

# Diagnostic Specification—A Proposed Approach

**W. H. Carroll**

Air Force Directorate of Nuclear Surety,  
Kirtland AFB

**V. L. Linden**

Air Force Test and Evaluation Center,  
Kirtland AFB

**C. R. Waldo**

Air Force Test and Evaluation Center,  
Kirtland AFB

**Key Words**—Fault detection, Fault isolation, Mean time to repair.

**Reader Aids**—

**Purpose:** Present considerations in diagnostic specifications.

**Special math needed:** None.

**Results useful to:** Acquisition agencies and contractors.

**Abstract**—The U.S. Air Force experience with operational test and evaluation of weapon system diagnostics has not been good. Many of the problems encountered stem from poorly written specifications. The development of successful diagnostic systems is predicated on the user's identifying valid system requirements and accurately articulating these requirements, via specifications, to the contractor.

This paper identifies important considerations in developing user requirements and presents an approach to diagnostic specifications for future systems.

## 1. INTRODUCTION

Automatic diagnostics are intended to provide rapid detection and isolation of faults so that a system can be returned to an operational condition as quickly as possible. In addition, many diagnostic systems have been introduced with the intent of reducing the need for highly skilled technicians, extensive training, technical data, and support equipment. In these instances, the projected diagnostic capability has driven maintenance and support planning.

Recent U.S. Air Force operational test and evaluation (OT&E) experience with automatic diagnostics has shown that the capability of delivered diagnostics has in many cases fallen far short of expectations. In these cases the system has been unable to meet user requirements, with a resulting inadequate support posture, and in some cases, total invalidation of the maintenance concept. Much of the difference between anticipated diagnostic capability and what was delivered can be attributed to specifications that either inaccurately articulated the user's valid requirements, or accurately interpreted user requirements that were invalid.

This paper identifies important considerations in developing user requirements and presents an approach to diagnostic specifications for future systems.

## 2. CONSIDERATIONS IN THE DEVELOPMENT OF USER REQUIREMENTS

The development of successful diagnostic systems is predicated on the identification of valid systems requirements by the user. In developing such requirements the user must evaluate operational and logistics considerations and how they will be translated into system specifications.

**1. Operational Considerations.** The evaluation of operational considerations is the starting point for identifying system requirements. First, the user must determine the prime function of the system and relate it to the operational concept. Next, the user must identify any operational constraints that impact the system. Normally, these are translatable into limiting parameters within which the system must perform; for example, a required quick-turn-around time or missile build-up-rate. These parameters become the driving function, establishing the maximum repair time that will enable all operational scenarios to be accomplished. The system requirements developed from these considerations retain their validity only so long as the operational concept remains valid. If the concept or the prime function of the system changes, then, unless the possibility of change was allowed for, there is a high probability that the system will be unable to meet the changed requirement.

**2. Logistics Considerations.** Once operational constraints for the system have been established, meeting these constraints essentially becomes a problem of logistics. There are numerous logistics considerations that the user must evaluate in determining how best to develop a system that will meet operational requirement. First, the user must realize that no diagnostic system will provide 100 percent automatic fault detection/fault isolation (FD/FI) coverage for the entire spectrum of failure modes; that only through a combination of automatic diagnostics and manual procedures aided by support equipment, adequate technical data, and thorough training will 100 percent maintenance capability be achieved. With this realization, the user, in conjunction with the developer and acquisition agency, must decide on the mix of automatic and manual diagnostics that will best satisfy the operational requirement. In trying to optimize the diagnostic mix, the following must be considered: the available manpower; the skill levels of available personnel; desired maintenance concept; desired organizational structure; safety requirements; impact of diagnostic circuitry on system reliability; and the balance of costs between development of automatic diagnostics and manual diagnostic support. Once the diagnostic mix has been established, the user must employ an integrated approach that ties the development of the diagnostics to operational and logistics support elements of the system under development. The approach to user requirements is shown graphically by Figure 1.

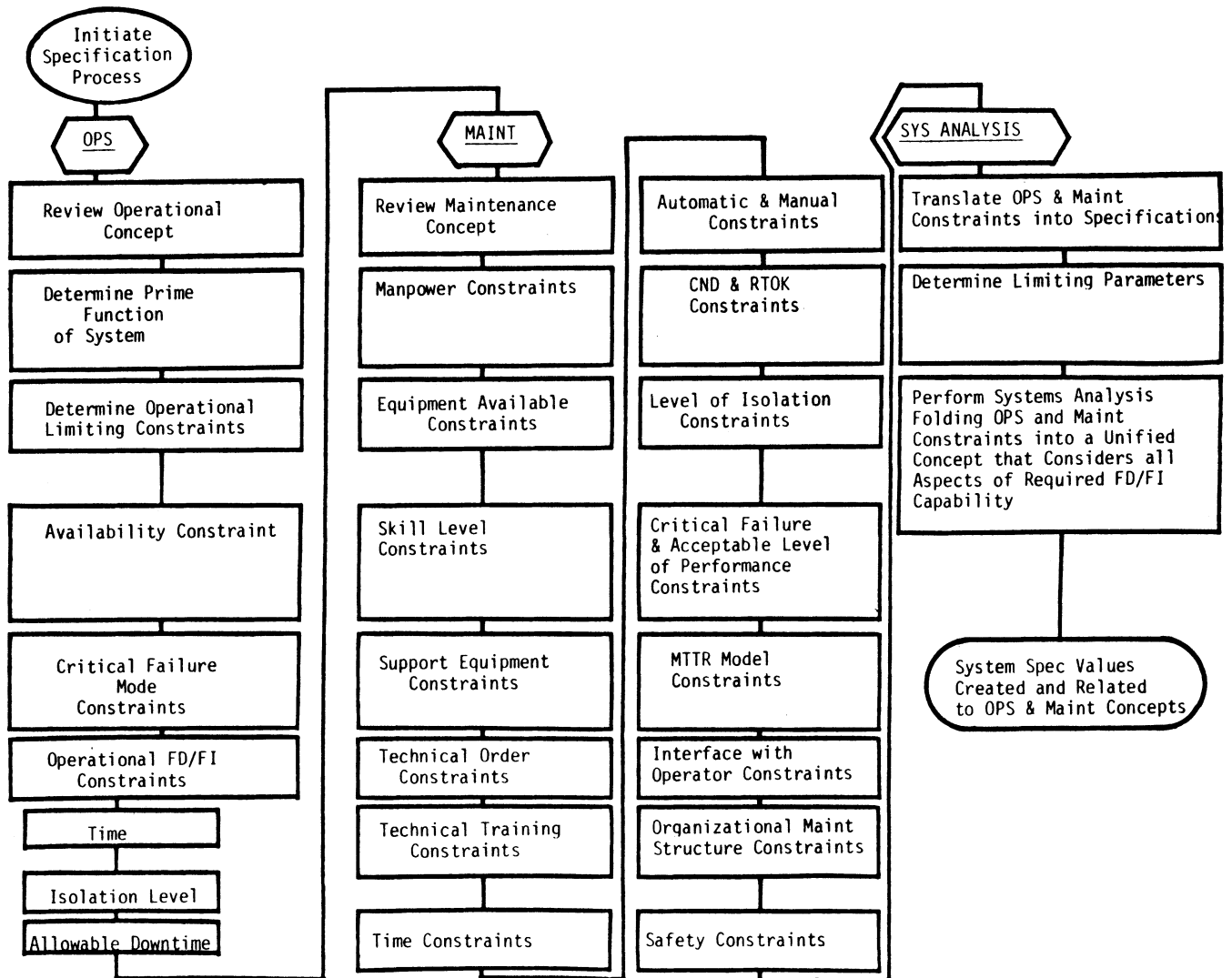


Fig. 1. Specification Process.

There are two important considerations in diagnostic development often overlooked by users in creating their requirements: the need for a back-up for automatic/diagnostics; and the need for parallel development. The cost of developing additional technical data and support equipment must be balanced against the possible loss of mission capability and time lost in after-the-fact development of manual capability in the event the automatic diagnostics fall short of expectations. The parallel development of logistic support elements is another important user consideration. The elements must complement each other if the system is to be successful. One area where failure to consider parallel development can degrade system effectiveness is that of automatic test equipment (ATE). Ideally, the capabilities of ATE at the three levels of maintenance (organizational, intermediate, depot) should form a pyramid; i.e., the testing tolerances should get tighter at the higher level of maintenance. This is known as a vertical testability. If parallel development is not considered, it is possible that the ATE would be developed us-

ing unrelated specifications. This could result in a problem being identified at a lower level which could not be duplicated at the higher levels of maintenance.

3. *Translating User Requirements.* Once the user has considered all of the factors involved and developed a set of valid requirements, it is necessary to convey those requirements to the contractor via specifications. In order to insure the fidelity of the translation of requirements to specifications, the user and the contractor must agree on terminology and the specific approach employed to meet the user requirements.

A. *Diagnostic Terminology.* Differing terminology is used within the DoD and industry to describe a diagnostic system's automatic capability. Some examples are fault-detection / fault-isolation (FD/FI); fault-detection / isolation (FD/I); built-in test / fault-isolation test (BIT/FIT); self-test / built-in test (ST/BIT); and built-in test equipment/built-in test (BITE / BIT). The proliferation of such terminology has resulted in confusion and misunderstanding. The basic intent of diagnostic

terminology is to portray the same meaning: automatic FD and automatic FI. This basic intent, however, might not be satisfied, depending on how a diagnostic system is mechanized. To illustrate this point, Table 1 shows the FD/FI terminology used in three recent programs.

Table 1  
FD/FI Terminology

PROGRAM		FAULT DETECT	FAULT ISOLATE
E-3A		BIT	FIT
F-16	Flight Control	ST/BT	BIT
F-16	MUX BUS	BIT	BIT
EF-111A		BITE	BIT

The E-3A terminology for diagnostic capability was the term BIT/FIT. The system has automatic detection (BIT) and semiautomatic isolation (FIT). The semiautomatic isolation capability is a result of the requirement for an active operator interface when FI is accomplished. In the case of the F-16, ST/BIT means semiautomatic operation as a result of an active operator-interface specifically in the flight control system, while BIT refers to automatic FI on detection of a fault. For the Multiplexer Bus (MUX BUS), BIT refers to both automatic FD and FI. Finally, BITE and BIT in the EF-111A means semiautomatic FD and FI due to active operator-interface.

It is readily apparent that diagnostic terminology differs from program to program, causes confusion and doesn't always accurately connote total automatic FD and FI. Consequently, diagnostic terminology must be clearly understood before being used in contractual specifications. Table 2 proposes standardized diagnostic terminology that could be used by both the DoD and industry to accurately reflect FD and FI capabilities.

Table 2

Proposal for Standardized Diagnostic Terminology

MODE	CAPABILITY	FAULT DETECTION	FAULT ISOLATION
AUTOMATIC		AFD	AFI
SEMI-AUTOMATIC		SFD	SFI

Table 2 uses four different terminologies to connote a system's capability is reflected in the first letter of each term which denotes the intended mode, that is, A for automatic and S for semiautomatic. Therefore, the key to this set of proposed standardized diagnostic terminology lies in the definitions of the terms automatic and semiautomatic, as follows:

- A Automatic - FD and/or FI without operator interface.
- S Semiautomatic - FD and/or FI with operator interface which might require operator use of support equipment and technical data.

**B. Typical Approach to Satisfy Requirements.** In specifying diagnostic systems, both the user and the acquisition agency must understand the strategies by which the contractor can satisfy the user's requirements. An understanding of these strategies provides the basis for creating meaningful specifications. For example, suppose a user requirement for a 90 percent FD and 80 percent FI diagnostic capability is generated and specified by the acquisition agency. The developer could use the basic model as depicted in Figure 2 in complying with the specification

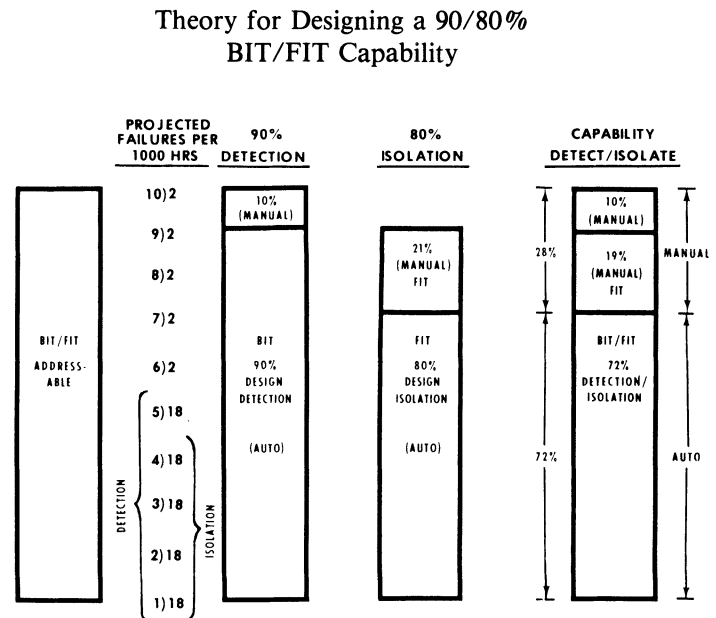


Fig. 2. Design Model.

requirements and implicit program cost constraints. Column 1 represents the system to be developed and the line replaceable units (LRUs) theoretically addressable by FD/FI diagnostics. This system consists of 10 LRUs, each possessing a specific failure rate as shown in column 2. From a design standpoint, the 90 percent detect rate can be met by providing 100 percent detection capability for the first five LRUs based on the failure rates as shown. The developer does not have to provide a fault detect capability for nine of the ten LRUs as one intuitively may have thought. The 90 percent detect capability (first five LRUs) is defined as "automatic detection" under column 3. Faults within the remaining 10 percent will be manually troubleshot since they have a low projected probability of occurrence. Moreover, FI in column 4 is treated in the same manner as FD. Based on failure probabilities, only four of the five LRUs detected have to be isolated through the automatic capability in order to meet the 80 percent requirement. Manual troubleshooting techniques are used to fault isolate the remaining LRUs (5 through 10). Based on the probability of failure for each LRU, column 5 shows the design of a system that contains: an automatic detect and isolate capability of 72 percent (90 percent FD  $\times$  80 percent FI); an automatic detect and manual isolate

capability of 18 percent; and a manual detect and isolate capability of 10 percent.

### 3. PROPOSED SPECIFICATION.

The proposed specification is based on three general factors: diagnostic system performance parameters; diagnostic system time limitations; and required constraints. Suggested specifications are discussed under each factor.

1. *Performance.* The two basic performance parameters in specifying diagnostic systems are the detection rate and isolation rate. Whether these two parameters should be specified separately or combined into a single parameter depends on the requirements of the system.

A. The FD capability shall provide for an  $\underline{X}$  percent detection of system faults addressable by FD capability using automatic procedures.

B. The FI capability shall provide for a  $\underline{Y}$  percent isolation capability of system faults addressable by FI capability using automatic procedures.

C. Should the decision be made to state these requirements as the combined value of the detection and isolation rates, the following method is suggested. A combined requirement for FD/FI capability shall provide for a  $\underline{Z}$  percent detection and isolation of system faults addressable by automatic diagnostic capability using automatic procedures. The combined requirement is composed of distinct FD and FI capabilities. The individual values for  $\underline{X}$  percent and  $\underline{Y}$  percent may vary within the range defined by the following equation:

$$(\underline{X} \text{ percent}) (\underline{Y} \text{ percent}) = \underline{Z} \text{ percent}$$

where,  $\underline{Z}$  percent is a constant (required value) and  $\underline{X}$  percent and  $\underline{Y}$  percent are variable values.

D. Isolation of a fault worked with the automatic diagnostic capability must be accomplished, unambiguously to the (specify level) level for  $\underline{E}$  percent of all diagnostic isolations.

E. One hundred percent detection and isolation shall be required for all critical fault modes. A critical failure mode is one which will result in catastrophic failure, death, or injury if not corrected.

2. *Time Limitations.* Time limitations are the diagnostic system's capability to meet the constraints dictated by the operational and maintenance concepts. The index determining this quality is system mean-time-to-repair (MTTR).

A. MTTR is composed of setup, troubleshoot (FD/FI), remove/replace/repair, and verification of corrective action (checkout). The system MTTR associated with the automatic diagnostic system shall not exceed  $\underline{T}$  clock hours. The maximum repair time shall not exceed, in the 99th percentile case,  $\underline{T} + \underline{S}$  clock hours when accomplished by a (specify number) person maintenance crew with a skill level of (specify skill level), where  $\underline{S}$  is the difference between required maximum repair time and the

desired MTTR.

B. The frequency of operations using automatic techniques, as measured by the number of maintenance actions, shall be equal to  $\underline{Z}$  percent value. The frequency of operations requiring manual techniques shall be equal to  $100 - \underline{Z}$  percent. Manual techniques are employed when automatic procedures reach an unresolved condition, and usually involve the use of procedures and capabilities requiring skill levels higher than automatic techniques.

C. The MTTR time model for the average maintenance action processed by automatic capability should be structured similar to the following examples:

- a. Setup — 10 percent of MTTR or  $\underline{P}$  minutes, whichever is greater, where  $\underline{P}$  represents a projected set-up time.
- b. Trouble-shooting (FD/FI) — 50 percent of required MTTR.
- c. Remove/replace/repair time — 30 percent of MTTR.
- d. Verification of corrective — 10 percent of MTTR or  $\underline{R}$  minutes, whichever is greater, where  $\underline{R}$  represents a projected verification time.

3. *Constraints.* Constraints deal with the minimization of adverse factors that would degrade the automatic diagnostic capability in relation to stated requirements.

A. *FD Cannot Duplicate (CND)* — CNDs shall not exceed some percent of all faults addressable by automatic detection capability. A CND results when the FD capability detects a fault which cannot be confirmed during subsequent troubleshooting. CNDs can be caused by various factors, such as test tolerances being too tight or not applicable to the domain of the failure mode, momentary excursions of the measured test parameter, effects of other equipment loading factors, or environmental effects. They can also be caused by effects such as test voids, testing incompatibilities, and operator and maintenance errors. In any case, because a failure was indicated to the operator, these events can result in generating a maintenance action where no failure may be apparent to the technician in subsequent testing.

Care must be taken when specifying the CND rate to preclude conflict with the proposed FD rate. For example, if you specify a FD rate of 90 percent and maximum allowable CND rate of 30 percent, you are essentially saying that you only need to accurately detect 63 percent of FD/FI addressable faults ( $0.90 \times (1 - .30) = 0.63$ ). From the standpoint of the technician, the practical FD capability, considering the effects of CNDs, would be 63 percent even if the theoretical 90 percent FD rate had been attained.

B. *Retest OK (RTOK)* — RTOKs shall not exceed some percent of all faults detected and isolated by the automatic diagnostic capability when the item is subsequently processed by the intermediate/depot repair facility. RTOKs result from the failure to confirm a fault at the

intermediate or depot level even though the FD/FI system has identified a faulty component. Similar of the effects of CNDs on FD capability, RTOKs degrade the practical FI capability of a system. For example, if a FI rate of 79 percent is specified with an allowable RTOK rate of 30 percent, then a failure can only be accurately isolated 55 percent of the time ( $0.79 \times (1 - 0.30) = (0.55)$ ). As with CNDs, the technician sees the practical fault-isolation capability as 55 percent, not the 79 percent theoretically possible. The problems associated with vertical testability, previously mentioned, are particularly apt to contribute to the distortion effects of RTOKs on the FI capability. The RTOKs cause an expenditure of man-hours at the intermediate and depot levels and reduce the amount of pipeline spares.

Diagnostic specifications should call for a planned demonstration point within the acquisition process where the diagnostics are to be tested by the user under actual operational conditions. It is at this demonstration point where it must be determined whether the diagnostics meet user requirements. If not, the risk of continued development must be assessed, as well as the consideration of specific trade-offs to offset any diagnostic shortfalls. For example, if, in a system being developed for only two levels of maintenance (organizational and depot), it is discovered that the diagnostic system falls appreciably below the specifications, it might mean that if the diagnostic system cannot be further improved, a change in the maintenance concept (such as the addition of intermediate maintenance capability) is warranted. Such a drastic change would also require parallel changes in other logistic support elements, such as technical orders, support equipment, spares, manpower, and training.

#### 4. SUMMARY

Diagnostic requirements must be related to the user's operational maintenance concept. The user and acquisition agency must fully understand the developer's FD/FI

tion agency must fully understand the developer's FD/FI design theory and must employ a standardized diagnostic terminology in addressing the proposed system. Support equipment systems must ensure that testing of the suspected failure is consistent and compatible throughout all levels of maintenance. It must also be recognized that there will always be maintenance faults beyond an automatic FD/FI system's capability. Therefore, maintenance technicians must be provided with clear and complete procedures for dealing with such situations. Developer achievement of specifications must be demonstrated in an operational environment. Finally, the specification of requirements for a diagnostic system should be clearly defined in terms of performance capabilities, time limitations, and constraints.

#### AUTHORS

William H. Carroll; Air Force Directorate of Nuclear Surety; Kirtland AFB, New Mexico 87117 USA.

**Lt. Col. William H. Carroll:** has a BS in Electrical Engineering from the University of New Hampshire, a BA in physics from the University of California at Berkeley, and an MBA from the University of New Mexico. He recently completed a 4-year tour at the Air Force Test and Evaluation Center (AFTEC) where he served as the Chief, Aerospace Systems Branch, Directorate of Logistics.

Vincent L. Linden; Air Force Test and Evaluation Center (AFTEC/LGL); Kirtland AFB, New Mexico 87117 USA.

**Major Vincent L. Linden:** has a BS in Biochemistry from Saint Joseph's College, Rensselaer, Indiana, and a MA in Education from George Washington University, Washington, D.C. He is assigned to the AFTEC Logistics Assessment Procedures Branch, Logistics Directorate.

Clarence R. Waldo; Air Force Test and Evaluation Center (AFTEC/LGMA); Kirtland AFB, New Mexico 87117 USA.

**Lieutenant Clarence R. Waldo:** has a BS in Industrial Technology from Southern Illinois University, Carbondale. He is working for an MS degree in Systems Management through the University of Southern California. He is a program manager in the Aerospace Systems Branch, Logistics Directorate.

Manuscript TR80-174 received 1980 December 8; revised 1981 February 2. ★ ★ ★

## Manuscripts Received

For Information, write to the author at the address listed; do NOT write to the Editor

"Overall reliability evaluation for large computer communication networks: An MHC approach", Dr. K. K. Aggarwal; Electronics & Comm. Engg. Dept.; Regional Engineering College; Kurukshetra 132 119 INDIA. (TR81-48)

"A tightened multilevel continuous sampling plan for Markov-dependent production process", V. S. Sampath Kumar; Dept. of Statistics; University of Poona; Pune - 411 007 INDIA. (TR81-43)

"Using the decomposition-tree of a network in reliability computation", Dr. Jane N. Hagstrom; Dept. of Quantitative Methods; University of Illinois; Box 4348; Chicago, IL 60680 USA. (TR81-44)

"Estimation of fault-coverage by statistical-sampling of faults", Dr. Wayne Nelson; 37-578; GE Corp. R&D; Schenectady, NY 12345 USA. (TR81-41)

"Cost-effective analysis of typical substation arrangements", W. J. Lannes; Louisiana Power & Light; POBox 6008; New Orleans, LA 70174 USA. (TR81-45)

"Stress-margin setting", Keisuke Yamamoto (FU-088); IBM Japan Ltd.; 1 Kirihara-cho, Fujisawa; Kanagawa, 252 JAPAN. (TR81-50)

"Interference analysis for Bernstein-distributed strength and stress", Dr. Munir Ahmad; University of Petroleum & Minerals; Box 476; Dhahran, SAUDI ARABIA. (TR81-47)