AEROSPACE INFORMATION REPORT

AIR4845™	REV. A
Issued 1993-06 Stabilized 2022-04 Superseding AIR4845	

The FMECA Process in the Concurrent Engineering (CE) Environment

RATIONALE

It is recommended that this document be stabilized due to the release of the new SAE J1739 FMEA Standard. This document will address all content within AIR4845. Once this document has accepted in the industry, there is a need to keep AIR4845 available for current customer use.

STABILIZED NOTICE

This document has been declared “Stabilized” by the SAE G-41 Reliability Committee and will no longer be subjected to periodic reviews for currency. Users are responsible for verifying references and continued suitability of technical requirements. Newer technology may exist.

TO PLACE A DOCUMENT ORDER: **Tel: 877-606-7323 (inside USA and Canada)**
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: **http://www.sae.org**

For more information on this standard, visit
https://www.sae.org/standards/content/AIR4845A/

FOREWORD

This SAE Aerospace Information Report (AIR) by the G-11AT (Automation and Tools) subcommittee of the SAE G-11 RMS Committee, examines in detail the failure mode, effects and criticality analysis (FMECA) and how it relates to concurrent engineering. FMECA is probably the most labor intensive analysis performed by any of the RMS disciplines. The report outlines the FMECA process and the users of the FMECA as it is currently performed and indicates the various requirements which the analysis satisfies. Suggestions are made on which parts of the current process could be automated and how this may be accomplished. Finally a set of recommendations are given for integrating FMECA automation into the concurrent engineering process.

TABLE OF CONTENTS

1. SCOPE:

This AIR by the G-11AT (Automation and Tools) subcommittee, examines the failure mode, effects and criticality analysis (FMECA) requirements and procedures as performed on current and earlier vintage engineering programs. The subcommittee has focused on these procedures in relation to the concurrent engineering (CE) environment to determine where it may be beneficial, to both FMECA analysts and users, to automate some or all of the FMECA processes.

Its purpose is to inform the reader about FMECAs and how the FMECA process could be automated in a concurrent engineering environment. There is no intent on the part of the authors that the material presented should become requirements or specifications imposed as part of any future contract.

The report is structured to include the following subjects:

a. A FMECA overview
b. The current FMECA process
c. FMECA in the concurrent engineering environment
d. FMECA automation
e. The benefits of automation

2. REFERENCES:

The following publications form a part of this specification to the extent specified herein. The latest issue of all SAE Technical Reports shall apply.

2.1 SAE Publications:

Available from SAE, 400 Commonwealth Drive, Warrendale, PA 15096-0001.

2.1.1 Reliability, Maintainability & Supportability Guidebook (Ref. ISBN 1-56091-039-9). By SAE G-11 RMS Committee.

2.1.2 ARP926 Fault/Failure Analysis Procedure, (SAE Aerospace Recommended Practice) Revised 11-15-79. By: SAE S-18 Ad Hoc Committee to update ARP926.

2.2 Military Publications:

Available from Standardization Documents Order Desk, Building 4D, 700 Robbins Avenue, Philadelphia, PA 19111-5094.

2.2.1 Procedures for Performing a Failure Mode, Effects and Criticality Analysis (Ref. Mil-Std-1629A). By Department of Defense.

2.2.2 Reliability Program for Systems and Equipment Development and Production (Ref. Mil-Std-785B). By Department of Defense.

2.2.3 Military Standard System Safety Program Requirements (Ref. Mil-Std-882B). By Department of Defense.

2.2.4 Potential Failure Mode and Effects Analysis in Design (Design FMEA) and for Manufacturing and Assembly Processes (Process FMEA) Instruction Manual by Ford Motor Company, September 1988.

2.3 Other Publications:

2.3.1 Memorandum for Secretaries of the Military Departments-- Subject: Concurrent Engineering - A Total Quality Management Process. By: Dr. R. Costello, OSD/USD(A), 9 March 1989.

2.3.2 Results of the Aeronautical Systems Division Critical Process Team on Integrated Product Development. By: Lavern J. Menker, Deputy Chief of Staff, Integrated Engineering & Technical Management, November 1990.

2.3.3 Nonelectronic Parts Reliability Data 1991 (NPRD-91). By Reliability Analysis Center, Rome Laboratory, Griffiss AFB, NY 13441-5700, 1 May 1991.

2.4 List of Acronyms:

AI	Artificial Intelligence
AFSC	Air Force Systems Command
BIT	Built-in Test
CAA	Civil Aviation Authority
CAD	Computer Aided Design
CAE	Computer Aided Engineering
CALS	Computer-aided Acquisition and Logistics Support
CDR	Critical Design Review
CE	Concurrent Engineering
CID	Change in Design
DOD	Department of Defense (U.S.)
FAA	Federal Aviation Administration (U.S.)
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
G-11	SAE RMS Committee
G-11CR	SAE G-11 Computerization of RMS Subcommittee
ILS	Integrated Logistics Support
IPD	Integrated Product Development
IPT	Integrated Product Teams
JAA	Joint Airworthiness Approval
LCC	Life Cycle Cost
LCN	Logistic Support Analysis Control Number
LSA	Logistic Support Analysis
LSAR	Logistic Support Analysis Record
M	Maintainability
MIL-HDBK	U.S. Military Handbook
MIL-STD	U.S. Military Standard
MTBF	Mean Time between Failures
NASA	National Aeronautics and Space Administration
OODB	Object Oriented Data Base
PC	Personal Computer
PDR	Preliminary Design Review
PHS&T	Packaging, Handling, Storage and Transportation
QA	Quality Assurance

2.4 (Continued):

R	Reliability
RCM	Reliability Centered Maintenance
RLA	Repair Level Analysis
R&M	Reliability and Maintainability
RMS	Reliability, Maintainability and Supportability
RPN	Risk Priority Number
S	Supportability
SAE	Society of Automotive Engineers
STEP	STandard for the Exchange of Product data
US	United States
USAF	United States Air Force
USN	United States Navy
WUC	Work Unit Code

3. TECHNICAL REQUIREMENTS:

3.1 FMECA Overview:

Failure mode and effects analysis (FMEA) is a logical, structured analysis of a system, subsystem, piece part, or function. Identified in the analysis are potential failure modes, their causes and the effects associated with the failure mode's occurrence at the piece part, subsystem and system levels and its severity rating. FMECA is an extension of the FMEA task, where each failure mode is evaluated for its "criticality", i.e. an assessment of the severity of the event at the "system" level and the probability of its occurrence.

A FMECA provides a basis for the recognition of failure modes developed from historical "lessons learned" data bases of similar equipment and the unacceptable effects which limit the achievement of design requirements. FMECA is best performed as early as possible in the design process in order to verify adequacy of the design, change the design if not adequate, and/or incorporate appropriate controls. Problems discovered during the design phase are much easier and less costly to correct than if they are identified after hardware has been produced. In addition, FMECA also provides:

a. A common communication tool between product designers, manufacturing engineers, test engineers, reliability and maintainability (R&M) engineers, and logistic support analysts.

b. A means of identifying potential single point failure modes.

c. A means for identifying the types of test and testing environments needed to certify whether a design or process is suitable.

d. The basis for the evaluation and/or certification of changes in design, process, or materials.

e. A means of identifying Reliability Critical Items.

3.1 (Continued):

The FMECA process is addressed in this document in terms of its structure, the requirements of the user and potential opportunities for automation, in order to better adapt the FMECA into an integrated product development environment, encompassing design, manufacturing, quality and product assurance. These automation alternatives are discussed in the report together with recommendations and the benefits to be gained by the user from automating.

Paragraph 3.2 examines the current FMECA process in a largely manual environment. It identifies the types of data needed for the analysis, sources of that data, who uses it and for what. The last part of paragraph 3.2 describes the difficulties with the current process that may be alleviated by automation within a concurrent engineering environment. Since all of the sources of information normally needed for the FMECA are represented on a concurrent engineering design team, that environment facilitates the analysis - in fact, FMECA plays a central role in the CE process. Paragraph 3.3 gives a general overview of concurrent engineering and how FMECA will fit into that environment. The availability of data in a CE environment is conducive to automating much of the FMECA. Many possibilities and approaches for doing this are addressed in paragraph 3.4. Prioritization of tasks for automation will depend on the individual company's situation and needs.

It should be pointed out that many of the approaches and techniques described in the report are more applicable to large companies with sizable FMECA tasks to perform. Several off-the-shelf computer programs are available to help smaller companies document the FMECA analysis. Some of these do as little as enhance formatting and editing the FMECA report while others have features designed to improve the quality of the analysis.

3.2 The Current FMECA Process:

Failure modes are often determined by subjective assessment based on the past records of similar existing systems. The effects of failure mode interaction and propagation are estimated from analysis of comparable systems. This qualitative and rather abstract approach makes it difficult to draw a decisive conclusion on the criticality of specific design items. To make matters worse, it is often difficult to find data for comparable systems which reflect the current materials technology or state of the design art. Also, the FMECA is often not conducted until the design is nearing completion, which lessens its impact as a tool for improving the product.

3.2.1 FMECA Needs: A FMECA must meet the needs of multiple users. The users served by this reliability tool can be broken into two major groups, internal users and customer/ contract users. Typical internal users are:

a. Design
b. Reliability
c. System safety
d. Maintainability/human factors

3.2.1 (Continued):

e. Logistics support
f. Quality assurance
g. Manufacturing
h. Systems
i. Testability
j. Internal Regulatory Agency Representative

Typical customer/ contract users are:

a. Prime contractors
b. Government agencies (e.g. FAA, USAF, USN, US Army, NASA)

Each of these users has different needs that must be served by the FMECA. The following sections contain brief descriptions of the users, their functional responsibilities and their perceived FMECA needs.

3.2.1.1 Internal Users:

3.2.1.1.1 Design: Design has overall responsibility for product engineering, analysis, and detailed design. The fundamental reason for doing a FMECA is to improve the product design. Therefore the most important FMECA user is the design engineer, since the design engineer uses the FMECA to address potential failure modes, causes, and effects, developed from previous "lessons learned", and designs the product to remove, mitigate, or compensate for unacceptable failure modes or failure mode effects.

In most companies the design engineer is a major contributor to the FMECA by providing schematics, logic diagrams, drawings and other detailed product input to the FMECA analyst. The essence of producing a meaningful FMECA, which impacts the product design and benefits the end-user, is a close working cooperation between the reliability engineer (who has overall responsibility for coordinating all FMECA data elements) and the design engineer (who has the detailed product knowledge and the ability to make the design changes dictated by the analysis).

3.2.1.1.2 Reliability: Reliability engineering is responsible for providing analyses to assess the probability of the product successfully performing its intended function in a specified operating environment over a given period of time. FMECA provides reliability engineering with a direct interface to the designer, to ensure that the product meets or exceeds reliability goals and requirements. Reliability engineering has the overall responsibility for developing and maintaining the FMECA data base. This entails coordinating input from design engineering with that of the R, M & S functions into the complete FMECA format. The completed FMECA is the basis for future design and cost trade-off analyses of major hardware items. Documentation supporting changes in design (CID's) compares potential failure modes and compensating provisions of the proposed new design to

3.2.1.1.2 (Continued):

those of the baseline design. Reliability engineering is responsible for the FMECA input to the LSA and failure rate predictions for the failure modes of the hardware design.

3.2.1.1.3 System Safety: System safety engineering provides analyses which prove that a product can be safely operated and maintained in its intended operating environment. Safety is responsible for developing system and subsystem hazard analyses which identify potential Category I and II hazards (see Mil-Std 882B for detailed definitions) and indicate the piece parts and/or subassemblies which could cause them. The FMECA is a source for identifying failure modes and causes which can lead to these hazards. The criticality analysis portion of the FMECA identifies and quantifies hazard probabilities within these categories. The FMECA requirements for safety engineering, therefore, are similar to those of the LSAR except that generally they only consider the two most serious hazard categories. A close working cooperation should exist between the reliability engineer and the safety engineer since FMECA and hazard analyses are closely related.

3.2.1.1.4 Maintainability: Maintainability engineering works with design to ensure the product can be maintained and operated by the end-user in the most efficient, safe, and cost-effective manner. This function entails analysis of removal, replacement, teardown and build-up of the product, including the time to perform maintenance tasks, the necessary skills required and coordination with integrated logistic support (ILS) on the required support equipment and technical documentation. Maintainability uses the FMECA to identify potential maintenance tasks, for which detailed task analyses are needed. FMECA failure rates (including false alarm rates) are used to estimate personnel requirements in terms of maintenance manhours per operating hour. FMECA also provides maintainability with a list of potential preventive maintenance tasks derived from the compensating provisions and the estimated frequency of required repair tasks. FMECA can also highlight potential maintenance induced failure modes and causes. A close working relationship should exist between the maintainability engineer, human factors engineer, reliability engineer, and the ILS engineer in development of the FMECA.

3.2.1.1.5 Integrated Logistics Support (ILS): ILS has responsibility for ensuring that the product can be supported in the most effective manner by the end-user. This includes spare parts provisioning, support equipment, technical publications, facilities, maintenance personnel, training, and PHS&T (packaging, handling, storage and transportation). ILS also has management responsibility for logistic support analysis (LSA), the logistic support analysis record (LSAR) and associated analyses such as reliability centered maintenance (RCM) and repair level analysis (RLA). FMECA data are input to the logistics data base (LSAR for military programs) to identify the need for maintenance tasks and other logistics requirements, such as spares, support equipment, and publications.

3.2.1.1.5 (Continued):

The scope of FMECA failure modes required by logistics includes failure modes induced as a result of the manner in which the product is operated or maintained. Close cooperation between reliability engineering and logistics is needed to develop induced failure modes, causes and rates.

3.2.1.1.6 Quality Assurance (QA): QA participates in defining a system's "critical item" list specifying those items requiring special considerations during procurement, fabrication, assembly, or test. FMECA provides QA with a list of potential critical parts which require these special quality considerations. QA subsequently implements the required procedures.

3.2.1.1.7 Manufacturing: Manufacturing engineering also participates in defining the critical item list considering items which have special producibility concerns. FMECA provides manufacturing engineering with failure modes and effects which will be used to refine the manufacturing process to prevent manufacturing defects or recommend design changes to reduce potential failure modes.

3.2.1.1.8 Systems: Systems engineering uses the FMECA as a "window" on the design to facilitate trade studies involving the various disciplines which contribute to product development. In the early design phases, failure modes identified in the functional FMECA may require system level design changes to control or mitigate their effects. Changes in technology, such as utilizing computer control instead of analog, electronic or hydraulic control systems, may eliminate or reduce the system effects of some component failure modes and they may introduce new failure modes. When systems built using "old technology" are upgraded the potential failure modes and their effects identified in the FMECA are key inputs for ensuring compatibility between the old system and its replacement.

3.2.1.1.9 Testability: FMECA provides testability engineers with information on expected failure modes and causes, against which to match fault detection and isolation features. In a CE environment, testability engineering, in consultation with design, uses the FMECA to ensure that the detectability of all failures has been considered, that appropriate tests are developed and that built-in test (BIT) will detect and isolate all important failure modes. The FMECA may also be used to develop both built-in and off-line diagnostic routines.

3.2.1.1.10 Testing: The failure modes identified in the FMECA may be used to develop test sequences to simulate component failures during testing to verify that the system responds correctly. A functional FMECA may also be used to develop appropriate tests for a module or product. Test results are input to the FMECA to verify design considerations and address new failure modes precipitated by testing.

3.2.1.1.11 Internal Regulatory Agency Representative: A company's internal regulatory agency representative (such as the FAA designated engineering representative) ensures that all regulatory requirements are met. FMECA provides the internal regulatory agency representative with critical component lists and assurance that potential reliability problems and safety risks are addressed in the design consistent with the regulatory agency's requirements.

3.2.1.2 Customers/ Contract Users:

3.2.1.2.1 Prime Contractors: The prime contractor is responsible to the ultimate end-item user (such as a government agency or an airframe company) for assuring that all the subsystems, and the interfaces between subsystems, have been thoroughly analyzed for their potential failure modes, causes and the effects on the prime's system design. The prime contractor assembles all the subsystem FMECAs and analyzes the "system" effects caused by failure of the subsystem. The prime also generates any interface FMECAs needed to cover all potential failure modes of the system.

3.2.1.2.2 Government Agencies: Government agencies (such as the FAA, CAA, JAA, USAF, USN, US Army and NASA) are responsible for assuring that the users receive a system which is cost-effective, reliable, safe, and easy to maintain and use. FMECA is one of the analyses specified by government agencies for their readiness reviews and certification procedures to document that the designer has considered historical failure modes and causes and designed the product to minimize the effects of these failure modes. FMECA data are also required in the LSAR, to indicate maintenance tasks which must be performed and substantiates the need for support equipment and other logistic support elements.

Government agencies usually require access to the FMECA data base either via paper on older products or electronically on newer products.

3.2.2 FMECA Requirements: FMECA data are generally required by contract in the aerospace, defense, and nuclear power industries. It is also developed in different format and under other titles in the construction, automotive, medical technology, and consumer product industries. The level of detail, format and schedule are specified by the customer in the data item description or contract wording. These aspects are discussed in the following sections.

3.2.2.1 FMECA Type: The type of FMECA performed depends on the type of equipment for which the FMECA is being performed, the level of detail available for the equipment and the phase of the equipment's life cycle at which the FMECA is required. It can range from "functional" in the case of a control system logic where functions are initially the only things defined, to detailed "piece part", in the case where the hardware design is defined. It can also range from the system indenture level when

3.2.2.1 (Continued):

considering failures of the top level item, down to piece parts when that level of indenture is specified. A system level FMECA usually consists of a collection of subsystem FMECAs. A subsystem FMECA is usually bounded at the interface with other subsystems. The system integrator is responsible for any required coordination between the system and subsystem designers.

3.2.2.2 FMECA Indenture Level: The level of analysis (or the indenture level) applies to the level of indenture at which failures are postulated. The FMECA can be accomplished at various levels of indenture from system to piece part level depending upon the information available and the needs of the program, and customer requirements. The lower the indenture level the higher the level of detail since more failure modes will be considered. In general the FMECA needs to be performed only to the level necessary to identify opportunities for design improvement. For example, product features involving new technologies or critical functions would likely benefit from more in-depth analysis.

3.2.2.3 Schedule (Timing and Dates): The FMECA should commence as a functional or interface analysis, as soon as conceptual designs are available, to provide timely feedback to designers. The time-phasing of the FMECA effort is important and should be identified to assure that analysis results will be available to support the project decision points during system development. Refinements should be made as the design matures to reflect observed results of development testing and field service.

3.2.2.4 FMECA Methodology: Variations in design complexity and available data generally dictate the FMECA analysis approach to be used. There are two primary approaches. The first is the functional approach which recognizes that every item is designed to perform a number of functions that can be classified as outputs. These functions are listed and their failure modes analyzed. The other is the hardware approach which lists individual hardware items and analyzes their possible failure modes. For complex systems a combination of the two approaches may be used.

3.2.2.4.1 Functional Approach: The functional approach is typically used for subsystems or components, such as control system components, where functionality is more readily understood than the specific hardware, especially early in the design cycle. The functional approach is often referred to as the "black box" approach where segments of hardware are modeled functionally to allow early resolution of system output issues.

3.2.2.4.2 Hardware Approach: The hardware approach is normally used when hardware items can be uniquely identified from schematics, drawings, and other engineering and design data. It is utilized when detail is required at the piece-part or "bottom-up" level. The hardware approach is commonly used for design engineering's input to the FMECA.

3.2.2.5 Procedure: Each failure mode should be treated independently as its effects are analyzed. When redundant or back-up systems exist, the analysis should be broadened to include the failure conditions which result in the perceived need for such items and how the failure condition will be detected when the redundant or back-up system is employed. Possible design changes or special control measures should be considered and defined for all important failure modes. All single point failure modes identified during the analysis will be uniquely identified to maintain their design visibility.

3.2.2.6 Documentation: FMECA documentation requirements are generally specified by the customer and take the form of a FMECA worksheet. Typical FMECA worksheet formats and the required analysis data are shown in MIL-STD-1629A (reproduced in this report as Figures 1 through 3). Customers may tailor these worksheets as necessary to accommodate their own requirements. As a minimum the FMECA worksheets should contain the following information:

a. Identification number
b. Nomenclature
c. Function
d. Functional failure
e. Failure mode and causes
f. Failure effects (local, next higher level, top)
g. Criticality severity class
h. Failure detection method
i. Design compensating provisions
j. Failure rate (or MTBF) by failure mode

Header information should also be provided which gives a brief description of the item.

3.2.3 FMECA in the Current Design Process: The major FMECA purpose is assessing reliability and maintainability features of the product design and influencing design improvements. The FMECA influences design for reliability and safety by identifying failure modes that require elimination or mitigation because of their system effects. It also influences design by determining whether designed-in redundancy or standby capabilities are needed and if they can be successfully utilized. The FMECA influences design for maintainability by determining whether any designed-in fault detection and isolation capability satisfies the maintenance concept and requirements.

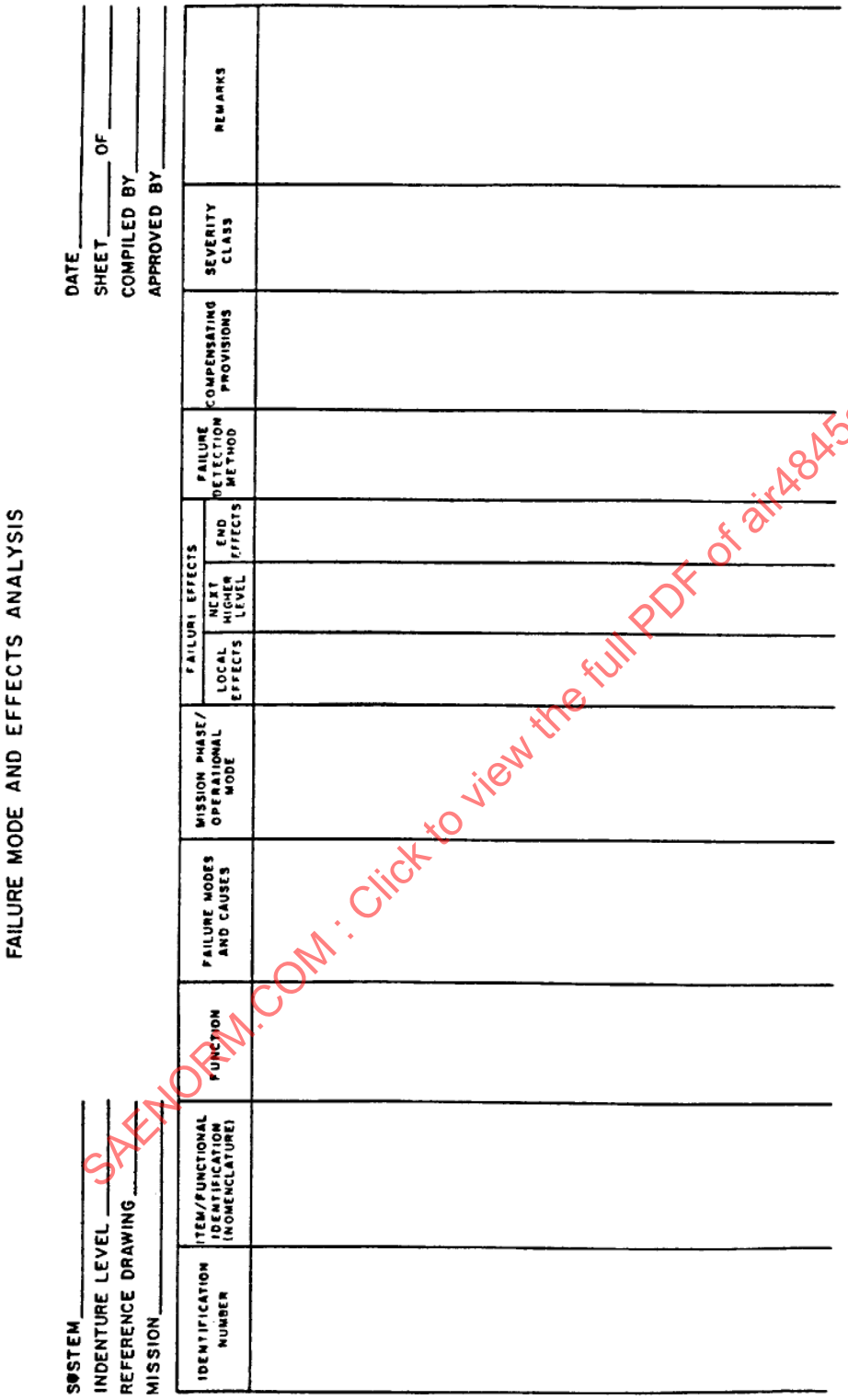

FIGURE 1 - Example of FMEA Worksheet Format (Task 101)

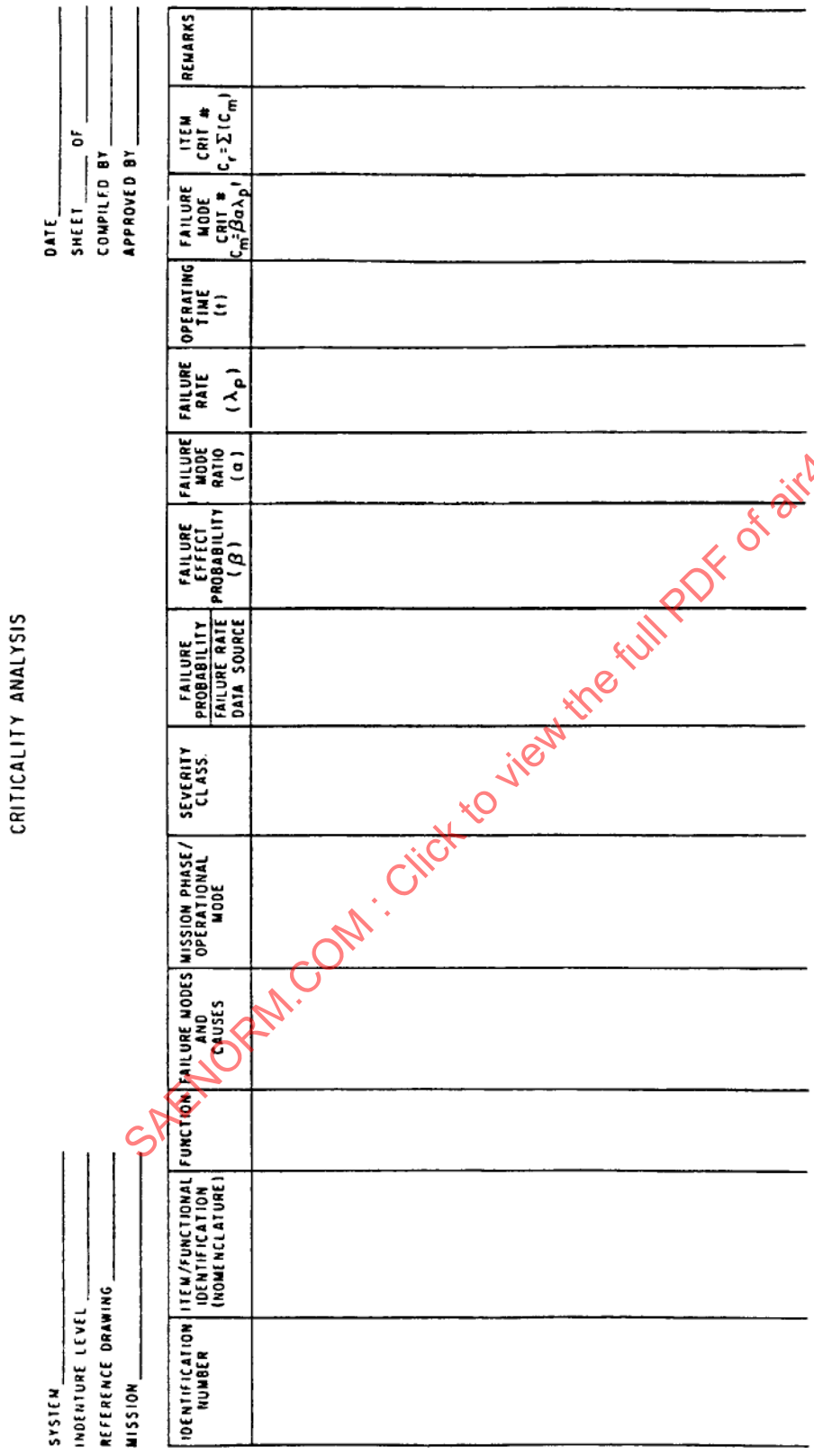

FIGURE 2 - Example of CA Worksheet Format (Task 102)

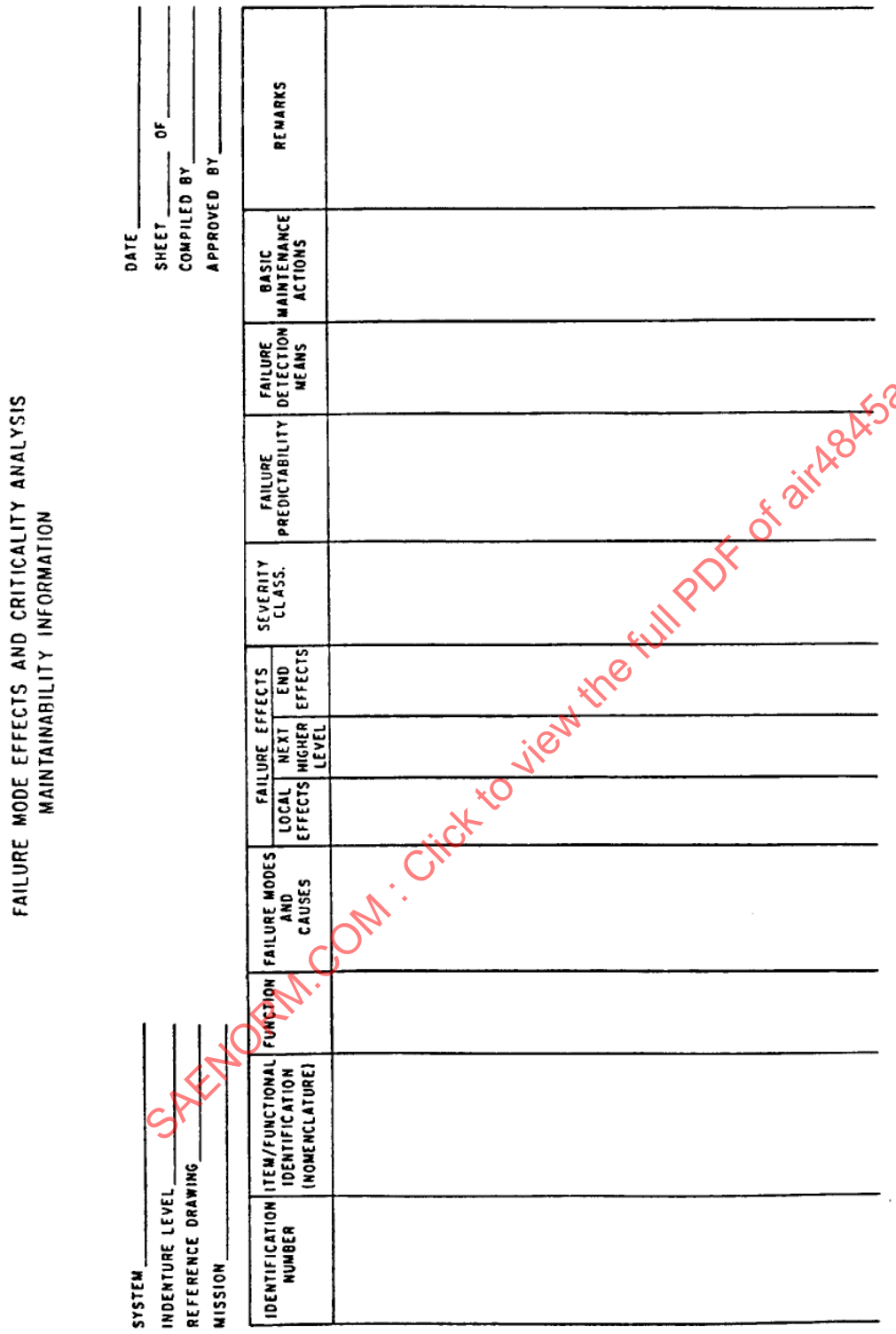

FIGURE 3 - Example of FMECA - Maintainability Information Worksheet Format (Task 103)

3.2.3 (Continued):

The other major FMECA purpose is providing the base data essential to developing the diagnostic steps necessary for isolating a detected failure to the element requiring maintenance. For example, the group of different failure modes that are manifested in the same manner, and their probability of occurrence, forms the basis for selecting the sequence of diagnostic steps which isolate the specific failure mode and the repairable element that caused the failure indication. To achieve this purpose the detailed FMECA of the production design configuration is used.

To influence the design requires that the FMECA be both timely and appropriate to the design phase and the depth of the design definition at that phase. At the outset of the design process, when the system concept is evolving, a functional FMECA is conducted. As the detailed design is developed the detailed hardware FMECA is conducted including the interfaces between hardware. At each phase, the FMECA is performed concurrent with the design so that the FMECA findings can be incorporated into the hardware design and not have to be added later.

3.2.3.1 Design Description: In the early phases of a program, there are often frequent and considerable changes in the design of systems and components. Each design iteration can affect complex three-dimensional characteristics in conceptual arrangements where the relationships between subsystems and components are not always evident. Drawings should be made available to the FMECA analyst as soon as possible to identify additional design concerns and to firm that previously areas of concern were properly addressed in the design.

Therefore, there is a need for the FMECA analyst to develop alternative means of representing the design in terms that can be easily understood and in a form that can be rapidly prepared. These simplified design representations are also required in the final FMECA report, where they become an essential part of the documentation required by the reader to understand the results of the analysis. This documentation is described in the following sections.

3.2.3.1.1 Functional Block Diagrams: Functional block diagrams are one method of representing the design of systems and components in a form that can be easily analyzed. They show functional interactions, inputs and outputs of each represented system/component. Functional block diagrams are used to develop the functional FMECA (see 3.2.3.2.1). Similarly, hardware block diagrams are used to represent the level of hardware break down in a hardware FMECA (see 3.2.3.2.2).

The functional analysis starts with a functional block diagram and may be accomplished by looking at the highest level and determining the potentially critical failures of each functional block. Each of these function blocks can be further broken down into lower level functional block diagrams with each of the lower level blocks analyzed to determine which of the failures associated with the next higher functions could occur in each of the lower levels. This process can be

3.2.3.1.1 (Continued):

repeated at progressively lower levels until the appropriate level is reached. The following examples of functional block diagrams are taken from ARP926. A hydraulic power generation system is used to illustrate this process of progressively moving to the next lower level as the analysis proceeds. Figure 4 (ARP926 Figure 2) is a schematic of this system.

Figure 5 (ARP926 Figure 3) shows a functional block diagram at the system level where all input functions and output functions are listed.

Figure 6 (ARP926 Figure 4) shows a functional block diagram at a subsystem level. In this example, the "return fluid flow" input function is broken down into subfunctions required to accomplish the higher level function.

Figure 7 (ARP926 Figure 5) shows the subsystem functions in terms of hardware required to fulfill each of the lower level functions.

At the lowest level the block diagrams are often numbered to cross-reference the FMECA item numbers, i.e., to each item number corresponds a block diagram with one block identified to the same number and representing the same item.

3.2.3.1.2 Schematics: Schematics are another means of representing a design in a simplified form. Schematics are usually made as line diagrams representing the arrangement and relationships between constituents of a system. Typical applications of schematics are the simplified representation of electrical/ electronic circuits, of hydraulic/ pneumatic systems, and of complex mechanical systems.

Figure 4 (ARP926 Figure 2), described in 3.2.3.1.1, is a schematic for a hydraulic power generation system.

3.2.3.1.3 Drawings: Drawings are typically the most complete and comprehensive representation of a design. Their disadvantage is that they are available relatively late in the design definition process and they carry a lot of information required by the design community but not useful to the FMECA analyst.

The types of drawings normally used in the FMECA process are:

a. Cross-sections
b. Layouts
c. Detail drawings
d. Assembly drawings
e. Interface drawings

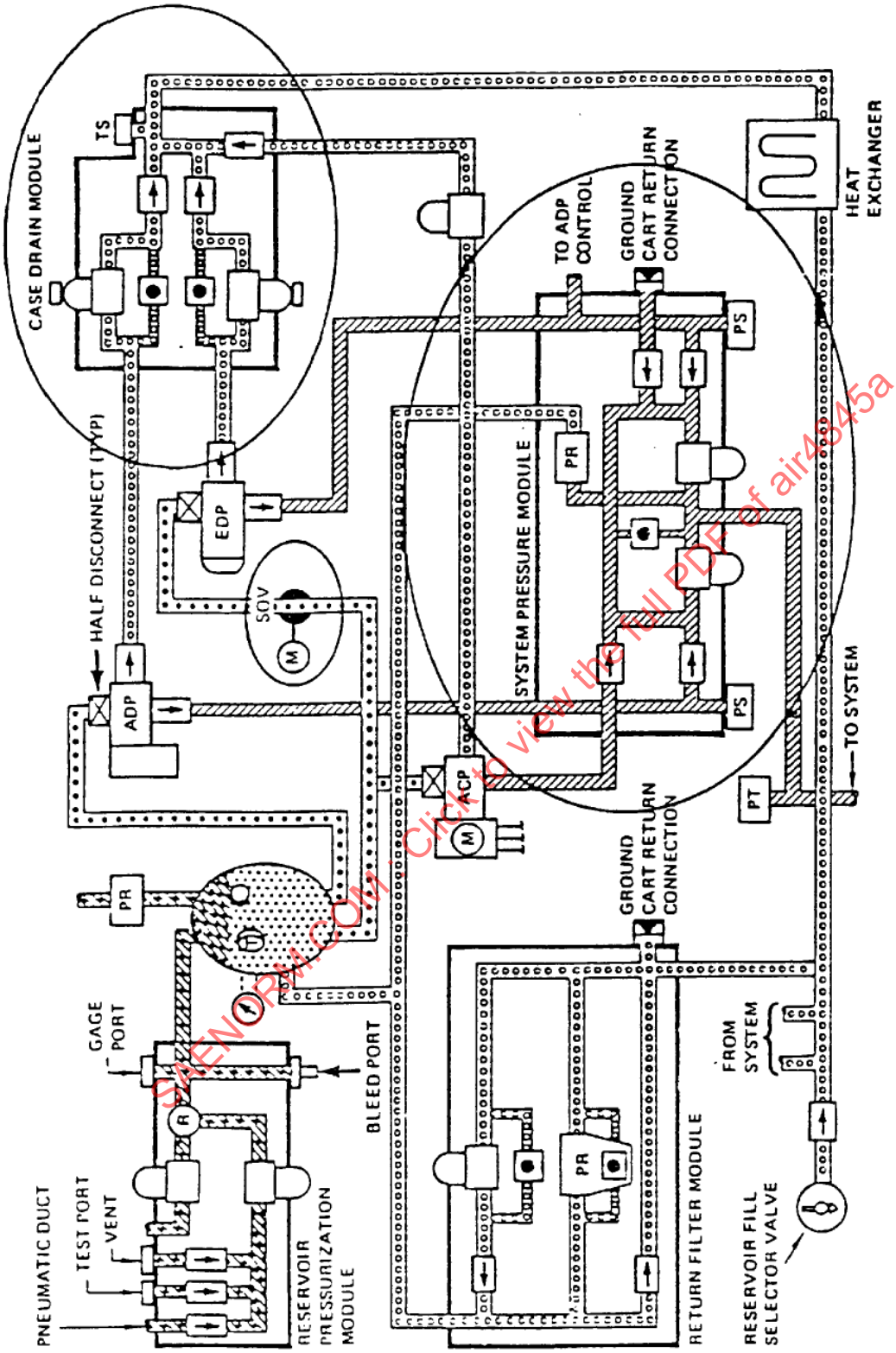

FIGURE 4 - Schematic Diagram of Hydraulic Power Generation System (ARP 926A, Figure 2)

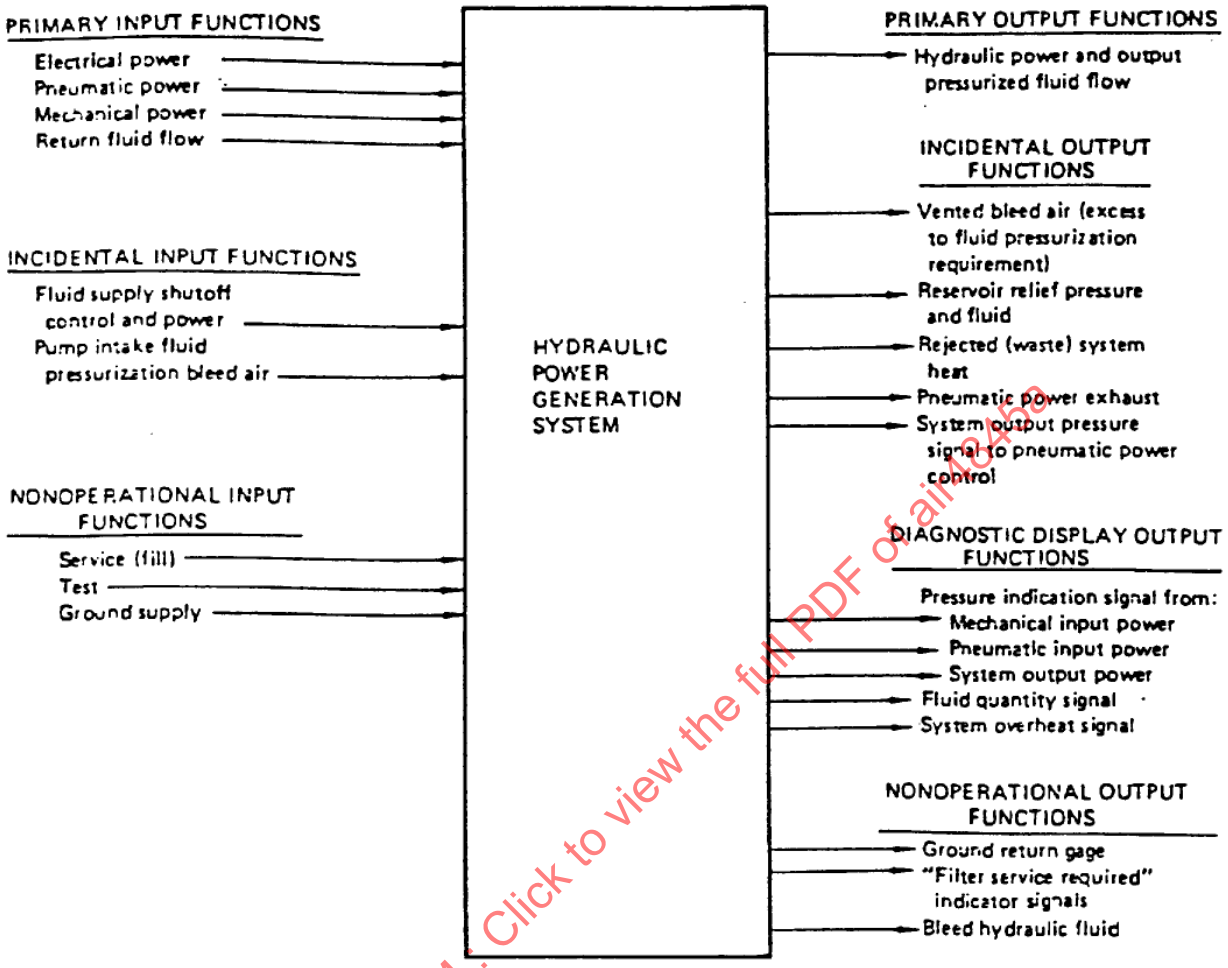

FIGURE 5 - System Functional Block Diagram (ARP926A, Figure 3)

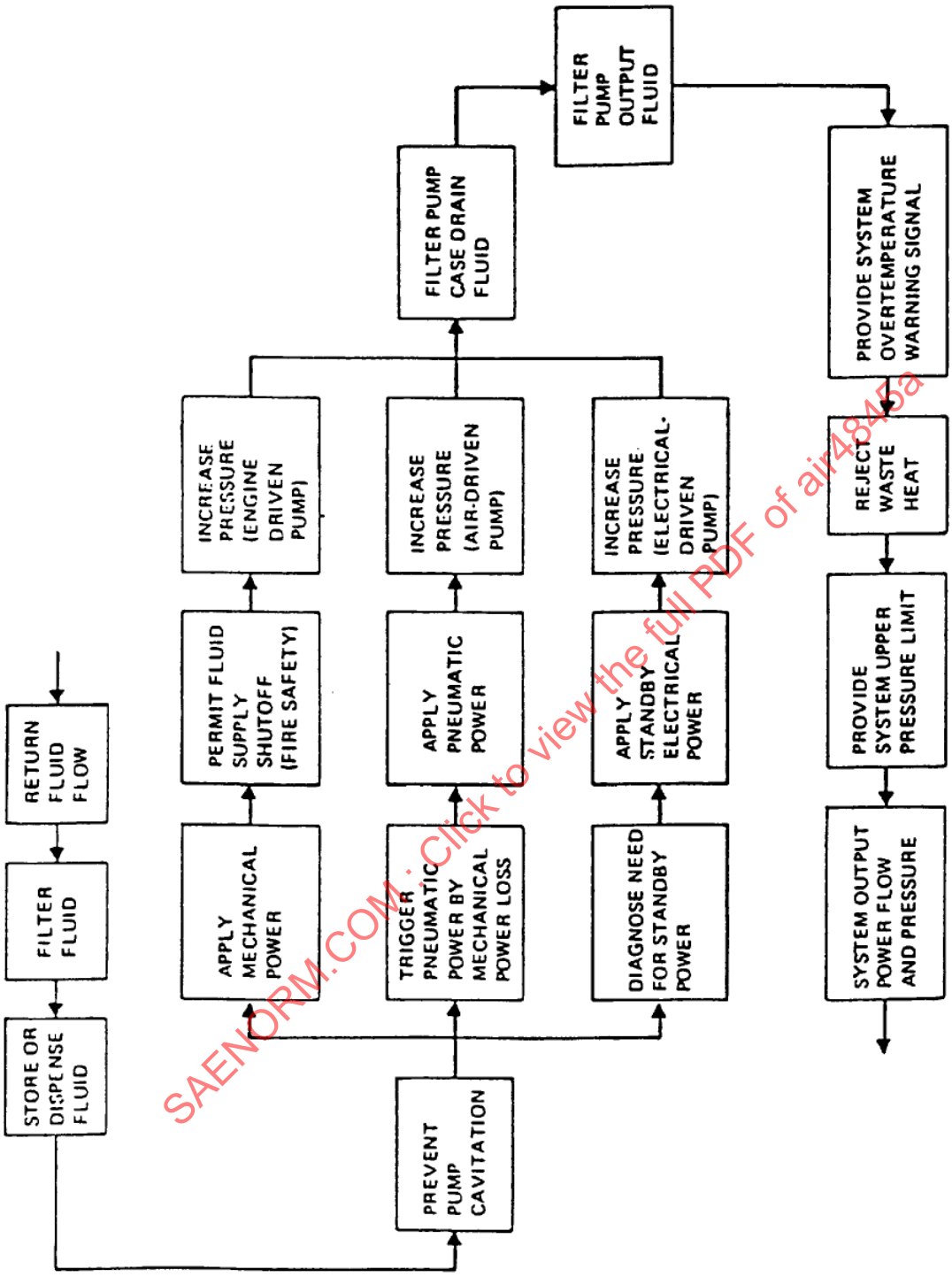

FIGURE 6 - Subsystem Functional Block Diagram (ARP926A, Figure 4)

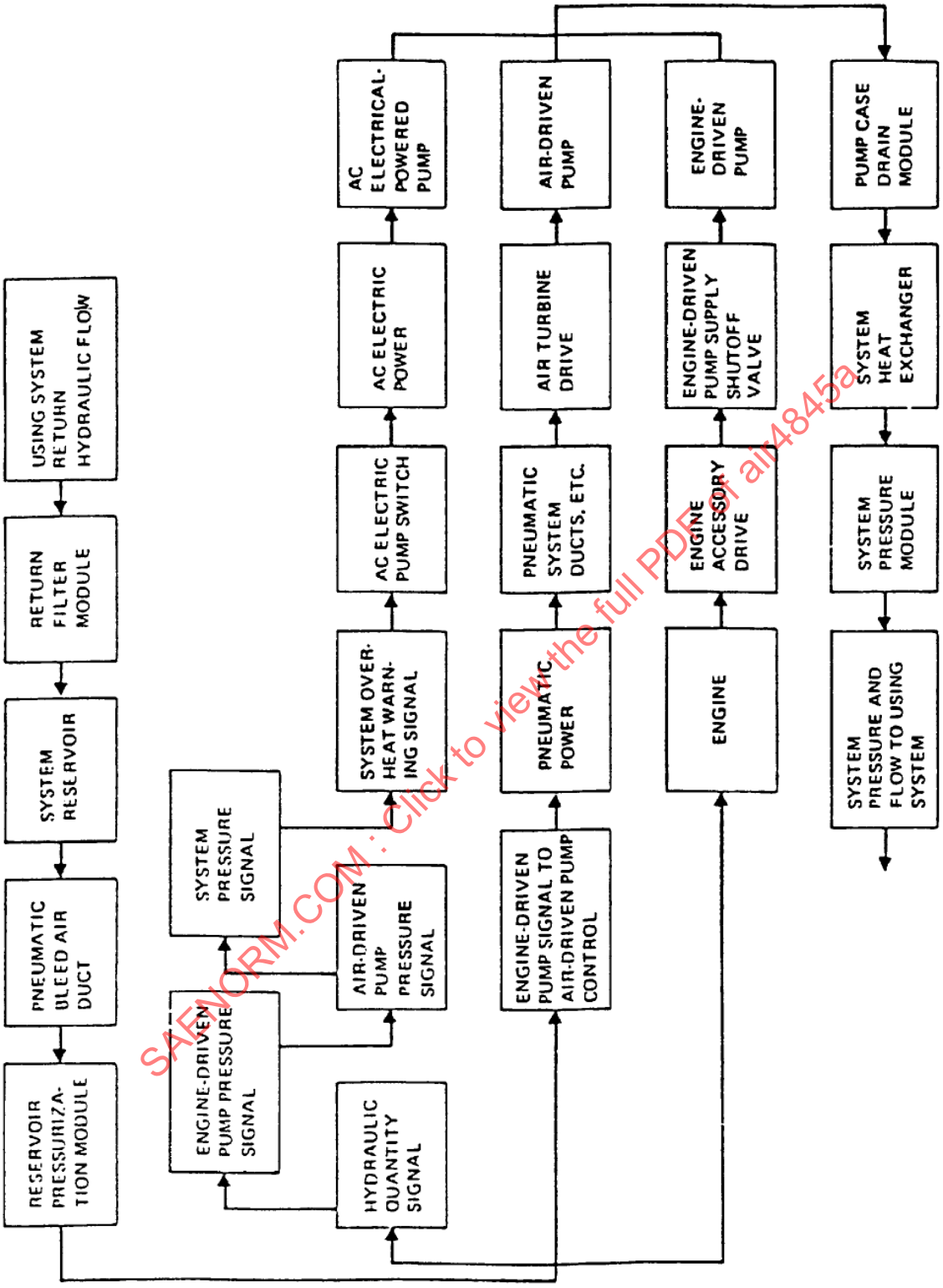

FIGURE 7 - Subsystem Hardware Functional Block Diagram (ARP 926A, Figure 5)

3.2.3.1.3 (Continued):

A thorough FMECA analysis requires the utilization of the three different forms of design representation described. The functional block diagrams and schematics allow a good and rapid understanding of the design intent and they may identify areas of concerns and deficiencies. The drawings represent the execution of the design intent and they may reveal deficiencies that were not visible on diagrams and schematics. Drawings can also be used to confirm that areas of concern revealed by schematics and diagrams have been properly addressed.

3.2.3.2 Major Types of FMECA: Appendix A contains examples of the hardware and functional FMECAs described in this section. The FMECA examples are generic, for reference only and should not be construed as representing any specific product or component.

3.2.3.2.1 Functional FMECA: A functional FMECA is performed early in the design process (e.g., during the concept development and proposal phases) when only a high level description of the system design has been established. It is aimed at evaluating design options and influencing the direction the final design will take. The type of design documentation needed to perform a functional FMECA includes: functional block diagram; reliability block diagram; mission phase definition; mission/system time profile; environmental profile; high level definition of the system's health monitoring subsystem; and functional failure modes and failure mechanisms. It defines failure modes and system effects, failure modes that must be eliminated or mitigated, undetected failure modes, fault detection and isolation tests or diagnostics required. The functional FMECA provides input to the testability, safety, maintainability and LSA groups and should be completed prior to the system preliminary design review.

3.2.3.2.2 Hardware FMECA: The hardware FMECA starts at the piece part level and continues through higher levels of design (component, subsystem, system). It is done iteratively and incrementally as the design evolves and helps to improve the detailed hardware design. The design documentation needed for a hardware FMECA includes: schematics; parts lists; and detailed parts drawings. The outputs include a matrix of all failure modes producing the same failure indication; the failure effect at all levels up to the system level; a detailed failure rate prediction or probability of occurrence; and the criticality of each failure mode. The hardware FMECA provides input to testability analyses and refines the functional FMECA as the detailed design matures. The detailed FMECA should be completed before the critical design review.

3.2.4 Initiating the FMECA:

3.2.4.1 FMECA Overview: As mentioned earlier, to influence design the FMECA logic must be developed and documented concurrent with the development of the design itself. The FMECA is not an effective design tool if it is only documented after the design is fixed. Each preliminary design concept should have a FMECA completed before further detailed design proceeds. Before a preliminary design idea is approved or progresses an approved FMECA should be attached. This process requires constant updating of the FMECA and thereby provides an audit trail for the decisions that determined the final design all the way from the first concept.

3.2.4.2 FMECA Phases (Type and Depth): The different types of FMECA were addressed in 3.2.3.2. The depth to which FMECAs are completed is a function of the customer's requirements, the contractor's experience, the available funding for the task and the time schedule for completion of the task. The depth of analysis must keep pace with the product design. As more detail of the design is decided the FMECA must be constantly revised.

The FMECA process begins the same day a concept or idea is perceived. At this stage a functional FMECA is started, because in most cases the hardware is still undefined. One of the most common reasons for delaying the FMECA is the desire for "real" data to support the design assumptions. If the designers wait until test or analysis data are available to substantiate the design, there will be long program delays. The assumptions made in the FMECA will be confirmed or rejected as the design progresses and various analyses and tests are completed. FMECA assumptions must be documented and updated or corrected as data become available.

3.2.4.3 Flow Down of FMECA Requirements: It is the responsibility of the prime contractor to flow down FMECA requirements to subcontractors and vendors to ensure completeness and compatibility with program requirements. This direction should provide examples of the depth of analysis required for each stage of development. The goal is to document all design concepts and to require a completed FMECA before the subcontractor or vendor's design is approved.

3.2.4.4 Data to Support a FMECA: Design information needed to support the FMECA includes:

a. Equipment and part drawings, design descriptions and design change history, system schematics, functional block diagrams, and narrative descriptions

b. Relevant military, commercial, company and customer specifications, and design guidelines for the equipment being analyzed

3.2.4.4 (Continued):

c. Reliability data, including historical data on failures, cause and effect analyses of previous failures, part failure rates, field service data, and the effects of environmental factors such as temperature, radiation, moisture, vibration, dust, etc. on the part and equipment reliability

d. Operating specifications and limits, interface specifications, and configuration management data

e. Maintainability data including test equipment and scheduled maintenance intervals.

Failure modes, failure rates/ratios and failure effects can be based on similar in-service systems or hardware. If the design is unique then the FMECA failure data must be developed from conservative assumptions. Early identification of these assumptions may indicate the need for testing to verify them before changes become too costly.

A detailed description of the operating environment is needed to assess the probability of a failure's occurrence. In addition, a detailed mission profile and the mission operating requirements are needed to assess the importance of certain failures at the system level.

Previous substantiated FMECA analyses on similar parts and equipment are useful for organizing the analysis, for ensuring that a complete FMECA has been done and as a source for appropriate failure mode, effects and criticality evaluation.

3.2.4.5 FMECA Level: If the FMECA keeps pace with the design there is no need to specify the level of FMECA detail required at any particular design phase. What can be lost in developing FMECAs concurrent with the design is the relationship to other systems. To prevent loss of this relationship an upper level functional relationship FMECA should be performed from time to time during the design. The failure relationship between systems will become more clear as the design nears completion. This raising of the analysis will also show the failure modes that can be handled as a group if they have similar severity consequences.

3.2.5 FMECA Control/FMECA Control to a Hardware Configuration: Controls of the FMECA process help to ensure that it is an integral part of the design process, is dynamic, and that revisions must be formally documented and linked to design changes.

3.2.5.1 Definition: FMECA control is defined as the methods or procedures that ensure:

a. That the FMECA completely and accurately reflects the design;

b. That design changes are captured by FMECA revision; and

3.2.5.1 (Continued):

c. That FMECA results are distributed to appropriate in-house and external users.

d. That FMECA meets the needs and requirements of the customer and solicits feedback.

3.2.5.2 Controls for FMECA Preparation: Controls during the FMECA preparation stages assure that:

a. The FMECA is performed to the appropriate indenture level and detail.

b. The FMECA is linked to a specific hardware configuration.

c. The FMECA is linked to a specific product application or environment.

Typically, this control is established as part of the initial FMECA task definition. The task definition should be formally documented and specify:

a. Whether the FMECA should be done to the system, subsystem, or piece part level.

b. The parts list or bill of material of the product configuration to be analyzed.

c. The product application and environment, including such details as:

(1) Preventive maintenance and inspection intervals
(2) Available failure detection means (such as aircraft cockpit displays)
(3) Environment variables such as pressures, temperatures, loads, and operating times and frequencies

Controls also provide a structured FMECA filing system so that in-process and completed FMECAs can be conveniently accessed by using groups. A centralized computer data base, if available, facilitates convenient access. Completed FMECA reports should be formally published, serialized and filed in the company or department library.

3.2.5.3 Controls During Revision Cycle: As product design changes are proposed or evaluated, the FMECA should be used to assess their impact on reliability and safety. Controls provide the structure to ensure that:

a. All design changes trigger a FMECA effort

b. FMECAs become an integral part of evaluating the design change

c. FMECA revisions are formally documented, and linked to the corresponding design change documents

3.2.5.3 (Continued):

FMECA revisions may also be needed to reflect testing or field service experience, or to incorporate review comments from interfacing disciplines. Controls provide a history of these FMECA revisions, and the background and rationale for each.

3.2.5.4 Controls for FMECA Distribution: As the FMECA results are distributed to the using organizations, controls are needed to:

a. Tailor the report format to the needs of each user

b. Allow users to provide feedback

c. Ensure appropriate reviews and approvals precede external distribution

3.2.5.5 Implementation of FMECA Controls: FMECA controls should be defined and enforced via formal company or department procedures. These published procedures should completely define the "who, how, and when" of each step in the FMECA process.

3.2.6 Generation of the FMECA Report: In the past for many companies, the FMECA report was generated and published without benefit of computer technology. Reliability analysts complete preprinted FMECA forms by hand, and a final typed copy was prepared by clerical personnel. It is now common to utilize PCs and spreadsheet or word processing software for FMECA reports, to provide efficiencies for corrections and updates. A few companies have implemented a more complete computerized data base system, that provides additional flexibility in customizing FMECA report formats for special purposes and specific using groups. The most successful of these systems have been developed "in-house" for use on a mainframe computer, allowing multiple user access for both reporting and data input.

Just as there are several using groups for the FMECA data, there are several common FMECA report formats. The "standard" report formats defined in MIL-STD 1629 (Figures 1 through 3) have often been used as "thought starters" to assist in designing a report that meets the specific needs of a given program or using group. For example, a report for the maintenance planning group would likely focus on the FAILURE DETECTION and FAILURE RATE portions of the analysis. A report for the safety group would focus on the FAILURE EFFECTS and CRITICALITY portions of the analysis.

3.2.7 Current Difficulties (With Generating FMECAs): In most cases, generating the FMECA report is the most tedious FMECA activity. The reporting step is often the first opportunity to integrate inputs from the various disciplines, and review the analysis for gaps and inconsistencies.

Some of the difficulties often encountered in generating FMECA reports are:

a. The baseline data have not been updated to reflect the most recent product design or configuration

3.2.7 (Continued):

b. FMECA data supplied from subcontractors or vendors do not use the established format, ground rules, definitions, etc.

c. The needs of one or more using groups (e.g., LSAR) were overlooked in the initial FMECA planning and the data needed are incomplete or missing

d. Funding has not been provided or budgeted for producing the needed report updates, as test experience and technical analyses become available

e. The burden of "meeting schedule" falls inordinately on the reporting task, since the recognized customer due date is for a report. It often falls to the reporting task to compensate for delays in the data collecting and analysis steps.

Many of these difficulties can be alleviated by fully implementing an automated FMECA process within a concurrent engineering environment. Even issues not directly addressed by automation, such as budget and schedule, can benefit from the discipline that a concurrent engineering environment would provide.

FMECA also brings many benefits to the concurrent engineering environment. These are discussed in 3.3.

3.3 FMECA in the Concurrent Engineering Environment:

Numerous papers have been written and seminars held which describe the benefits of concurrent engineering (CE). Many commercial and aerospace applications have convincingly demonstrated these benefits. Aerospace is implementing CE under the name of integrated product development (IPD). Recognizing the importance and potential benefits of the IPD concept, Dr. Robert Costello, while DOD Undersecretary of Defense for Acquisition, required the services to begin implementation of IPD (Reference 2.3.1). The Air Force found that through the use of IPD it is possible to increase the quality, reduce the cost, and decrease the time it takes to get a new system into the hands of the user.

CE brings representatives from different functions together at the beginning of product development to simultaneously refine the definition of the total product including its manufacturing, training and support capabilities. Figure 8 depicts the Air Force Systems Command (AFSC) functional architecture for this process (Reference 2.3.2).

It should be noted that this process architecture is supported by computer technologies which utilize digital data, common data bases, 3D-solid modeling, etc., to improve the quality of product definition, manufacturing, training and support.

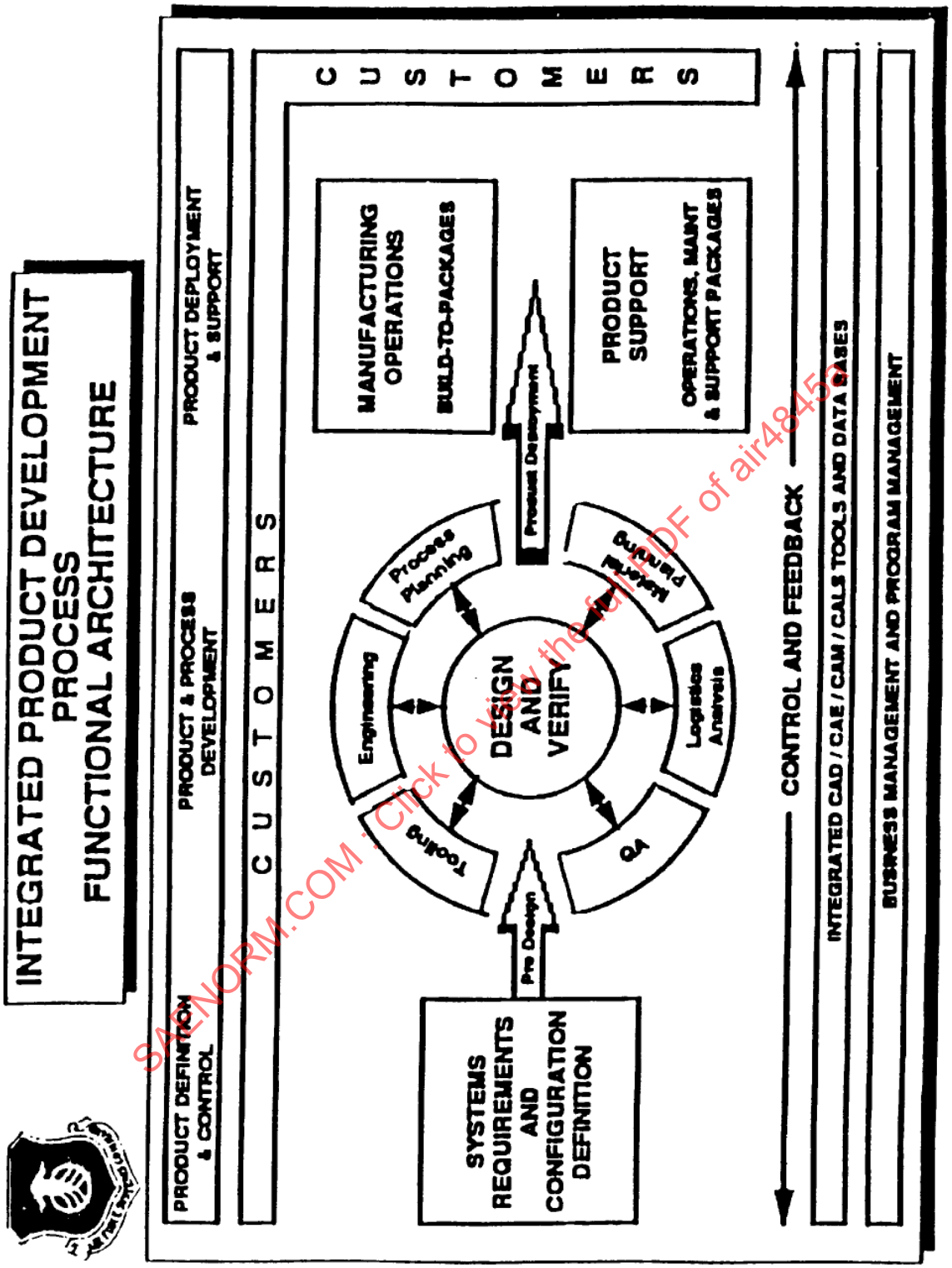

FIGURE 8 - Integrated Product Development Process Functional Architecture

3.3 (Continued):

The systems engineering process controls the development of the total product. The key products out of the early systems engineering effort are integrated requirements documented in specifications, interface control documents, plans, schedules and budgets. The products establish the constraints on the integrated product teams (IPTs) who continue to use the process to accomplish the development activities.

IPTs are the core of the CE process and have the responsibility for all aspects including product cost, schedules, reliability, safety, maintainability, performance, integration with interfacing products, testing, quality, supportability and training. IPTs include representatives from all disciplines associated with the product. Figure 9 depicts a typical aircraft weapon system organization, IPT representatives, and interfaces with other teams. It is within these IPTs that the FMECA work is accomplished.

As the design process transitions into a CE Environment, the FMECA process has the potential for becoming one of the unifying elements for the CE design team. This potential lies in its ability to systematically and methodically combine failure mode input from different disciplines/viewpoints and permit team exploration of the consequences. The FMECA becomes part of a centralized data base, tracking both the results of design trade study decisions and the reasons for the options chosen, given that FMECAs will become a continuing process rather than a one-pass data item, as is the current tendency.

3.3.1 Relevant Aspects of the CE Environment: Current thinking is that future system designs will be more complex, aimed at higher availability, lower operator and maintenance work-loads and lower acquisition and life cycle costs (LCC). These requirements will produce more flexible designs, with redundancy to circumvent benign failures and the capability to correct problems with little or no crew intervention. The CE design environment will attempt to design and develop these systems in the most cost-effective manner.

The most significant factors in the CE environment are the following:

a. Multidiscipline teams working in parallel during the design cycle

b. Enhanced communication and synergy between team members

c. Enhanced consideration and documentation of design alternatives and trade studies

d. Reduced development time and cost for more complex systems through problem avoidance

Working in parallel the CE team members can interject their specific viewpoints and expertise at each stage of the process until the design is finalized. A common data base will facilitate this interaction. FMECA should be part of this data base.

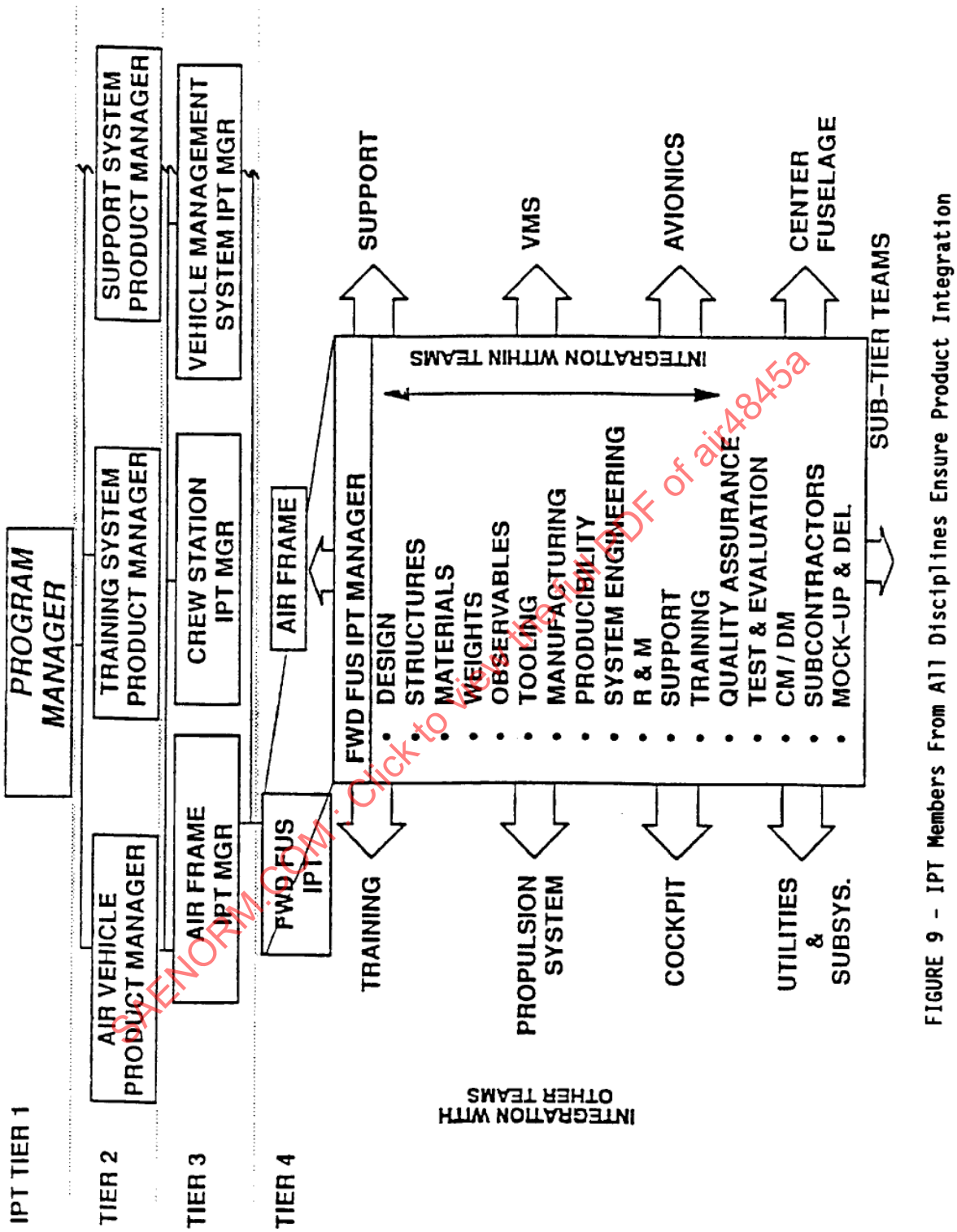

FIGURE 9 - IPT Members From All Disciplines Ensure Product Integration

3.3.1 (Continued):

The volume of information which must be considered necessitates the need for enhanced communication supported by automation to keep the design team focussed on the common goal. Extensive numbers of design iterations will occur and communicating the changing requirements to each team member will be a constant challenge. Because a lot of the design process focuses on elimination of potentially harmful failure modes and mechanisms the FMECA is a vital part of this focus.

Enhanced documentation will be required to keep track of the evaluation of design alternatives. This will provide an audit trail for the design records, with the rationale for selecting the chosen design. FMECA will be an integral part of the documentation process. A bi-product of all the documentation will be a historical data base which will benefit future designers at no extra cost. Input to trade studies can be made/accessed by CE team members, significantly reducing the time taken to generate these analyses and ensuring that they are properly performed. FMECAs will be an integral part of the trade-study procedure by providing data on failure modes and design features of the alternatives.

Overall, the cycle time for development of a product under a CE environment should be significantly reduced and analyses can be accomplished which were previously not done because of time or cost constraints. It should be noted that much of the cycle time and cost reduction results from the avoidance of problems that traditionally surfaced during development and forced costly redesign.

3.3.2 The Role of the FMECA in the CE Environment: Traditionally, the FMECA has functioned as a design coordinating element among the various disciplines inputting to the analysis. The FMECA analyst had to solicit information from the contributing disciplines and resolve data discrepancies or disagreements. The CE environment expands on this coordination. CE provides an input point for design requirements originating from QA, supportability, manufacturing, and other functions not traditionally an integral part of the design process. The FMECA process is an integral part of the overall design process, allowing evaluation of alternatives to a given requirement with failure modes taken into account. The fact that so many disciplines are focussed on the prevention of failures or dealing with the effects of failures, gives the FMECA an important role in the CE process.

3.3.3 Timing: The FMECA process should start at the beginning of the conceptual design phase and will continue through the life of the product. The features of the FMECA allow easy migration from the cursory, simplistic analyses needed to trade off conceptual design sketches to the detailed analyses needed as the design matures through production until retirement. This timing of the FMECA is also important as it contributes to maintaining a proper balance between the need to explore a larger number of design alternatives and the need to reduce the evaluation cycle time for each alternative.

3.3.3 (Continued):

This contribution comes from the fact that the FMECA process is both a unifying factor and a communication device opened to use by more disciplines than has been traditional for this analysis. The FMECA will become a fluid, iterative process rather than a static report.

The reduction in evaluation cycle time will be attainable only by streamlining the processes through automation and modifying the current design processes to ensure that the appropriate functions receive information and provide input to the overall decisions in a timely fashion.

3.3.4 Users of the FMECA Data in a CE Environment: All of today's users will continue to use the process with access to the data base becoming easier. In addition FMECA will be applied to new applications such as manufacturing processes, repair procedures and software design.

Reconciliation between the needs of the different FMECA users (e.g., design, reliability, safety, supportability, etc.) will also be a necessary step in how FMECA is used in the CE environment, with each viewpoint being a valuable input to the design process.

3.3.5 Benefits of FMECA in the CE Environment: There are many obvious benefits to the design community in having a FMECA available within the CE process. Many of these have been discussed earlier in the text and are repeated here in summary form:

a. Multidiscipline trade studies - faster response - more iterations

b. Data communication - easier data availability - input from multiple users

c. Better documentation - historical record and audit trail - variety of reports available from data base

d. Data available to multiusers

e. More timely RMS design influence - shorter response cycle time

f. Improved quality of analyses - clearer focus on critical design areas

g. Improved FMECA results in better product - more robust and balanced design

h. Lower product development and support cost

i. Provides specialty disciplines with broad perspective

j. Consistency and uniformity of analyses

3.4 Automation of FMECA Within CE:

In order for the FMECA to be fully integrated into the overall design process much of the work that is currently done to develop the FMECA "by hand" will need to be automated. In addition to helping to integrate the FMECA into the design process, automation provides benefits that help to improve both the quality of the FMECA and make it a more useful design tool.

One of the most important benefits of automation is that it allows more engineering effort to be concentrated on the analysis of failure effects rather than on the largely clerical tasks of collecting and organizing input data, formating the FMECA report, and copying data (such as lists of failure modes) onto the appropriate forms. Automated FMECA aids can also guide a novice through the steps of the analysis and check its completeness and consistency so that less experience is required to do a thorough analysis. Automation helps to improve the uniformity and consistency of the analysis by encouraging the use of common terminology, a common data base, standardized formats, and standard approaches to doing the analysis.

The prime contractor receives large quantities of FMECA data from subcontractors and can benefit substantially by receiving the data in a consistent, electronically-generated format, which can be assembled into a system-level data base with minimal reformatting.

Automation will facilitate the use of the FMECA in fault tree and system safety analyses and provide a computerized interface with other engineering functions. The documentation for a complete FMECA on a large system, such as an aircraft, is frequently several hundred thousand pages. Electronic storage will reduce the amount of storage space required for the FMECA and facilitate the development of a historical archive of FMECAs by providing easy access to "old" FMECAs.

Automation can provide faster and more timely access to both the data needed to do the analysis and to the FMECA itself as it evolves. In addition, access to the FMECA and permission to make changes to it can be better controlled than with manual methods. Electronic approvals of the FMECA may help reduce the review cycle time.

The following FMECA tasks can be automated:

a. Information gathering
b. Analysis
c. Report generation

3.4.1 Information Gathering: As discussed in 3.2.4.4, a FMECA requires a great deal of data and design documentation that must be collected and available to the analyst while the FMECA is being done. These data are generally produced and maintained by different organizations within a company or, in large projects, by several companies within a contractor tier. In a CE environment the necessary data will be maintained on-line and will be readily accessible to the person or group responsible for doing the FMECA. In addition to giving ready access to the needed information, automation will facilitate screening out unnecessary and irrelevant information. For

3.4.1 (Continued):

example, automation can provide the analyst with a list of potential component or module failure modes that are applicable to a particular component, and sorted by probability of occurrence in a particular environment.

3.4.2 Analyses: Preparation of the FMECA requires many types of analyses to trace the high level effects of a failure, determine the likelihood of various failure modes, and assess the criticality of a given failure mode. These analyses require:

a. Modeling or simulation of the system dynamics in both fully functional and degraded modes of operation to determine both the local and high level failure effects. Such simulations must allow for simulation of the system with all possible failure modes for each component and they must include the effects of component tolerancing on the system behavior.

b. Failure rate predictions from device or system models and extrapolation from historical failure data and documentation.

c. Completeness and consistency checks to ensure that each part or subsystem and all known failure modes have been analyzed and that the local effects of all failures have been propagated through the entire system to determine the system level effects.

d. Identification of failure cascades (chains of failures which result in a major system failure). In addition, any undetected failures or degraded operating modes that could give rise to such failure cascades must be identified.

e. The effect of all system level failures on the equipment mission must be evaluated in order to determine the failure criticality.

3.4.3 Report Generation: The end product of a FMECA is a report documenting the results of the analysis. These reports must be kept up-to-date as the design evolves. They must provide identification of the equipment failure modes and failure effects, assessment of the failure criticality, and design changes or compensating provision recommendations for the equipment. Since many organizations both contribute to and use the results of the FMECA, the reports must be available in a variety of formats and they should be tailored to the needs of each organization.

Some of the capabilities provided by automatic generation of the FMECA report and some of the requirements imposed on the system include:

3.4.3 (Continued):

a. The ability to combine both text and graphics in the report. Pertinent drawings, schematics, X-ray views, cut-away views, and equipment break-down drawings, etc. should be integrated in an appropriate way with the text in the report or as an explanatory note. Automation of report housekeeping chores such as format editing and checking spelling, grammar and terminology will be useful. In addition users of the FMECA report should have the ability to add comments to the report and access referenced supporting materials and analyses.

b. The report should be available in a variety of user specified formats with content tailored to a user's specific needs. It should be possible to generate subreports such as critical item lists; identification of failures that result in a set of system level failures or failure modes; and sorts by failure rate, cause, criticality level, etc. In many applications a report suitable for direct input to an LSAR is highly desirable.

c. Users should have on-line access to the most up-to-date FMECA report and also to earlier versions of the report that provide a history of the analysis. Electronic approval capability should be supported both for in-house approvals and for approvals required by contractual agreements.

3.4.4 Today's Capabilities: In today's environment, FMECAs are typically done "by hand" with the system designer selecting components for analysis, determining the failure modes to be examined, and analyzing how the system will behave when a component fails. Since these types of analyses require that the analyst infer the behavior of the system from a given set of component parameters, rather than determine the set of parameters needed to effect a given type of behavior, they may be more difficult than the original design of the system.

Some automated aids in the form of stand-alone tools and networking to share information are available. These support:

a. System simulation
b. Reliability prediction
c. FMECA forms
d. Networking

3.4.4.1 System Simulation: Simulation enables the design engineer to examine the behavior and operational parameters of a system without having to build a physical prototype. By using a simulation, the effects of a failed component on the system outputs can be examined.

Simulation programs enable an analyst to simulate subsystems and examine the effects of component tolerances on the system behavior. Various types of component failures can be simulated by changing the component parameters to match those of the component in its failed state. System descriptions for these programs can often be loaded directly from the schematic on a CAD/CAE system.

3.4.4.1 (Continued):

General purpose programming and simulation languages have been used to develop behavioral level simulations of a large number of systems. These types of simulations enable the analyst to examine the system performance parameters and study the effects of failures on these parameters. Many companies have developed proprietary and/or special purpose simulation programs for the products they build.

3.4.4.2 Reliability Prediction: Electronic reliability prediction programs, many of which in the past have been based on the failure rate models in MIL-HDBK-217, or the Bellcore Reliability Prediction Procedure (with their known limitations), provide failure rate predictions for most types of electronic components. These programs compute device failure rates using either a "parts count" model or a "stress" model. In the parts count model, a generic, or average, failure rate for each type of part is used. The overall system failure rate is the sum, over all component types, of the generic component failure rate multiplied by the number of components of that type. In the stress model a device's failure rate is computed based on a detailed analysis of the environment in which the device operates, its operating parameters, its quality as determined by tests and inspections during its production. The overall system failure rate is computed as the sum of the failure rates of all components in the system.

Most reliability prediction programs are essentially stand alone programs. The reliability analysis data must be entered manually even though (in some cases) it is run on the same machine as other design aids and product detail from a CAD system is available as input.

Reliability prediction models and data for nonelectrical parts are not as well developed as those for electrical components. However, some reliability prediction programs are available, such as those based on the Rome Laboratory Reliability Analysis Center's "Nonelectronic Part Reliability Data" (Reference 2.3.3). Specific reliability models utilizing techniques like Weibull distributions have been developed for speciality equipment such as bearings, gears, and jet engine parts.

Where detailed failure mode likelihood data are needed, supplier or company data based on field service or experience with similar items may provide more accurate predictions.

3.4.4.3 FMECA Forms: A number of programs have been developed to help with the mechanics of preparing the FMECA documentation. These programs assist in formating and editing the FMECA. Some are little more than spread sheets that keep the typing in a tabular format. Other programs have features that improve the quality of the analysis. Some of these features include:

a. Lists of potential failure modes and effects which help to standardize the descriptions of these events in the FMECA

3.4.4.3 (Continued):

b. Checks to ensure that the sum of all failure mode apportionments is 100%

c. Automatic calculation of the item criticality number or risk priority number (RPN) from the failure probability, severity, and detection probabilities. The criticality index number, defined by MIL-STD-1629, is the sum, over all failure modes, of $\alpha\beta\lambda t$ where α is the failure rate apportionment for the mode, β is the failure effect probability, λ is the part failure rate, and t is the operation time.

Some FMECAs especially in the automobile industry use the RPN defined by Reference 2.2.5 to help assess the criticality of the failure. It is calculated as the product of P x S x D where: P is a ranking of the failure probability; S is a ranking of the severity of the effect of the failure; and D is a ranking of the probability of detecting the failure. Failures with high criticality numbers or RPNs are the most critical.

d. The ability to combine subsystem FMECAs into a single, unified system level FMECA.

3.4.4.4 Networking: Computer networking allows users to share data and information. In today's environment this sharing is usually limited to transferring data files or sending electronic mail from one user or system on the network to another. Users can also remotely access and use other systems on the network.

The ease with which a user can access files on other systems connected to the network varies widely. Local area networks and long distance networks utilizing satellite or fiber optic transmission media generally provide a high bandwidth which allows rapid data transfer. Networks utilizing the telephone network are generally slower. In some cases access to data stored on remote systems is "seamless", meaning that remote files are accessed as easily as files on the local system. In other cases various system or network security mechanisms limit the ease of access.

A major limitation in using a network to obtain the information needed to do a FMECA is that the user must know where the data are stored on the network to be able to access them.

3.4.5 Needed Automation Capabilities: The large amount of data and engineering expertise needed to do a FMECA and the fact that this information is usually scattered throughout an organization make automating the FMECA (or to be more precise, developing automated aids for doing the FMECA) a challenging task. Some of the capabilities that must be developed and applied to the FMECA task are described in the following paragraphs.

3.4.5.1 Networking/Integration: Computer networks facilitate access to the information needed to do a FMECA within an organization. However, access alone is not enough. The network should also be able to help the FMECA analyst locate the needed information through some kind of indexing, library, or archiving facility. Remote access to the FMECA as the design develops must also be provided. Networking with high bandwidth communications is needed to integrate all of the tools and expertise required for the FMECA, especially when graphics are being transmitted.

3.4.5.2 Security: Proper security of the FMECA must be maintained to ensure its integrity and availability only to authorised users. Although this is necessary in a manual environment, security becomes especially important in an automated environment where changes may not be as obvious. Since data contained in the FMECA could be quite sensitive, access must be limited to authorized personnel. Back-up copies of the FMECA should be made at appropriate intervals (often daily). An audit trail of when changes were made and by whom must be maintained. A means of allowing electronic approval of the FMECA should be implemented.

3.4.5.3 Artificial Intelligence: Application of artificial intelligence (AI) technology to the preparation of the FMECA provides the most promise for giving the engineer tools for doing the analysis. AI uses "intelligence" in the form of underlying system models, knowledge about the properties of system components, design guidelines and heuristic "rules of thumb" to aid the analyst.

Some applications of AI technology include:

a. Data base systems
b. Expert system technology
c. Case-based reasoning
d. Distributed AI

3.4.5.3.1 Models and Reasoning Methodologies: When experts solve a problem they frequently use theoretical knowledge about the domain to model different system states. By making changes to the model, such as introducing an item failure, the expert can provide explanations of the induced effect by simulating (perhaps mentally) the behavior of the altered system. All system failure modes can be analyzed in this way if the simulation can be extended to all possible item failures.

The underlying simulation model must relate to the real world system without a significant mapping gap for the simulation to provide meaningful input for a FMECA. For this reason, symbolic reasoning is often preferred over purely numeric system models since it is able to give a human-like interpretation of the simulation. Often, exact simulation values are not significant or available for the analysis. Qualitative thresholds, such as high, low, full, open, short, etc., are usually more relevant than continuous expressions for FMECAs. In addition, qualitative models have several other advantages over numerical simulations, as follows:

3.4.5.3.1 (Continued):

a. Numerical simulations require very specific system descriptions that may not be available early in the design process

b. The computation burden is generally less for a qualitative model because of the comparative simplicity of the model

c. Explanations at an appropriate level for human comprehension are possible because the underlying model more closely matches the structure of the system model

AI systems to aid in performing a FMECA may have to apply several types of system models and associated reasoning methodologies in order to adequately assist the analyst with the analysis. The most important types of models for FMECA studies are:

a. Physical structure and behavior models
b. Functional models
c. Causal models

3.4.5.3.1.1 Physical Structure and Behavior Models: Physical structure and behavior models are best exploited when the system can be described by assembling objects that also specify a behavioral component. The behavior of the overall system is synthesized from individual item behaviors. This has the advantage of allowing an item's structural and behavioral characteristics to be reused in other system descriptions using that item. Hence, a library of item structure/behavior characteristics can be stored for future system synthesis. Also, the system's behavior can be simulated based on item failure modes.

In general, physical structure and behavior models progress from system descriptions, such as schematics, to behavior, to functions. Hence, a system's functionality is derived from its physical structure. It may be inefficient or impossible to model large processes and systems where the system's behavior cannot be readily construed from its constituent components.

3.4.5.3.1.2 Functional Models: Functional models (see Figure 10) emphasize the function of a device rather than the detailed behaviors that make up the function. These models decompose a design into its constituent functions made up of a hierarchy of behavioral pieces rather than physical components. This approach eliminates the extensive detail that results from describing a system as a long sequence of causal states.

The functional modeling approach is most promising for FMECAs when the system complexity requires a top down analysis from some general indenture level proceeding down to the component level. Alternatively, a bottom up approach for preparing a FMECA emphasizes the relationships between components and functions of subassemblies.

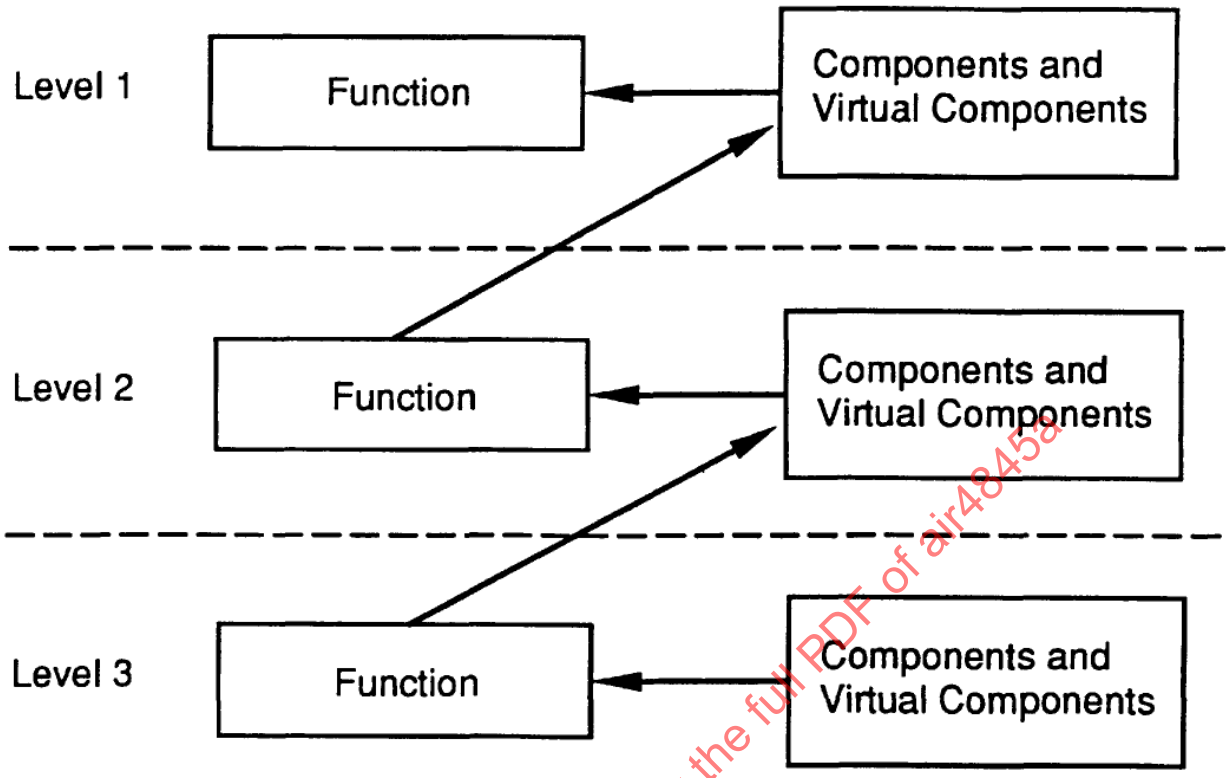

FIGURE 10 - Bottom-Up Functional Model

3.4.5.3.1.2 (Continued):

In this approach, lower levels of function, i.e., subassembly functions, are virtual components of the next higher assembly level.

Functional system models and functional reasoning about item failures are particularly useful when performing a functional FMECA and early in the design process when detailed characterizations of the operation of a system or subsystem are not yet available and a module can only be described in terms of its functions. For example a radio might be described structurally as consisting of a chassis and a headset with the chassis having the subcomponents: repeating coil, power supply, antenna, buzzer, etc. and the headset having the subcomponents: speaker, microphone, etc. A functional description of the same radio might identify the radio's transmit, receive, buzz, and energize functions. The transmit function would then include the subcomponents: repeating coil, microphone, and antenna. The receive function would include the subcomponents: speaker and antenna. The buzz function would include the buzzer, and the energize function would include the power supply. The functional decomposition of the radio reveals more about its operation and facilitates reasoning about how component failures will affect the system. For example, a failure of the repeating coil will disable the transmit operation. Figure 11 illustrates the examples of structural and functional decomposition of a radio system.

3.4.5.3.1.3 Causal Models: Causal system models relate cause and consequence. For example, a "dead battery implies car will not start" is a causal model of the relationship between the battery and the car starting. Using causal models and reasoning, a device such as a resistor might be characterized as follows:

a. In normal operation with input voltage V the output voltage is V-IR where I is the current into the resistor and R is its resistance.

b. When failed short with input voltage V the output voltage is V.

c. When failed open with input voltage V the output voltage is 0.

d. When the input voltage is V and VI is much greater than the rated power of the resistor, the resistor will burn, the output voltage will be 0, and a fire may be ignited.

This type of reasoning is necessary to describe the effects of different types of failures on the components of a system.

3.4.5.3.2 Data Base Systems: A simple data base system can help the FMECA analyst and the FMECA users by giving them the information they need in a form that is ready to be used. For example: