JOHNS HOPKINS
WHITING SCHOOL
of ENGINEERING

Medical Device Development

Peter Kazanzides
Johns Hopkins University

February 27, 2024

My Background

1989-1990 Postdoctoral research at IBM on ROBODOC

1990-2002 Co-Founder of Integrated Surgical Systems

- Commercial development of ROBODOC® System
- Commercial sales in Europe (CE Mark)
- Clinical trials in U.S. and Japan
- ISO 9001 certification

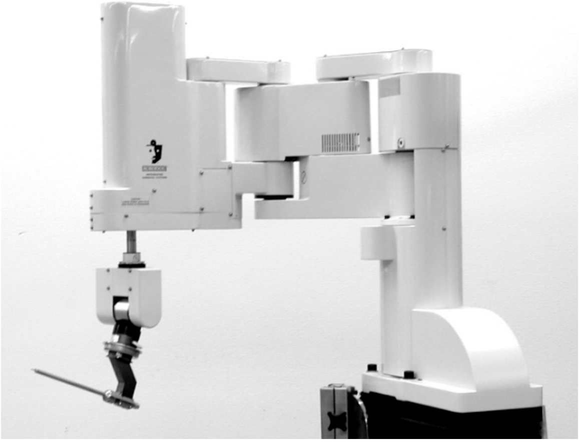
2002-present Research Professor at JHU

May 1990

Caveats

1. My experience is primarily from working on ROBODOC … and it was over 20 years ago
2. My focus was mostly on the software development process (though the same process is used for hardware / systems)
3. Many things have changed since then (e.g., more standards, guidance documents)

1990
Veterinary
prototype



1996
CE marked
medical device

Medical Device Regulations

- Medical devices are highly regulated:
  - FDA approval (United States)
    - UL listing might be required by customer
  - CE mark (Europe)
  - MHW approval (Japan)
  - Other national requirements

FDA Approval

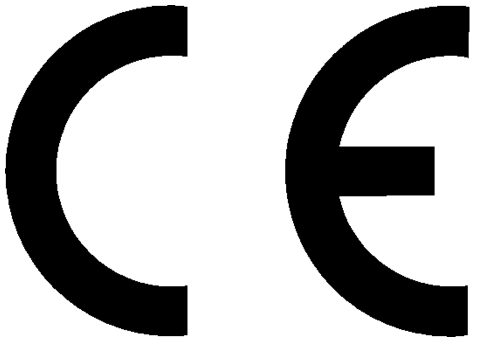
- Pre-Market Approval (PMA)
  - Path to market for new devices
  - Generally requires clinical trials
  - Company submits extensive documentation and data
- 510(K)
  - Establish “substantial equivalence” to a predicate (existing) device
  - May include clinical trials
  - Less extensive documentation and data

FDA Approval

- Investigational Device Exemption (IDE)
  - Can do clinical trials
    - Also need hospital Institutional Review Board (IRB) approval
  - Not allowed to market the device

CE Marking

- Indicates that product satisfies European safety requirements
- Managed by “notified bodies”, such as:
  - TUV (Germany)
  - BSI, SGS (United Kingdom)
  - Many others



CE Marking and ISO 9000

- ISO 9000 Quality Standards encompass:
  - ISO 9001: Design and Manufacturing
  - ISO 9002: Manufacturing Only
  - ISO 9003: Inspection and Testing Only
- Company with ISO 9001 can (within limits) self-certify (CE Mark) its products
- Notified Body periodically audits Quality System

Design Controls

- Quality System component that applies to product design
  - ISO 9001
  - FDA QSR (Quality System Regulations)

- Goal: prevent failures due to bad design

Design Controls

- “Say what you will do and then do what you say”

  – Company defines its development process

  – Regulatory body reviews the process

  – Company follows the process, producing supporting documentation (Quality Records)

  – Regulatory body periodically reviews records

System/Software Development Procedure

- Typical phases are:
  - Requirements
  - Design
  - Implementation
  - Integration and Test
  - Design Transfer (to production)
  - Maintenance
- Regulators are most familiar with “waterfall process”
  - Each phase performed sequentially

Requirements Phase Inputs

- Customer Requirements document
  - also called: User Requirements, System Requirements Definition, Concept of Operations
  - Usually generated by marketing department

Requirements Phase Outputs (1)

- Software (or Project) Development Plan
- Software Quality Assurance Plan:
  - Defines standards to be used (e.g., coding standards, documentation standards)
  - Defines review and audit plan
  - Specifies configuration management plan
  - Usually generated by Quality Assurance, with input from Engineering

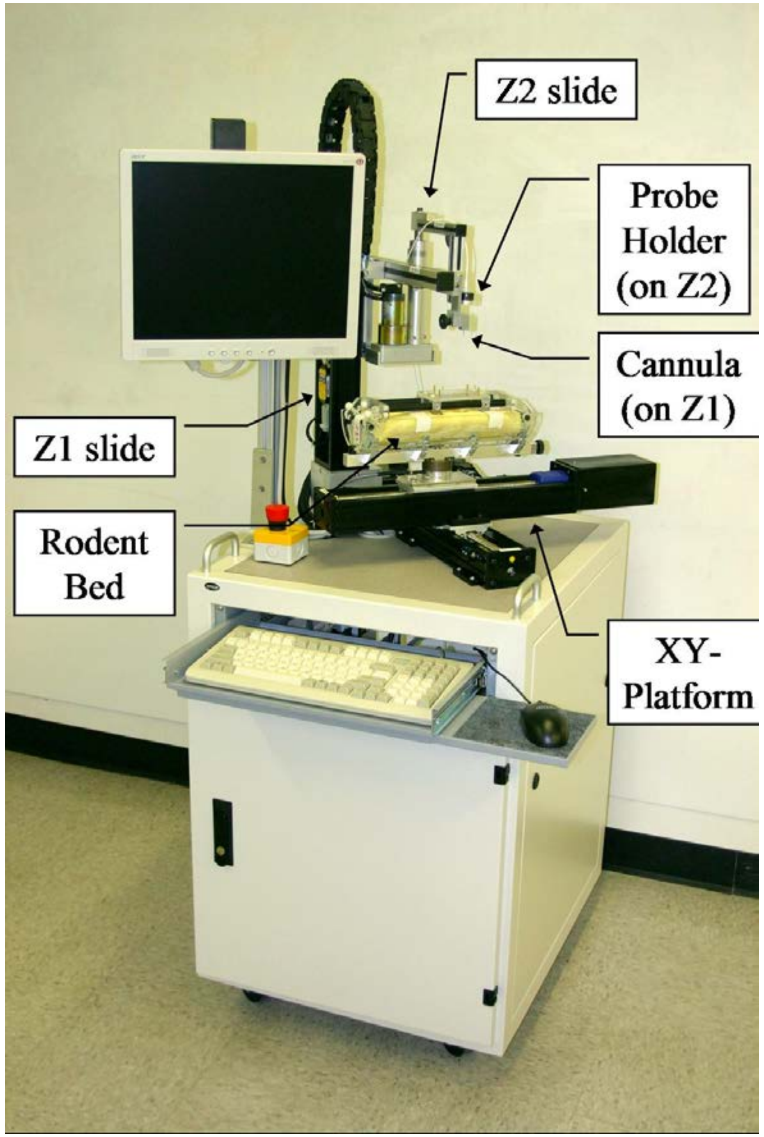
Requirements Phase Outputs (2)

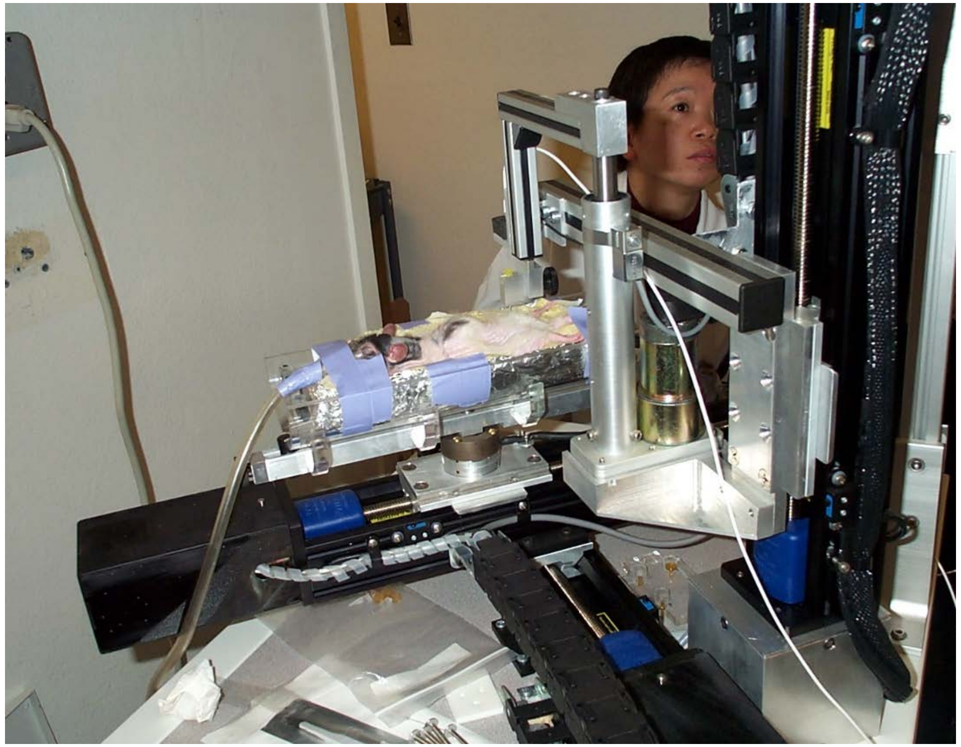
- System/Software Requirements Specification (SRS)
  - Should specify requirements, not design
  - Should be unambiguous and testable
  - Must be traceable to Customer Requirements
- System and software requirements specifications can be combined (small projects) or be separate documents

Sample SRS Outline

- Introduction
- References
- System Description
- External Interface Requirements
- Functional Requirements
- Performance Requirements
- Safety Requirements
- Design Constraints

Sample SRS





System in use at Memorial Sloan Kettering Cancer Center (MSKCC), New York City

P. Kazanzides, J. Chang, I. Iordachita, J. Li, C. Ling, G. Fichtinger, “Design and validation of an image guided robot for small animal research,” Computer Aided Surgery, 2007 (also MICCAI 2006)

J. Chang, B. Wen, P. Kazanzides, P. Zanzonico, R. Finn, G. Fichtinger, C. Ling, “A robotic system for 18F-FMISO PET-guided intratumoral pO2 measurements," Medical Physics, 2009.

Requirements Phase Outputs (3)

- Preliminary Risk (or Hazard) Analysis
  - Identifies safety requirements
  - Should be performed by cross-functional team, including application expert
  - Various techniques can be used
    - Failure Modes and Effects Analysis (FMEA)
    - Failure Modes, Effects and Criticality Analysis (FMECA)
    - Fault Tree Analysis (FTA)

Risk Analysis – FMEA/FMECA

- Most common risk analysis method
- Analyzes the effect of component failure
  - Bottom-up analysis
- An iterative process:
  - Determine risks for initial system design
  - Add methods of control where necessary
  - Determine risks for system design including methods of control
- Typically presented in tabular format:
  - Failure Mode
  - Effect on System
  - Cause of Failure
  - Method of Control

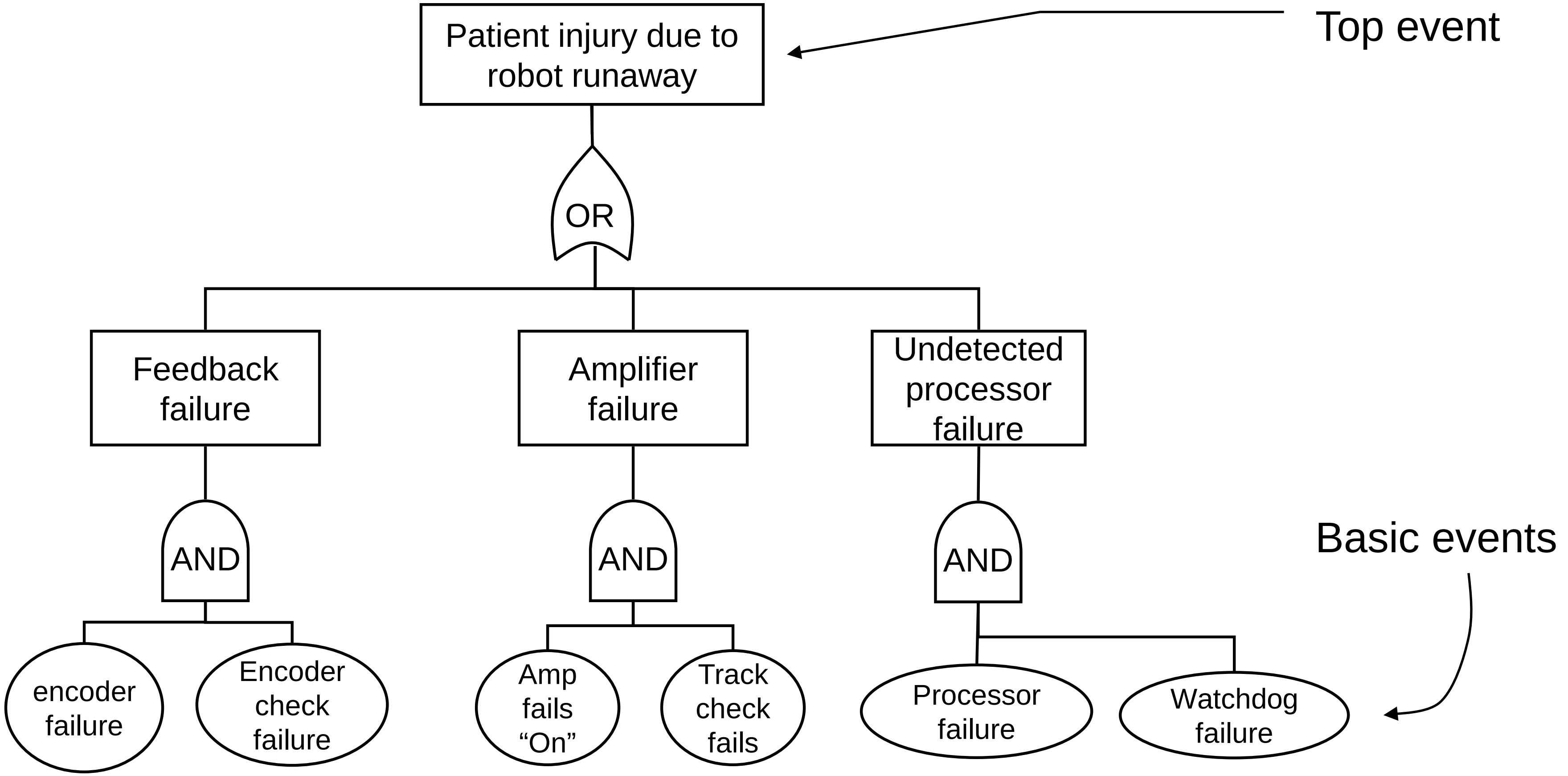
Sample FMEA

Failure Mode	**Effect on System**	**Cause**	**Method of Control**
Incorrect feedback	Incorrect robot motion	Encoder failure	Redundant encoders with software check
Uncontrolled motor current	Incorrect robot motion	Power amplifier failure	Tracking error software check
Robot continues previous motion	Incorrect robot motion	Processor failure	Watchdog to disable power

FMECA

- FMECA adds risk assessment to FMEA
- Risk assessment (criticality)
  - Severity (S) – seriousness of effect of failure
  - Occurrence (O) – likelihood of failure
  - Detection (D) – ability to detect failure
  - Risk Priority Number (RPN) = (S) x (O) x (D)
- Assign numerical values (e.g., 1-10) for (S), (O) and (D)
- Prioritize risks by RPN
- Table can include both initial and final, or just final, risk assessment

Sample FTA



Can include probabilities of failure if known

Some Medical Device Safety Standards

- IEC 60601-1: Medical Electrical Equipment (Safety)
- IEC 62304: Medical Device Software – Software Life Cycle Processes
- ISO 14971: Application of Risk Management to Medical Devices
- IEC 60812: Analysis Techniques for System Reliability (FMEA)
- IEC 61025: Fault Tree Analysis (FTA)

Requirements Phase Outputs (4)

- Preliminary Software Validation Plan
  - System Testing (e.g., test that requirements have been met)

- Design Review of all Requirements Phase Outputs
  - Meeting minutes

Design Phase

- System/Software Architectural Design
  - Architecture diagrams, data flow diagrams, etc.
- System/Software Detailed Design
  - System/Software Design Specification (SDS)
  - Traceability analysis from SDS to SRS

Design Phase

- Update Software Validation Plan
  - Integration testing
- Update Risk Analysis
- Design Review II

Implementation Phase

- Write software according to Software Quality Assurance Plan (SQAP):
  - Programming Guidelines
  - Documentation Standards
- Update Software Validation Plan
  - Unit or module testing
- Traceability analysis (SVP to SDS/SRS)
- Run module tests and write Test Reports

Integration and Test Phase

- Run Integration Tests and write Test Reports
- Run System Tests and write Test Reports

Verification vs. Validation

Verification and Validation

- Verification:
  - “objective evidence that the design outputs … meet all of the specified requirements …”
  - Methods: testing, design reviews, code walkthroughs, etc.
- Validation:
  - “confirmation … that software specifications conform to user needs and intended uses …”
  - Methods: testing in simulated use environment, user site testing, etc.

General Principles of Software Validation; Final Guidance for Industry and FDA Staff, January 2002

https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-principles-software-validation

Design Transfer

- Write relevant manufacturing procedures
  - Software installation procedure
  - Software duplication procedure
- Ensure user documentation is complete
  - Labeling review
- Release system/software
  - Change control procedure

Maintenance Phase

- Review and update any necessary documents (e.g., SRS, Risk Analysis, SDS)
- Implement changes
- Assess testing requirement
  - Test changes
  - Possible regression testing
- Release via Change Control Procedure

Summary

Development process seems overwhelming!

But:

- It can be customized for each company
- It can be improved over time
- It is not that bad when you get used to it
- It generally produces better systems/software
- It is required for medical products!