CPS Assurance:

Definitions, Examples, and Research Issues

Kang G. Shin
Department of EECS
The University of Michigan
kgshin@umich.edu
http://www.eecs.umich.edu/~kgshin

What are Cyber-Physical Systems?

- Composed of tightly-coupled and deeply-integrated cyber and physical parts, i.e., C and P are on par with each other!
  - Examples: Automobiles (especially, EVs), airplanes, intelligent robots, smart buildings, electric power grids, health care systems,….
- Some defining characteristics:
  - Cyber capability in every physical process and component
  - Networked at multiple and extreme scales
  - Complex at multiple temporal and spatial scales
  - Dynamically reorganizing/reconfiguring
  - High degrees of automation, control loops must close at all scales
  - Extremely heterogeneous
  - Longevity is often a must=> self-healing and self-organizing

What is then CPS assurance?

- Resilience of integrated C and P to failures, attacks, and other unexpected events
  - Assurance of C alone is NOT, e.g., highly effective IA
  - Assurance of P alone is NOT, e.g., heavy-duty locks, doors, chains
  - But C and P together is YES
- How?
  - Make C aware of the impact of its decision on P
  - Make C sense and respond to P's unassurance
  - Make P sense and respond to C's unassurance
- Examples
  - Resilient surveillance robots
  - Automobiles, trains, ships, and airplanes
  - Most, if not all, DoD systems
  - Smart buildings
  - Smart medical devices
  - Public infrastructures: power grids, water-supply systems, bridges,…
  - Etc.
- Bridges/abstractions between C and P are the key!

Example: Water-Supply Systems

- Forms mutiple loops, connecting a reservior, cities and towns
- Likely to `measure' or `sense' water quality and pressure only at reservior and kitchen faucets
- *What can we do if terorrists mount attacks on water-supply system?*
  - Where and how fast should we detect such attacks?
    - Where, what types of sensors, and how many to deploy?
    - How to collect and process sensor data?
    - How to ensure genuinity of delivered data?
    - How to ensure timeliness of data collection and processing?
  - *How to recover?*
  - *How to prevent?*

A Common Misconception

- Majority of CPSes must sense, process, and respond both correctly and in time
- But cyber security concerns have often been decoupled from their impacts on P, e.g., timeliness and other metrics.

Very secure but late response may be useless or even harmful!

CPS Assurance

- Now, we know how to guarantee CPS timeliness and achieve a certain level of fault-tolerance, each *in isolation*
- But their integration is still hard.
- Adding security/privacy makes it harder, especially in view of heterogeneity and scale of CPS devices, protocols, apps, and operating envrionments
- *One-fits-all solution* is unacceptable and strong inter-dependencies exist among different assurance dimensions and abstraction layers

  => Need to customize by capturing and optimizing tradeoffs

Secure CPSes

- Unlike patch-after-failure for desktops and clusters, CPSes often must *continue operation* in spite of security compromises/threats

  => Must self-secure and self-organize

- Heterogeneity of CPS architectures provides multiple attack opportunities

- Specialized, embedded, secure storage silicon and coprocessors offload security authentication and encryption tasks to dedicated hardware

Research Issues

- Science-based characterization of C-P coupling in CPS assurance context
- CPS attack and failure models
- Identification of assurance dimensions
- Characterization and optimization of tradeoffs between diff assurance dimensions
- Longevity=>self-healing and self-organizing
- Heterogeneity, scalability, and interoperability of CPS assurance solutions
- CPS assurance tailored to apps and situations
- Privacy while performing intended functions
- Usability and user education
- Social impact

Battery management
is key to green cars!

Batteries for Electric Vehicles

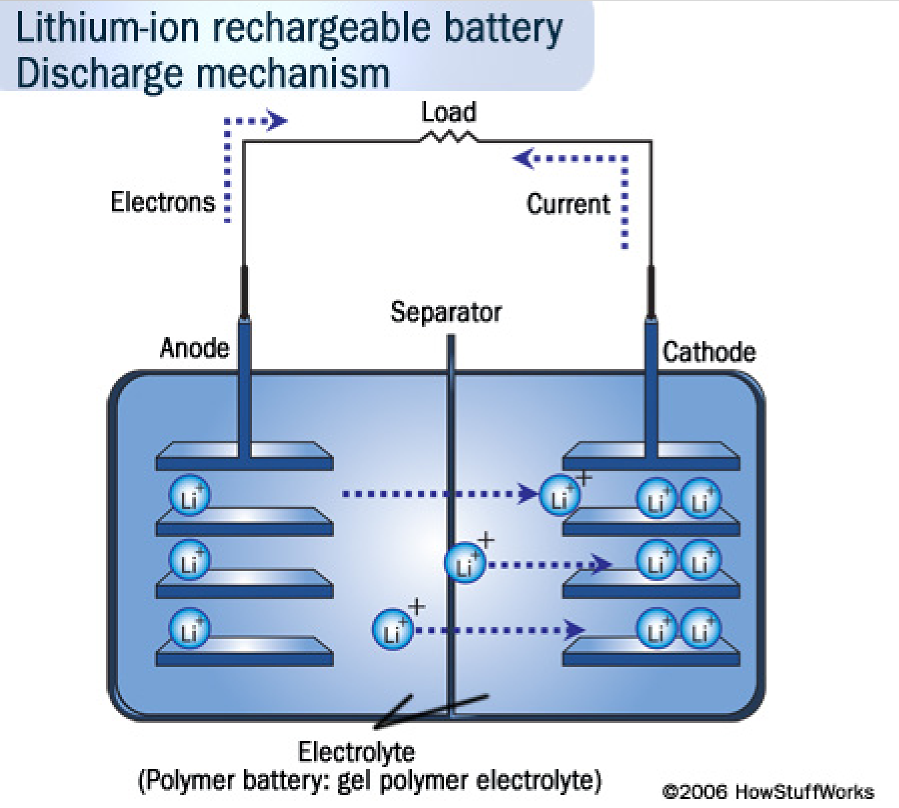
- A total of 36.0% of motorists worldwide were willing to buy a hybrid car in 2007 while 45.8% were interested in purchasing an electric vehicle
- Current Evs are powered solely by multi-cell battery packs
- The battery packs should last as long as major parts of the car, e.g., 10-15-year warranty

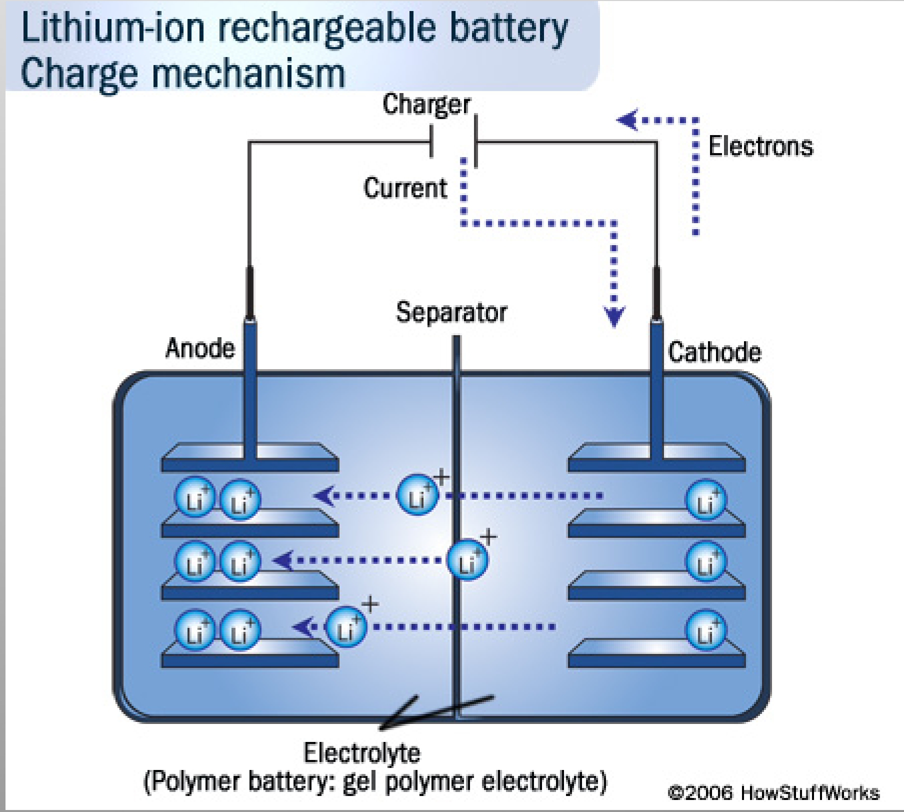
Battery Packs for EVs

Characteristics	Numbers
Manufacturer	Tesla Motor
Battery Type	Lithium-Ion (the size of a double-AA)
# of cells	6831
Output Voltage	415V
Nominal Capacity	54kWh
Charging time	4 to 7 h (via a special charger)
Mileage per charge	250 miles
Battery pack weight	900 pounds

Snapshot of Lithium-ion battery packs for EVs

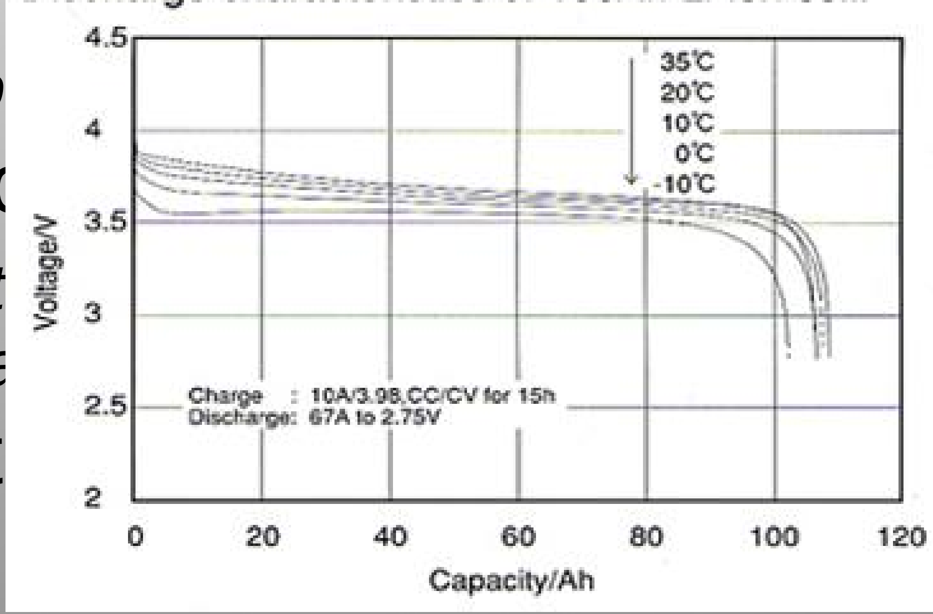
Preliminary: Lithium-ion Battery charge/discharge





Characteristics of real-life battery cells

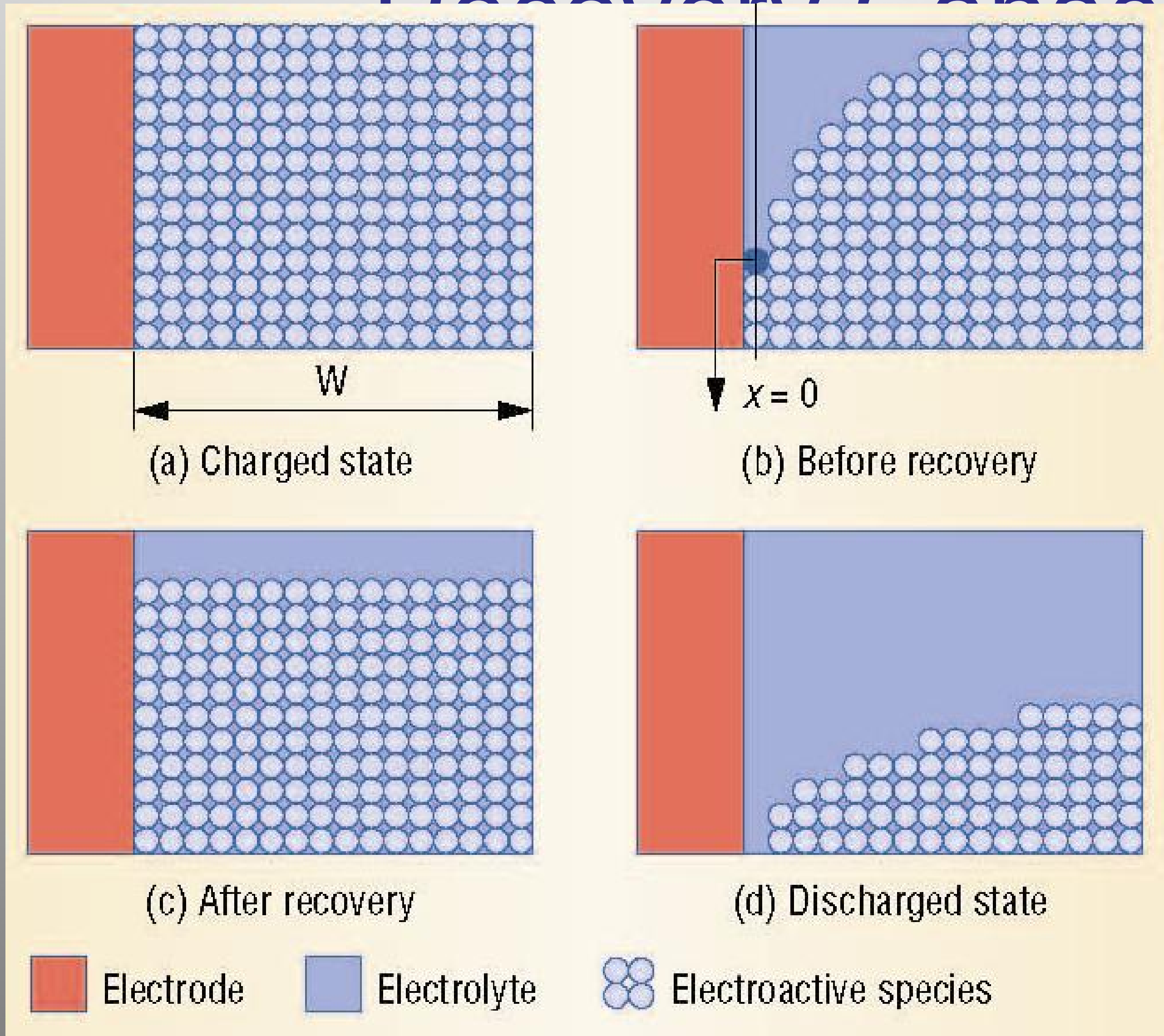
- *Battery output voltage is not constant during discharge*; feedback-based DC-DC conversion circuitry is required



Discharge characteristics of 100Ah Li-ion cell.

- *Battery capacity dep*
  current, actual c
- *Nominally equal batt*
  differences in interna
  connecting batt
  a safe design
- Batteries have some recovery capacity when discharged at high current loads

Recovery Capacity



- How much does the rest time help?

Terminologies

- *Weak/faulty cell*: its discharge rate may be larger than those of healthy cells; its impedance level may be higher (capacity decreases)
- *Dead battery*: Actual capacity retention is lower than 70~80% max nominal capacity
- *Reconditioning*: the process of adding appropriate chemical to a (lead acid) battery and properly charging it; of eliminating memory effect on a (NiCd/NiMH) battery

Problems

- Failure rate for an *n*-cell battery pack will be *n* times the failure rate of the individual cells
- Charging/discharging rate, battery temperature, ambient temperature, internal gas pressure, internal impedance, aging, etc., have a great impact on the battery condition
- Replacing *faulty/dead cells* in the pack is unrealistic because unpacking not only risks damaging other healthy cells, but they also become weaker
- Replacing *entire pack with faulty cell(s)* increases costs and also requires effective battery management

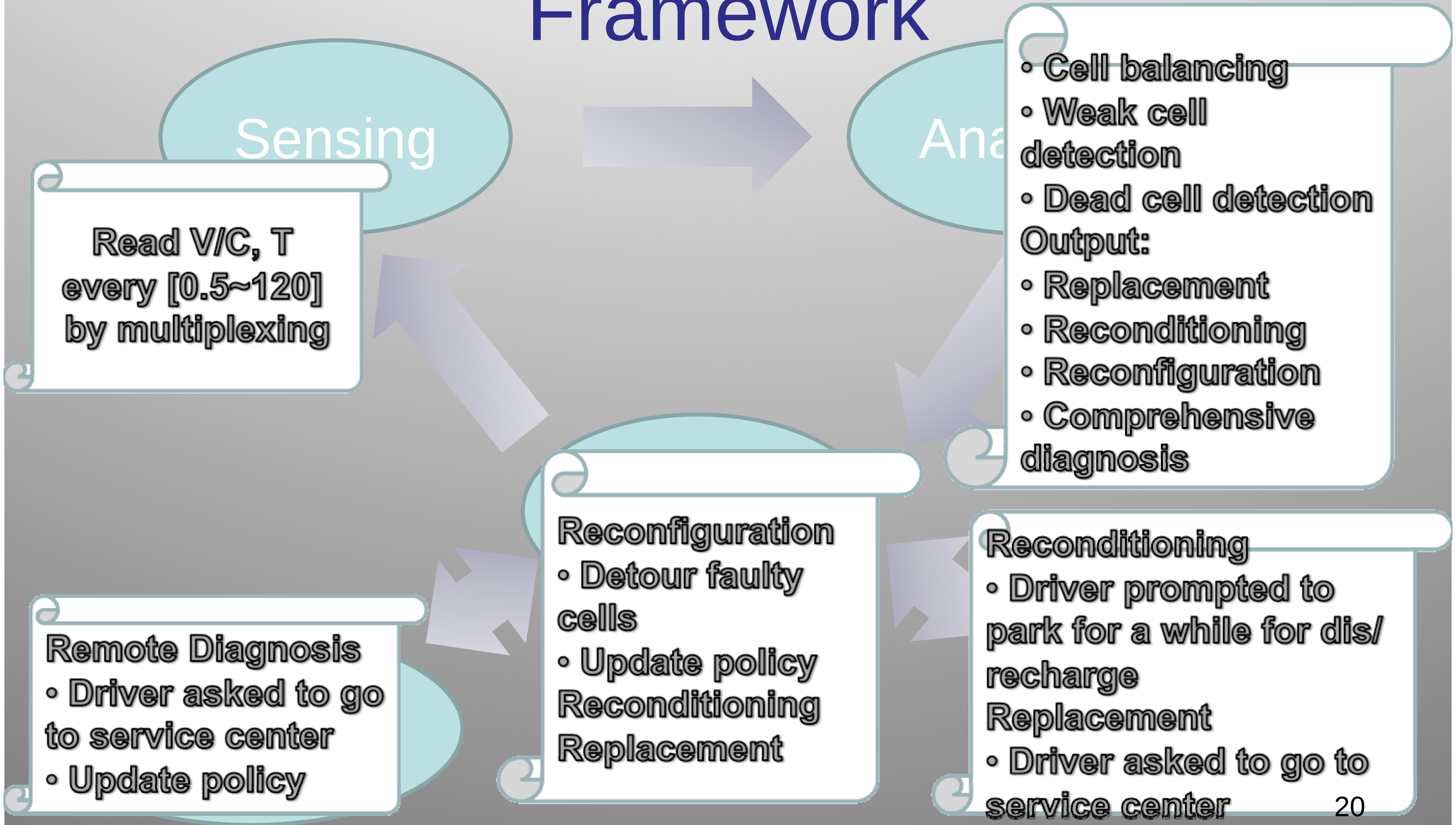
Objectives of Our Research

- Increase the *actual capacity*, the amount of energy that can be drawn from the battery packs
- Make each entire battery pack robust against *weak/dead cells* without replacing them
- Offer an effective and comprehensive diagnosis and hence reduce maintenance costs

What we propose

- Dependable Battery Management Framework
  1. Configurable battery cell arrangement
  2. Dynamic load balancing
  3. Comprehensive diagnosis
  4. Adaptive control via a feedback loop
- 50% increase in battery lifetime expects to be achieved

Key Components of Our Framework



Main References

1. Bruni *et al.* “Discharge Current Steering for Battery Lifetime Optimization”, Trans. On Computers, 2003
2. Chiasserini *et al.* “Energy Efficient Battery Management”, JSAC in Comm. 2001
3. Alahmad *et al.* “Battery switch array system with application for JPL’s rechargeable micro-scale batteries”, J of Power Sources, 2007
4. Linden *et al*., “Handbook of batteries”, 2002

More details from RTAS09 and RTSS09 proceedings

Thank You!‼