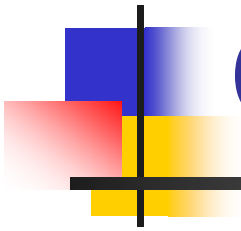
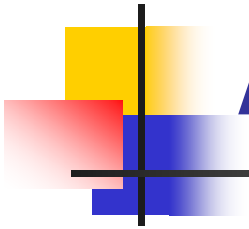


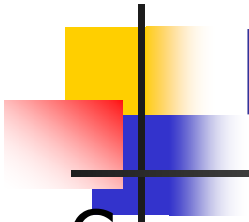
Well-formed Dependency and Open-loop Safety (Continued)

Based on Slides by Professor Lui Sha

Discussion: Patient Controlled Analgesia

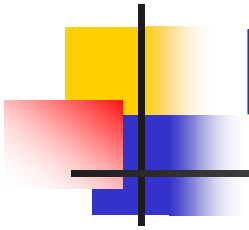


- When pain is severe in a post-surgery patient, the patient can push a button to get more pain medication (morphine: drug overdose will cause death). This is an example of a lethal device in the hands of an error-prone operator (the patient). How can we ensure safety of software controlled PCA?



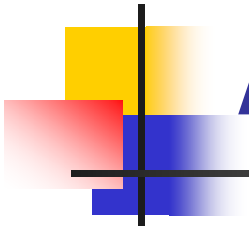
Patient Controlled Analgesia

- Component list:
  - Infusion pump (with embedded micro-controller)
  - Oxymeter (clipped on finger to measure blood oxygen level)
  - ECG Reader (taped to patient's chest)
  - Network that connects them
  - Inexperienced user
- Design questions:
  - Q1: What is the safety core? What's a safe state?
  - Q2: What components we can use but not depend on?
  - Q3: What is the fault model for each component?
  - Q4: How can the safety core withstand those faults?



Discussion: Avionics

- In avionics, the autopilot must be level-A certified.
- The autopilot receives trajectory input from a flight guidance system that is only level-C certified.
- Can the overall system be level-A certified? (Note: Assume that manual flight control is a safe state)



Avionics

- Component list:
  - Autopilot
  - Flight guidance system
  - Network that connects them
  - Skilled pilot
- Design questions:
  - Q1: What is the safety core? What's a safe state?
  - Q2: What components we can use but not depend on?
  - Q3: What is the fault model for each component?
  - Q4: How can the safety core withstand those faults?

Discussion: Ventilator/X-Ray Interaction

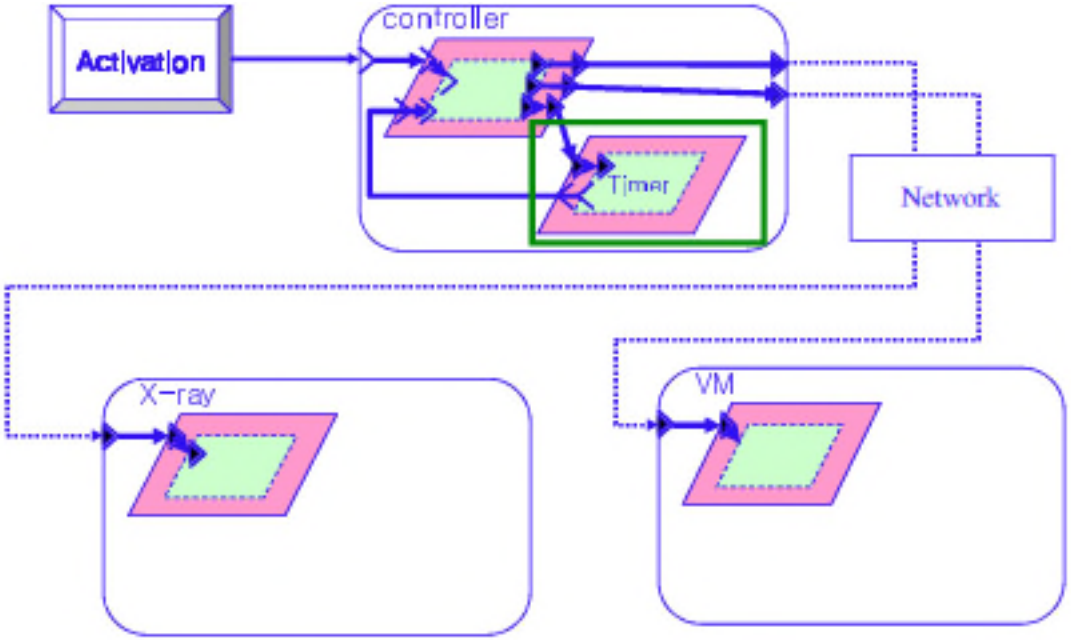
Case study:

- "A 32-year-old woman was having a laparoscopic cholecystectomy performed under general anesthesia. During that procedure and at the surgeon's request, a plain film x-ray was shot during a cholangiogram.
- The anesthesiologist stopped the ventilator for the x-ray. The x-ray technician was unable to remove the film because of its position beneath the table. The anesthesiologist attempted to help the technician, but found it difficult because the gears on the table had jammed.
- Finally, the x-ray was removed, and the surgical procedure recommenced.
- At some point, the anesthesiologist glanced at the EKG and noticed severe bradycardia. He realized he had never restarted the ventilator. This patient ultimately died"

APSF Newsletter, Winter 2005

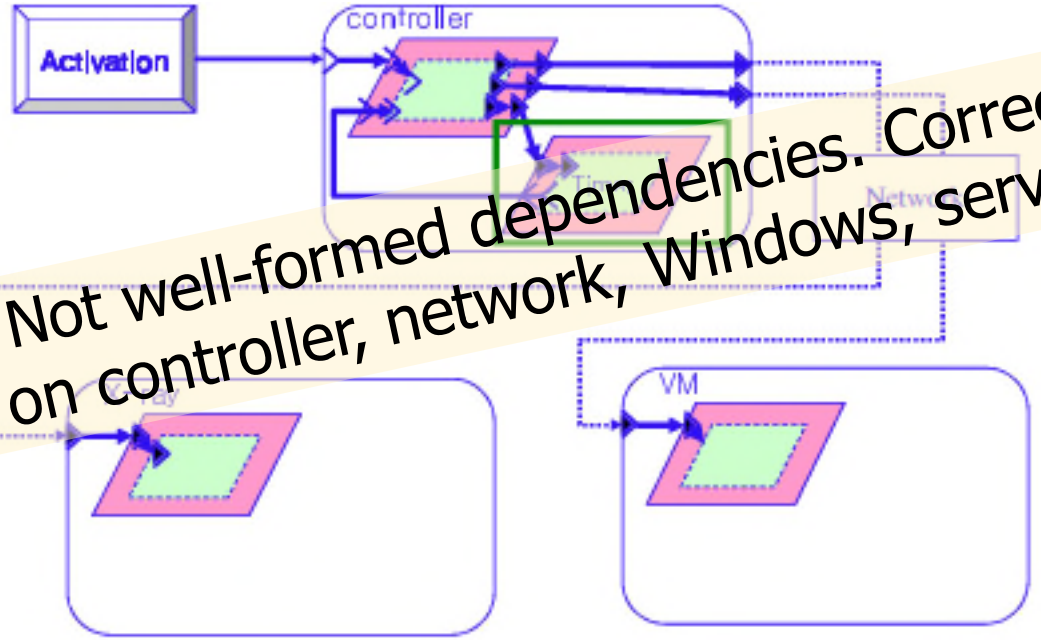
Ventilator/X-Ray Interaction

- Architecture #1: Master controller on a Windows server orchestrates ventilator and X-ray machine actions over a network. Controllers tells machines to stop and re-start, and ensures that ventilator is not off too long. Comments?



Ventilator/X-Ray Interaction

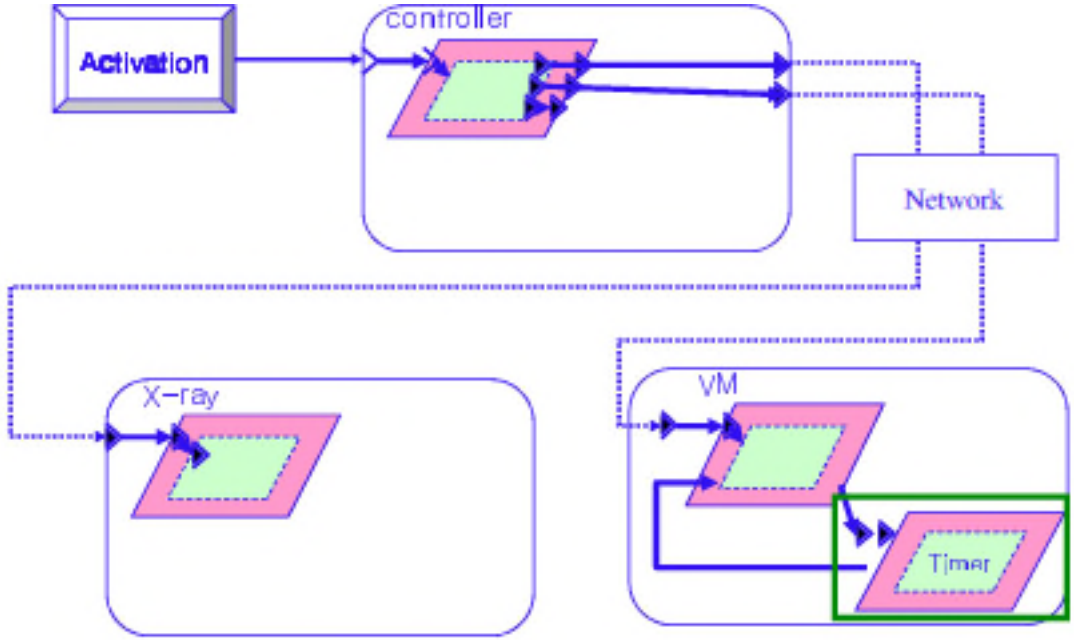
- Architecture #1: Master controller on a Windows server orchestrates ventilator and X-ray machine actions over a network. Controllers tells machines to stop and re-start, and ensures that ventilator is not off too long. Comments?



Problem: Not well-formed dependencies. Correct operation depends on controller, network, Windows, server, etc.

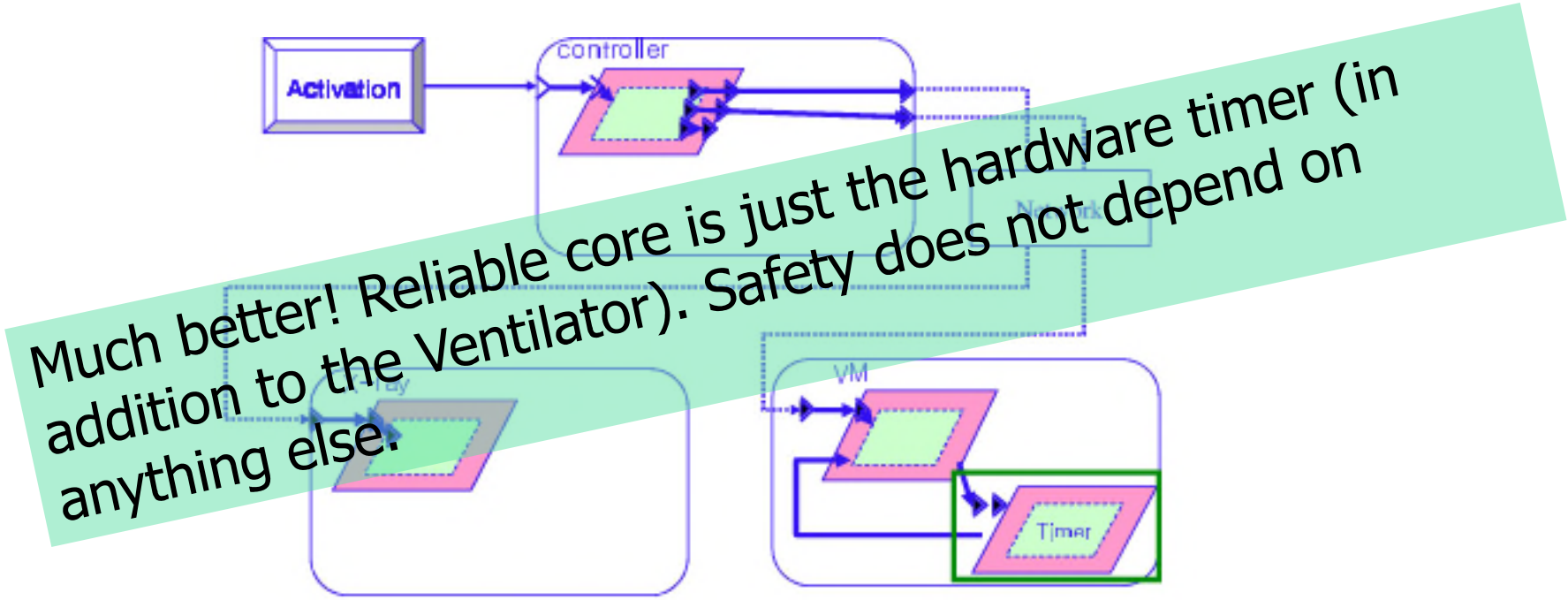
Ventilator/X-Ray Interaction

- Architecture #2: Master controller on a Windows server tells ventilator when to pause. Ventilator has a hardware timer and restarts automatically once timer expires.

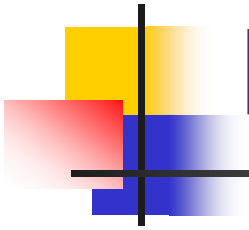


Ventilator/X-Ray Interaction

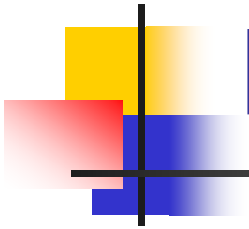
- Architecture #2: Master controller on a Windows server tells ventilator when to pause. Ventilator has a hardware timer and restarts automatically once timer expires.



Discussion: Asimov Laws of Robotics



Discussion: Asimov Laws of Robotics



- A robot may not injure a human being
- A robot must obey the orders given to it by human beings, except where such orders would conflict with the First Law.
- A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.