

# Systems Engineering for FDA QSR Compliance

James H. Jones

Optants Documented Decision Support Company (ODDSCO)

297 Casitas Bulevar, Los Gatos, CA 95032-1119

[www.optants.com](http://www.optants.com) [jjones@optants.com](mailto:jjones@optants.com)

Copyright © 2007 by James H. Jones.

**Abstract.** Many engineers have work experience with defense and aerospace suppliers and other government funded entities that included exposure to classical Systems Engineering methods with an Integrated Product/Process Team (IPPT) approach for products development. However, such employment is not universal, so even experienced Systems Engineers should know of one category of commercial enterprises that can benefit greatly from application of their fundamental processes knowledge. Manufacturers of medical devices must comply with Food & Drug Administration (FDA) 21 CFR 820 Quality System Regulation (QSR). The QSR requires enterprise as well as processes compliance. Even clearance to advertise (market) a device is based on evidence of compliance with QSR design controls provisions. Accordingly, high emphasis is on producing documents and records of tasks performed for auditable evidence of the compliance. Thus, this paper describes the author-proven Systems Engineering methods that may be employed to virtually automate project deliverables compliance with QSR design controls.

## Introduction

**Purposes.** This paper is intended to accomplish three objectives:

1. Show, via selected quotations, that FDA 21 CFR 820, the Quality System Regulation (QSR), reaches into how medical device development enterprises must be organized and operated, as well as the expected grasp of the safety and effectiveness of their products.
2. Show, using the context of medical devices based upon embedded computer systems with which most INCOSE members are familiar, that relatively fundamental Systems Engineering methods are the means to provide integrated processes for QSR compliance.
3. Show, with additional constraints of generally small medical device development enterprises and lack of methods knowledge many INCOSE members assume is obvious, that advancing Systems Engineering must await organizational assimilation of the fundamentals.

**Text Conventions.** Direct quotations from the QSR are in double quote marks. Key FDA terms are underlined for emphasis. Author summaries and interpretations of QSR are in brackets.

## The Quality System Regulation (QSR), Summarized

**The QSR, General.** Medical devices built for sale and use with patients in the United States must have been auditably compliant with FDA 21 CFR 820 Medical Device Quality System Regulation (QSR), throughout their development process. The first sentence of the regulation states the FDA emphasis: “Current good manufacturing practices (CGMP) requirements are set forth in this quality system regulation.” In 820.1 Scope, the second sentence of (a) Applicability

is: “The requirements in this part govern the methods used in, and the facilities and controls used for, the design, manufacture, packaging, labeling, storage, installation, and servicing of all finished devices intended for human use.”

Quoting from Sec. 820.1 Scope (c) Authority, “The failure to comply with any applicable provision in this part renders a device adulterated under section 510(h) of the act. Such a device, as well as any person responsible for the failure to comply, is subject to regulatory action.” The FDA has many tools for enforcement. Regulatory action may include financial penalty, stopping sales, seizing or detaining devices, etc. A Recall can include removing equipment from a medical facility or hospital or prohibiting its use (stopping treatment where device is used). Publication of simply receiving an FDA Warning Letter can negatively impact future business.

Preventing such undesired outcomes means withstanding audits through provision of records that effectively show compliance with the QSR for issues that could arise. In other words, the company work practices, products, and records all must show the manufacturer as being in a state of control (from the FDA perspective) throughout the device development.

**What the FDA Requires of Developer Quality Systems.** Subpart B—Quality System Requirements, covers major aspects of Management Responsibility, Quality Audit, and Personnel.

The first section sets forth what the management with executive responsibility must do to ensure “the quality policy is understood, implemented, and maintained at all levels of the organization” and provide an organizational structure adequate for compliant design and production. The management representative is appointed to ensure effective establishment of a “quality plan” along with “procedures and instructions” and formally report on its performance at intervals defined for management review.

The Quality Audit section requires conducting quasi-independent audits “to assure that the quality system is in compliance with ...” and record its performance in a report for management review of the results “determined by individuals not having direct responsibility for the matters being audited.”

The Personnel section states, to quote fully:

- (a) General. “Each manufacturer shall have sufficient personnel with the necessary education, background, training, and experience to assure that all activities required by this part are correctly performed.”
- (b) Training. “Each manufacturer shall establish procedures for identifying training needs and ensure that all personnel are trained to adequately perform their assigned responsibilities. Training shall be documented.”

An Integrated Product/Process Team (IPPT) approach is appropriate to ensuring that training and the “procedures and instructions” fully accomplish their purposes.

**What the FDA Requires of Medical Device Developers.** Requiring QSR compliance is how the FDA fulfills its purpose for ensuring that each medical device is safe and effective. For the FDA to approve a medical device for marketing, sale, and use for patient treatment, the records documenting its development must accompany a statement of device Intended Use.

These records are mostly device development documents produced to show compliance with the ten sections of QSR Subpart C—Design Controls: (a) General. (b) Design and development

planning. (c) Design input. (d) Design output. (e) Design review. (f) Design verification. (g) Design validation. (h) Design transfer. (i) Design changes. (j) Design history file.

Application of Systems Engineering methods to the design controls provision is individually described below in a separate Section, after remainder of the QSR is described.

**Manufacturing Related Provisions of the QSR.** The QSR requires substantial control of the medical device manufacturing following its design. Subparts D through L generally instruct that “Each manufacturer shall establish and maintain procedures ...” These Subparts closely related to device manufacturing are named Document Controls, Purchasing Controls, Identification & Traceability, Production and Process Controls, Acceptance Activities, Nonconforming Product, Corrective and Preventive Action, Labeling and Packaging Control, Handling, Storage, Distribution, and Installation.

**Documentation (Records) Requirements of the QSR.** Subpart M—Records, has five sections. The general section requires that records be maintained at a location accessible to responsible officials, made available for review and copying by FDA inspectors, be legible, etc. The FDA also can require an employee with executive responsibility to certify that management reviews and quality audits were performed and formally documented – and required corrective action has been undertaken.

The Device Master Record: [Contains the information needed to replicate the device.]

Device History Record: [Contains information related to manufacture and acceptance of each device, by serial number.]

Quality System Record: [The sets of records not specific to particular types of device(s), while conforming to provisions for Document Controls.]

Complaint Files: [Review of possible failure of a device, labeling, or packaging to meet its specifications is emphasized, reportable event gets special treatment, the investigation record has required subsections, etc.]

**Servicing Related Requirements of the QSR.** Subpart N—Servicing, includes “(a) Where servicing is a specified requirement [make procedures], (b) Each manufacturer shall analyze service reports [keep statistics], (c) [If service report involves event that must be reported to FDA, generate a formal complaint], and (d) Service reports shall [include specific information].”

**Volume Manufacturing Related Provision of the QSR.** Subpart O—Statistical Techniques, includes “(a) Where appropriate, [make procedures for valid process statistics] and (b) Sampling plans, when used, shall be written [be adequate and documented].”

## **The Systems Engineering Relationship to the QSR**

**Why Systems Engineering Assists QSR Compliance.** The QSR is not a recipe for developing medical devices. It most resembles a customer provided specification for a supplier process and was deliberately modeled on ISO 9001. It specifies what documented functions must result from a medical device product development system without fully specifying how to do them. Clearly, ‘requirements specifications’ for such a process are in a classical Systems Engineer’s domain of experience and capability.

**The Benefits of QSR Compliance.** When medical device manufacturer employees know QSR compliance is their basic job, applying IPPT approaches to improving processes is made easier.

‘Extra’ work to update non-compliant documentation as part of a retrofit, becomes just part of the job. Furthermore, the documentation to ‘prove’ QSR compliance is what employees already are (or should be) doing to ensure tasks completion.

Templates and other means to audit-proof documents help make the compliance relatively automatic. Further, applying best practices of classical Systems Engineering to work groups means that future product development projects also gain from auditable process improvements because they provide new efficiencies as well as effectiveness. That is, although there is some cost to install (especially when legacy specifications must be revised), applying basic Systems Engineering to attain demonstrable compliance is cost effective for the overall project.

## **Applying Systems Engineering to QSR Design Controls Provisions**

**820.30 (a) General.** Subsection (1) states, “Each manufacturer of any ... class III or class II device ... shall establish and maintain procedures to control the design of the device ... to ensure that specified design requirements are met.”

Procedures and Instructions (P&Is) are made to ensure medical devices development work performance and products are auditably compliant with all associated provisions of the QSR. P&Is must be maintained for correspondence to evolving and improving work processes. IPPT approaches to controlling P&Is development and maintenance, as well as performing project tasks, clearly are suitable arenas for applying classical Systems Engineering methods.

**820.30 (b) Design and development planning.** The Project Management Plan (PMP) is to “describe or reference the design and development activities and define responsibility for implementation”. The PMP describes the scope, scale, and complexity of the project. For more complex projects, where a PMP section and standard design specialty development plan would be inadequate, a subsidiary plan may be required. “The plans shall identify and describe the interfaces with different groups or activities that provide, or result in, input to the design and development process.” Thus, a PMP sets forth milestones sequencing of most project documents development. Another PMP objective is to drive auditability within each project document. The PMP must be reviewed and approved (and updated with fresh approval when project is revised).

Because projects may be a mix of new development and replacement of obsolete equipment, the scope and scale of development tasks range from extremely simple to relatively complex. A predetermined need may be to submit a 510(k) package for obtaining FDA Premarket Approval (to allow advertising a new or upgraded medical device to potential customers). Required content of 510(k) submissions for medical devices containing software is set forth in (21 CFR 807.87, 2005). Associated instruction is provided (“Guidance ...”, 2005). Accordingly, the PMP must support planning for conceptual worst case new or upgrade projects as well as accommodate tailoring instructions for it and associated documents (to reduce their contents in accordance with actual scope and scale of intermediate to small projects). Total reduction that may be defined by planned documentation tailoring is limited by minimum set of records necessary to comply with applicable QSR design controls provisions and to fulfill the 510(k) submittal. After tailoring of selected document templates to a defined reduction in scope and scale, the revised instructions enable each new author to know precisely what information must be obtained to complete each project document type, where therein to put it, and to what breadth and depth it must be set forth. This knowledge of deliverables content greatly assists developing initial budget and schedule estimates that correlate well with intent of the approved project plan.

When tailoring is complicated, relevant subsections of a separate (sibling) tailoring document can be cited by the PMP. Approval of a separate tailoring document must be by the same persons who approve the PMP. In any case, project work must be in accordance with an approved plan.

When needed, subsidiary plans may be cited by the PMP and developed in parallel. A major caveat: Although a purpose of project plans is to provide general guidance for developing the project deliverables, an exception is that tailoring instructions must be unambiguous and clear for tasks and documents to ensure project plans fulfillment remains auditable.

If defined as part of tailoring for a project, the content required in each specification type also can be tailored to the project scope and scale. Further, when multiple specifications of the same type are used, their tailoring can differ in accordance with planned project emphasis on new or high expense technology applications.

**820.30 (c) Design input.** Design input is defined in QSR 820.3 as “physical and performance requirements of a device that are used as the basis for a device design.” Design input therefore ranges from elicited customer inputs to requirements for addressing “the intended use of the device, including needs of the user and patient” to at least the top level software and hardware requirements specifications that drive detailed device design. Further, “procedures shall include a mechanism for addressing incomplete, ambiguous, or conflicting requirements.” [Intended Use is statement of purpose and function, target patient population, intended environment, and medical device safety and effectiveness claims, as set forth in the 510(k) premarket submittal.]

Marketing surveys, Medical department user studies, predicate or competitor device features, Quality Function Deployment (QFD, with “House of Quality”) and other sources, if any, may be used to determine a set of economically prioritized customer needs and wants as inputs.

A document for capturing customer inputs to the design requirements is the Customer Requirements Document (CRD). Its content must be approved by a representative of the customer (or some surrogate, such as corporate Marketing or Medical). The document that sets forth the highest level customer inputs as functional, performance, and design qualification requirements (a system specification) often is named Product Requirements Document (PRD). CRD inputs to the PRD must be addressed formally, but not necessarily by immediate project implementation. Some customer input can be noted as a deferral or partial implementation when full implementation is dependent on a prerequisite event or capability uncertain of occurrence. A PRD provides the design inputs to system level Hardware Requirements Specification(s) (HRS) for deriving all of the mechanical and electrical functional, performance, and design qualification requirements. Similarly, the PRD provides design inputs to system level Software Requirements Specification(s) (SRS). The PRD and each HRS and SRS “shall be reviewed and approved by a designated individual(s).”

**An IPPT Approach to Requirements and Traceability (Design Input, Explained).** The Requirements Management methods are the means to produce the auditable design inputs and outputs records that are evidence of compliance with the QSR design controls provisions.

Requirements are the formal means to describe a product such that any competent entity could be contracted to design and build it. A requirement in a specification is a natural language statement that sets forth a mandatory characteristic or functional behavior to be provided by the developed product or process. In fact, unambiguous and verifiable requirements become the single recipe that development teams must follow for design, manufacture, and testing of a

specified item. A “desirement” is very similar to a requirement, but describes some additional or extended characteristic or function. Requirement and desirement statements are placed in many specifications throughout a device development project, beginning with customer inputs, so both types should be accurate and comprehensive.

Because requirements and desirements may swap status during the early to middle phases of a project, for many reasons, they should be similarly worded. One standard convention is to use the word “shall” in requirements and replace it with the word “should” in desirements. A requirement statement is correct and complete when it fully responds to its design input and is verifiable by one or more of: instrumented test, demonstration, inspection, and/or analysis. A simple method to enable writing such requirements is to consistently use a predefined standard sentence structure and simple rules for their wording. See such a list in (Jones, J., 2002)

The CRD is intended to capture comprehensive statements of clinical needs, goals, and constraints elicited from the customer. Expressing such customer inputs in “requirements” text form can be helpful during their requirements analysis for development of the PRD.

The PRD fulfills primary purposes of a product system specification. PRD requirements translate customer inputs into general engineering terms for development of project deliverables by the hardware and software design teams. The PRD specifies requirements for functions and performance to be provided by the system, usually without predetermining the implementation; so its requirements state what is needed without stating how the resulting product is to do it.

The PRD also may list various corporate and external (domestic and/or international) medical device safety standards and other design qualification criteria (the “...ilities”) with which design output must be in accord, such as: Feasibility (technological, economic, socio-political), Availability (Reliability and Maintainability), Adaptability (future use), Producibility, Supportability, Usability, Disposability, Vulnerability/ Survivability (harsh use), and Safety.

Patient and user safety must be first among medical device requirements, so the PRD design qualification section may contain a large list of potentially applicable provisions that have been extracted from cited standards or previously developed risk analysis process documents.

To fulfill the FDA requirement that customer inputs be explicitly addressed, the PRD should (at minimum) contain a simple trace table in a concluding section or appendix that shows which individual requirement(s) respond(s) to each CRD requirement. When a CRD requirement is not included or only partly addressed, the PRD requirement identifier is replaced by a notation of the reason, such as deferred or awaiting funding. Because reverse trace of CRD inputs to the PRD requirements is a one to one (or one to few) relationship, a simple matrix is adequate.

The assigned System Engineer(s) develop the draft PRD to fulfill the objective that its requirements be directly or indirectly validated. To support tracing with verbal communication, the unique identifier (PUI) for each requirement should indicate its location within the document. (Header paragraph numbering for requirements does this, provided they always are at the same level, so the Table of Contents can be set to display only to the next higher level.)

Next, hardware and software engineers contribute missing requirements and correct wording until their translation into engineering terms conveys intent of the customer inputs. Together, project System Engineers and project design engineers analyze PRD requirements as aggregated constraints and develop concepts for potential hardware and software architectural solutions that satisfy customer clinical needs and fulfill the device’s intended use. Most PRD requirements are

allocated into the subsidiary system level hardware and software requirements specifications (HRS and SRS) based on functional subsystems of the conceptual system architectures. When a system is relatively complex, major subsystems may have their separate HRS and SRS.

Each system level hardware and software requirement results from deriving one or more parts of its source PRD requirement into the separate mechanical, electrical, and/or software requirements as needed to specify a system providing the specified functions and performance. Emphasizing the general rule, HRS and SRS requirements state what the hardware and software must do but not how to do it. (Implementation should be specified in a system level requirement only if interface with an existing separate system must be retained.) Just as for a PRD, each subsidiary requirement needs a project unique identifier (PUI) that provides its location within the specification document as well as its support of the trace linkage and verbal communication.

Again, unambiguous and verifiable requirements are the recipe that development teams follow for design, manufacture, and test of a specified item, so they should be accurate as well as comprehensive. Finally, a requirement should specify only one function (or be the parent to only closely affiliated functions). The requirements should define a product such that its design and build could be outsourced. (When requirement writing is poorly done, the information transfer begins at inadequate.).

A key concern is that text stating that something is to be done for a function to be fulfilled (and/or how well it must be done) is necessary but is not sufficient to form a valid requirement. A design engineer's comprehension of full intended meaning is likewise insufficient. That is, until fulfillment of a product or process requirement statement may be unambiguously confirmed (via test, demonstration, inspection, or analysis), it is not valid for use and should be rewritten.

Auditable evidence of compliance with the FDA QSR provisions for design controls must be produced during every medical device development. Requirements Management is the name for activities that result in such evidence via providing traceability of requirements from customer inputs to their eventual validation. Such traceability is provided by the project Requirements Verification/Validation Trace Matrix/Report (RVTM).

Each PRD requirement relating to selected design qualification items (e.g., accelerated life, environmental, or electromagnetic compatibility) is traced directly to its general validation procedure in the RVTM. Each PRD requirement that is allocated to hardware and/or software is traced to its derived requirement(s). Because it provides complete text for each requirement, an RVTM enables inspecting each subsidiary hardware and software requirement for both correct and complete response to its driving PRD requirement (and thereby is the "mechanism for addressing incomplete, ambiguous, or conflicting requirements").

Each derived requirement also is traced to its formal verification procedure/test case, thus indicating where its driving PRD requirement is indirectly validated. Listing the requirements being verified or validated in each cited procedure test case ultimately completes the tracing. The summary reports of verification and validation procedures results provide objective evidence of requirements fulfillment.

To show design addressing of unacceptable assessed risk levels, the RVTM also traces from a derived HRS (or SRS) requirement to the project Hazard Analysis item for which a PRD requirement was cited as the driver for implementing an abatement action for that hazard. Proof of risk reduction by design implementation then is provided in verification procedure results for

the HRS/SRS requirements with such trace citations. Such a comprehensive RVTM provides a medical device development with its “roadmap” to the evidence of design controls compliance.

Below system requirement level, the design engineers provide implementation, design, test, and manufacturing “requirements” that describe how many of the HRS or SRS requirements are to be fulfilled. In simple, small scope and scale projects, the implementation detail may be included in an HRS or SRS using a lower paragraph header level than the driving system level requirements (for automatic tracing) or in a separate document section or appendix. Separate documents for this application are the Hardware or Software Design Descriptions (HDD, SDD, etc.). This is when design engineers determine what is needed for implementing subsystems and components for delivering the functions and performance and begin to develop the detailed drawings, schematics, and software modules for the described solutions.

Verification of these lower level “requirements” is informal and may be performed by the assigned design specialists (or their peers, if independence is desired).

As the PRD was developing, the project team built a preliminary system concept architecture diagram with major subsystem blocks that show internal and external connection. This concept architecture is revised during derivation of system level requirements into the various system and/or subsystem specifications (HRS and SRS).

With the system functions becoming known, a Hazard Analysis is begun as the first element in the project Risk Analysis portion of design validation. Previous hazard analyses are sources of potentially applicable hazards for the new products. Hazard Analyses should be compliant with ISO 14971, Medical Devices – Application of Risk Management to Medical Devices (2000), by using its hazard catalog organization. Also cite PRD requirements derived into the HRS/SRS (or the service/operations manual subsection or part number for caution or warning label and its physical location) where the corrective actions stated for abating the assessed risk level were driven (or implemented). These ideas are adapted from recommendations in (Jones, P., 2002). As stated, hazards for which risk abatement is mandatory are identified in the RVTM by the derived HRS or SRS requirements that will result in that abatement action. Abatement action is thereby traced to the verification procedure that confirms its system level requirement fulfillment.

Another risk analysis document, developed in parallel with the Hazard Analysis, is a Fault Tree Analysis (FTA) that begins with an Event of Serious Injury or Death and defines categories of equipment or process (or human action) faults that could result in that top event as logical OR gate inputs. Each category is subdivided into faults that could lead to an event in the category. The subdivision of faults continues until each subsystem or component either is below a logical AND gate with an associated crosscheck process or component (that also must fail to permit fault event causing the defined harm). Or, the fault is flagged as a single point failure item that must have adequate availability to support intended use of the device over its lifetime (plus a prudent margin).

When subsystems implementation is well defined, each is subjected to a bottom-up Failure Mode and Effects Analysis (FMEA) evaluation as the last element of the project Risk Analysis portion of its design validation. Each FTA identified single point failure must be included in an FMEA for evaluation and design input.

As the design is further refined for the hardware, design specialists translate subsystem concepts into mechanical drawings and electrical schematics. When design and fabrication

require external specialty firms, procurement specifications are developed. Because commercial off-the-shelf (COTS) components with second sources are preferred, selection of these items is made. The electrical documents include interconnect diagrams, electrical crate and/or rack diagrams indicating individual chassis locations, cables drawings, and the Interface Control Document (ICD), as well as new design schematics. The implementation requirements in the HDDs are updated to describe the developing designs, so they can become theory of operation descriptions that can accompany the drawings and schematics in the maintenance manual.

As a design is refined for software, design specialists assign architecture and graphical user interface concepts into modules and units of code. In limited cases, such as diagnostics for COTS equipment or reusable code from other recently developed systems, existing code may be purchased. Code development may be contracted to specialists in the design domain.

Software failure is “not working as expected.” In that sense, software applications reveal errors in design, or a modification, that were latent from the initial programming until triggering combination of conditions occurs. To assist determining areas to emphasize during verification testing that attempts to detect such problems, software can be evaluated with a form of FMEA.

**Note:** With Risk Analysis for medical devices as just described, project Risk Management differs substantially from that familiar to the classical Systems Engineers, where risk evaluation is of hazards to achieving the project cost and schedule goals and to fulfilling requirements for system technical performance (so human safety usually is a subsidiary measure of effectiveness).

**820.30 (d) Design output.** The definition for Design output in QSR 820.3 is “the results of a design effort at each phase and at the end of the total design effort. The finished design output is the basis for the device master record. The total finished design output consists of the device, its packaging and labeling, and the device master record.” Despite the association with the early development and the design review(s) implied by “each phase” in the first sentence of that definition, this subsection emphasizes a finished device: “Design output procedures shall contain or make reference to acceptance criteria and shall ensure that those design outputs that are essential for the proper functioning of the device are identified.”

In keeping with the above definition for Design output, many design inputs are outputs from the previous stages in the “total design effort.” Along with the device, total finished design output includes a device master record (DMR) that is associated closely with this subsection because it contains information necessary to replicate the device in its delivered configuration. QSR 820.181 lists DMR content as the following information (or as a reference to its location).

- (a) Device specifications, including drawings as well as component and software specifications;
- (b) Production process specifications and procedures;
- (c) Quality assurance procedures and specifications (esp. acceptance criteria);
- (d) Packaging and labeling specifications (more related to high volume items),
- (e) Installation, maintenance, and servicing procedures and methods.

As described in QSR 820.130, “packaging and shipping containers are ... to protect the device from alteration or damage ...” Labeling extends beyond ordinary meaning for identifiers and warnings affixed to equipment and packaging to include Maintenance and User/Operating Manuals because they are among the means to ensure that the device will be “safe and effective” each time it is used.

**820.30 (e) Design review.** The definition for Design review in QSR 820.3 is “a documented, comprehensive, systematic evaluation of a design to evaluate adequacy of the design requirements, to evaluate the capability of the design to meet these requirements, and to identify problems.”

Output of each phase of device development is subject to design review procedures. A System Requirements Review (SRR) ensures that the PRD responds to the CRD outputs for inputs accepted for implementing. The Preliminary Design Review (PDR) ensures that each HRS and SRS responds to the PRD outputs as its inputs. The hardware and software design requirements, which may be captured in the HRS and SRS or in separate design descriptions, detail how the design is to be implemented. Detailed drawings, schematics, and software module definitions are developed by the mechanical, electrical and software design specialists in parallel with initial requirements verification procedures development. A Critical Design Review (CDR) ensures that physical incarnation of the design(s) and installed software will fulfill their functional and performance requirements. Components are defined in preparation for procurement. A Production Readiness Review (PRR) ensures that the designs are suited for manufacture or purchase or contracting to an approved developer or supplier. User and Maintenance Manuals are developed from the design information as part of the labeling.

Each document produced as part of the design output is reviewed by project team members and corrected until its signatories approve its designation as a formally released item. Some documents are crucial to the design process and must be reviewed for their “final” release to enable advancing to the next phase in the project.

The Requirements Verification/Validation Trace Matrix/Report (RVTM) that was developed throughout the stages of the device’s design and manufacturing, provides a map of HRS and SRS requirements derivation from PRD requirements to their subsequent verification procedures. The trace assists design engineers in ensuring that correct design output results from the design input and that the device will fulfill its requirements when installed, reducing quantity and scope of the PDR and CDR Action Items.

**820.30 (f) Design verification.** The definition for Verification in QSR 820.3 is “confirmation by examination and provision of objective evidence that specified requirements have been fulfilled.” Verification is showing that the medical device was built correctly. The design is verified when fulfillment of every derived requirement is confirmed by performing HRS and SRS verification procedure(s) and reporting the results. (Assuming deficiencies correction and regression testing that passed, of course.) The verification procedures, results, and reports “shall be reviewed and approved by designated individuals.”

The RVTM also identifies the verification means to be employed in the procedure(s) as: instrumented test, demonstration, inspection, or analysis. RVTM mapping assists designers in developing the comprehensive set of informal verification test cases that will confirm (or deny) that the subsystem will fulfill its implementation/ design requirements (as included within HRS/SRS or as allocated into a separate HDD/SDD).

The RVTM trace similarly assists Systems Engineers in developing comprehensive sets of formal verification test cases to confirm (or deny) that the implemented and installed system fulfills its functional and performance requirements as set forth in HRS(s) and SRS(s). When identified Verification Procedures are near readiness for release, the RVTM is updated to indicate the location therein of each test case for verifying the associated requirement.

Each system level Verification Procedure identified in the RVTM references its Verification Report as a sibling document. Each Verification Report has a one-to-one section correspondence with the test cases in its sibling Verification Procedure. Thus, each hazard requiring assessed risk level abatement in the Hazard Analysis or FMEA is traced to confirmation of its implementation. This provides auditable evidence of compliance with Risk Analysis as well as the Requirements Management aspects of QSR provisions for design controls.

**820.30 (g) Design validation.** The definition for Validation in QSR 820.3 is “establishing by objective evidence that device specifications conform with user needs and intended use(s).” It is confirmation that the correct medical device was built; that the device will fulfill the customer clinical and user inputs to requirements as fielded.

Functional and performance requirements in the PRD are derived from customer inputs to requirements (the CRD). Because most PRD requirements are derived into system level requirements in a subsidiary HRS or SRS, and thence into the implementation/design requirements, indirect verification is the vast majority of the validation. Remainder of validation involves confirming fulfillment of system design qualification requirements that cannot use simple, one-time measurements because a cumulative assessment must be developed. For example, a number of production units may undergo accelerated life tests.

Validation method examples are deliberate use of erroneous inputs to user interfaces, accelerated life or use tests, electromagnetic compatibility testing, environmental stress screening, showing conformance to domestic and international standards, and other such means for determining system suitability for its intended use(s). For lengthy predicted device use periods and other areas where test, demonstration, and inspection are not directly applicable, analysis becomes the only practical validation method.

The RVTM uses the column that identifies verification means to similarly identify validation means to be employed in that procedure. Also, the RVTM trace assists Systems Engineers in developing formal validation test cases that will confirm (or deny) that the implemented and installed system will fulfill its design qualification requirements. When identified Validation Procedures are standard or near release, the RVTM is updated to indicate location therein of each test case for validating the associated design qualification requirement.

Each project unique Validation Procedure identified in the RVTM references its Validation Report as a sibling document. Validation Procedures often are broadly conceived standards that are common to all projects, so references to their project unique Validation Reports can accompany identification procedures in the RVTM. This approach to validation also provides auditable evidence of compliance with the applicable QSR provisions for design controls.

**820.30 (h) Design transfer.** Here, emphasis is on ensuring “that the device design is correctly translated into production specifications.” Depth and breadth of each translation depends entirely on which permutation of a make or buy decision applies to the system, subsystem, or component to be produced. Device design may be contracted to an external entity that performs or arranges for fabrication and supply of design drawings and schematics in accordance with company standards for their inclusion in the DMR. A recommended approach for the design transfer process is to go beyond ensuring auditable compliance by including Manufacturing Engineering early in the design process such that ease of fabrication and assembly join maintainability as a concern of the design specialists.

**820.30 (i) Design changes.** No substantive device design project will proceed from customer inputs validation without at least minor design changes that may affect finished devices. A manufacturer must provide “procedures for the identification, documentation, validation, or where appropriate verification, review, and approval of design changes before their implementation.” Released documentation that is revised due to design change must be reviewed by their identified signatories and approved.

Whenever a requirement above the implementation level is affected, the described RVTM becomes invaluable. Locating that requirement enables determining if one or more driving or responding requirement(s) also must be revised. Further, need for evaluation of effect upon implementation necessary to reduce the assessed risk level for an FMEA fault or Hazard Analysis item is indicated. Requirements Management and attention to Risk are maintained, as is the auditable evidence of compliance with QSR provisions for design controls.

**820.30 (j) Design history file.** The definition for Design History File in QSR 820.3 is “a compilation of records which describes the design history of a finished device.” This subsection of QSR provisions for design controls states that “The DHF shall contain or reference the records necessary to demonstrate that the design was developed in accordance with the approved design plan and the requirements of this part.”

Because “this part” means the entire QSR, work requested of and decisions made by those that impact development and production of a medical device through a project are pertinent for capture and retention in the DHF. This can affect any employee, as well as members of the project team and management representatives. Regardless, this provision shows value of clear minutes of meetings, especially regarding decisions and action items, in words that will be understood by those persons not in attendance or not extremely familiar with the topics.

With pervasive use of email for communications, maximizing automatic capture of the project decisions and action items is enabled by establishing one company network email alias for each development project DHF and instructing the appropriate use by persons accomplishing any work on that project. The traditional Memo to File is simplified in its execution and vastly improved for project-wide team member notification.

## **IPPT Design Controls Compliance Tools**

**Document Templates.** The IPPT supporting toolset providing greatest increase in effectiveness and efficiency of development project teams is integrated document templates that standardize their content and interrelationships. (Data Item Descriptions are military standard equivalents.) Most documents named during exposition of QSR provisions for Design Controls may be built from a tailored template. Because they expand upon predefined outline formats of the named document types, authors are assisted in rapid creation of design controls compliant documents.

A Project Management Plan template provides detailed instructions for tailoring the project work to a reduced scope and scale as well as providing the worst case of full-scale project plan content. Document templates for requirements specifications contain detailed guidance, in early (sub)sections, which provide project information at an appropriate breadth and depth for the PRD and HRS/SRS (with inclusion of HDD/SDD implementation design “requirements” when desired). The instructions show formal specification language sentence structure along with requirements writing rules, such as those set forth in (Jones, J., 2002). Templates for ancillary documents also instruct providing the records necessary for fulfilling several internal, customer,

and regulatory objectives beyond required QSR compliance, such as showing adherence to specified document standards. Thus, even initial draft versions of the work products provide auditable Design Controls compliance support.

Predefined content descriptions help ensure that everything will be in its expected location, so project team members can learn quickly where information of interest should be placed. This standardization is especially helpful when upgrading poorly documented legacy systems that require extensive reverse engineering and capture of sparsely distributed, poorly written, and untraced requirements information.

Detailed guidance in document templates, describing what belongs therein, enables all reviewers to evaluate likely adequacy of provided content – even if outside their domains of expertise. (Similar to familiar Data Item Descriptions, detailed content guidance helps regulatory and quality assurance personnel tasked to support the medical device development projects.)

**Requirements Management Tools.** Essentially, commercial requirements management tools are a database program that imports requirements from specification documents and assigns a project unique identifier (PUI) to each requirement. Requirements in one document are assigned PUI to PUI linkages to requirements in other documents to establish source driver and responder relationships. A major feature of requirements management tools is automatic notification of which other requirement(s) possibly are affected (based on their PUIs linking) by revision to a requirement. Support for a custom report, such as the described RVTM, is provided to some extent by most requirements management tools.

## **Project Management Support for Estimating/Reporting**

**Document Templates.** An integrated set of document templates greatly helps project planning when estimating how much time will be required to develop and review each project document. Because the documents preparation from embedded instructions is closer to “right the first time,” the completed design information is available sooner and (when based on prior experience with developing similar documents and earned value accounting of tasks) fewer project schedule estimates will be greatly exceeded.

**Traditional Project Status Estimates.** Traditional status taking is to assign a percent complete value for association with the hours expended relative to the hours bid for the task. For documents, an arbitrary percent complete is assigned to developing each of the initial outline format, the first draft completion proportion, the first submittal for general team review, and to the final release review. Estimates of percent complete for each document development task are improved with the templates guidance for content.

**Project Status Metrics Using Actuals.** Alone, those stated benefits of document templates argue well for their adaptation and adoption wherever they can be applied. But how about percent complete status of the overall project, with respect to the Requirements Management (or end to end development phases) as represented by the documents development? How about the percent complete status for the verification and validation tasks? A benefit of the RVTM is support for accurate percent complete status metrics based on actual task accomplishments for each requirement in the system level documents, as also is described in (Jones, J, 2002).

## Conclusions

The FDA Quality System Regulation is essentially a medical device development process specification and thereby clearly is within a classical Systems Engineering skillset. The QSR requires executive responsibility for a quality policy and quality system applied by well-trained staff of adequate size with procedures and instructions that are enforced within the development organization and independently audited for compliance. The QSR is concerned about product development, manufacturing, and service processes, with an emphasis on auditable records.

Experienced Systems Engineers should feel confidence in applicability of the fundamental methods to all aspects of medical devices development. The differences in Risk Management for medical devices from the classical concepts of project cost, schedule, and technical risks are easily learned. Thus, using the IPPT approach to introduce the familiar processes recommended in this paper can lead to automating compliance with the QSR provisions for design controls.

Fortunately, although it is easiest to begin applying them at the start of a project, individual methods and templates can be applied separately as appropriate to the project situation. These examples lead to tentative localized acceptance and then assimilation of the improved processes, which paves the way to quicker and more general acceptance of the next improvements.

When the last few recommended improvements are to be installed, it will be time to evaluate the many potential improvements to the Systems Engineering processes for applicability to the planned device development projects.

## References

- FDA 21 CFR 807.87 “Information required in a premarket notification submission”, April 2005  
“Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices”, FDA Center for Devices and Radiological Health, Office of Device Evaluation, May 11, 2005
- FDA 21 CFR 820 Medical Device Quality System Regulation, 1996 (Revised 31 March 2006)
- ISO 14971, Medical Devices – Application of Risk Management to Medical Devices, 2000
- Jones, James, “Verification ‘Auditability’ can be ‘Free’”, INCOSE Proceedings, July 2002
- Jones, P., Jorgens, J., Taylor, A., and Weber, M., “Risk Management in the Design of Medical Device Software Systems”, AAMI Proceedings, February 2002

## BIOGRAPHY

**James H. Jones** is Owner/Principal of ODDSCO (Optants Documented Decision Support Company), a consulting business providing practitioner level seminars and educational material on Project and System Engineering processes that are adapted from a Mil-Std approach to suit commercial new product developers.

He has a B.S. in Business Administration and an M.S. in Industrial and Systems Engineering.

He acquired skills in comprehensive, rigorous requirements management for embedded systems during work for defense corporations. His experience applying Systems Engineering to medical device new product development began with an IV infusion pumps manufacturer and now includes development of upgrades to a high throughput proton beam treatment system.