Managing Secure Survivable Critical Infrastructures to Avoid Vulnerabilities

IEEE Int'l Symposium On High Assurance Systems Engineering

Tampa, Florida – March 25-26, 2004

Frederick T. Sheldon, Ph.D.

Oak Ridge National Laboratory

Applied Software Engineering Research Laboratory

Director – Software Engineering for Dependable/Secure Systems Lab

Including:

Tom Potok and Andy Loebl

Applied Software Engineering Research

Oak Ridge National Laboratory

Oak Ridge, TN 37831 USA

PotokTE | LoeblA@ornl.gov

Axel Krings and Paul Oman

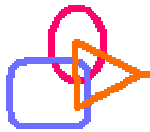
Department of Computer Science

University of Idaho

Moscow, ID 83844 USA

Krings | Oman@cs.uidaho.edu

Agenda

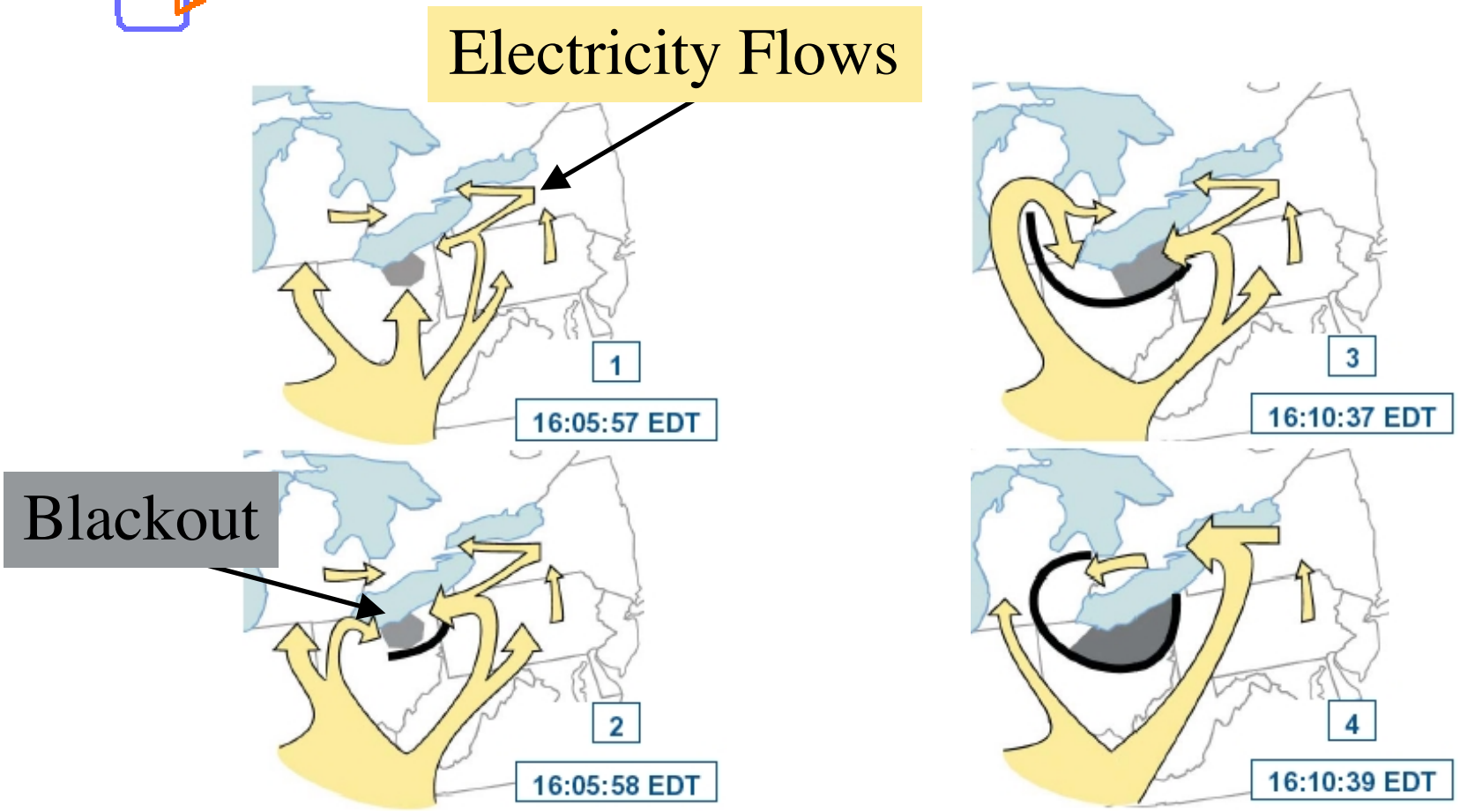


- Problem Stmt: *Energy Infrastructure Survivability (EIS)*
  - August 14 2003 Blackout Post Mortem
- ORNL Research Activity on Critical Infrastructure (CI) Vulnerabilities
- Managing energy infrastructure survivability, inherent limitations, obstacles and mitigation strategies
  - Case Study 1996 West Coast Blackouts
  - GSPN used to model/assess interdependencies
  - Conclusions
  - Key Issues in SE and Infrastructure Survivability

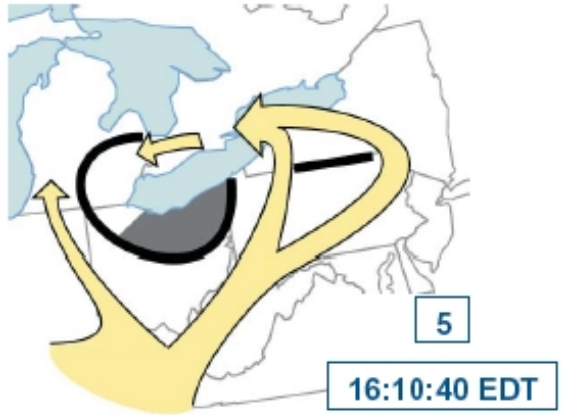
Ensuring networks are secure, robust, and reliable is critical for the strategic and economic well being of the Nation.

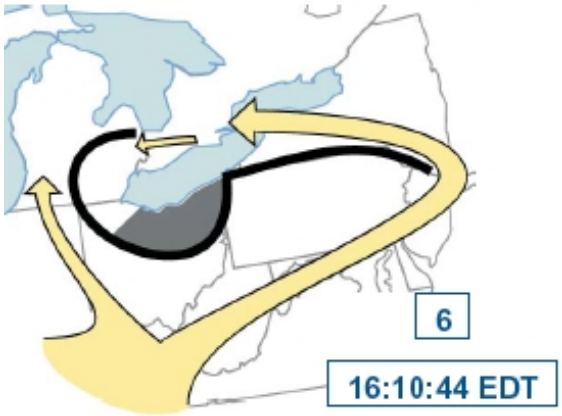
- *August 14, 2003 blackout affected **8 states** and **50M people** and may cost up to **$5 billion**. The DOE/NERC interim reports indicate:*
- ***Outage progressed as a chain of relatively minor events consistent with previous cascading outages caused by a domino reaction**. The increasing use of distributed systems to manage our technologically complex society makes knowing the vulnerability of such systems essential to improving their intrinsic reliability/survivability. Our discussion employs the power transmission grid.*
- Experts widely agree that failures of the power-transmission system are a nearly **unavoidable product of a collision between the system physics and the economic regulatory rules**. The nation must either physically transform the system to accommodate the new rules, or change the rules to better mesh with the power grids physical behavior

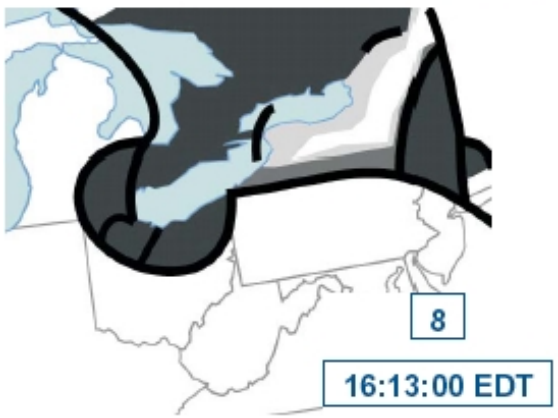
Cascade Sequence 1st 4.5mins



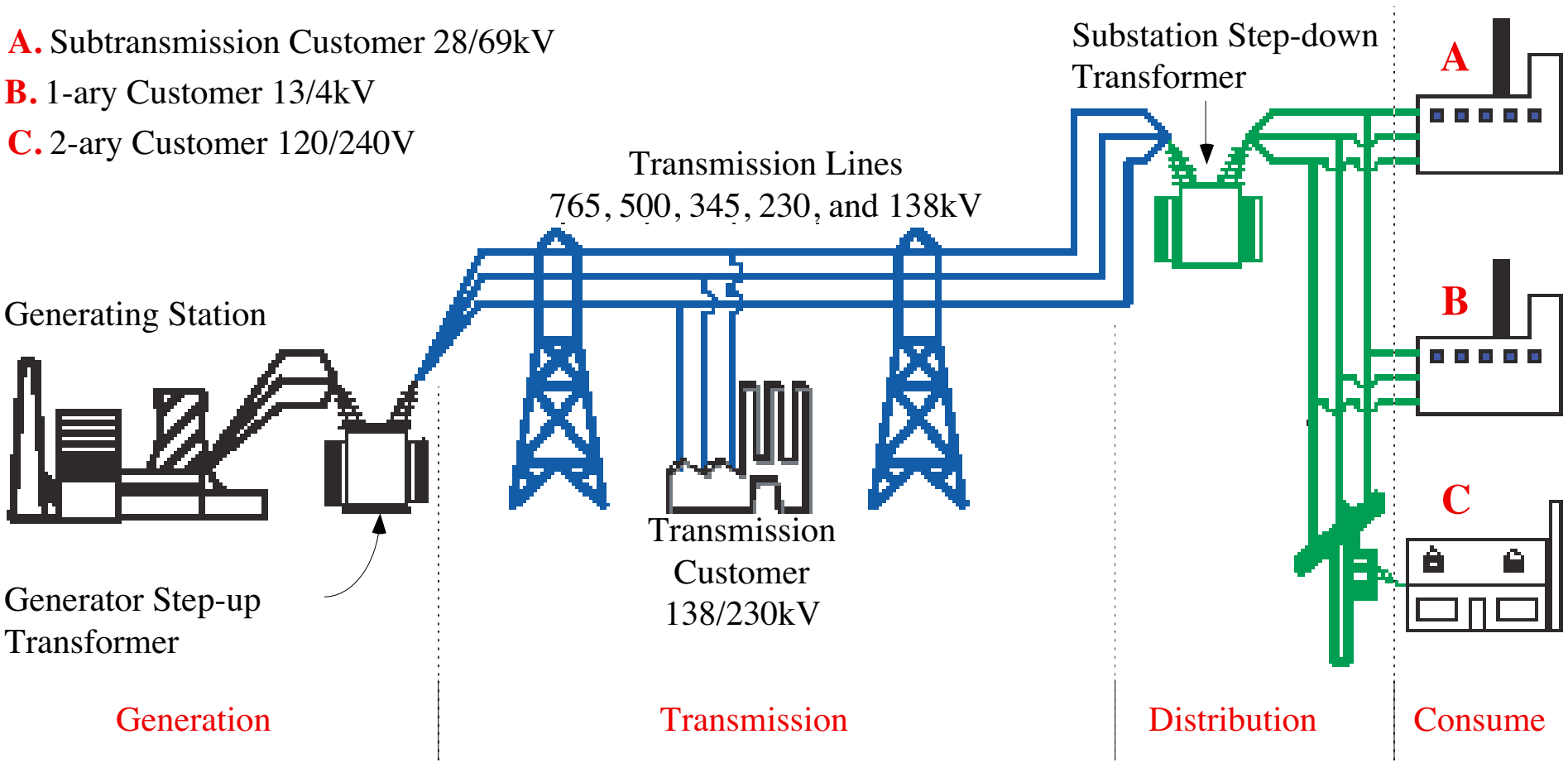
Cascade Sequence 2st 2.5mins







7 minutes later


A. Subtransmission Customer 28/69kV
B. 1-ary Customer 13/4kV
C. 2-ary Customer 120/240V
Substation Step-down Transformer
A
Transmission Lines
765, 500, 345, 230, and 138kV
B
Generating Station
C
Transmission Customer 138/230kV
Generator Step-up Transformer
Generation
Transmission
Distribution
Consume

The Causes of the Blackout

The initiation of the August 14, 2003, blackout was caused by deficiencies in specific practices, equipment, and human decisions that coincided that afternoon. There were three groups of causes:

Group 1: Inadequate situational awareness at FirstEnergy Corporation (FE). In particular:

A) FE failed to ensure the security of its transmission system after significant unforeseen contingencies because it did not use an effective contingency analysis capability on a routine basis. (See page 28.)

B) FE lacked procedures to ensure that their operators were continually aware of the functional state of their critical monitoring tools. (See page 31.)

C) FE lacked procedures to test effectively the functional state of these tools after repairs were made. (See page 31.)

D) FE did not have additional monitoring tools for high-level visualization of the status of their transmission system to facilitate its operators' understanding of transmission system conditions after the failure of their primary monitoring/alarming systems. (See page 33.)

Group 2: FE failed to manage adequately tree growth in its transmission rights-of-way. This failure was the common cause of the outage of three FE 345-kV transmission lines. (See page 34.)

Group 3: Failure of the interconnected grid's reliability organizations to provide effective diagnostic support. In particular:

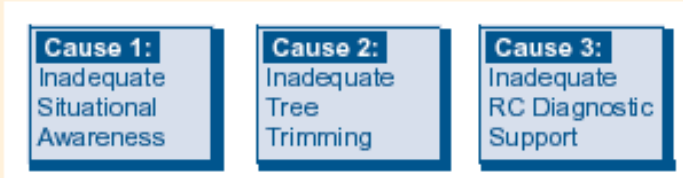
A) MISO did not have real-time data from Dayton Power and Light's Stuart-Atlanta 345-kV line incorporated into its state estimator (a system monitoring tool). This precluded MISO from becoming aware of FE's system problems earlier and providing diagnostic assistance to FE. (See page 24.)

B) MISO's reliability coordinators were using non-real-time data to support real-time "flowgate" monitoring. This prevented MISO from detecting an N-1 security violation in FE's system and from assisting FE in necessary relief actions. (See page 39.)

C) MISO lacked an effective means of identifying the location and significance of transmission line breaker operations reported by their Energy Management System (EMS). Such information would have enabled MISO operators to become aware earlier of important line outages. (See pages 27 and 36.)

D) PJM and MISO lacked joint procedures or guidelines on when and how to coordinate a security limit violation observed by one of them in the other's area due to a contingency near their common boundary. (See page 38.)

In the pages below, sections that relate to particular causes are denoted with the following symbols:

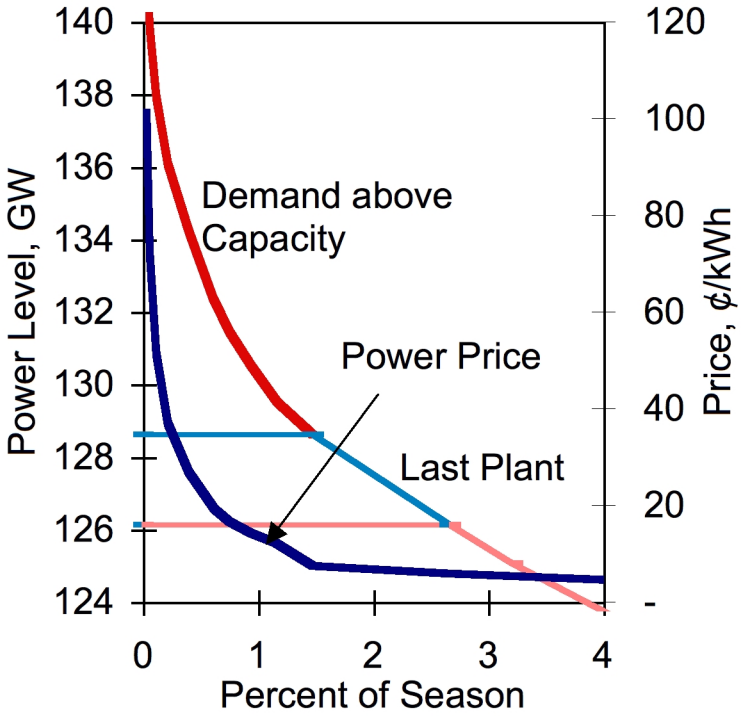


Variety OF CI Vulnerability Studies @ Oak Ridge National Laboratory

- Electric power systems analysis
  - Systems monitoring, reliability, restructuring
- Vulnerability assessments
- Transportation analysis
- Buildings technologies
- Emergency response management
- Others

Regional Power Analysis models

- Oak Ridge Competitive Electricity Dispatch (ORCED)
  - Regional power generation
  - Loss of Load Probability and generation inadequacy
- Transmission & Distribution Load Flow models
  - Industry standard models
  - Analyze instabilities
  - Requires massive data from utilities



Modeling Blackout Dynamics in Power Transmission Systems

- Goal: Understanding large cascading events
- Approach: Combining the engineering constraints of power systems with economical and human factor.
- The power system is analyzed as a complex system
- This research is a collaboration:

  B. A. Carreras and V. E. Lynch, ORNL

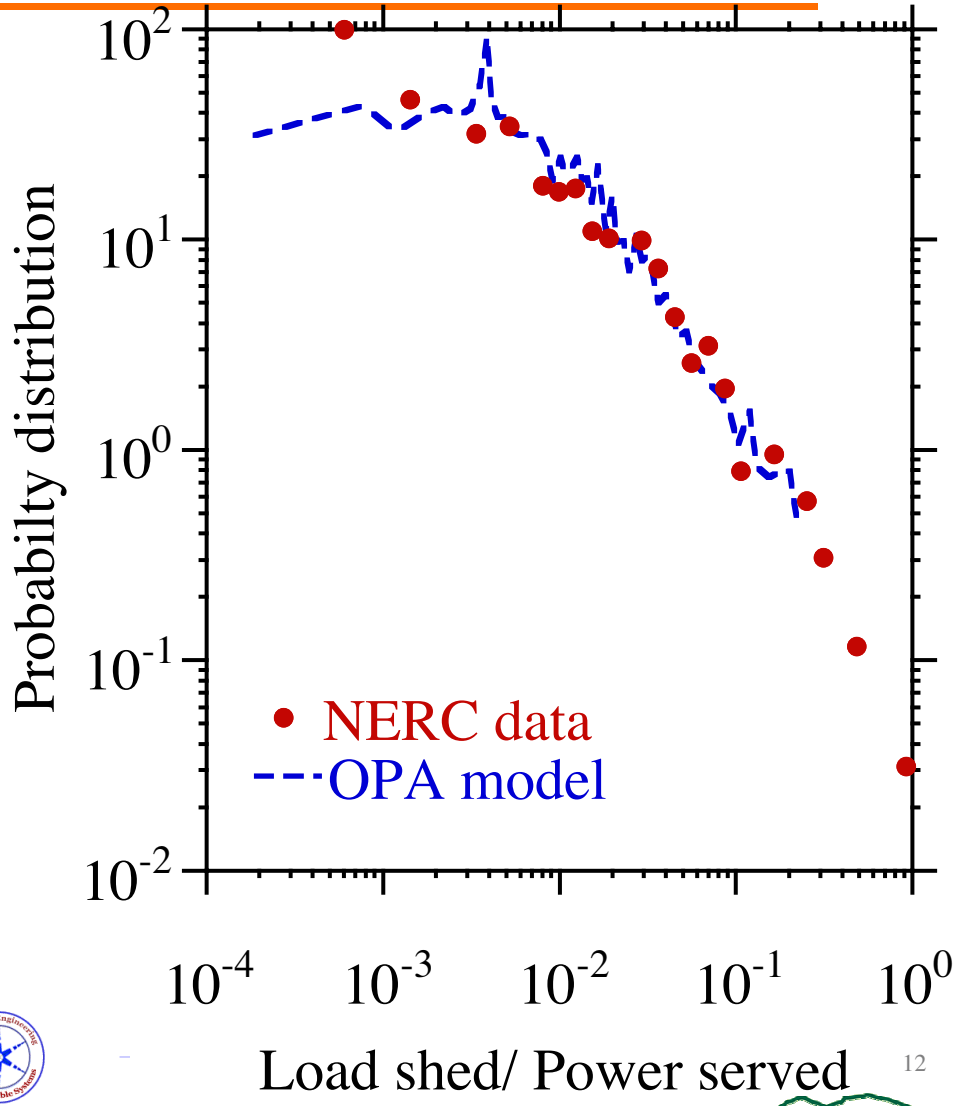
  I. Dobson, P-Serc, Madison, Wisconsin

  D. E. Newman, University Alaska

Funded by CERTS and NSF

The OPA model predicts the probability of large blackouts

- Prob. Dist. derived from NERC blackout data 84-98.
- The power tail in pdf of the NERC data is consistent with the model *and* implies that the power system is being operated near criticality.
- The grid is vulnerable to large cascading events.



OPA model includes both engineering and economic forces…

- Blackout dynamics result from opposing forces:
  - Increase demand ⇒ push toward critical/catastrophic threshold
  - Engineering response to failures
    - Transmission system upgrades
    - Investment in new power plants

      ⇒ push away critical/catastrophic threshold
  - Regulatory measures may set constraints in this process
- OPA solves the network circuit equations as the system is evolved under these long-range dynamic forces.

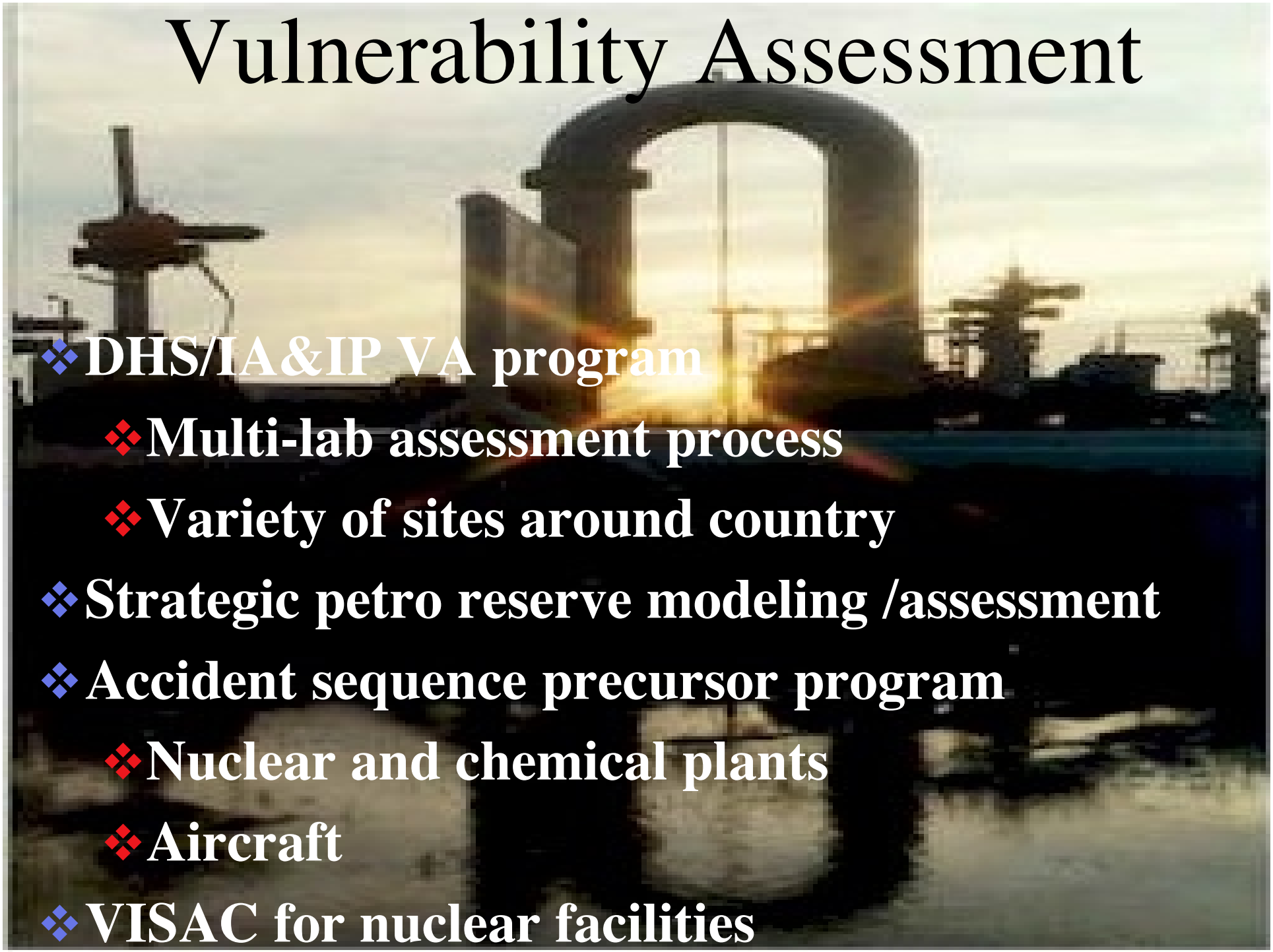
Ongoing Developments/Research

- Large cascading events are similar to the "domino effect" :
  - Force needed to trip 1st domino gives 1st threshold.
    - Like the *n*-1 criterion used in designing networks.
  - A 2nd threshold is given by the ratio of the separation between dominos to their height
    - Causes all the dominos to fall.
- Using the OPA model ORNL researchers are ***investigating this second threshold to determine what network parameters control it***

Power Systems Research Program

- National Transmission Test Research Center
  - Improve transmission carrying capacity and recovery speed
  - Critical equipment inventory
- Energy/Ancillary Services
  - Nuclear vulnerability to grid degradation
  - Power quality, reserves, reliability, blackstart recovery
- Power network monitoring and simulation
- Multi-level inverter for grid support

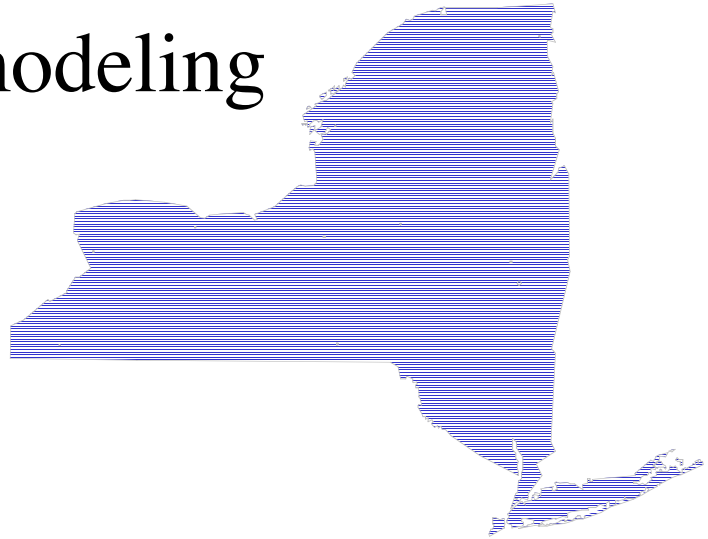
Vulnerability Assessment



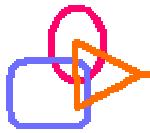
- DHS/IA&IP VA program
  - Multi-lab assessment process
  - Variety of sites around country
- Strategic petro reserve modeling /assessment
- Accident sequence precursor program
  - Nuclear and chemical plants
  - Aircraft
- VISAC for nuclear facilities

Vulnerability Analysis

- Assisted DOE/DHS in vulnerability studies
  - Top 25 critical energy facilities
  - New York State assessment
- Regional power systems modeling
  - Generation adequacy
  - Restructuring impacts



Emergency Response Management



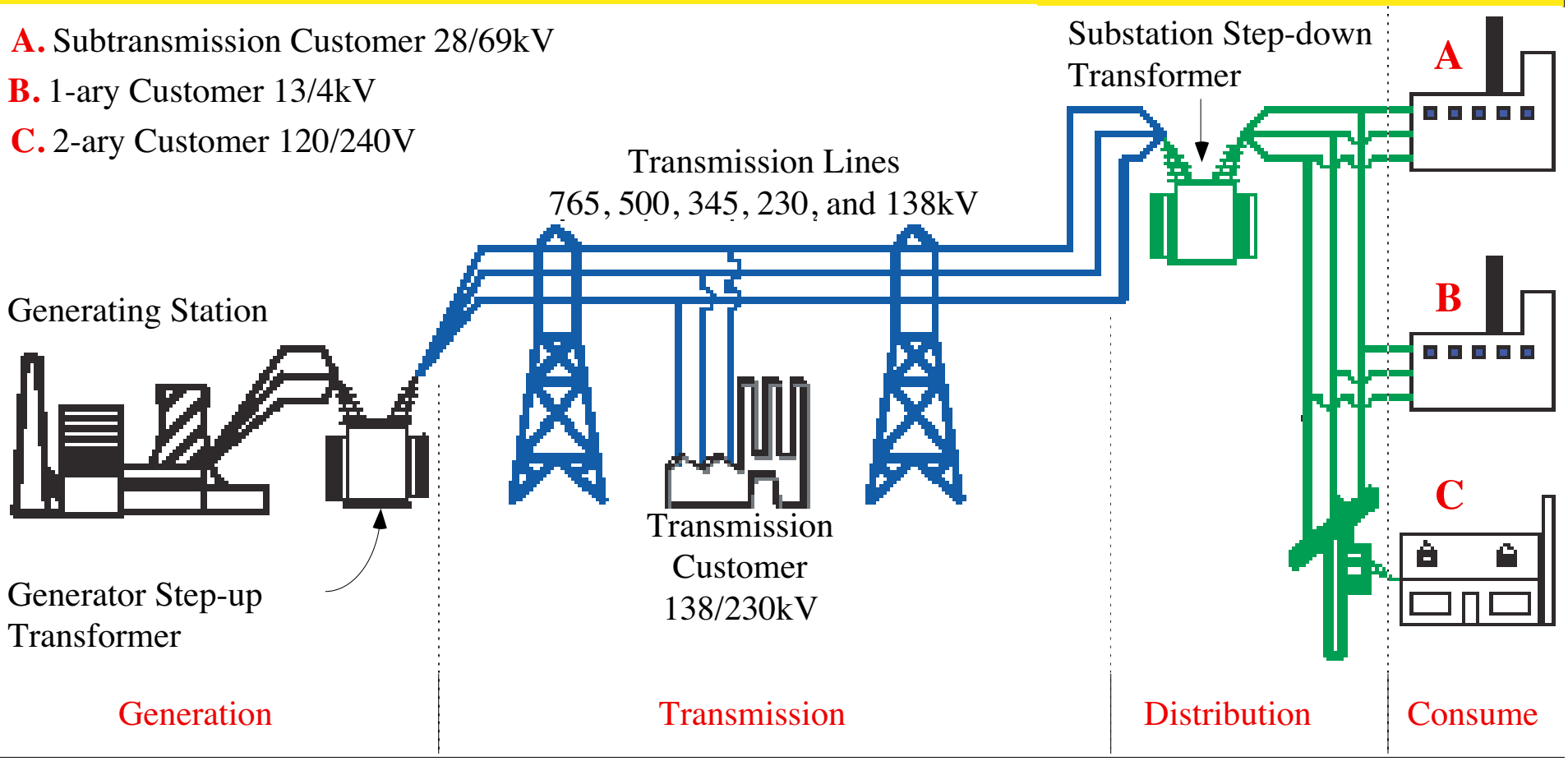
- Oak Ridge Evacuation Modeling System
  - Only DOT-endorsed regional evacuation model
- Intelligent Consequence Management LDRD
  - New sensor networks or links to existing sensor networks designed to detect and monitor the threats of concern
  - High-speed communications and data exchange
  - Real-time simulations running on high-speed machines
  - Faster than real-time predictive capabilities
  - **Advanced decision support tools** that can process data and simulation outputs into a format useful to decision-makers

12 Facilities Modeled for the NRC

- All are US Plants
  - 9 PWRs / 3 BWRs
- Basic "building-level" models
- Textured animations including site terrain

On August 14, 2003, the NE U.S. and Canada experienced a widespread electrical power outage affecting an estimated 50 million people. **Nine** U.S. nuclear power plants experienced rapid shutdowns (reactor trips) as a consequence of the power outage. **Seven** nuclear power plants in Canada operating at high power levels at the time of the event also experienced rapid shutdowns. **Four** other Canadian nuclear plants automatically disconnected from the grid due to the electrical transient but were able to continue operating at a reduced power level and were available to supply power to the grid as it was restored by the transmission system operators. **Six** nuclear plants in the US and **one** in Canada experienced significant electrical disturbances but were able to continue generating electricity.

Energy Infrastructure Survivability, Inherent Limitations, Obstacles and Mitigation Strategies



†Energy Infrastructure Survivability Map

Modeling, Analysis for Countermeasure & Avoidance

†Leverages Critical Infrastructure Protection and Survivability Inter-Institutional Research Initiative (NIST Investment)

Collaborators

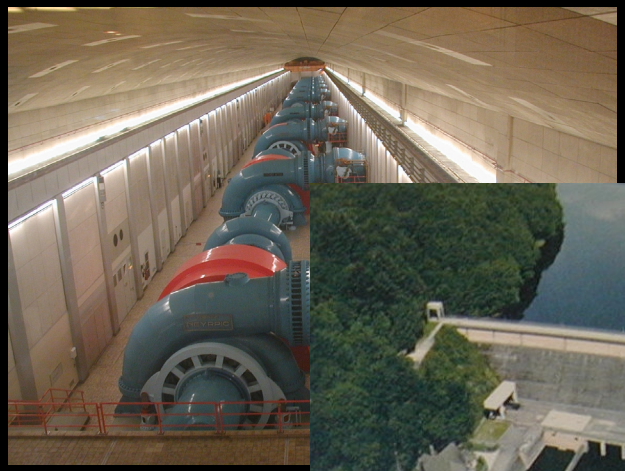
- ORNL & Univ Idaho & EPRI PEAC Inc.

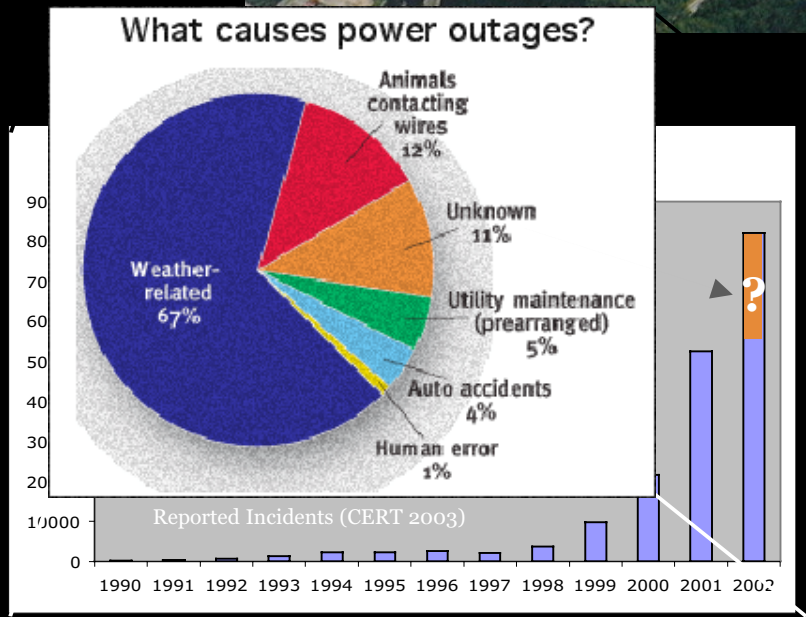
Contacts

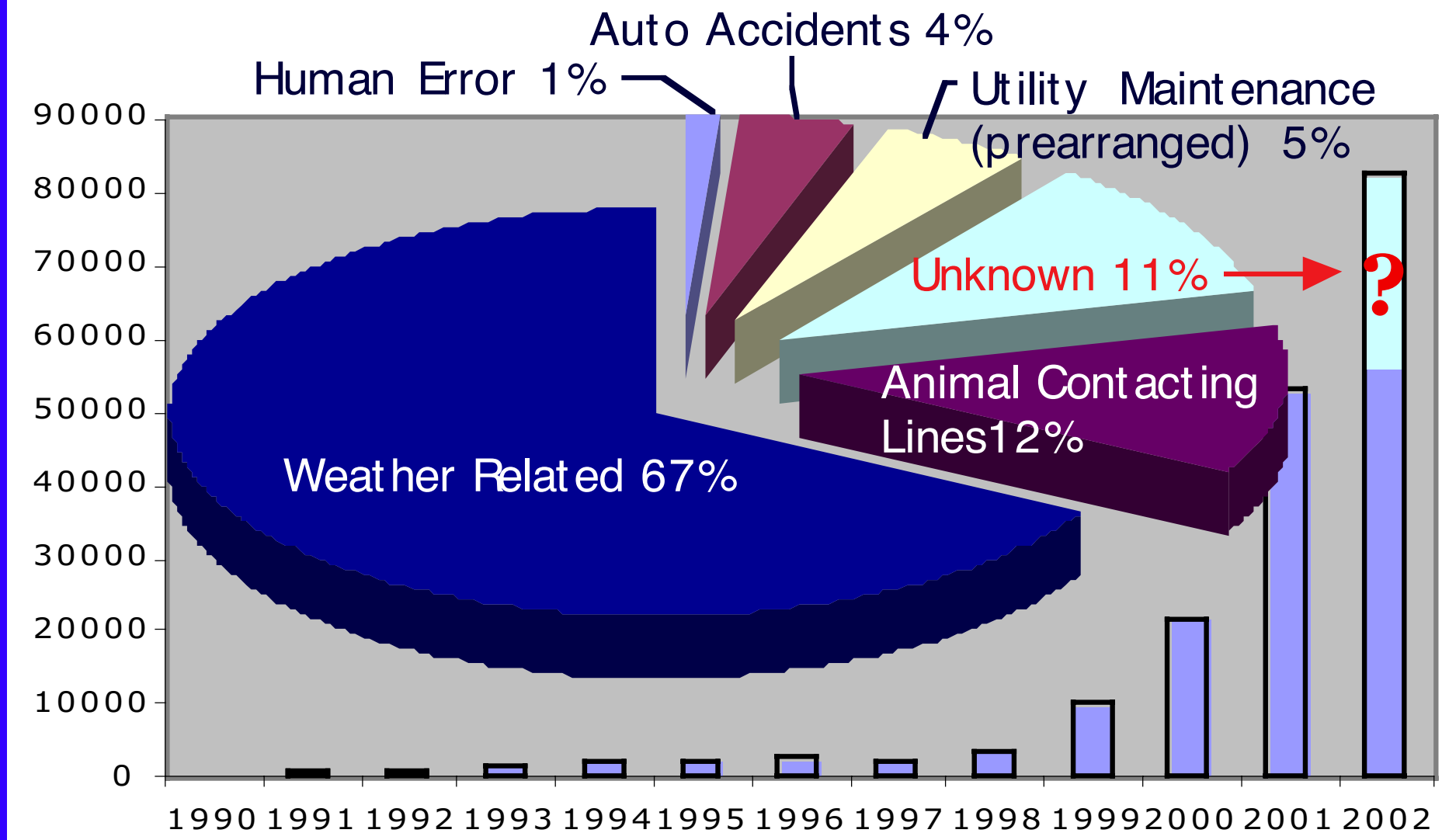
- Dr. Frederick Sheldon, ORNL
- Dr. Krings & Dr. Oman UI Dept of CS

Justification

- **Malicious acts targeting computers have reached epidemic proportions.**
- **All Critical Infrastructures in the U.S. have computer-automated controls (energy, finance, telecommunications, water, transportation, health care)**
- **Interdisciplinary research needed to find security and survivability solutions**







Reported Incidents (CERT 2003)

Post Mortem Failure Analysis

28 Failure points but only 12 failure groups

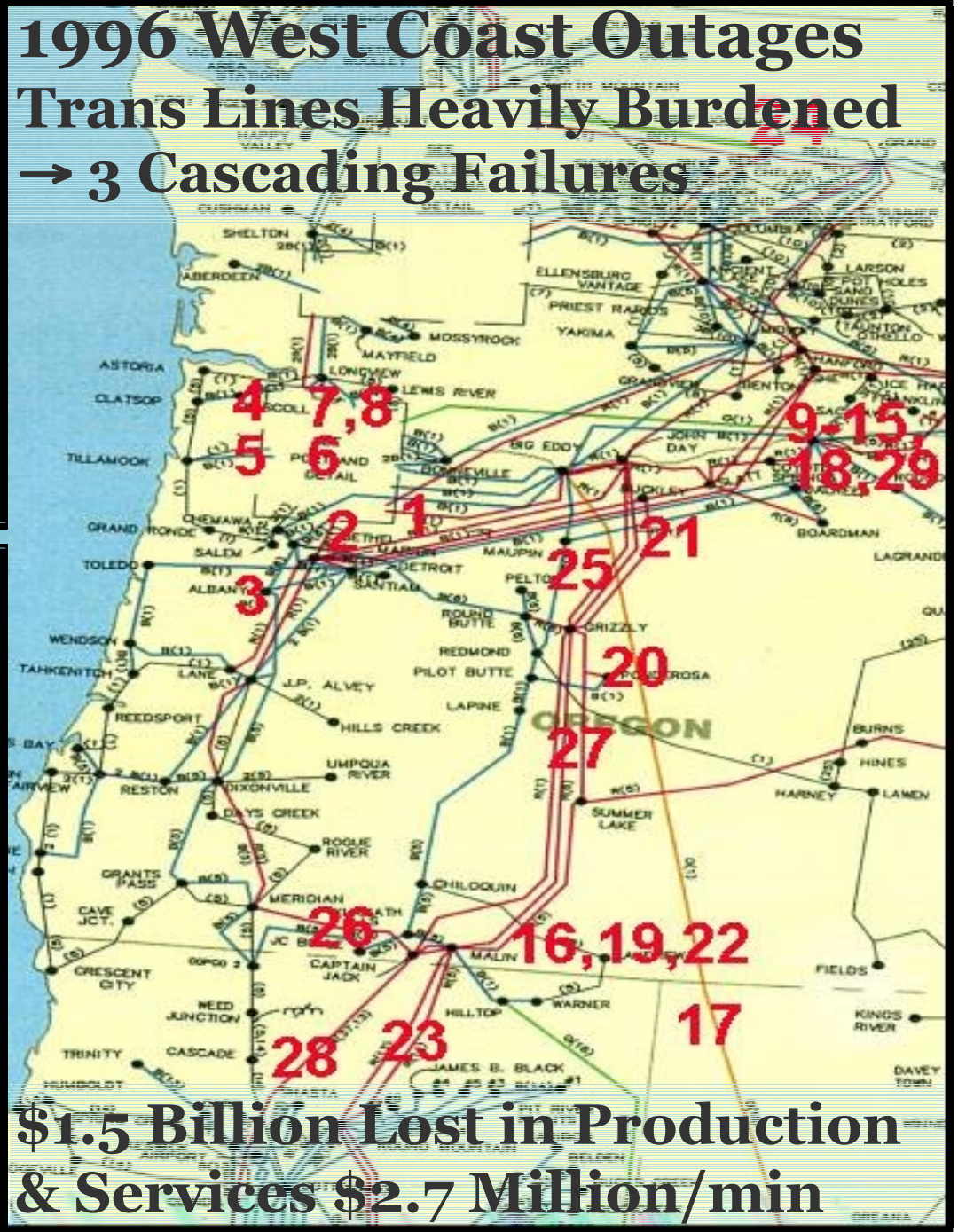
Line sag |Out of service equip | Relay malfunction | Single connection | Reactive power protection | Freq. Oscillation |Perceived phase imbalance | AC/DC Voltage instability | Trans line protection | AC voltage decay | Trans shortage

Modeling/ Analysis Conclude

Conclusion: Cascading Failure Triggered When System Was Stressed "Near-critical."

Speculation 1: Common Mode Faults Contribute to Cascading Failure

Speculation 2: Cascading Failure Can Be Induced by Physical or Electronic Sabotage



Survivability

- Survivability of a system can be expressed as a combination of *reliability*, *availability*, *security*, and human *safety*
- Each CI (components) will stress a different combination of these four facets to ensure the proper operation of the entire system(s).
  - **Threats from within** (malfunctioning components, normal but complex system interrelationships that engender common failures)
  - **Threats from without** (malicious attacks, and environmental insult, etc.).

Structured Models Enable

- System reliability to be derived from determined reliabilities of its components.
- Reliability analysis provides an understanding about the *likelihood of failures* occurring in a system and can provide deterministic insight to developers about *inherent (and defined) "weaknesses" in the system components and among systems*

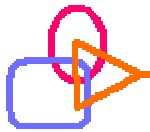
Long Term Reliability/Survivability

- Encompasses…
  - Case studies
  - Mitigation of common mode failures
  - Cyber security
  - Inherent limitations and obstacles
  - Design/develop tools products and processes to *support better management of CI investments*

Managing Secure Survivable Critical Infrastructures to Avoid Vulnerabilities

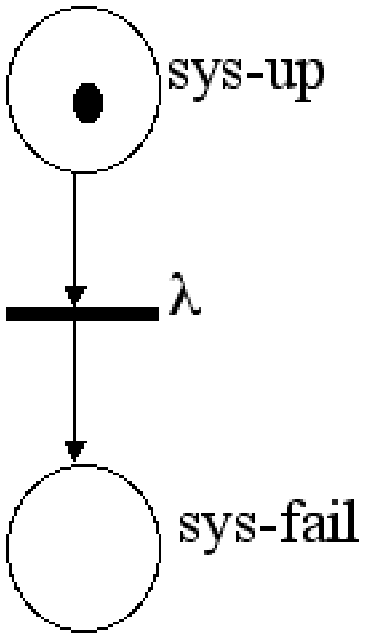
GSPN presentation

Generalized Stochastic Petri Nets

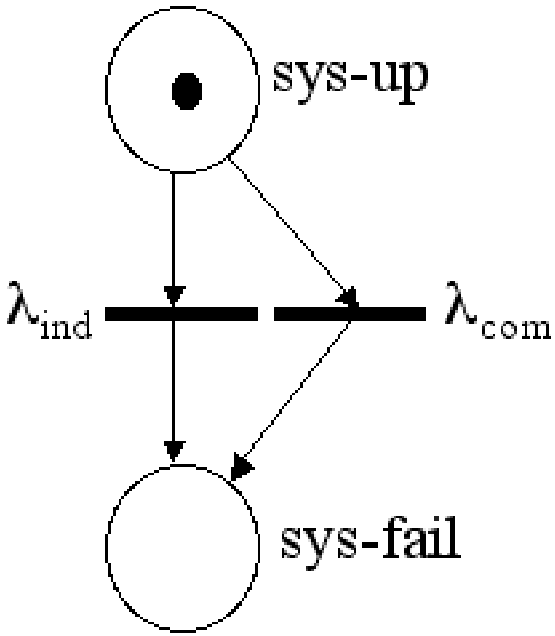


- Simple Constructions
  - ✓ Compact
  - ✓ System parameters
  - ✓ Interconnections
- Quintuple (P, T, A, W, m_0)
  - ✓ P, finite set of places
  - ✓ T, finite set of transitions (denoted by bars)
  - ✓ A, set of arcs from $(P \times T) \cup (T \times P)$
  - ✓ W, weight function on arcs within A
  - ✓ m_0, the initial marking
- Two Types of Transitions
  - ✓ Immediate (thin bars)
  - ✓ Timed (thick bars)

Simple GSPN Primitives

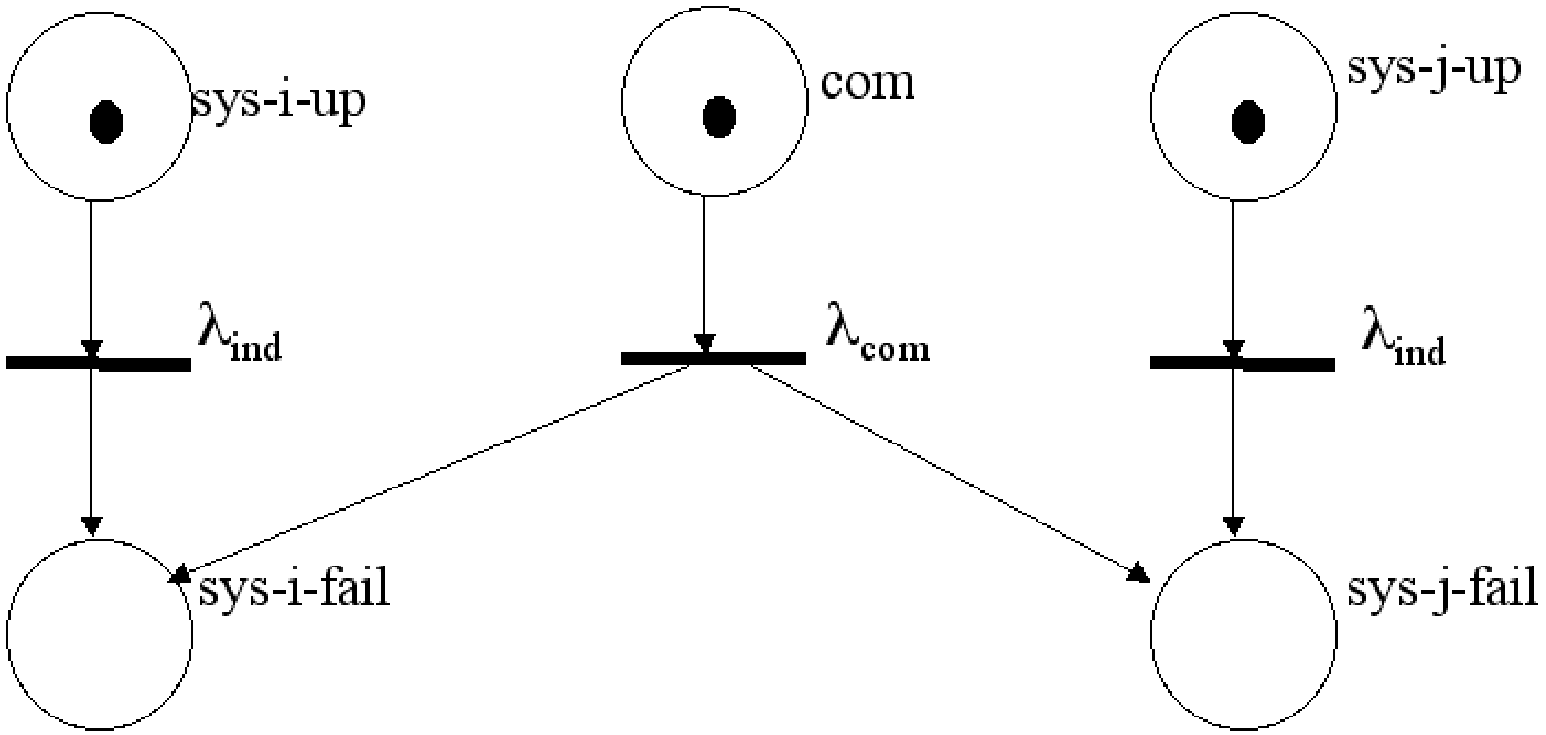


Single Mode Failure Model

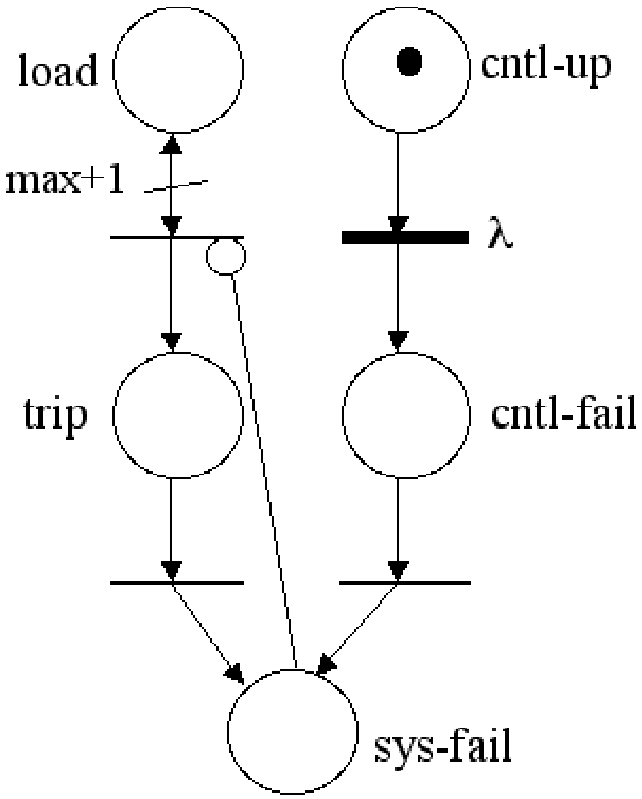


Multi-mode Failure Model

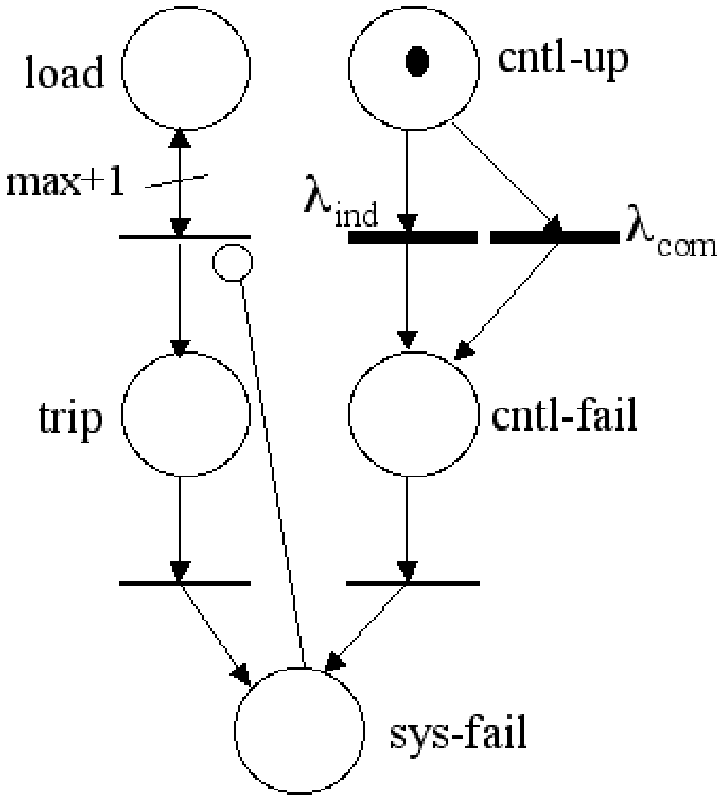
Common Mode Failure Primitive



Hybrid Primitives

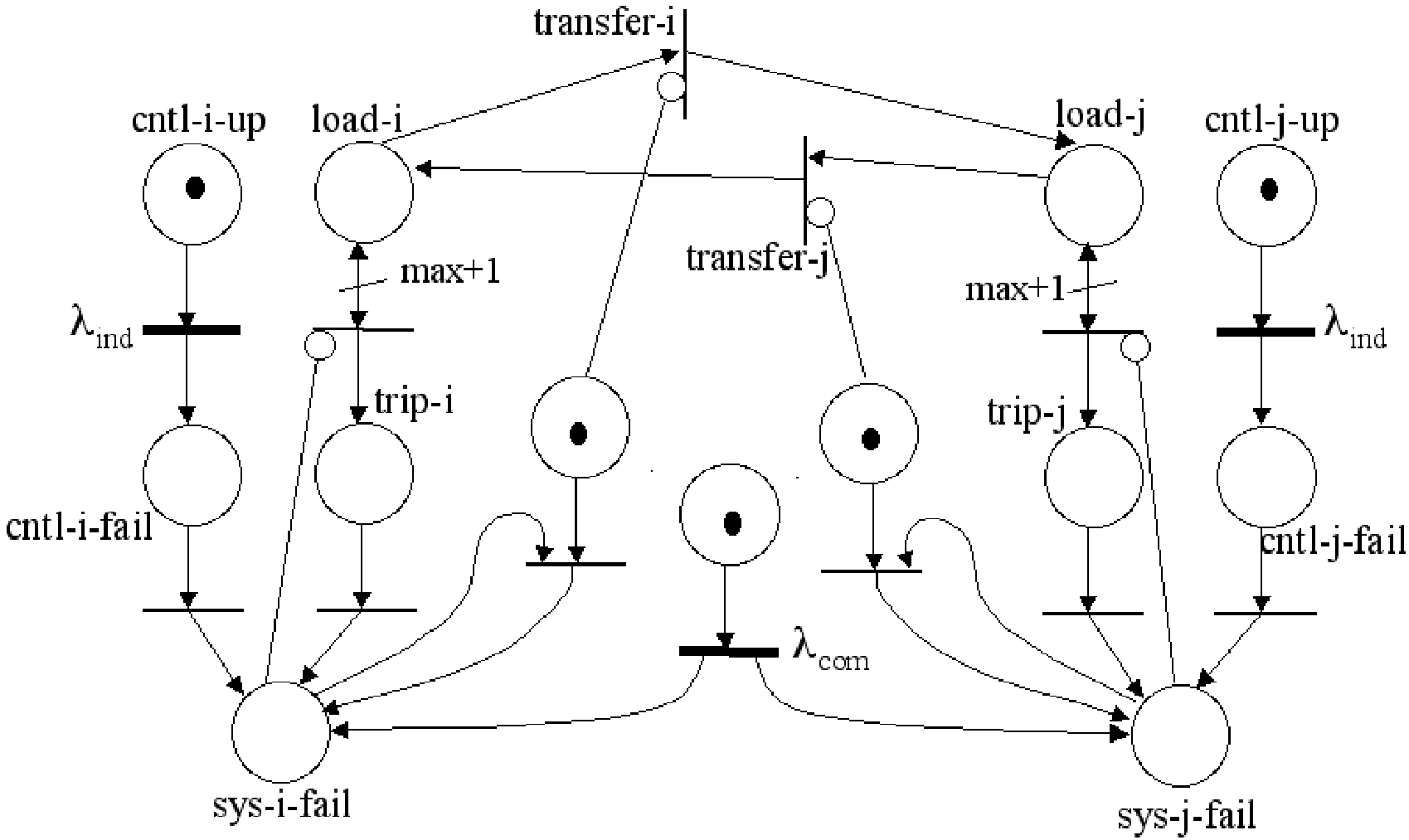


Single Mode Failure Model

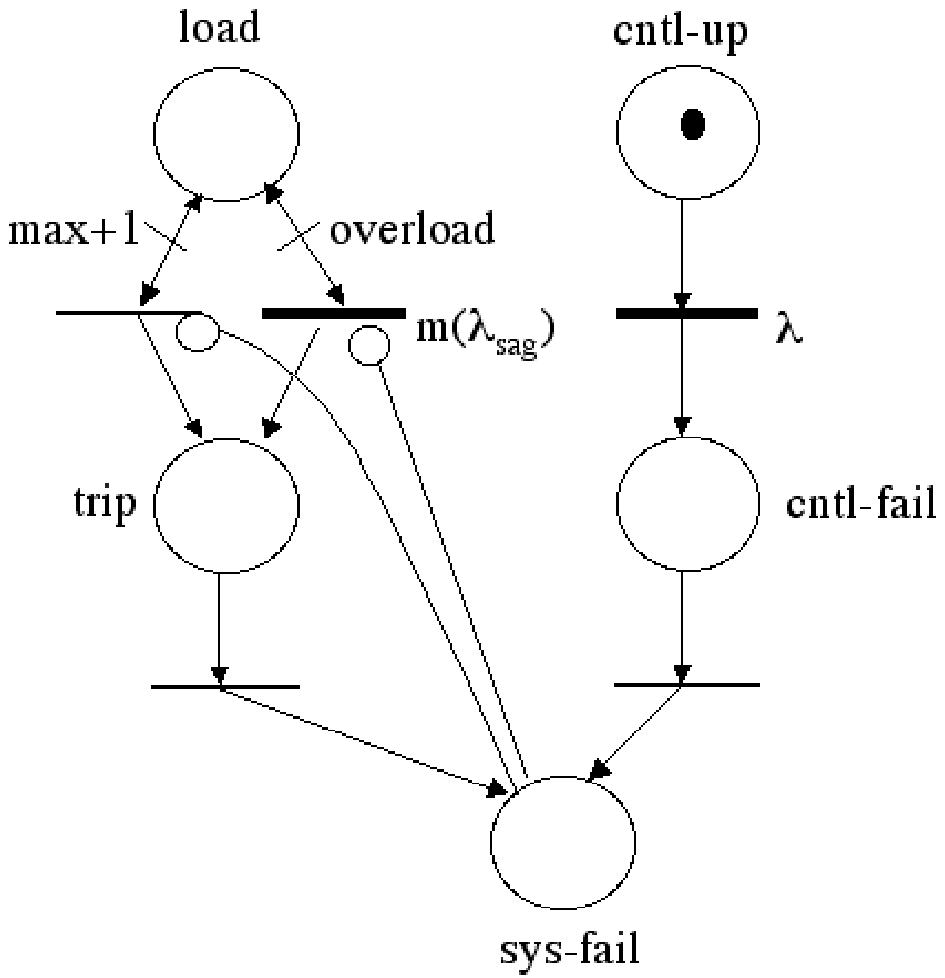


Multi-mode Failure Model

Hybrid Common Mode Failure



Multi-mode Failure Model GSPN



Summary

- Critical infrastructures are complex control systems with interdependencies and fragilities beyond common expectations.
- The roots of these characteristics lie in the relatively benign, but fast paced development environment in which our digital society has developed.

Conclusions

- Infrastructures Fragile
  - Real-time complex control systems
  - Evolved in benign environments
  - Optimized for non-malicious reliability
  - Little consideration for survivability
  - Loaded with common mode faults
  - Susceptible to cascading failure
- Common Mode Faults Trigger/Accelerate Cascading Failures

Conclusions (continued)

- *GSPNs help model Common Mode Interdependencies*
- Survivability should be a design consideration
- **Hostile environments should be a design assumption**
  - Malicious code | malicious intrusion | physical and data sabotage
- Elimination / mitigation of common mode faults a necessity

SEDS/EIS Related Publications

- **Sheldon, F.T.** Potok, T.E. and Kavi, K.M., "Multi-Agent System Case Studies in Command and Control, Information Fusion and Data Management," To appear 2004, *Informatica Jr., SSI, (SI Agent Based Computing)* 2004.
- **Sheldon, F.T.** Potok, T.E., Krings, A. and Oman, P., "Critical Energy Infrastructure Survivability, Inherent Limitations, Obstacles and Mitigation Strategies," To Appear: Int'l Jr of Power and Energy Systems –Special Theme Blackout, ACTA Press, Calgary Canada, 2004
- **Sheldon, F.T.**, Potok, T.E., Loebl, A., Krings, A. and Oman, P., "Energy Infrastructure Survivability, Inherent Limitations, Obstacles and Mitigation Strategies," *IASTED Int'l Power Conf. -Special Theme Blackout, New York NY, Dec. 10-12, 2003.*
- **Sheldon, F.T.** and Jerath, Kshamta, "Assessing the Effect of Failure Severity, Coincident Failures and Usage-Profiles on the Reliability of Embedded Control Systems," *ACM SAC, Cyprus, Mar. 2004.*
- **Sheldon, F.T.,** Jerath, K., and Greiner, S.A., "Examining Coincident Failures and Usage-Profiles in Reliability Analysis of an Embedded Vehicle Sub-System," *Proc. 9th Int'l. Conference on Analytical and Stochastic Modeling Techniques ASMT 2002*, Darmstadt, June 3-5, 2002.

Key SE Issues in EIS I

- Provide readier access to formal methods for developers of EIS-critical systems by further integration of informal and formal methods.
- Develop better methods for EIS analysis of product families and safe reuse of Commercial-Off-The-Shelf software.
- Improve the testing and evaluation of EIS-critical systems through the use of requirements-based testing, evaluation from multiple sources, model consistency, and virtual environments.

Key SE Issues in EIS II

- Ensure SW technology transfer from the lab to practice with case studies to *enable* earlier adoption of potentially cost savings / EIS ensuring advances.
- Advance the use of runtime monitoring to detect faults and recover to a safe state, as well as to *profile system usage to enhance safety analyses*.
- Promote collaboration with related fields in order to exploit advances in areas such as security and survivability, software architecture, theoretical computer science, human factors engineering, and software engineering education.

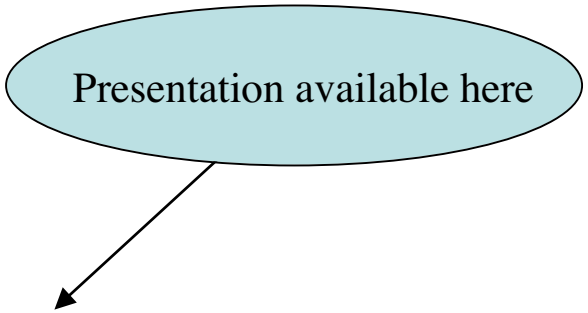
Key SE Issues in EIS III

- Stimulate vulnerability research case studies and test beds
- Acceptance testing for security by federal government
  - Safety regulations, ethics education, investigate infrastructure (5-10 yrs), light-weight common criteria, certifiable security process
- How to measure security to say I am at the level four or five needed from the feds
- What are the motivations... having power over computers (white/gray/black hats).
- Work with network providers mitigate the flow of viruses
- Anti-virus emergency response team and *automatic* proactive intrusions detection
- Cyber first responders (provide nature of threats)

Contact Information

Frederick T. Sheldon, Ph.D. and Tom Potok, Ph.D.
Software Engineering for Dependable for Systems
Applied Software Engineering Laboratory

Rick: 865-576-1339
Tom: 865-574-0834
Fax: 865-574-6275



URL: http://www.csm.ornl.gov/~sheldon/pubs.html
http://computing.ornl.gov/cse_home/acer.shtml

The end…