SAND2007-3359C

Singapore Infocomm Vulnerability Study for National Critical Infrastructure

June 4-8, 2007

Karen Page
Assurance Technology and Assessments

Jason Stamp
Energy System Analysis

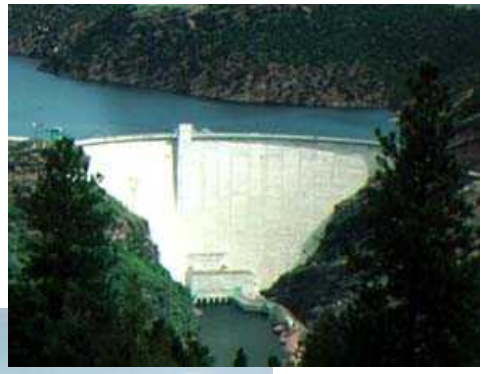
Bill Young
Networked Systems Survivability & Assurance

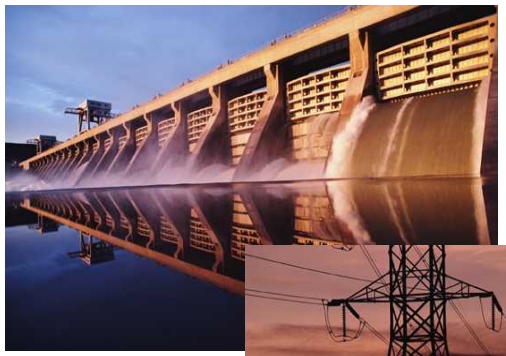
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Sandia National Laboratories

Information Systems Used in Critical Infrastructure Sectors

- Electric power generation, transmission, and distribution
- Water treatment and distribution
- Telecommunication systems
- Manufacturing and chemical production
- Transportation control systems
- Banking and Finance
- Health Services





Data Collection Workshop

Sandia National Laboratories

Data Collection - Purpose

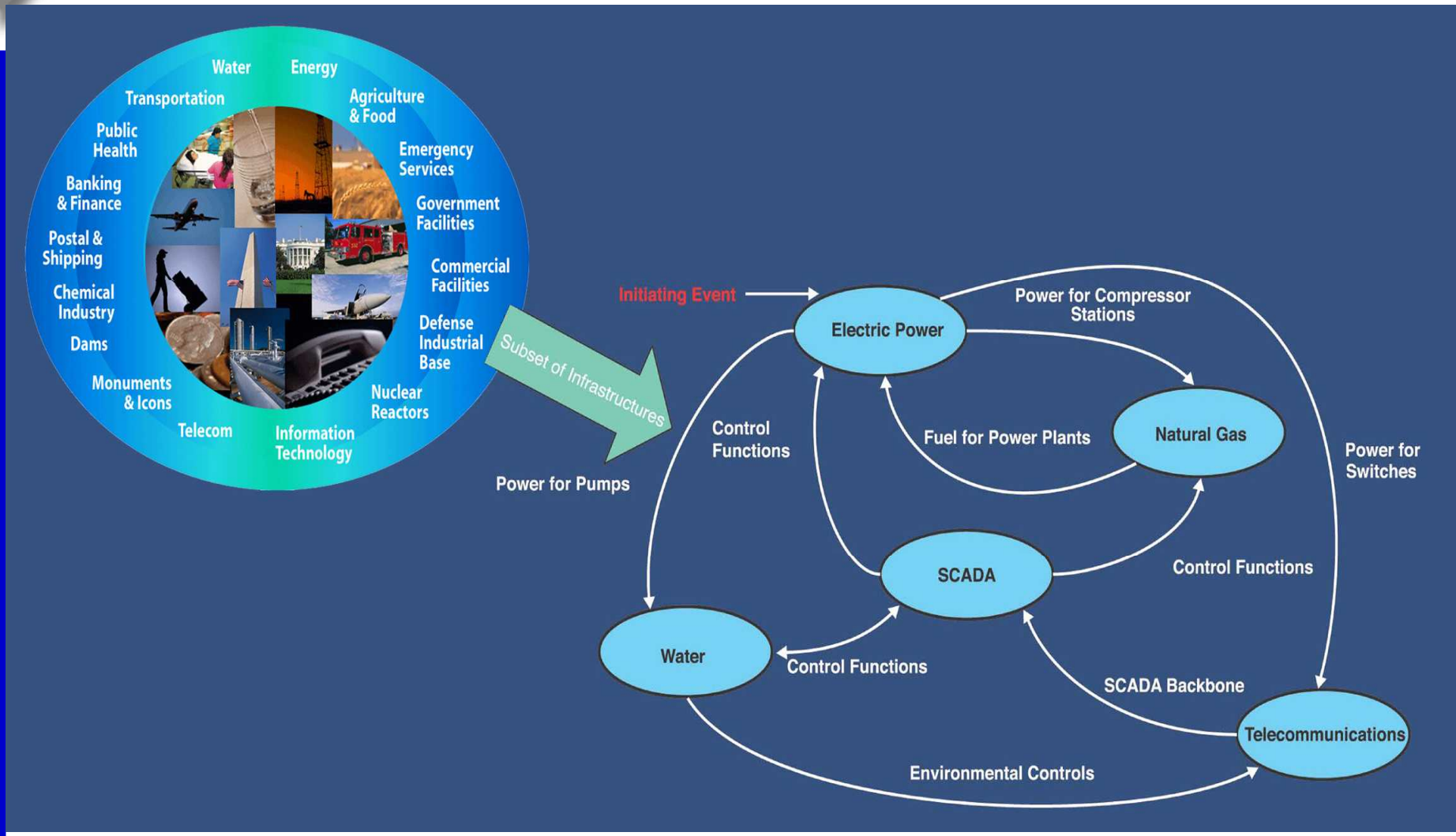
Understanding the system

- mission/purpose
  - Primary missions
  - Secondary missions
- design/architecture
- dependence on information systems
- consequences of information system compromise
- interplay between Critical Infrastructure (CI) sectors

Data Collection- Additional Elements to Consider

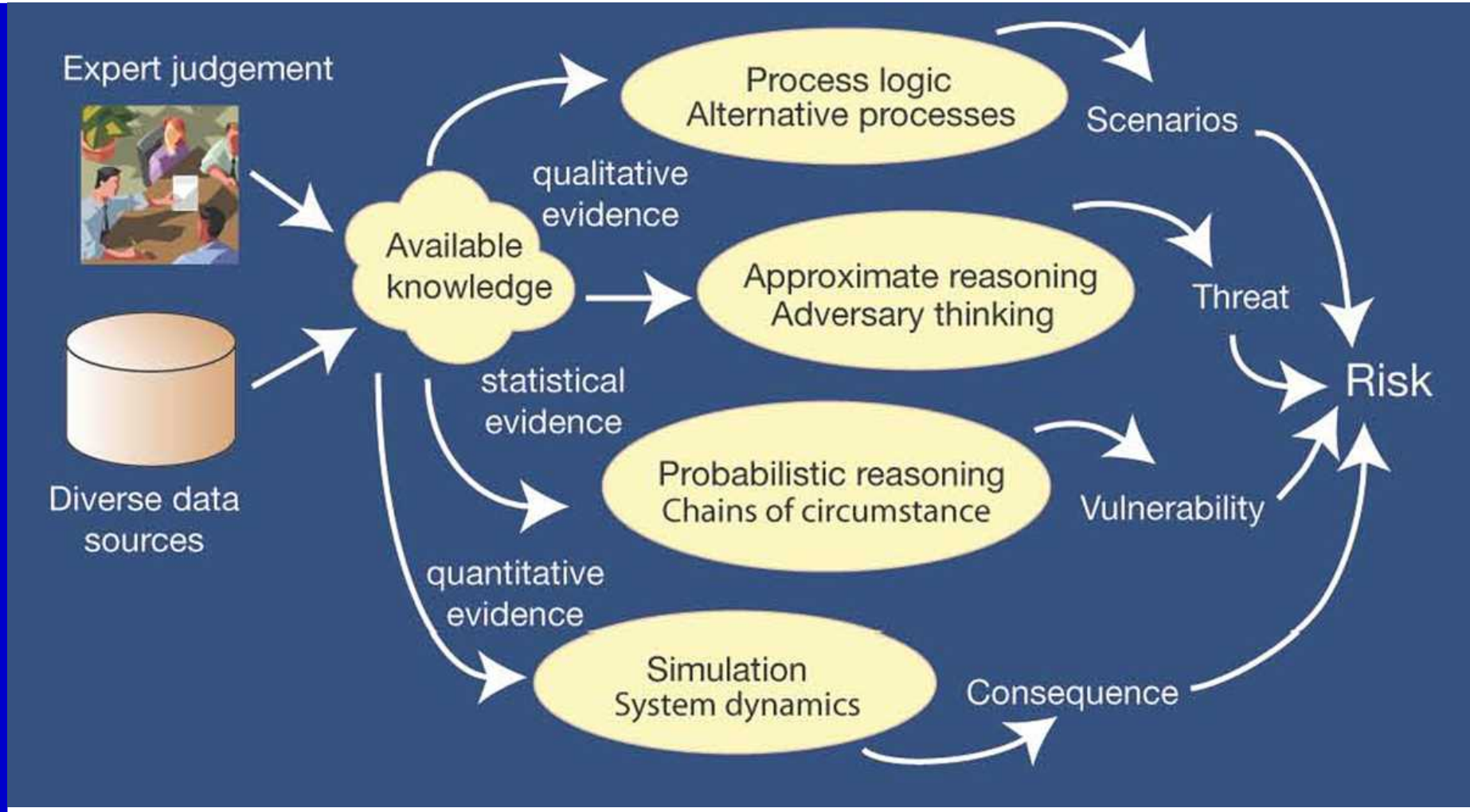
- Understanding the threat
- Identifying the overlap between adversaries' objectives and owners'/stakeholders' consequences of concern
- Recognizing that information systems typically evolve on a much shorter time scale than the associated CI system

Critical Infrastructure Interdependencies



Sandia National Laboratories

Critical Infrastructure Risk Elements

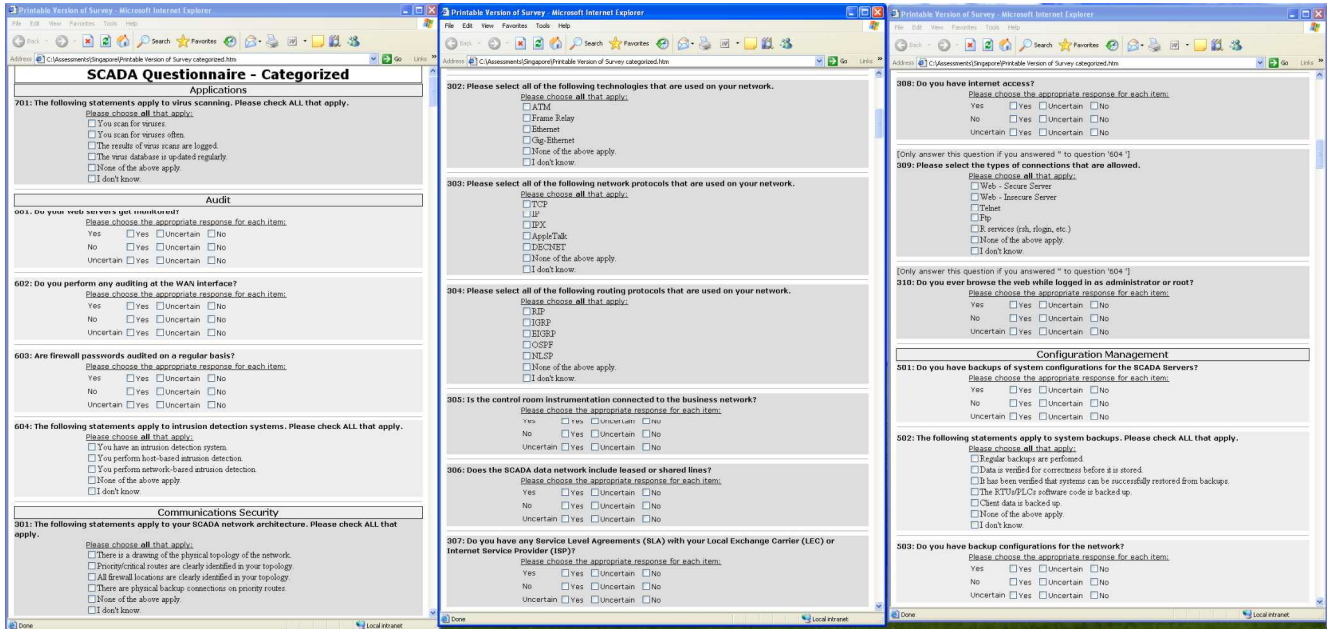


Critical Infrastructure

- **Discover interdependencies**
  - **Capacity, connectivity, storage, physical and nonphysical connections**
  - **Contingency planning**
    - **Abnormal operations**
    - **Backup power**
    - **Chain-of-command**
  - **Interview SME's/Operators**
    - **Hypothetical scenarios help facilitate discussions that uncover vulnerabilities**
    - **Describe workarounds if information system fails**
    - **Follow the leads: cascades of contacts**
  - **Modeling**
    - **Tool of the discovery process**

Collection Methods

- **Questionnaires and Interviews**
  - **Owners/Operators**
  - **System/network administrators**
  - **Designers/Developers/Testers**
  - **Network/physical security personnel**



Sandia National Laboratories

Other Information Sources

- Review system documentation and records
  - System security requirements documents
  - System design documents
  - Implementation documents
  - Concept of operations documents
  - Hardware schematics
  - Network diagrams
  - Device configurations
  - User/Installation/maintenance guides
  - Security plans, procedures, policies
  - Previous security appraisals, penetration tests
- Physical examination and observation
  - On-site visit

System Characterization

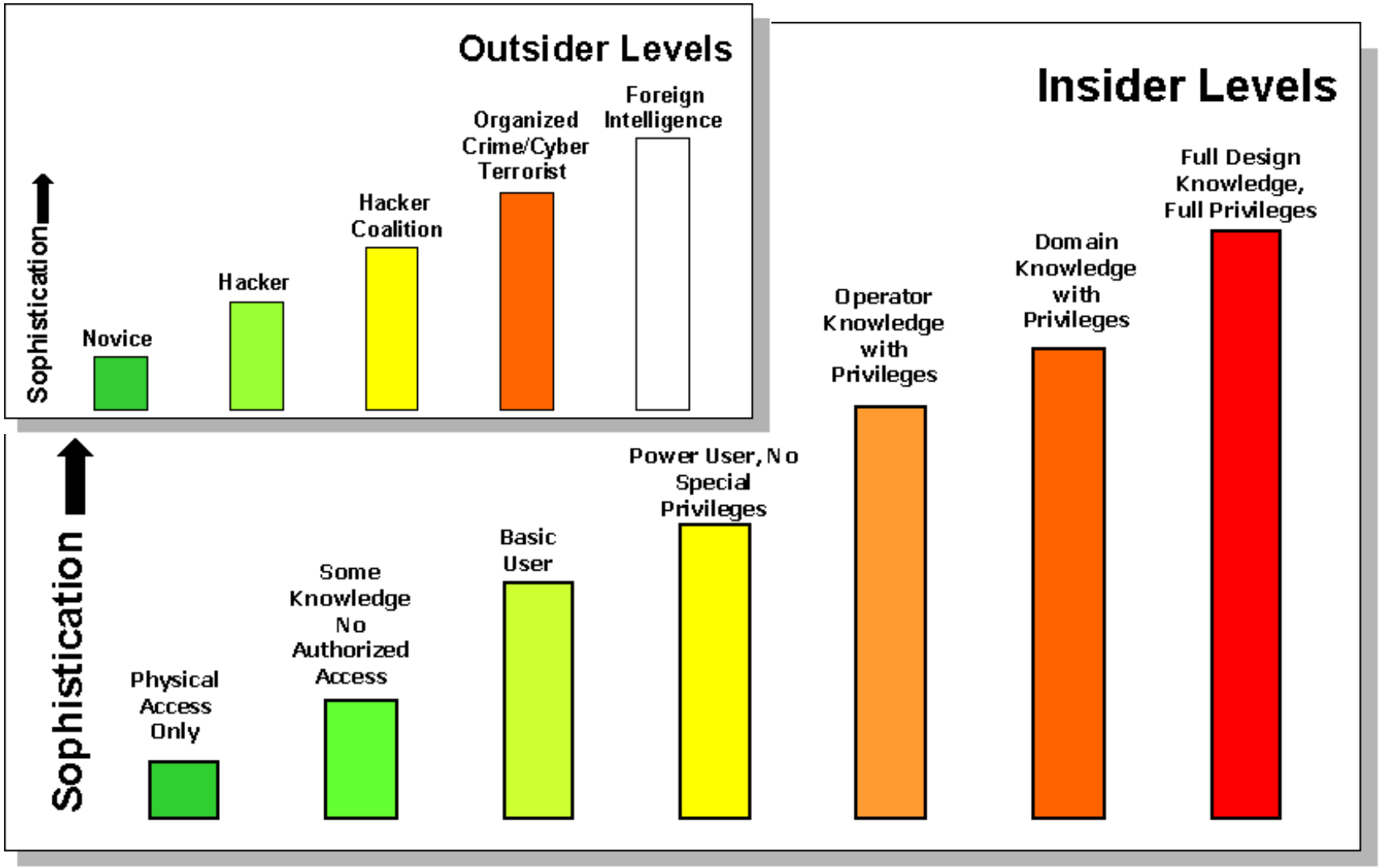
- System architecture
  - Individual sectors
  - Information systems
  - Supervisory Control and Data Acquisition (SCADA) systems
- Information flows
  - Categorization and prioritization
  - Within a CI sector
  - Among CI sectors
- Functional/logical interactions and behaviors
- Physical location of key infrastructure and infocomm elements
- Other system specifics

Leveraging the Adversary Characterization

- Consequences can be broadly characterized:
  - Consequences that are of concern to stakeholders and are also of interest to adversaries
  - Consequences that have not been identified by stakeholders but are of interest to adversaries
- The former comprises the bulk of consequences that are of highest concern, while the latter may include severe unknown consequences
- In both cases, the interests, goals, and constraints of the adversaries are very relevant

Must consider adversary's perspective during data gathering for risk analysis.

Adversary model: Sophistication



Sandia National Laboratories

Consequences of System Compromise: Metrics

- Loss of life – 1, 100s, 1000s?
- System interruption – secs, mins, hrs?
- Poor public image – # tech support calls, CNN
- Liability- $$
- Equipment damage - $$
- System degradation
- Regulatory non-compliance

Summary

- Many sources of information are available.
- Gathering a complete set of data is difficult, expensive, and time consuming.
- The quality of the assessment outcome depends on the accuracy and completeness of collected data.

Your participation is the most critical part of the data collection activity.

Additional Slides

Outsider Adversary Attributes

	Resources	Mission	Risk Tolerance	Sophistication
Hacker	**Low – Skills Only**	**Tactical – knowledge, visible effects**	**Moderate – knowledge of penalties, accepts risk of being caught**	**Moderate**
Cyber Terrorist	**High – ~$10M**	**Strategic – goal oriented, political**	**Low – does not want to be caught**	**High**

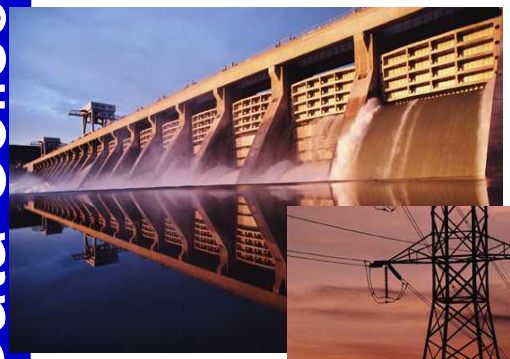
Insider Adversary Attributes

	Resources	Mission	Risk Tolerance	Sophistication
Physical Access Only	**Low**	**Disruption**	**Low – Moderate**	**Low**
Operator Knowledge	**Low**	**Disruption/Financial gain**	**Low**	**Moderate – High**
Full Design Knowledge	**Moderate**	**Disruption/Financial gain**	**Low**	**High**

Additional slides for the SCADA portion of the workshop, June 8

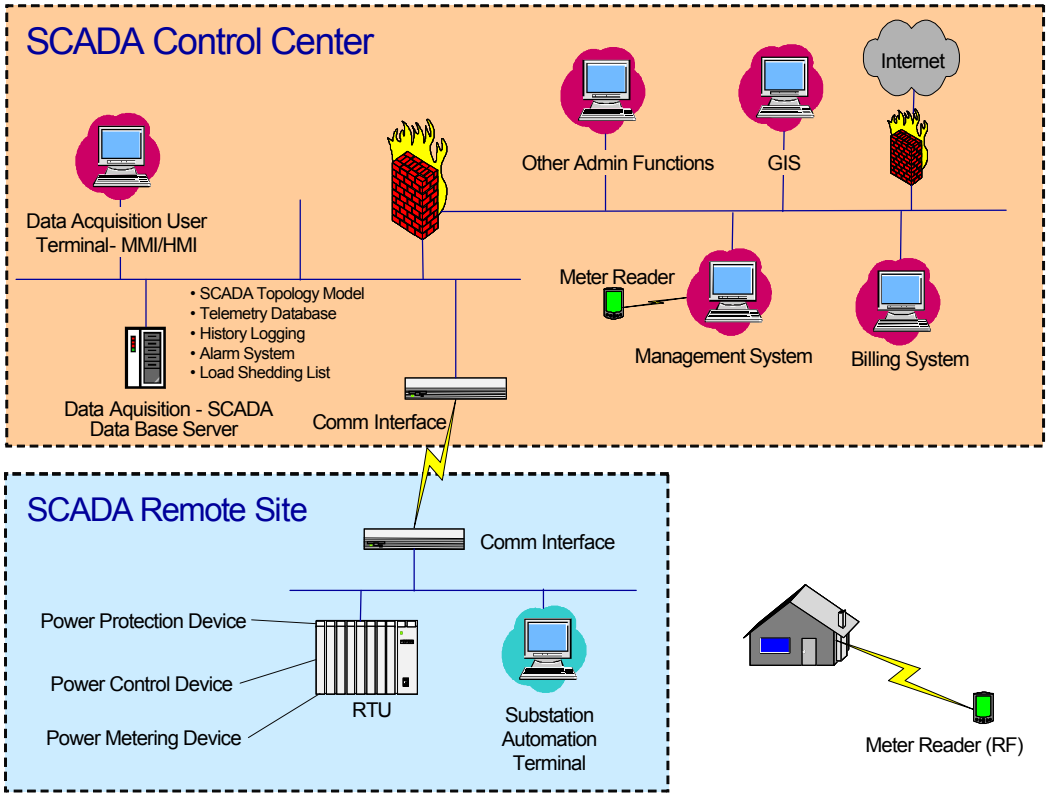
Information Systems Used in Critical Infrastructure Sectors

- Electric power generation, transmission, and distribution
- Oil and gas pipelines
- Water treatment and distribution
- Telecommunication systems
- Manufacturing and chemical production
- Transportation control systems



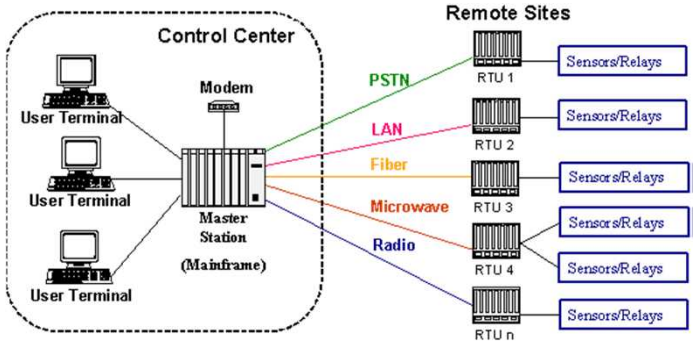
Automation System Elements

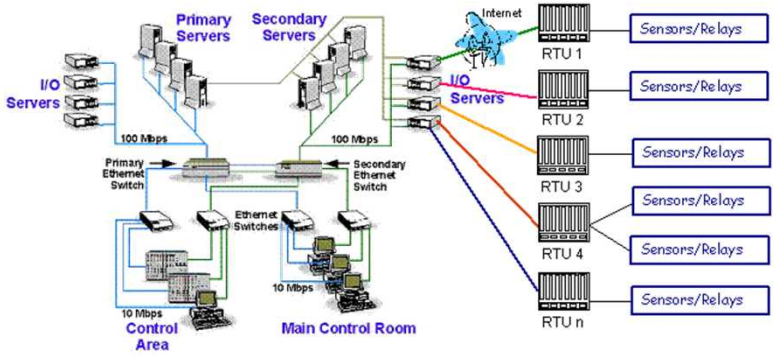
- Operating systems
- Computers
- HMIs and GUIs
- Databases
- Sensors
- Relays
- Switches
- RTUs, PLCs, IEDs
- Networks
- Applications
- Etc.



Adoption of Standardized Technologies With Known Vulnerabilities

- Conventional operating systems
- Modern networking
- Open protocols and standards
- Adopted the entire class of cyber threat faced by normal information technology systems
- Web services, including http servers, telnet configuration, etc.
- Weak authentication services
- Little or no encryption support
- Same mistakes as IT, only years later



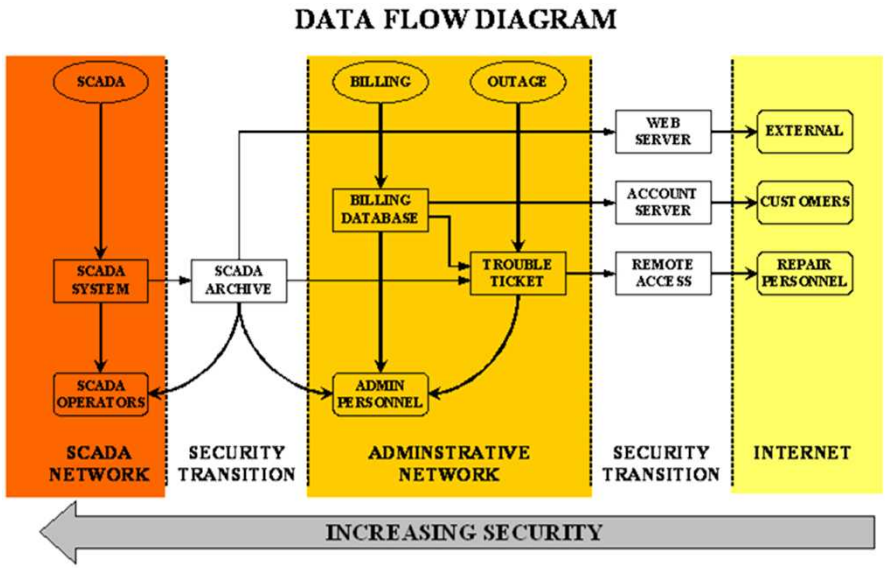


Data Collection Workshop

Sandia National Laboratories

Connectivity of Control Systems to Other Networks

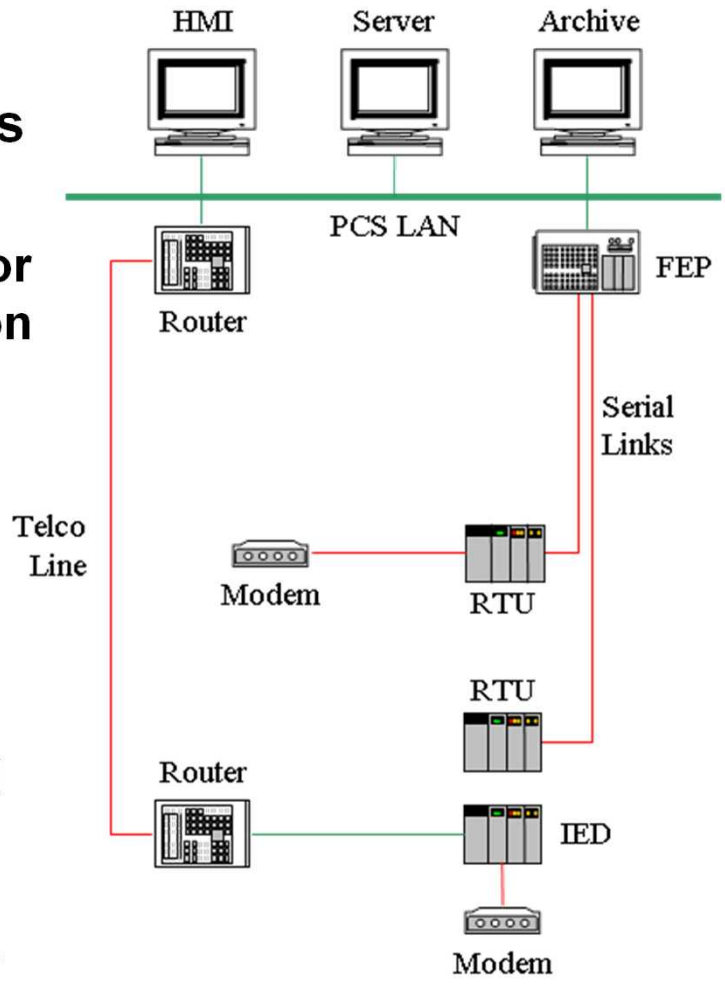
- Connection to enterprise networks
  - Transfer data with economic value
  - Process optimization settings pushed into the SCADA system
  - Poor security controls at the perimeter
- Use of enterprise network for SCADA backbone connectivity



- Internet publishing of data directly from SCADA
- Connections between automation systems for coordinated control among multiple entities
  - Data relationships – one system depends on data from another
  - Direct control of others' assets (less common)

Insecure Connections

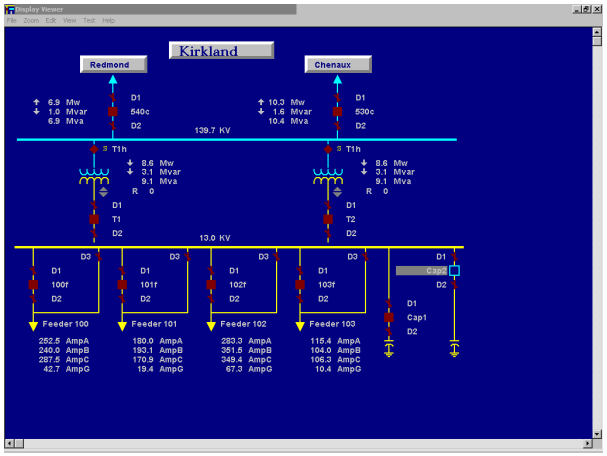
- Vulnerable remote access procedures
  - Insecure modem connections
  - Access from business VPN network for SCADA maintenance and configuration
  - Vendor access
    - Unsecured connectivity
    - High-privilege accounts
- PCS WAN perimeters and security
  - Some may own a physically private network, but it typically is not entirely contained within a controlled physical perimeter
  - Some PCS WAN depends on a VPN formed from leased telecom assets or Internet connectivity



Widespread Availability of Technical Information

- Infrastructure information
  - Locations are generally well-known for telecom and other assets
  - Diagrams and drawings for public projects
- Vendor product data
  - Literature and manuals
  - Training sessions
  - Default passwords and workarounds
- This issue in particular accentuates the capabilities of even low-level threats

Increasing Deployment of SCADA and Automation



- Some processes cannot be run manually at all
- In other cases, the manual interface is only through automation equipment
- Use of automation networks for security and environmental systems
- Little or no training programs to ensure proficiency for manual capabilities
- Attrition of key personnel with manual operation skills

Leveraging the Adversary Characterization

- Consequences can be broadly characterized:
  - Consequences that are of concern to stakeholders and are also of interest to adversaries
  - Consequences that have not been identified by stakeholders but are of interest to adversaries
- The former comprises the bulk of risks that are of highest concern, while the latter may include severe unknown risks
- In both cases, the interests, goals, and constraints of the adversaries are very relevant

Must consider adversary's perspective during data gathering for risk analysis.