Challenges In Deeply Networked System Survivability

Philip Koopman

February 2007

koopman@cmu.edu

http://www.ece.cmu.edu/~koopman

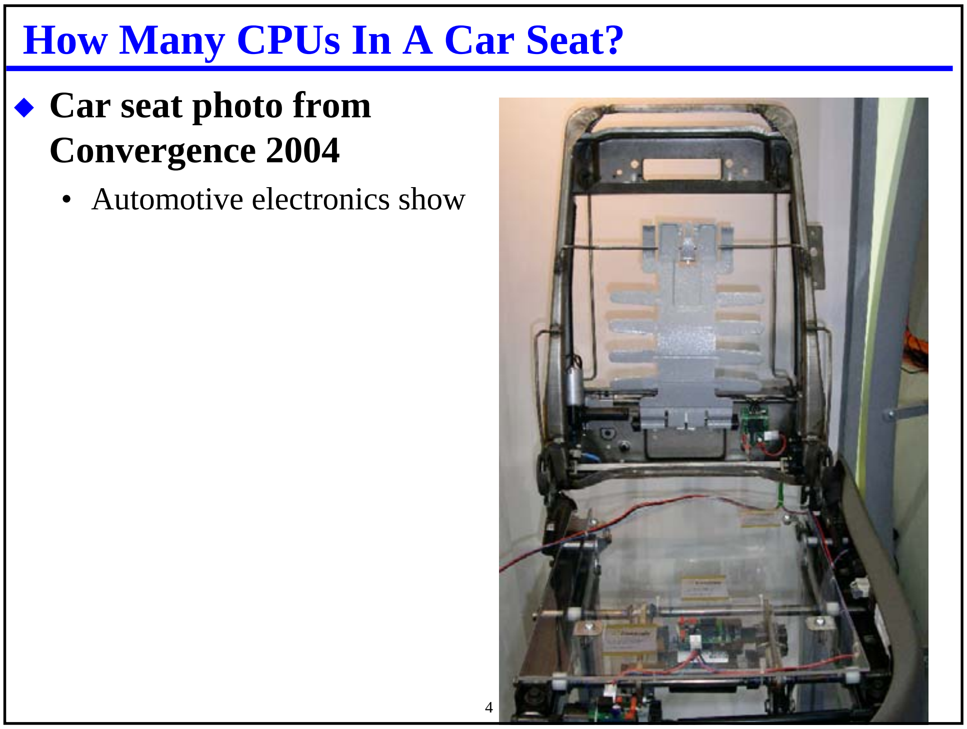
Electrical & Computer ENGINEERING

Carnegie Mellon

Overview

- **Brief introduction to the world of embedded control**
  - To a first approximation, desktop CPUs are 0% of the market
- **High Level look at two issues**
  - Embedded / Internet Gateways
  - An example threat: household thermostats

My Experience in Embedded Systems

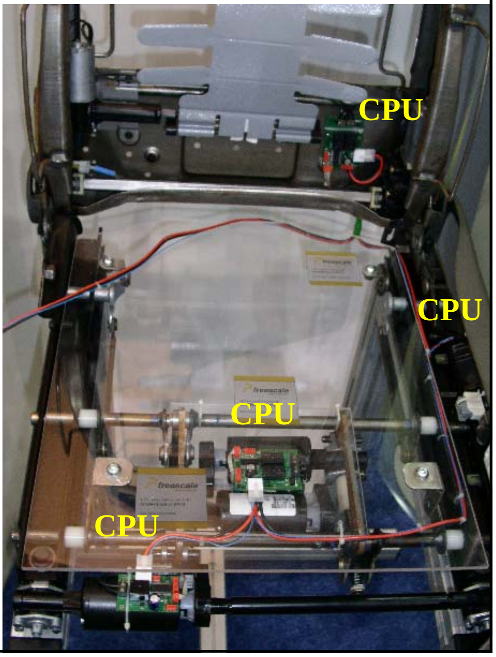


How Many CPUs In A Car Seat?

- **Car seat photo from Convergence 2004**
  - Automotive electronics show

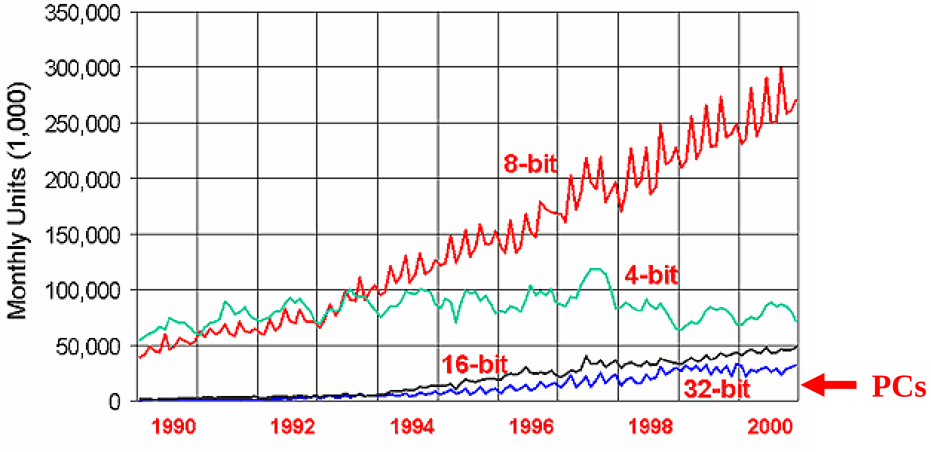
Car Seat Network (no kidding)

- Low speed LIN network to connect seat motion control nodes
- This is a distributed embedded system!
  - Front-back motion
  - Seat tilt motion
  - Lumbar support
  - Control button interface
  - Connects to body controls network beyond seat for per-driver customization



Microprocessor Unit Sales

All types, all markets worldwide



Source: WSTS

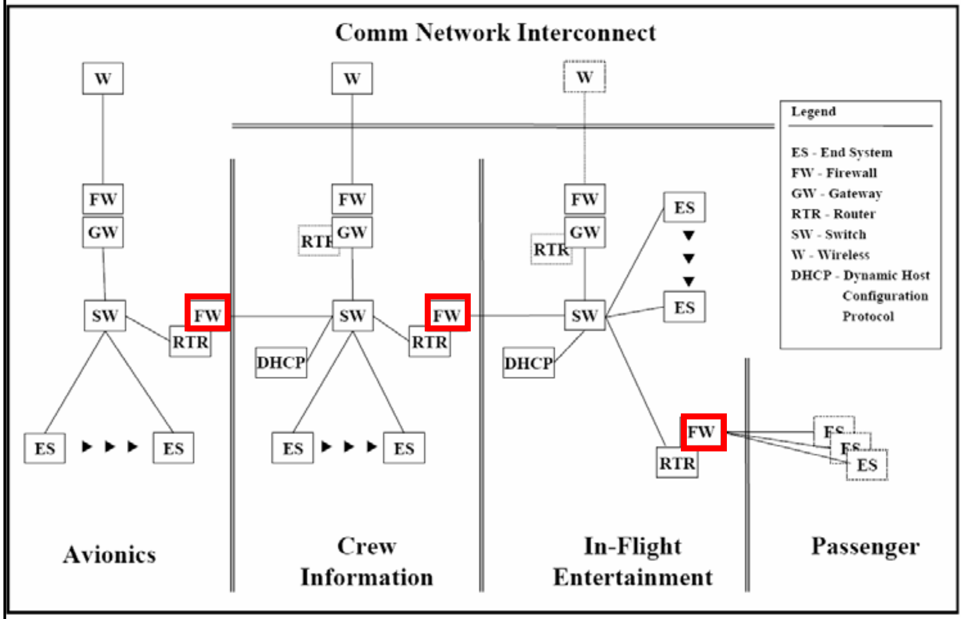
15 Million PCs per month in 2004 (15,000 on this graph)

Trend: External Connectivity

- **Safety critical subsystems will be connected to external networks (directly or indirectly)**
  - German proposal:
    wireless networks control car’s max. speed
  - E-enabled aircraft architecture (next slide)

Computer graphics by I3M

[Airbus 2004] A-380 scheduled to enter service in 2006



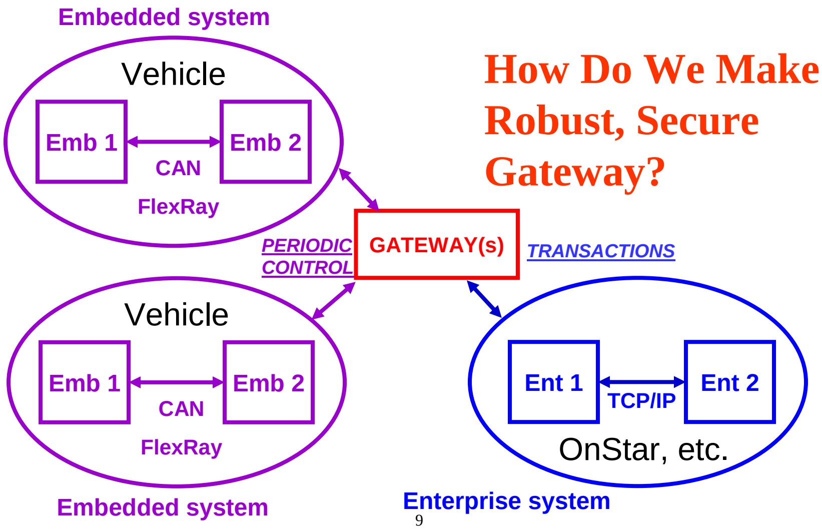
Wargo & Chas, 2003, proposed Airbus A-380 architecture

Passenger laptops are 3 Firewalls away from flight controls!

Deeply Embedded System Gateway

Enterprise system + Embedded System =
"Deeply Embedded System"

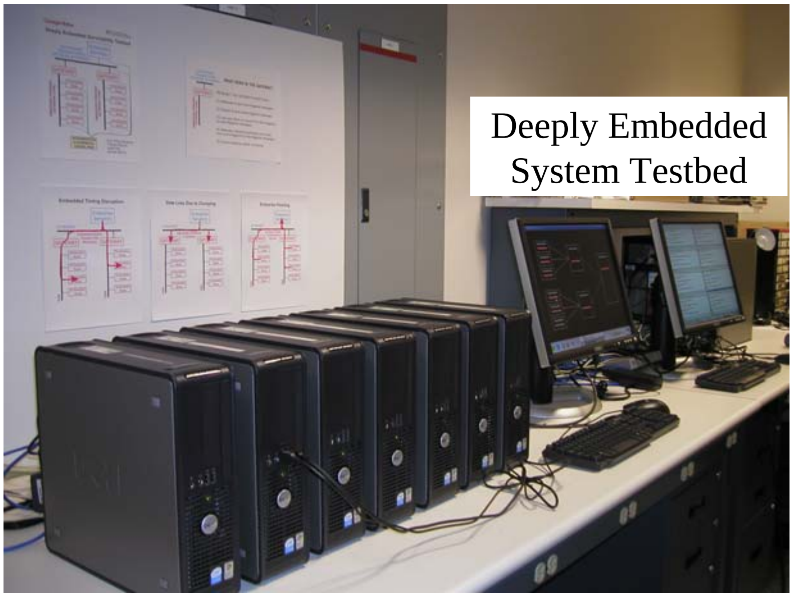
How Do We Make A Robust, Secure Gateway?



Research Area: Embedded/Internet Gateway

- **What happens at the embedded/internet interface?**
  - Fault propagation across the gateway presents fundamental challenges

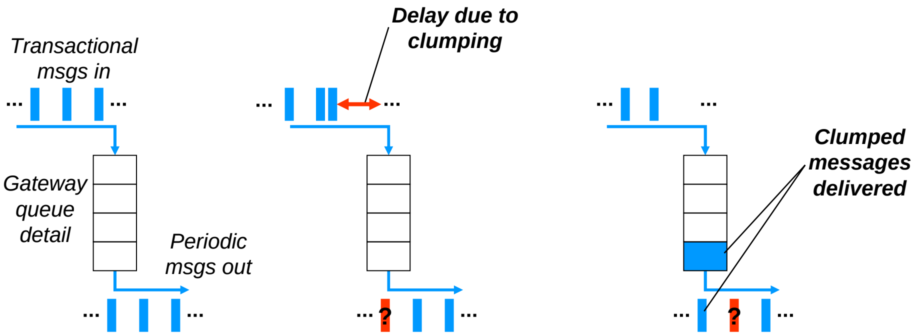
Embedded Side	GATEWAY	Enterprise Side
Control-oriented		Transaction-oriented
Time Triggered		Event Triggered
Continuous		Discrete
Real Time		Mostly not Real Time
Periodic Messages		Aperiodic Messages
Short Messages		Longer messages
Roll-forward		Rollback
Lower cost		Higher cost



Deeply Embedded System Testbed

Initial Experiment: Queue overflow

- How having a long queue can cause you to operate on stale data



Transactional msgs in

Gateway queue detail

Periodic msgs out

Delay due to clumping

Clumped messages delivered

Ideal case: Queue is empty in the steady state

Clumping delay leads to missed deadline for periodic messages

Need a policy for dealing with having no message to send.

Two messages delivered, so a message is stuck in the queue.

Now all the messages delivered to the embedded system are 1 period old.

Deeply Embedded Scary Scenario

- **Consider the lowly thermostat**
  - Koopman, P., "Embedded System Security," *IEEE Computer*, July 2004.
- **Trends:**
  - Internet-enabled
  - Connection to utility companies for grid load management
- **Proliphix makes an Internet Thermostat**
  - (But it we're not saying that system has these vulnerabilities!)
  - Somebody else makes one almost exactly like this, deployed July 2005

Waste Energy Attack

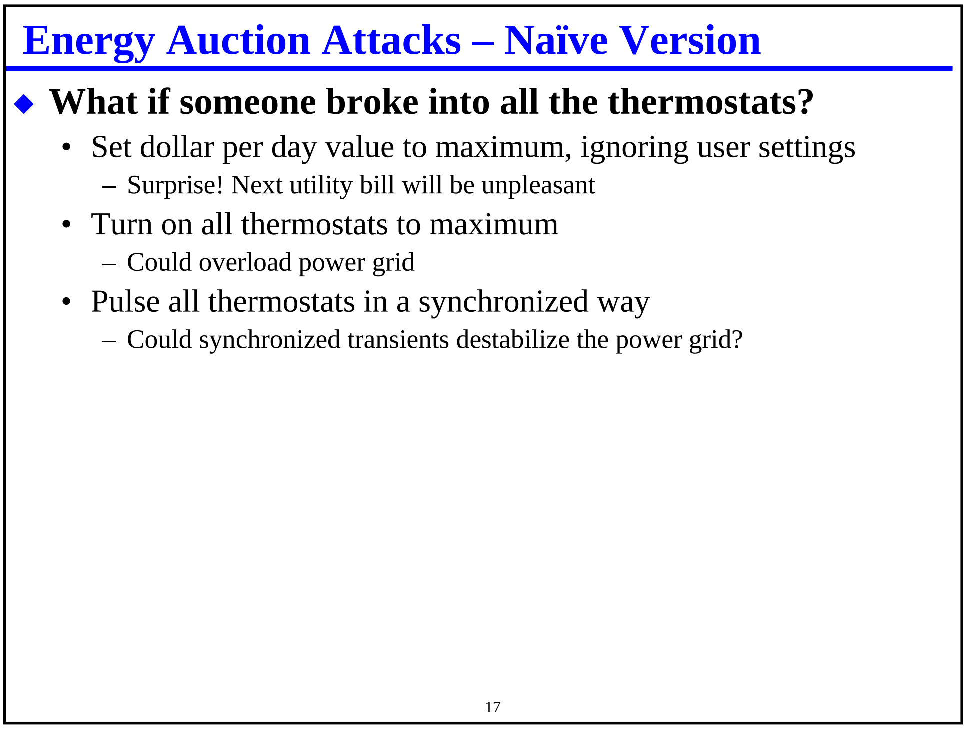
- **"I'm coming home" function**
  - Ability to tell thermostat to warm up/cool down house if you come home early from work, or return from a trip
  - Save energy when you're gone; have a comfy house when you return
  - Implement via web interface or SMS gateway
- **Attack: send a false "coming home" message**
  - Causes increase in utility bill for house owner
  - If a widespread attack, causes increased US energy usage/cause grid failure
  - Easily countered(?) – if designers think to do it!
    - Note that playback attack is possible – more than just encryption of an unchanging message is required!

Discomfort Attack

- **Remotely activated energy saver function**
  - Remotely activated energy reduction to avoid grid overload
  - Tell house "I'll be home late"
  - Saves energy / prevents grid overload when house empty
- **Attack: send a false "energy saver" command**
  - Will designers think of this one?
  - Some utilities broadcast energy saver commands via radio
    - In some cases, air conditioning is completely disabled
    - Is it secure??
  - Consequences higher for individual than for waste energy attack
    - Possibly broken pipes from freezing in winter
    - Possibly injured/dead pets from overheating in summer

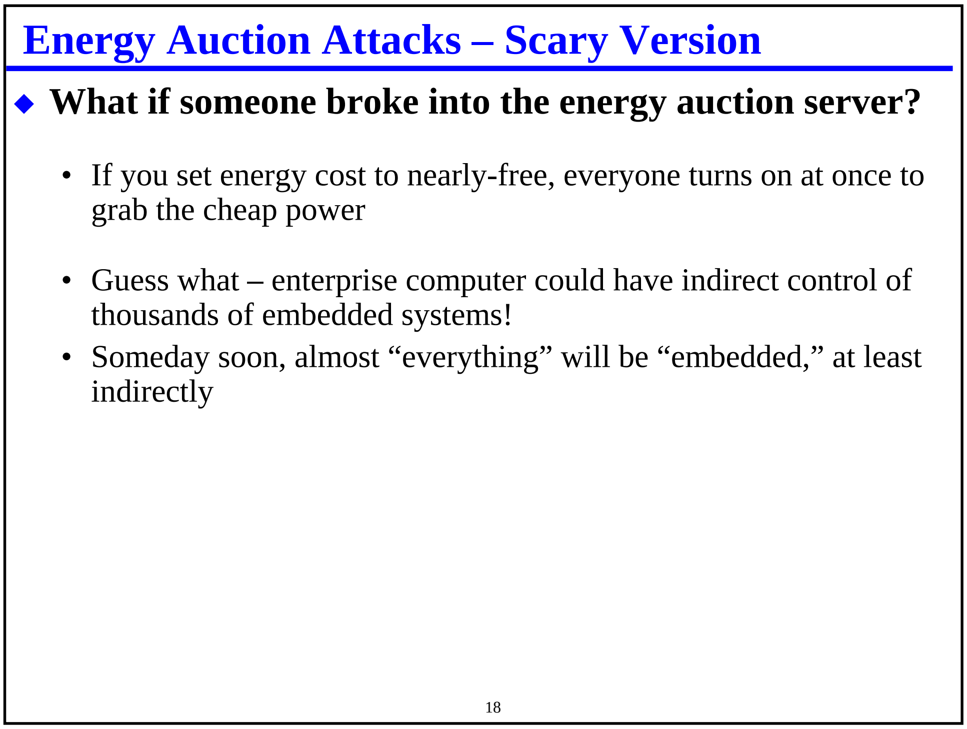
Energy Auction Scenario

- **What if power company optimizes energy use?**
  - Slightly adjust duty cycles to smooth load (pre-cool/pre-heat in anticipation of hotest/coldest daily temperatures)
  - Offer everyone the chance to save money if they volunteer for slight cutbacks during peak times of day
  - Avoid brownouts by implementing heat/cool duty cycle limits for everyone
- **You could even do real time energy auctions**
  - Set thermostat by "dollars per day" instead of by temperature
    - More dollars gives more comfort
  - Power company adjusts energy cost continuously throughout day
  - Thermostats manage house as a thermal reservoir



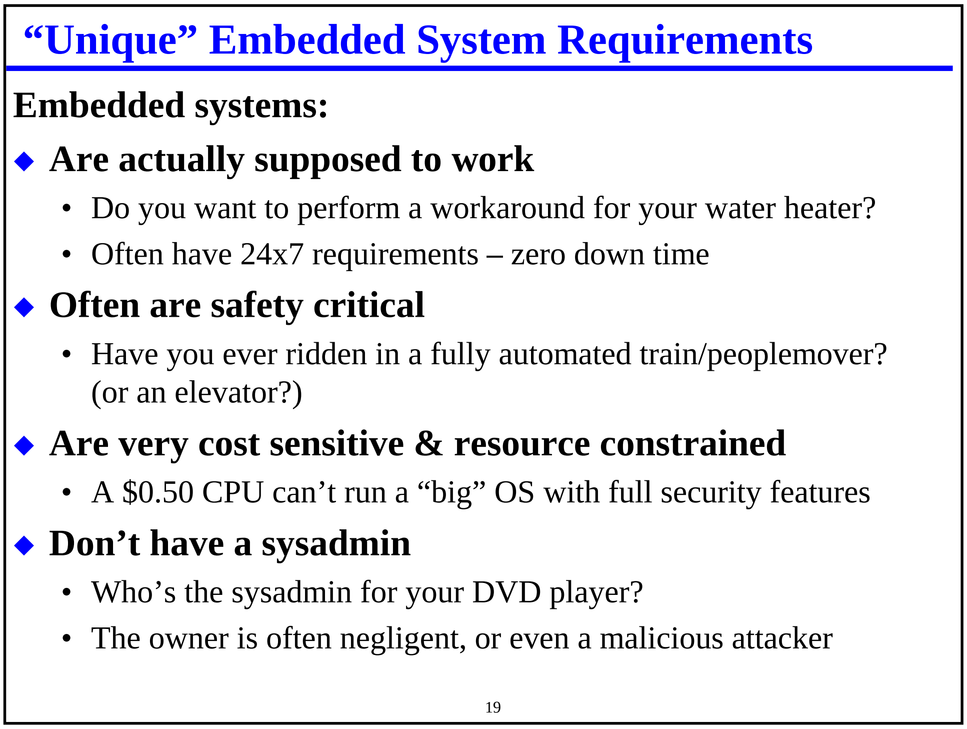
Energy Auction Attacks – Naïve Version

- **What if someone broke into all the thermostats?**
  - Set dollar per day value to maximum, ignoring user settings
    - Surprise! Next utility bill will be unpleasant
  - Turn on all thermostats to maximum
    - Could overload power grid
  - Pulse all thermostats in a synchronized way
    - Could synchronized transients destabilize the power grid?



Energy Auction Attacks – Scary Version

- **What if someone broke into the energy auction server?**
  - If you set energy cost to nearly-free, everyone turns on at once to grab the cheap power
  - Guess what – enterprise computer could have indirect control of thousands of embedded systems!
  - Someday soon, almost “everything” will be “embedded,” at least indirectly



“Unique” Embedded System Requirements

Embedded systems:

- **Are actually supposed to work**
  - Do you want to perform a workaround for your water heater?
  - Often have 24x7 requirements – zero down time
- **Often are safety critical**
  - Have you ever ridden in a fully automated train/peoplemover? (or an elevator?)
- **Are very cost sensitive & resource constrained**
  - A $0.50 CPU can’t run a “big” OS with full security features
- **Don’t have a sysadmin**
  - Who’s the sysadmin for your DVD player?
  - The owner is often negligent, or even a malicious attacker