarizing the reliability data.

7.4.1 *Up to 1 h*—Any failure that lasts less than 1 h falls in this category. This interval is selected because failures this short usually have small impact on the laboratory.

7.4.2 *From 1 to 4 h*—Failures in this range usually require that short duration backup procedures be employed.

7.4.3 *From 4 to 24 h*—After 4 h, full backup procedures are often needed.

7.4.4 *More than 24 h*—Failures of long duration are the most disruptive.

7.5 *Report Content*—Each report shall consist of the following information. An example report is given in Fig. 2.

7.5.1 Report heading shall consist of:

7.5.1.1 The name of the report, such as “Laboratory Computer System Reliability Summary."

7.5.1.2 The name of the hospital, company, or institution.

7.5.1.3 The identification or name of the laboratory computer system to which it applies.

7.5.1.4 The name and job title of the person preparing the report.

7.5.1.5 A place to identify whether this is a monthly or yearly report and to indicate which year or month the report covers. If the system is newly installed, and has not yet been in operation for a whole month or whole year, this space will be filled with the words “First nn days," where nn is the number of days the system has been in operation. In a similar manner, the words “Last nn days" is used when a system is retired from use during the month or year covered by the report.

7.5.2 The body of a reliability report shall contain a table giving the number of Level 1 failure incidents during the covered time period grouped by probable cause and failure duration.

7.5.2.1 The table will consist of 5 columns labeled “up to 1 hour,” “1–4 hours,” “4–24 hours,” “over 24 hours,” and “summary.” The table will have 5 rows labeled “hardware cause,” and “summary.”

7.5.2.2 Count the number of Level 1 failures that occurred in the time period covered by the report that lasted less than 1 h and were attributed to hardware. Enter this count in row 1 of column 1. Enter the total number of software-caused Level 1 failures that lasted less than 1 h in the second row of column 1. In a similar manner, fill in the rest of the first 4 rows of the first 4 columns.

7.5.2.3 Add all of the failures caused by hardware (across row 1) and enter that value in row 1 column 5. Add all the failures less than 1 h and put that value in row 5 of column 1. In a similar manner, fill in the rest of the summary column and summary row.

7.5.2.4 The total number of Level 1 failures in this time period should be entered in row 5 column 5.

7.5.3 The body of the reliability report shall also contain a summary of the Level 2 failures. Fill in another table identical in format to the Level 1 failures using the same directions as 7.5.2.1–7.5.2.4, except this time use only those failures that meet the Level 2 criteria as defined in 7.3.2.

7.5.4 Compute the following miscellaneous statistics and enter them in special spaces provided in the reliability summary report form.

7.5.4.1 Sum the failure duration times (6.4.2) found in the individual failure reports for all Level 1 failures that occurred during this reporting time, and enter the total time for level 1 to the nearest 0.1 h.

7.5.4.2 Sum the failure duration times (6.4.2) found in the individual failure reports for all Level 2 failures that occurred during this reporting time, and enter the total time for Level 2 to the nearest 0.1 h.

7.5.4.3 Sum the failure duration times found in 7.5.4.1 and 7.5.4.2 and report the total time the system experienced Level 1 or Level 2 problems. Report this as the total time impaired. Optionally, additional summaries or percentages may be calculated for internal management purposes, such as user action time, vendor response time, repair time, or recovery time.

7.5.4.4 Determine the time scheduled, or number of hours that the system should have been operating during this reporting time. Subtract the time impaired found in 7.5.4.3 and divide this difference by the time scheduled. Multiply the resulting fraction by 100. Report the percent time the system was perfect.

$$\% \text{ time perfect} = \frac{\text{Time Scheduled} - \text{Time Impaired}}{\text{Time Scheduled}} \times 100 \qquad (1)$$

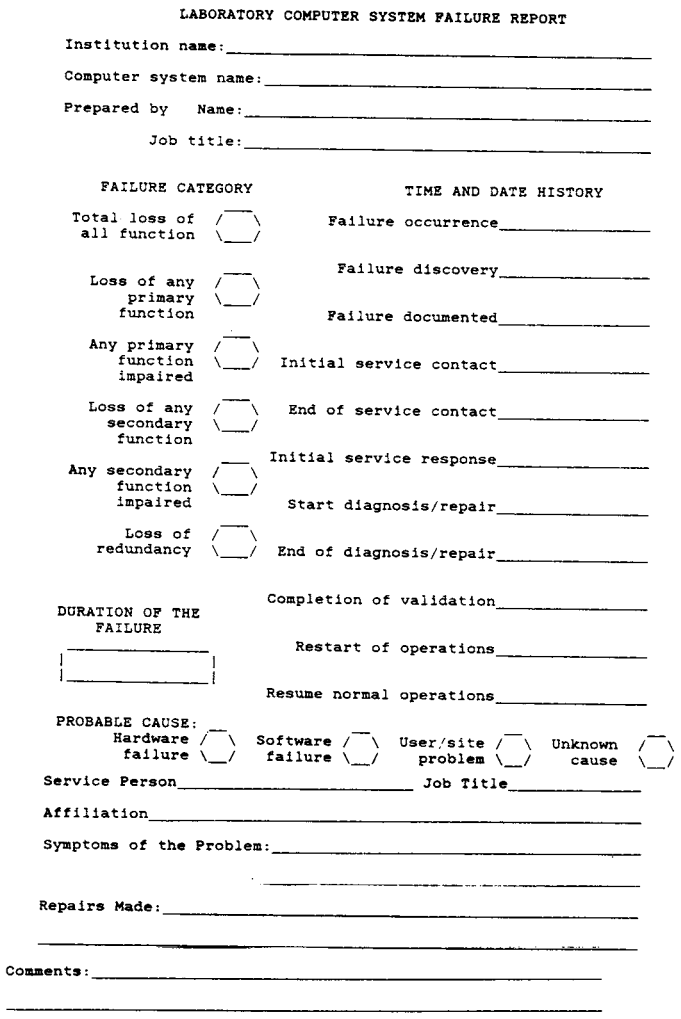


FIG. 1 Example Failure Report

LABORATORY COMPUTER SYSTEM RELIABILITY SUMMARY

Institution name _____ Computer System Name _____

Prepared by _____ Job title _____

For the month/year of _____

NUMBER OF LEVEL 1 FAILURES

	Up to 1 hour	1 - 4 hours	4 - 24 hours	Over 24 hours	Summary
Hardware failures					
Software failures					
User/Site problems					
Unknown cause					
Summary					

NUMBER OF LEVEL 2 FAILURES

	Up to 1 hour	1 - 4 hours	4 - 24 hours	Over 24 hours	Summary
Hardware failures					
Software failures					
User/Site problems					
Unknown cause					
Summary					

Total level 1 down time	Total level 2 down time	Total impaired time	Percent time perfect

FIG. 2 Sample Reliability Report

APPENDIX

(Nonmandatory Information)

X1. FAILURE REPORT DATA STRUCTURE

X1.1 Data Structure:

System Name (M) ←[horbar][horbar][horbar][horbar][horbar][horbar][horbar]
Component System (M) [horbar][horbar][horbar][horbar]|
Institution
Failure Event Discovery Date-time (M)
Failure Category
Probable Cause
Failure Documentation Date-time
Initial Service Contact Date-time
Start Diagnosis/Repair Date-time
End Diagnosis Repair Date-time
Complete Validation Date-time
Restart Operations Date-time
Resume Normal Operations Date-time
Duration of Failure
Person Preparing Report
Service Person Name
Symptoms
Repairs made
Comments

NOTES

NOTES

NOTES

NOTES

NOTES

NCCLS ▼ 940 West Valley Road ▼ Suite 1400 ▼ Wayne, PA 19087 ▼ USA ▼ PHONE 610.688.0100
FAX 610.688.0700 ▼ E-MAIL: exoffice@nccls.org ▼ WEBSITE: www.nccls.org ▼ ISBN 1-56238-494-5