Cyber Security and Survivability of Current and Future Energy Systems –

Technical and Policy Challenges

Howard F. Lipson, Ph. D.

March 10, 2008

Fourth Annual Carnegie Mellon Conference
on the Electricity Industry

Outline

1. Some General Cyber Security Issues
2. Survivability Concepts
3. Energy System Cyber Security & Survivability Issues

What does Internet survivability have to do with protecting energy systems?

To support major improvements in business efficiency and decision making, energy systems are moving toward

- Highly sophisticated, fine-grained forms of control
- Ever-increasing network connectivity among control systems, business systems, and end-user devices
- Progressively more dependence upon Internet-based technologies
- Increasing Internet-connectivity

Cyber security issues

- The Internet was not designed to resist highly untrustworthy users
- The Internet was never designed for tracking and tracing user behavior
- The current threat and usage environment far exceeds the Internet’s design parameters
  - Severe real-time constraints for control systems takes this to a new level
- The expertise of the average system administrator continues to decline

Cyber security issues (2)

- Commercial-off-the-shelf (COTS) software and public domain software are ubiquitous, and widely accessible for experimentation to discover vulnerabilities

- Security is usually an afterthought in the software development life cycle
  - “patch and pray” is not enough
  - need security training & education for developers
  - need to “build security in” from the start
  - see DHS-sponsored “Build Security In” Website **https://buildsecurityin.us-cert.gov**

Cyber security issues (3)

- Systems designed for use on closed (private) networks were not engineered with the security necessary for today's Internet
  - Policies and procedures (e.g., who has access to what assets) not planned with cyber security in mind
- "Security through obscurity" often fails
- Cyber attacks are often not recognized by the victim
- General trend: more targeted ("day-zero") attacks

The Problem

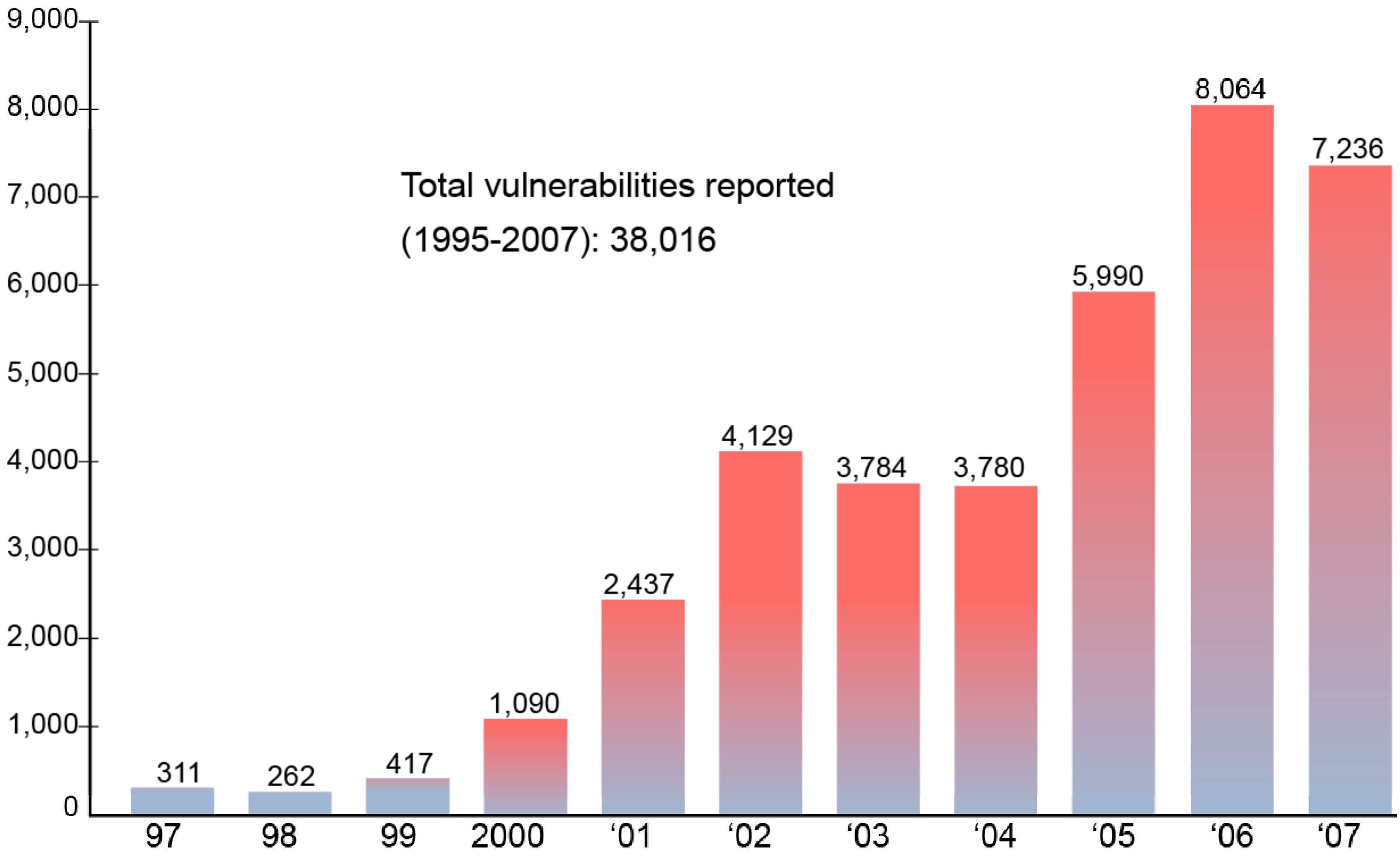
Large-scale, highly distributed systems cannot be totally isolated from potential intruders.

No amount of system “hardening” can guarantee that such systems are invulnerable to attack.

Increasing complexity of systems provides more opportunity for attackers.

Serious consequences if things go wrong.

Vulnerabilities Reported to CERT/CC



Total vulnerabilities reported (1995-2007): 38,016

Control System Software Vulnerability Coordination by CERT/CC

- As of March 2008
  - 42 reports of control system vulnerabilities
  - 14 Vulnerability Notes
  - 24 vendor contacts established

•

Survivability Concepts

Why Survivability?

Traditional computer security is not adequate to keep highly distributed systems running in the face of cyber attacks.

Survivability is an emerging discipline –

a risk-management-based security paradigm.

In the beginning . . .

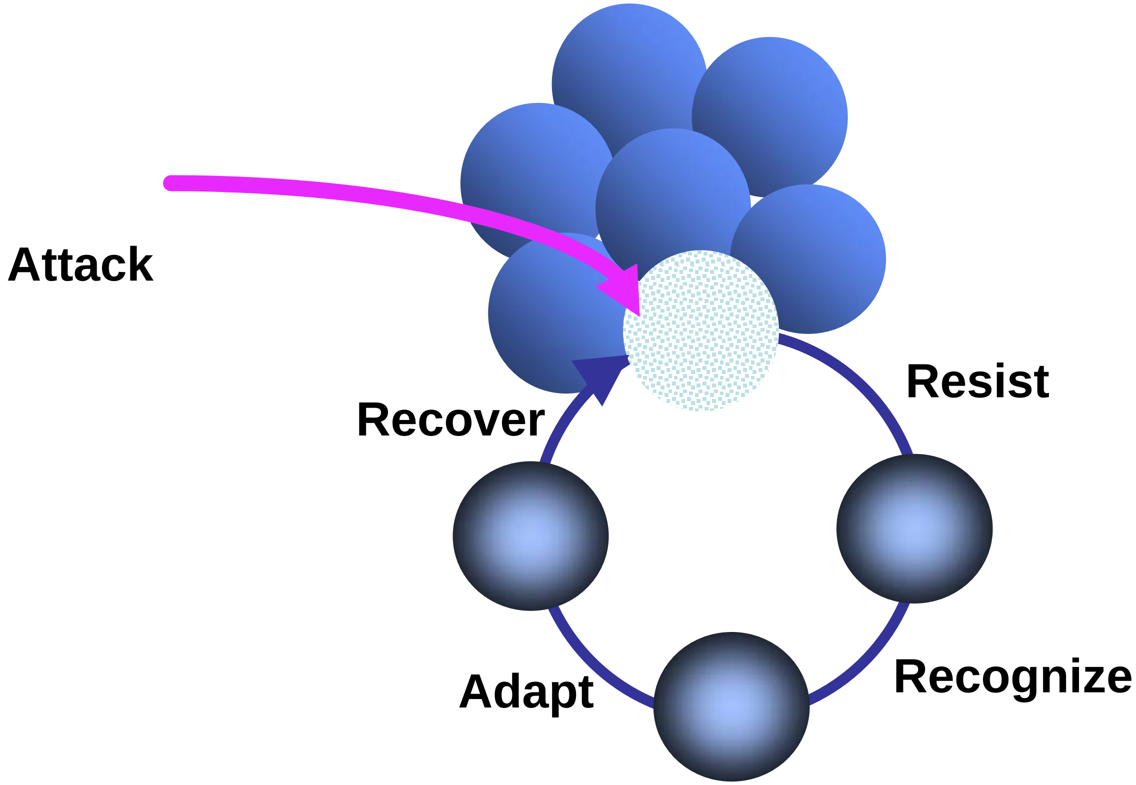
“Can we build DoD systems that will continue to operate despite a successful cyber-attack?”

DARPA (Survivability Program)

Late 1995, early 1996

Survivability

Survivability is the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.



3 R's of Survivability

Resistance

ability of a system to repel attacks

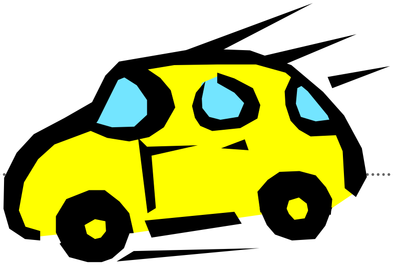
Recognition

ability to recognize attacks and the extent of damage

Recovery

ability to restore essential services during attack, and recover full services after attack

For Short-term Survivability



Deal with the effects of a crisis (survivability scenario): Car rounding a sharp curve is about to veer off a cliff.

A guardrail is a “survivability solution”, whether the underlying cause is:

- Ice on the road
- Drunken driver
- Brakes have been tampered with

For long-term survivability: Do the forensics!

An Analogy Is Becoming Reality

Emerging trend: X-by-Wire replacing mechanical and hydraulic control linkages.

X = { fly, steer, brake, ... }

Today,

- Power steering degrades to difficult but functional manual steering
- Power braking degrades to manual braking

Tomorrow ?

For Long-term Survivability

System adaptation and evolution are essential, because …

- New vulnerabilities are discovered
- New attack patterns appear
- Continual attacker-defender escalation
- Underlying technologies change
- Collaborators become competitors
- Political, social, legal changes
- Missions evolve, or change drastically

Traditional Assumptions for Information Security

- Clearly defined boundaries
- Central administrative control
- Global visibility
- Trustworthy insiders

“Fortress” Model

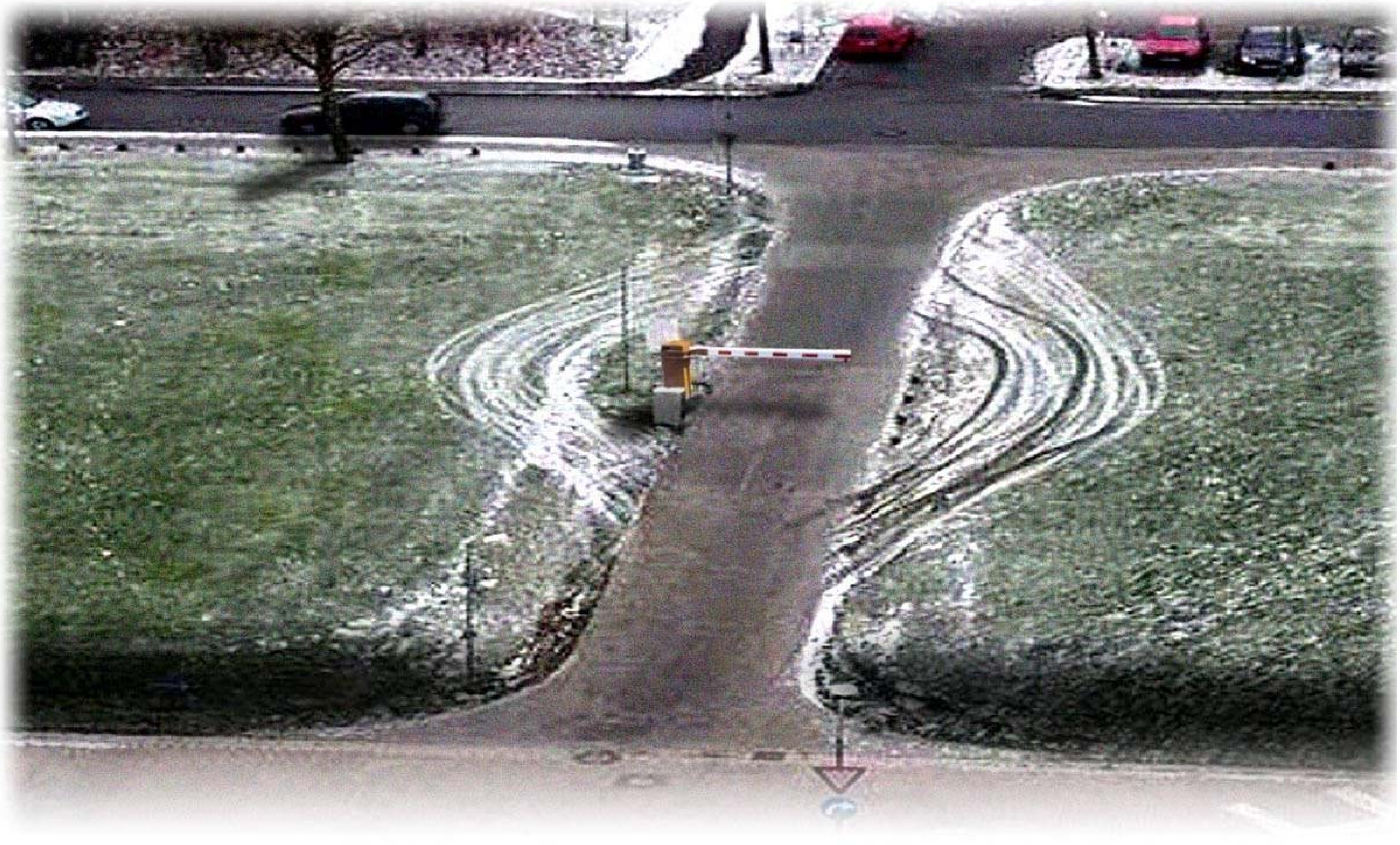
Today’s Computing Environment

~~Everything on the previous slide~~

Unbounded Systems

- No unified administrative control
- No global visibility
- Untrustworthy insiders
- Lack of complete, timely information

Bounded Thinking in an Unbounded World



Another Example of “Breaking the Model”

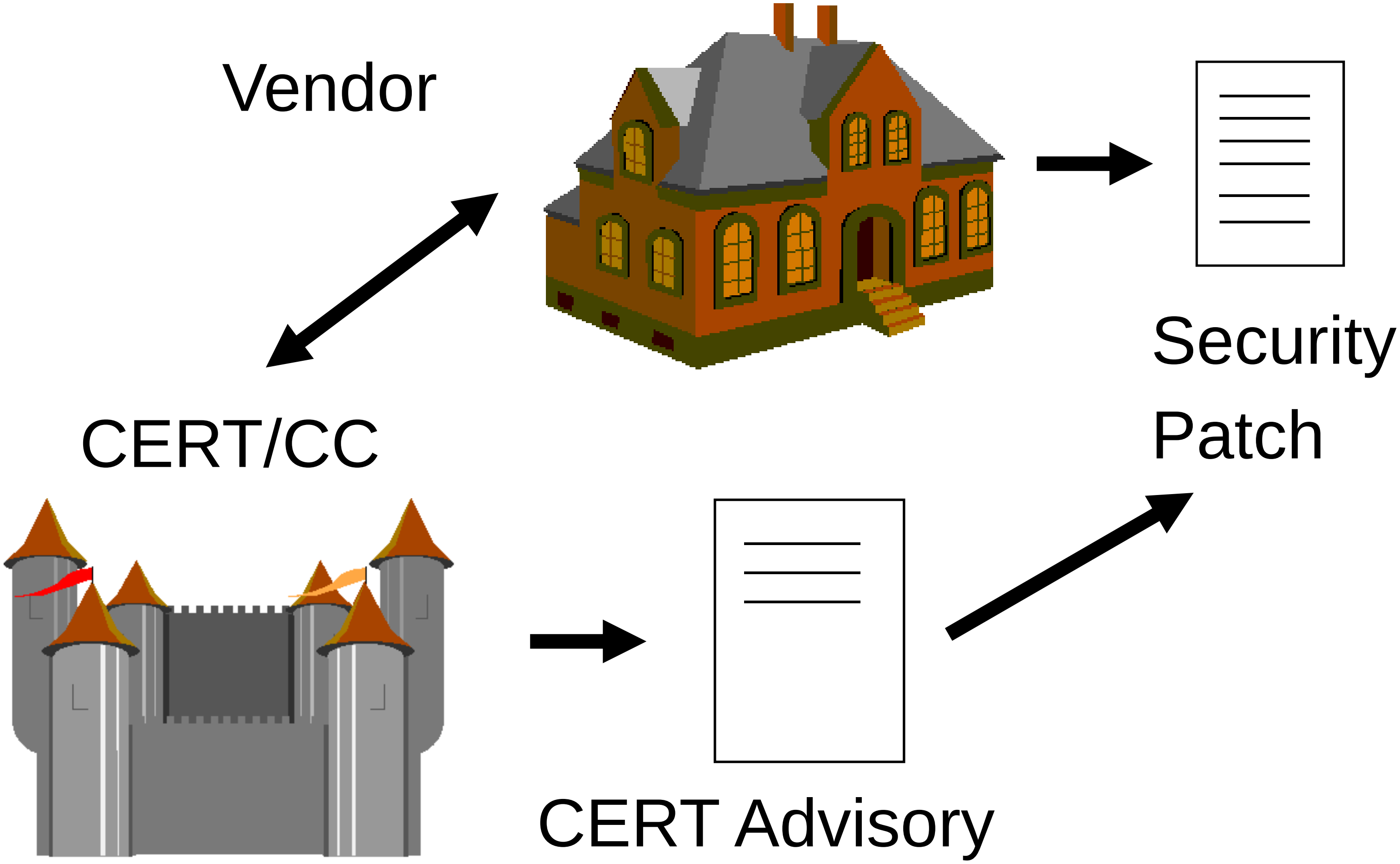
Indiana Jones Attack

A successful defense against a “saber attack”

Vulnerabilities arise when assumptions about the (threat) environment in which a system operates are incorrect or incomplete, or when presumed constraints on the behavior of a potential adversary do not reflect reality.

Personal Example: 1st Survivability Attack

Security Advisory Process



Vendor

CERT/CC

CERT Advisory

Security Patch

Fundamental Assumption

No individual component of a system is immune to all attacks, accidents, and design errors.

Characteristics of Survivability

- Survivability is an *emergent property* of a system.

- Desired system-wide properties “emerge” from local actions and distributed cooperation.

- An emergent property need not be a property of any individual node or link.

Fundamental Goal

The mission must survive.

- Not any individual component
- Not even the system itself

Mission

A very high level statement of context-dependent requirements:

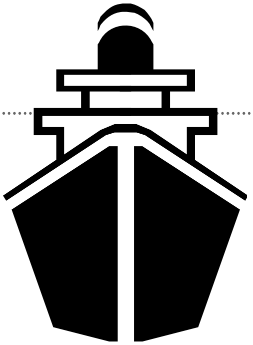
(1) Under normal usage

(2) Under stress

. . . graceful degradation

. . . essential services maintained

Example: Mission of the Titanic



Under normal conditions:

Luxurious transatlantic transportation

Under stress:

Buoyancy

Example: GridWise™ Constitution

- **“Article U - Usability Principles**

  U02 In the event of a communications failure between interacting parties, the parties must assume operating positions that best preserve stable operation of the overall electric system.”

  [*GridWise Constitution* – December 2005]

Survivability Requirements

Mission-critical functionality

- (alternate sets of) minimum essential services
- graceful degradation of services

Mission-critical software quality attributes

- security, safety, reliability, privacy, performance, usability

Requirements for the 3 R's and evolution

Survivable Systems Engineering

- Incorporate survivability into the traditional software engineering lifecycle (i.e., the Spiral Model)

- **GOAL:** To build and sustain systems with high assurance of survivability

BOTTOM LINE: A “grand challenge” problem

Survivable System Analysis

Intrusion Scenario	Softspot Effects	Architecture Strategies for →	Resistance	Recognition	Recovery
(Scenario 1) ...		Current			
		Recommended			
(Scenario n)		Current			
		Recommended			

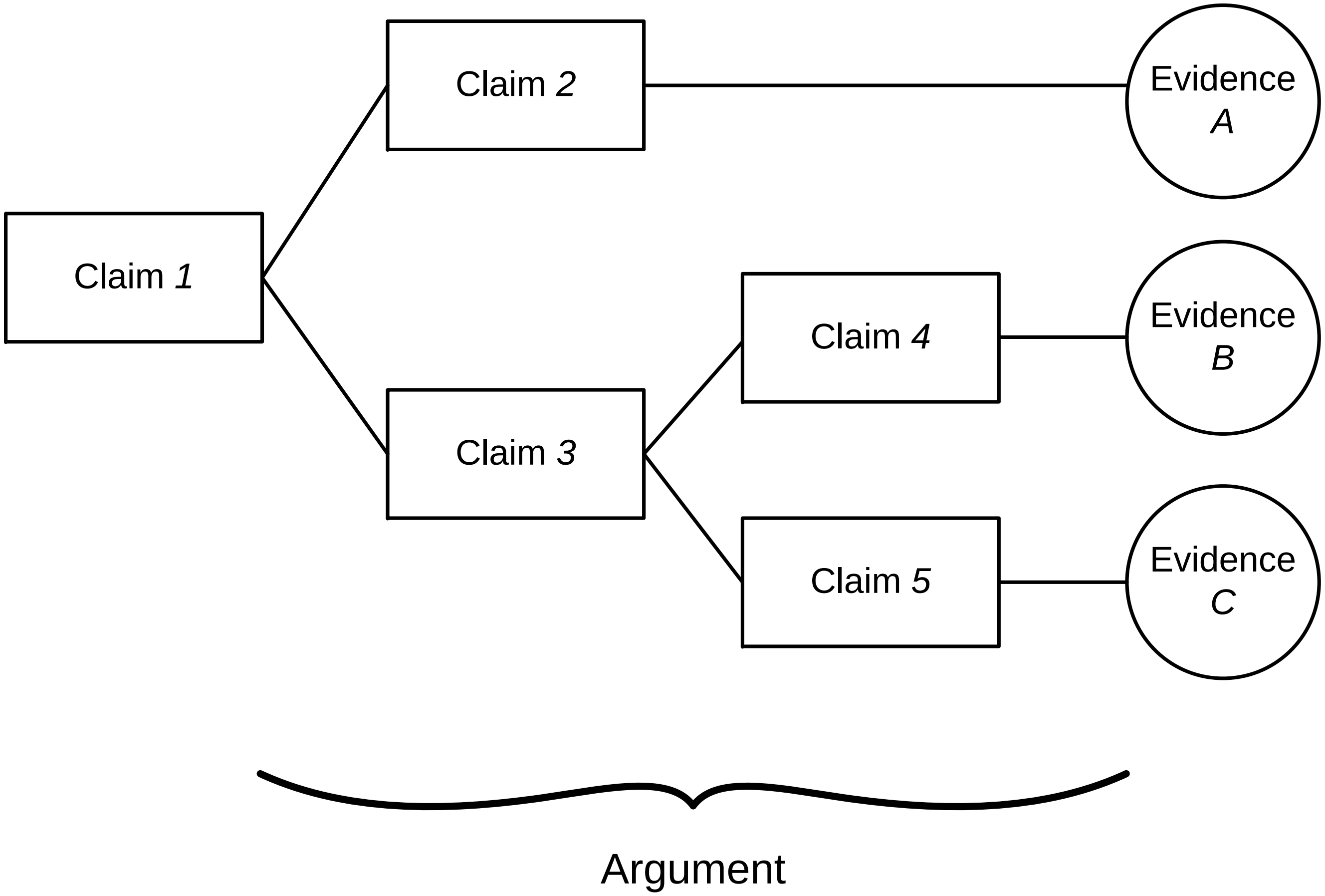
Defines survivability strategies for the three R's based on intrusion softspots

Relates survivability strategies to the architecture

Makes recommendations for architecture modifications

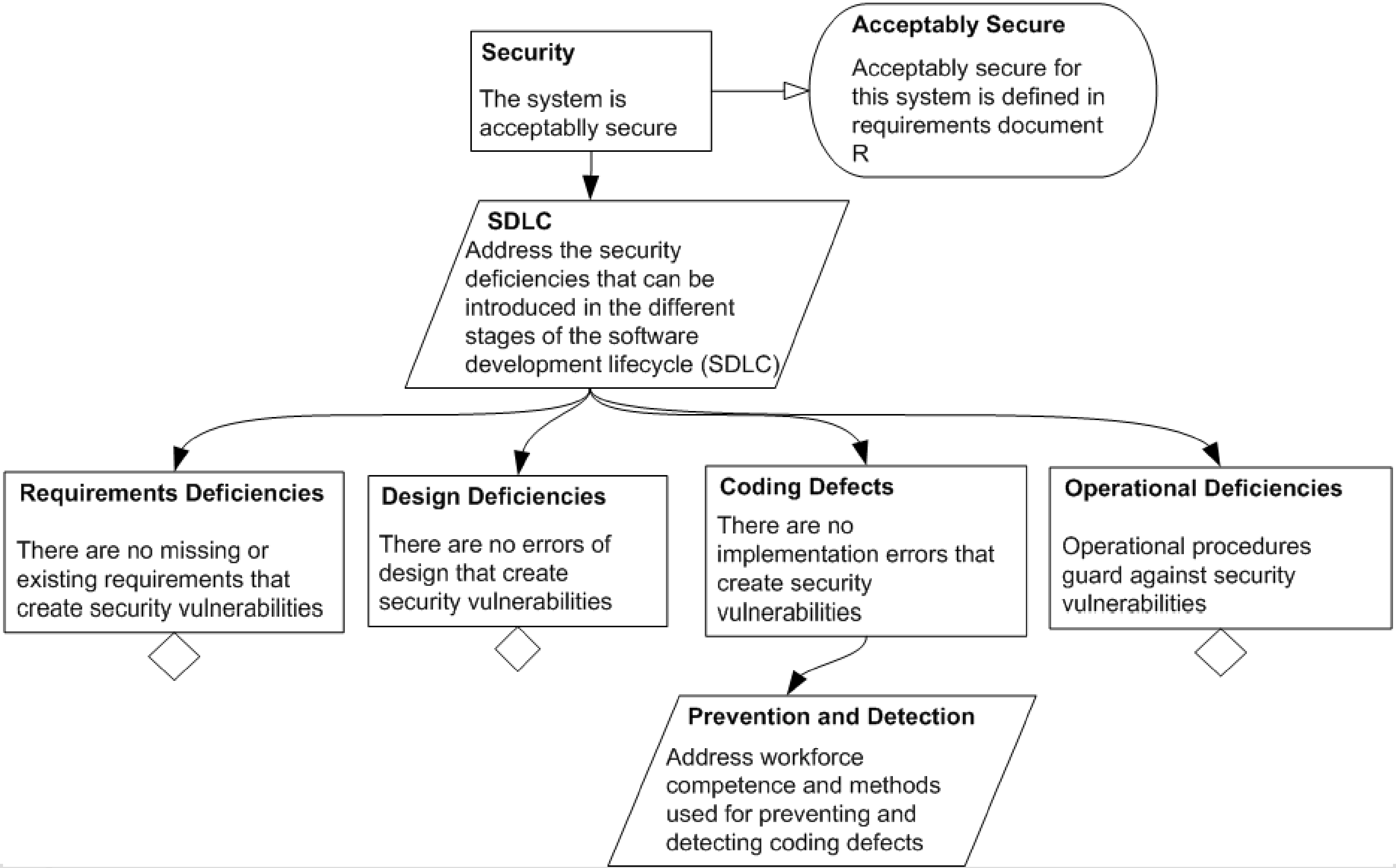
Provides basis for risk analysis, cost-benefit tradeoffs

Assurance Cases for Security and Survivability



For further info, see DHS “Build Security In” Website
https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/assurance.html

Assurance Case Example (Fragment)



Security

The system is acceptablly secure

Acceptably Secure

Acceptably secure for this system is defined in requirements document R

SDLC

Address the security deficiencies that can be introduced in the different stages of the software development lifecycle (SDLC)

Requirements Deficiencies

There are no missing or existing requirements that create security vulnerabilities

Design Deficiencies

There are no errors of design that create security vulnerabilities

Coding Defects

There are no implementation errors that create security vulnerabilities

Operational Deficiencies

Operational procedures guard against security vulnerabilities

Prevention and Detection

Address workforce competence and methods used for preventing and detecting coding defects

Evidence of Assurance

- Evidence that specific actors have the competence to correctly carry out a particular risk mitigation process

- Evidence that a given tool correctly implements a security analysis process

- Evidence that a specific actor followed a prescribed procedure *P* by applying a security analysis tool to component *C*, version *V*, on date *D*

Evidence-Based System Development

- "… the pursuit of dependability in software systems should focus on the construction and evaluation of evidence."

- "… software is 'guilty until proven innocent,' and that the burden of proof falls on the developer to convince the certifier or regulator that the software is dependable."

- "… a software system should be regarded as dependable only if it has a credible dependability case …"

[Jackson, Thomas, Millett (Editors), *Software for Dependable Systems: Sufficient Evidence?* National Research Council, 2007]

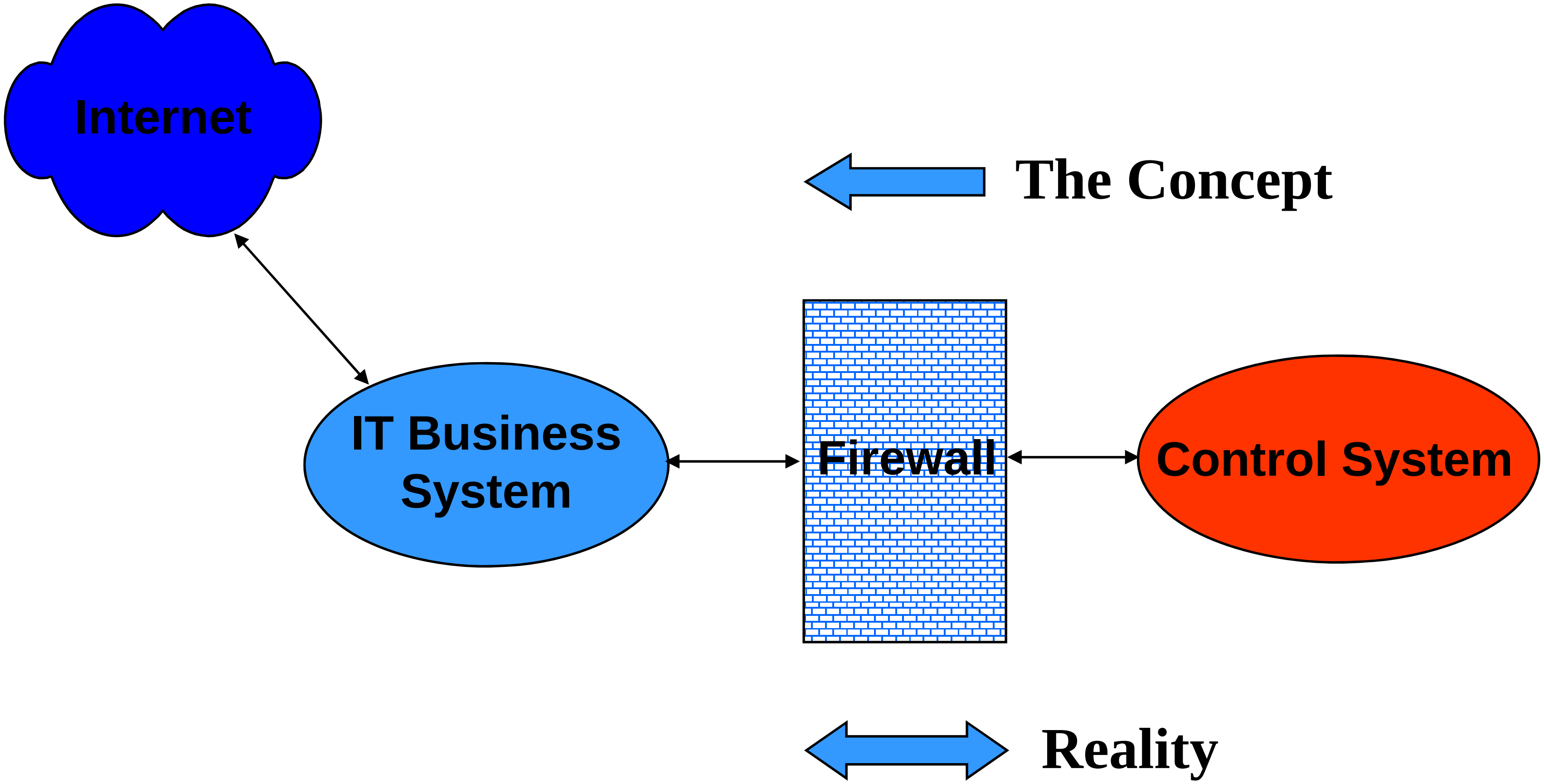
Survivability – Summary

Survivability is a blend of security and mission-specific risk management

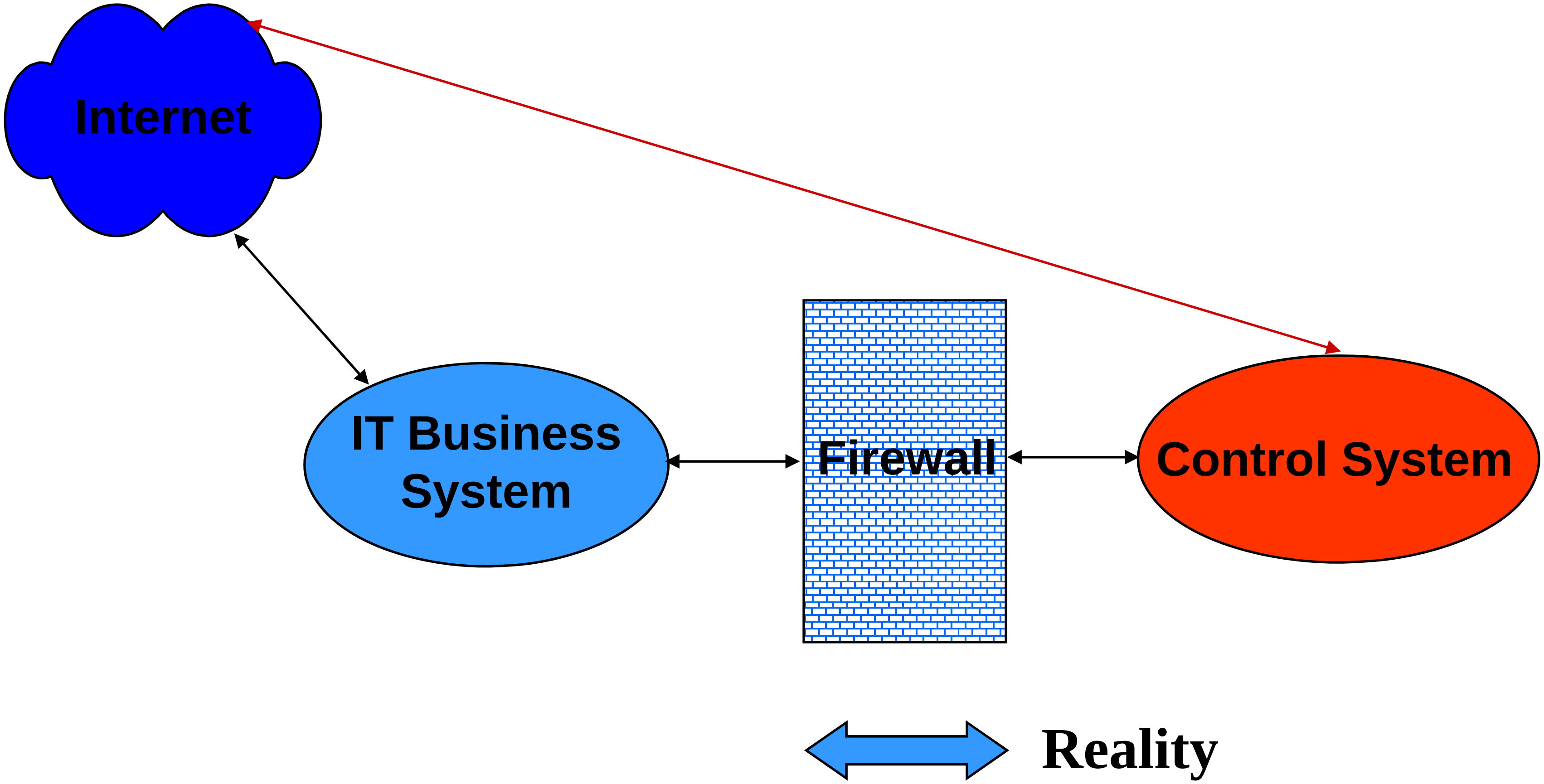
- graceful degradation
- essential services maintained
- all stakeholders must contribute
  - domain experts must be full partners

Energy System Security and Survivability Issues

Internet-connected Control System



A further dose of reality ...



Wireless Control – A Dam Good Idea?

OPEN DAM
GATE 8, 9
YES
NO

Internet connectivity issues

- Energy systems now faced with all the engineering issues associated with Internet connectivity
- Exposed to general Internet malware and attacks
- Subject to targeted attacks (“day-zero” attacks) for which no attack signatures are available
- Subject to probes and vulnerability scans in preparation for attack
- Denial of service attacks, tampering with monitoring results, or injecting malicious control requests can have disastrous consequences

Internet connectivity issues (2)

- Control system devices and protocols designed for a “closed” system environment don’t have the security properties needed in an “open” environment
  - — no strong authentication
  - — no encryption

- CPU power and storage may be too limited to support needed security tasks (e.g., encryption)

- As with IT systems, “security through obscurity” for control systems will often fail

- IT or security staff may be unaware of all Internet access points or other remote access

Internet connectivity issues (3)

- Blended threats are a major concern – multiple types of cyber attack, or attacks across multiple realms (e.g., physical and cyber)
- Security and survivability degrade over time, so continual adaptation / evolution is necessary
- Traditional long replacement / evolution cycle versus the need to react quickly to security advisories
- How can you resolve the need for rapid application of security patches with the necessity for extremely careful testing and evaluation of those patches in a control system environment?

Internet connectivity issues (4)

- Need education and training (operators, managers, software developers), new policies and procedures (including changes to physical security to protect cyber assets)
- What is the right vulnerability disclosure policy and information sharing policy for energy systems?
- As control system components move from proprietary protocols towards open standards, for use across multiple industries, the vulnerability landscape may begin to resemble that of COTS products on the Internet today
- Need an incident response coordination center, specialized for control systems

Survivability Research Issues

How do you assess and measure the survivability of control systems?

How do you effectively model, simulate, and visualize survivability in the control system domain?

What are the necessary capabilities of a test bed for control system security and survivability?

- INL - National SCADA Test Bed Program
  http://www.inl.gov/scada/

Survivability Research Issues (2)

What architectural approaches are best?

- context (scenario and domain) dependent
- must be capable of supporting rapid evolution

What control system architectures (and component mix) provide the redundancy and true diversity needed to contribute to a high assurance of survivability?

How can control system devices (components) be designed (what security and survivability properties must they have) so that they can demonstrably contribute to the overall survivability of the composite system (or system of systems)?

Survivability Research Issues (3)

What methodologies could help incorporate survivability into the engineering life cycle for control systems?

How do you manage the risks and tradeoffs to design survivable and affordable control systems?

How do you design control systems that can sustain their survivability in the face of ever-escalating attacker capabilities?

What are the survivability strategies for dealing with legacy devices coexisting with Internet-enabled devices?

Survivability Research Issues (4)

How can society’s public policy decisions be incorporated into survivability solutions?

What economic incentives for vendors, or what regulatory-legal environment would lead to enhanced survivability for control systems?

There is a full spectrum of survivability issues relating to the interdependencies and intra-dependencies of society’s critical infrastructures

For further reading …

Some of the publications I've authored or co-authored on security and survivability:

- *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*
  http://www.cert.org/archive/pdf/02sr009.pdf (Report sponsored by the U.S. State Department)
- "Survivability—A New Technical and Business Perspective on Security"
  http://www.cert.org/archive/pdf/busperspec.pdf
- "Arguing Security – Creating Security Assurance Cases"
  https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/assurance/643.html?branch=1&language=1
- *Evolutionary Systems Design: Recognizing Changes in Security and Survivability Risks*
  http://www.sei.cmu.edu/publications/documents/06.reports/06tn027.html
- "Can We Ever Build Survivable Systems from COTS Components?"
  http://springerlink.com/openurl.asp?genre=issue&issn=03029743&volume=2348
- "Emergent Algorithms: A New Method for Enhancing Survivability in Unbounded Systems"
  http://www.cert.org/archive/html/emergent-algor.html

More on survivability research is available at: http://www.cert.org/research/

Contact Info

Howard F. Lipson, Ph.D.

Sr. Member of the Technical Staff
CERT, Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA USA
lipson@cert.org
+1-412-268-7237

http://www.cert.org/research/staff/Howard_Lipson.html

Adjunct Professor
Department of Engineering and Public Policy
Carnegie Mellon University
http://www.epp.cmu.edu/