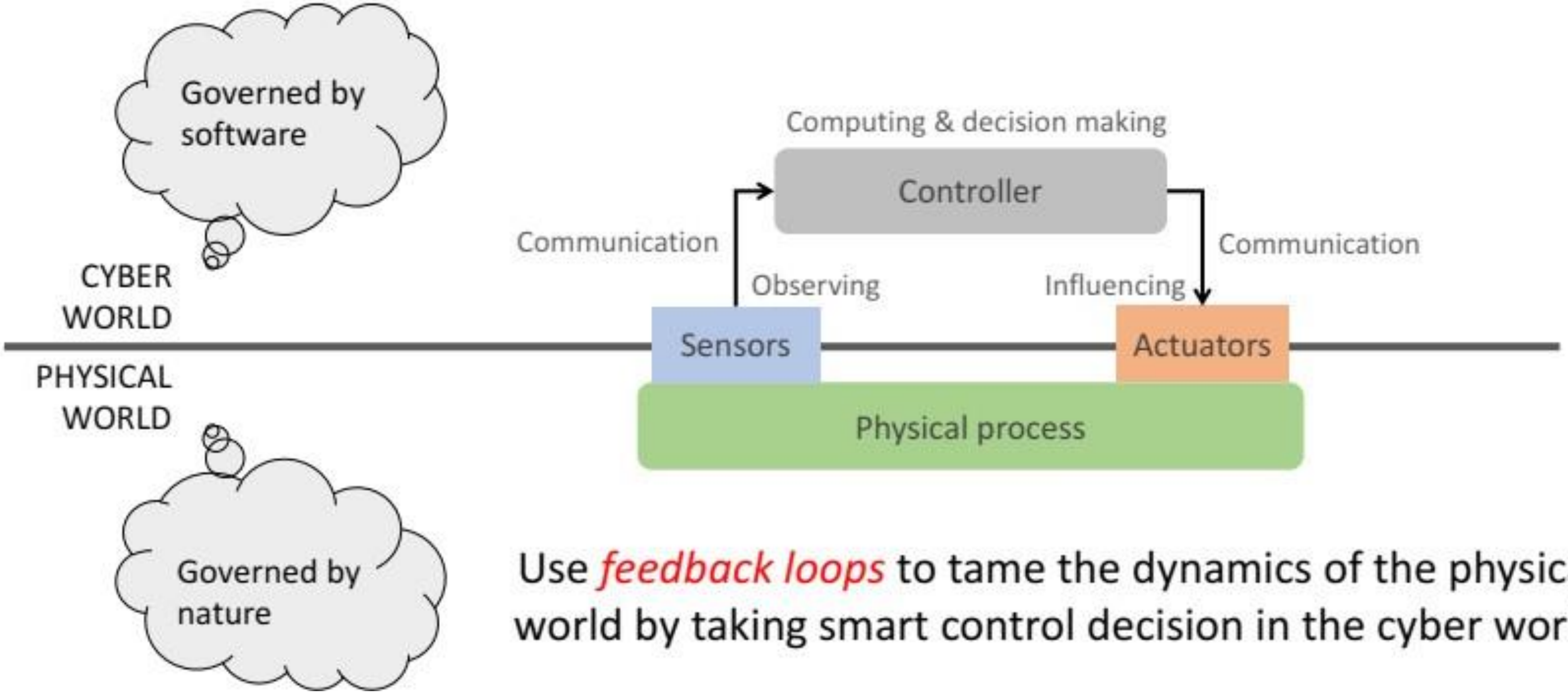
Cyber-Physical Systems

Cyber-physical Systems (CPS): Overview



Use *feedback loops* to tame the dynamics of the physical world by taking smart control decision in the cyber world

Cyber-physical Systems (CPS): Definitions

- [Lee07]: “A cyber-physical system (CPS) is an integration of computation with physical processes.”
- [Raj10]: “Cyber-physical systems (CPS) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core.”
- [Der11]: ”Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa. The design of such systems, therefore, requires understanding the joint dynamics of computers, software, networks, and physical processes.”

[Lee07] E. Lee, Computing Foundations and Practice for Cyber-Physical Systems: A Preliminary Report, 2007.
[Raj10] R. Rajkumar et al., *Cyber-Physical Systems: The Next Computing Revolution*, Proc. of DAC, 2010.
[Der11] P. Derler at al., *Modeling Cyber-Physical Systems*, Proc. of the IEEE, 2011.

Cps applications include:

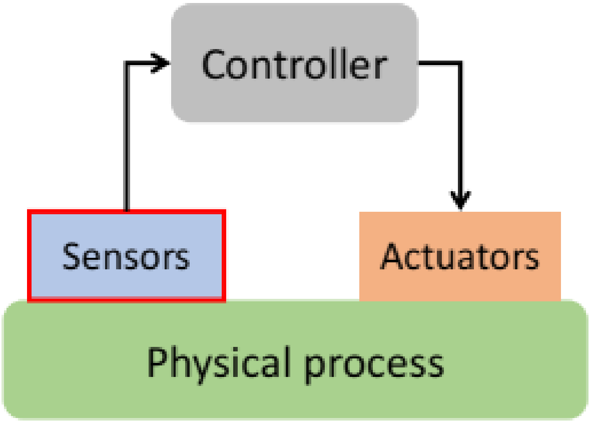
High confidence medical devices and systems
Traffic control and safety
Advanced automotive systems
Process control
Energy conservation
Environmental control instrumentation
Critical infrastructure control (electric power, water resources)
Communications systems
defense systems
manufacturing.

Sectors	Opportunities	
Transportation	Aircraft that fly faster and further on less energy. Air traffic control systems that make more efficient use of airspace. Automobiles that are more capable and safer but use less energy.	
Defense	More capable defense systems; defense systems that make better use of networked fleets of autonomous vehicles.	
Energy and Industrial Automation	New and renewable energy sources. Homes, office, buildings and vehicles that are more energy efficient and cheaper to operate.	
Health and Biomedical	In-home healthcare delivery. More capable biomedical devices for measuring health. New prosthetics for use within and outside the body. Networked biomedical systems that increase automation and extend the biomedical device beyond the body.	
Agriculture	Energy efficient technologies. Increased automation. Closed-loop bioengineering processes. Resource and environmental impact optimization. Improved safety of food products.	
Critical Infrastructure	Highway systems that allow traffic to become denser while also operating more safely. A national power grid that is more reliable and efficient.	

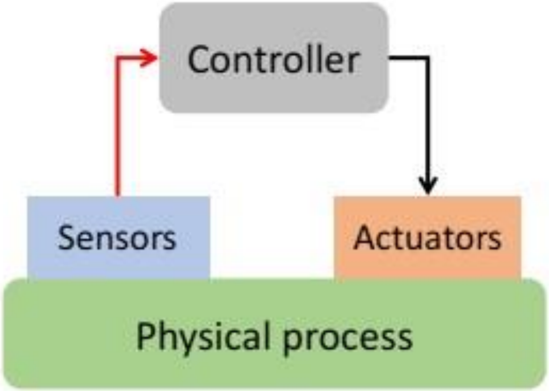
CPS Requirements

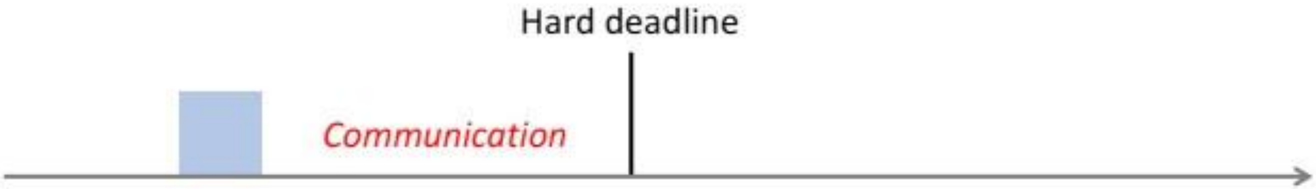
1. **Safety**
   - All such systems interact with the environment.
   - System failure can have catastrophic consequences.
   - System correctness depends on both logical results and the time at which results are produced (real-time).
2. **Performance**
   - Safety is number#1 requirement, but we still need to achieve sufficient performance.
   - Many systems are resource constrained (in either weight, power, cost, etc.)
3. **Interoperability**
   - Individual subsystems connected by open protocols.

Example: Timing Predictability

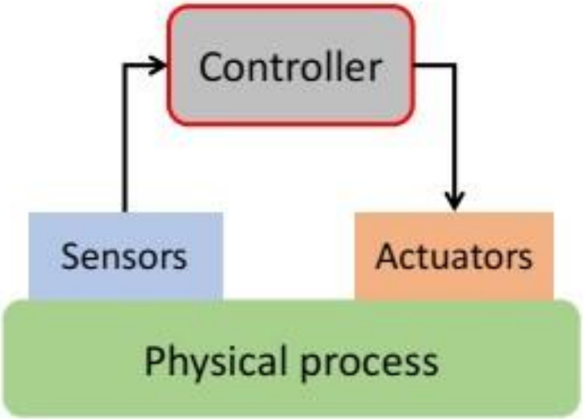


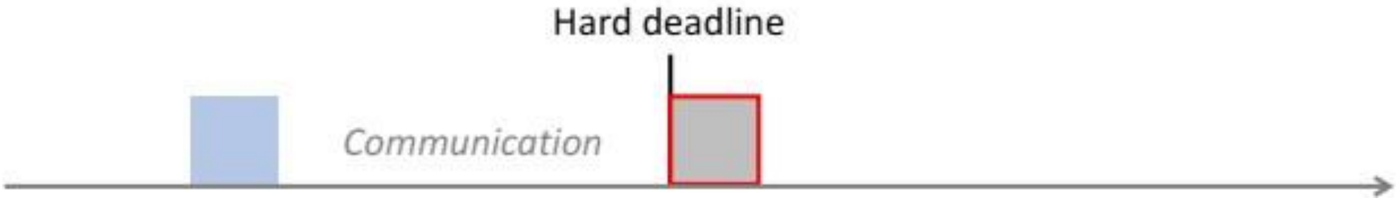
Example: Timing Predictability





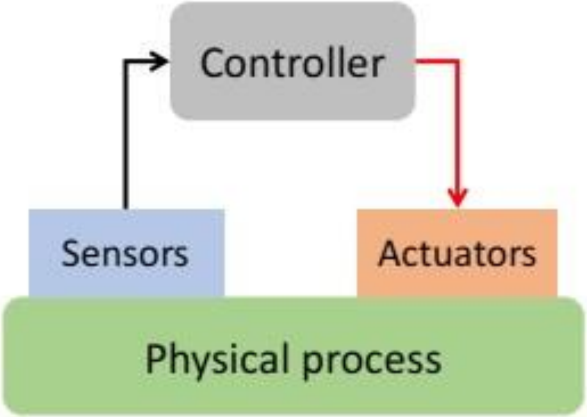
Example: Timing Predictability

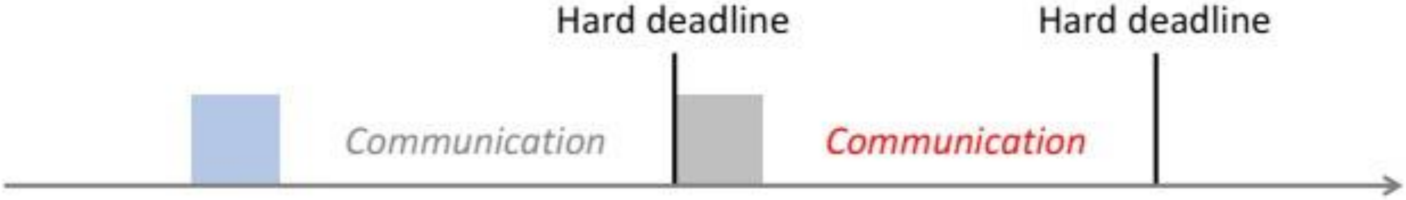




i

Example: Timing Predictability





CPS as multidisciplinary approach

Within ECE, CPS design requires competences in…

- Computer Architecture
- CAD & Embedded Design
- Software Engineering
- Control
- Formal Verification
- Real-Time Analysis

… plus whatever engineering field(s) are related to the design of the plant/actuator.

Problem: all such field and subfields have very different design & development conventions.

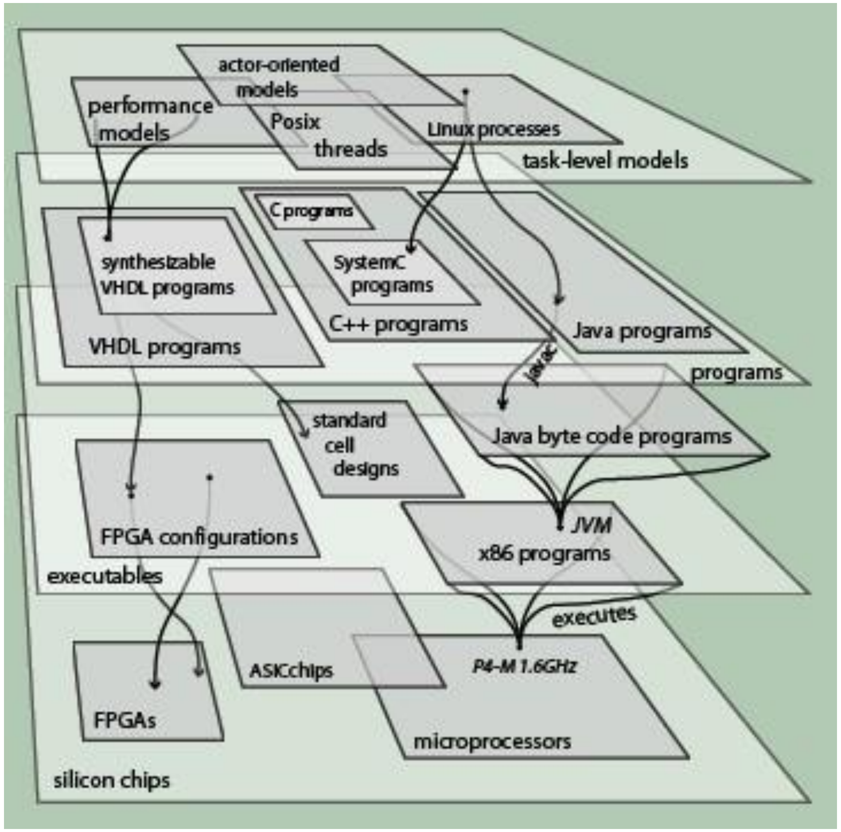
Perhaps we need a new science of CPS design?

CPS Challenges – Design Abstractions

BITS Pilani

We could argue that the biggest design challenge is in abstractions – the entire ECE design is a stack-based process.

- Unfortunately, most such abstractions do not directly encapsulate characteristics of the environment such as:
  - Concurrency
  - Criticality
  - Timing
- It is very hard to predict if the cyber part will meet the requirements of the physical part!



(from Prof. Edward Lee)

The principle we need to follow

Technologically feasible: Components at any level of abstraction should be made predictable and reliable.

not technologically feasible: then the next level of abstraction above these components must compensate with robustness.

For example :It is harder to make wireless links predictable and reliable. So we compensate one level up, using robust coding and adaptive protocols.

Memory systems Example :

Designers of memory systems, despite the high reliability and predictability of the components, still put in checksums and error-correcting codes.

If you have a billion components (one gigabit RAM, for example) operating a billion times per second, then even nearly perfect reliability will deliver errors upon occasion.

C Example:

At the foundations of computer architecture and programming languages, software is essentially perfectly predictable and Reliable.

C, designers can count on a computer to perform exactly what is specified with essentially 100% reliability.

The problem arises when we scale up from simple programs to software systems, and particularly to cyber physical systems.

The fact is that even the simplest C program is not predictable and reliable in the context of CPS.

C example cont.

It may execute perfectly, exactly matching its semantics, and still fail to deliver the behavior needed by the system.

it could miss timing deadlines. Since timing is not in the semantics of C, whether a program misses deadlines is in fact irrelevant to determining whether it has executed correctly. But it is very relevant to determining whether the system has performed correctly.

A component that is perfectly predictable and reliable turns out not to be predictable and reliable in the dimensions that matter. This is a failure of abstraction.

Reliable CPS: not so much!

In 2007, 12 F-22s were going from Hawaii to Japan.

After crossing the IDL, all 12 experienced multiple crashes.

- No navigation
- No fuel subsystems
- Limited communications
- Rebooting didn't help

F-22 has 1.7 million lines of code.

F-22 Raptor

CPS Challenges - Safety

Safety is hard to guarantee in interconnected and interdependent systems.

1. **Do not trust communication channels**.

- Ex: medical plug-and-play initiative is looking to interconnect medical devices using wireless technology.
- **Problem: what happens if somebody jams the signal**?
- Each subsystem must be independently safe.

2. **Do not trust the users**.
   - Users are an (unfortunate) part of the systems.
   - Users are very error prone: over 90% of avionic accidents are caused by flight crew/controllers.
   - System must be protected against user mistakes

Verification & Certification

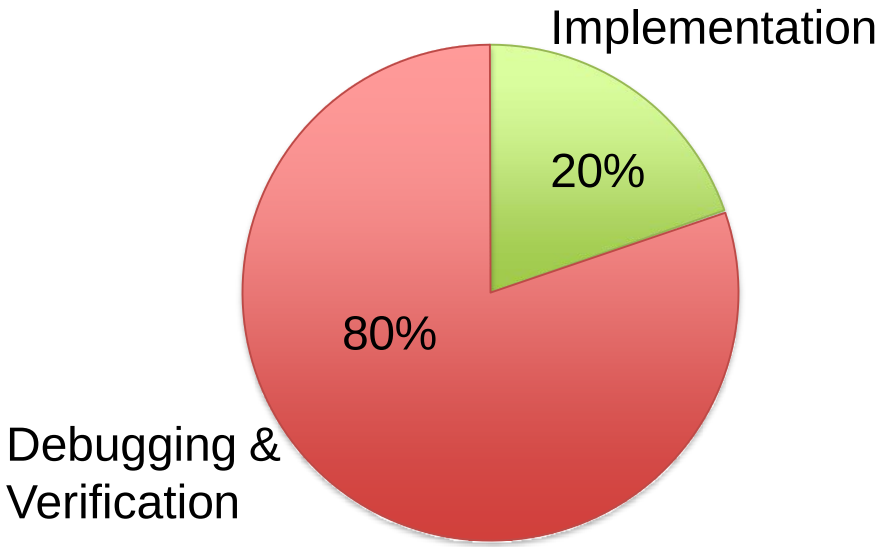
How do we ensure safety?

1. Formal Verification
   - Build a model of the systems.
   - Prove (mathematically) that the system satisfies some safety property.
   - Problem#1: no good model for the whole system.
   - Problem#2: model is not implementation.
2. Certification
   - Usually a process-based mechanism: show that you have performed all process step according to some standard (ex: DO178a/b/c, IEC 61508).
   - Typically includes extensive testing.
   - Very expensive.

CPS Challenges - Integration

Putting the system together is much more challenging that implementing the individual subsystems.
Quiz (avionic systems): can you guess what % of $ goes in implementation vs debugging?

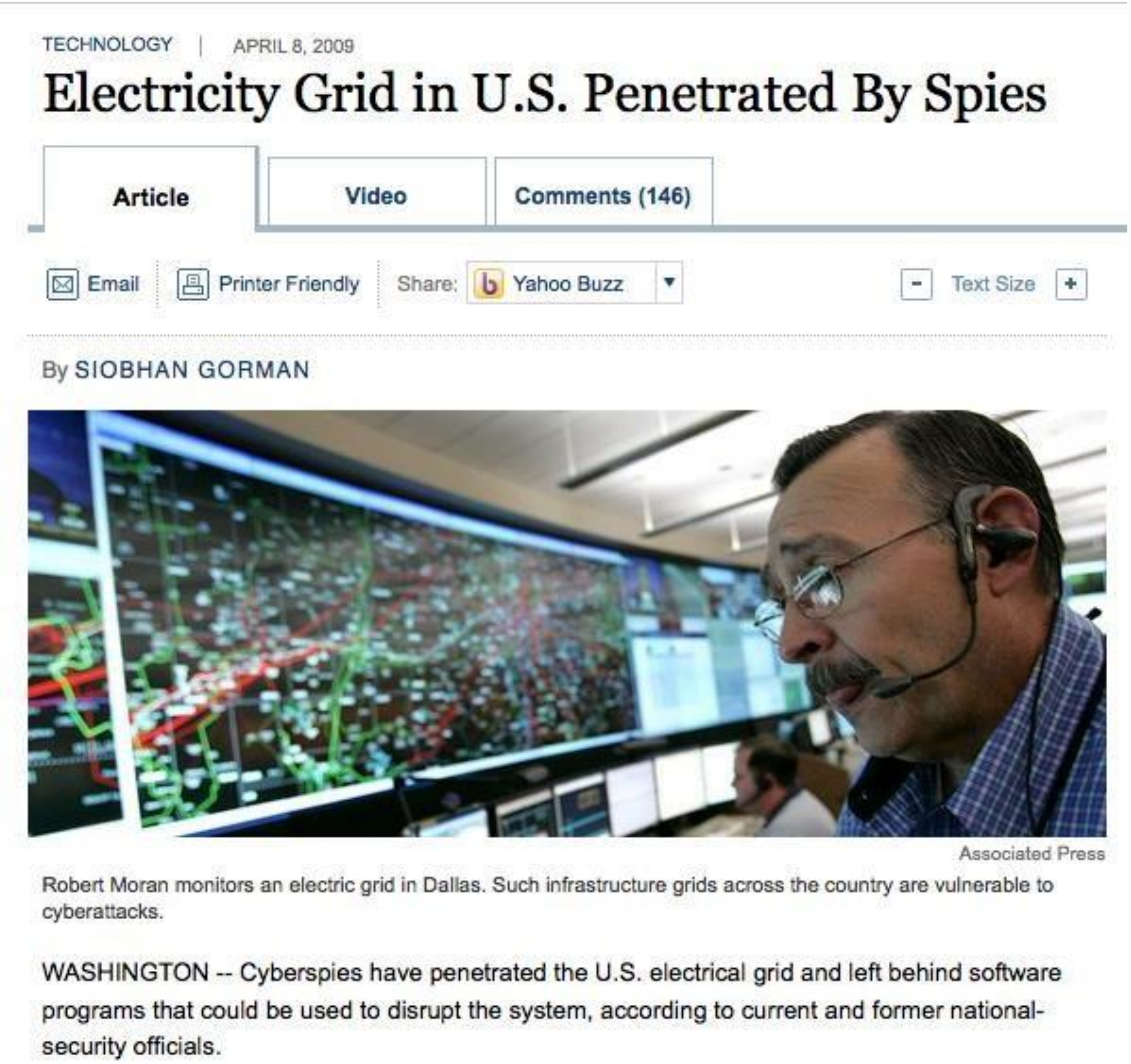
- Individual productivity for safety-critical code is reported as 6 lines/day!
  - F22: 1.7 million lines / 6 = 776 man-years
  - Perhaps the US$66.7billion program cost is not a surprise…
- Clearly the design process must be improved…



Avionic Development Cost

Security issues

BITS Pilani



TECHNOLOGY | APRIL 8, 2009

Electricity Grid in U.S. Penetrated By Spies

By SIOBHAN GORMAN

Associated Press

Robert Moran monitors an electric grid in Dallas. Such infrastructure grids across the country are vulnerable to cyberattacks.

WASHINGTON -- Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.