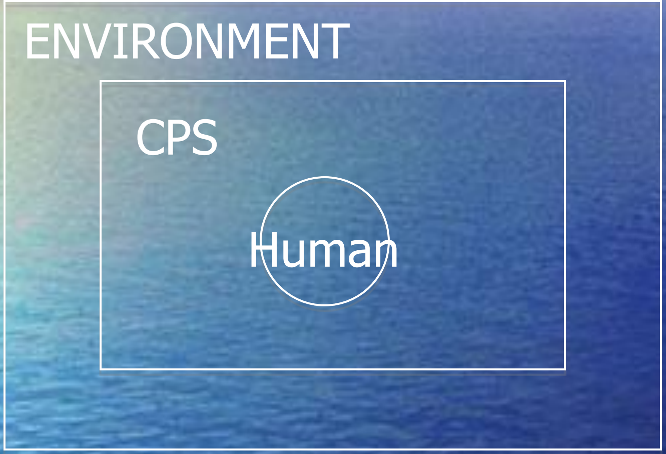
HCMDSS
High Confidence Medical Device, Software, and Systems

Paul L. Jones
Sr. Systems/Software Engineer
FDA/CDRH/OSEL

Medical Device Cyber-Physical Systems

Cyber-Physical Systems



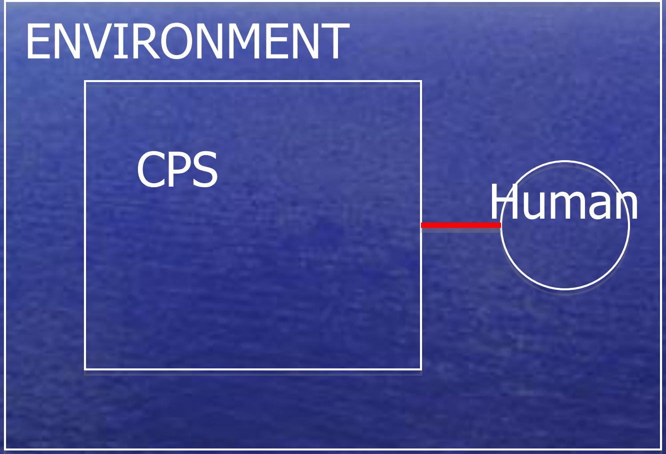
ENVIRONMENT

CPS

Human

physics

Automotive
Protect human from environment



ENVIRONMENT

CPS

Human

physiology

Medical Device
Life Supporting / Sustaining

Regulatory Environment

- Safety critical systems
- Regulator is between the manufacturers and the market
- Short review times
- Increasing device complexity driven by new technology and need for better health care

Assured Verification Research

- Generic Infusion Pump Safety Model
- Generic Insulin Infusion Pump Safety Model
- Medical Device Plug-n-Play (MDFC)
- Static Analysis
- “Life (Flight) ” Recorder

Assured Verification Research

- Assurance Cases
  - Safety cases
  - Security cases
  - New proposed research
    - Traceability Metrics
    - Architecture Analysis
      - Architecture Metrics
      - Architecture driven SAT

Assured Verification Research

- Assurance Cases cont’d
  - New proposed research cont’d
    - Architecture driven requirements checking
    - Architecture driven code verification modeling
    - Mock data bases
    - Artifact based differencing for safety analysis
    - How does one know a hazard analysis is complete?

Assurance Case Experience

- A regulator or third party must be able to trust "evidence" used to justify a "claim"
- A regulator or 3P must provide an assurance claim template for the mfr
- Standards (measures & metrics) and legal infrastructure must exist
- Need component & system composition technology

Conclusion

Need to identify critical system properties and the means to demonstrate that these properties are satisfied.