Failure in Design

• Part or product no longer performs
  – Extremes
    • Graceful degradation
      – You see it coming
    • Catastrophic
      – You don’t

• Many flavors to choose
  – Bent, fractured, broken
  – Melted, fused, vaporized
  – “blue screen of death”
## Failure Rates

(Dieter+Schmidt, 2009)

<table>
<thead>
<tr>
<th>Components</th>
<th># per 1000 hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bolts, shafts</td>
<td>$2 \times 10^{-7}$</td>
</tr>
<tr>
<td>Gaskets</td>
<td>$5 \times 10^{-4}$</td>
</tr>
<tr>
<td>Pipe joints</td>
<td>$5 \times 10^{-4}$</td>
</tr>
<tr>
<td>Plastic hoses</td>
<td>$4 \times 10^{-2}$</td>
</tr>
<tr>
<td>Valves, leaking</td>
<td>$2 \times 10^{-3}$</td>
</tr>
</tbody>
</table>

**Systems**

<table>
<thead>
<tr>
<th>Systems</th>
<th># per 1000 hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compressor</td>
<td>$1.5 \times 10^{-1}$</td>
</tr>
<tr>
<td>Diesel Generator</td>
<td>1.2-5</td>
</tr>
<tr>
<td>Refrigerator</td>
<td>$4-6 \times 10^{-2}$ (~2 yrs)</td>
</tr>
<tr>
<td>Mainframe Computer</td>
<td>4-8 (~10 days)</td>
</tr>
<tr>
<td>PC</td>
<td>$2-5 \times 10^{-2}$ (~3 yrs)</td>
</tr>
<tr>
<td>Printed Circuit Board</td>
<td>$7-10 \times 10^{-5}$</td>
</tr>
</tbody>
</table>
The Bathtub Curve

• For electronics

Dead on Arrival

Failure Rate

Constant rate

“infant mortality”

Burn-in

Wear out

Time
The Bathtub Curve

• For Mechanics

![Bathtub Curve Diagram]
Risk, Reliability, and Safety

• Risk
  – the likelihood of being exposed to a hazard

• Reliability
  – A measure of the capability of the part/product to operate without failure
    • probabilities

• Safety
  – Relative protection from exposure to a hazard
    • Risk assessment (probability computation)
    • Acceptability (value judgment)
Risk Assessment

• Tolerable Risk
  – We are prepared to live with, every day
    • But periodic review is desired

• Acceptable Risk
  – As needed, but in order to achieve some goal

• Unacceptable Risk
  – We won’t, and/or we won’t allow others to

• ALARA (ALARP)
  – “As low as reasonably achievable” (possible)
    • Common principle for regulations
# Common Risks

(From Dieter+Schmidt, 2009)

<table>
<thead>
<tr>
<th>Cause of Fatality</th>
<th>Fatalities per person per year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smoking (20/day)</td>
<td>$5 \times 10^{-3}$</td>
</tr>
<tr>
<td>Cancer (general)</td>
<td>$3 \times 10^{-3}$</td>
</tr>
<tr>
<td>Race Car driving</td>
<td>$1 \times 10^{-3}$</td>
</tr>
<tr>
<td>Motor Vehicle driving</td>
<td>$3 \times 10^{-4}$</td>
</tr>
<tr>
<td>Fire</td>
<td>$4 \times 10^{-5}$</td>
</tr>
<tr>
<td>Poison</td>
<td>$2 \times 10^{-5}$</td>
</tr>
<tr>
<td>Industrial machinery accident</td>
<td>$1 \times 10^{-5}$</td>
</tr>
<tr>
<td>Air Travel</td>
<td>$9 \times 10^{-6}$</td>
</tr>
<tr>
<td>Rail travel</td>
<td>$4 \times 10^{-6}$</td>
</tr>
<tr>
<td>California Earthquake</td>
<td>$2 \times 10^{-6}$</td>
</tr>
<tr>
<td>Lightning</td>
<td>$5 \times 10^{-7}$</td>
</tr>
</tbody>
</table>
Design for Reliability

- Margin of Safety
  - e.g. using $\frac{1}{2}$ of the yield strength as the limit
- Derating
  - Lowering the allowed limits, due to other circumstances
    - Requiring a 40W bulb in a 60W fixture, due to limited air-flow
- Redundancy
  - N+M units doing the work of N
  - Active/standby ("hot spares")
- Durability
  - Material choice
- Damage Tolerance
  - Often a design choice (making something thicker)
- Ease of Inspection
- Simplicity
- Specificity
  - Adherence to standards, standard parts
Reliability Data

• The Reliability Information Analysis Center
  – www.theriac.org/
    • Department of Defense
    • MIL-HDBK-217
      – Electronics
    • NPRD-95
      – Non-electronics reliability

• ASME (www.asme.org), others
Design for Safety

“A safe product does not cause injury or property loss”
(Dieter+Schmidt, 2009)

– But we need to consider the hazards associated with use

• Inherent in normal use
• Originates from component failure
• Caused by user misuse
  – “Do not use this lawn mower to trim hedges”
• Exists during normal maintenance
• Created by improper maintenance
• Stems from a lack of maintenance

http://www.stuff.co.nz/oddstuff/3070920/High-rider-trims-his-hedge
Safety Guidelines

- Perform appropriate analyses
- Comply with published standards
- Use state-of-the-art technology
- Include reasonable safety features or devices
- Take into account how the user might misuse the product
- Consider hidden dangers that might surprise the user
- Consider variations in materials or manufacturing, or effects of wear
- Carry out appropriate testing and interpret results correctly
- Implement superior quality control
- Document everything!
Safety Hierarchy (Safety Dance?)

• Identify the Hazard!
• **Eliminate the hazard**
• Protect against the hazard
• Warn against the hazard
• Provide Training
• Provide Personal Protection Devices (PPDs)
Legal Implications

- **Product Liability**
  - Civil Action
    - If you hurt people or property
      - “loss”
  - Criminal Action
    - If you break the law

- **Occupational Safety**
  - Protection of workers
    - Local, state, and federal laws
  - Occupational Safety and Health Administration
    - OSHA
    - [www.osha.gov/](http://www.osha.gov/)
      - US Department of Labor
How can we make safe, reliable designs?

• Standards!

• Regulatory Bodies
  – Advancement of Medical Instrumentation (AAMI)
  – California Administrative Code (CAC) Title 22
  – Code of Federal Regulations (CFR)
  – Environmental Protection Agency (EPA)
  – FDA - Center for Devices and Radiological Health (CDRH)
  – Federal Communications Commission (FCC)
  – Food and Drug Administration (FDA)
  – International Electrotechnical Commission (IEC)
  – International Organization for Standardization (ISO)
  – Joint Commission
  – National Fire Protection Association (NFPA)
  – Occupational Safety and Health Administration (OSHA)
  – Office of Statewide Health Planning and Development (OSHPD)
  – The American National Standards Institute (ANSI)
  – Underwriters Laboratories, Inc.
A standard is a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose.

### Popular standards

**ISO 9000 - Quality management**

Make sure your products and services meet customers' needs with this family of standards.

[Learn more about ISO 9000](#)

**ISO 14000 - Environmental management**

Improve your environmental performance with this family of standards.

[Learn more about ISO 14000](#)

**ISO 45001 - Occupational Health and Safety**

Reduce workplace risks and create safer working environments.

[Learn more about ISO 45001](#)

**ISO 27001 - Information security**

Ensure your organization's information is secure with this family of standards.

[Learn more about ISO 27001](#)

**ISO 26000 - Social responsibility**

Help your organization to operate in a socially responsible way with this standard.

[Learn more about ISO 26000](#)

**ISO 50001 - Energy management**

Make energy savings and help make your organization more efficient with this standard.

[Learn more about ISO 50001](#)
Standards are made up of over 250 requirements summarized as

- Determine needs and expectations of interested parties
- Establish policies, objectives and work environment to satisfy needs of interested parties
- Design, resource and manage numerous interconnect processes to meet objectives and policy
- Measure and analyze effectiveness of each process in meeting its purpose and objectives
- Pursue continual improvement of the system through on-going evaluation of system performance
How can we make safe, reliable designs? How do we know what tests to perform?

- Advancement of Medical Instrumentation (AAMI)
- California Administrative Code (CAC) Title 22
- Code of Federal Regulations (CFR)
- Environmental Protection Agency (EPA)
- FDA - Center for Devices and Radiological Health (CDRH)
- Federal Communications Commission (FCC)
- Food and Drug Administration (FDA)
- International Electrotechnical Commission (IEC)
- International Organization for Standardization (ISO)
- Joint Commission
- National Fire Protection Association (NFPA)
- Occupational Safety and Health Administration (OSHA)
- Office of Statewide Health Planning and Development (OSHPD)
- The American National Standards Institute (ANSI)
- Underwriters Laboratories, Inc.
Examples of Standards in Biomedical Design

- Electronic medical devices have their own standard: IEC 60601: Medical Electrical Equipment

- Software projects should follow ISO 62304: Medical Device software – software life cycle processes (there is a similar standard through AAMI as well)

- All software should follow AAMI TIR32: Medical Device Software Risk Management
On Campus

Engineering Standards & Technical Papers

Standards and Technical Papers can be accessed in print at the Grainger Engineering Library

Search

SAI Global
A useful, broad search for standards, usually without access to full-text.

IHS Standards Expert
A useful, broad search for standards with full-text access to ASTM Standards only. Click the first link "IHS Standards Expert" on the gateway page.

Online Access (UIUC Patrons Only)

ASTM Standards
Click the first link — "IHS Standards Expert" — then check the "My Subscription" checkbox on the left to limit searches to ASTM standards.

SAE Technical Papers
SAE often reissues their standards as Technical Papers. If the standard you are looking for is not available as a Technical Paper a hardcopy may be at the Engineering Library.

IEEE Standards
IEEE Xplore Digital Library provides access to journals, books, papers and standards published by IEEE which includes some AIEE & ANSI standards.

OSHA Standards
Occupational Safety & Health Administration Law and Regulations page includes current standards.

Print Access

Print standards in Grainger Engineering Library are located on the west side of the first floor next to the Current Periodicals. Microfiche are on the lower level. Please ask at the Circulation / Reference Desk if you need help with a standard. Our collection includes a selection of standards from the following organizations:

ACI (American Concrete Institute)
ANSI (American National Standards Institute)
ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers)
AASHTO (American Association of State Highway and Transportation Officials)
ISO (International Organization for Standardization)
SAE (Society of Automotive Engineers) — the SAE often reissues their standards as Technical Papers.

http://search.grainger.uiuc.edu/top/standards.html
You can go directly to the regulatory page and find information:

http://www.aami.org/applications/search/
http://www.iso.org/iso/home/store/catalogue_ics.htm
http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm
FDA Recognized Consensus Standards Search Engine guides you to ones that they expect you to use.
Standards are constantly evolving

Device Security to Take Center Stage at AAMI 2017 Conference

Kevin Fu, a widely respected leader in the field of medical device security, has been selected to give the annual Dwight E. Harken Lecture during the AAMI 2017 Conference & Expo in Austin, TX, June 9–12. This general session honors the significant contributions that Harken, AAMI president from 1969–1970, made to medical science and technology.

Fu is chief scientist of Virta Labs, Inc. and an associate professor at the University of Michigan where he directs the Archimedes Center for Medical Device Security and the Security and Privacy Research Group. Virta Labs helps hospitals strategically manage cybersecurity risk for safety-critical inventory on clinical networks.

“This is a great honor,” Fu said. “I really appreciate AAMI recognizing the importance of the field, which is critical for the safety and effectiveness of medical devices.”

In hospitals today, it would be difficult to find medical device technology that does not critically depend on computer software. Network connectivity and wireless communication have transformed the delivery of patient care. But connectivity comes at a price—vulnerability to hackers, viruses, and other malware.

Since federal regulators began tracking major health data breaches, more than 1,700 incidents impacting nearly 170 million people have been posted to the Department of Health and Human Services Office of Civil Rights’ breach portal. More than 90 hacking incidents were reported in 2016 alone.

“I think things will continue. Delivery organizations and devices were not designed co-chaired by Ken Huang.”

During his presentation, Fu plans to probe the risks, benefits, and regulatory issues for medical device cybersecurity and provide insight into the development of trustworthy medical device software.

“I hope that people will come out of my presentation with a less sensational view of the issues and a more optimistic view of the future of medical device security,” Fu said. “It’s not about eliminating risk but about controlling and managing risk. It can be done—it’s not impossible.”

Registration for AAMI 2017 is now open, and those who register before March 20 will receive an “early bird” discount. For more information, visit www.aami.org/ac.

“Most medical devices were not designed with security in mind, and we’re still trying to catch up”
The Engineers Role in ISO 9000

• ISO 9000 does not prescribe a specific approach
  – Organization can design the process as efficient or inefficient as desired

• ISO 9000 does require 21 categories of records be maintained
  – Design review
  – Design validation
  – Management review
  – Internal quality audit
Clause 7.3.1- Design and Development Planning “During design and development planning, the organization shall determine”

- Design and development stages
- Review, verification, validation that are appropriate to each design phase
- Responsibilities and authorities for design and development
Design Controls
“input is really a list of requirements from customers (either direct from customer or indirect through market studies), tempered by realities of budget, competition, capability, capacity, government regulation”
– Wes Bucey, Medical Device Consultant
Design Output

*Design output:*  
– Means the results of a design effort at each design phase and at the end of the total design effort.  
– The finished design output is the basis for the device master record  
– Finished design output consists of the device, its packaging and labeling, and the device master record.

*Specification:*  
means any requirement with which a product, process, service, or other activity must conform
The Engineers Role in ISO 9000

• Clause 7.3.5- Design and Development Verification “Verification shall be performed in accordance with planned arrangements (7.3.1) to ensure that the design and development outputs have met the design and development input requirements” “Records of the results of the verification and any necessary actions shall be maintained”
After decades of working with ISO and FDA/CE Mark Standards, they have integrated into their own ISO standard

ISO 13485:2016 Medical devices -- Quality management systems -- Requirements for regulatory purposes

QMS Standard for medical devices, general quality system requirements modified for highly regulated medical device industry (from ISO 9001)

Input from FDA, HealthCanada, Euro CE Mark, etc.
Table of Contents for ISO 13485:216

- 1 Scope
- 3 Terms and definitions
- 4 Quality management system
  - 4.1 General requirements
  - 4.2 Documentation requirements
  - 5.6 Management review
  - 6.2 Human resources
  - 6.3 Infrastructure
  - 6.4 Work environment and contamination control
  - 7.1 Planning of product realization
  - 7.2 Customer-related processes
  - 7.3.2 Design and development planning
  - 7.3.3 Design and development inputs
  - 7.3.5 Design and development review
  - 7.3.6 Design and development verification
  - 7.3.7 Design and development validation
  - 7.3.8 Design and development transfer
  - 7.3.9 Control of design and development changes
  - 7.3.10 Design and development files
- 7.4.1 Purchasing process
- 7.4.2 Purchasing information
- 7.4.3 Verification of purchased product
  - 7.5.1 Control of production and service provision
  - 7.5.2 Cleanliness of product
  - 7.5.4 Servicing activities
  - 7.5.6 Validation of processes for production and service provision
  - 7.5.7 Particular requirements for validation of processes for sterilization and sterile barrier systems
  - 7.5.8 Identification
  - 7.5.11 Preservation of product
- 8.2.1 Feedback
- 8.2.2 Complaint handling
- 8.2.3 Reporting to regulatory authorities
- 8.2.6 Monitoring and measurement of product
- 8.3 Control of nonconforming product
- 8.4 Analysis of data
- 8.5.2 Corrective action
- 8.5.3 Preventive action
7.3.7 Design and Development Validation

- Planned & documented arrangements
- Plan includes: Method, acceptance criteria and statistical technique with rationale for sample size
- Connection to other devices
- Report includes: Results (same) and conclusions (new)
- Clinical/performance evaluation not released for use (from notes in the 2003 version).
- Use of production units (representative product)/document equivalency (rationale for choice of product)
- Clinical evaluation or performance evaluation in accordance with regulatory requirements.
Traceability + objective evidence = everything!!
You MUST Address any and all standards related to your design

• Everyone should address at least ISO 9000 quality control through design process

• Most will need to address AAMI and/or FDA

• This must be included in your final reports and would be something good to test in spring for Six Sigma or other user studies