ASQ
The Global Voice of Quality™

Reliability
DIVISION

软件控制的电子机械系统可靠性

杜允健
http://sites.google.com/site/resiliencereliability/

Software controlled Electro-Mechanical Systems Reliability

by David Tu

Reliability
DIVISION

专项 SPECIALTIES
可靠性工程 Reliability Engineering
可靠性计划，测试计划和平均无故障时间预测
Reliability Program, Test plans, Mean Time Between Failures prediction
法规遵从 Regulatory Compliance
FDA, FCC, Telecom, Wi-Fi, Bluetooth, UL and CE
质量保证 Quality Assurance
资格，验证/确认，全球制造商/供应商/客户
Qualification, Verification/Validation, global manufacturers/suppliers/ customers

教育/证书 EDUCATION/CERTIFICATES
工业工程学士，中原大学，台湾
Bachelor of Industrial Engineering, Chung Yuan Christian University, Taiwan
电机工程硕士，纽约石溪大学，美国
Master of Electrical Engineering, Stony Brook University, New York, USA
认证可靠性工程师和质量工程师，美国质量协会
Certified Reliability Engineer, Quality Engineer and Quality Auditor by American Society of Quality

ASQ
The Global Voice of Quality™

Reliability
DIVISION

议程 AGENDA

- 简介 Introduction
- 政府机构 Government agencies
- 标准和准则 Standards and Guidelines
- 可靠性模型和功能 Reliability model and function
- 个案研究 Case Study
- 结论与探讨 Conclusion & Discussing

ASQ
The Global Voice of Quality™

Reliability
DIVISION

目标 **Goal**
开发可靠的软件控制的电子机械系统。
Develop reliable software controlled electronic mechanical systems.

方法 **Approach**
利用机构, 法规和准则来支持可靠性工程，而不是当成障碍。
Utilize agencies and regulations as supportive guidelines instead of obstacles.

程序 **Procedures**
1) 确定政府机构 Identify government agencies
2)了解法规和标准 Understand regulations and standards
3) 确定活动和制定程序 Identify activities and develop procedures
4) 开发可靠性计划，平均故障时间分析和测试计划
Develop Reliability Program, MTBF analysis and test plan
5) 进行合作的分析和测试 Collaborate analysis and test
6) 审查结果 Review results
7) 执行根本原因分析的结果 Perform root cause analysis for findings
8) 进行合作和实施整改措施 Collaborate and implement corrective actions
9) 写报告 Write reports
10) 监控，提高产品的可靠性在产品寿命周期期间
Monitor and improve reliability during product life cycle

ASQ
The Global Voice of Quality

Reliability
DIVISION

政府机构 GOVERNMENT AGENCIES

- 美国食品和药物管理局
  Food and Drug Administration FDA http://www.fda.gov/
  Develop and enforce compliance for safety, effectiveness and reliability. FDA does not develop engineering specifications and standards for Medical Devices. FDA regulations are free for reference.

- 国际电工委员会
  International Electrotechnical Commission http://www.iec.ch/
  Develop regulatory and engineering safety specifications and standards for medical device safety. Medical devices at European market requires CE marking. It is a self declaration process with the compliance of all applicable standards. IEC standards are available for purchase online.

美国食品和药物管理局
Food and Drug Administration FDA

医疗器械;现行良好生产规范, 最终规则

21 CFR Parts 808, 812, and 820 Medical Devices; Current Good Manufacturing Practice (CGMP) Final Rules Monday, October 7, 1996 Page 2

SUPPLEMENTARY INFORMATION: I. Background (Design controls vs. Production controls)

"Specifically, in January 1990, FDA published the results of an evaluation of device recalls that occurred from October 1983 through September 1989, in a report entitled "Device Recalls: A Study of Quality Problems". FDA found that approximately 44 percent of the quality problems that led to voluntary recall actions during this 6-year period were attributed to errors or deficiencies that were designed into particular devices and may have been prevented by adequate design controls."

"A subsequent study of software-related recalls for the period of fiscal year 1983 through 1991 indicated that over **90 percent** of all software related device failures were due to design related errors, generally, the failure to validate software prior to routine production."

Note: FDA makes CGMP as a regulation for companies to comply with.

ASQ
The Global Voice of Quality™

Reliability
DIVISION

美国食品和药物管理局
Food and Drug Administration FDA

21 CFR Parts 808, 812, and 820 Medical Devices; Current Good Manufacturing Practice (CGMP) Final Rule
A. General Provisions, page 55, § 820.3 Definitions

(b) *Complaint* means any written, electronic, or oral communication that alleges deficiencies related to the identity, quality, durability, reliability, safety, effectiveness, or performance of a device after it is released for distribution.

ASQ
The Global Voice of Quality™

Reliability
DIVISION

美国食品和药物管理局 软件验证的一般原则;
已确认的工业指南和工作人员

General Principles of Software Validation;
Final Guidance for Industry and FDA Staff

Document issued on: January 11, 2002

2.4. Regulatory requirements for software validation

The FDA's analysis of 3140 medical device recalls conducted between 1992 and 1998 reveals That 242 of them (7.7%) are attributable to software failures. Of those software related recalls, 192 (or 79%) were caused by software defects that were introduced when changes were made to the software after its initial production and distribution. Software validation and other related good software engineering practices discussed in this guidance are a principal means of avoiding such defects and resultant recalls.

4.4. Software life cycle

Software validation takes place within the environment of an established software life cycle. The software life cycle contains software engineering tasks and documentation necessary to support the software validation effort. In addition, the software life cycle contains specific verification and Validation tasks that are appropriate for the intended use of the software. This guidance does not recommend any particular life cycle models - only that they should be selected and used for a Software Development project.

美国食品和药物管理局 软件验证的一般原则;
已确认的工业指南和工作人员
General Principles of Software Validation;
Final Guidance for Industry and FDA Staff

Document issued on: January 11, 2002

3.3. SOFTWARE IS DIFFERENT FROM HARDWARE

While software shares many of the same engineering tasks as hardware, it has some very Important differences. For example:

- One of the most significant features of software is branching, i.e., the ability to execute alternative series of commands, based on differing inputs. This feature is a major contributing factor for another characteristic of software – its complexity. Even short programs can be very complex and difficult to fully understand.

- Typically, testing alone cannot fully verify that software is complete and correct. In addition to testing, other verification techniques and a structured and documented development process should be combined to ensure a comprehensive validation approach.

- Unlike hardware, software is not a physical entity and does not wear out. In fact, software may improve with age, as latent defects are discovered and removed. However, as software is constantly updated and changed, such improvements are sometimes countered by new defects introduced into the software during the change.

- Unlike some hardware failures, software failures occur without advanced warning. The software's branching that allows it to follow differing paths during execution, may hide some latent defects until long after a software product has been introduced into the marketplace.

美国食品和药物管理局 软件验证的一般原则;已确认的工业指南和工作人员

General Principles of Software Validation; Final Guidance for Industry and FDA Staff

Document issued on: January 11, 2002

- Another related characteristic of software is the speed and ease with which it can be changed. This factor can cause both software and non-software professionals to believe that software problems can be corrected easily. Combined with a lack of understanding of software, it can lead managers to believe that tightly controlled engineering is not needed as much for software as it is for hardware. In fact, the opposite is true. Because of its complexity, the development process for software should be even more tightly controlled than for hardware, in order to prevent problems that cannot be easily detected later in the development process.

- Seemingly insignificant changes in software code can create unexpected and very significant problems elsewhere in the software program. The software development process should be sufficiently well planned, controlled, and documented to detect and correct unexpected results from software changes.

美国食品和药物管理局 软件验证的一般原则;
已确认的工业指南和工作人员
General Principles of Software Validation;
Final Guidance for Industry and FDA Staff

Document issued on: January 11, 2002

- Given the high demand for software professionals and the highly mobile workforce, the software personnel who make maintenance changes to software may not have been involved in the original software development. Therefore, accurate and thorough documentation is essential.

- Historically, software components have not been as frequently standardized and interchangeable as hardware components. However, medical device software developers are beginning to use component-based development tools and techniques. Object-oriented methodologies and the use of off-the-shelf software components hold promise for faster and less expensive software development. However, component-based approaches require very careful attention during integration. Prior to integration, time is needed to fully define and develop reusable software code and to fully understand the behavior of off-the-shelf components.

For these and other reasons, software engineering needs an even greater level of Managerial scrutiny and control than does hardware engineering.

美国食品和药物管理局

III. APPLICATION OF DESIGN CONTROLS

Design controls may be applied to any product development process. The simple example shown in Figure 1 illustrates the influence of design controls on a design process.

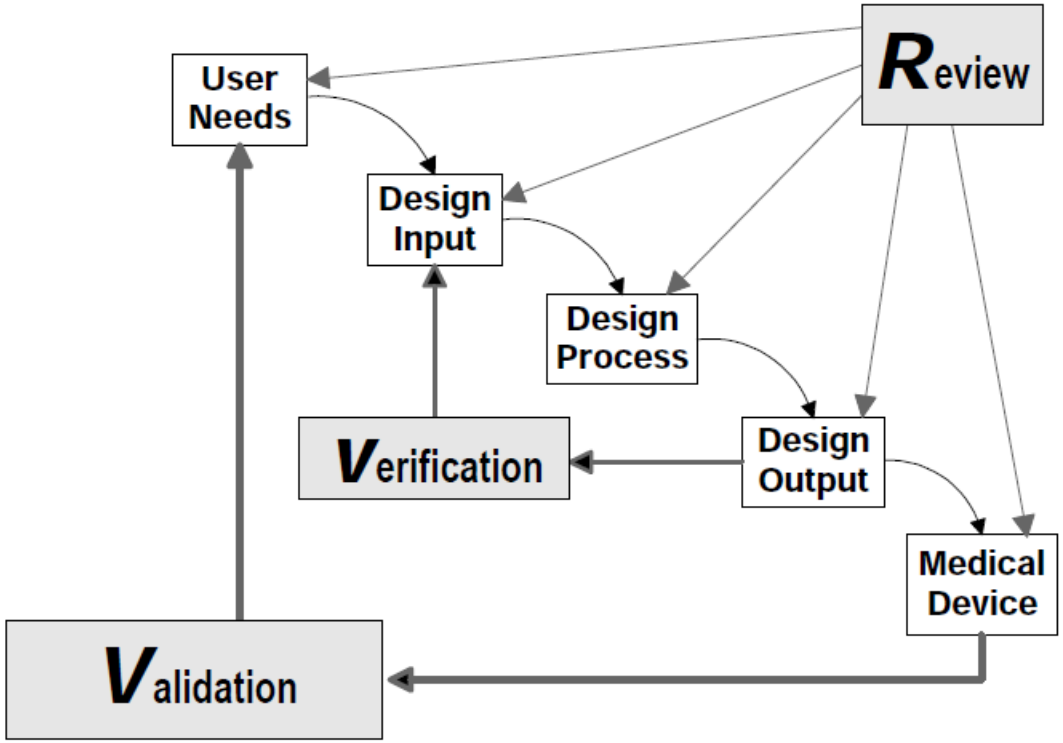
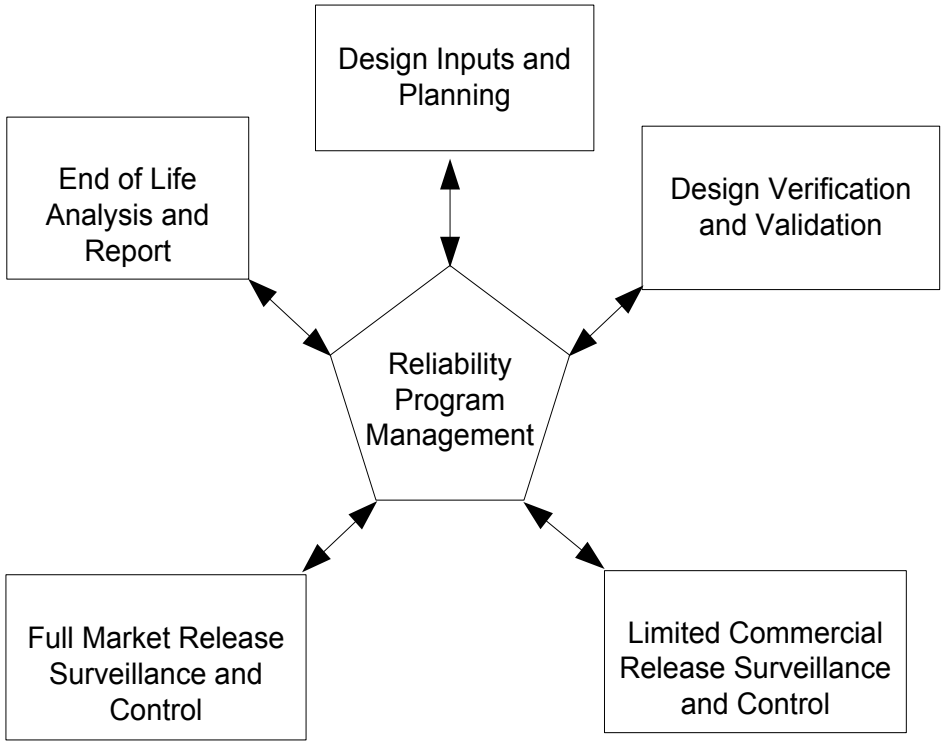


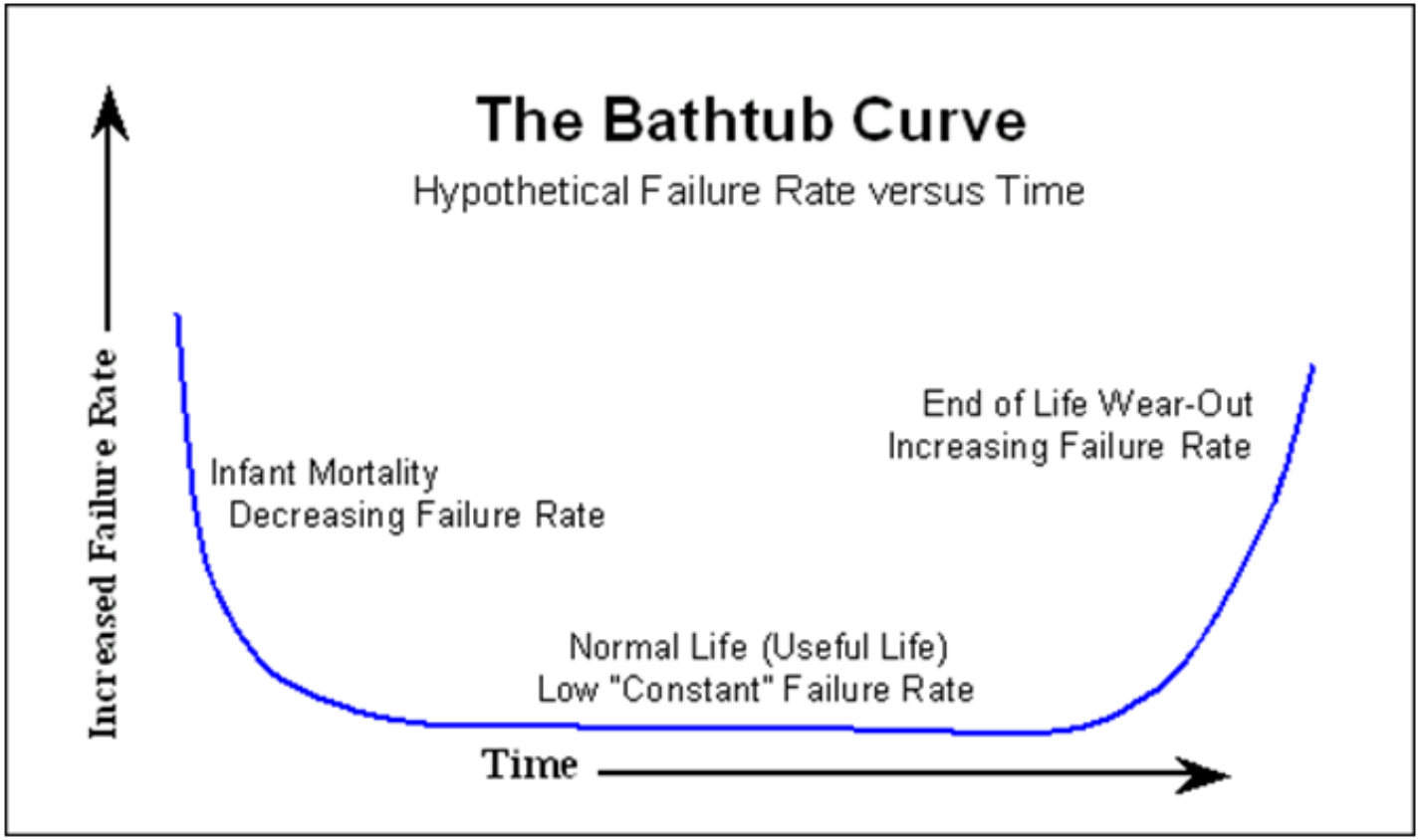
Figure 1 – Application of Design Controls to Waterfall Design Process (figure used with permission of Medical Devices Bureau, Health Canada)

可靠性模型和功能 Reliability model and function

A Reliability Program detects, identifies and mitigates the risks of product defects.



可靠性模型 Reliability model



可靠性建模与假设 Reliability Modeling with assumptions

机械 Mechanical

机械可靠性被假定为正态分布。
Mechanical reliability is assumed to be a Normal distribution.

硬件（电子系统，子系统，组件，连接器及印刷电路板等）
Hardware (Electronic systems, subsystems, components, connectors and PCBA etc.)
可靠性函数被假定为一指数分布。它的平均值（平均故障时间) 为卡方分布。包括婴儿死亡率和磨损程度高失败率时期。
Reliability function is assumed to be an Exponential distribution. Its Mean (MTBF) is a Chi-Square distribution. Include infant mortality and wear-out high failure rate periods.

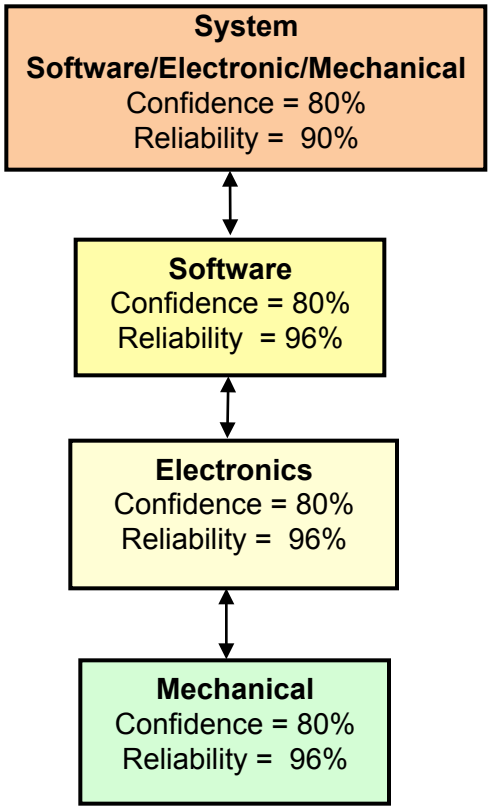
软件 Software

软件可靠性函数被假定为一个离散均匀分布, 具有恒定故障率。
Software reliability function is assumed to be a discrete uniform distribution with constant failure rates.

系统 System

系统可靠性函数被假定为正常, 指数和离散均匀分布的组合。机械的平均故障时间是一个正态分布的平均值。硬件和软件的平均故障时间是卡方分布。系统有婴儿死亡率和耗损故障率较高时期。软件故障率将会提升系统故障率浴缸曲线。系统结合三个子系统需要更多的研究。应当使用模型效仿的物理寿命试验，而不是数学的模型。
System Reliability function is assumed to be a combination of Normal, Exponential and discrete uniform distribution. Mechanical MTBF is the mean of a normal distribution. Hardware and Software MTBF is a Chi-Square distribution. System has higher failure rates at infant mortality and wear-out periods. Software failure rate elevates System failure rate Bathtub curve. The combination of three sub-systems need more study. Should be modeled by life tests, not mathematical models.

可靠性模型图 Reliability Modeling Diagram



- Allocate 7.7% x 5 factor to estimated failure rate for software reliability
- Mechanical part has the highest failure rate allocation by author's experience
- Field return database provides realistic pictures

Reliability DIVISION

案例研究 CASE STUDY
前生产 Pre Production Release

产品名称：心脏起搏器讯问设备
PRODUCT: Pacemaker Interrogating Equipment

进行的测试 Tests Performed

- 性能测试(各种起搏器) Performance tests (Various Pacemakers)
- 安全（电磁兼容性及安全规例，CE标志）
  Safety (Electromagnetic Compatibility and Safety per CE marking regulation)
- 环境试验（振动，温度，湿度）
  Environmental tests (Vibration, Temperature, Humidity)
- 平均故障时间预测
  MTBF Prediction (SR-332)
- 风险分析
  Risk Analysis
- 失效模式影响及危害性分析
  Failure Mode Effects and Criticality Analysis
- Submit and obtain FDA approval

ASQ
The Global Voice of Quality™

Reliability
DIVISION

案例研究 CASE STUDY
产品发布 Production Release

产品：起搏器讯问设备 **PRODUCT: Pacemaker Interrogating Equipment**

- 供应商监督 **Supplier surveillance**
  - 供应商质量改进 Supplier yield improvement
  - 供应商最终检验和试验控制，发展和实施
    Supplier final inspection and test control, development and implementation
- 生产质量保证 **Production quality assurance**
  - 进料检验和试验开发和实施
    Incoming inspection and test development and implementation
  - 生产线检验和试验开发和实施
    Production line inspection and test development and implementation
- 工程更新和升级控制 **Engineering update and upgrade controls**
  - 审查，重新测试，重新核实和控制变更
    Review, re-test, re-verify and control changes
- 返回故障管理 **Field returns management**
  - 根本原因分析 Root Cause Analysis
  - 工程所有已确定故障模式
    Engineering for all identified failures
  - Re-verification and implement solutions
  - Document all findings and corrective actions

纠正行动证实发现不合格产品

- 重新验证和实施解决方案
- 记录所有结果及整改措施

案例研究 CASE STUDY
产品名称：心脏起搏器讯问设备
PRODUCT: Pacemaker Interrogating Equipment
产品生命周期结束分析
End of Product Life Cycle Analysis

- 文档 Documentation
  - 设备型号，序列号和纠正措施
  - Equipment models, serial numbers and corrective actions
  - 什么时候，谁，在哪里，为什么和怎样
  - What, when, who, where, why and how

- 工程检讨
  - 无缺陷退货的数据库分析
    Failure Return data base analysis

ASQ
The Global Voice of Quality™

Reliability
DIVISION

概要

- 笔者的经验证实了**FDA**的故障率指导
- 符合**FDA**良好生产规范，**IEC60601 - 1**安全, 风险分析**ISO14971**（**EN1441**及**IEC60601 - 1 – 4**
- 进行风险分析，失效模式影响及危害性分析，平均故障时间预测，加速寿命试验，环境试验，
  检验测试及安全符合性测试
- 分析测试结果，确认根本原因和纠正协作行动

SUMMARY

- Author confirms FDA failure rate guidance by experience
- Comply with FDA Good Manufacturing Practice, IEC60601-1 Safety, Risk Analysis per ISO14971(EN1441) & IEC60601-1-4
- Perform Risk Analysis, Failure Mode Effects and Criticality Analysis, MTBF prediction, Accelerated Life Tests, Environmental tests, Validation tests & Safety compliance tests
- Analyze test results, confirm root causes and collaborate corrective actions