SRI International

Securing the Future of Transportation
— Some Challenges and Research Directions

Ulf Lindqvist, Ph.D.
Program Director, Infrastructure Security Research
Computer Science Laboratory
SRI International

Presented at the 2014 NSF National Workshop
on Transportation Cyber-Physical Systems

What Is A Research Agenda?

- The basic questions a research agenda should answer:
  - Where are we today?
    - What are the current technology and research?
    - What are the important technology gaps and research problems?
  - Where do we want to be X years from today?
    - What will solutions look like?
    - What will the solutions enable us to do?
  - What will it take to get us there?
    - How can we divide the problem space?
    - What can be done in the short, mid, and long term?
    - What resources are needed?
  - How will we know that we got there?
    - How should we evaluate technologies and validate results?
    - What are the metrics of success?

Safety Requires Security

- Safety drives automation in transportation
- The assumption is that a computer system is much more likely to make timely and correct decisions than a human
- However – we cannot have safety without security from intentional attacks
- Consequences for attacks on CPS: Potential loss in terms of human lives and health

→ We must have better security in CPS than in current IT systems

Which Car Has Better Safety?

Which Car Has Better Safety?

5-star safety ratings from NHTSA, www.safercar.gov

Which Car Has Better Cybersecurity?

Which Car Has Better Cybersecurity?

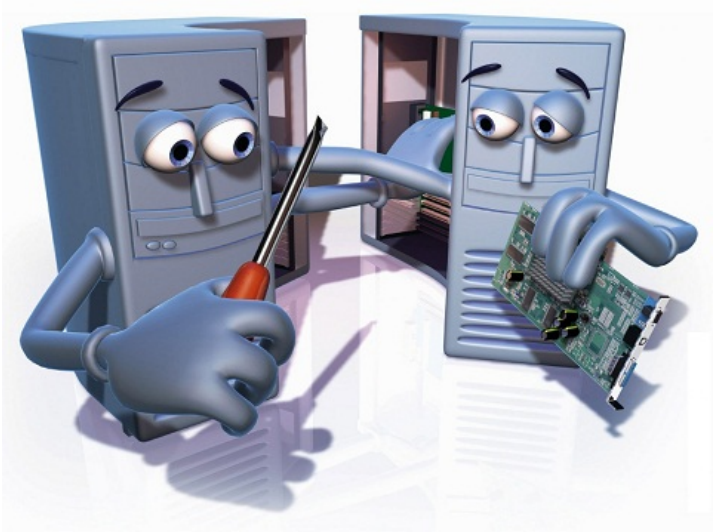
?

Vision #1

By the year 2020, all new automobiles on the consumer market will go through a mandatory comprehensive cybersecurity assessment with a resulting rating similar to the 5-star safety rating system

Robustness and Resilience

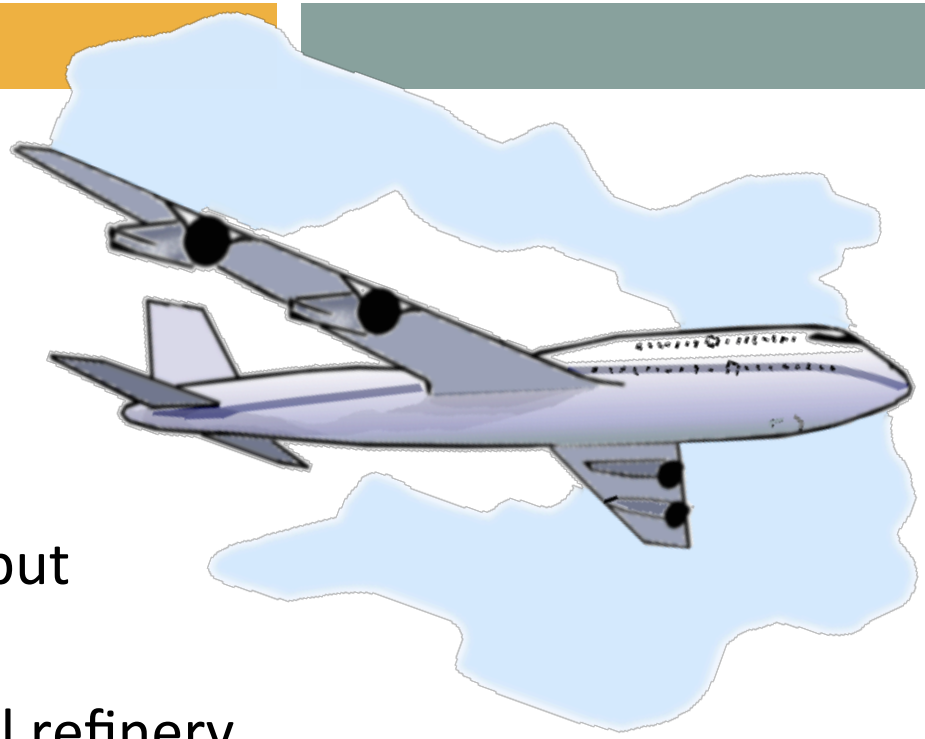
- Development is fast-paced and feature-driven
- Vulnerabilities will be repeatedly introduced
- CPS must have strong robustness and resilience properties
- Limit the scope and effect of vulnerabilities and attacks
- Desirable capabilities:
  - Self-healing
  - Intrusion tolerance
- Research areas:
  - Verifiable security properties
  - Automated attack detection, diagnosis, and response



Vision #2

By the year 2025, there are automobiles on the consumer market with a built-in transparent capability to automatically detect and safely react to any cyberattacks against its on-board systems

Safe At Any Speed



- Mass transit (rail, air) are traditional targets for terrorism
- Stationary CPS has challenges, but transportation CPS are mobile
- In a a manufacturing plant or oil refinery, safety systems can shut down control systems in a fail-safe manner
- For an aircraft flying at cruising altitude, what does a **safe system shutdown** look like?
- A CPS must be able to maintain safety, as defined by its particular application, even when it is under cyberattack

Vision #3

By the year 2020, all safety requirements and certifications of rail and aviation CPS include stringent cybersecurity metrics and assessments

Thank You

Ulf Lindqvist
650.859.2351
ulf@sri.com

Headquarters: Silicon Valley

SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025-3493
650.859.2000

Washington, D.C.

SRI International
1100 Wilson Blvd., Suite 2800
Arlington, VA 22209-3915
703.524.2053

Princeton, New Jersey

SRI International Sarnoff
201 Washington Road
Princeton, NJ 08540
609.734.2553

Additional U.S. and international locations

www.sri.com