Challenges In Embedded System (Cyber Physical System) Security

Philip Koopman

koopman@cmu.edu

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

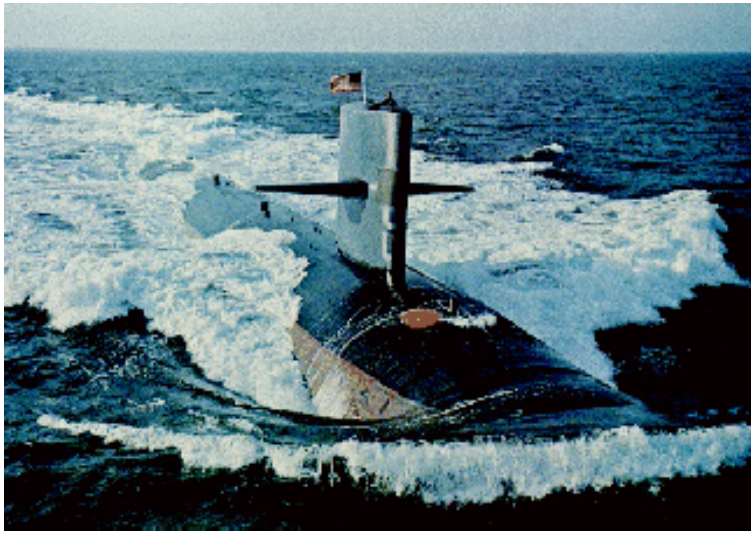
With contributions from Justin Ray

Electrical & Computer ENGINEERING

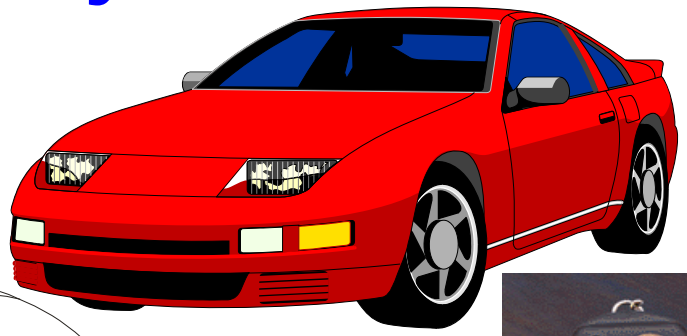
Carnegie Mellon

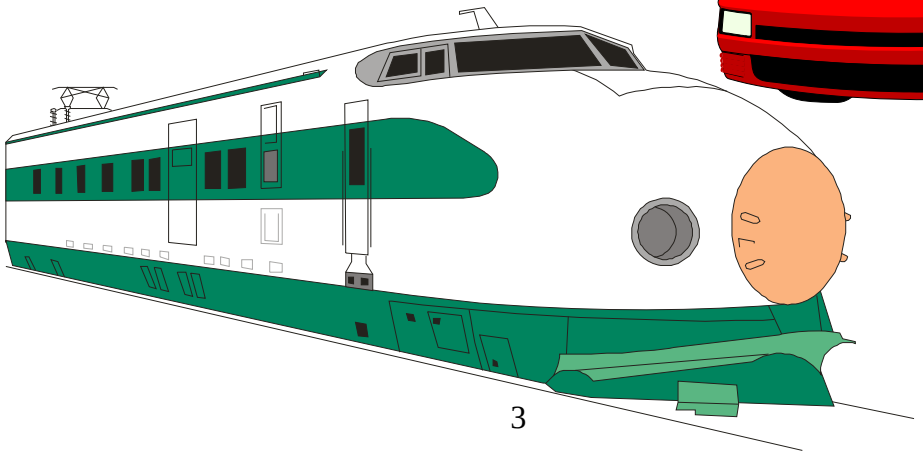
Overview

- **Small-CPU embedded systems are nearly 100% of computing**
  - At least by number of CPUs
  - Often there is a collection of small CPUs in an embedded system
- **Embedded/CPS survivability presents unique problems**
  - Survivability ≈ security + fault tolerance
    - For safety critical systems, you can argue they are similar problems
  - Not everything will look like a smaller version of desktops
  - Combining desktop & embedded technology is problematic
  - Connecting embedded systems to the Internet is hard to do well
- **Example research area:**
  - What goes in the embedded/Internet firewall?



My Experience in Embedded Systems





Lots of CPUs, But No Pentiums Here

Most embedded CPUs don't run an operating system either.

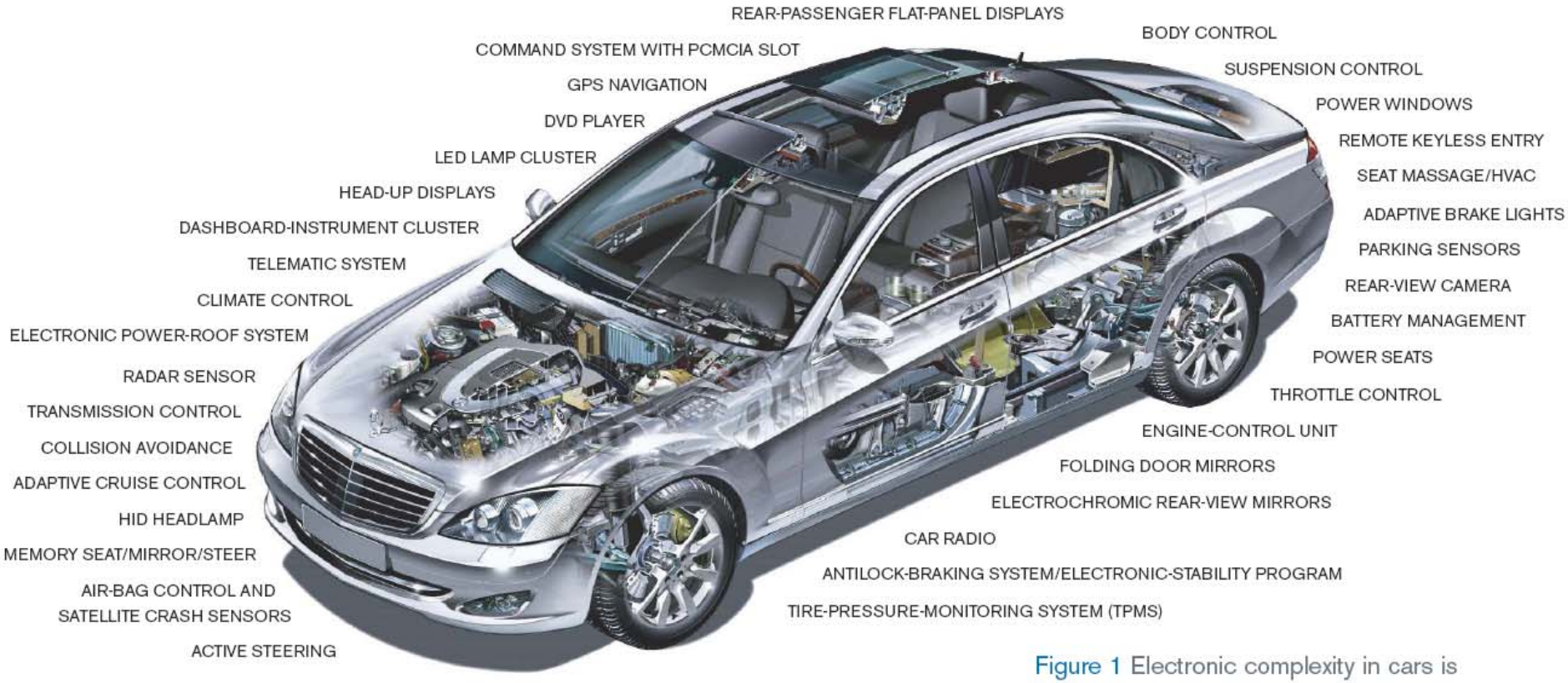
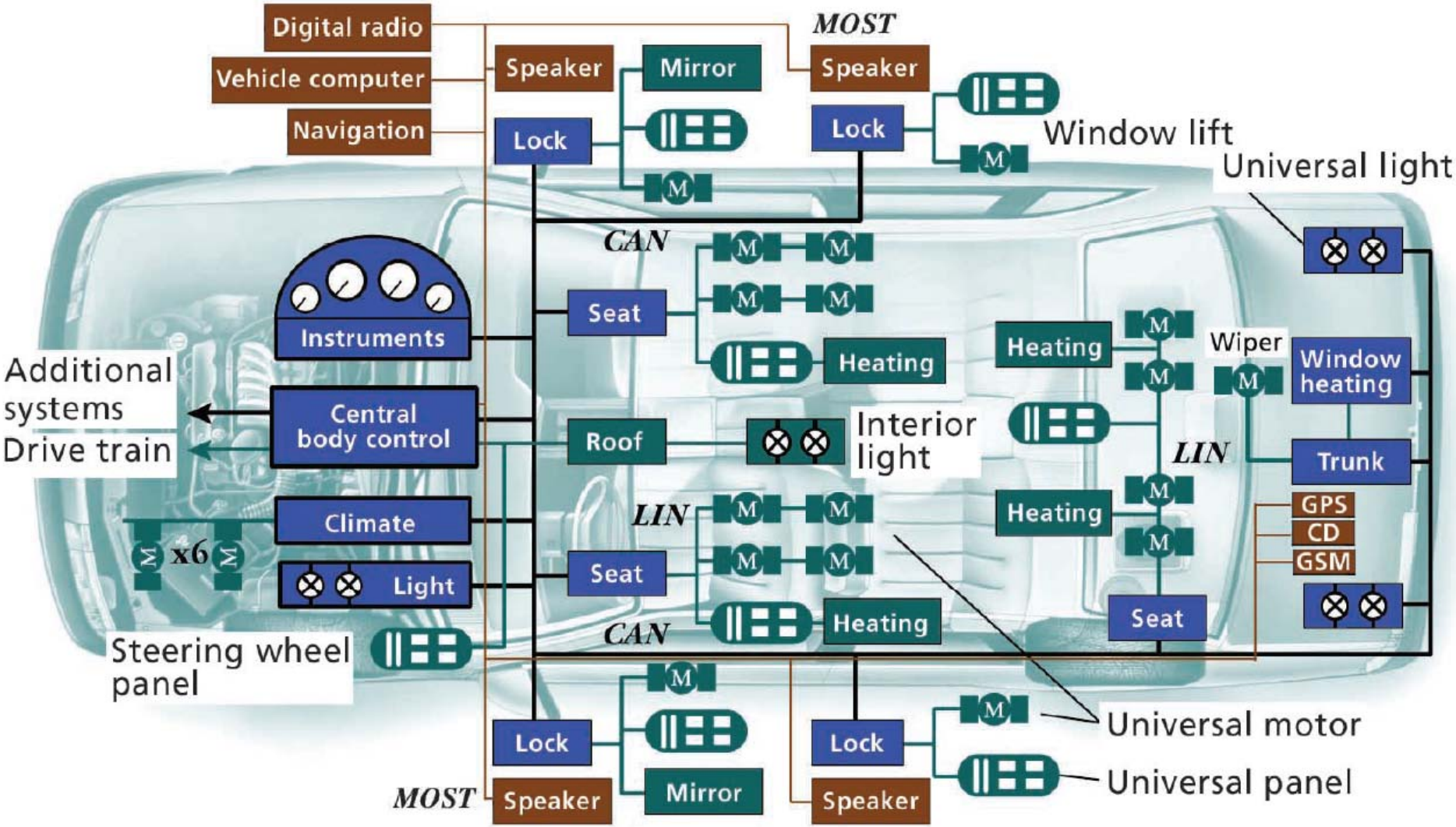


Figure 1 Electronic complexity in cars is increasing. New Mercedes S-Class cars employ at least 70 networked ECUs (electronic control units); 10 years ago, most cars had three ECUs (photo courtesy of DaimlerChrylser; source: Gartner Research, November 2005).

[Santarini06]

Automotive: An Engineering View

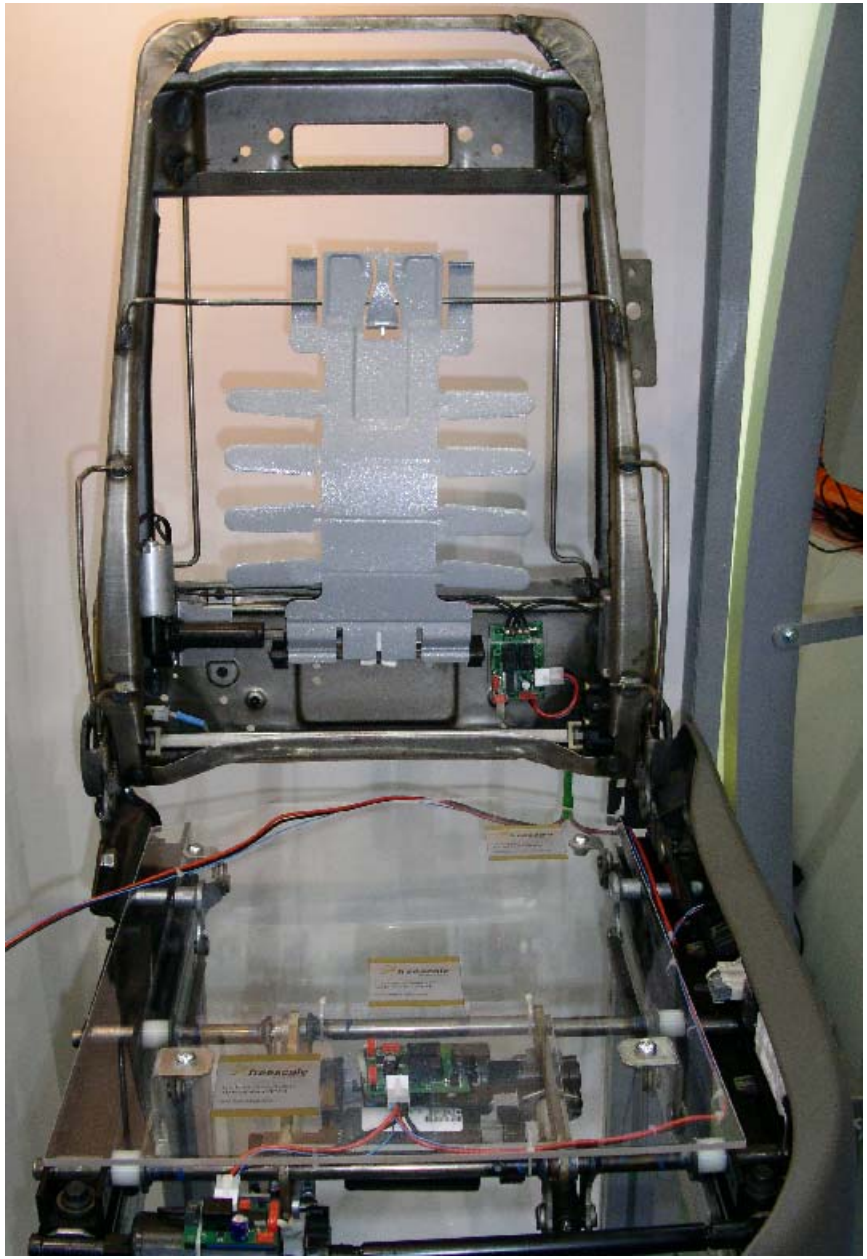


CAN Controller area network
GPS Global Positioning System
GSM Global System for Mobile Communications
LIN Local interconnect network
MOST Media-oriented systems transport

[Leen02]

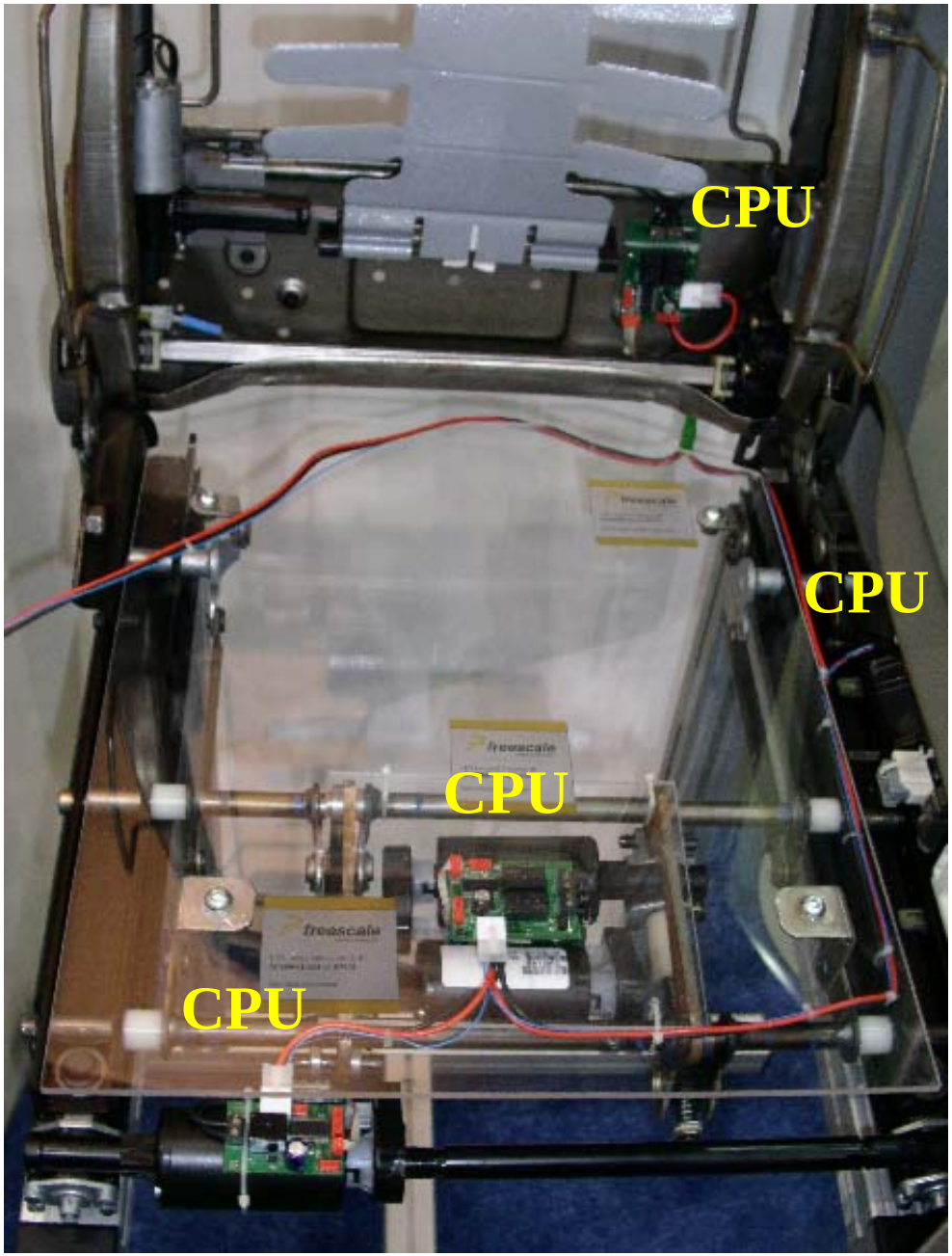
How Many CPUs In A Car Seat?

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



Car Seat Network (no kidding)

- **Low speed LIN network to connect seat motion control nodes**
  - Reduces wiring and mechanical complexity
- **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



But, Is Security An Issue For CPS?

- **YES … but only recently becoming real news**

- **Potential problems are already there**
  - Modems that control embedded systems where "security" is an unlisted number
    - Example: an unprotected modem controlling a high-voltage power transmission line (Shipley & Garfinkel, 2001)
  - Stories of insider attacks on critical systems
  - User-modified critical systems
    - "Hot PROM" approach to modifying automotive engine controllers

- **Will this be different than, say, bank security?**
  - Beyond them being mostly 8- & 16-bit CPUs with no OS?

Who Is The Sysadmin?

- **Who keeps your washing machine patches up to date?**

Surf Among Suds With Web-Enabled Washing Machine

LG Electronics unveils its second Internet-aware appliance, which downloads clothing care programs.

Martyn Williams, IDG News Service
Tuesday, October 17, 2000

Carnegie Mellon

Use Of Desktop-Quality Software

http://www.coed.org/photodb/folder.tcl?folder_id=3334

"When ATMs go bad by Carla Geisser“, March 18, 2004

(See also: http://midnightspaghetti.com/newsDiebold.php)


U·S AIRWAYS
Internet Explorer Script Error
An error has occurred in the script on this page.
Line: 3235
Char: 6
Error: Subscript out of range: 'CurrentAd'
Code: 0
Do you want to continue running scripts on this page?
Yes
No
To Select
Info
Movies
TV
Music

Windows isn’t the only thing that crashes

Linux kernel booting on train schedule system display

Grenoble, France
Train Station
January 2007

Hackers Crack Into Texas Road Sign, Warn of Zombies Ahead

Thursday, January 29, 2009
FOX NEWS

By Joshua Rhett Miller

E-Mail | Print | Share

i-hacked.com

Texas Dept. of Transportation officials confirm a portable traffic sign at Lamar Boulevard and West 15th Street in Austin was hacked into last week.

Transportation officials in Texas are scrambling to prevent hackers from changing messages on digital road signs after one sign in Austin was altered to read, "Zombies Ahead."

Chris Lippincott, director of media relations for the Texas Department of Transportation, confirmed that a portable traffic sign at Lamar Boulevard and West 15th Street, near the University of Texas at Austin, was hacked into during the early hours of Jan. 19.

"It was clever, kind of cute, but not what it was intended for," said Lippincott, who saw the sign during his morning commute. "Those signs are deployed for a reason — to improve traffic conditions, let folks know there's a road closure."

"It's sort of amusing, but not at all helpful," he told FOXNews.com.

Safety Criticality => Potential Release Of Energy

Polish Teen Hacks His City's Trams, Chaos Ensues

By Chuck Squatriglia January 11, 2008 | 4:29:44 PM Categories: Public Transit

A teenager in Lodz, Poland hacked the city's tram system with a homemade transmitter that tripped rail switches and redirected trains, a prank that derailed four trams and injured a dozen people.

According to reports in the Register and the Telegraph, the 14-year-old boy - described by his teachers as an electronics genius (Gee- you think?) - spent months studying the city's rail lines to determine the best places to redirect trains and cause the most havoc, then converted an old TV remote into an infrared transmitter capable for tripping the switches.

"He treated it like any other schoolboy might a giant train set, but it was lucky nobody was killed," Miroslaw Micor, a spokesman for Lodz police, told the Telegraph. "Four trams were derailed, and others had to make emergency stops that left passengers hurt. He clearly did not think about the consequences of his actions."

[Wired Blog Jan 11, 2008]

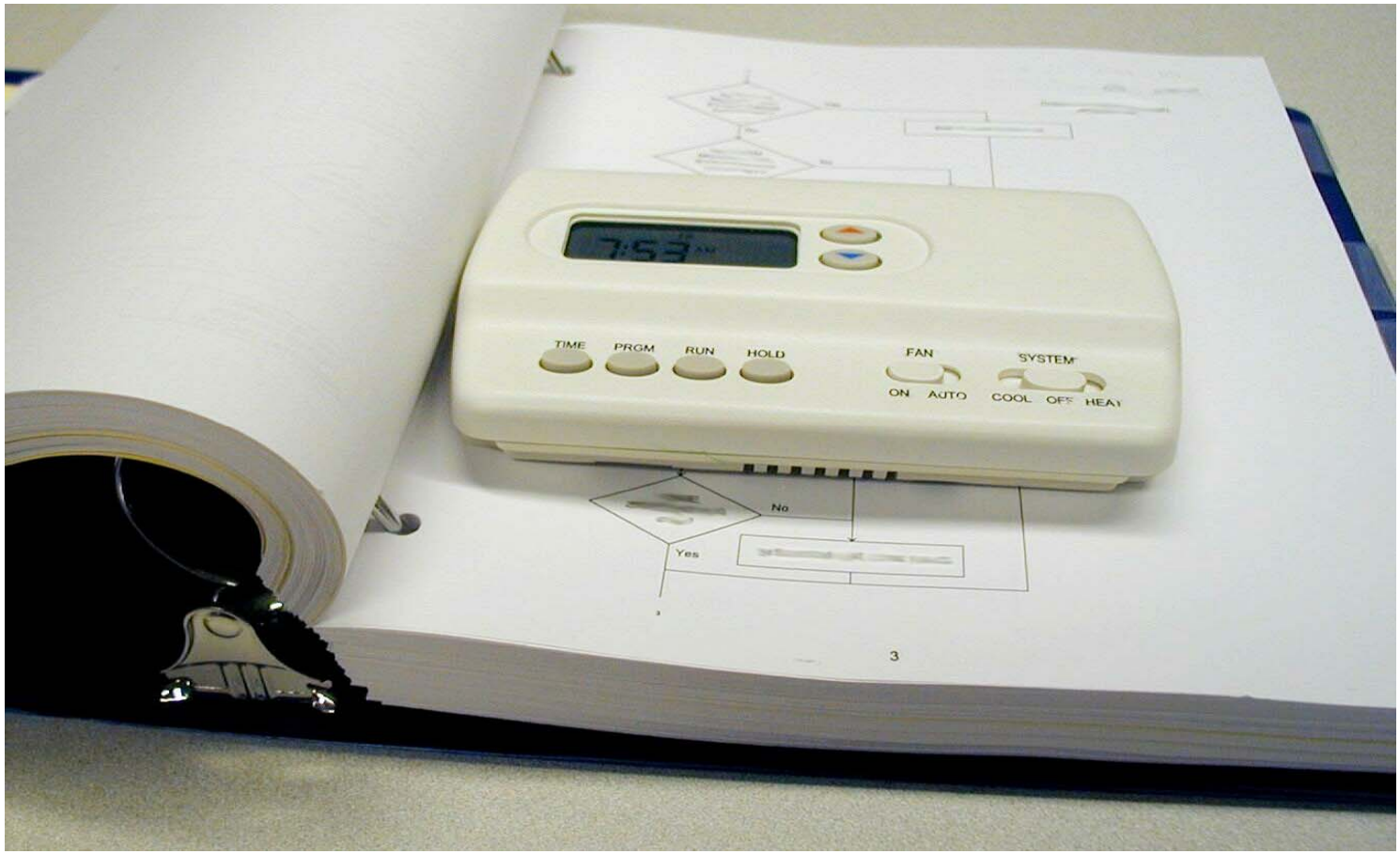
Photo courtesy Telegraph.

Direct Attacks On Infrastructure

- **SCADA systems – *"Supervisory Control And Data Acquisition"***
  - Control factories, refineries, power plants, etc.
  - Mostly they are Internet-Connected via a firewall
  - 2003 – Slammer worm disables a safety monitoring system at Davis-Besse nuclear power plant in Ohio
    - Access via contractor network connection that bypassed firewall

Indirect Attacks On Infrastructure

- **Household thermostat & flow charts**
  - Yes, they really are this complicated…
  - … and this one doesn't have Internet connectivity!



What Happens With Internet Connectivity?

- **Koopman, P., "Embedded System Security," *IEEE Computer*, July 2004.**

- **Several companies make these thermostats already**
  - (We're not singling out one product – but the capabilities we discuss are here or will soon be here.)

[Prolifix; Aprilaire]

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
  - Easily countered (probably) – if designers think to do it!
    - Note that playback attack is possible – more than just encryption of an unchanging message is required!

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
    - This is already done via FM radio transmissions

- **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 Attack – Local

- **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?

- **Big vulnerability would be central coordination point**
  - Is there one that can be attacked?

Energy Auction Attack – Area-Wide

- **You don't have to break into all the thermostats**
  - The auction server has ability to release energy at **all** thermostats
- **What if someone just broke into the 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!
  - An attack along these lines is already possible in some areas, although not quite this attack

Cyber-Physical System Safety

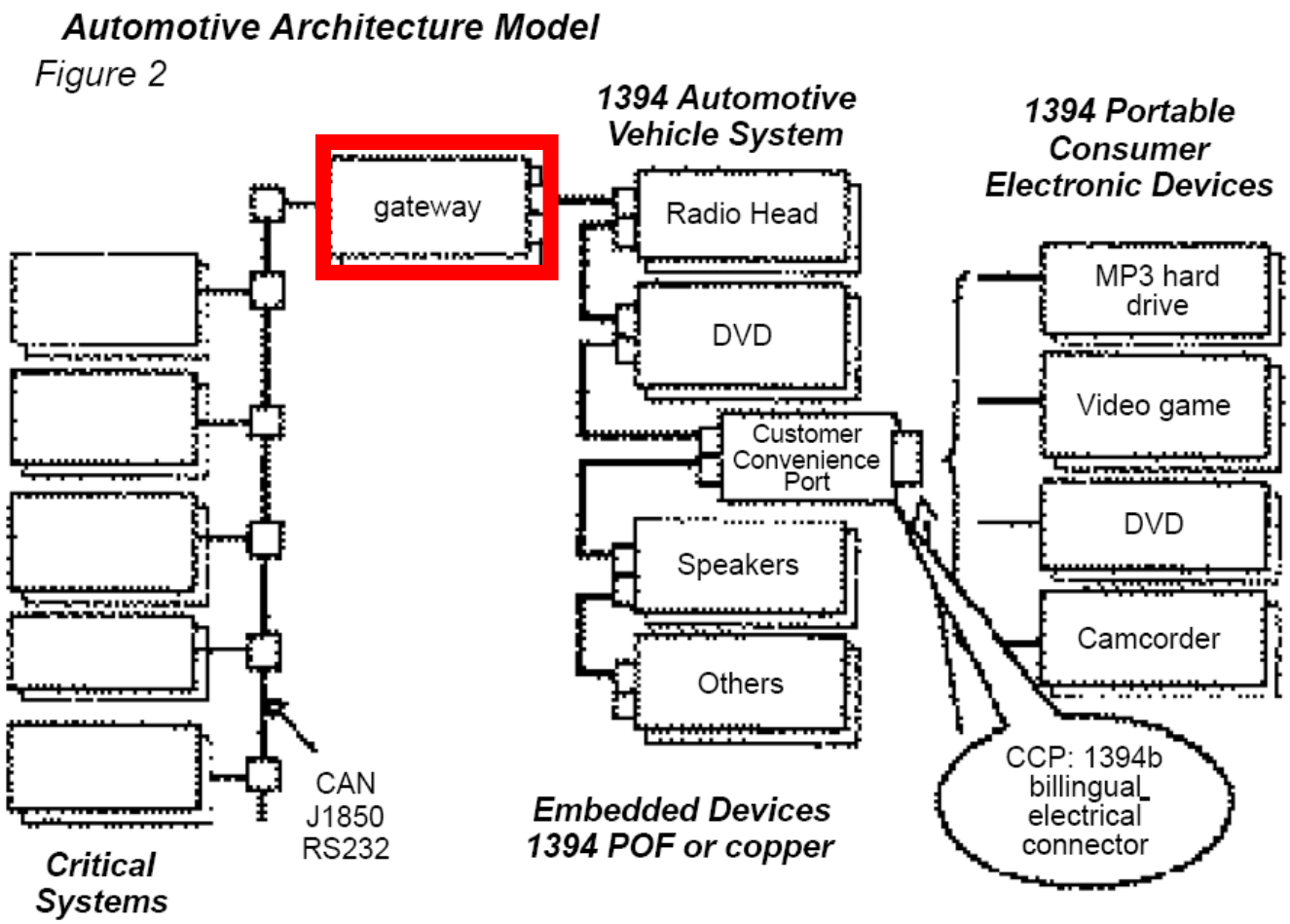
- **In Cyber-Physical Systems web servers can indirectly release energy into the environment**

- **Safety incidents involve uncontrolled release of energy**

- **So, by extension:**
  - At least some Internet components will be safety critical!

- **That means you have to worry about:**
  - Component failures
  - Software defects
  - Malicious attacks
  - Whether you believe firewalls will be enough

Automotive Gateway Connectivity



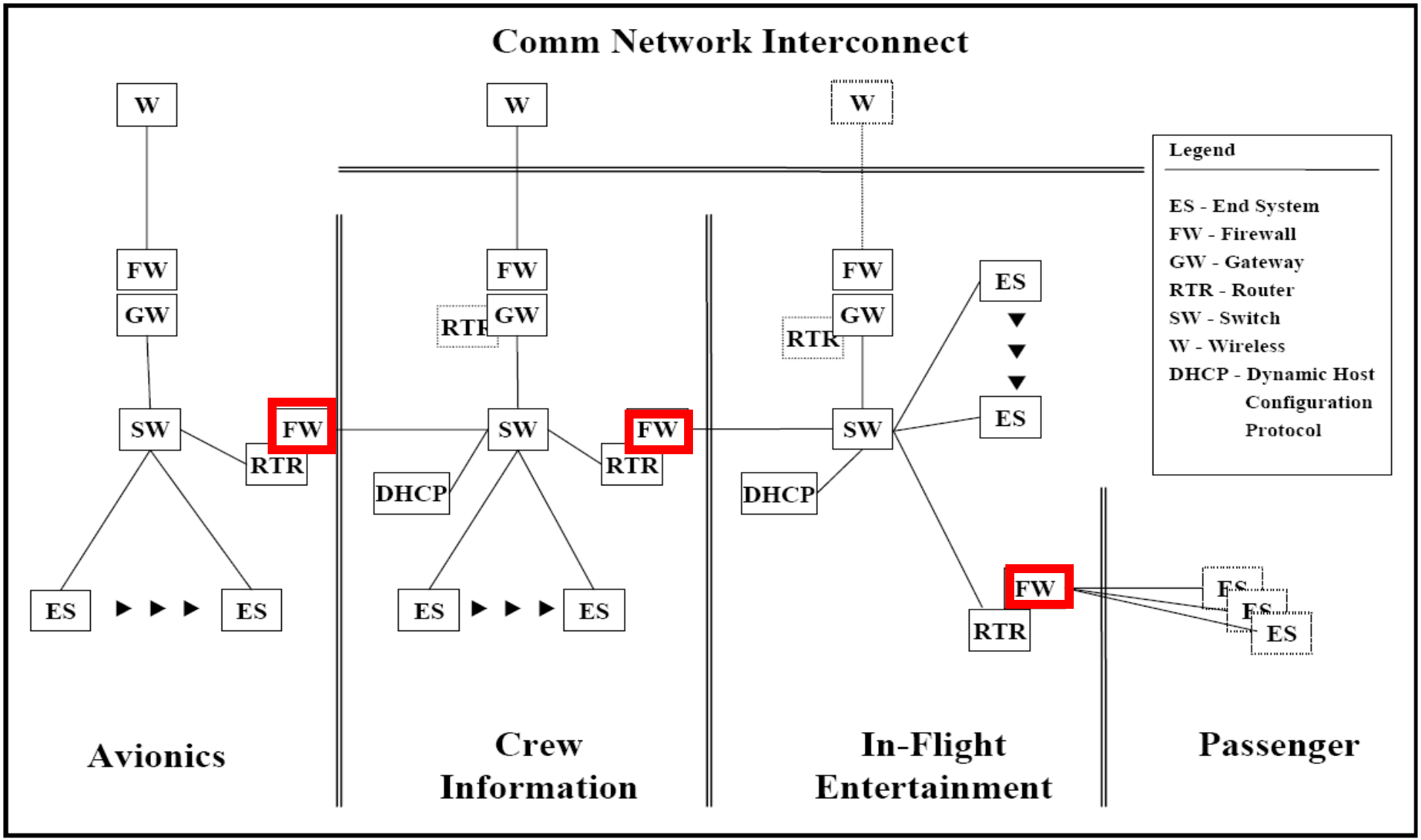
Polishuk, 2001, proposed automotive vehicle architecture

Infotainment 1 FW away from critical systems!

Would You Connect A Laptop To Flight Controls?

- **Safety critical subsystems will be connected to external networks (directly or indirectly)**
  - E-enabled aircraft architecture (next slide)

[Airbus 2004] Airbus 380 uses IP-based flight controls



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

Passenger laptops are 3 Firewalls away from flight controls!

Internet connects somewhere as well

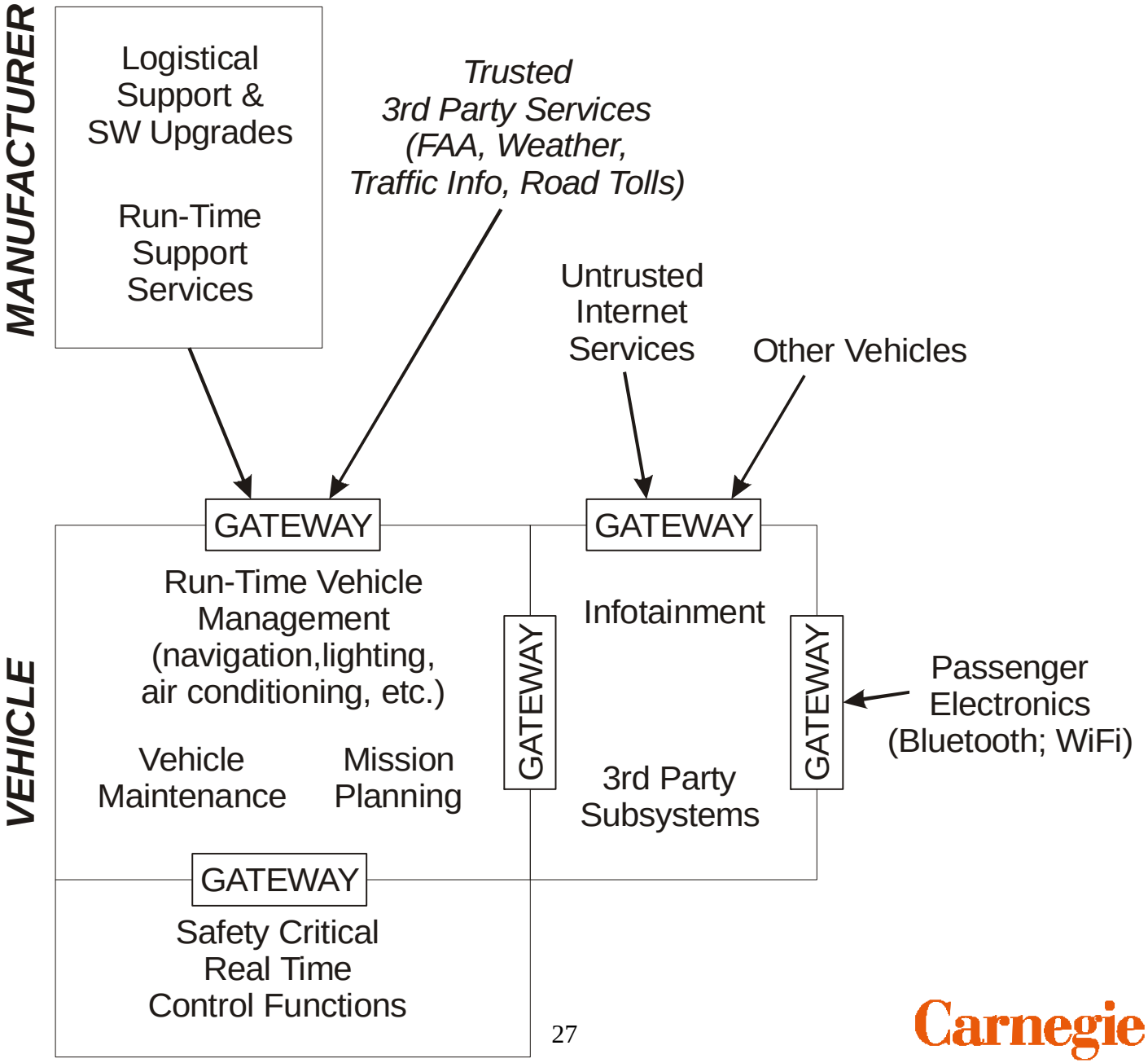
Carnegie Mellon

Research: What Goes In The Gateway?

- **The embedded and enterprise sides are quite different**

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

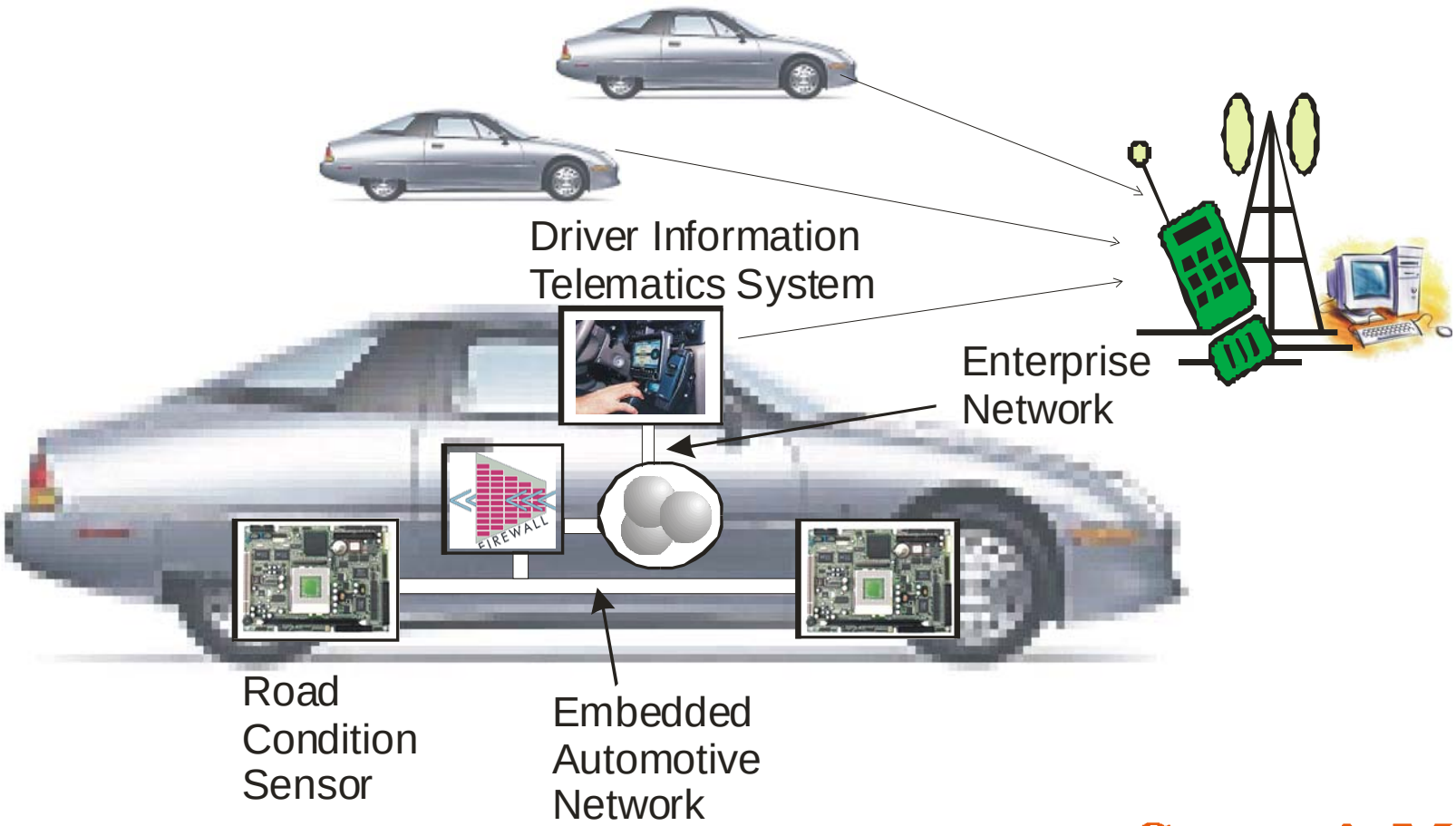
General Vehicle Architecture With Gateways



Carnegie Mellon

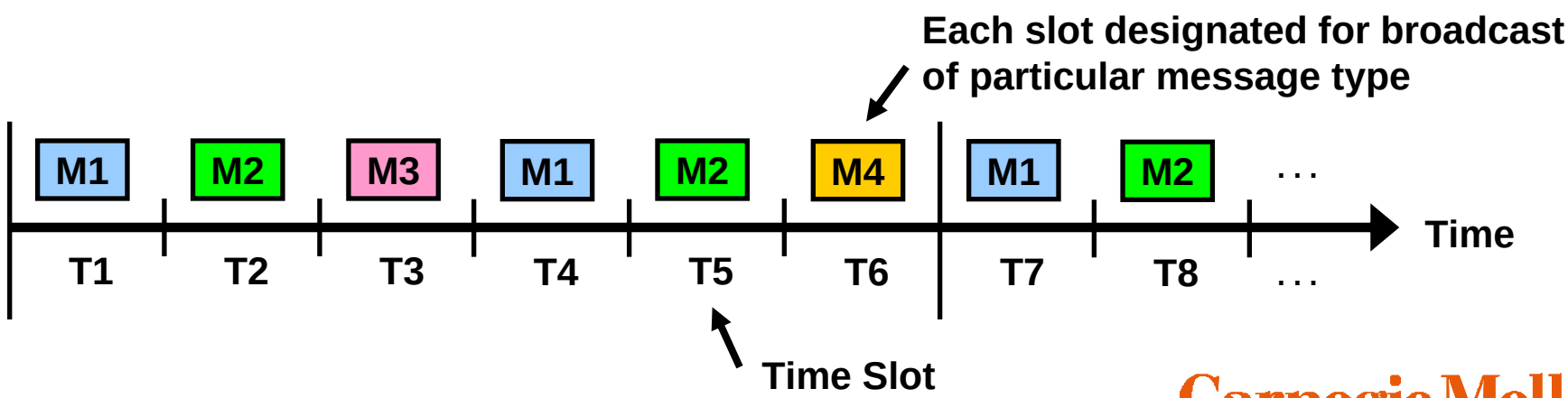
Current Research Topics – Automotive Domain

- **Example application: traffic speed look-ahead**
  - The obvious thing to put in the car's firewall is a queue
  - But, is using a queue a good idea?



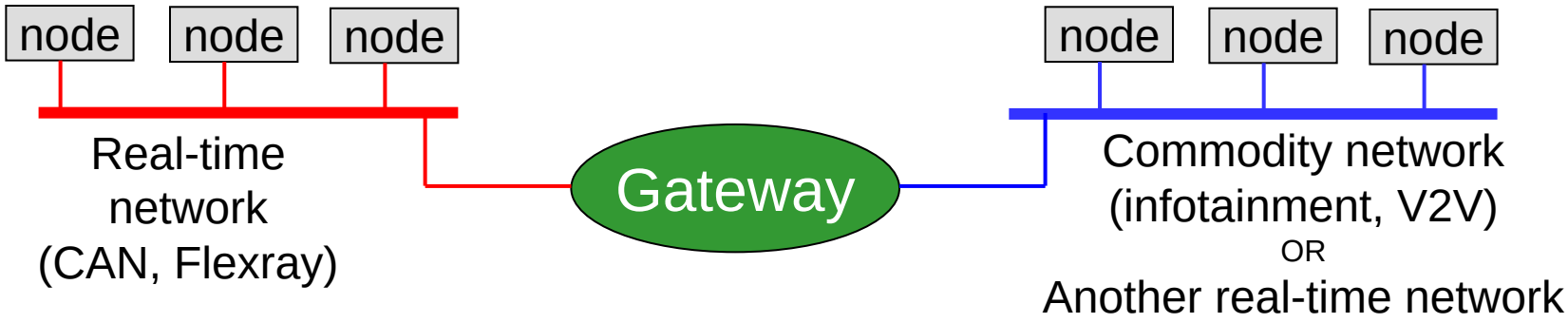
Time Triggered Operation

- **Embedded systems have many periodic functions**
  - Rotating machinery control
  - Closed-loop control equations that assume periodic samples
  - Periodic schedules for worst-case delay assurance
- **Embedded control networks are optimized for:**
  - Periodic messaging
  - Small message size to minimize bandwidth cost
  - Safety critical messages are time triggered for determinism



Idea: Use A Queue To Smooth Message Clumping

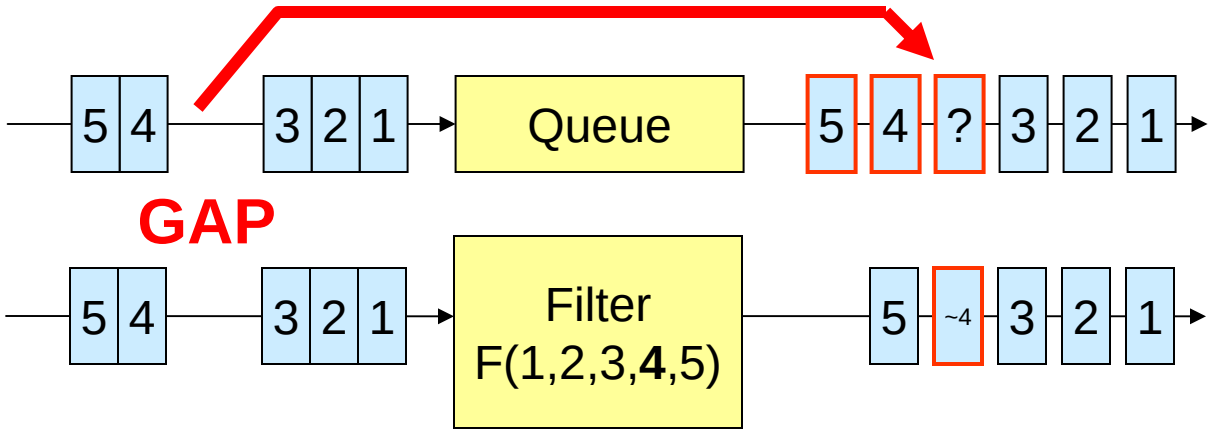
- **Clumping of messages from enterprise-side is a problem**
  - Could be an attack … or a fault … or normal operation



- **The usual way to deal with this is adding a queue**
  - But, will that work with a time-triggered embedded system?
  - Once a periodic slot is missed, that bandwidth is wasted
  - Problem is that it is difficult for embedded side to "catch up" if it gets behind

[Ray & Koopman, DSN 2009]

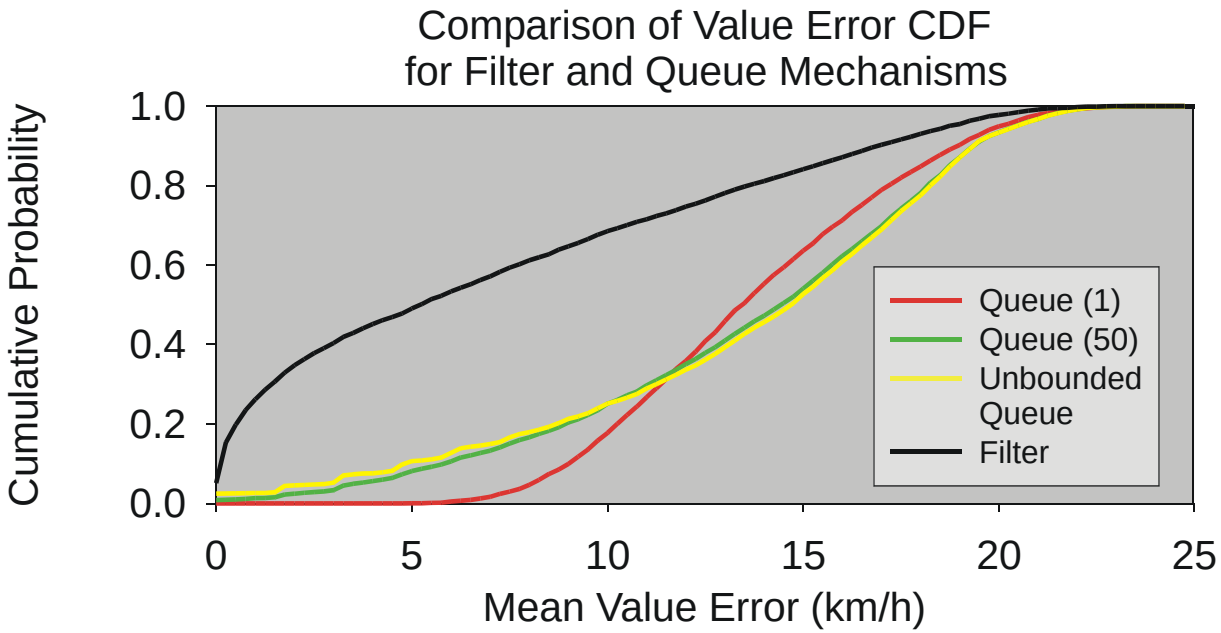
A Simple Filter Mechanism

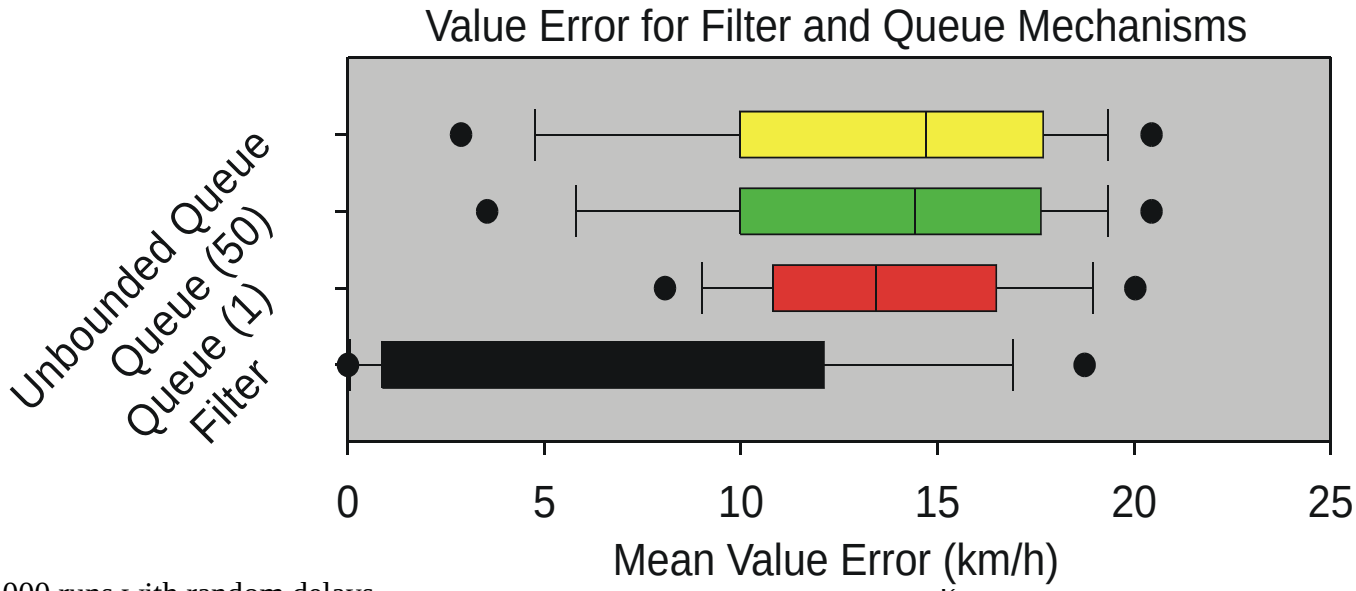


[Ray & Koopman 2009]

- **Missing data (underflow) is approximated by model**
- **Late data is stored in the model but not transmitted**
  - Reduces delays
  - Late data improves future approximations
- **Our model uses a zero-order approximation**
  - Use most recently arrived value
  - Repeat last value if no new value
    - (e.g., in above, "~4" is just "3" sent again)

Filter Results On Several Driving Scenarios





[Ray & Koopman 2009]

5000 runs with random delays

Carnegie Mellon

Preliminary Conclusion: Queues Are Bad

- **Queues are designed to get all the info delivered**
  - Over-provisioning the embedded network is too expensive
- **But, we don't necessarily care about all the info…**
  - … it's much more important to have **current info**
  - Leaving out the queue might be the right answer
    - Zero order filter means no queue at all
  - For this experiment **"No Queue"** was better than any queue
- **Potential better idea: use data filtering**
  - Use a data filter of some sort to aggregate clumped data
  - Probably the data filter will be application specific

Wrap-Up

- **Remote access to embedded systems is a big concern**
  - Probably typical enterprise security techniques will be inadequate
  - Enables IT systems to release energy via actuators

- **The interface between embedded + Internet is tricky**
  - Different computational and communication assumptions
  - Different assumptions about safety
  - Different assumptions about security
  - Timing and fault propagation across interface isn't straightforward

- **Example problem is "what goes in the gateway?"**
  - We think gateway will have to understand how data is used
    - Need latest value vs. need complete delivery of series of values