THE MORE THINGS CHANGE, THE MORE THINGS STAY THE SAME

John Knight

Department of Computer Science

University of Virginia

Meeting Statement

In many ways, dependability for medical devices is more challenging than for transportation and infrastructure systems. Human physiology is a far more varied and variable environment than air or space, especially when the patient is ill, and many devices may be attached to and interacting through a network implicitly including the patient. The devices are often operated by doctors, nurses, and patients rather than technical specialists, and a single hospital may be responsible for managing thousands of devices of widely different types and configurations, which are often attached to networks.

The device industry spans a wide range of capabilities in software development, human factors, dependability engineering and safety culture, and quirks in the regulatory framework complicate adoption of modern approaches to software and system assurance. On the other hand, medical devices provide great social benefit and also are among the most innovative and fastest growing applications of cyber-physical systems.

Let’s Examine This Statement

Transportation System

In many ways, dependability for medical devices is more challenging than for **transportation** and infrastructure systems.

Infrastructure System

In many ways, dependability for medical devices is more challenging than for transportation and **<u>infrastructure</u>** systems.

Norfolk Southern

CSX

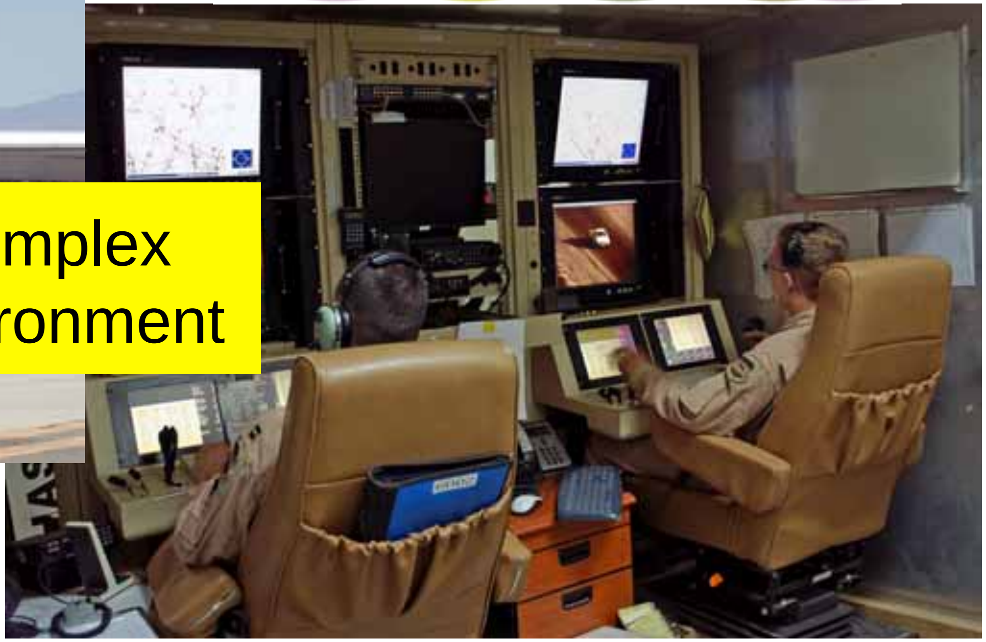
Meeting Statement

In many ways, dependability for medical devices is more challenging than for transportation and infrastructure systems. Human physiology is a far more varied and variable environment than air or space, especially when the patient is ill, and many devices may be attached to and interacting through a network implicitly including the patient. The devices are often operated by doctors, nurses, and patients rather than technical specialists, and a single hospital may be responsible for managing thousands of devices of widely different types and configurations, which are often attached to networks.

The device industry spans a wide range of capabilities in software development, human factors, dependability engineering and safety culture, and quirks in the regulatory framework complicate adoption of modern approaches to software and system assurance. On the other hand, medical devices provide great social benefit and also are among the most innovative and fastest growing applications of cyber-physical systems.

Unmanned Aircraft System

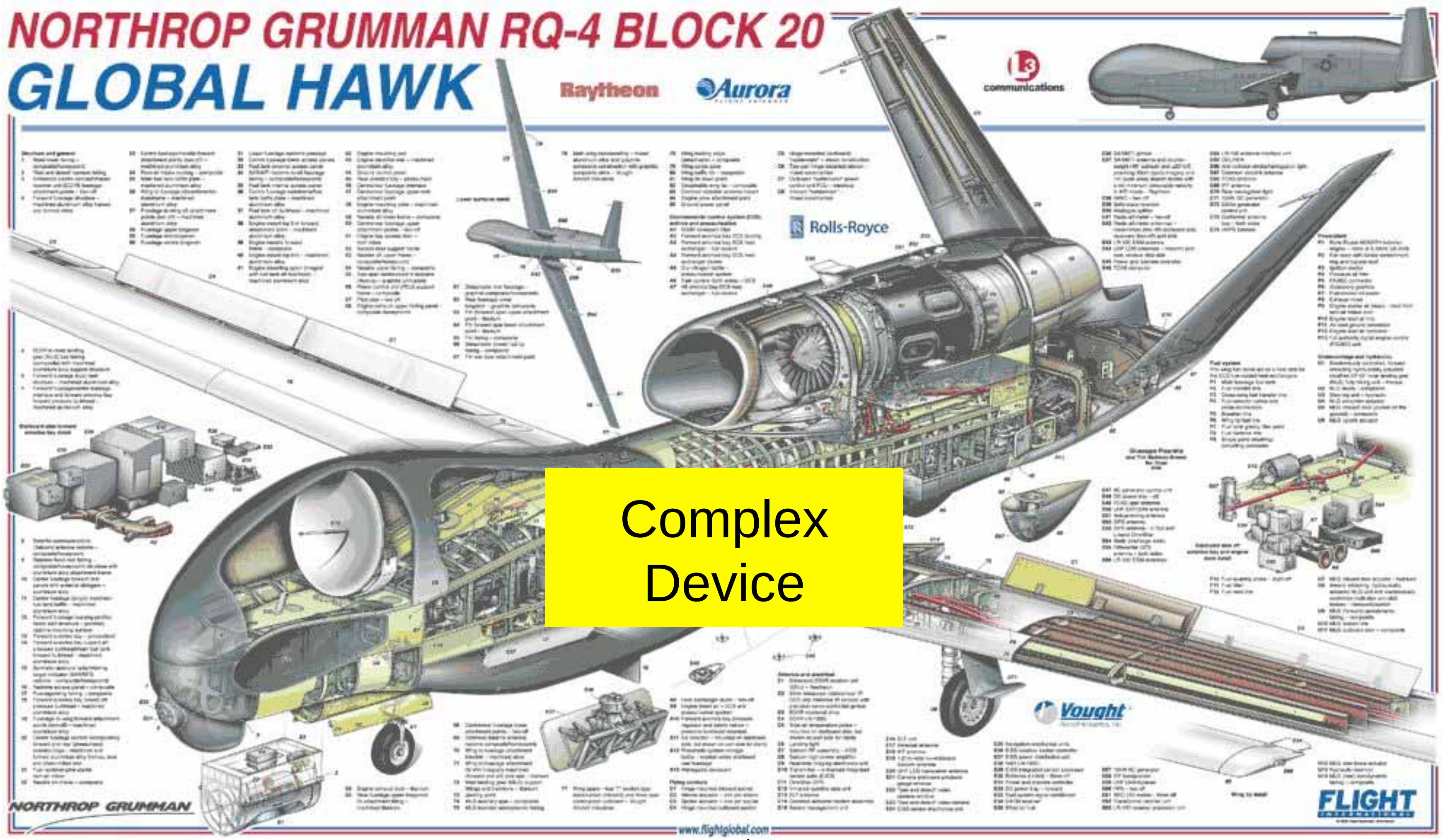
Human physiology is a far more **varied** and variable environment than **air** or space,



Complex Environment

USAF Global Hawk

Global Hawk Architecture



Complex Device

Lufthansa Flight 2904

- Airbus A320
- September 1993
- Landing in Warsaw
- Overran runway

- Landed above speed and banked because of expected cross wind
- Wind turned to tailwind
- Left landing gear touched d[illegible] seconds after right
- Prevented braking and thrust reversers—weight on wheels check
- ***Why were the circumstances not monitored?***

Complex Environment

British Airways Flight 38

- Beijing to London
- January 2008
- Engines failed to throttle up on flare
- Fuel system frozen and fuel flow blocked
  - Design defect
  - Human errors
- No serious injuries
- ***Why were the circumstances not monitored?***

Complex Environment

Meeting Statement

In many ways, dependability for medical devices is more challenging than for transportation and infrastructure systems. Human physiology is a far more varied and variable environment than air or space, especially when the patient is ill, and many devices may be attached to and interacting through a network implicitly including the patient. The devices are often operated by doctors, nurses, and patients rather than technical specialists, and a single hospital may be responsible for managing thousands of devices of widely different types and configurations, which are often attached to networks.

The device industry spans a wide range of capabilities in software development, human factors, dependability engineering and safety culture, and quirks in the regulatory framework complicate adoption of modern approaches to software and system assurance. On the other hand, medical devices provide great social benefit and also are among the most innovative and fastest growing applications of cyber-physical systems.

Regulation

and quirks in the regulatory framework complicate adoption of modern approaches to software and system assurance

- Not a technical issue
- I don’t understand why this remains the case

What Is Different?

- Safety critical domains differ in ***<u>many</u>*** ways:
  - Consequences of failure
  - Safety requirements
  - Hazards
  - Types of fault to which they are subject
  - System designs
- Devices differ in ***<u>many</u>*** ways:
  - Functionality
  - Users/consumers
- Medical devices are “different” in ***<u>all</u>*** of these areas
- But so are ***<u>all</u>*** safety-critical systems

Medical Devices Are ***Different*** And So Face The ***Same*** Challenges As Other Systems

What Is The Same?

- Medical devices are safety-critical systems
- **<u>All</u>** safety-critical systems are:
  - Complex
  - Difficult to design
  - Difficult to assess
  - Technical challenges of the first order
- But:
  - Many powerful technologies developed
  - Technologies that should be used are not used

Safety Engineering

- Sophisticated branch of engineering
- Extensive – many tools and technologies:
  - Hazard identification and analysis
  - FTA, FMECA, HazOp, PRA, safety cases, etc.
- Proven in many domains and on many systems:
  - Aerospace
  - Nuclear
  - Transport
- But there remain things we cannot do:
  - E.g., quantification of residual risk levels

But…

I actually think the meeting statement is right…

The question is: what makes medical systems more challenging?

Medical System Dependability

- ***Is*** more challenging than aerospace and infrastructure system dependability
- Systems are more complex
- Dependability:
  - Safety is harder to achieve
  - Security is ***much*** harder to achieve
- Defining the difference and the associated challenges is the critical first step
- I think there are two ***core*** differences

Crucial Difference: Automation

Automation Spectrum

Aerospace:

- Automation:
  - **Auto**pilot
  - **Auto**throttle
  - **Auto**land

Interconnection is a small but important part of the problem

Medical:

- Automation:
  - Support not replacement
  - Decision proces... and pro... es derive
  - fr... man in...
- Contro...
  - Poorly u...

We tend not to discuss autosurgeons

Crucial Difference: Access

- Security:
  - Can affect safety
  - Confidentiality with appropriate access is a unique problem
- Security is a problem for all devices, esp. networked devices
- At least as hard as “traditional” safety concerns
- Medical confidentiality is really hard (perhaps the hardest):
  - Unknown access control requirements
  - Information with:
    - No financial value (unlike SSNs and credit card numbers)
    - Ultra high privacy “value”

Shameless Self Promotion

- Two of my projects
- Both apply safety and computer engineering to medical systems as case studies
- **Project 1** **(inspired by a talk by Julian Goldman)**:

Application of safety engineering to patient environment

- **Project 2** **(inspired by history of software failure)**:

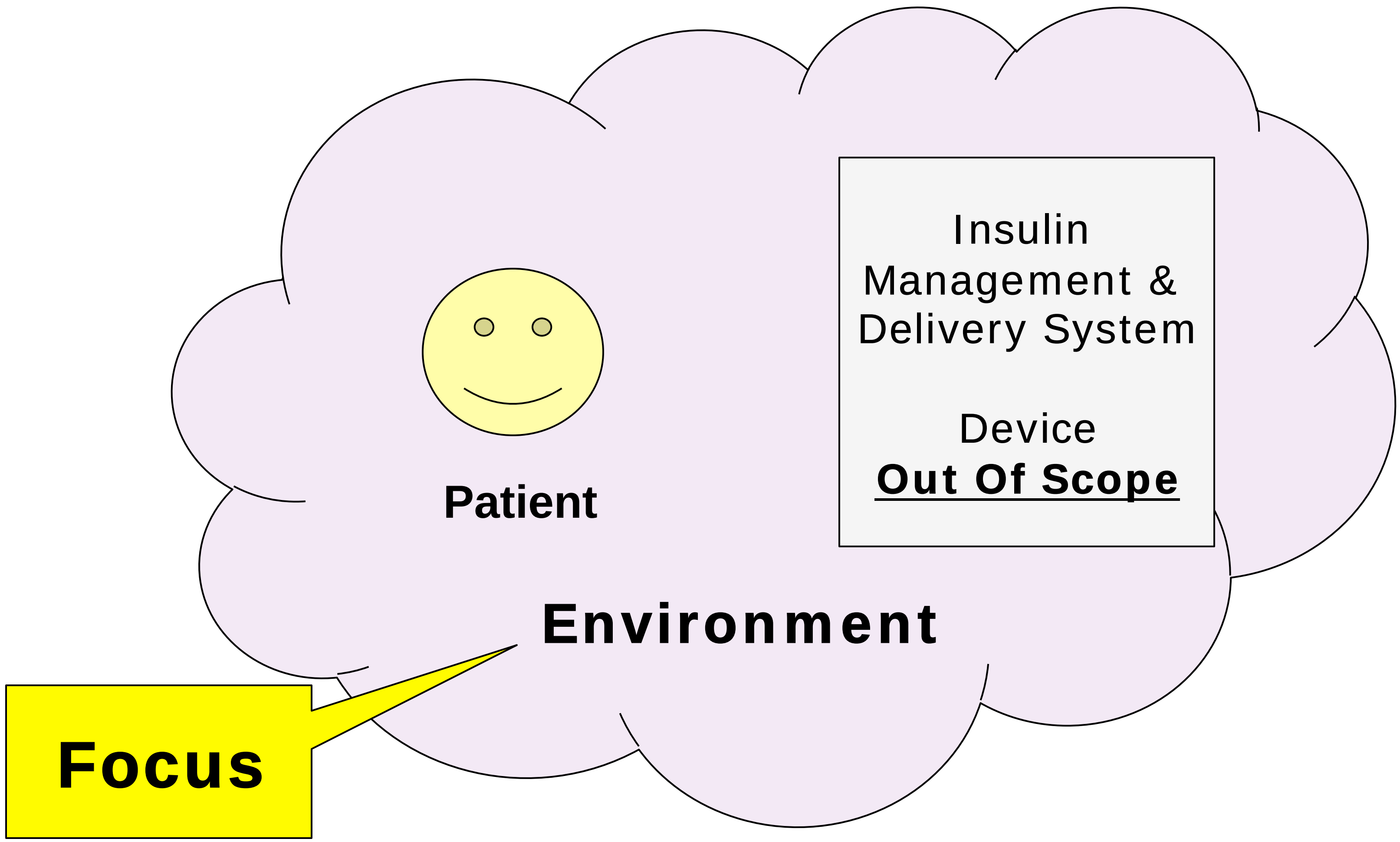
Assessment of limits of software dependability for a medical device

Project 1: DAIS

Diabetes Automated Information System

- Challenge:
  - *Type 1 diabetic patient*
  - *Competent, intelligent young person*
  - *Lives alone*
  - *Has had serious incidents of hypoglycemia*
- What would we find if we applied comprehensive safety engineering?
- **Could we cut risk of hypoglycemia?**

DAIS Goal


Insulin
Management &
Delivery System

Device
Out Of Scope
Patient
Environment
Focus

DAIS Safety Engineering

- Hazard identification
- Hazard analysis
- Fault-tree analysis
- Restricted PRA (some probability estimates)
- Development of:
  - System risk mitigation techniques
  - Revised system analyses
  - System design

So What Did We Find?

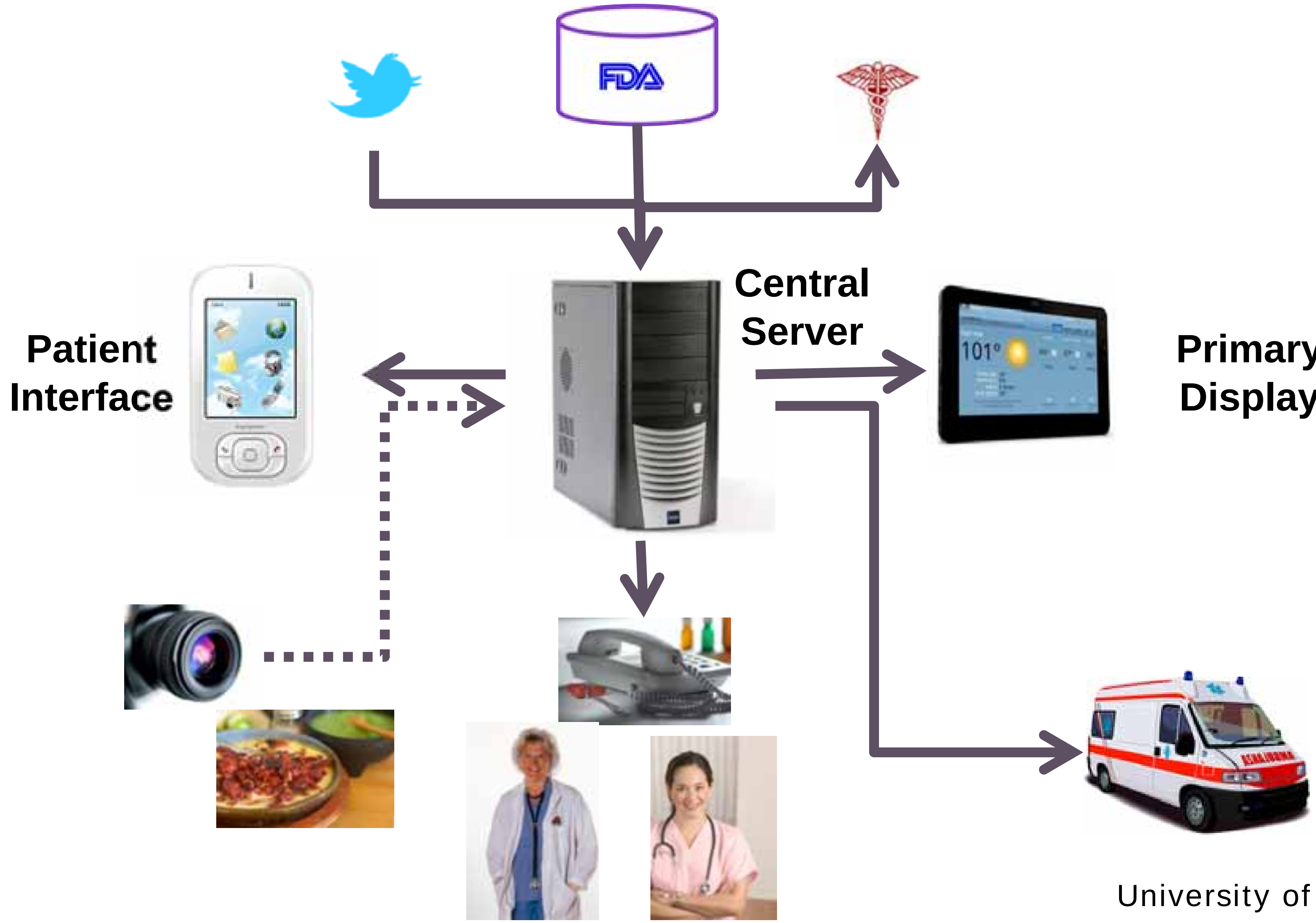
- Patient had no idea
  - Patient needs help
  - Supporter unable to
- Patient medication
  - Insulin sensitivity af
  - Multiple hypoglycer
- No consideration of e
  - Pump failed at 10:3
  - No backup plan to maintain blood glucose control
- Etc.

Safety Analysis Yielded **Dozens** Of Events That Could Injure The Patient

Almost All Are **Easily** Preventable

DAIS Is Designed To Do That

DAIS Prototype Design



Lessons Learned

- We know a lot about the risk exposure of the patient
- We are convinced that the residual risk has been reduced to ALARP levels
- We are convinced that the risk reduction is worthwhile and significant

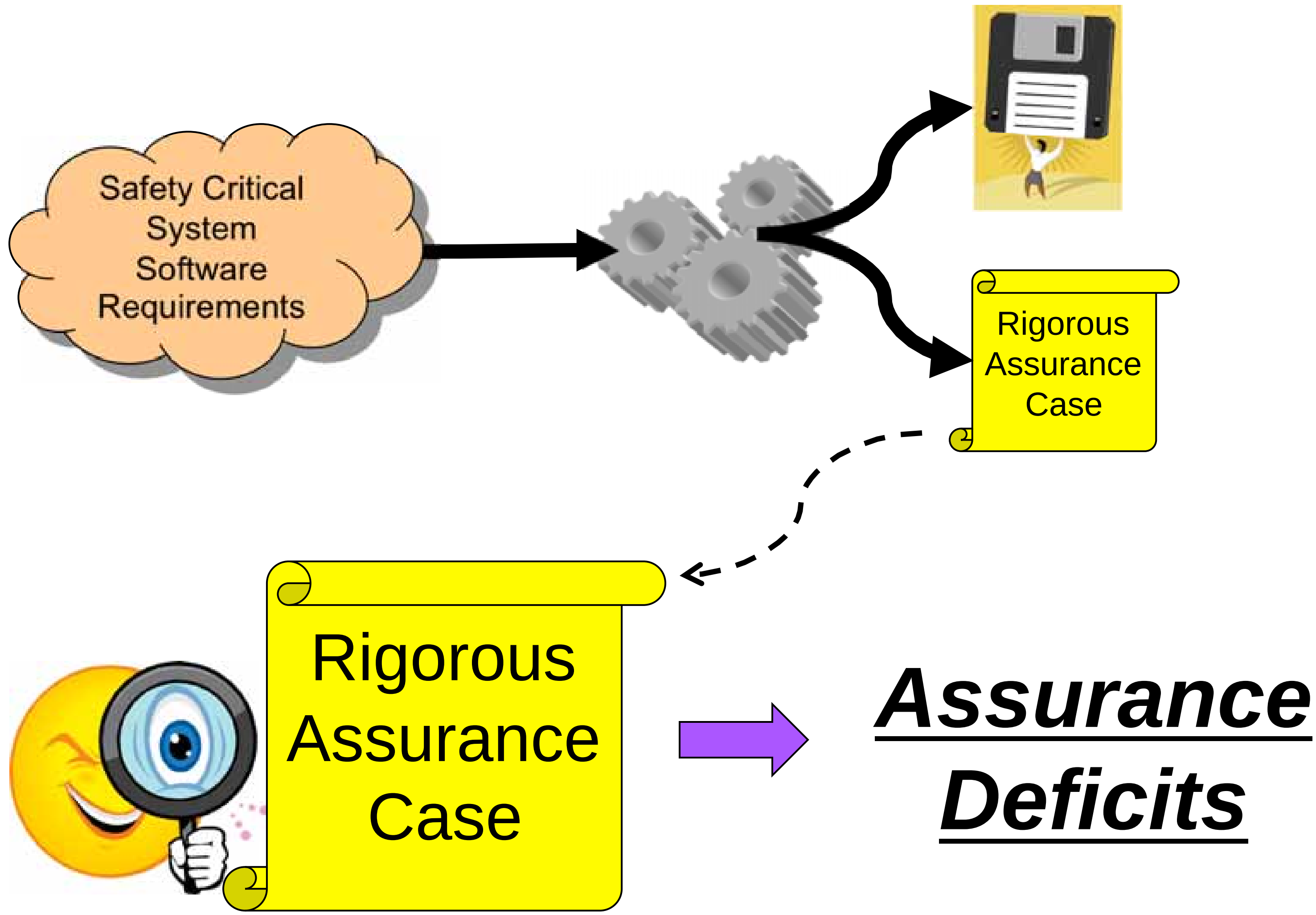
Rigorous application of safety engineering to some medical systems can be effective at reducing residual risk

Project 2: Perfect Software

- Many medical systems are software intensive
- Many accidents and incidents have had software as a causal factor
- ***Why*** is software imperfect?
- Would “better” development and analysis techniques help?
- Is software somehow ***inherently*** less dependable than we would like?

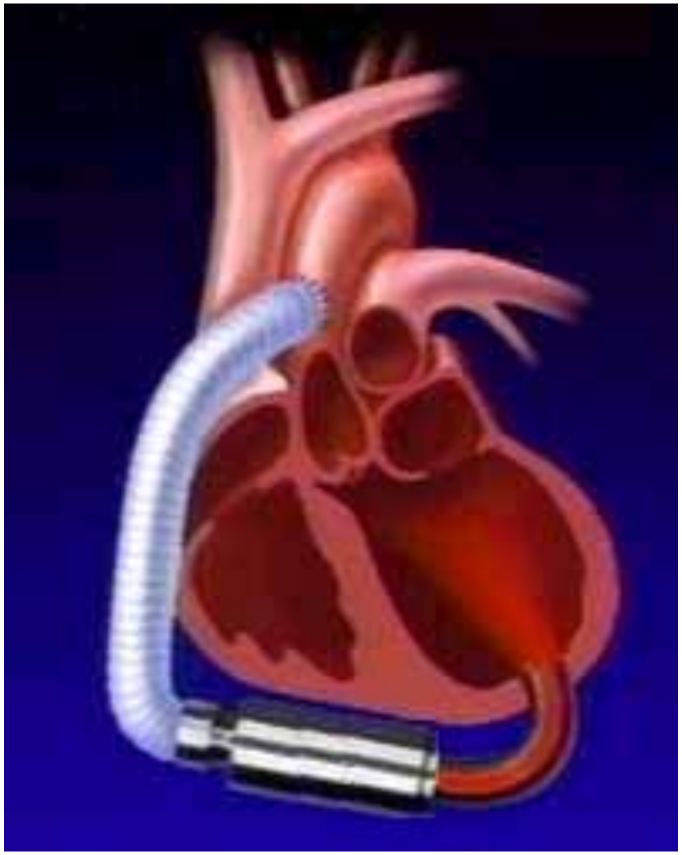
We did an experiment to see

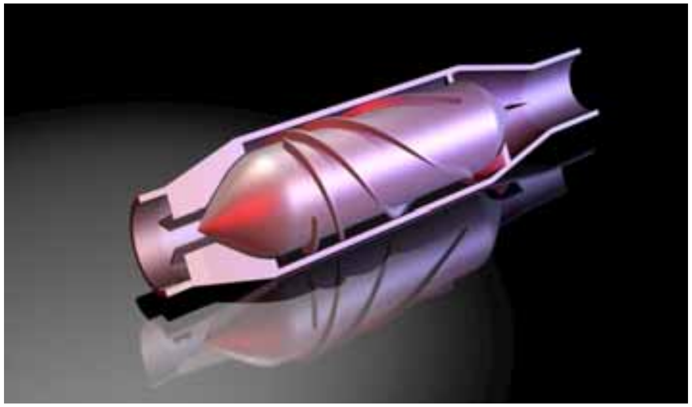
Design of the Case Study



Example: LVAD

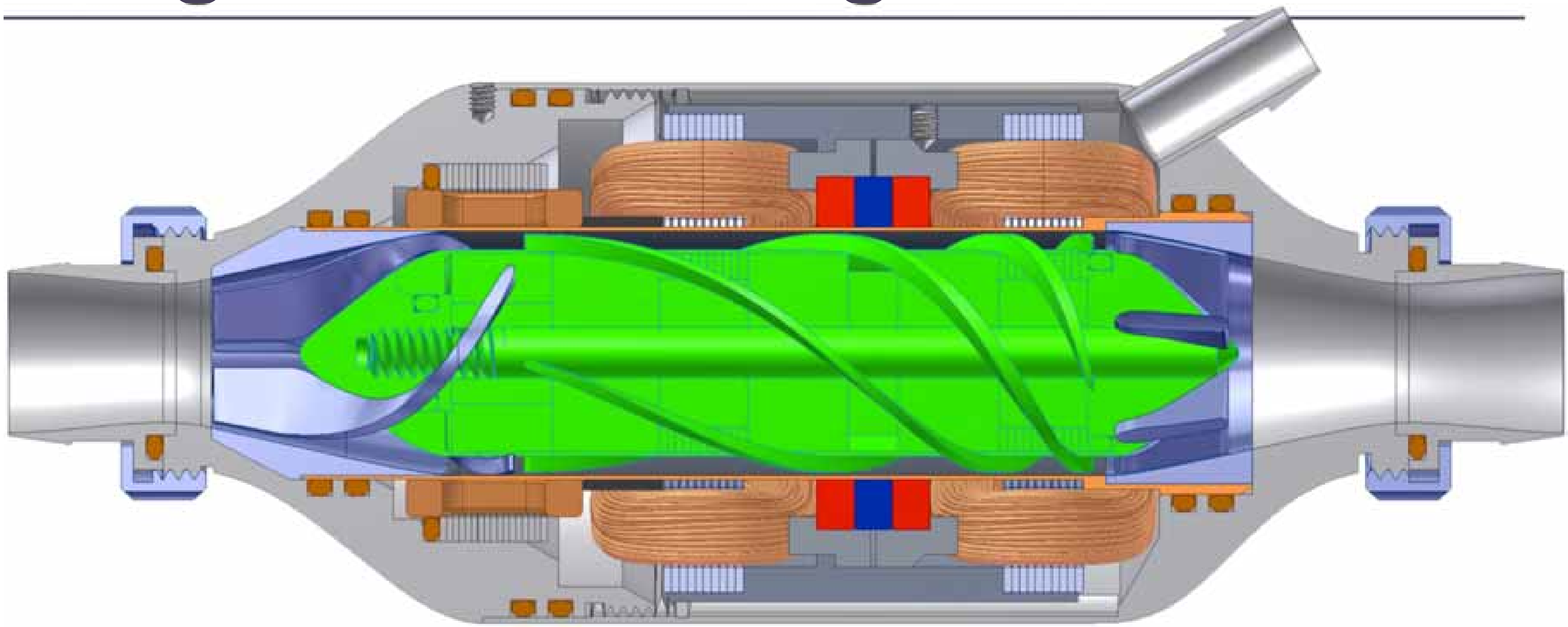
- Left Ventricular Assist Device





- **Magnetic bearings**
- Continuous-flow axial design
- Less blood damage than current models

Magnetic Bearing Control



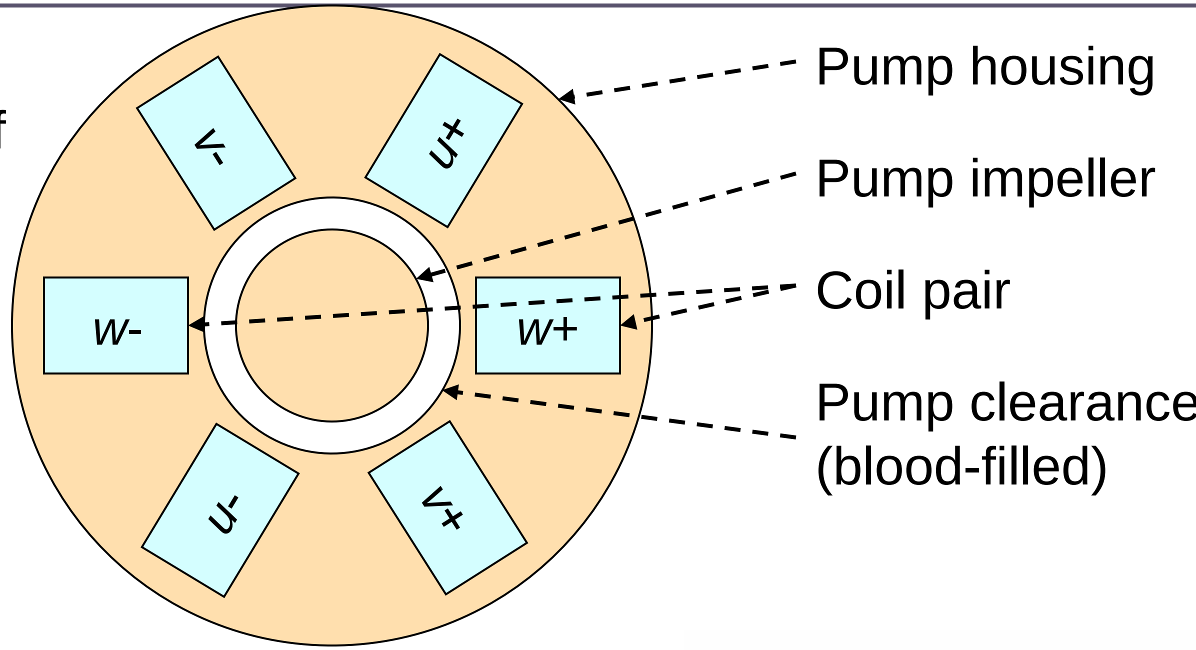
- Compute control updates in hard-real-time (5 kHz)
  - State-space control model, 16 states
- **No more than 10^{-9} failures per hour of operation**

Active Mag Bearing Controller

Magnetic bearing controller is part of larger LVAD system.

LVAD's goal: adequately support patient's circulation.

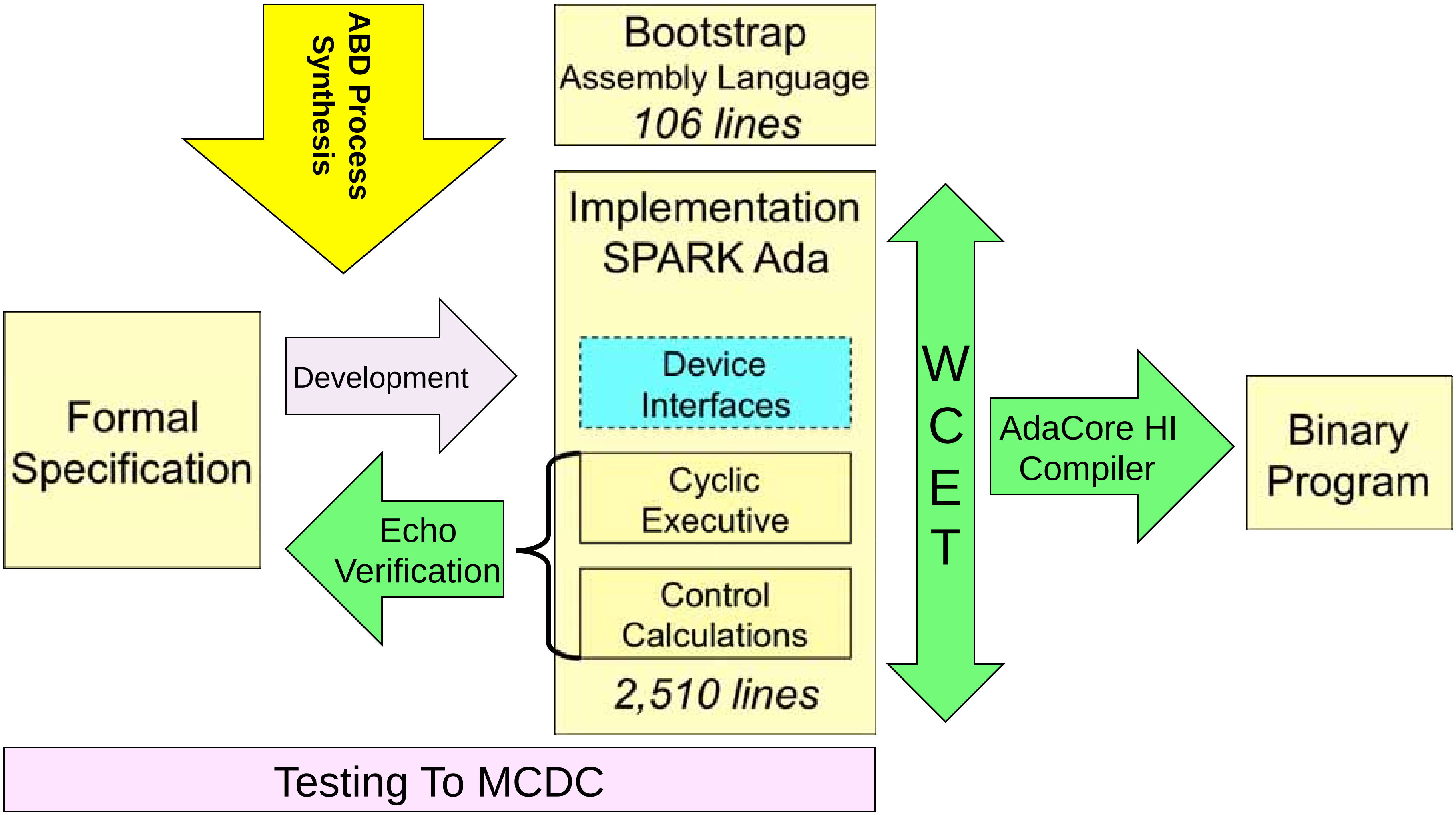
Some responsibility falls on magnetic bearings.



Target:

Freescale MPC5554
+ custom DACs
No system software

Overall Development Process



Assurance Deficits

- Reliance upon:
  - Correct requirements
  - Reliable human-to-human communication
  - Understanding the semantics of formalisms
  - Reviews or inspections
  - Human compliance with protocols
  - Unqualified tools
  - Tools that lack complete hardware models
  - Testing
  - Human assessment of dependability
- The unavoidable use of low-level code
- The ability to verify floating-point arithmetic

Not Specific To Medical Devices

Core Software Dependability Research Problems

Proposed Research Agenda

Safety

- Devices:
  - Existing safety engineering is mostly sufficient
- Systems:
  - Existing safety engineering is:
    - Useful start
    - Not up to the challenge
  - Devices need to accommodate
  - Some directions seem useful:
    - Formal specification
    - Model checking
    - Property proofs

Security

- Devices:
  - Existing security engineering is mostly sufficient
- Systems:
  - Existing security engineering is:
    - Useful start
    - Far short of the challenge
  - Devices need to accommodate
  - Sizes of systems and complexity of systems define the challenge
  - Need serious basic research

Contact

- E-mail address:

  knight@cs.virginia.edu

- For more information see:

  http://www.cs.virginia.edu/knight/

  http://dependability.cs.virginia.edu/