Guidance for
Off-the-Shelf Software Use
in Medical Devices

Draft Guidance - Not for Implementation

This guidance document is being distributed for comment purposes only.

Office of Device Evaluation

Draft released for comment on: 8/17/98

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

Center for Devices and Radiological Health

Preface

Public Comment:

Comments and suggestions regarding this draft document should be submitted by November 16, 1998 to Docket No. 98D-0565, Dockets Management Branch, Division of Management Systems and Policy, Office of Human Resources and Management Services, Food and Drug Administration, 5630 Fishers Lane, Room 1061, (HFA-305), Rockville, MD 20852.

Additional Copies:

World Wide Web/CDRH home page at http://www.fda.gov/cdrh/ode/otssguid.pdf or CDRH Facts on Demand at 1-800-899-0381 or 301-827-0111, specify number 1252 when prompted for the document shelf number.

Table of Contents

I. OVERVIEW 1

A. Introduction and Background 1

B. Purpose / Scope 1

C. Definitions 2

D. OTS Software Decision Schematic 3

Figure 1. OTS Software Decision Schematic 3

II. OTS SOFTWARE USE 4

A. BASIC REQUIREMENTS for OTS Software 4

B. Hazard Analysis and Hazard List 7

Figure 2. Hazard Management Schematic 7

C. Hazard Mitigation 8

Table 1. Injury Reduction Countermeasures 9

D. SPECIAL REQUIREMENTS for OTS Software 10

E. Describe Hazard Level & Justify Safety and Effectiveness 10

III. OTS SOFTWARE IN MARKETING APPLICATIONS 11

A. Examples 11

Corneal Topographer -- Minimal hazard medical device (II-A) 11

Perineometer -- Minimal hazard medical device (II-A) 12

Implantable Medical Device Programmers -- Describe Hazard, Justify Safety and Effectiveness (II-E) 12

B. 510(k) Issues with OTS software 13

Typical OTS Software Changes Requiring a 510(k) 15

Exemption of Laboratory Information Management Systems 15

C. IDE Issues with OTS software 15

Exemption of Diagnostic Devices 16

D. PMA Issues with OTS software 16

Artificial Intelligence 16

E. Product Labeling 17

IV. BIBLIOGRAPHY 17

A. References for this Guidance 17

B. Additional Reading ..... **Error! Bookmark not defined.**

V. APPENDICES 19

A. Operating Systems 19

B. Utilities and Drivers 20

C. Local Area Networks (LANs) 21

D. Device Master Files 22

E. Maintenance and Obsolescence 23

Numbers in square brackets [##] appearing in this guidance refer to citations in the Bibliography (Section IV)

I. Overview

A. Introduction and Background

Off-the-shelf (OTS) software is commonly considered for incorporation into medical devices as the use of general purpose computer hardware becomes more prevalent. The use of OTS software allows device manufacturers to concentrate on the application software needed to run device-specific functions. However, it must be recognized that OTS software intended for general purpose computing may not be appropriate for a given specific use in a medical device. The medical device manufacturer using OTS software generally gives up software life cycle control, but does bear the responsibility for the safe and effective performance of the medical device.

This guidance document was developed to address the many questions asked by medical device manufacturers regarding what they need to provide to the FDA when they use OTS software. The response to these questions depends on the medical device in question and the impact on patient safety when the OTS software fails. Thus, the answer to the question, "What do I need to do or document?" will be based on the hazard analysis that is an integral part of designing a medical device. The detail of documentation to be provided to FDA and the level of life cycle control necessary for the medical device manufacturer increase as the hazard to the patient from software failure increases.

This document lays out in broad terms how the medical device manufacturer should determine what is necessary to do and to document for submission to the agency. A BASIC set of need-to-do items is proposed for all OTS software, and a detailed discussion is provided on additional (SPECIAL) needs and responsibilities of the manufacturer when hazards from OTS software failure become more significant.

B. Purpose / Scope

This guidance document represents the agency's current thinking on use of OTS software in medical devices. It does not create or confer any rights for or on any person and does not operate to bind FDA or the public. An alternative approach may be used if such approach satisfies the requirements of the applicable statute, regulations or both.

The **purpose of this document** is to describe the information that should be provided in a medical device application involving OTS software. While this document is not intended for compliance with Quality System (GMP) requirements, many of the principles outlined herein may be helpful to device manufacturers in establishing design controls and validation plans for use of off-the-shelf software in their devices. Further industry guidance on these subjects will be issued by the Office of Compliance, CDRH. This guidance discusses key elements reviewers should look for in the submission thereby providing a common baseline from which both manufacturers and reviewers can operate. This document provides guidance in support of the Blue Book Memorandum G97-__, *Use of Off-the-Shelf (OTS) Software in Medical Device Applications* [1]. This should improve predictability of agency interaction with sponsors regarding applications involving OTS software.

C. Definitions

Off-the-Shelf Software (OTS software) -- A generally available software component, used by a medical device manufacturer for which the manufacturer can not claim complete software life cycle control.

Following a patient-based approach to hazard analysis, we define:

Hazard -- A possible source of danger or a condition which could result in human injury.

Hazard Mitigation -- Reduction in the severity of the hazard, the likelihood of the occurrence, or both.

Minimal Hazard --Where failure, malfunction, or misuse of the OTS software poses no possibility of serious injury to the patient, then the OTS software is said to present a MINIMAL HAZARD.

Safety -- In the regulation of medical devices, safety means that the probable benefits to health... for its intended use... when accompanied by adequate directions and warnings against unsafe use, outweigh any probable risks. In this guidance we will use the words "safety and effectiveness" to remind ourselves that safety is only meaningful in the context of the benefit-risk considerations and the labeling.

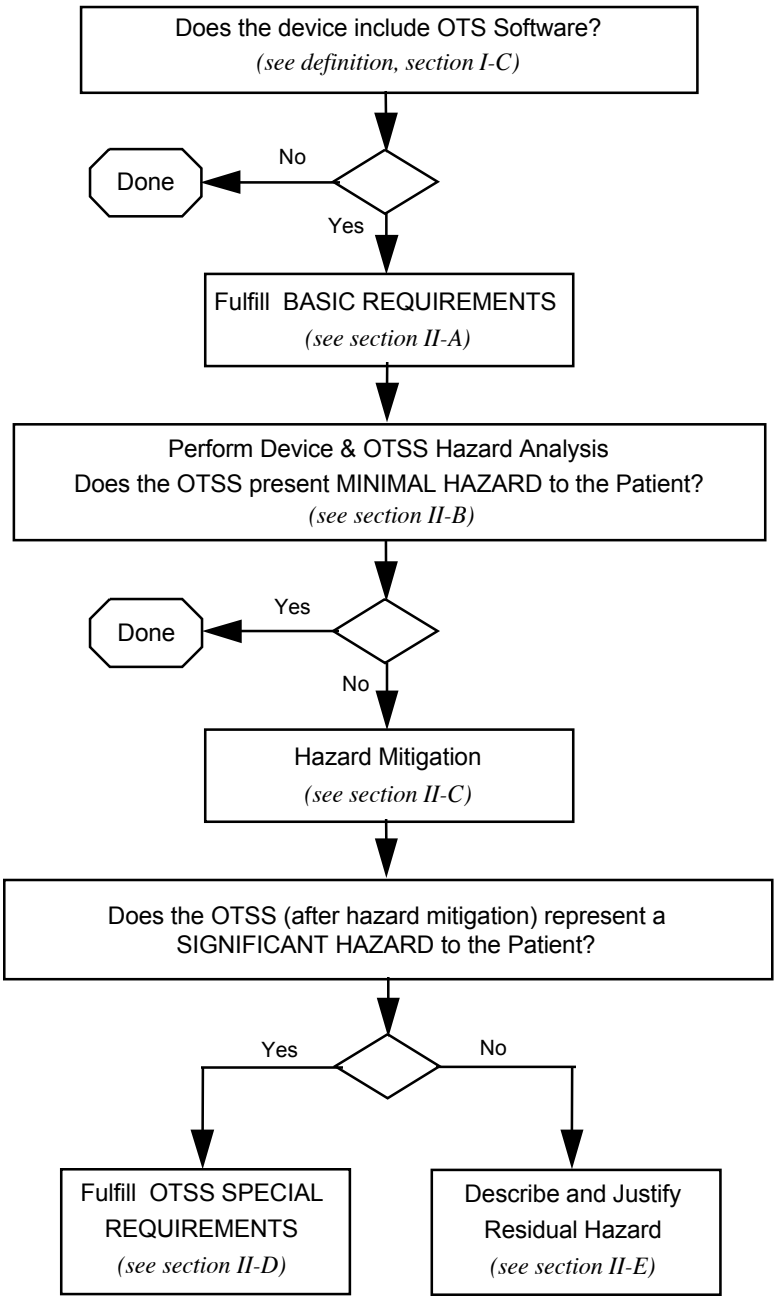
Significant Hazard -- Where failure, malfunction, or misuse of the OTS software is likely to result in death or serious injury to the patient, then the OTS software is said to present a **SIGNIFICANT HAZARD**

Other software terminology used in this document are defined in the *FDA Glossary of Computerized System and Software Development Terminology* [2].

D. OTS Software Decision Schematic

The content of the medical device application supporting use of OTS software (OTSS) in a medical device depends on the results of the hazard analysis. Figure 1 provides a schematic of the decision process and a table of contents for Section II of this guidance document.

Figure 1. OTS Software Decision Schematic



As summarized in Figure 1, BASIC REQUIREMENTS should be fulfilled for any OTS software used in a medical device. If the hazard analysis shows that the OTS software failure presents only a MINIMAL HAZARD to the patient, then only the hazard analysis and BASIC REQUIREMENTS would be expected in the submission.

If the OTS software failure presents more than a MINIMAL HAZARD to the patient, then the sponsor will need to describe the measures taken in hazard mitigation. If, after the measures to mitigate hazards, any SIGNIFICANT HAZARD remains, then the medical device manufacturer should fulfill the SPECIAL REQUIREMENTS for OTS software.

If after the measures taken in hazard mitigation the residual hazard is not significant, then the OTS software falls in the "middle ground". The application should then include the hazard analysis and a benefit risk assessment of the remaining hazard to the patient (see section II-A for examples).

II. OTS Software Use

A. BASIC REQUIREMENTS for OTS Software

The detail used satisfying these BASIC REQUIREMENTS should be appropriate to the hazard of the medical device.

The OTS Software BASIC REQUIREMENTS are intended to answer the following questions:

1. **What is it?** - For each component of OTS software used, specify the following:

   a) Title and Manufacturer of the OTS software;

   b) Version Level, Date, Patch Number and Upgrade Designation as appropriate; and

   c) OTS documentation (user manual) which will be provided to the end user.

   Note: Unless documented by an approved "Software Change Request", the medical device manufacturer should only use the OTS software as specified in the Software Requirements Specification (SRS). This requires verbatim compliance to name, version level, patch additions and tailored configuration.

2. **What are the Computer System requirements for the OTS?** - For the entire system, specify the following:

   a) Hardware requirements: processor, RAM, hard disk, other storage, communications, display, etc.

   b) Software requirements: operating system, drivers, utilities, etc. The SRS listing for each item should contain the name (e.g., Windows 95, Excel, Sun OS, etc.), specific version levels (e.g., 4.1, 5.0, etc.) and a complete list of any patches that have been provided by the OTS software manufacturer.

3. **What Actions must be taken by the End User?** - What aspects of the OTS software and system can (and/or must) be installed/configured?

   a) What steps are permitted (or must be taken) to install and/or configure the product?

   b) What are the acceptable and usual ranges of data which must be provided and the default values should no data be provided.

   c) When will the configuration need to be changed?

4. **What does the OTS software do?** - For the entire system, specify the following:

   a) What is the OTS software intended to do? The sponsor's design documentation should specify exactly which OTS programs, modules, units, routines and/or functions will be included in the design of the medical device. Specific attention should be directed at the error control and messaging interfaces.

   b) What is the interface with other software including software outside the medical device (not reviewed as part of this or another application)? The interface to outside software should be completely defined for each medical device, module, unit, routine and/or function. The design documentation should include a complete description of the interface between the medical device software and any outside software.

5. **What does the OTS software NOT do?** - For the entire system, specify:

   a) What are the expected / design limitations of the OTS software?

   b) Is there a current list of OTS software problems (bugs) and access to updates?

6. **How do you know it works?** - Describe testing, verification and validation of the OTS software and ensure it is proper for the device hazard.

   a) How was the OTS software tested?

   Note: Software test, verification and validation plans must identify the exact OTS software (title and version) that is to be used. When the software is tested it must be integrated and tested using the specific OTS software that will be delivered to the user. This requirement applies at all levels of software testing (module, integration, and system)

   b) What were the results of the testing which verify successful completion of the testing?

   Note: If the manufacturer allows the use of the medical device with different versions of OTS software then the manufacturer is required to validate the medical device for each OTS software version.

7. **How will you keep track of (control) the OTS software?** - An appropriate plan should answer the following questions:

   a) What education and training are suggested or required for the user of the OTS software?

   b) What measures have been designed into the medical device to prevent the introduction of any non-specified OTS software, e.g., word processors, games, etc. Introduction of non-specified OTS software may be prevented by design, i.e., disabling input (floppy disk, CD, tape drives, modems).

   c) What measures have been designed into the medical device to prevent the introduction of incorrect versions? On startup, ideally, the medical device should check to verify that all software is the correct title, version level and configuration. If the correct software is not loaded, the medical device should warn the operator and shut down to a safe state.

   d) How will you maintain the OTS software configuration?

   e) Where and how will you store the OTS software?

   f) How will you ensure proper installation of the OTS software?

   g) How will you ensure proper maintenance and life cycle support for the OTS software?

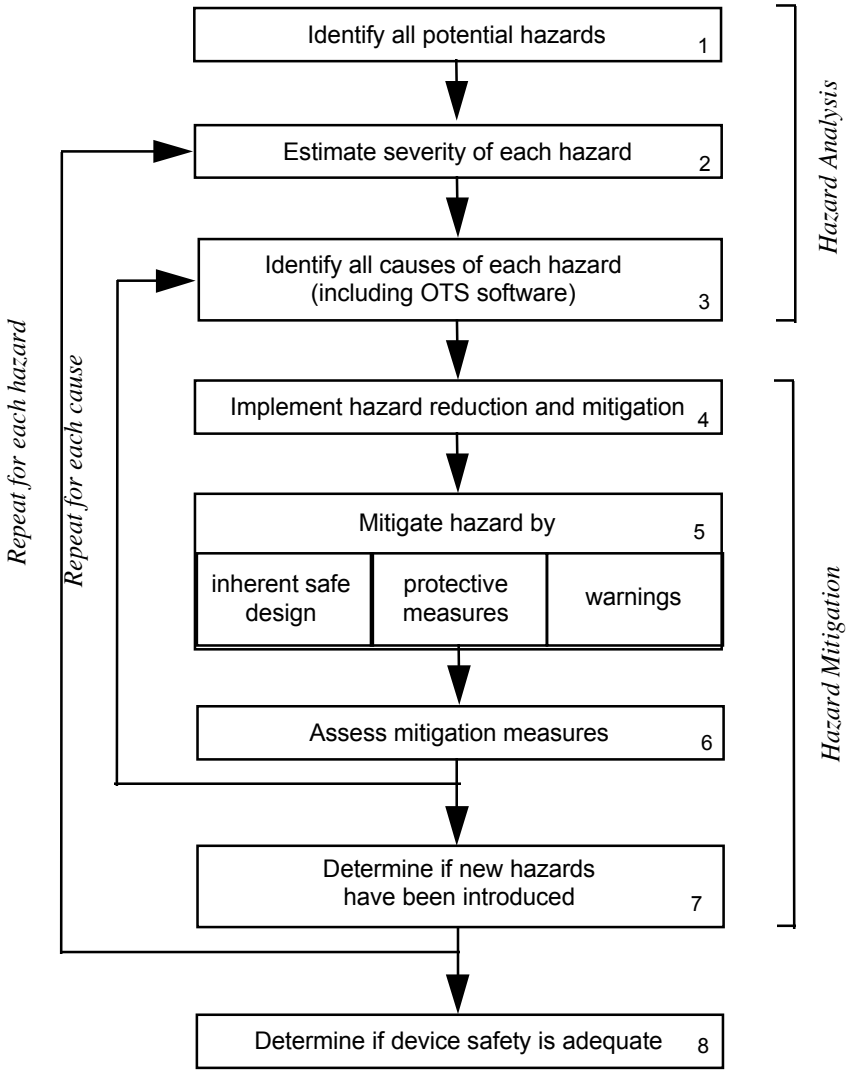
B. Hazard Analysis and Hazard List

A comprehensive hazard management approach includes hazard analysis and hazard mitigation that continues iteratively throughout the life of the product. The manufacturer is expected to perform an **OTS software hazard analysis** as a part of a **medical device (system) hazard analysis**.

The OTSS hazard can be no greater than the hazard posed by the device itself. The hazard analysis for such a device may simply document the minimal hazard of the device.

Hazards to patient safety and effectiveness from OTS software failure, malfunction, or misuse must be identified. Figure 2 summarizes the hazard management process.

Figure 2. Hazard Management Schematic



The submission should include the following information to document the medical device HAZARD ANALYSIS:

1. A list of all identified medical device hazards
2. The estimated severity of each identified hazard
3. Potential causes of each identified hazard

Note: A tabular format of the hazard management or a tabular summary will facilitate review.

Where failure, malfunction, or misuse of the OTS software poses no possibility of serious injury to the patient, then the OTS software is said to present a **MINIMAL HAZARD**, and the fulfillment of the BASIC REQUIREMENTS (see section II-A) will be considered sufficient.

C. Hazard Mitigation

Hazard mitigation activities may seek to reduce the severity of the hazard, the likelihood of the occurrence, or both. Hazard mitigation interventions may be considered in three categories with the following order of precedence:

1 - Design (or redesign)

2 - Protective measures (passive measures)

3 - Warning the user (labeling, active measures)

These approaches are by no means mutually exclusive and often may be used concurrently. The most desirable approach is to design in effective hazard controls, i.e., eliminate the need for a hazardous operation or component. Protective measures are considered passive (from the user's standpoint) since they do not require any action on the part of the user. Least desirable, is to depend on some action (or lack of action) on the part of the medical device user.

With implementation of each hazard mitigation, the residual hazard is assessed as well as assessment of any new hazards introduced.

The submission should include the following information to document the medical device HAZARD MITIGATION:

1. A list of all identified medical device hazards associated with the OTS software
2. The steps taken to mitigate the hazard
3. The residual hazard

Note: A tabular format of the hazard management or a tabular summary will facilitate review. These results will typically be included as a part of the overall medical device hazard mitigation.

One example of a comprehensive approach to injury prevention in public health was developed around ten "countermeasures" [3]. Table 1 illustrates a generic approach to the hazard mitigation, in this case, to preventing injury-related energy release to patients.

Table 1. Injury Reduction Countermeasures

1.	Prevent accumulation of the energy.
2.	Reduce the amount of the energy delivered.
3.	Prevent inappropriate release of the energy.
4.	Modify the release of the energy.
5.	Separate the patient from the energy in time and space.
6.	Provide physical barriers between the energy and the patient.
7.	Change the surfaces or basic structures at the interface.
8.	Strengthen resistance of the patient.
9.	Provide rapid emergency response to injury.
10.	Improve medical care and rehabilitation.

Following the HAZARD MITIGATION steps, the sponsor needs to assess the remaining hazard.

Where failure, malfunction, or misuse of the OTS software is likely to result in death or serious injury to the patient, then the OTS software is said to present a **SIGNIFICANT HAZARD**. Likely here is taken to mean "more likely than not".

Acceptable levels of hazard mitigation depend on the intended use of the medical device and the function performed by the software.

In the case of diagnostic tests, injury includes results which can lead to unnecessary invasive diagnostic testing (e.g., biopsy) or withholding or delaying important diagnostic or therapeutic procedures.

If the residual hazard from the OTS software presents SIGNIFICANT HAZARD, the sponsor will need to fulfill SPECIAL REQUIREMENTS (II-D), otherwise, the sponsor will need to describe and justify the residual hazard (section II-E).

D. SPECIAL REQUIREMENTS for OTS Software

To fulfill SPECIAL REQUIREMENTS for OTS software the medical device manufacturer is expected to:

1. Provide assurance to FDA that the product development methodologies used by the OTS software developer are appropriate and sufficient for the intended use of the OTS software within the specific medical device. This should include an audit of the OTS software developer's design and development methodologies used in the construction of the OTS software. This audit must thoroughly assess the development and qualification documentation generated for the OTS software.

   If such an audit is not possible, and the OTS software represents an unmitigated SIGNIFICANT HAZARD, the use of such OTS software may not be appropriate for the intended medical device application.

2. Demonstrate that the procedures and results of the verification and validation activities performed for the OTS software are appropriate and sufficient for the safety and effectiveness requirements of the medical device. Verification and validation activities include not only those performed by the OTS software developer, but also includes those performed by the medical device manufacturer when qualifying the OTS software for use in the specific medical device.

3. Demonstrate the existence of appropriate mechanisms for assuring the continued maintenance and support of the OTS software should support be terminated by the original OTS software developer.

E. Describe Hazard Level & Justify Safety and Effectiveness

The sponsor should provide a detailed (complete) discussion of the hazard which remains.

The hazard related to the use of OTS software should be considered in relation to the hazard of the alternatives, i.e., custom developed software. Any experience (data) with the use of the OTS software in this or a related application should be presented and considered. Acceptable levels of hazard mitigation depend on the specific medical device application.

III. OTS Software in Marketing Applications

A. Examples

Examples of medical devices using OTS software which have been cleared under 510(k) applications are described in this section. These examples illustrate the reasoning which leads to defining the level of hazard from a medical device and thus the kinds of development processes which should be used and the information to be provided in a regulatory submission.

Corneal Topographer -- Minimal hazard medical device (II-A)

Intended Use: A corneal topographer provides images of the abnormalities in the curvature of the cornea, the simplest being astigmatism.

Description: A corneal topographer consists of a hollow cone which the patient looks into from the base looking towards the interior of the point (like looking into the big end of a megaphone with one eye). The inside of the cone is white with black concentric circles. The concentric circles reflect off the eye and are imaged by a camera with a computer controlled lens situated at the point of the cone looking at the patient's eye. The shape of the reflected concentric circles are used to develop a topographic map of the cornea curvature which is printed out.

OTS software: An OTS operating system such as Windows is commonly used to interface the user, the microcomputer hardware platform, the corneal topographer, data storage, and output devices.

OTS software Hazard: A corneal topographer represents minimal hazard of direct harm to the patient. The hazard of indirect harm from a misdiagnosis relating to medical device malfunction is small since the worst case is an incorrect image which is considered correct. The OTS software in this medical device thus represents a MINIMAL HAZARD (see section II-B) and must satisfy BASIC REQUIREMENTS (see section II-A).

Perineometer -- Minimal hazard medical device (II-A)

Intended Use: Perineometers are used to provide feedback to a patient performing muscle strengthening exercises (Kegel exercises) for the treatment of certain types of urinary incontinence.

Description: There are two types of perineometers: those which measure pressure, and those which measure electrical activity (EMG) from muscles. Each device consists of a probe that is placed into either the vagina or the rectum, and a monitoring unit. The pressure devices use an air-filled probe connected to the monitoring unit by a piece of plastic tubing. When the patient performs the exercise, the probe is compressed, and the monitoring unit reports the change in pressure. The electrical devices use an electrode to measure the electrical activity of the target muscles during the exercises, and this information is reported by the monitoring unit.

OTS software: An OTS operating system, such as DOS or Windows, may be used to record and display the data collected by the monitoring unit.

OTS software Hazard: Perineometers represent a minimal hazard of direct injury to the patient, since no energy is applied by the medical device to the patient. The hazard of indirect injury due to inaccurate feedback during the exercise session is expected to be small, as these medical devices are only used as an adjunct to exercise therapy, and they are used under clinical supervision. The OTS software in this medical device thus represents a MINIMAL HAZARD (see section II-B) and must satisfy the BASIC REQUIREMENTS (section II-A).

Implantable Medical Device Programmers -- Describe Hazard, Justify Safety and Effectiveness (II-E)

Intended Use: An implantable medical device programmer provides interface and two-way communication with an implantable cardioverter-defibrillator (ICD) or cardiac pacemaker.

Description: An implantable medical device programmer consists of an electromagnetic programming head which is placed over the implanted device and provides through-the-skin communication with the implanted device, the personal microcomputer (PC) interface, and the PC hardware and software. The programmer permits the physician-user to:

- query the implant for performance history (device and patient), and, in some systems, for print-out of the recorded electrograms;
- set the adjustable (programmable) characteristics of the implant;
- provide the induced shock for system initialization and diagnostic purposes; and
- verify implant operating characteristics and status (including battery) *via* signals from the implant.

OTS software: An OTS operating system such as DOS or Windows is used to provide a user interface (sometimes graphical), interface to the PC (hardware platform), and interface with data storage, and output devices.

OTS software Hazard: The on-board software for the implant satisfies the definition of high-hazard software (life supporting/life sustaining) and would need to satisfy the SPECIAL REQUIREMENTS (see section II-D). Whether the device programmer can be considered of lesser hazard depends primarily on the protection designed into the implant. Steps taken to mitigate the hazard might include:

- design of the implant to minimize the possibility of misprogramming to inappropriate operational states;
- design of the programmer interface to minimize the chance of miscommunication including hardening of the hardware against electromagnetic interference (EMI);
- limiting the part of the OTS software which is utilized in the programming application;
- protecting the PC from use for other applications;
  - What are the software design features to protect against adding unwanted software, modification or system use?
  - What are the hardware design features to protect against unwanted system use?

Other points which might be offered to support use of OTS software in the programmer might include:

- documented experience (data) with use of the OTS software in this application
  - What was the system in place to detect and report problems?
  - What is the rate of problems reported compared to other (perhaps non-OTS software) systems?
- documented experience with the OTS software in other relevant applications
  - What are the reported problems (bug list) and how many are relevant to this application?
  - Has there been difficulty in developing work-arounds for the problems relevant to this application?

The review team must decide whether the overall programmer system as implemented satisfies the necessary system safety and effectiveness (see section II-E).

B. 510(k) Issues with OTS software

The conditions under which a new or changed medical device including OTS software will require a new 510(k) are the same as for a device not involving OTS software. These conditions are given in CDRH's guidance *Deciding When to Submit a 510(k) for a Change to an Existing*

Device [4]. The section (B) on Technology Engineering and Performance Changes in the 510(k) guidance is most applicable to OTS software.

Section B of the guidance includes the following questions:

B1 Is it (the modification) a control mechanism change?

B2 Is it an operating principle change?

B5 Is it a change in performance specifications?

B8 Is it a change in software or firmware?

B8 Is it a change in software or firmware? The types of changes identified at decision points B4 through B8 have frequently been called design changes or engineering changes. They encompass everything from the routine specification changes necessary to maintain or improve medical device performance as a result of feedback from users, field or plant personnel, etc., up to and including significant product redesign.

B8.1 Does the change affect the indications for use? As with an explicit labeling change, if the change affects the indications for use, i.e., if it creates an implied new indication for use, a new 510(k) should be submitted.

B8.2 Are clinical data necessary to evaluate safety and effectiveness for purposes of determining substantial equivalence? Whenever a manufacturer recognizes that clinical data are needed because bench testing or simulations are not sufficient to assess safety and effectiveness and, thus, to establish the substantial equivalence of a new design, a 510(k) should be submitted.

In the case of *in vitro* diagnostic devices, however, if a scientifically valid test of clinical samples demonstrate that the medical device continues to conform to performance specifications as contained in a voluntary standard or as described in a previous 510(k), a new 510(k) is usually not necessary.

B8.3 Do results of design validation raise new issues of safety and effectiveness? All changes to medical device design will require some level of design validation or evaluation to assure that the device continues to perform as intended. The successful application of routine design validation activities will logically result in manufacturers documenting their efforts and proceeding with the design change, i.e., assuring that no issues of safety or effectiveness are raised.

A yes answer to any of these questions in section B will require a new 510(k).

Typical OTS Software Changes Requiring a 510(k)

For medical devices where the OTS Software represents a MINIMAL HAZARD, OTS Software changes would not require a new 510(k). However, the manufacturer is responsible for validating the change.

For other medical devices, the decision as to whether a new 510(k) is required depends on the intended use of the device, the function of the OTS software, and to what extent the hazards due to OTS Software have been mitigated (see guidance on when to submit a 510(k) [4]).

Exemption of Laboratory Information Management Systems

Laboratory information management systems (LIMS) are Class I devices (21 CFR 862.2100, Calculator/Data Processing Module for Clinical Use). They are included in the category of electronic medical devices intended to store, retrieve, and process laboratory data. LIMS may also handle scheduling, billing and other non-device functions. LIMS have been **exempted from 510(k)** since June 8, 1988. However, compliance to all other requirements is required, including registration, listing, GMP, and MDR are applicable.

The LIMS exemption does not apply to applications of artificial intelligence or other algorithms intended to assign a probability of diagnosis for the purpose of guiding therapy or further diagnostic studies.

Clinical data management functions may be subject to FDA regulations as are blood establishment software systems.

C. IDE Issues with OTS software

An IDE is required for the same conditions as for a medical device not containing OTS software. The OTS software may be a component of a medical device or the OTS software may be the entire medical device, e.g., diagnostic software. These conditions are specified in 21 CFR 812 and generally include changes such as to effect: the patient population for which the medical device is intended, conditions of use of the device (including those recommended or suggested in the labeling or advertising, the probable benefit from the use of the device weighed against any probable injury or illness from such use), or the reliability of the medical device.

Some specific issues related to OTS software might include initial (beta) testing of an OTS software medical device with clinical studies. Such a study must comply with applicable IDE requirements. For non-significant risk medical devices, that includes approval by an institutional review board and patient informed consent. For significant risk studies, the initial user testing (beta testing) protocol would be included in an IDE submission to ODE. For example, beta testing of radiation treatment planning software, including any OTS software modules, would be conducted under a full IDE with FDA approval as a prerequisite.

Exemption of Diagnostic Devices

If the product incorporating the OTS software is a diagnostic medical device, it may be exempted from IDE requirements, if it meets the criteria in section 21 CFR 812.2(c)(3). For example, clinical (beta) testing of a noninvasive diagnostic device that does not require significant risk invasive sampling procedure and that does not introduce energy into the body, is exempted from IRB approval, patient informed consent, and other IDE requirements, if a medically established diagnostic product or procedure is used to confirm the diagnosis.

D. PMA Issues with OTS software

The criteria and requirements for premarket approval applications are in 21 CFR 814. When a manufacturer submits a premarket approval for a medical device, there must be valid scientific evidence (including clinical evidence, if needed) to support a reasonable assurance of safety and effectiveness of the device.

The OTS software used in a medical device is evaluated in the context of the overall medical device. The extent to which the manufacturer must demonstrate conformance to appropriate life cycle control depends upon the overall hazard of the medical device, the role of the OTS software, and the hazard associated with possible failures of the OTS software component.

For example, a commercially available neural network used by a medical device manufacturer for pattern recognition, would require extensive validation if used in a Pap smear screening device, in computer-assisted radiology, or for computer-assisted analysis of EKG wave forms. The same neural network, used for less critical computer-assisted analysis of EEG wave forms, might require less rigorous software documentation. Likewise, a commercially available personal computer operating system with graphical user interface, would require extensive documentation and evidence of validation when intended for use in a cardiac pacemaker programmer. Less documentation and verification of the OTS operating system would be required for programming an artificial ear.

Artificial Intelligence

OTS knowledge-based software (artificial intelligence, expert systems, neural net software, et al) are being developed for a number of medical applications. A typical system accepts clinical findings (sometimes including imaging data) and generates probabilities of disease states and/or recommendations for subsequent data gathering or treatment. The clinician may order a surgical biopsy or other invasive tests or initiate therapy based on the system output. Such systems, should be tested and reviewed in a manner consistent with both their safety and effectiveness of their direct effects (recommendations) and indirect effects (missed appropriate diagnostic testing and treatment). See *Diagnostic OTS software for Triage of Patients for Further Testing or Therapy for Abnormal Pathophysiologic Conditions*, Section III-A and the software guidance [5].

E. Product Labeling

The user's manual should specify the version(s) of the OTS software that can be used with the medical device. Such specification would not be required for embedded software (i.e., the user does not select the OTS software and cannot change the software provided by the medical device manufacturer).

The user's manual should contain appropriate warnings to the user indicating that the use of any software other than those specified will violate the safety, effectiveness and design controls of this medical device. Such use may result in an increased hazard to users and patients. Further description of what comprises a warning and how to write it are included in *Medical Device Labeling -- Suggested Format and Content* [6]

When OTS medical device software is delivered on a magnetic/ user installable medium, the package should include labeling that indicates the specific hardware platform on which the software is validated to run (processor, memory, disk, interface etc.). The appropriate testing for the user to assure proper installation should also be described in the labeling.

If the hardware on which the OTS software runs is a stand-alone computer, the user should be warned against installing any other software (utilities or applications programs) on the computer if they are not "locked out" by hardware or software system features.

IV. Bibliography

A. References for this Guidance

1. USPHS DHHS FDA CDRH: Use of Off-the-Shelf (OTS) Software in Medical device Applications, Blue Book Memorandum G97-__, Issued ___, 2 pages. Abs: This document contains the brief policy statement concerning the use of OTS software in medical devices. It is the cover memorandum for this guidance document.

2. USPHS DHHS FDA ORA: FDA Glossary of Computerized System and Software Development Terminology. The Division of Field Investigations, Office of Regional Operations, Office of Regulatory Affairs, US Food and Drug Administration, August 1995, 36 pages. Abs: This document provides the definitions (except for OTS software) relied on in our OTS software guidance. Available on the FDA Home Page at `http://www.fda.gov//ora/inspect_ref/igs/gloss.html`

3. Haddon W, Baker SP: Injury protocol. in Duncan, Clark Brain, MacMahon (eds): Preventive Medicine, New York, Little, Brown, 1979. Abs: A readable discussion of basic injury reduction strategies from some of the most experienced in the field.

4. USPHS DHHS FDA CDRH: Deciding When to Submit a 510(k) for a Change to an Existing Device. 510(k) Memorandum #K97-1. final Version, November 4, 1996. copies are available as of __ Abs: CDRH's final draft guidance was released 1/14/97, text version is available on the FDA home page at `http://www.FDA.GOV/cdrh/ode/510kmod.html`.

5. USPHS DHHS FDA CDRH: ODE Guidance for the Scientific Review of Premarket Medical device Software Submissions. Draft Version 1.2, March 13, 1996 copies of this work-in-progress are available as of 3/4/96, Abs: This document provides the current guidance in the review of software which comprises part of (or all of) a medical device. Available on the FDA Home Page at http://www.fda.gov//cdrh/ode/dtswguid.html

6. USPHS DHHS FDA CDRH: Medical Device Labeling -- Suggested Format and Content. DRAFT Version 4.2, copies of this work-in-progress are available as of March 4, 1997 Abs: This document provides the current guidance on the policy, format and content of the labeling of medical devices.

V. Appendices

A. Operating Systems

The purpose of this appendix is to provide background and comment on the use of OTS operating systems for medical devices.

The **operating system** software is the primary software program which manages the basic functions of the computer and its associated hardware, including peripherals. The operating system provides a basic user interface, is responsible for managing applications programs and tasks, controlling memory allocation and data storage devices, and providing input/output for the computer as well as any additional peripheral devices which are present.

Utility software is associated with operating system software is, which is designed to work with a specific operating system. Unlike applications software, utility software is intended to supplant or enhance functions typically performed by the operating system. Examples of utility programs are memory managers, file managers, and virus checkers. Networking software can also be considered as utility software in that it allows multiple computers to access the same resources. Operating systems can also be designed to support or enable network operations without any additional utility software.

Off-the-shelf operating systems are commonly considered for incorporation into medical devices as the use of general purpose computer hardware becomes more prevalent. The use of OTS operating system software allows device manufacturers to concentrate on the application software needed to run device-specific functions. However, it must be recognized that an OTS operating system software is intended for general purpose computing and may not be appropriate for a given specific use in a medical device. Developers of OTS operating systems typically design their systems for general purpose business or consumer computing environments and tasks where software failures and errors are more accepted. This acceptability of errors in the

general purpose computing environment may make the OTS operating system software inappropriate for less error-tolerant environments or applications.

The incorporation of OTS operating system software **may also introduce unnecessary functions and complexity** into a medical device. General purpose functional requirements typically result in the OTS operating system software being large and unwieldy in the attempt to incorporate more functionality into the operating system. This excess functionality is typically never used for specific medical device applications and increases the likelihood that errors may be introduced into the operating system. The basic functions of an OTS operating systems used for medical device applications are typically the graphical user interface environment and the hardware interface functions. There are a number of operating systems used for timing- or resource-critical applications that provide the basic functionality needed to support user and hardware interfaces, but do not have many of the disadvantages of general purpose business or consumer operating systems.

Operating systems designed for **"open" hardware architectures**, such as the IBM PC or Apple Macintosh type machines, are problematic because they are designed with a level of acceptable variances in hardware tolerances and interface protocols that can adversely affect the operation and performance of software. It is common for such operating systems and applications software to perform well on one hardware configuration, but fail catastrophically on a slightly different configuration. The existence of this "open" architecture environment makes it very important that operating system software to be designed to be "robust" and perform appropriately on different hardware configurations when there is no control by the medical device manufacturer of the specific configuration of the target hardware platform.

B. Utilities and Drivers

The purpose of this appendix is to provide general recommendations and background for the use of OTS utility and driver software packages in the medical device validation process that are the responsibility of the medical device developer.

OTS utility software packages perform the following functions, math functions (fast Fourier transform, sin, cos); display functions (graphic); management functions (copy, delete, store various computer data/files); and the data manipulation function (transfer from one Boolean type or both. The validation for these types of the software should include:

Numerical type - evaluate the maximum and minimum numerical boundaries for both input and output values including the error handling process for out of the range values.

Boolean type - evaluate all the possible combinations for both input and output for patient hazard. If the number of the possible modes is large, then develop a subset of the modes including prevalent and worst case conditions.

Either type (data management and data manipulation) - validate functions within the system qualification process for the final finished medical device (not the prototype or development system).

OTS driver software packages provide interface functions between the CPU, operating system, and the input/output peripheral. However, the performance and functionality of the OTS driver software may be affected by the overall system configuration and the OTS hardware. In general, OTS driver software packages can be classified into the following input/output interface types: serial, parallel, video signal, telemetry, LAN, and internal bus. In most cases, a particular software driver derives from a particular interface protocol and contains the data signals, control signals, and timing signals for proper operation.

Since tests for most input/output interface/bus configurations require the particular bus analysis or logic analysis, scope, and the knowledge of the particular interface protocol, it is recommended that the validation process for the OTS driver software package be part of the system interface validation process. This includes the verification of the data values in both directions for the data signals; various mode settings for the control signals in both directions (if applicable); and the input/output interrupt and timing functions of the driver with the CPU and operating system. In addition, it is recommended that the system hazard analysis should include the involuntary disabling or partial disabling of the OTS driver communication during the therapeutic or diagnostic session of the medical device.

C. Local Area Networks (LANs)

The purpose of this appendix is to provide general recommendations and background for the network aspects of OTS software use. Medical devices, particularly multi-parameter patient monitors and imaging systems, are increasingly networked for clinical work groups, centralized monitoring, and storage of patient medical data and records. LANs and other networks support more and more communication and sharing of images, measurement data, audio, video, graphics, text, etc. This heterogeneous media environment comes at a cost of more processing power, higher bandwidth or network speed, sophisticated object-relational databases, security and access considerations.

The evaluation of networked medical devices begins with a definition of the technical requirements of the network application and the understanding of those requirements.

Requirements Analysis

1. Speed - The response time required for safe and effective operation determines the LAN data rate (bandwidth) for the medical device system. The CPU processing power and clock speed required at device monitors, workstations, and client machines must be appropriate so that bottlenecks do not occur.

2. LAN Architecture - The size of the LAN (the number of user nodes) and the topology of the LAN should be specified. The following questions might be considered in the design of the LAN architecture:
    - Does the LAN need to be fault tolerant, e.g., when a workstation fails?
    - Does the LAN need to be scaleable, i.e., can new user nodes be added without degrading system performance?
    - Will the main device software be computationally self-sufficient or distributed?

3. Network Operating System (NOS) - Specify the NOS to be used. Whether off-the-shelf or proprietary, this selection should consider the trade-off between robustness and flexibility.

4. Data Integrity - One of the most important issues for any medical device operating in a network is data integrity. The manufacturer must insure that the network system software and hardware incorporate error checking, handling, and correction measures commensurate with the intended use of the device.

    Transmission of data packets and files should include error detection and correction. Error detection methods include parity, checksum, and cyclic redundancy check (CRC).

    Transaction rollback after non-committed changes or network failure, supports data integrity in medical device LANs.

    Critical data and files may be stored in duplicate at separate locations.

5. Network Management and Security - User authorization and authentication should precede accesses to sensitive patient information.

The above five items are not independent. Decisions made in one item area may affect the performance of the LAN in another area.

Implementation

The speed required by the medical device system dictates the hardware selection, the network interface cards and transmissions protocols. For example, if the conventional Ethernet protocol (maximum transmission speed of 10 Mbps) is too slow for the intended application, then a different transmission protocol will be needed.

Simplicity of the LAN architecture versus fault tolerance is a trade-off that may arise in the implementation of the networked medical device systems. The LAN could be implemented as a linear bus network (perhaps the simplest scheme), but if any connecting link on the bus fails the whole network can fail. A star topology with redundant centralized hub is an example of a more complex but more robust network structure.

Segmentation of high bandwidth applications may be employed to improve LAN performance. Limiting the data traffic to data intensive clusters reduces traffic throughout the overall LAN.

D. Device Master Files

Much of the information regarding development and validation of OTS software may not be readily available to the medical device manufacturer who wishes to use the OTS software as a device component. Commercial OTS software vendors who wish to make their OTS software available for use in medical devices, but do not want to share the confidential and/or proprietary details of their software development and validation with customers (medical device manufacturers) may direct the information in a device master file to the FDA for clearance.

The master file should contain information regarding the OTS software development, validation and known software bugs in support of use of the software by medical device manufacturers. The intended level of hazard of potential device applications should guide the OTS vendor in deciding what level of detail to provide in the master file.

The OTS software vendor should also consider which types of device applications may or may not be appropriate uses of the OTS software as a component. The vendor can then grant permission to specific device manufacturers to reference the master file in their premarket submissions. Information regarding device master files is contained in DSMA's "Premarket Approval (PMA) Manual", or via Facts-on-Demand or from the FDA home page (http://www.fda.gov).

E. Maintenance and Obsolescence

This appendix addresses relevant maintainability issues with regard to OTS Software in medical devices. Normally maintenance activities are performed relative to a system baseline configuration.

Maintenance activities are generally considered to begin subsequent to the establishment and distribution of a medical device product baseline. There are many design issues related to maintenance activities not generally of concern during the development of this product baseline. Some of these issues are outlined in this section.

The distinction between maintenance and product development is an important one. Product development design activities generally lead to a system structure of highly integrated components and logic. Maintenance activities introduce changes into this structure which may lead to a loss in the integrity of the structure. Structure integrity may be effected through changes due to new design requirements, corrections, or environmental adaptations. These types of changes may impact the integrity of the structure organization, architecture, logic, integration, or any

combination of these characteristics. Maintenance of products with OTS software components may be particularly problematic for reasons discussed in the main body of this document, i.e. the sponsor does not have control of the OTS software component life cycle process.

In particular, this section identifies general safety and effectiveness, design, verification / validation, change, installation, and decommissioning profiles to consider. These profiles may be applied to all regulated Programmable Electrical Medical Systems (PEMS) and stand-alone medical software devices. Device specific profiles may subsequently be necessary for appropriate evaluation.

Assumptions for this section include:

a) Manufacturer Good Software Development Practices (GSDP)s and Good Corrective Action Practices (GCAP) are in place.

b) A product baseline exists

c) A new product baseline based on a prior product baseline is under review

E.1 Profiles

Each profile below maps to a product development life cycle phase. The profiles identify fundamental maintenance concerns relevant to all regulated PEMS and stand-alone medical software devices. Guidance in the main body of this document provides the procedural foundation for profiles in this section.

E.1.1 Safety

Introduction of new or modified OTS components to a product baseline may impact the safety of the product. Therefore a safety impact assessment must be performed and associated hazards documented in a Failure Modes and Effects Analysis (FMEA) table. Each hazard's consequence should be provided and expressed qualitatively; e.g. major, moderate, minor. Traceability between these identified hazards, their design requirements, and test reports must be provided.

Analysis should include the review of release bulletins (known error reports), user manuals, specifications, patches, literature and internet searches for other user's experience with this OTS Software.

The submission should answer the following questions:

a) has a FMEA with traceability to requirements and test reports been provided?

b) are safety functions isolated from new OTS component(s)?

c) does the new OTS component affect system safety integrity?

d) what new human factors conditions are introduced with new OTS components?

E.1.2 Design

Introduction of new or modified OTS software components to a product baseline may impact the original design of the product. This impact may result from necessary changes to the product structure organization, architecture, logic, integration, or combination of these characteristics.

Problems attributable to structural changes include:

1) new system resource requirements, such as shared and/or fixed memory
2) new timing considerations
3) new memory organization (e.g., 16 bit to 32 bit to 64 bit words), partitioning
4) new human factor issues
5) new data integrity issues
6) new software required to create the final code (build tools)

Consequently the submission should answer the following questions:

a) How will the new OTS software component(s) change the performance characteristics?

b) How will the new OTS software component(s) change the operational environment?

c) Is data integrity preserved?

E.1.3 Verification & Validation

As in the establishment of a product baseline, verification and validation (v&v) activities must occur when maintenance changes are made to a product baseline. Analysis of these changes directs necessary v&v activities. New OTS software components in a product baseline introduce unknown logic paths and complexities into the product. "Black-box" testing of OTS software components may allow some validation claims to be made. However, the unknown logic paths and complexities of OTS software components make it important to know that design structure or logic elsewhere in the system are not impacted. This means a full system regression test should be performed. Results of these validation activities should be documented.

The submission should answer the following questions:

a) Do test reports provide objective evidence that identified OTS software component hazards have been addressed?

b) Do test reports provide objective evidence that all identified SYSTEM hazards have been addressed?

c) Has a complete system regression test been performed?

E.1.4 Installation

Changes in a product baseline structure resulting from the integration of new OTS software components may impact installation requirements. This impact can range from minor documentation changes to field upgrades. The reviewer should ascertain the impact of OTS software component changes on fielded products.

The submission should answer the following questions:

a) What is the impact of new OTS software components on fielded medical device products?

For example: Do new OTS software components correctly operate within the specifications of medical devices currently fielded?

E.1.5 Obsolescence

Rapid technology changes, economics, and market demand are shrinking product life spans. A direct consequence of these phenomena is that an OTS software component today may not exist two years from now. Short life spans are a particular characteristic of software because it is relatively easy to change. Obsolescence of OTS software components can have significant impact on regulated products because the sponsor may lose the ability to properly support fielded products. The sponsor needs to support fielded medical device products with OTS software components.

The submission should answer the following questions:

a) Is the old OTS software component still available for fielded medical devices?

b) Is there a retirement plan for OTS software components to be replaced/eliminated?

c) Do new OTS software component(s) replace fielded components?

E.1.6 Change control

The submission must identify the product to be considered. Therefore, the product configuration provided should specify:

a) hardware platform

(e.g. microprocessor, minimum memory required, addressable word size)

b) software platform

(e.g. operating system, communications, database's, necessary utilities, etc.)

c) OTS component(s) other than (b) above

(See basic requirements in the main body of this document)

d) internally developed application(s)

---------- end of guidance document ----------

Center for Devices and Radiological Health

Food and Drug Administration

Respectfully submitted,

The OTS Software Team

Name	Email	Unit	Mail	Phone
Carr, Joe	CarrJJ.nimitz@navair.navy.mi		703-604-6237	
Cheng, Jim	JMC	DCRND	HFZ-450	443-8517
Crumpler, Stewart	ESC	OC	HFZ-343	594-4659
Jones, Paul L	PXJ	OST DECS	HFZ-141	443-2536 x 64
Lee, James	JXL	DCRND	HFZ-450	443-8609
Madoo, Lark	LWM	DCRND	HFZ-450	443-8609
Mischou, Bruce	BXM	DOD	HFZ-464	594-2018
Murray, John F.	JFM	OST DECS	HFZ-141	443-2536 x 63
Ogden, Neil	NRO	DGRD	HFZ-410	594-1307
Robinowitz, Max	MYR	DCLD	HFZ-440	594-1293
Rudolph, Harvey	HXR	OST OD	HFZ-141	443-2444
Spyker, Dan	DXS	DCRND	HFZ-450	443-8320
Tillman, DonnaBea	DBT	DRAERD	HFZ-470	594-1180