The electric power industry has become a fundamental underpinning of 21st century life. In a landmark report on “The Electricity Economy,” author Jesse Berst and colleagues describe the convergence of growing demand, an increasing dependence on computerized supervisory control and data acquisition (SCADA) systems, and the inevitable complexity of interactions among elements controlled by diverse entities with limited coordination.[1] To illustrate the growth in electricity demands, the report’s Table 1 shows global electricity demands of 2.06 terawatts (TW) in 1950 vs 3.8 TW in 2000 and a predicted 6.99 TW in 2050. The proportion of electricity as a percentage of global energy utilization was 10.4% in 1950 and 25.3% in 2000; by 2050 it may reach 33.7%. The authors add,

Today we depend on electricity for basic needs such as food, water, shelter, communication, employment and health care. Those needs are served by infrastructures for food preservation, water treatment, heat and light, phone service, Internet, offices, factories, hospitals and emergency response, to name a few. Yet all of those essentials degrade or disappear without electricity.[2]

Electric power has become a central component of what has come to be known as *critical infrastructure*. John Moteff and Paul Parfomak of the Resources, Science and Industry Division of the Library of Congress’ Congressional Research Service trace the evolution of this term through several administrations. The broadest definition they display includes the following sectors:

- Transportation
- Water supply/waste water treatment
- Education
- Public health
- Prisons
- Industrial capacity
- Waste services
- Telecommunications
- Energy
- Banking and finance
- Emergency services
- Government continuity
- Information systems
- Nuclear facilities
With the possible exceptions of “monuments and icons” and “large gathering sites,” every single one of these sectors depends critically on electric power for continued operations.

In October 1997, the President’s Commission on Critical Infrastructure Protection (the “Marsh Report” named after Commission Chairman Robert T. Marsh[4]) included the following warning:

Prolonged disruption in the flow of energy would seriously affect every infrastructure.

The significant physical vulnerabilities for electric power are related to substations, generation facilities, and transmission lines. Large oil refineries are also attractive targets. The increase in transportation of oil via pipelines over the last decade provides a huge, attractive, and largely unprotected target array. Oil and gas vulnerabilities include lines at river crossings; interconnects; valves, pumps, and compressors; and natural gas city gates. Large metropolitan areas could be deprived of critical fuel for an extended period by a properly executed attack.

The widespread and increasing use of Supervisory Control and Data Acquisition (SCADA) systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means. The exponential growth of information system networks that interconnect the business, administrative, and operational systems contributes to system vulnerability.[5]

In May 1998, responding to the Marsh Report, President Clinton issued Presidential Decision Directive 63 (PDD-63) entitled “Critical Infrastructure Protection” in which he set forth the following national goals:

No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from today the United States shall have achieved and shall maintain the ability to protect the nation’s critical infrastructures from intentional acts that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- state and local governments to maintain order and to deliver minimum essential public services.
• the private sector to ensure the orderly functioning of the economy and the
delivery of essential telecommunications, energy, financial and transportation
services.

Any interruptions or manipulations of these critical functions must be brief, infrequent,
manageable, geographically isolated and minimally detrimental to the welfare of the
United States.[6]

This series of articles reviews computer and operational security issues in the electric power
industry and explores the need for timely information on vulnerabilities, threats and attacks to
support rapid response and effective process improvement in the industry.

The next articles include a literature review in four parts with subsections:
• Review of Security Incidents Involving Electric Power Plants
  o Data Leakage, Industrial Espionage, and Insider Threats
  o SCADA and other Power Industry Information Systems Sabotage
  o Criminal Hackers and Malware versus Power Systems
• Recognition of Infrastructure Vulnerabilities
• Industry and Government Reports
• SCADA Security Organizations and Working Groups

Later, the series presents an analysis and discussion of the key findings from the literature
review.

The series ends with a set of fundamental proposals and practical suggestions for improving
security of SCADA systems in the electric power industry.

***

M. E. Kabay, <mailto:mekabay@gmail.com> PhD, CISSP-ISSMP, specializes in security and
operations management consulting services and teaching. He is Chief Technical Officer of
Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/> and Associate Professor
of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html >
in the School of Business and Management< http://norwich.edu/academics/business/faculty.html>
at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and

Copyright © 2010 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without
limit on any Web site, and to republish it in any way they see fit.

Endnotes
[1] Berst 2008, Table 1, p 12
Bibliography


