Safety For Surgical Robotics

Arjang Hourtash
2009-Sept-12

Overview

- My Background
- daVinci Si
- Safety
- Q&A

My Background

- BS Nuclear Engineering, University of California, Santa Barbara
- MSME (Dynamics), University of California, Santa Barbara
- PhD ME (Robotics & Control), University of California, San Diego
  - Thesis: Path Planning for Manipulators.

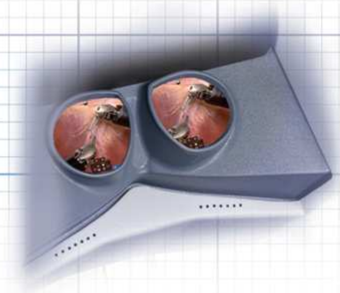
- Mechanical Design: Hewlett-Packard (Inkjet printers)
- Manipulator Kinematics and Dynamics Analyses and Simulations: NASA Johnson Space Center

- daVinci Si Master Manipulator: Control, Analysis, Calibration: Intuitive Surgical (2007 - Present)
  - http://www.intuitivesurgical.com

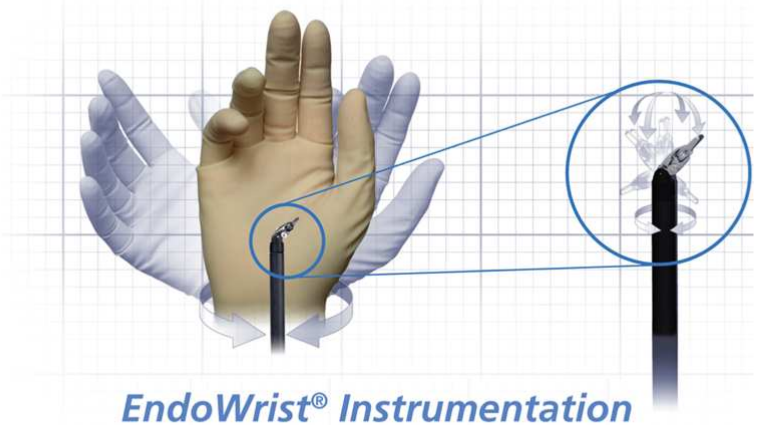
daVinci Si

Fundamentally New Capability

Intuitive® Motion



3D HD Vision



EndoWrist® Instrumentation

INTUITIVE SURGICAL®

Master Manipulators

daVinci Si

INTUITIVE SURGICAL

First Impressions

"… A (((ROBOT))) is going to operate on me??? …"

INTUITIVE SURGICAL

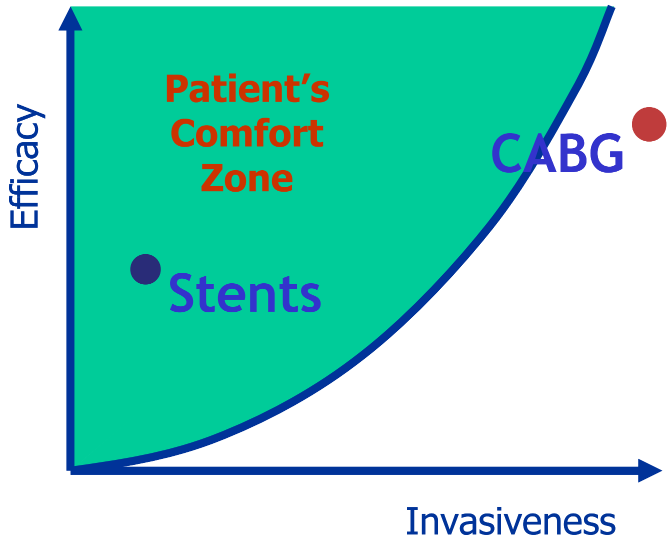
ISI Priorities

1. Patient Value
2. Surgeon Value
3. Hospital Value
4. Employee Value
5. Stockholder Value

Patient's Perception of Value

An imprecise equation with no defined units, but work with me…

$$Value = \frac{Efficacy}{Invasiveness^2}$$

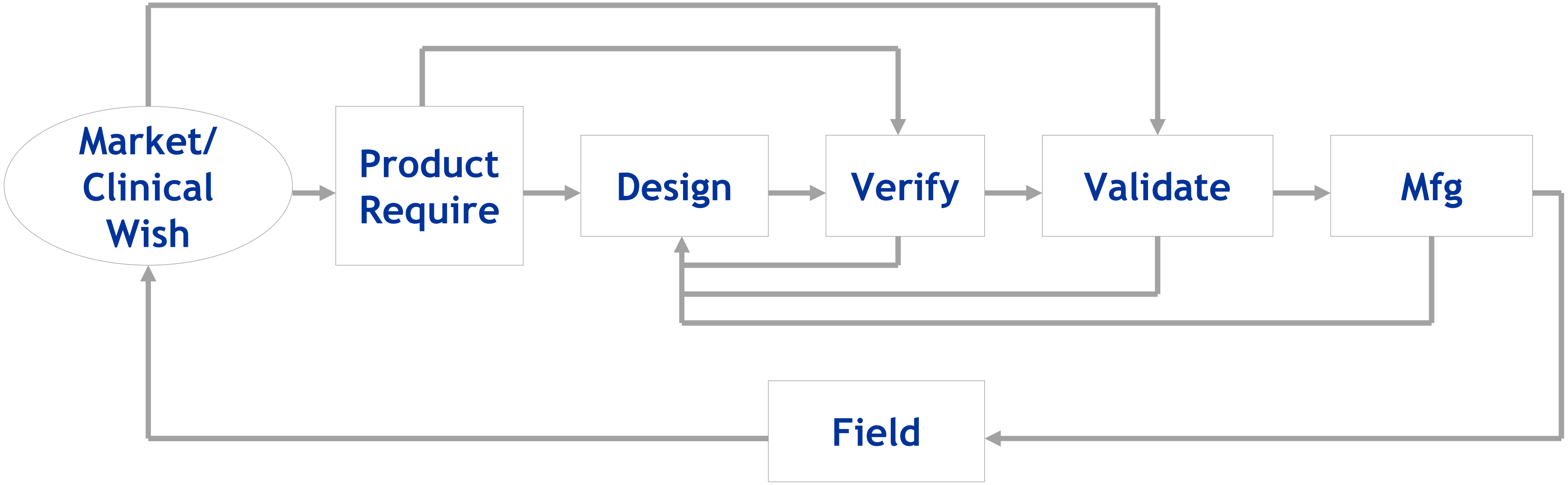


You mean my chances of cure are only 5% better if you cut me open, versus taking this pill? I'll take the pill and take my chances!!

Safety

- Failures and Risk Analysis
- Design for Safety
- The Designer

Design Process



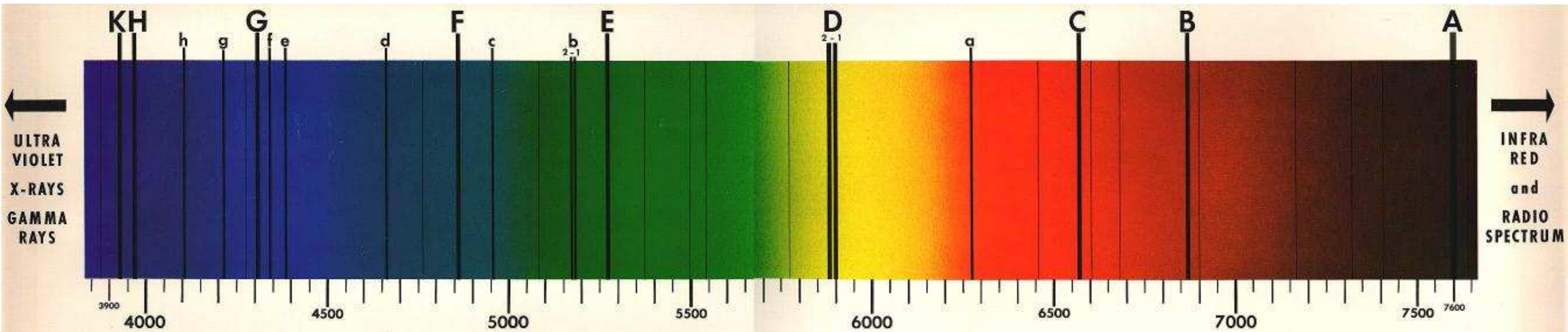
INTUITIVE SURGICAL

Product Requirements

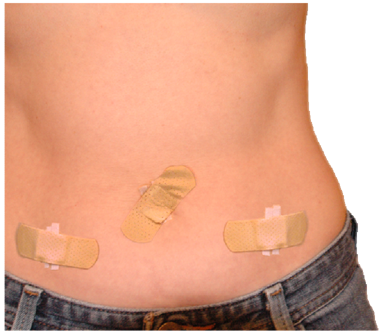
Examine potential risks:

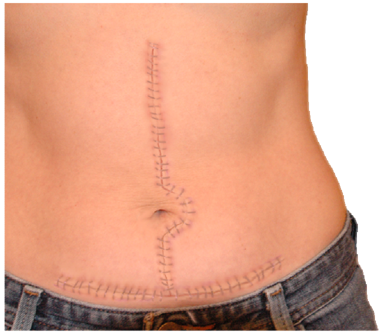
1. Failure to design something that is buildable.
2. Failure to consistently manufacture the design.
3. Failure in the field due to reliability.
4. Failure in the field resulting in safety hazards.

1 2 3 4



Safety Related Failures



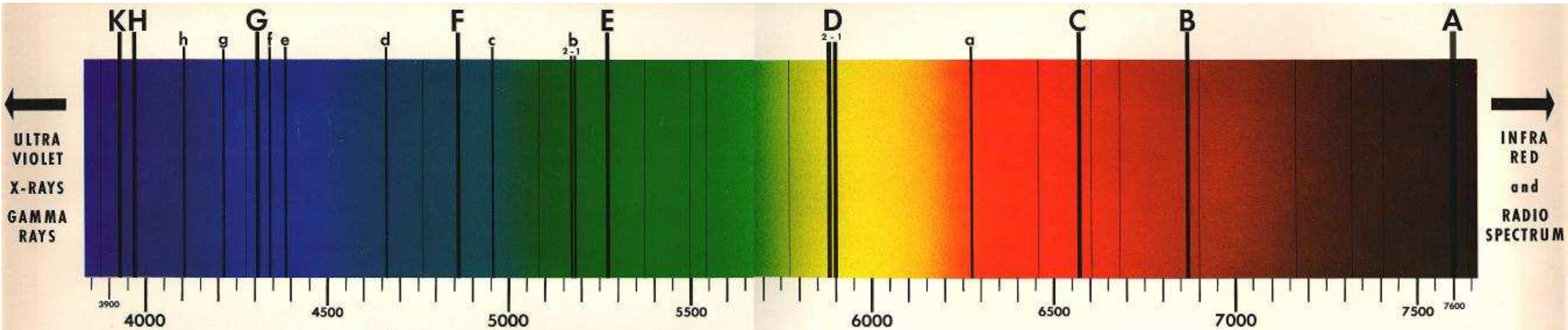


Measurements: Injuries, Converts, & Aborts.

Failures due to:

1. Technical shortcoming.
2. Incorrect system behavior.
3. Usability due to poor User Interface.
4. Lack of use (surgeon frustration, confidence).
5. Surgical error.

1 2 3 4 5



Risk Analysis

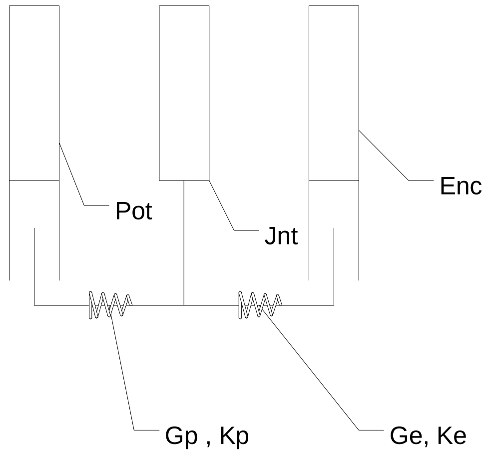
- Risk Prioritization:
  - Probability of Occurrence
  - Degree of Severity
  - Probability of Detection
  - Composite = (PO) x (DS) x (PD) < (Threshold)

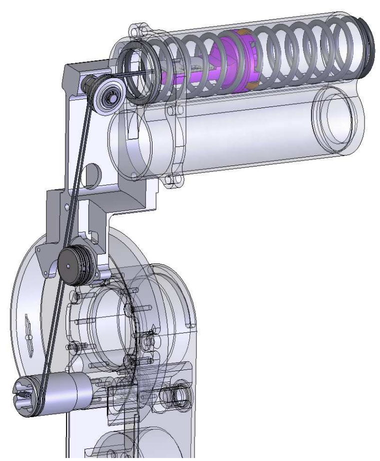
- Top-down: Clinical Risks: Hazards of the robot features in the clinical environment.
  - Uncontrolled motion
  - Uncontrolled applied load
  - Non-intuitive motion

- Bottom-up: Sub-system failure risks: Failure Modes and Effects Analysis (FMEA).
  - Sensor failure
  - Communication link failure
  - Cable break

Design For Safety (1)

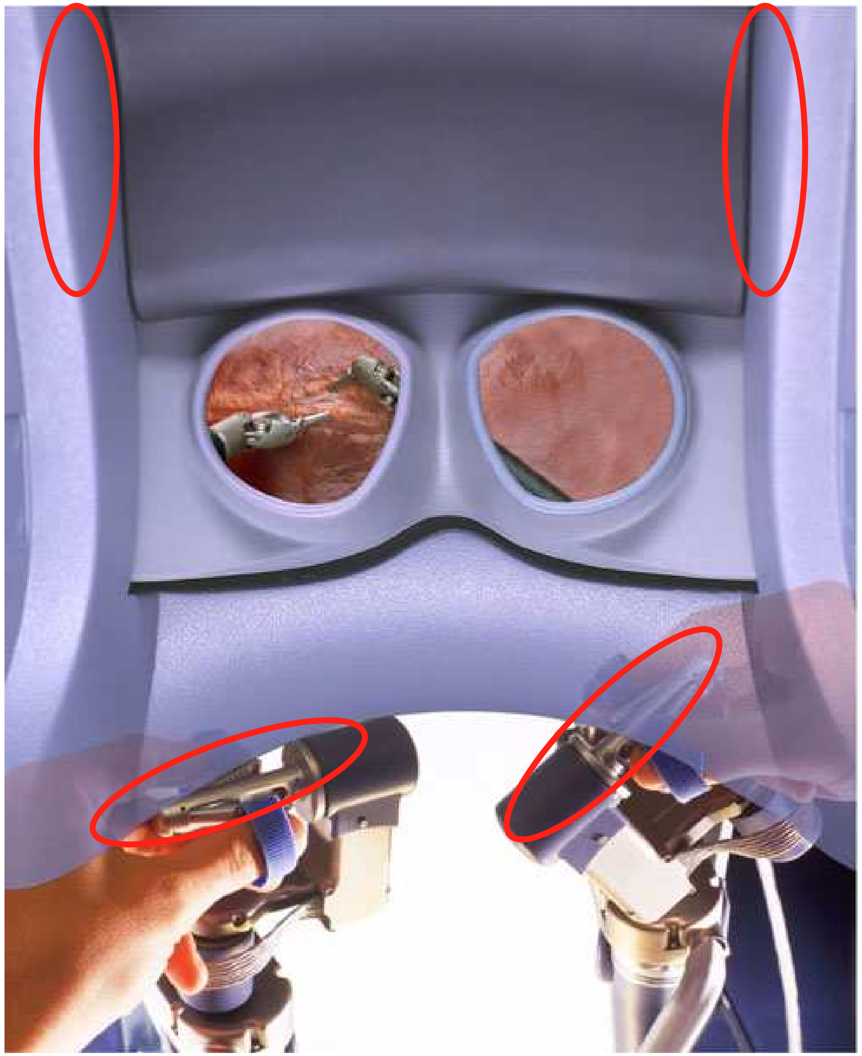
- Redundant sensors
  - Mechanical coupling
  - Resolution
  - Latency
- Redundant transmission
  - Single-failure operation
- Use of brakes





Design For Safety (2): Algorithms

- Risk mitigation using interlocks and UI logic
- Startup health tests
- Math models of healthy subsystems
- Redundancy in calculations
- Multiple bit gates: (10100101) instead of just (1) for TRUE
- Sensor health monitoring
- Communication link monitoring
- Voltage supply monitoring
- CRC and checksum
- Watchdogs



Signal Lifecycle: Sensor → Actuator

1. Sensor output is read.
2. Check sensor output to be within lower and upper bounds.
3. Check sensor health monitoring.
4. Check health of signal transmission (CRC, other monitors)
5. Compare with redundant sensor.
6. Compare with math model.

7. If all is OK, use to generate actuator input.
8. Compare with redundant calculation.

9. Check actuator input to be within lower and upper bounds.
10. Compare with math model.
11. If all is OK, output to actuator.

Fault Handling

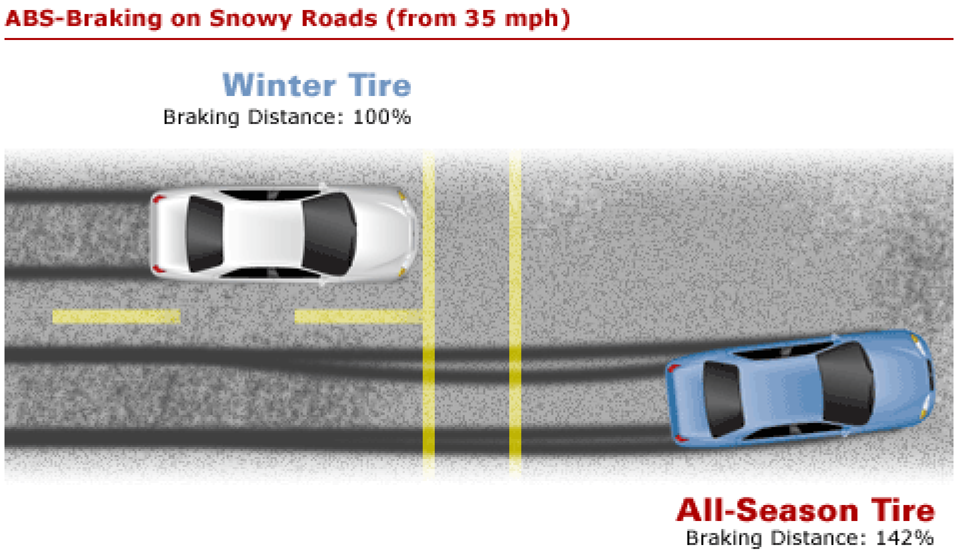
- Fast Faults:
  - Timeline of a servo cycle.
  - Example: Encoder stops counting.
  - System must intervene.

- Slow Faults:
  - Timeline of several seconds or slower
  - Example: Gravity compensation is out of calibration.
  - Human judgment is often required.

Fast Fault Handling

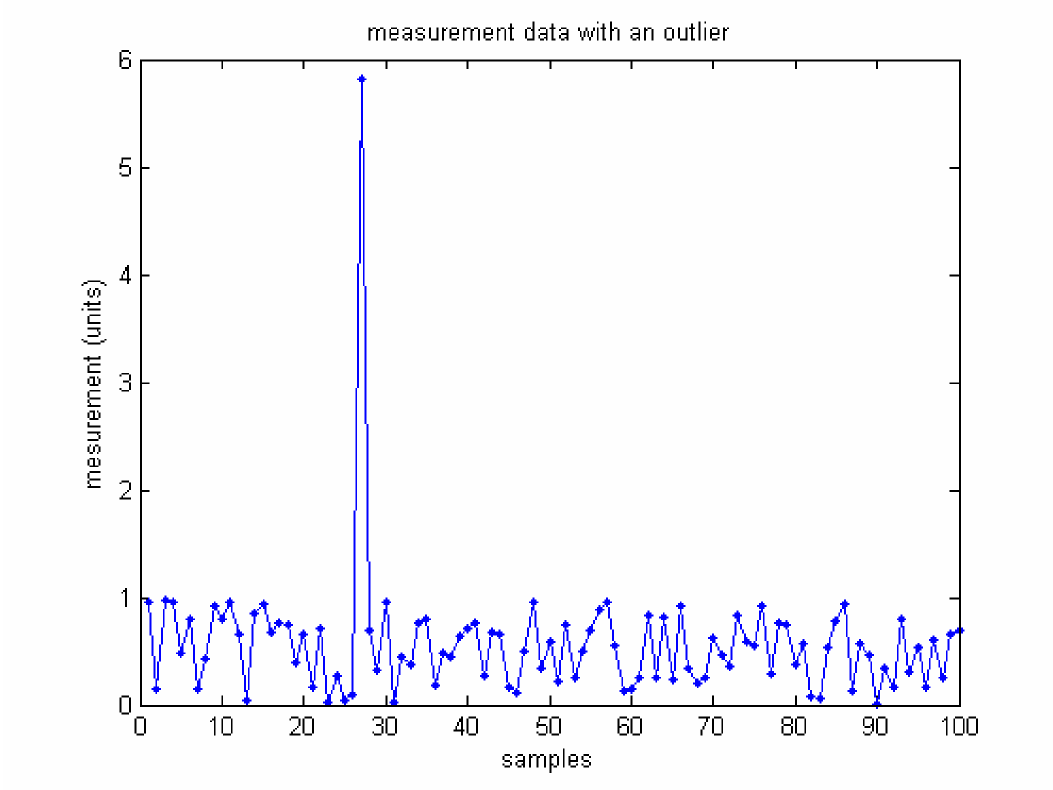
Safe State controlled by Fault Reaction Logic (FRL):

- Available to software at all times
- Power bus is shorted to ground by fail-safe hardware relay
- All manipulator motors are unpowered
- All manipulator motors are shorted to provide regenerative braking
- Brakes are activated to stop motion
- Critical stopping distances must be met



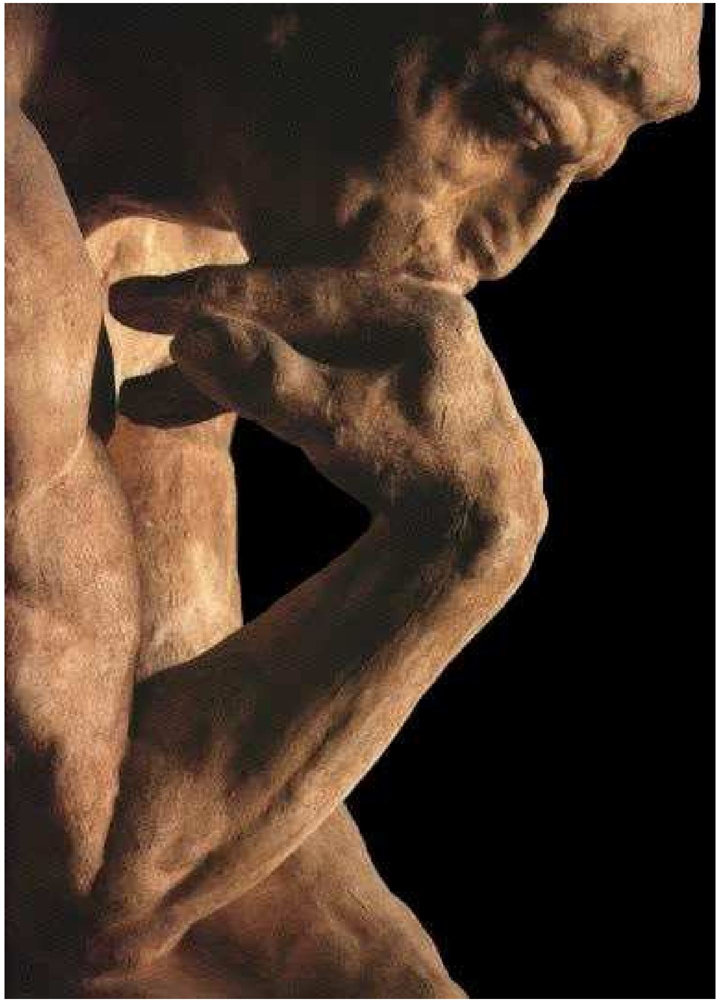
Verification & Validation

- Verify that the design function has been met.
- Verify that the clinical objective has been met.
- Outliers?



The Designer: Habits / Discipline

Sow a thought and you reap an action. Sow an act and you reap a habit. Sow a habit and you reap a character. Sow a character and you reap a destiny.



- Use software to test your source code:
  - Lint
  - Memory Leaks, Uninitialized Variables, …
  - Static Source Code Verification
- Identify good programming habits.
- Use checklists to remind yourself to reinforce the habits.
- Write scripts for enforcing habits:
  - If-else, switch-default
  - Check arguments to functions with limited domain
    - sqrt( ), log( ), asin( ), acos( ), "/"
- Regression tests
- Process for layers of other people to systematically test your code.

Q&A


VULTURES
© copyright: Hadi Farahani
"We just ignore them. They never harm living people!"