Standards and Guidance and Rules, Oh My!

WARREN B CRAYCROFT
wcraycroft@ieee.org
Sept 2017

https://www.youtube.com/watch?v=Etx-nDCZzLo

What I Hope to Accomplish This Hour

- Consultant Opportunities
- The Regulatory Environment
- The Legitimacy of Medical Device Regulation
  - Medical device development in the 80's
- Regulatory Intelligence for Developers and PMs
  - Attacking the knowledge management problem
- Integrating Regulation with Project Management

Medical Device Development; A Consultant's Perspective

- Opportunities in early-stage small-headcount companies
  - Development project managers
  - Direct engineering contributors
- Regulated development: more areas of responsibility than headcount
  - Valuable contributors wear multiple hats
- **Safety is paramount**
- **Everyone has a regulatory role**

What I Hope to Accomplish This Hour

- Consultant Opportunities **√**
- **The Regulatory Environment**
- The Legitimacy of Medical Device Regulation
  - Medical device development in the 80's
- Regulatory Intelligence for Developers and PMs
  - Attacking the knowledge management problem
- Integrating Regulation with Project Management

The Regulatory Environment

- Rules (US Acts and Regulations)
  - 21 CFR 820: The Quality System Regulation
    - Design controls are required at an early stage
    - Current Good Manufacturing Practices
  - Acts and Rules on market clearance and approvals, recalls, clinical investigations, …
- Standards
  - ISO, IEC, AAMI, ASTM, there are a bunch
- Guidances
  - FDA: hundreds of guidances for medical devices

The Regulatory Environment: Moving Target w.r.t. Projects

- Changes in Rules (US Acts and Regulations)
  - Relatively slow rate of change; **lots of warning** in the rule-creation process
- Changes in Standards
  - Usually some warning (need "ear to the ground")
  - Can be **a significant factor** in a 12 – 24 month project
- Changes in FDA Guidances
  - "Current thinking" can change **without warning**

Some Opinions on Regulation

- A out-of-control bureaucratic nightmare?
- An adversarial relationship to be gamed and minimized?
- A significant burden to be grudgingly endured?
- Too much of a good thing?
- My point of view: NONE OF THE ABOVE

What I Hope to Accomplish This Hour

- Consultant Opportunities **√**
- The Regulatory Environment **√**
- **The Legitimacy of Medical Device Regulation**
  - **Medical device development in the 80's**
- Regulatory Intelligence for Developers and PMs
  - Attacking the knowledge management problem
- Integrating Regulation with Project Management

Key Rules and Standards over Time

- 1976 Good Manufacturing Practice
- **1996 Quality System Regulation**
  - **Major addition: design controls**
- ISO 13485 2016: Quality Management Systems
  - A medical spinoff of ISO 9001
- ISO 14971 2007: Risk Management Process
  - A mature defect containment process
- IEC 60601-1 2012: Basic Medical Device Safety
  - A mature general safety standard

Key Rules and Standards over Time

- FDA Usability Engineering Guidances
  - "Do it by Design"
  - 2012 and 2016 Guidances: FDA Human Factors / Usability Engineering Guidances
- IEC 62366 2015 Part 1: Application of usability engineering to medical devices
- HE-75 2013: Human Factors Engineer
  - Both reflect current FDA thinking
  - Regulatory submissions MUST show UE/HF process

The Roots of the Quality System Regulation

- 1996: Final Rule; Quality System Regulation
  - Major revision of the Current Good Manufacturing Practices of 1978
  - Major addition: pre-production design controls, 21 CFR 820
  - The culmination of a 6-year rule-writing process with significant industry input.
- Driven by the Safe Medical Devices Act of 1990
  - Congress passed this act in response to **studies of medical device accidents and recalls from 1983 to 1989**
- Therac-25: the "poster child" of nonconformances in:
  - Medical device system design, software design, and human interface design
  - Risk management process
  - Quality management systems like CAPA, and
  - The FDA reporting requirements at that time

A Quick Word on Case Histories

- *Medical Devices: The Therac-25*, Nancy Leveson, 49 pages, available online
- Case histories often involve a series of decisions and actions over time.
- It is unfair to pass judgment using present-day knowledge of all events
- You must walk the time line with the decision makers, AND USE ONLY THE KNOWLEDGE AND TOOLS KNOWN TO THEM AT THAT TIME.

Therac-25

- A radiation therapy machine: 11 installed in the U.S. and Canada
  - Therac-25 a major upgrade of Therac-20 that REMOVED hardware safety interlocks and relied on software only for beam strength and position
  - hundreds of patients were successfully treated
- 6 patients massively overdosed over nearly 2 year period (!)
  - 4 patients died as a result of overdose
  - “worst accidents in 35-year medical accelerator history”

Timeline of Overdose Events

1. 6/3/85: Marietta Georgia; patient seriously injured
2. 7/26/85: Ontario, Canada: patient died 11/3/85
   - 7/30/85: FDA first informed; issues Class II recall
3. 12/1985: Yakima, WA; minor disability
   - 3/86: AECL (Mfg) notifies FDA of 1st lawsuit (rec'vd 11/85!)
4. 3/21/86: Tyler, TX; patient died 8/86
5. 4/11/86: Tyler, TX; patient died 5/1/86
   - 6/13/86: Mfg's 1st Corrective Action Report (CAR) to FDA
6. 1/17/87: Yakima, WA; patient died 4/87
   - 5/26/87: Mfg's 4th CAR to FDA; **FDA Class I Recall**
   - 7/21/87: Mfg's 5th CAR to FDA; intensive list of changes

Therac-25 Lessons Learned 1

- Lessons Learned are interrelated
- Overconfidence in Software
  - Hardware interlocks of Therac-20 were removed
  - First Risk Analysis did not include software!
- Confusing Software Reliability with Safety
  - Mfg. assumed software was safe because it was reliable
  - Probability of systemic failure was falsely estimated as extremely low.

Therac-25 Lessons Learned 2

- Lack of Defensive Design
  - Lack of self-checks, independent checks and effective exception handling.
  - Machine “lied” to operators on dosage levels
    - Low doses were displayed while patients yelled in pain
  - Single-point failures were allowed in software
- Failure to Eliminate Root Causes
  - Inadequate depth of investigation; stopped at first defect
  - Incomplete fixes dribbled out over 2 year period

Therac-25 Lessons Learned 3

- Unrealistic Risk Assessments
  - "Complacency" in a technology with risk
  - "Software does not wear out" mentality
  - Assigned single low probability to systemic soft errors
- Inadequate Investigation or Follow-up on Accident Reports
  - No risk-based process of investigation at first hint of a problem

Therac-25 Lessons Learned 4

- Inadequate Software Engineering Practices
  - Specs and documentation were “afterthoughts”
  - No software quality assurance practices/standards
    - No V & V activities other than testing
  - Inadequate testing practices: no test plan, no unit testing, undocumented testing …
- Complacency
  - Two previous decades of excellent medical accelerator safety
  - False assumption of mfg’s cumulative safety design experience

Therac-25 Lessons Learned 5

- Safe versus Friendly User Interfaces
  - Poor presentation of information to operators
  - Cryptic, undocumented error messages
  - Never tested with real users under actual use conditions
- User & Government Oversight and Standards
  - Inadequate incident reporting requirements
  - Users kept in dark; late but effective user group response
  - Inadequate FDA rules and guidance on software

Influence on Current Regulation 1

- "Overconfidence in Software"
  - In general, significant improvement in rules, standards, and guidance for safety-significant software development and maintenance
  - Software Risk assessments are required (14971, 62304)
    - Significant risks mitigated by software alone are now suspect from a risk control perspective
    - Examples include independent hardware watchdogs on software systems

Influence on Current Regulation 2

- "Confusing Software Reliability with Safety"
  - Systemic software failures are evaluated by severity only; probability not considered (14971)
  - True reliability assessed by unit testing, code reviews and inspections, user testing, ….
- "Lack of Defensive Design"
  - Self-checks, independent checks and effective exception handling are state-of-art safety-significant software design practices.
  - Single-point failures directly causing hazards not allowed (60601-1)

Influence on Current Regulation 3

- "Failure to Eliminate Root Causes"
  - Corrective and Preventive Action process (21 CFR 820.100)
  - **FDA: HEART OF QUALITY MANAGMENT**
- "Unrealistic Risk Assessments"
  - Each new device judged on its own risk assessment
  - Systemic software failures are evaluated by severity only; probability not considered (14971)

Influence on Current Regulation 4

- "Inadequate Investigation or Follow-up on Accident Reports"
  - A "complaints" reporting process required
- "Inadequate Software Engineering Practices"
  - Extensive "temporal" doc requirements (62304)
  - SQA plans required (62304)
    - Including detailed V & V plans– NOT JUST TESTING
  - Extensive test planning and testing requirements

Influence on Current Regulation 5

- "Complacency"
  - An intensive, thorough risk assessment is best defense against complacency
  - Defensive design: apply Murphy's law
- "Safe versus Friendly User Interfaces"
  - Usability Engineering Process (62366)
  - Clear, documented error messages (60601-1, 62366)
  - Early usability testing with rep. users (62366)

Influence on Current Regulation 6

- "User & Government Oversight and Standards"
  - FDA Reporting requirements strengthened and expanded to users (21 CFR 803)
  - Clinical trial reporting "near misses" (ISO 14155:2011)

Influence on Current Regulation, Summary

- Current S, G, and R, along with current safety-significant software development practices, would have either
  - eliminated many issues during design, or
  - given earlier warning to FDA and users
- Exercise: highlight Leveson case-history where events are prevented by regulation
  - Original flawed design would not have occurred
  - “If it did”, detection would have occurred earlier

“What if” Examples

- Assuming no AECL malfeasance, an effective CAPA process would have collected incident info in one place with a process to investigate and correct.
  - June, 1985: The first phone call to AECL after first non-fatal overdose triggers a “safety” CAPA.
  - July, 1985: The 2nd overdose “connects two overdose dots”; Therac-25 taken out of service
  - Result: One non-serious injury, one death

“What if” Examples

- Other examples of connecting dots early:
  - The manufacturer’s Complaint process triggers a CAPA after second overdose incident
  - Improved FDA reporting requirements; especially user-required reporting

Legitimacy

- **Painful lessons learned can be directly traced to current regulation, standards, and guidance**
- Legitimacy analogous to building and fire codes
- The volume of lessons-learned is continually increasing – that's a good thing!
- It's a Knowledge Management Problem

What I Hope to Accomplish This Hour

- Consultant Opportunities **√**
- The Regulatory Environment **√**
- The Legitimacy of Medical Device Regulation **√**
  - Medical device development in the 80's **√**
- **Regulatory Intelligence for Developers and PMs**
  - **Attacking the knowledge management problem**
- Integrating Regulation with Project Management

Regulatory Intelligence

- **Regulatory intelligence:** the process of gathering, monitoring and analyzing regulatory information and data to track developments in the changing regulatory environment.
- Mature companies: most of this burden is on Regulatory Department
- Early-Stage companies: You may not yet have a seasoned, “current” Regulatory person

Regulatory Intel Methods

- Join your local regulatory affairs group
  - San Diego Regulatory Affairs Network (SDRAN)
  - Orange County Regulatory Affairs Discussion Grp
- Subscribe to FDA newsletters
  - Notification of guidances, recalls, **warning letters**
- Subscribe to a standards service
  - British Standards BSOL

Regulatory Intel Methods

- Consultants that dangle content:
  - Rob Packard, Greenlight, Emergo
- Consultancies in the trenches:
  - Experien, Norblitt and Rueland, …
  - SDRAN is thick with consultants

Regulatory Intel Methods

- FDA: CDRH Learn, Device Advice
- Buy training on key regulations, standards, and quality management processes
  - If you have Regulatory personnel, schedule regular presentations to development personnel
  - Buy lunch!
  - Build a company knowledge base on your particular device space

What I Hope to Accomplish This Hour

- Consultant Opportunities **√**
- The Regulatory Environment **√**
- The Legitimacy of Medical Device Regulation **√**
  - Medical device development in the 80's **√**
- Regulatory Intelligence for Developers and PMs **√**
  - Attacking the knowledge management problem **√**
- **Integrating Regulation with Project Management**

Effective Project Management

- Regulatory Affairs is a roiling cauldron of change.
- PMs MUST keep current on regulatory affairs pertaining to the medical device “space”
  - By systematic interaction with Regulatory personnel as well as your own intel gathering
  - Keep current on FDA guidance docs
- MUST know the key standards pertaining to the “space”
- Embrace change!

Risk Management (ISO 14971)

- A vital input to product requirements
- Make Risk Management the centerpiece of requirements management
  - The risk assessment process generates safety requirements
  - Trace to design implementation, verification and validation testing
- Start risk assessment early in the design process!

We Did It!

- Consultant Opportunities **√**
- The Regulatory Environment **√**
- The Legitimacy of Medical Device Regulation **√**
  - Medical device development in the 80's **√**
- Regulatory Intelligence for Developers and PMs **√**
  - Attacking the knowledge management problem **√**
- Integrating Regulation with Project Management **√**