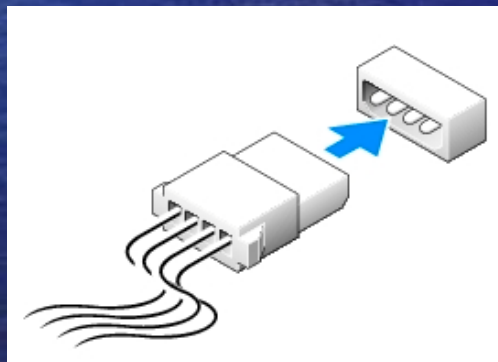


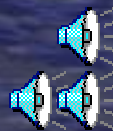
The Convergence of Software in the Medical Device Industry



Joseph Azary

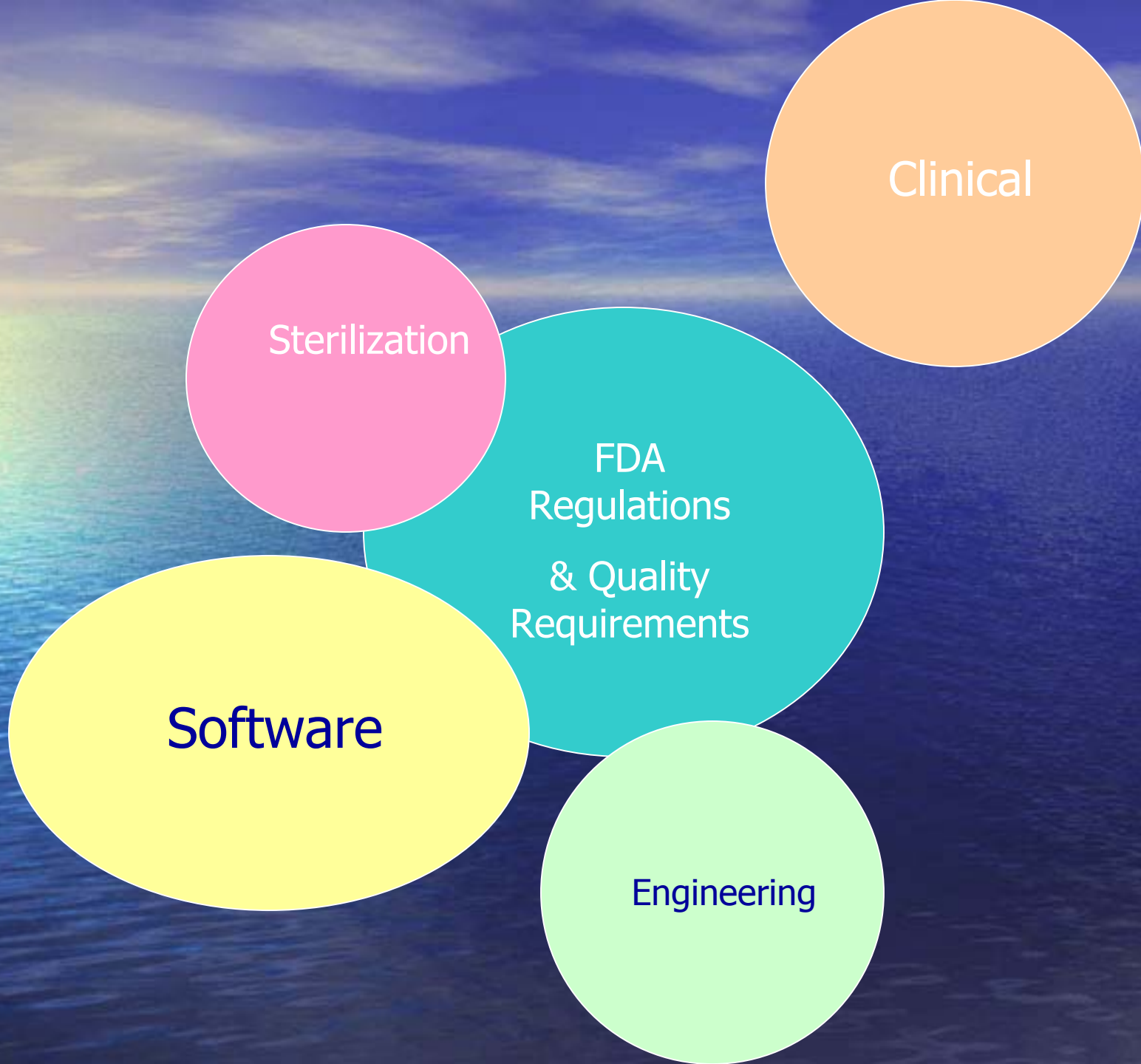
203-944-9320

Info@azarytech.com





FDA
Regulations
& Quality
Requirements



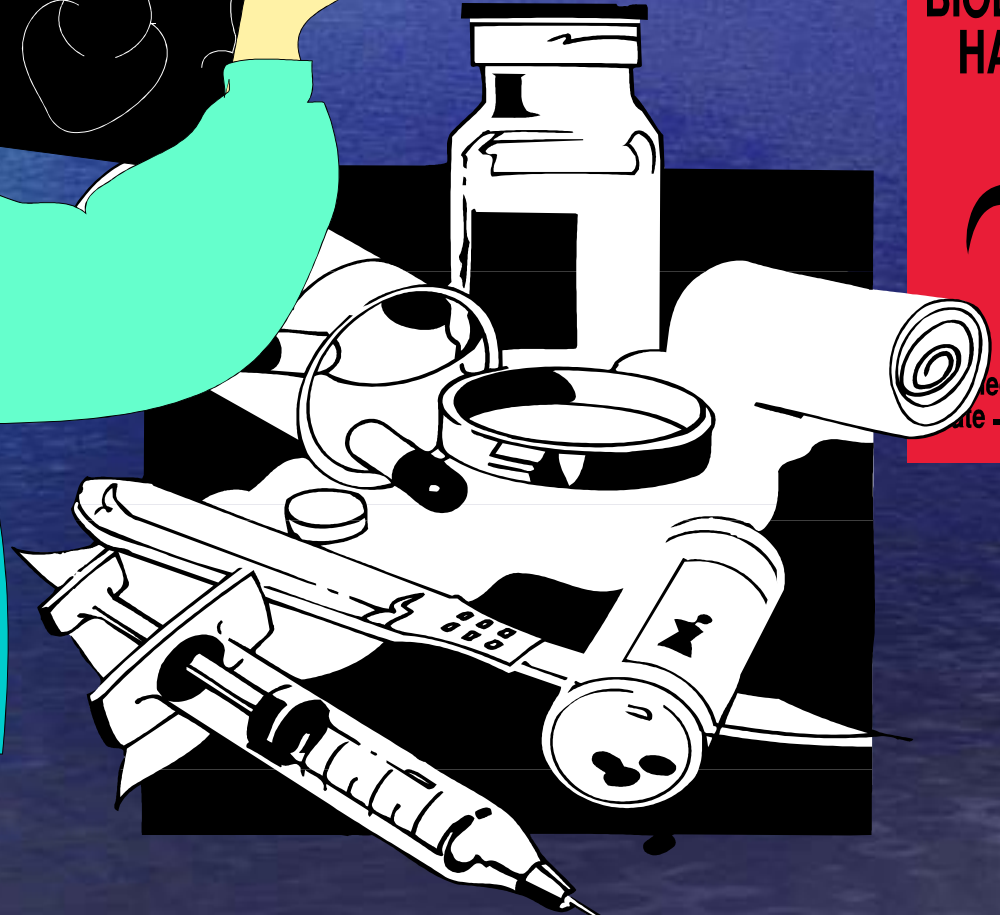
Clinical

Sterilization

FDA
Regulations
& Quality
Requirements

Software

Engineering



**CAUTION
BIOLOGICAL
HAZARD**



ed By _____
ate _____

A red rectangular warning sign with the text "CAUTION BIOLOGICAL HAZARD" in bold black letters. Below the text is a black biohazard symbol. At the bottom, there are two lines of text: "ed By _____" and "ate _____".

Medical Device Definition

An Instrument, Apparatus, Implement, Machine, Contrivance, Implant, In Vitro Reagent, or other similar or related article, including any component, part, or accessory which has the following characteristics:

- Is recognized by USP or National Formulary
- Intended for use in diagnosis of disease or other conditions or in the cure, mitigation, treatment, or prevention of disease
- Is intended to affect the structure or any function of the body
- Achieves its primary intended purpose through physical action, and not chemical or metabolic action.



Nanotechnology

- Biochips
- Surgery Nanotechnology
- Implantable BioMEMS
- Surface Modification
- Nanosystems for Drug Delivery
- Point-of-Care Diagnostic
- Hybrid Bio/Artificial
- Nanoprobes



Telemedicine

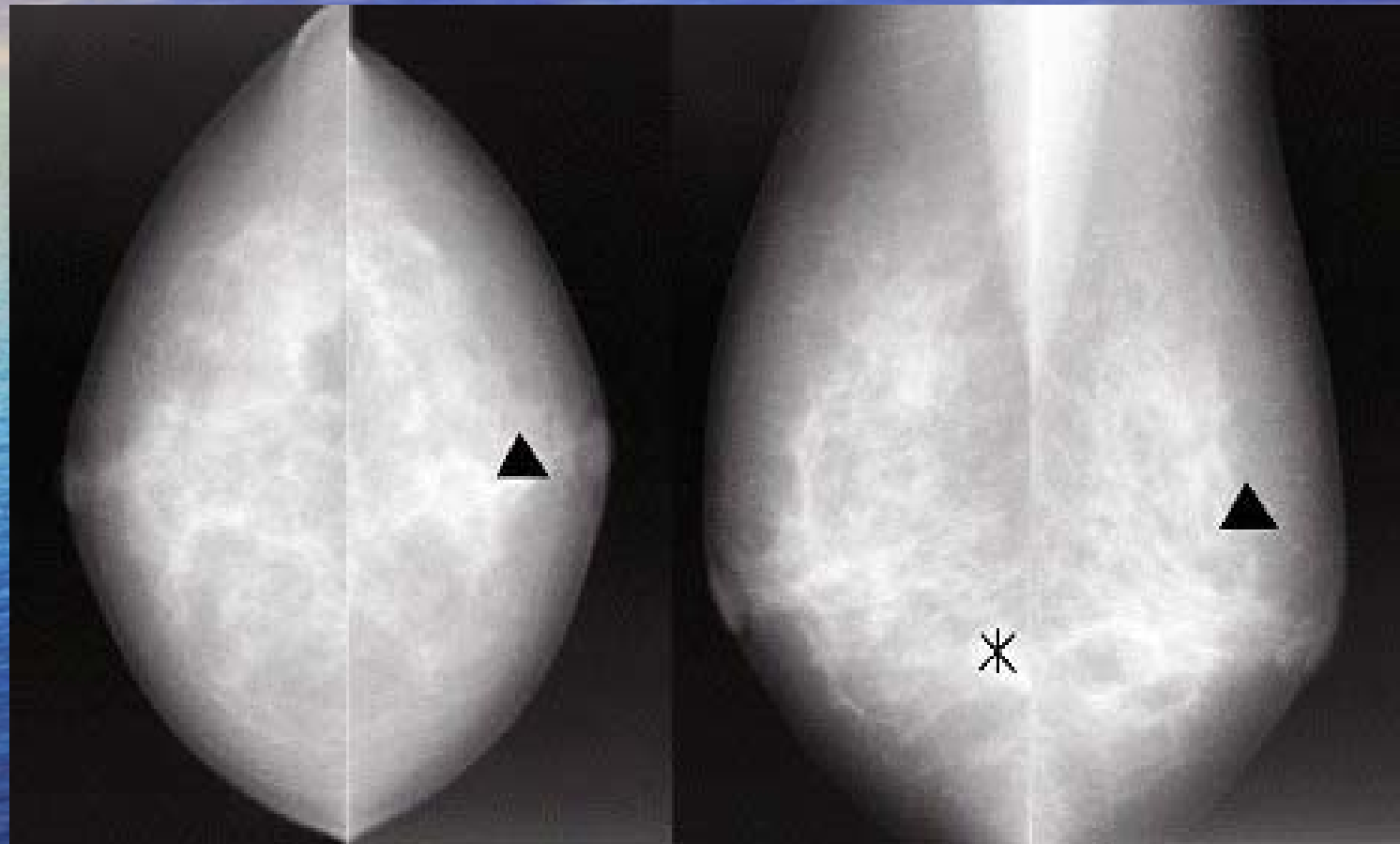


Remote Robotic Surgical System



Robotic Revolution - Device works wonder in prostate cancer surgery.
New York Daily News [read more](#)

Computed Aided Diagnosis



Software Controlled People



Medical Device Industry Facts

- Global Market of \$169 Billion
- U.S. consumes >40% of medical devices in world
- Steady annual rate of growth (7%)
- 70% have <50 employees
- 25,905 device manufacturers in U.S.
- Aging Population
- **High Tech**

North East

- Massachusetts – 686
- New York - 842
- Connecticut – 298
- Rhode Island – 73
- New Jersey – 440

*Manufacturers (not including specification developers or contract sterilizers – source FDA DSMA)

Trends in Device Industry

- Aging Population
 - By 2020 53.7 million people over 65
- Chronic Illness
- Reimbursement
- Lifestyle
 - >8 million cosmetic surgeries in 2000
- Reuse of Single Use Devices

Trends (continued)

- Group Purchasing Practices
- Outpatient Treatment
- Telemedicine
- Regulatory / Legal
- Moving devices into new areas
 - Drug coated devices
 - Artificial organs
 - Nanotechnology

Regulated Industry



Health Santé
Canada Canada



- Heavily Regulated by FDA, as well as ministries of health around the world
- European Medical Device Directives
- Canadian Medical Device Bureau

Harmonization

- In 1996 FDA harmonized medical device GMPs (Good Manufacturing Practices) with ISO 9001:1994.
- Facilitate compliance for medical device companies.
- Facilitate global harmonization.

What Is GMP

- GMP stands for **G**ood **M**anufacturing **P**ractices

Food & Drug Administration

- FDA is responsible for protecting public health by regulating products such as:
 - Medicine / drugs
 - Blood supply
 - Medical devices
 - Food
 - Cosmetics



History of GMPs

- 1905 Food and Drug Act
- 1962 Drug Amendments
- 1982 Tamper Resistant Packaging
- 1985 AIDS Testing for blood supply

History of GMPs

+++++



WHITE EAGLE
INDIAN
RATTLE-SNAKE OIL
Will Cure
Any Kind of
PAIN

PRICE, 50 CENTS.
ST. LOUIS, MO.

+++++



Dr. Mixer's Condition
After Cured by
his Cancer and Scrofula Syruu.

DRS. MIXER,
SOLE MANUFACTURERS
AND PROPRIETORS OF

SPECIAL TREATMENT
GIVEN

MIXER'S CANCER
AND
SCROFULA SYRUP

Cancer, Tumors,
Erysipelas,
Abscesses, Ulcers,
Fever Sores, Goiter,
Catarrh, Salt Rheum,
Scald Head, Piles,
Rheumatism,
and ALL BLOOD DISEASES.

The World Renowned
BLOOD PURIFIER.

ESTABLISHED 1862



DR. CLIAS. W. MIXER,
GEN'L MANAGER

Not a Physician.

Ex-Bard executives sentenced

Three given 18 months in heart catheter case

By Jennifer S. Lee
GLOBE CORRESPONDENT

In what prosecutors term a significant judicial statement about individual responsibility in corporate wrongdoing, three former executives of medical device manufacturer C.R. Bard were sentenced yesterday to 18 months in prison, the maximum sentence allowed under federal guidelines, for their roles in conspiring to hide potentially deadly flaws in heart catheters.

Former Bard executive vice president David Prigmore; John Cvinar, former president of Bard's Billerica-based USCI division; and former USCI vice president Lee Leichter were convicted last August following an eight-week jury trial for conspiring to defraud the US Food and Drug Administration. The execution of the sentences were stayed pending appeal.

The Murray Hill, N.J.-based company, one of the largest health-care device manufacturers in the country, had pleaded guilty to \$91 charges and paid a fine of \$61 million in 1998 — at the time the largest amount ever paid in a health-care fraud case.

The men were charged with making false statements to the FDA on the reliability of the heart catheters, devices often used in place of bypass surgery to clear clogged arteries. Malfunctioning or misused catheters can clog up the blood vessels they

are supposed to clear, causing heart failure.

Two deaths have occurred in operations involving malfunctioning Bard catheters, though, no causal link with the men's conspiracy has been established in court.

US District Court Judge Joseph L. Tauro called the relative severity of the sentence "a wake-up call" to corporate board rooms, saying executives traditionally have not been assigned personal responsibility in the actions of the companies they run. He pointed out that the men were not evil, and in fact were exemplary family men and community members.

"From this district, this court, this setting, it was a very significant sentence," said James B. Farmer, criminal division chief in the US attorney's Boston office. "It was clearly a sentence with a judicially intended message," he said. The trial was presented by assistant US attorneys Michael K. Loucks and Stephen A. Higginson, and Kay Cook, associate counsel for the FDA.

Jeffrey Newman, an attorney for five alleged victims of faulty Bard catheters, said of the sentence: "All my clients were informed and feel the same as I do — it was reasonable and well considered."

Newman said he believes he has the evi-

dence to establish a causal link in his three pending civil cases against Bard. The case brought by the family of Eunice Beavers of Lamar, Mo., who died in 1987 as a result of a catheter failure, was confidentially settled out of court two months ago. Another case had been settled last year.

The defense attorneys for Prigmore, Cvinar and Leichter filed an appeal yesterday, confident that the sentence and the conviction would be overturned in appellate court.

"I think these people will be vindicated on appeal," said Bill Kettlewell, attorney for Cvinar. He said the case hinged upon the vagueness of FDA regulations, and not on alleged victims.

Goal

- Control the process
 - To make improvement to the quality of the software
 - To reduce impact of changes and errors
 - To ensure user requirements are understood and met
 - To increase reliability and usability

Automated Processes

- Validate processes that cannot be fully verified.
 - Examples (molding, welding, sterilization, robotics, automated processes)
- Computer or automated data processing systems used in production or the quality system
- Validation is to ensure process consistently produces a result that meet specifications

Process Validation

- Validation Protocol
 - Defines the testing to be conducted, pass/fail criteria, and responsibilities
- Validation Report
 - Outlines the test results
- Define processes that require validation
- Define changes that require revalidation

Process Validation

- Establishing by objective evidence that a process consistently produces a result or product meeting its predetermined specifications.
 - Installation Qualification (IQ)
 - Operation Qualification (OQ)
 - Performance Qualification (PQ)

Process Validation (continued)

- Pharma – “Validate the performance of those manufacturing processes that may be responsible for causing variability”
- Device – “Where the results of a process cannot be fully verified”, “the process must be validated”

Processes Requiring Validation

- Water Purification
- Freon Degreasing
- Air Systems for Clean Rooms
- Cleaning
- Sterilization
- Sterile Packaging Sealing
- Plastic Injection Molding

Molding

- 32 Cavity Mold
- Use 90 shots (One shot fills all 32 cavities)
- Vary Time and Pressure

Time	Low Pressure	Med Pressure	High Pressure
4 secs	10 shots	10 shots	10 shots
5 secs	10 shots	10 shots	10 shots
6 secs	10 shots	10 shots	10 shots

Software

- 242 recalls between 1992 – 1998 were attributed to software failures.
- Of the software failures 79% were caused by software defects introduced when changes were made to the software after initial release.
- Validation and design controls are supposed to help avoid such defects.

Software

- All devices that contain software are subject to design control requirements as found in 21 CFR 820.30.

Software Validation

- Confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses and that the particular requirements implemented through software can be consistently fulfilled.

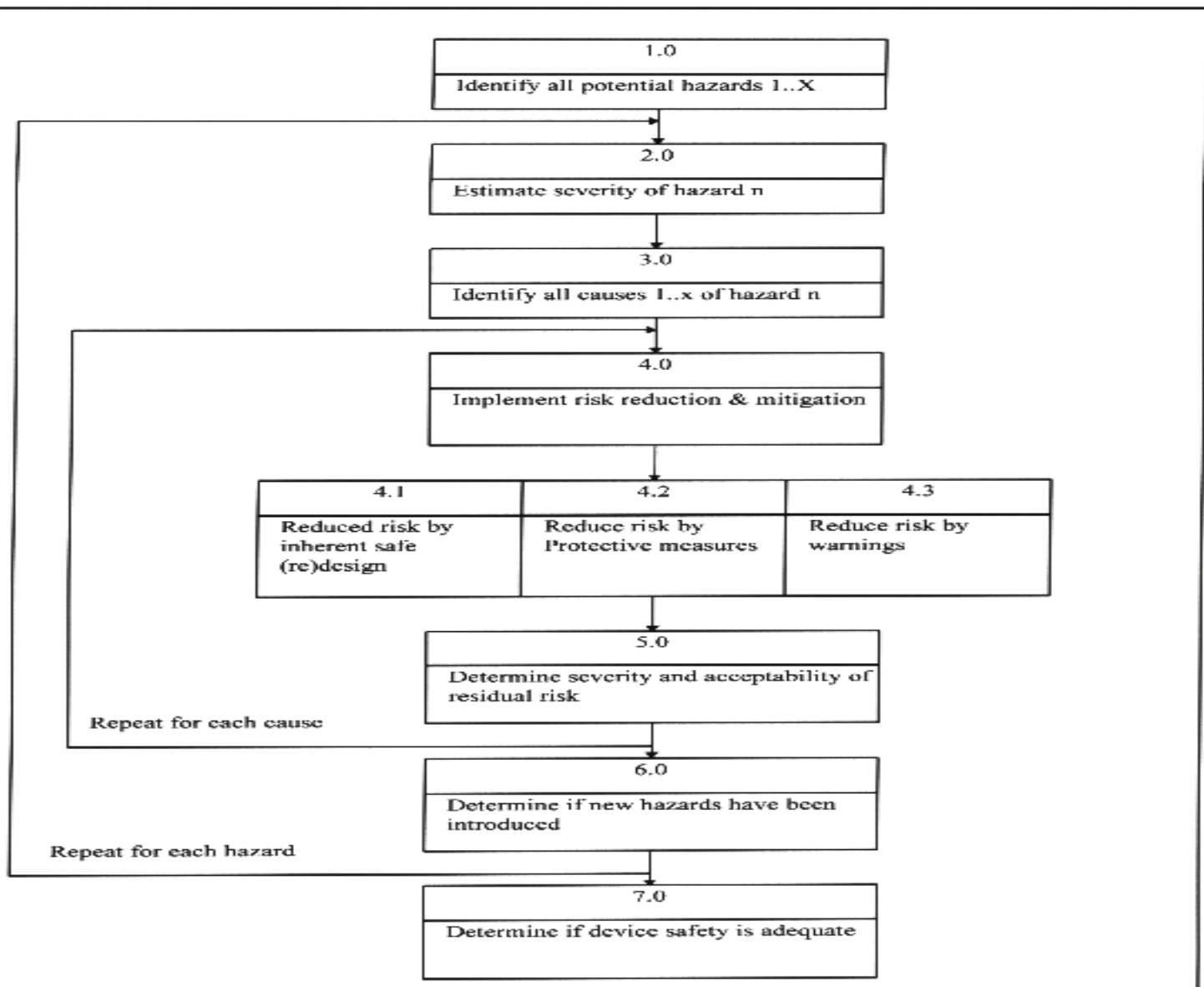
What software needs validating?

- Software that is part of a medical device
- Software that is the medical device
- Software used in production
- Software used in the implementation of the quality system

Risk Based

- The level of validation is based on the intended use and safety risks associated with the software

Risk Management



Level of Validation

- Validate to develop a level of confidence that the software meets all requirements and user expectations.
- The old FDA “IQ/OQ/PQ” validation model may not be suitable or relevant to software.
- Validation increases usability and reliability resulting in decreased failures, less risk to patients and users, and reduced liability. Can also reduce costs in the long-term.

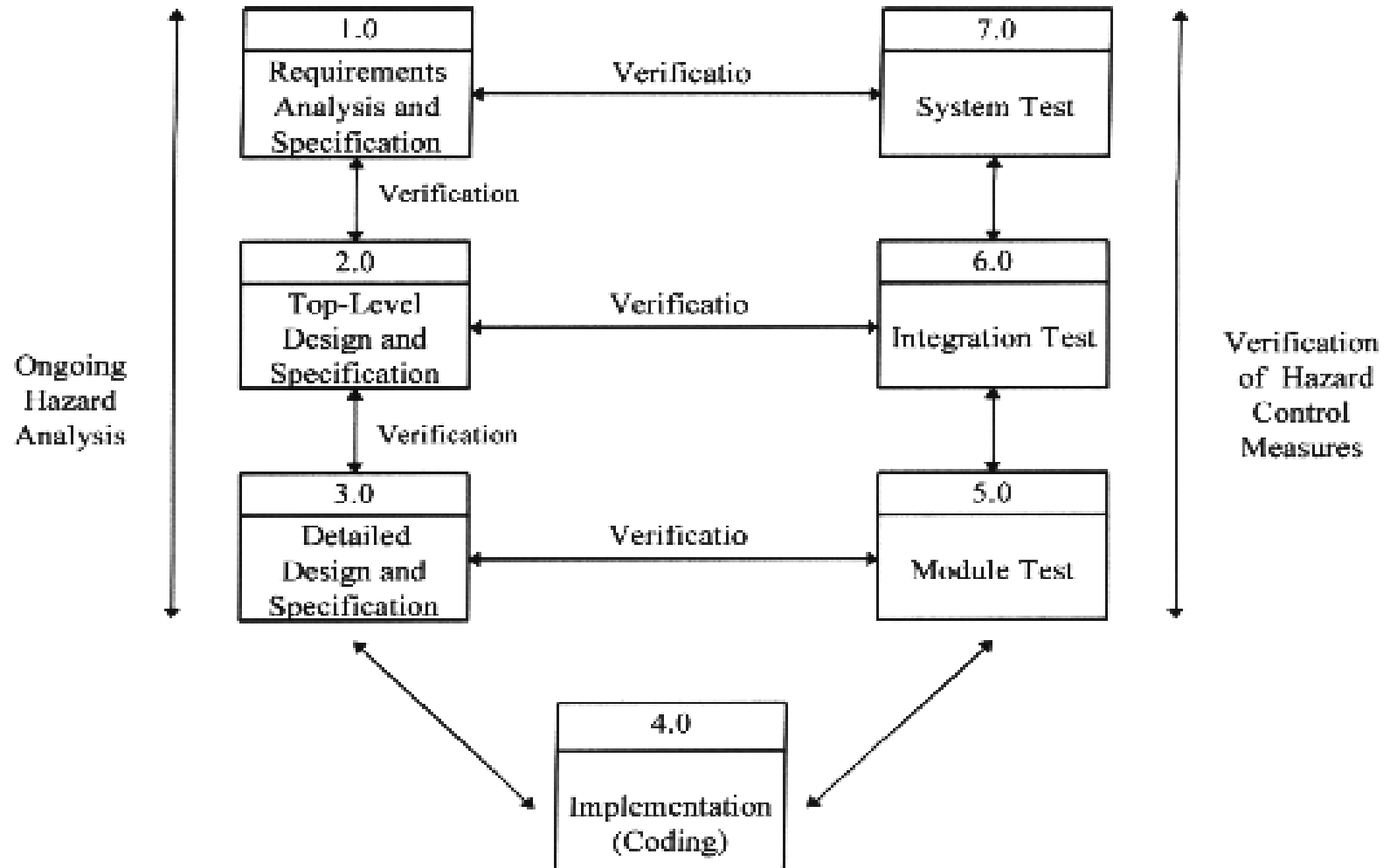
Software Design

- Most software errors are traceable to design.
- Branching (ability to execute alternative series of commands based on differing inputs) is significant part of software.
- Testing alone cannot fully verify software is complete and correct.
- Highly mobile workforce and high turnover.
Need documentation.

Software Changes

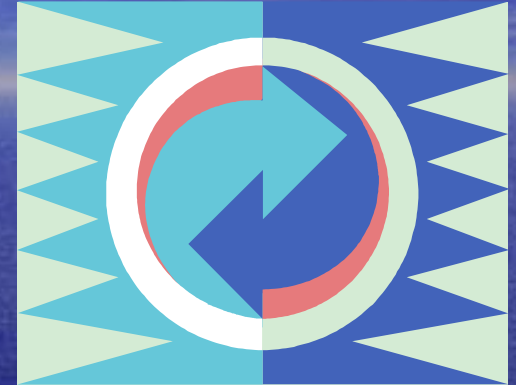
- Insignificant changes to software code can create unexpected and significant problems in the program.
- Solid design and validation helps with creating a reliable and usable software.
- Changes must be analyzed to determine the extent and impact on the entire system.

Software Life Cycle



Software Life Cycle

- Planning
- System Requirements
- Software Requirements / Specifications
- Coding
- Testing
- Installation
- Operation and Support
- Maintenance
- Retirement

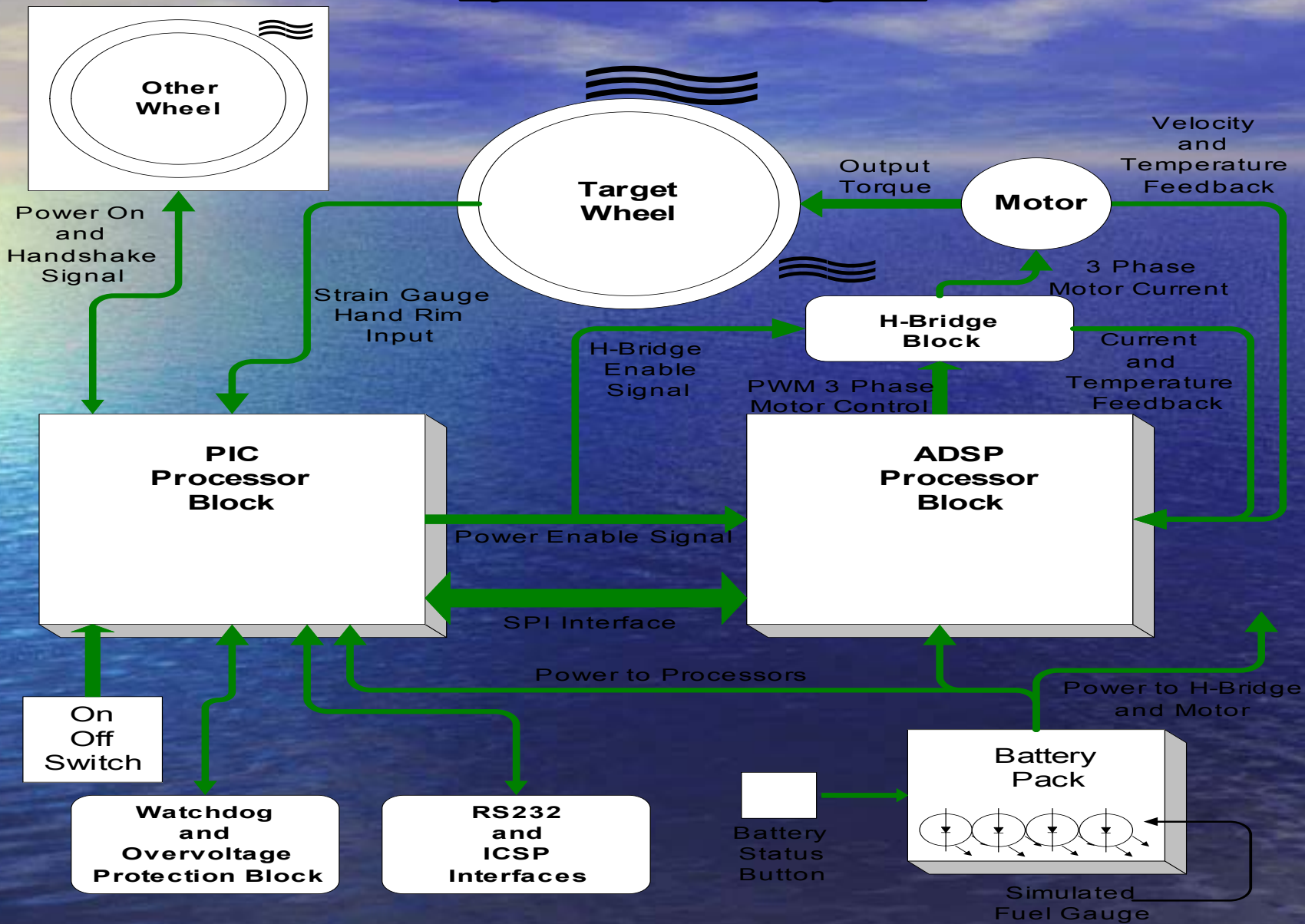


Planning



- Factors (reliability, maintainability, usability, etc)
- Methods / Procedures for each task
- Acceptance criteria
- Defining outputs
- Compare outputs to inputs
- Roles, resources, responsibilities
- Risks
- Documentation of user needs

System Block Diagram



Coding

- Different levels of error checking may be used during coding.
- Source code should be evaluated to verify its compliance with specified coding guidelines.
- Source code traceability analysis will verify that all code is linked to established specifications and test procedures.

Structural Testing

- Branch Coverage – test each decision or branch so each possible outcome occurs once.
- Condition Coverage – Sufficient test cases for each condition in a program decision to take all possible outcomes at least once.
- Path Coverage – Sufficient test cases for each feasible path from start to exit of a defined program segment to be executed at least once.

White Box vs Black Box

- White Box testing refers to structural testing of the software to show that the creator followed standards. Usually involves inspection of the program code.
- Black Box testing refers to functional testing of the program under known conditions with defined inputs.

Testing



- Unit (module or component) – focuses on early examination of sub-program functionality and ensures that functionality not visible at the system level is examined by testing
- Integration – Transfer of data and control across a program's internal and external interfaces (operating system, hardware, users)

System Testing

- All specified functionality exists and software is trustworthy
 - Performance (reliability, response times)
 - Response to stress conditions (under max load continuous use)
 - Security
 - Effectiveness of recovery
 - Usability
 - Compatibility with other software
 - Behavior in defined hardware configurations
 - Accuracy of documentation
 - Robustness (behavior during unexpected and invalid inputs)

User Site Testing

- Beta Testing, Site Validation, User Acceptance Testing
 - High Volume of Data
 - Heavy loads or stresses
 - Security
 - Fault testing
 - Error Messages
 - Safety
 - Usability

Software Changes

- Corrective Maintenance – to correct errors or faults.
- Perfective Maintenance – to improve performance.
- Adaptive Maintenance – ensure software is usable in changed environments
 - Sufficient regression analysis and testing should be conducted to demonstrate that portions of the software not involved in the change were not adversely effected.

Anomaly Evaluation



- Document
- Identify root cause
- Corrective Action
- Verification
- Identification of trends
- Problem and resolution tracking

Process Software

- Examples
 - Plant Wide Electronic Record System
 - Statistical Process Control
 - Controller for a Sterilization Cycle
 - Robotics
 - Automated Test Equipment for inspection of circuit boards in a life sustaining device
- Level of Validation Commensurate with risk

Define User Requirements

- Intended use
- Performance
- Quality
- Security
- Safety (alarms, sensors, interlocks, commands)

Off-The-Shelf Software



- Estimation of risk
- Hazard – possible source of danger or a condition that could cause injury
- Hazard Analysis – Identification of hazards and their causes.
- Risk control and mitigation

Off-the-Shelf

- Conduct research into program's use history.
 - Know limitations, other user experiences, and known problems.
- Evaluation software development activities.

Hazard Analysis

- List all potential hazards
- Estimate severity of hazards
- List potential causes of hazards
- Hazard Mitigation
 - Design
 - Protective Measures
 - Warnings / Labeling

Level of Concern

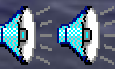
- Major – Directly affects patient, operator, or by-stander, failure could result in death or serious injury or delayed or incorrect information that could result in death or serious injury.
- Moderate – Could result in non-serious injury.
- Minor – Not expected to result in any injury

Off-the-Shelf

- Identify “what is it”
- Specifications (hardware, OS)
- Actions to be taken by end users (installation, configuration, training)
- Identify “what does it do”
- Identify “How do you know it works”
- Identify “How is it controlled” (maintenance, life cycle support, storage)

Y2K

- Watch out, this is going to be big!



Electronic Records



- 21 CFR 11
 - When first introduced this regulation was broadly interpreted resulting in unnecessary controls and costs, discouraging innovation and technological advances without providing benefit to public health.
 - A more narrow interpretation is used now.

Electronic Records

- Applies to any records required to be maintained by FDA, and
- Only if electronic format is kept in place of paper.

Electronic Records

- Validate software to ensure accuracy, reliability, integrity, availability, and authenticity of required records.
- Validation must include stress conditions (high number of users, error conditions, unexpected entries)
- Live user tests

Electronic Records

- Audit Trail – computer generate time stamped audit trails to record entries and actions that create, modify, or delete records.

Electronic Records

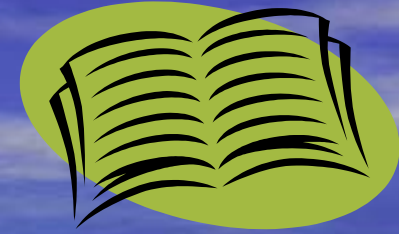
- Legacy Systems in place prior to 1997, FDA will use discretionary enforcement.
- Accessibility – Records must be accessible.
- Retention – Records must be retained in accordance with retention requirements.

Security



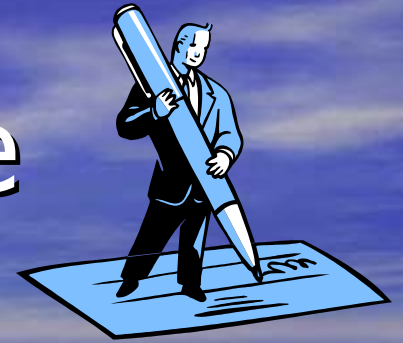
- Access only by authorized individuals
- Audit Trail
- Operational system checks to enforce permitted sequencing of steps and events
- Authority checks
- Use of device checks to determine validity of source data

Policies



- Written policies to hold individuals accountable and responsible.
- Training and experience to perform assigned tasks.
- Controls for distribution and access to records.
- Controls for revision and change control.

Electronic Signature



- Name of signer
- Date / Time of Signature
- Meaning (approval, review, authorship, etc)
- Controls to ensure signature cannot be copied or transferred to falsify records.
- Signature must be unique to one individual.

Electronic Signature

- Verify identify of person
- Certify to FDA that signatures are used and are legally binding
- Two identification components (ID code and Password)
- Biometrics can also be used
- ID code and password must be unique

Electronic Signature

- Periodic Checks of ID Code and Password
- Deauthorize lost, stolen, missing ID info
- Safeguards to prevent unauthorized use of passwords or ID codes
- Testing of devices to ensure they function properly.
- Certify to FDA if signatures are to be used.