Cyber Security and Critical Infrastructure Protection

S. Massoud Amin, D.Sc.
Director, Technological Leadership Institute
Honeywell/H.W. Sweatt Chair in Technological Leadership
Professor, Electrical & Computer Engineering
University Distinguished Teaching Professor

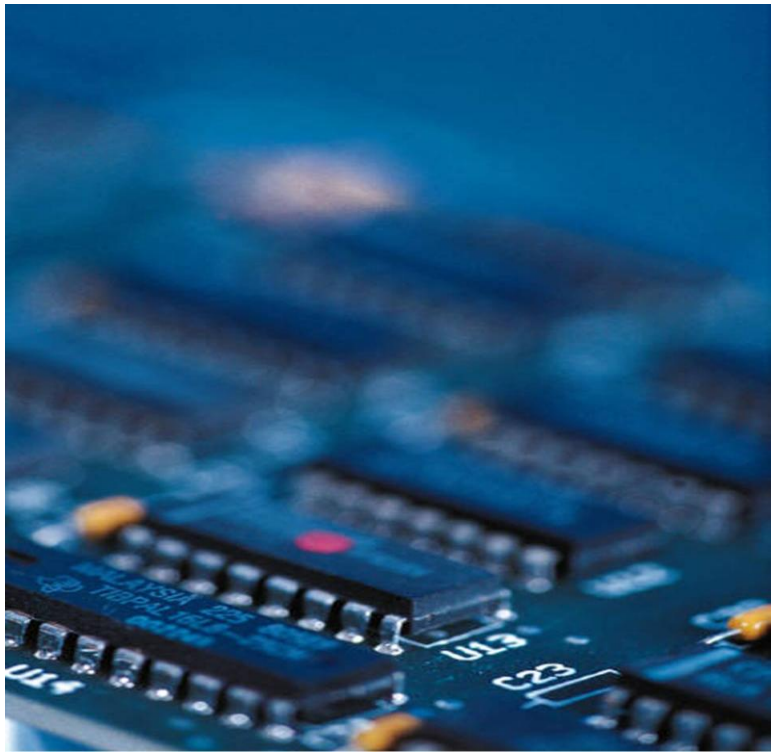
NRC Workshop on Resiliency of the Electric Power Delivery System
February 27, 2013

Material from the Electric Power Research Institute (EPRI), and support from EPRI, NSF, ORNL Honeywell and SNL for my graduate students' doctoral research is gratefully acknowledged.

TECHNOLOGICAL LEADERSHIP INSTITUTE
UNIVERSITY OF MINNESOTA
Driven to Discover℠

Unconventional Threats to Security

Connectivity



Complexity

A “Sanitized” Example: Lack of awareness and inadvertent connection to the Internet

- Power plant: 2- 250MW, gas fired turbine, combined cycle, 5 years old, 2 operators, and typical multi-screen layout:
- “A: do you worry about cyber threats?
- Operator: No, we are completely disconnected from the net.
- A: That’s great! This is a peaking unit, how do you know how much power to make?
- Operator: The office receives an order from the ISO, then sends it over to us. We get the message here on this screen.
- A: Is that message coming in over the internet?
- Operator: Yes, we can see all the ISO to company traffic. Oh, that’s not good, is it?”

Infrastructure Security

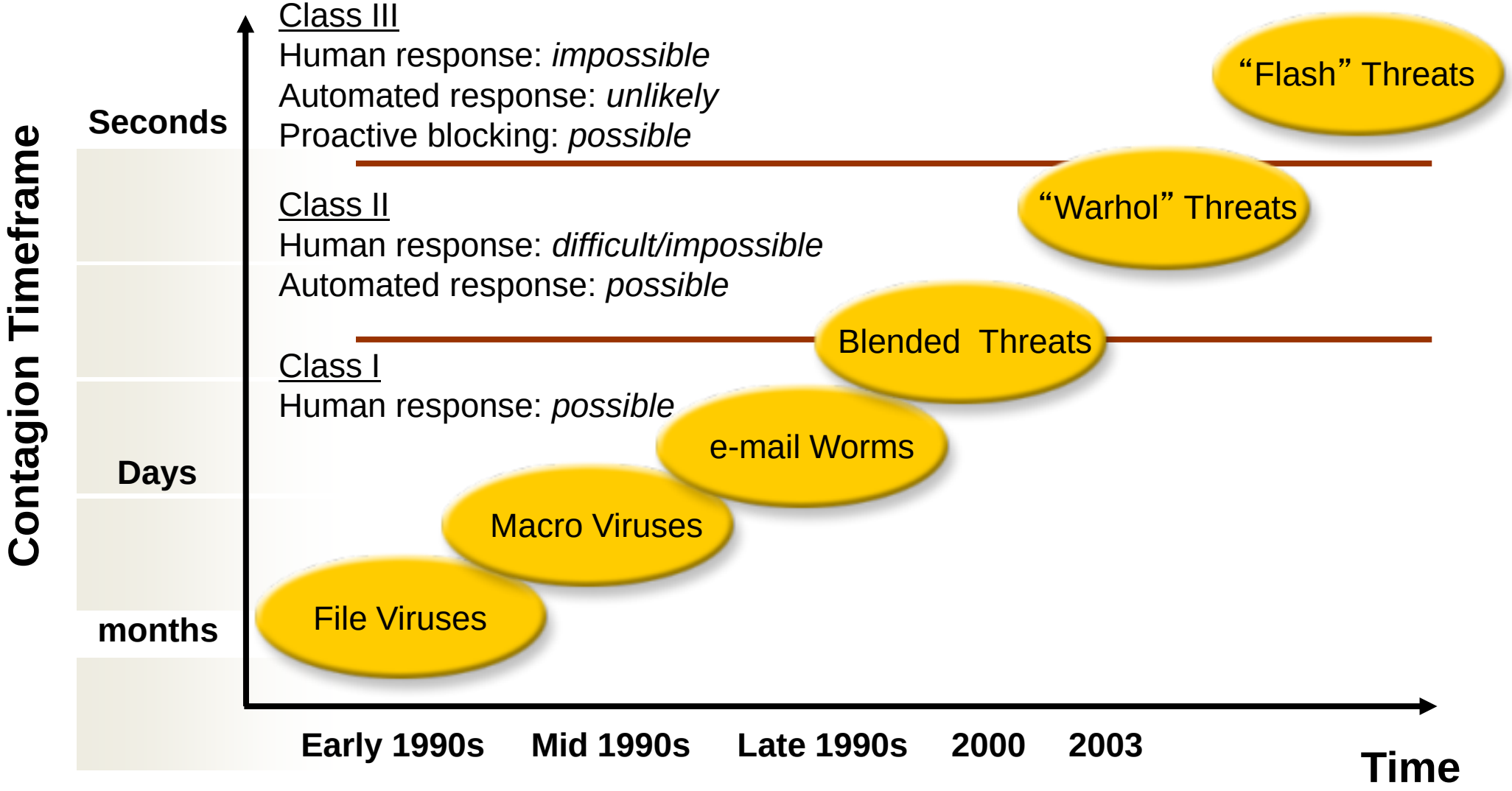
Context: Better Situational Awareness and Automation

- **Increasing Dependence on ICT, Computation and Communications.**

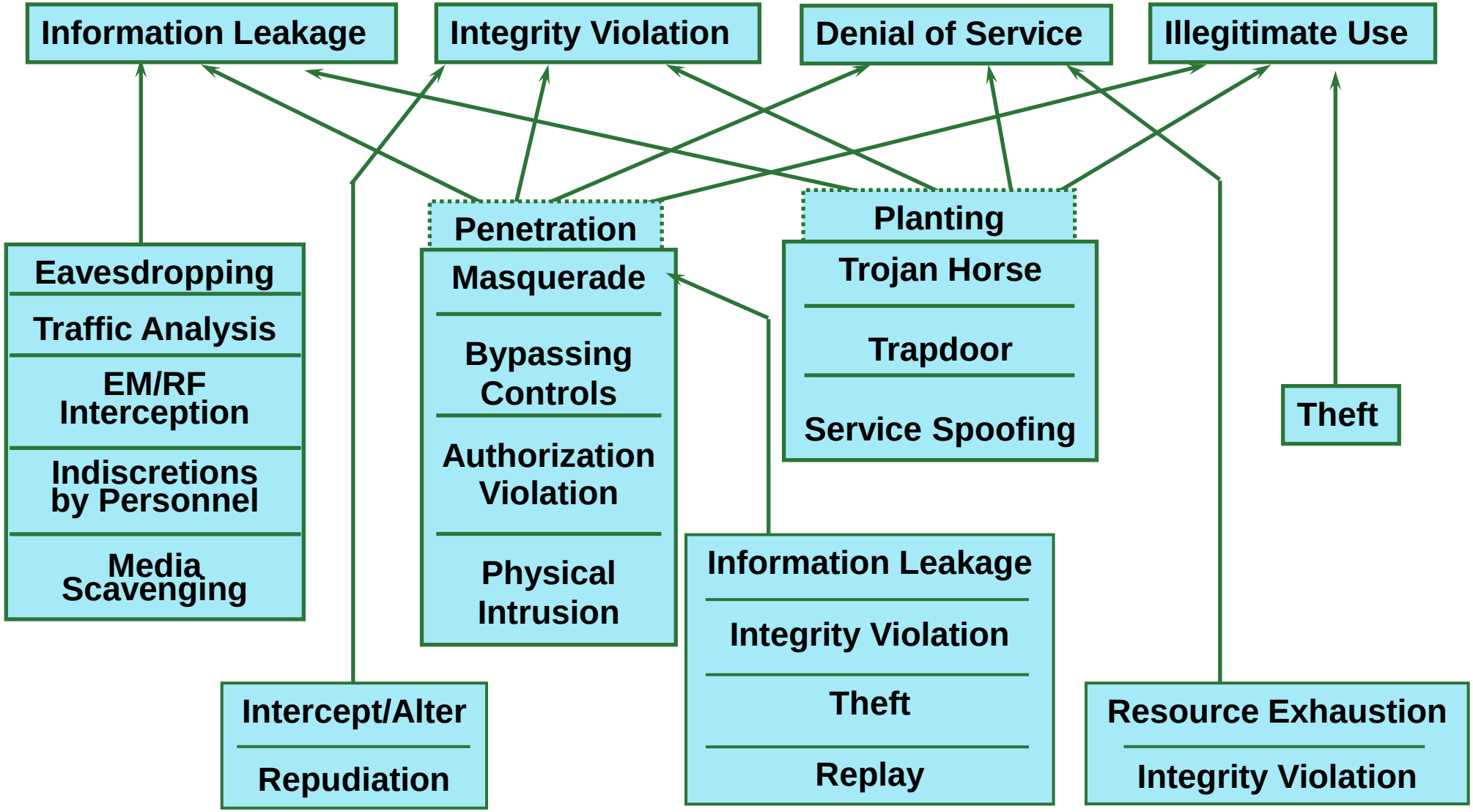
- **Increasing Complexity:** System integration, increased complexity: call for new approaches to simplify the operation of complex infrastructure and make them more robust to attacks and interruptions.

- **Centralization and Decentralization of Control:** The vulnerabilities of centralized control seem to demand smaller, local system configurations. Resilience rely upon the ability to bridge top--down and bottom-up decision making in real time.

Threat Evolution: Malicious Code



What Can They Do and How Can They Do It?



Overview of Focused Research Areas (1998-2003):

Programs Initiated and Developed at EPRI

1999-2001

EPRI/DoD Complex Interactive Networks (CIN/SI)

Underpinnings of Interdependent Critical National Infrastructures

Tools that enable secure, robust & reliable operation of interdependent infrastructures with distributed intelligence & self-healing

Y2K2000-present

Enterprise Information Security (EIS)

1. Information Sharing
2. Intrusion/Tamper Detection
3. Comm. Protocol Security
4. Risk Mgmt. Enhancement
5. High Speed Encryption

2002-present

Infrastructure Security Initiative (ISI)

Response to 9/11 Tragedies

1. Strategic Spare Parts Inventory
2. Vulnerability Assessments
3. Red Teaming
4. Secure Communications

2001-present

Consortium for Electric Infrastructure to Support a Digital Society (CEIDS)

1. Self Healing Grid
2. IntelliGrid™
3. Integrated Electric Communications System Architecture
4. Fast Simulation and Modeling

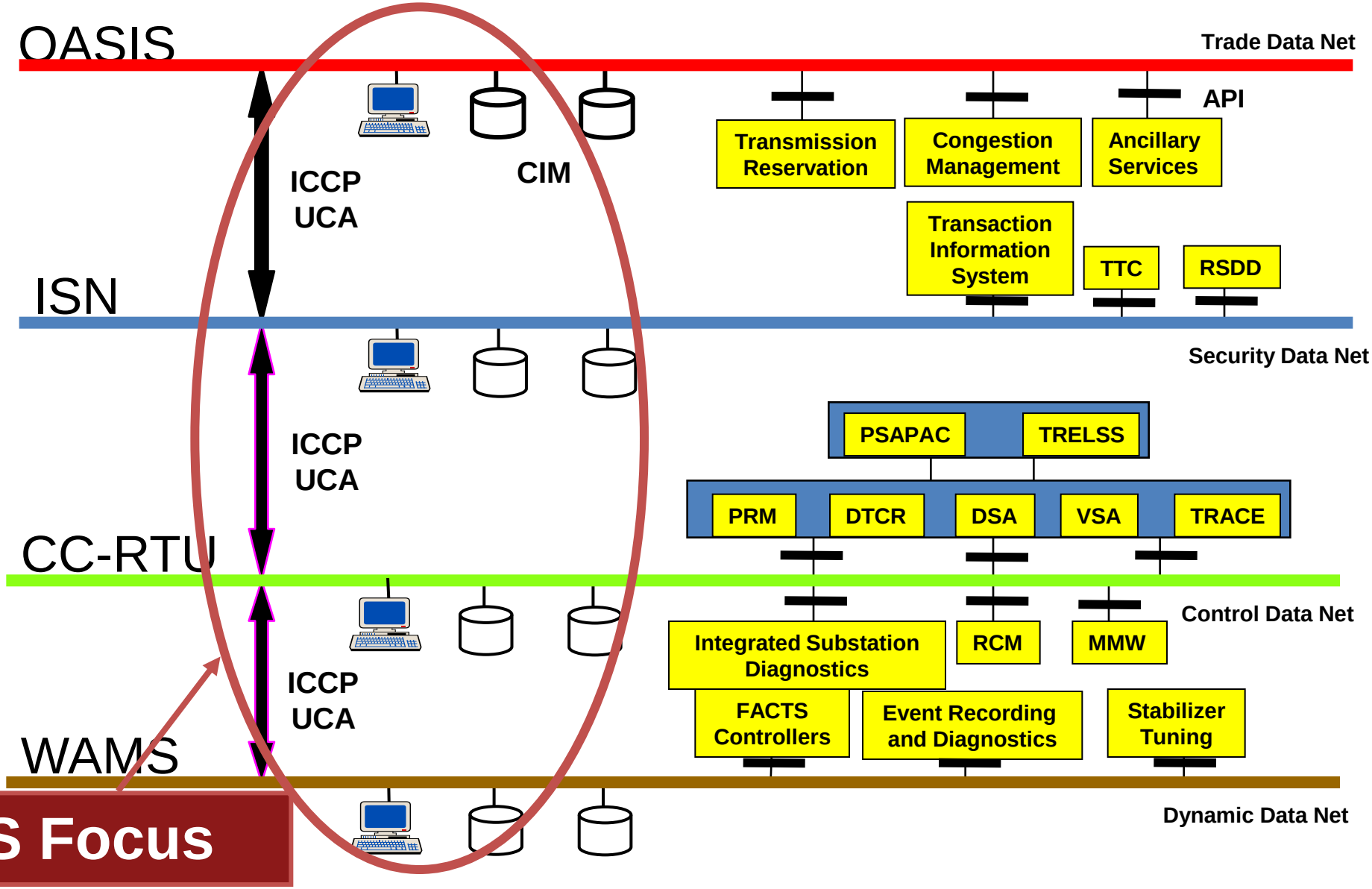
Infrastructure Security: The Threat

- Electric power systems constitute *the* fundamental infrastructure of modern society and therefore an inviting target for three kinds of terrorist attacks:

- Attacks upon the system
  - Power system itself is primary target with ripple effect throughout society
- Attacks by the system
  - Population is the actual target, using parts of the power system as a weapon
- Attack through the system
  - Utility networks provide the conduit for attacks on broad range of targets

Enterprise Information Security (EIS) program

Information Networks for On-Line Trade, Security & Control



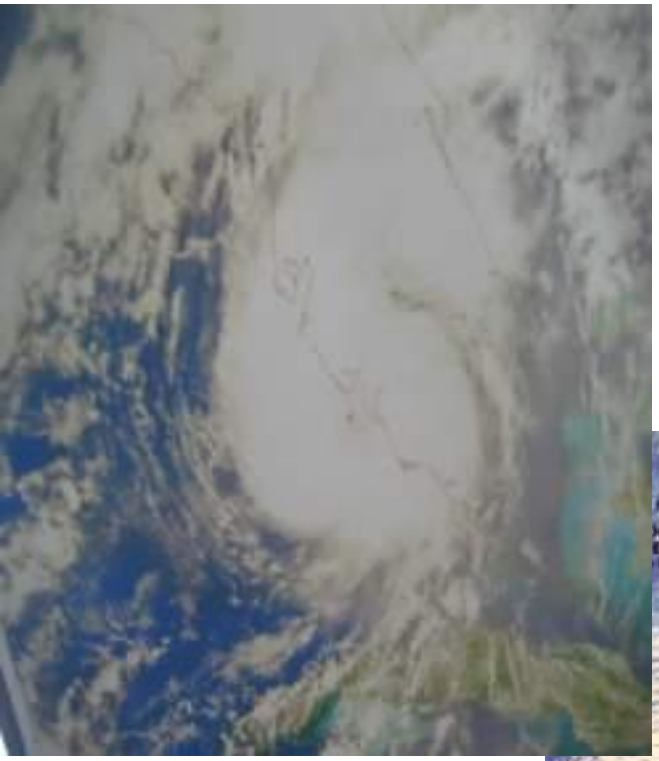
Example: Midway – Vincent 500 kV line tower damage, 2003

Midway – Vincent 500 kV line damage

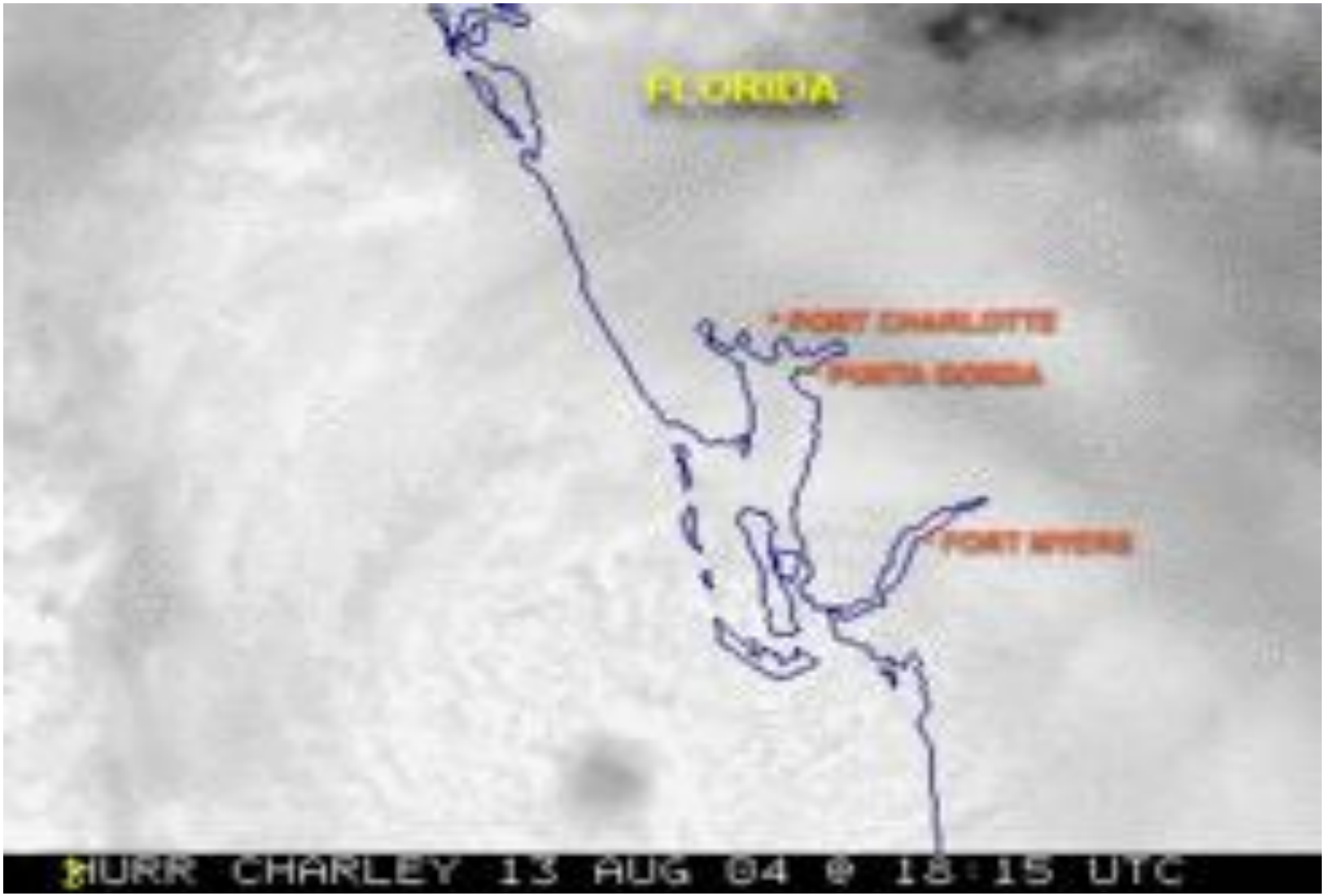
Vincent Substation before Transformer Explosion & Fire

500 / 230 kV Transformer Explosion & Fire, March 21, 2003, Vincent Substation

Hurricane Charley– August 13, 2004



Hurricane Charley (…went over our home in Bokeelia, Fl in Pine Island with winds >145 m/hr gusting to over 150 mi/hr)




PIKE


PIKE

The difficulty lies not with the new ideas, but in escaping the old ones. . . .

John Maynard Keynes

Observations

Threat Situation is Changing:

- Cyber has "weakest link" issues
- Cyber threats are dynamic, evolving quickly and often combined with lack of training and awareness.
- All hazard, including aging infrastructure, natural disasters and intentional attacks

Innovation and Policy:

- Protect the user from the network, and protect the network from the user: Develop tools and methods to reduce complexity for deploying and enforcing security policy.
- No amount of technology will make up for the lack of the 3 Ps (Policy, Process, and Procedures).
- Installing modern communications and control equipment (elements of the smart grid) can help, but security must be designed in from the start.
- Build in secure sensing, "defense in depth," fast reconfiguration and self-healing into the infrastructure.
- Security by default – certify vendor products for cyber readiness
- Security as a curriculum requirement.
- Increased investment in the grid and in R&D is essential.

Recommendations

- Facilitate, encourage, or mandate that secure sensing, “defense in depth,” fast reconfiguration and self-healing be built into the infrastructure
- Mandate security for the Advanced Metering Infrastructure, providing protection against Personal Profiling, guarantee consumer Data Privacy, Real-time Remote Surveillance, Identity Theft and Home Invasions, Activity Censorship, and Decisions Based on Inaccurate Data
- Wireless and the public Internet increase vulnerability and thus should be avoided
- Bridge the jurisdictional gap between Federal/NERC and the state commissions on cyber security
- Electric generation, transmission, distribution, and consumption need to be safe, reliable, and economical in their own right. Asset owners should be required to practice due diligence in securing their infrastructure as a cost of doing business
- Develop coordinated hierarchical threat coordination centers – at local, regional, and national levels – that proactively assess precursors and counter cyber attacks
- Speed up the development and enforcement of cyber security standards, compliance requirements and their adoption. Facilitate and encourage design of security in from the start and include it in standards
- Increase investment in the grid and in R&D areas that assure the security of the cyber infrastructure (algorithms, protocols, chip-level and application-level security)
- Develop methods, such as self-organizing micro-grids, to facilitate grid segmentation that limits the effects of cyber and physical attacks


THANK YOU
MINNESOTA