

Journal of Homeland Security and Emergency Management

Volume 1, Issue 4

2004

Article 402

Risks of Terrorism to Information Technology and to Critical Interdependent Infrastructures

Clyde G. Chittester*

Yacov Y. Haimes†

*Software Engineering Institute, Carnegie Mellon University, cc@sei.cmu.edu

†University of Virginia, haimes@virginia.edu

Copyright ©2004 by the authors. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher, bepress, which has been given certain exclusive rights by the author. *Journal of Homeland Security and Emergency Management* is produced by The Berkeley Electronic Press (bepress). <http://www.bepress.com/jhsem>

Risks of Terrorism to Information Technology and to Critical Interdependent Infrastructures

Clyde G. Chittester and Yacov Y. Haimes

Abstract

Coupled with the improved economic efficiency that information technology (IT) has generated are the adverse national impacts. A markedly increased reliance on IT and on the Internet has increased the complexity of our information systems because of the added interconnectedness and interdependencies between and among the infrastructures. This reliance has reduced the operational buffer zone in most infrastructures because of the ever-increasing adherence to the “just-in-time” philosophy as a vehicle for cost reduction and efficient operation, and it has enhanced accessibility of would-be terrorists to our telecommunications, defense, banking and financial institutions, as well as to other critical infrastructures.

When the operability of IT-based controls and equipment is affected by acts of terrorism, then the performance of critical interdependent infrastructures such as railroads, electric power grids, or oil and gas pipelines is profoundly affected. Such information technology includes supervisory control and data acquisition (SCADA) systems, the global positioning system (GPS), and satellites.

A detailed discussion is presented on the SCADA system and its use by railways. Hierarchical holographic modeling (HHM) and control objectives for information and related technology (CobiT) are introduced and used to identify sources of risk to SCADA systems in the railroad sector. The vulnerabilities to terrorist attacks of IT, SCADA, GPS, and satellites are explored. The risk assessment and risk management process is demonstrated on a railway system. In quantifying the probability of an attack, the intent and capabilities of terrorists are used as surrogates. The following terms are defined: vulnerability, threat, risk, intent, and capability.

Given the growing interdependency among our critical infrastructures and sectors of the economy, increasing Internet capability and user reliance on it, and on commercial-off-the-shelf (COTS) products, SCADA, geographical positioning systems (GPS), and satellites systems, the trade-offs between efficiency (reliance on technology) and reliability, availability, and security may have to be reevaluated, and appropriate risk assessment and management strategies must be developed.

KEYWORDS: Risk assessment, Risk management, SCADA, Terrorism, Railways, HHM, CobiT, Information technology, Internet, COTS, GPS, Satellites

A. INTRODUCTION

Our national critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, the defense/industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, and fiber-optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security...These computer networks also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, radar, and stock markets, all of which exist beyond cyberspace...Many industries in America have radically transformed the way they control and monitor equipment over the last 20 years by employing digital control systems (DCS) and supervisory control and data acquisition systems (SCADA).

George W. Bush
The National Strategy to Secure Cyberspace
The White House, February 2003

Information technology (IT) in its multifarious manifestations has profoundly increased the gross national products of many countries, and has improved the quality of life of millions around the world. Its major contributions have been improved efficiency and the replacement of myriad human tasks with computerized and automated functions. The cost of this efficiency has been the significant exposure of the IT systems and our physical infrastructures to risks of terrorism, because of the added interconnectedness and interdependencies between and among infrastructures. The effectiveness of IT has markedly increased adherence to the “just-in-time” philosophy as a vehicle for cost reduction and efficient operations. Furthermore, the use of IT by industry and government organizations for data acquisition, process control, information management systems, and numerous other cyber-based activities, has resulted in a large number of systems with common functionality, albeit with different acronyms, including digital control systems (DCS), supervisory control and data acquisition systems (SCADA), and computer aided dispatch (CAD). The SCADA system will be used throughout this paper to represent this class of systems, and the CAD system will be discussed in relation to the railroads.

Information technology has enabled the global positioning system (GPS) to become ubiquitous for military as well as civilian use. At the same time, the well-documented vulnerability of satellites to orbital nuclear attacks and to other threats renders the overall IT derivatives at risk, along with the systems that are dependent on them. Another element of concern is the continuous assault of hackers and would-be terrorists on the integrity of the Internet and on cyberspace and therefore, on information assurance (the backbone of all IT systems). Indeed, IT has enhanced the accessibility of would-be terrorists to our defense program, banking and financial institutions, and to other critical infrastructures. The interdependencies among IT, the effective performance of SCADA systems, and the dependence of GPS on the availability and survivability of satellites, constitute the roadmap of risks addressed in this paper.

In sum, the capability and increased functionality of our IT systems have given part of the business community a competitive advantage but also increased vulnerability, and thus risk. The combination of the many vulnerabilities to terrorist attacks of IT, SCADA systems, GPS, and satellites, and the corresponding risks to the systems that they serve or control, must be addressed systemically. The control systems of railroads are used here as an example to demonstrate the urgency of these risks. Section B presents an overview of the SCADA system; Section C presents an overview of risks associated with information technology, including GPS and satellites; Section D addresses the assessment of risks to the railway SCADA systems through hierarchical holographic modeling (HHM); Section E addresses control objectives for information and related technology (CobiT); Section F integrates the CobiT framework with HHM within the risk management process; and Section G summarizes the paper.

B. OVERVIEW OF SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS

B.1. Introduction

The fundamental purpose of a SCADA system is to control and monitor specific operations, local and/or remote. The need to store business information has added a new function to SCADA: the *management information system* (MIS). MIS enables managers and customers in remote locations to monitor the overall operations, and to receive data that allows higher-level business decisions to be made or reviewed. For example, Federal Express, UPS, and

other carriers make extensive use of SCADA systems by tracking the location of every package at any moment. Furthermore, SCADA systems enable railroads to divert goods on trains as they move across the country; enable the electric power companies to buy and sell power; and enable service companies to read meters remotely and bill customers.

The growth of high-speed, reliable telecommunication systems has lowered the development and maintenance costs of SCADA systems. In past years, SCADA systems used their own dedicated code or point-to-point communication systems that were maintained by either the users or the supplier of the system. However, highly reliable telecommunications, and more recently the Internet and wireless communications, have enticed the developers of SCADA systems to replace or supplement more reliable and trustworthy communications systems with less costly commercial-off-the-shelf (COTS) packages. This substitution lowers costs in several ways: (1) commercial hardware is usually cheaper to buy and maintain, (2) there are standard software packages that interface with the telecommunication systems, and (3) most system developers use the same telecommunication system as the developers of MIS, and this makes it easier to interface with the management information system.

Increasingly, SCADA systems and related technology are replacing and displacing human operators and data collectors in many critical infrastructures. Examples of the functions that SCADA railroad systems are performing include computer-aided train dispatching, underground track heaters for sensors, and control devices. In addition, other systems that are SCADA-controlled include transportation systems, oil and gas, and power supply schedule systems.

Critical infrastructures, such as water, oil and gas, electric power, telecommunications, and transportation, are becoming increasingly interconnected and interdependent. In particular, data collection, control, communication, and management, which are essential for the effective operation of large-scale infrastructures, are being performed by SCADA systems. These work remotely to improve the efficiency and effectiveness of the control, operations, and management of critical physical infrastructures.

Two equally important and separate components of SCADA—the engineering subsystem and the MIS for business—could be in conflict at times. The MIS cannot operate without the process control system (PCS) but the PCS can function without the MIS. Thus, although the two are equally important, the PCS has dominance over the other. Furthermore, if the process is not controlled correctly, it will diminish the usefulness of the data in the MIS. Also, because the designers of these two systems are usually separate companies, the customer generally buys the PCS from one vendor, and buys or develops the MIS separately. This makes integrating security into the SCADA system more difficult. The situation is further complicated by company hierarchy; in most companies, the MIS is under the control of the chief information office (CIO), while the PCS is controlled by engineering.

Risk is commonly defined as a measure of the probability and severity of adverse effects [Lowrance 1976]. The expected value of risk is (for the discrete case) the summation of the products of the consequences and the corresponding probabilities of all possible events (scenarios). This expected value has significant limitations, or may even be an erroneous metric of risk, for events of catastrophic consequences and low or not-unlikely probability [Haimes 2004, Haimes et al. 2004a, b]. This observation is particularly relevant and important for risks of terrorism, such as the September 11, 2001 attacks on the United States. An argument can be made that terrorist attacks such as these could be random events but not necessarily belong to a random process. Gnedenko [1963] defines the relationship between the occurrence of events and the conditions under which they can be considered random and be assigned probabilities: He writes, “In probability theory, random events possess a number of characteristic features: in particular, they all occur in mass phenomena.” Gnedenko defines mass phenomena as those occurring in assemblages of large numbers of entities of equal or nearly equal status, and with *regularities* of the randomness. Malevolent attacks do not satisfy the *regularities* condition for probability. In such cases, the probability of a terrorist attack may be represented by two surrogate measures: the *intent* and *capability* of the would-be terrorist. To better appreciate the discussion on risk management of extreme and catastrophic consequences, it is constructive to relate the centrality of state variables to the following terms [Haimes 2004, and Haimes and Horowitz 2004]:

- *Vulnerability* is the manifestation of the inherent states of the system (e.g., physical, technical, organizational, cultural) that can be exploited by an adversary to adversely affect (cause harm or damage to) that system.
- *Threat* is the intent and capability to adversely affect (cause harm or damage to) the system by adversely changing its states.
- *Risk* is the result of a threat with adverse effects to a vulnerable system.
- *Intent* is the desire or motivation of an adversary to attack a target and cause adverse effects.
- *Capability* is the ability and capacity to attack a target and cause adverse effects.

Thus, relative to the probability of an adverse effect, we distinguish in this paper between two major sources of failures: One related to terrorist attacks and the second includes all other non-terrorist-related failures. The reader is referred to Haimes [2004] and Haimes et al. [2004a, b] for detailed mathematical calculations for both cases.

B.2. The Internet and SCADA Systems

The Internet is not yet as reliable as dial-up telecommunication systems, and the latter are not as reliable as dedicated code systems. Thus, the developers of a SCADA system usually use a combination of all three media in their communication components. One unfortunate by-product of the evolution of telecommunications and the Internet is that it has made SCADA systems more vulnerable to outside intruders. This is due primarily to the open architecture of the telecommunication systems, which is necessary to allow equipment from various users to interface with them. As we know, the Internet has become so standard that anyone with a personal computer and a cable interface can connect to it by using one of the many service providers, such as AOL.

The Internet is in essence a large party-line system, where everyone is connected to everyone else. Users and systems have unique addresses, known as the Internet protocol (IP) address. Thus, if one party wants to communicate with another, all that he or she needs is the correct IP address. This, of course, also works well for an intruder who can secure access to the SCADA operator's IP address and then communicate with the SCADA system. Ironically, the factor that makes it possible for legitimate users to connect with several different systems in an asynchronous and random fashion, also benefits the intruder by making the Internet an easy target.

Flexibility makes the Internet both powerful and vulnerable. Knowledge of how the Internet works allows individuals to invade the security of other users, and thus also the SCADA system that is connected through the Internet. A malicious individual can send messages to IP addresses and try to break in, similar to an intruder entering a house through an unlocked door. Internet security is a difficult problem because it must be balanced with efficiency and accessibility. On the one hand, others must have access to a system to facilitate communication; on the other hand, access must be denied to unauthorized users. The nature of the Internet allows individuals to hide or assume false but legitimate identities, making it easy to gain access to the SCADA system.

High speed reliable communications have made the Internet possible, and standard operating systems, such as Microsoft OS, have made it practical and easy to use. Commercial operating systems have allowed all software developers to use the same basic programs to manage lower-level activities, such as communicating, storing data, and performing input and output. This standardization drastically lowers the cost of developing software and software developers use the same basic tools to build their systems. This common knowledge of the standardized operating system and of the tools used to gain access is what makes it so easy to break into Internet systems, including SCADA systems.

Thus, as with breaking into a house, getting through the door is just the first step. In many cases Internet intruders are stopped at the operating system. However, this is often far enough, because in essence, intruders can take over the operating system and convince the application programs that they *are* the operating system. In this way, intruders gain access to all vital information in the system.

To be effective, intruders need to understand how the system is designed. Their task is easier when users have adopted a standard operating system and standard tools. However, with special systems such as SCADA, more information is needed and this may have to be obtained without the use of a computer or the Internet. The intruder will need to secure access to the SCADA design and documentation, or have access to the developers of the systems.

B.3. SCADA System Configuration

SCADA systems are hierarchically distributed hardware-software subsystems interacting with human supervisory elements that enable the remote collection and analysis of vital information from physical infrastructures on a predetermined schedule [Boyer 1999; Bailey and Wright 2003]. The fundamental purpose of a SCADA system is to control local or remote operations. SCADA systems are generally comprised of several subsystems: the master control systems, remote units, communication systems, displays, and sensor input and output units. These subsystems are arranged in a specific way to create a system that will send and receive information that enables processes to be controlled and maintained. SCADA systems continue to assume additional roles and functions, including the recent requirement to mine and store information to meet the needs of management and customers. For example, an MIS has been added to enable remote monitoring of the overall operations of infrastructures, and to receive data that would facilitate higher-level business decisions.

SCADA systems are commonly composed of the following units (see Figure 1):

- *Master Terminal Units (MTU)* streamline and coordinate communications among the various units of the network.
- *Remote Terminal Units (RTU)* link the remote sensors and electronic devices with the MTU. Among the various modules within the RTUs and MTUs are:
 - *Analog Input Modules*
 - *Digital Input Modules*
 - *Analog Output Modules*
 - *Digital Output Modules*
 - *Modem* (an acronym for modulator-demodulator) that digitizes signals and transfers them through the MTUs and RTUs.
 - *Intelligent sensors* are the devices that collect remotely-controlled information.
 - *Telecommunications* is the medium within which signals are transferred (this includes the Internet, cable, dedicated telephone lines, radio, satellites, and others).
 - *Computer System Operator* who oversees the entire function of the SCADA system.
 - *Process* being controlled.
- Other units and functions that constitute SCADA systems include: data processing and communication subsystems, local user interfaces, self-diagnostics, and database maintenance.

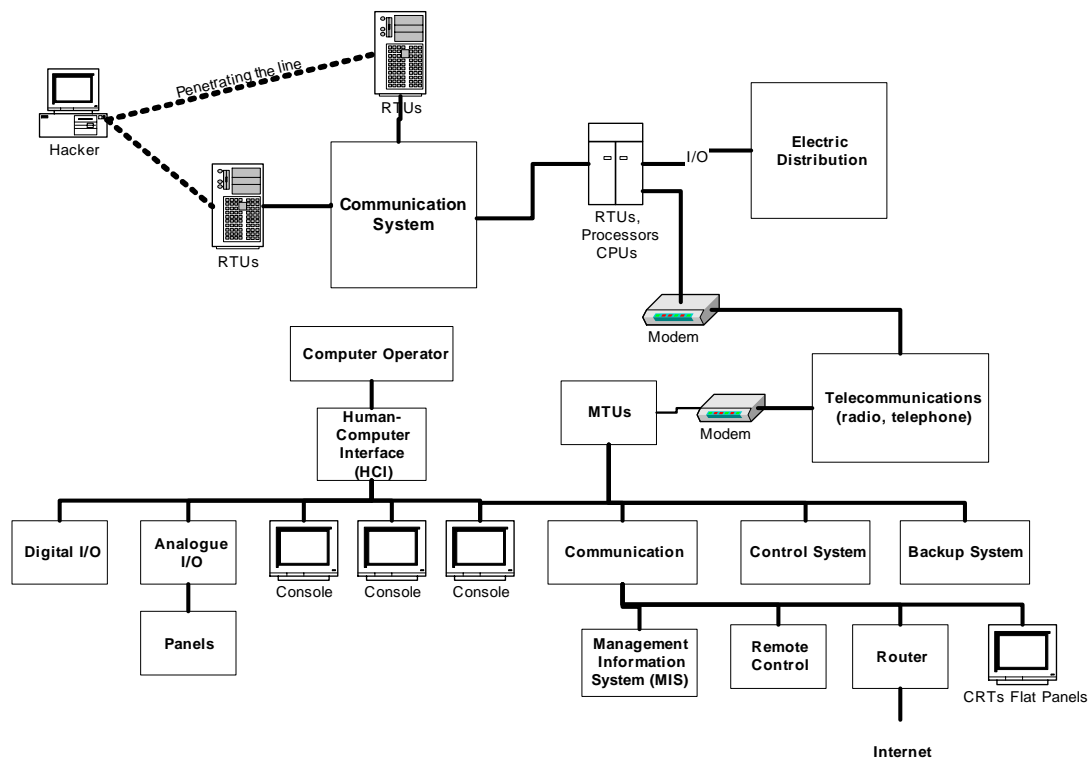


Figure 1. Configuration of SCADA Systems

B.4. SCADA Systems and Information Assurance

Cyber security and information assurance have increasingly high priorities on the agendas of civilian and defense organizations. Since computers have become an integral part of the planning, operations, and management of small and large organizations alike, the reliability of the information transmitted through the Internet, telephone and cable lines, satellites, and other media has become an urgently important concern. This is particularly true for safety-critical infrastructure systems whose control, and thus, safe operations depend on SCADA systems. Although the literature is replete with definitions of information assurance, we offer two here. The first is from the final report of the President's (Clinton's) Commission on Critical Infrastructure Protection [PCCIP 1997]:

Information Assurance is the preparatory or reactive risk management action intended to increase confidence that a critical infrastructure's performance level will continue to meet consumer expectations despite incurring threat-inflicted damage.

Longstaff and Haimes [2002] define information assurance as the trust that information presented by the system is accurate and properly represented; its measure of the level of acceptable risk depends on the critical nature of the system's mission and the perspectives of the individuals or groups using the information.

Malicious attacks on computer and SCADA systems may be initiated by diverse parties and take different forms. According to a recent report by the National Research Council [NRC 2002a], "[A]n attacker—who seeks to cause damage deliberately—may be able to exploit a flaw accidentally introduced into a system. System design and/or implementation that is poor by accident can result in serious security problems that can be deliberately targeted in a penetration attempt by an attacker." In particular, the authors of the NRC report argue that such "insidious accidental" problems arise because the software design, architecture, configuration, and integration of any operational system commonly are not being tested for security. To be sure, there are too many software system configurations to test and only a small fraction can be tested explicitly.

B.5. SCADA and Commercial-off-the-Shelf Software (COTS) Systems

As the SCADA systems grow in complexity, there is a need to reduce the time and effort to produce them, mainly to stay competitive. One way is to use commercial packages. The use of COTS, especially with open architecture, gives the SCADA developers more options when building their systems. At the same time, the increased use of COTS in SCADA systems and especially of commercial operating systems (OS) software products (prevalent in most IT-based products), increase the vulnerability, and thus the risk, to SCADA systems. The ubiquitous reliance within information technology on commercial hardware and software products has made the lives of users and computer programmers easier and seemingly more efficient. However, the hidden costs and risks remain very high and often unacceptable because of the uncontrolled quality assurance of COTS products [Longstaff et al. 2002]. In particular, as (1) the components of wireless electronic devices used in SCADA systems become standardized, and (2) the relatively low-cost uncontrolled reliability of COTS products, which dominate the market, renders the integrity and reliability of the information transmitted by SCADA systems becomes increasingly at great risk. Intruders and would-be terrorists may search for sensitive information or introduce malicious codes such as viruses and worms to modify or corrupt the information. SCADA systems do not have to be brought down to cause problems; misinformation can cause a disruption which is not easily diagnosed or corrected. Another critical role of SCADA systems where information assurance is essential is in the control of energy failures causing blackouts in electric-power distribution systems. SCADA systems are used to classify the energy losses of each of the distribution circuits online, and to detect those circuits that surpass the standard normal level of losses at any specific time. This situation has challenged planners and operators due to the associated technical and economic implications, and the fact that SCADA systems have become an important medium with which to control such failures [Khodr et al. 2002]. It follows that any malicious tampering with the SCADA system (by inducing and masking energy losses) can yield disastrous consequences for safety-critical systems.

In their quest to improve "economic efficiency" through the extensive use of SCADA systems, many organizations increased the centralization of their infrastructure operations. This markedly escalated the coupling among the multiple subsystems of these critical infrastructures and, consequently, their vulnerability to both cyber terrorism and to errors in human supervisory control. The adverse impact of SCADA systems on the ability of the operator of a complex system to respond to emergencies is highlighted by Perrow [1999] in his seminal book, *Normal Accidents*: "The swollen control room of the large facility is being decentralized in the face of the complexity, with "supervisory controls" or "distributed controls" as the new buzz words...This computerization has the effect of limiting the operations of the operator; however, it does not encourage broader comprehension of the system—a key requirement for intervening in unexpected interactions." If intruders "fool" the SCADA system, it may be very difficult, if not impossible, for the operator to quickly discover the problem and fix it. In fact, the SCADA system itself may fight the operator by resisting remedial actions.

Wireless COTS technologies are being widely employed within the nation's government and privately own systems today with no regard to how these technologies may be used in the control of critical infrastructures in the future. This vulnerability is being compounded by outsourcing the production of COTS hardware and software products abroad. Thus, by not employing sufficient protections in the COTS design and production of these wireless technologies, appropriate management options to reduce future risks (by using this technology) are lacking. For example, by employing additional security controls into the COTS design and implementation today, a concerted

effort should be made to avoid repeating historical mistakes made in the past in the introduction of other COTS technologies, such as the Internet and modem access.

B.6. SCADA Systems and Human Supervisory Control

Interest in human factors and ergonomics, which have been recognized as integral to good engineering since the 1950s, has grown by leaps and bounds during the last two decades. As covered in over 2100 pages of the second edition of the *Handbook of Human Factors and Ergonomics* [Salvendy 1997], the diversity of contributions to this discipline also attests to its importance in risk analysis. Experts in ergonomics and human behavior have been studying errors caused by operators, such as SCADA operators, who remotely control and monitor complex systems. Given the many safety-critical systems and physical infrastructures that are operated and managed through SCADA systems, the risks associated with human errors can be catastrophic. Two fundamental human elements in SCADA systems are pertinent to the assessment and management of such risks: (a) the human supervision, and (b) the intellectually-based software architecture and development. In essence, the operators know only what the SCADA systems are telling them, especially as these systems become more automated, with less human control. In a succinct figure, Helander [1997] relates the systems approach to human-computer interface, and human factors and ergonomics (see Figure 1). He warns that in reality, the operator-machine-environment interaction is much more complex, involving many more feedback loops and concepts. In this context, Stanton et al. [2003] argue that:

[E]rrors in human supervisory control can have potential disastrous consequences, which can impact upon the lives of many people, beyond those making the errors. This makes human supervisory control an important area of psychological research...Whilst virtual environments offer for physical “remoteness” to be overcome, there is the potential risk of the social consequences associated with the diffusion of responsibility if the control room engineers are not working in the same physical environment. Therefore the aspect of personal identity will also be a factor worthy of attention.

Furthermore, SCADA systems epitomize the essence of automation in terms of remotely controlling physical infrastructure systems. It is thus appropriate to evaluate the broad positive and negative effects of automation as we assess the risks to the infrastructures that are either directly controlled by SCADA systems, or are indirectly affected by them, due to their interdependencies and interconnectedness.

Sarter et al. [1999] describe some of the surprises and “unanticipated difficulties” with automation that are critical sources of risks associated with SCADA systems. They argue that, “In a variety of domains, the development and introduction of automated systems has been successful in terms of improving the precision and economy of operations.” Then they counterbalance this positive assessment by describing the nature of unanticipated difficulties with automation, through false hopes and misguided intentions associated with modern technology. A central theme in these unanticipated difficulties is the failure to understand and appreciate the interaction between humans and machines. In particular, SCADA designers and users have not seemed to recognize that automation, and thus seemingly independent systems, still require human involvement, supervision, and control. This prevailing mistake is at the heart of the inherent human-induced risks associated with SCADA systems.

Further, Sarter et al. [1999] identify a host of unexpected problems with human-automation interaction; for example, workload distribution is affected. Responsibilities and accountabilities within an organization are adversely disrupted because automation transcends the functionality of many operators. This is a fact that impinges on the quality of the work, since SCADA systems, not humans, are the controlling agents. Automated systems require more highly-skilled personnel and a longer span of attention to monitor their complexity. Also, the introduction of automation “changes the cooperative architecture, changing the human role, often in profound ways...[c]reating partially autonomous machine agents is, in part, like adding a new team member.” [Ibid.]

B.7. SCADA Systems and Infrastructure Interdependency

Cyber terrorism, to which SCADA systems are vulnerable, can adversely affect not only the remotely-controlled infrastructure, but also other interconnected and interdependent critical infrastructures. These include telecommunications; electrical power systems; gas and oil storage and transportation; banking and finance; transportation; water-supply systems; emergency services; and, continuity of government.

Half a century ago, the intra- and inter-connectedness and the dependencies among the various sectors of the economy were on the agenda of researchers. Wassily W. Leontief [1951] was the first to develop a comprehensive model of the US economy that accounts for the complex relationships among all its sectors. This came to be known

as the *Leontief Input-Output Model*, which won him the Nobel Prize in Economics in 1973. The emergence of terrorism as a form of unrestricted warfare worldwide has added a new dimension to the importance of the Leontief Input-Output Model for two major reasons. The first stems from the visionary perspectives that guided Leontief. He saw the economy as a complex interconnected and interdependent large-scale system of systems, so that if one sector or a critical infrastructure is affected, the cascading effects are registered in varying degrees on most, if not all, other critical infrastructures and sectors of the economy. Haimes and Jiang [2001] adapted Leontief's input-output model to address the impacts of terrorism. In their *Input-Output Inoperability Model (IIM)*, the input constitutes a terrorist attack on one or more infrastructures, and the output is the resulting inoperability of these as well as other interconnected infrastructure sectors. An advantage of building on the IIM is that it is supported by major ongoing data collection efforts of the Bureau of Economic Analysis (BEA), U.S. Department of Commerce [1997, 1998]. The cost and organizational efforts required to carry out such an effort provide an available basis for IIM modeling of a terrorist attack.

The dominance of information technology (IT) today, which was absent in the 1950s, and the accelerated increase in the use of SCADA systems in data collection and the control of critical interconnected and interdependent infrastructures are another reason that the IIM has been significantly expanded. Assessing the risks associated with a terrorist attack on a safety-critical SCADA system is a requisite for an effective risk management. Thus, models, such as the IIM, provide quantitative measures of the adverse consequences of such events.

C. RISKS ASSOCIATED WITH INFORMATION TECHNOLOGY (IT)

Many experts agree that the dominant technology in the world today is information technology (IT), and that terrorism constitutes a major threat. Indeed, The risk of terrorism to IT is clear and present. Longstaff et al. [2000] offer the following perspectives on this subject:

The growth of information technology (IT) and almost universal access to computers has enabled hackers and would-be terrorists to attack information systems and critical infrastructures worldwide because, for all practical purposes, international boundaries have been eliminated in cyberspace.

Here are a few adverse national impacts from a markedly increased reliance on IT and the Internet:

- Increased complexity to our information systems because of the added interconnectedness and interdependencies between and among infrastructures.
- Reduced operational buffer zone[s] in most infrastructures, and the ever-increasing adherence to the just-in-time philosophy as a vehicle for cost reduction and efficient operation.
- Enhanced accessibility of would-be terrorists to our defense, banking and financial institution[s], and to other critical infrastructures.

But can we go back? If we have now become so dependent on the Internet, we may have to deal with the risk in a way that does not reduce or limit the capability of the Internet. If so, fewer options are available to mitigate the risk. For example, some organizations may not be able to work without the Internet. If risk mitigation meant that these organizations could not continue to use the Internet, it might affect their critical infrastructures in the same way that an attack would. Also, because IT and Internet growth has been so rapid, it is not clear that we understand in detail how everyone is using the information infrastructure.

C.1. The Vulnerability of Satellites and Global Positioning Systems (GPS) to Terrorist Attacks

Telecommunications technology, GPS, and IT in general are all intricately dependent on satellites. The GPS has been hailed as one of the most important technological advances of the late 20th century. Initially developed as a military weapon guidance system for the US and its allies, GPS has become a cornerstone for numerous applications, including transportation. As the use of GPS has skyrocketed and continued growth is projected, there is increased concern among US government officials, corporate leaders, and foreign entities, that the system is vulnerable to large-scale failures, intentional terrorist attacks, and interference from natural phenomena. The pervasiveness of GPS in civil transportation systems is extraordinary. For example, the US Coast Guard has declared that GPS is the main navigation system for all commercial maritime operations. Additionally, the Federal

Aviation Administration (FAA) has approved GPS as a supplemental navigation system for instrument flight rule (IFR) operations. Both of these transportation applications use GPS for safety-critical operations. Based on the vulnerabilities of GPS and its role in life-safety applications, it is prudent for decisionmakers to fully understand the risks to society associated with this navigation system [Mahoney and Haimes 2001].

The vulnerability of satellites to a high-altitude nuclear detonation and the resulting electromagnetic pulse has been widely documented. For example, a report by the Defense Threat Reduction Agency [DTRA 2001] states:

LEO [low earth orbit] satellites will be of growing importance to government, commercial, and military users in coming years. Proliferation of nuclear weapons and longer-range ballistic missile capabilities is likely to continue. One low-yield (10-12 kt), high-altitude (125-300 km) nuclear explosion could disable—in weeks to months—all LEO satellites not specifically hardened to withstand radiation generated by that explosion.

The report states that a deliberate effort to cause economic damage with a lower likelihood of nuclear radiation fallout can be initiated by a “rogue state facing economic strangulation or imminent military threat; and pose economic threat to the industrial world without causing human casualties or visible damage to economic infrastructure.”

A recent article in *Scientific American* by Dupont [2004] further highlights the risks to the global satellite system from nuclear explosions in orbit. Dupont asserts that:

The launch and detonation of a nuclear-tipped missile in low orbit could disrupt the critical system of commercial and civil satellites for years, potentially paralyzing the global high-tech economy. More nations (and maybe non-state entities) will gain this capability as nuclear-weapon and ballistic-missile technology spread around the world. The possibility of an attack is relatively remote, but the consequences are too severe to be ignored.

A study conducted for the Commission to Assess the Threat to the United States from High-Altitude Electromagnetic Pulse Attack [Haimes et al. 2004a, 2004b] highlights the risks to interdependent infrastructures and to the US economy due to such attacks, and reiterates that the benefits of automation have brought an increased vulnerability. Finally, according to Dupont [2004]:

The Pentagon has been working for decades to safeguard its orbital assets against the effects of nuclear explosions...Hardening satellites is costly however. Greater protection means more expense and more massive protective materials. And heavier satellites cost significantly more to launch...Despite the risks to civil orbiters, however, the Defense Department has failed to persuade US satellite builders to harden their spacecraft voluntarily.

To sum up, the further advancement of information technology will depend on wireless, cellular, satellite, and fiber optic technology. And the effectiveness and security of GPS and satellites will depend to a large extent on IT.

C.2. Risk Assessment and Management of the GPS-Based SCADA System for Railways

Competitiveness and economic viability have forced the consolidation of the railway industry. Railroads are controlled through Computer Aided Dispatch (CAD), also known as Signaling and Train Control—a system comparable to a SCADA system [Giras 2004, Solomon 2003]. By its nature and design, a SCADA system is critically unsafe for the railroad, i.e., it is penetrable. (Although the term SCADA has been used throughout this paper to connote a remote computerized control, the term CAD will be used in this section and whenever the control of railroads is addressed.) The regional and centralized dispatching of a large number of passenger and freight trains has become highly dependent on CAD systems.

Major companies are advancing the state of technology in terms of efficiency and operational reliability, but only a minority is adding protection against intruders and would-be terrorists. The following five features of the Hitachi SCADA system [Hitachi-Rail.com 2003] represent the capabilities of these systems and provide a sample of the extent to which SCADA systems have become an integral part of the railway system. (Note that Hitachi uses the term SCADA and not CAD in its publication.) This SCADA system:

1. monitors the operating status of substation equipment. This ensures that control staff is immediately informed of changes or faults occurring in equipment.
2. can switch power supply equipment at each substation on or off individually via CRT monitors at the discretion of control staff.

3. allows automatic control of the equipment power supply corresponding to the train operating schedule.
4. allows automatic control of scheduled equipment power supply.
5. provides training functions for emergency operation procedures by simulating power-supply system abnormalities, such as equipment failures.

These features are promising for efficient and reliable operation of the equipment, but not for securing information assurance to the railway system. In other words, they fall short in terms of assessing and managing the cyber risks from terrorist attacks on the CAD systems, and thus on the infrastructures that they control. On the other hand, the Siemens CAD system [Siemens 2003] does have some security features that include automatic log-off after a predetermined time, locking a password after multiple incorrect attempts, and history of use and password expiration.

Railroads and trains are controlled in three major ways. The first two are the most commonly practiced today, and the third is primarily under development:

1. Direct traffic control, based on radio voice control by the railroad engineer, dispatcher, and roadway worker.
2. Centralized traffic control, based on signaling. Train crews have to observe the signals to control traffic.
3. Positive train control system, based on GPS. This system is the most vulnerable to cyber terrorism [Giras 2004] and is the focus of the risk management example demonstrated in Section F.

Except in direct traffic control, the CAD sends signals to wayside interlocking controllers (WIC) that are scattered in the hundreds along thousands of railroad miles. Therefore, maliciously intruding into the CAD system can affect not only efficient operation, but also the safety of the trains and their occupants. Although the GPS has some jamming capabilities, its reliability and availability can be impaired by injecting false positions through the CAD system or by “spooking” it. In addition, because the well-controlled WIC system is not used in the GPS control system, the possibility of a train collision due to human error and the risks of malicious terrorist attacks are much greater with GPS.

Today, large-scale CAD systems are stitched together from components and subsystems drawn from many vendors. They are increasingly constructed from COTS technology, and the products of any one vendor (equipment or software) must fit into a larger system containing components from many other vendors. Thus, COTS systems introduce critical risks into the CAD systems. In the old railroad design, the fault space in every component of the printed circuit boards was known. The WIC coverage prevents failures in the CAD system—its ability to recover was close to 100% using circuit boards. The heavy reliance on COTS, however, has added a programming black box to the control of critical systems, without providing the ability to know what is inside the process. In other words, controlling the states of the system, in this case controlling signaling and dispatching in the railroad system, is performed without complete knowledge of the detailed configuration of the controlling mechanism (software). Thus, the prevalent use of COTS has moved the operating system from a mostly deterministic to an event-driven stochastic system—an untenable situation when controlling a safety-critical infrastructure.

Furthermore, the use of wireless technology for SCADA systems is increasing rapidly. Although dedicated code systems are the most reliable and most secure, they are also the most costly to design, implement, and maintain. As the competition grows (both among developers and users of systems) the need to develop less expensive SCADA systems is imperative.

Identifying all important sources of risk associated with information technologies is a daunting task that is beyond the scope of this paper. Hierarchical holographic modeling (HHM), a systemic and well-tested risk identification methodology, is introduced in the next section, focusing for demonstration purposes on SCADA systems.

D. ASSESSMENT OF RISKS TO THE RAILWAY SCADA SYSTEMS THROUGH HIERARCHICAL HOLOGRAPHIC MODELING (HHM)

Risk assessment and management is a process that builds on two sets of triplet questions. In risk assessment, the analyst often attempts to answer the following set [Kaplan and Garrick 1981]:

- What can go wrong?
- What is the likelihood that it would go wrong?
- What are the consequences?

Answers to these questions help risk analysts to identify, measure, quantify, and evaluate risks and their consequences and impacts. Risk management builds on the risk assessment process by seeking answers to a second set of three questions [Haimes 1991, 1998, 2004]:

- What can be done and what options are available?
- What are the associated trade-offs in terms of all costs, benefits, and risks?
- What are the impacts of current management decisions on future options?

Note that the last question is a most critical one for any managerial decisionmaking. This is so because unless the negative and positive impacts of current decisions on future options are assessed and evaluated (to the extent possible), these policy decisions cannot be deemed “optimal” in any sense of the word. Indeed, the assessment and management of risk is essentially a synthesis and amalgamation of the empirical and normative, the quantitative and qualitative, and the objective and subjective effort.

Hierarchical holographic modeling (HHM) [Haimes 1981, 1998] is a methodology which can identify all conceivable sources of risk to SCADA systems and to the utilities and infrastructures that use them.

D.1. Hierarchical Holographic Modeling (HHM): An Overview

The fundamental attribute of SCADA systems is its inescapably multifarious nature. They:

- Are hierarchical, e.g., with multiple master terminal units (MTU) that streamline and coordinate communications among the various units of the network, and multiple remote terminal units (RTU) that link the remote sensors and electronic devices with the MTU.
- Have a hierarchy of multiple non-commensurable objectives, e.g., minimize overall costs of hardware, software, communications, and labor; and minimize risks of intrusion and failure.
- Are exposed to multiple sources of risk, e.g., telecommunications, systems acquisition, maintenance, operators, users, organization.
- Have a hierarchy of multiple decisionmakers, e.g., owners, customers, users, contractors.
- Have multiple transcending aspects, and elements of risk and uncertainty in such infrastructures as electric power, telecommunications, water, oil and gas, transportation.

Thus, it is impracticable to represent within a single model all the aspects of a truly large-scale SCADA system. Hierarchical holographic modeling (HHM) [Haimes, 1981, 2004], which forms the basis for risk assessment and management, reflects a difference in kind from previous modeling schemas. The name is suggested by holography—the technique of lensless photography. The difference between holography and conventional photography, which captures only two-dimensional planar representations of scenes, is analogous to the difference between conventional mathematical modeling techniques (yielding what might be termed “planar” models) and the HHM schema. We define hierarchical holographic modeling as “a holistic philosophy/methodology aimed at capturing and representing the essence of the inherent diverse characteristics and attributes of a system—its multiple aspects, perspectives, facets, views, dimensions, and hierarchies” [Haimes 1981, 2004].

In 2003, the President’s Commission on Critical Infrastructure Protection, and the Office of Energy Assurance, US Department of Energy [DOE 2003] issued a pamphlet identifying 21 steps to improve the cyber security of SCADA networks. Although these steps are quite comprehensive, they do not provide holistic answers to the fundamental question posed by Kaplan and Garrick [1981]: “What can go wrong?” On the other hand, HHM [Haimes 1981, 1998, 2004; Kaplan et al. 2001] will provide the answers to “What can go wrong?” and thus supplement and complement the 21 steps. The Department of Energy pamphlet offers better coverage in terms of risk management. For example, to minimize the risk of back-door attacks into the SCADA system, it advises: “[D]isable inbound access and replace it with some type of callback system.” SCADA networks can be hardened by removing or disabling unnecessary services from them, such as these examples: “automated meter reading/remote billing systems, email services, and Internet access” [DOE 2003].

The term *holographic* refers to a multi-view image of a system for identifying vulnerabilities. Views of risk can include, but are not limited to: 1) software, 2) hardware, 3) economic, 4) health, 5) technical, 6) political, and 7) social. Risks also can be related to geography, time, and other factors.

The term *hierarchical* in HHM refers to learning what can go wrong at the myriad levels of the system hierarchy—structurally or organizationally. In order to be complete, HHM recognizes that the macroscopic risks that are present at the upper management level of an organization are very different from the microscopic risks observed at lower levels. In a particular situation, a microscopic risk can become a critical factor in making things go wrong. In order

to carry out a complete HHM analysis, the assessment team must include people with a broad array of experience and knowledge along the entire hierarchy. Furthermore, most physical infrastructures controlled by SCADA systems are complex and hierarchical in terms of their hardware, software, and human interaction; thus, capturing their hierarchical nature is imperative for a sound risk assessment and management process.

HHM has been extremely useful in modeling large-scale, complex, and hierarchical systems, including defense and civilian infrastructure systems. Its multiple visions and perspectives add strength to risk analysis. It has been extensively and successfully deployed to study risks for government agencies such as the President's Commission on Critical Infrastructure Protection (PCCIP), the FBI, NASA, the Virginia Department of Transportation (VDOT), and the National Ground Intelligence Center, among others. The HHM methodology/philosophy is grounded on the premise that in the process of modeling large-scale and complex systems, more than one mathematical or conceptual model is likely to emerge. Each of these models may adopt a specific point of view, yet all may be regarded as acceptable representations of the infrastructure system. Through HHM, multiple models can be developed and coordinated to capture the essences of many dimensions, visions, and perspectives of infrastructure systems. One study was conducted for the PCCIP on the US water supply system. Sixteen different visions/perspectives (*Head Topics*) with an additional 94 sub-visions (*Subtopics*) were identified as sources of risk.

Another valuable and critical aspect of HHM is its ability to facilitate the evaluation of subsystem risks and their corresponding contributions to risks in the total system. This makes it the ideal application for SCADA systems and their associated interdependent and interconnected infrastructures [Ezell et al. 2001]. In the planning, design, or operational mode of SCADA systems, the ability to model and quantify the risks contributed by each subsystem markedly facilitates identifying, quantifying, and evaluating risks to the total system of systems. HHM has the ability to model the intricate relationships among the various subsystems and to account for all relevant and important elements of risk and uncertainty. This makes for a more tractable modeling process and results in a more representative and encompassing risk-assessment process.

The first article on HHM [Haimes 1981] was published in the same year as the article defining risk [Kaplan and Garrick 1981]. The diagram in the HHM is useful for analyzing systems with multiple, interacting (perhaps overlapping) subsystems, such as regional transportation or water supply systems. The various columns in the diagram reflect different "perspectives" on the overall system. Hierarchical holographic modeling can be seen as part of the theory of scenario structuring and vice versa [Kaplan et al. 2001].

D.2. Three Sub-HHMs to Characterize SCADA Systems

The vulnerabilities (or weaknesses) of SCADA systems are inherent in their hardware and software composition, architecture and configuration, the human supervision that controls and operates the system, and the environment within which they operate, among others. The inherent multifaceted nature of the vulnerability and threats related to SCADA systems cannot be modeled or quantified by a single state variable or a single metric. Indeed, the vulnerability of SCADA systems and their users is so complex that it can be measured only through multiple composite metrics. Three major sub-hierarchical holographic models (sub-HHMs) are envisioned to represent the multiple perspectives, dimensions, and facets of SCADA systems (see Figure 2):

1. *Hardware and software,*
2. *Human supervision, and*
3. *The environment within which SCADA systems function.*

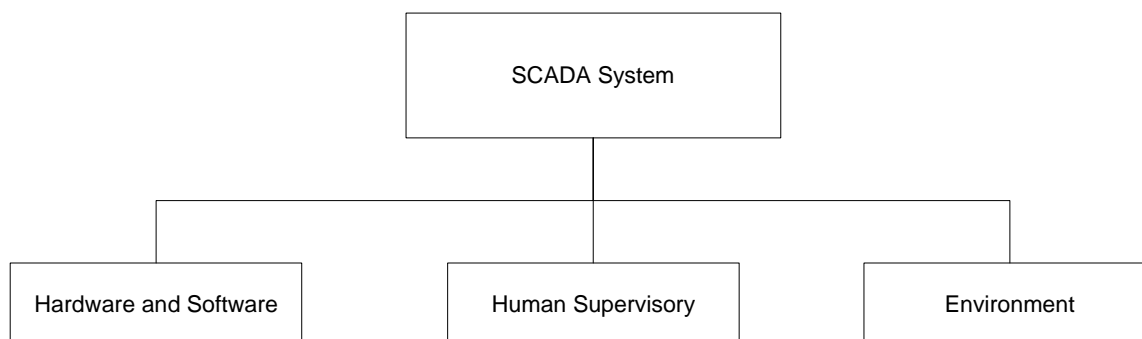


Figure 2. Three Major Sub-HHMs of the SCADA System

D.2.1. Hardware and Software Sub-HHM

The *hardware and software* composition of SCADA systems, which are the focus of this Sub-HHM, are manifested through:

- the *hardware*
- the *software*
- the *system configuration*
- the *telecommunications* through which they are connected
- their diverse *functionality* and the utilities they serve
- their easy *access* by users
- the *tools* they use
- the *utility* of the SCADA system, e.g., electric power, oil and gas, water supply
- the *impact/consequences* resulting from a failure of the SCADA system
- the *acquisition* of the SCADA system
- the *temporal domain* during which they are acquired, designed, manufactured, tested, operated, manufactured, updated, and replaced throughout their lifecycles
- the *model* perspectives used to represent the system
- the *management information systems (MIS)* with which they are controlled
- the *maintenance* of the system
- the *satellites* and the *GPS*

These 15 elements constitute the Head Topics in the *Hardware-Software Sub-HHM*, and are detailed through their corresponding Subtopics as represented in Figures 3.

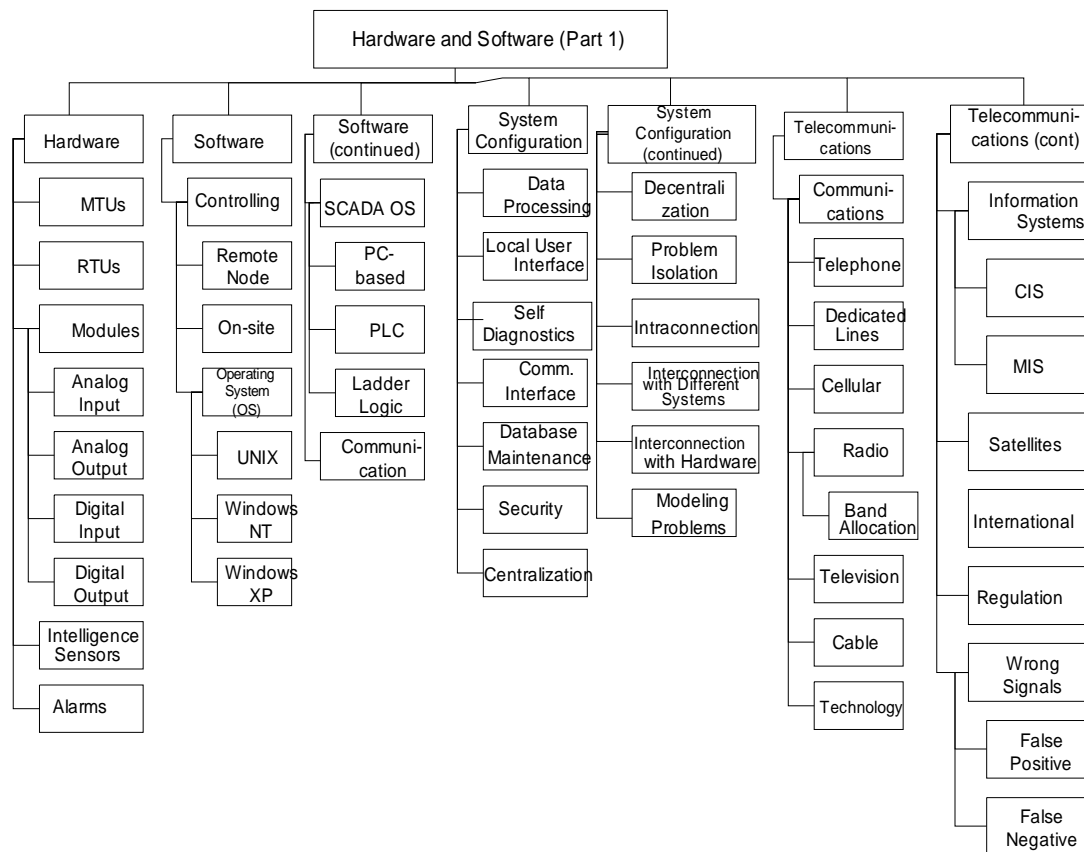


Figure 3. Sub-HHM of SCADA System: Hardware and Software, Part 1

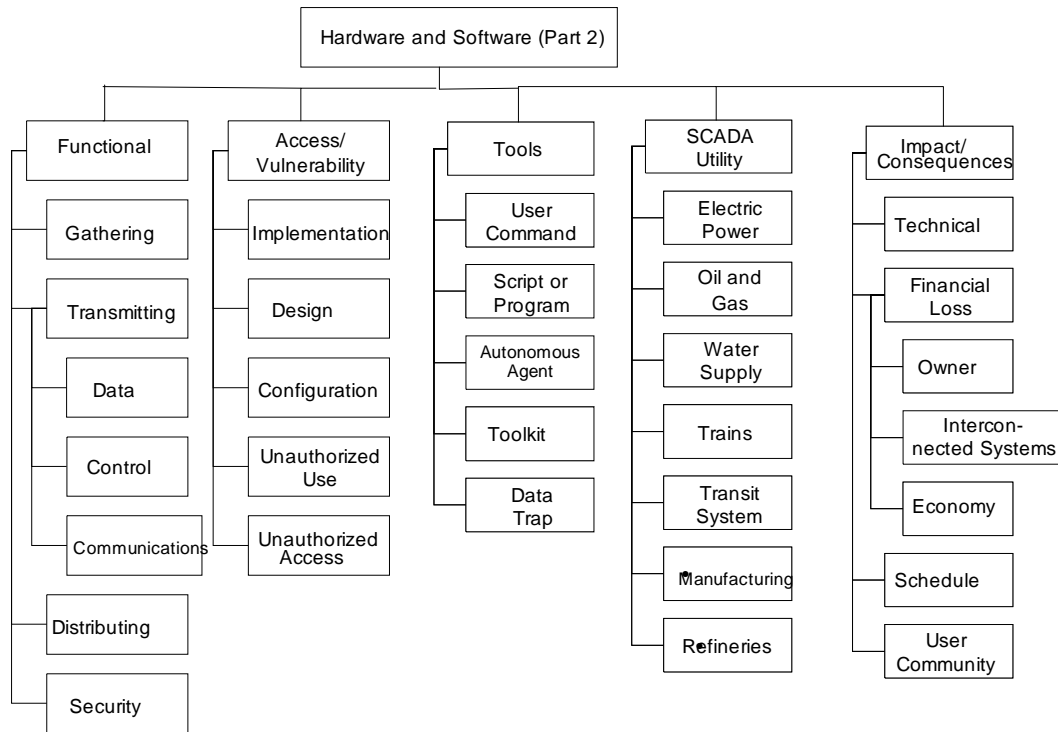


Figure 3. Sub-HHM of SCADA System: Hardware and Software, Part 2

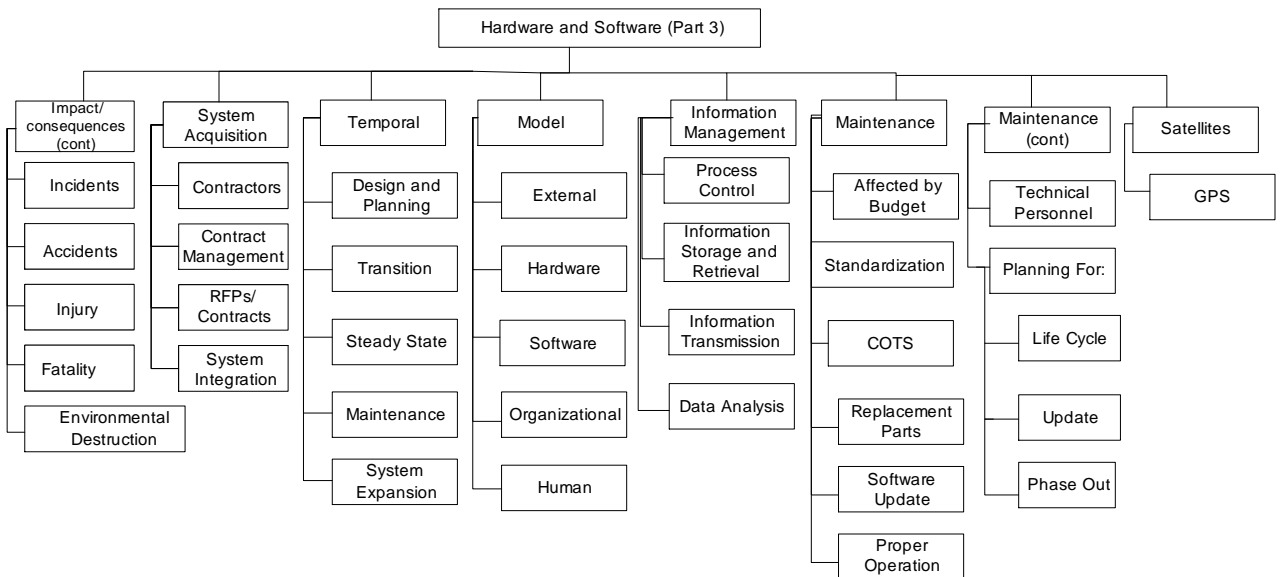


Figure 3. Sub-HHM of SCADA System: Hardware and Software, Part 3

D.2.2. Human Supervision Sub-HHM

As discussed earlier, human supervision and the associated human characteristics and ergonomics are central to the vulnerability and threats to SCADA systems. Six Head Topics are identified in the *Human Supervision Sub-HHM*:

- the *operator* who determines the signals that activate the SCADA system
- the *employees* who provide logistic and other support to the operators and to the organization

- the *interpersonal relationships* among the operators, employees, and management
- the *users and stakeholders* who directly benefit from the SCADA system, and who are also at risk due to vulnerability and threats
- the *maintenance* component of a SCADA system, without which its credibility, functionality, and security cannot be assured
- the *organizational* infrastructure that supports the proper operation of the system.

Each of these is detailed through its corresponding Subtopics as represented in Figure 4.

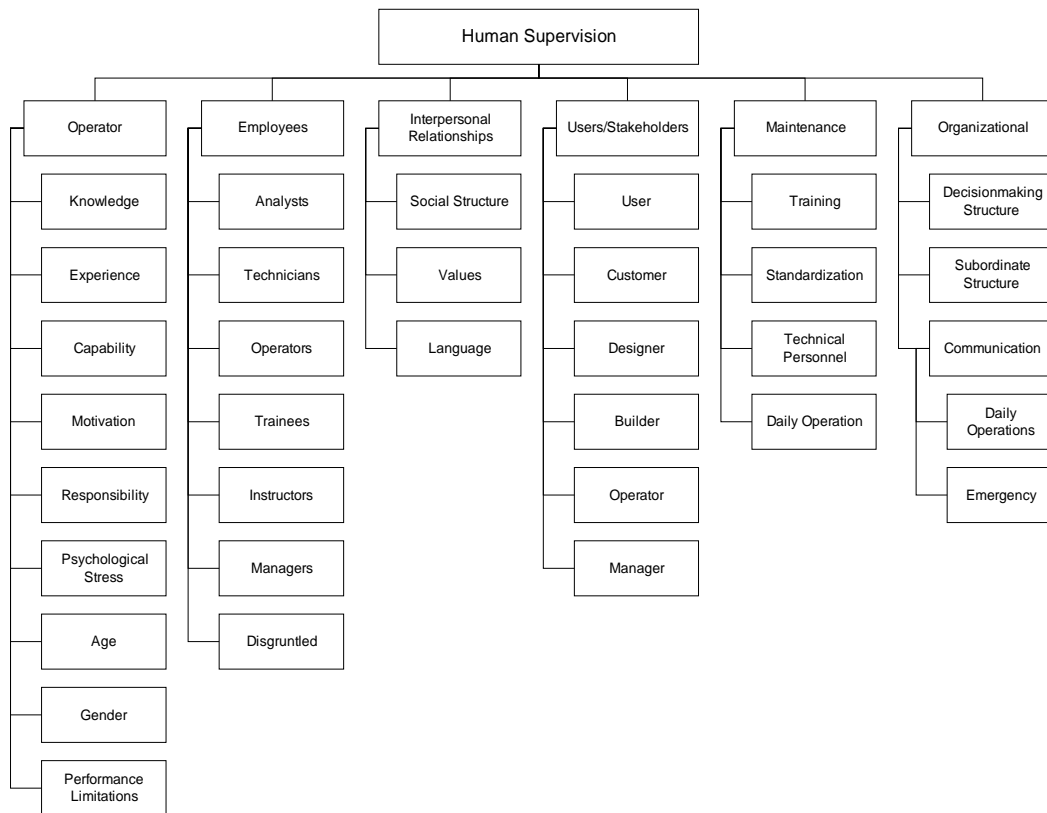
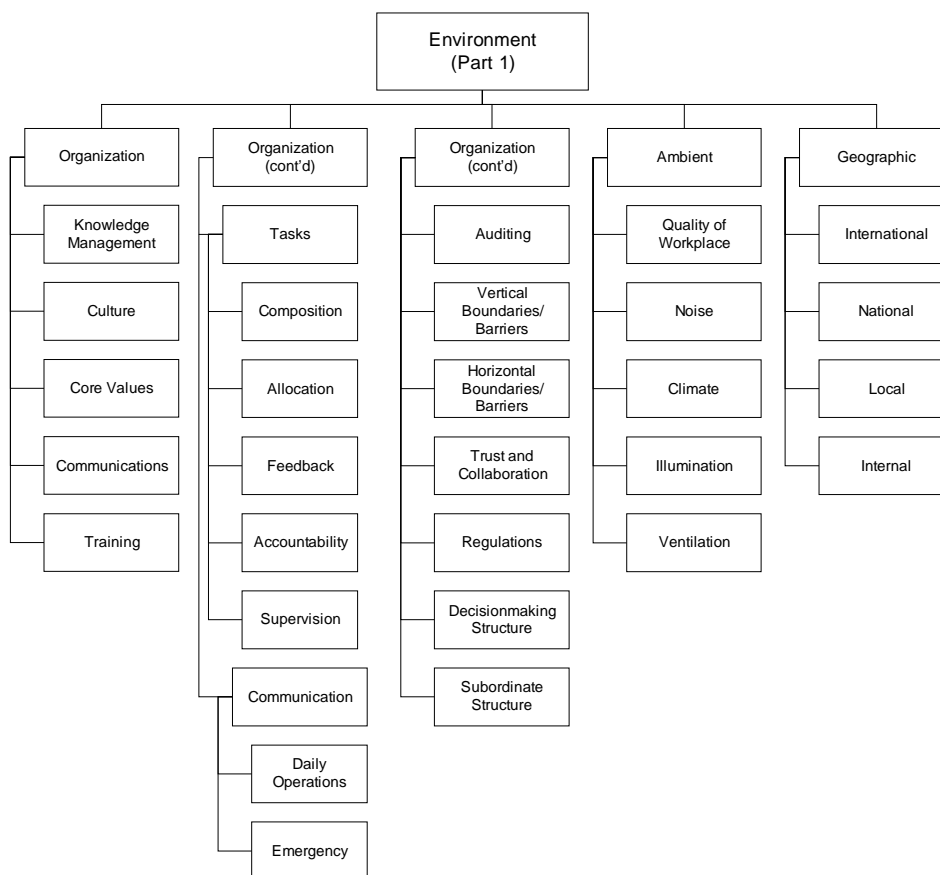


Figure 4. Sub-HHM of SCADA System: Human Supervision**D.2.3. Environment Sub-HHM**

The environments within which the employees, operators, users, customers, and stakeholders deal with each other and within which a SCADA system operates are represented in nine Head Topics in the *Environment Sub-HHM*:

- the *organizational infrastructure* (culture, knowledge management, etc.)
- the *ambience* of the workplace
- the *geographic area* in which the SCADA system operates
- the *types of attackers* that constitute a threat to the SCADA system
- the *nature* of the insurgency
- the *temporal domain* within which the SCADA system operates
- the reliability of the *electric power* that supports the SCADA system
- *finance and economics*

Each of these is detailed through its corresponding Subtopics as represented in Figure 5.

**Figure 5. Sub-HHM of SCADA System: Environment (Part 1)**

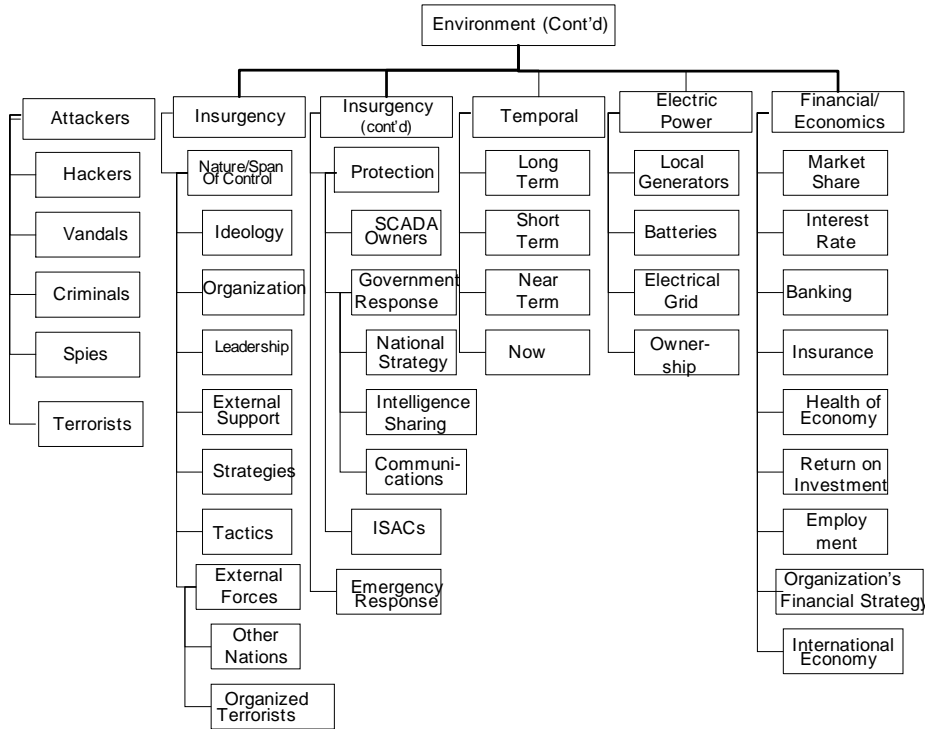


Figure 5. Sub-HHM of SCADA System: Environment (Part 2)
E. CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY [CobiT, 2000]

This paper builds on the principles developed by the Control Objectives for Information and Related Technology (CobiT) [2000] and integrates them with the principles of risk assessment and management [Haines 2004]. Both the CobiT and risk assessment and management principles espouse a holistic philosophy—the former focuses on the overall management of information technology (IT) and the latter on the assessment and management of risks. The objectives of the *Guides for Developing Security Plans for Information Technology Systems* published by the National Institute of Standards and Technology (NIST) [1998] are essentially similar to those of CobiT. Although the NIST framework is not addressed explicitly in this paper, it serves as a complementary asset to the analysis. Although not used in this paper, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), is a framework for identifying and managing information security risks developed at the Carnegie Mellon University’s Software Engineering Institute CERT® Coordination Center. It is a self-directed risk-based activity by a small team of people from the operational (or business) units and the information technology (IT) department working together to address the security needs of the organization [Alberts et al. 2002]. The framework requires the use of standard catalogs of information, which are known to the security community, to form a basis upon which to evaluate an organization. This leads to the identification of information assets and their values, threats to those assets, and infrastructure vulnerabilities exposing the assets to the threats. By analyzing the asset, threat, and vulnerability information in the context of intrusion scenarios, an organization can begin to understand what information is at risk. With this understanding, it can create and implement a protection strategy designed to reduce the overall risk exposure of its information assets.

Table 1. Control Objectives for Information and Related Technology [CobiT 2000]

<p>Domain 1: Planning and Organization PO1 define a strategic IT plan PO2 define the information architecture PO3 determine the technological direction PO4 define the IT organization and</p>	<p>Domain 3: Delivery and Support DS1 define and manage service levels DS2 manage third-party services DS3 manage performance and capacity DS4 ensure continuous service</p>
---	---

relationships	
PO5 manage the IT investment	DS5 ensure systems security
PO6 communicate management aims and direction	DS6 identify and allocate costs
PO7 manage human resources	DS7 educate and train users
PO8 ensure compliance with external requirements	DS8 assist and advise customers
PO9 assess risks	DS9 manage and control configuration
PO10 manage projects	DS10 manage problems and incidents
PO11 manage quality	DS11 manage data
Domain 2: Acquisition and Implementation	DS12 manage facilities
AI1 identify automated solutions	DS13 manage operations
AI2 acquire and maintain application software	Domain 4: Monitoring
AI3 acquire and maintain technology infrastructure	M1 monitor the process
AI4 develop and maintain procedures	M2 assess internal control adequacy
AI5 install and accredit systems	M3 obtain independent assurance
AI6 manage change	M4 provide for independent audit

The CobiT methodological framework provides the information that an organization needs to answer the following set of questions relative to information technology and its management: “How far should we go, and is the cost justified by the benefits? What are the indicators of good performance? What are the critical success factors? What are the risks of not achieving our objectives? What do others do? How do we measure and compare?” The CobiT framework builds around a set of 34 high-level Control Objectives, one for each of the IT processes, grouped into four domains: (1) *Planning and Organization*, (2) *Acquisition and Implementation*, (3) *Delivery and Support*, and (4) *Monitoring*. The CobiT framework is based on holism and the Gestalt philosophy. In many respects, it is comprehensive as to what should be done to effectively manage information technology, and by inference, SCADA systems.

The central focus of CobiT is on the life-cycle management of information assurance through a detailed framework that builds on a set of 34 high-level control objectives, and four domains [CobiT 2000] (see Table 1).

The CobiT mission is to “research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors.” Note that CobiT is effectively a general management framework of information technology that addresses the entire life cycle of product development and its operations. In this sense, it complements and supplements the HHM framework, which focuses on the assessment and management of risks (building on the two sets of triplet questions discussed in Section E.1). In the same spirit as CobiT, Longstaff et al. [2000] maintain that the mission of government and private-sector organizations should be to:

- Apply their educational, technological, management, and policy expertise to the vital task of ensuring the security and survivability of their information infrastructure systems, both present and future.
- Ensure resilient and robust information infrastructures that continuously provide reliable, high-integrity services while protecting the privacy of everyone who uses them.
- Incorporate trust, science, technology, technology-transfer and education, and organizational behavior, not as separate entities, but as one indivisible Gestalt view for information assurance (IA) and survivable dependable systems (SDS).
- Recognize the epistemological difference between IT and IA. Whereas IT is fundamentally a generic technology-based entity which connotes the development and deployment of hardware and software, IA is an integrated technology/people/organization-based entity, with trustworthiness as its hallmark

F. INTEGRATING THE CobiT FRAMEWORK AND HHM WITHIN THE RISK MANAGEMENT PROCESS

We continue to focus on SCADA systems as a representative on information technology. To summarize the preceding discussion:

1. SCADA systems epitomize the essence of IT.
2. SCADA systems are vulnerable to intrusion and attacks by would-be terrorists.
3. There is an urgent need for a systemic risk-based methodology that would add protection to SCADA systems, given their central role in controlling and operating critical interdependent infrastructure systems.
4. CobiT is a holistic and encompassing IT management framework.
5. HHM is a holistic and encompassing framework for identifying most, if not all, sources of risk (in the risk assessment process), and all conceivable risk management options (in the risk management process).
6. When the two sets of triplet questions (Section D), which constitute an essential roadmap for the risk assessment and management process, are supported by quantitative risk analysis methodologies, they will provide the needed tools for managing the risks to SCADA systems.

Integrating the CobiT framework into the HHM provides synergy in risk identification. Clearly, not all entries in Figures 3 – 5 and Table 1 will be relevant either to all SCADA systems or to any single one. Although a first-cut inspection would reduce this very large number of potential risk-management concerns, a more systemic process is preferable, such as the risk filtering, ranking, and management (RFRM) method [Haimes et al. 2002, Haimes 2004]. The RFRM is built around eight phases, employing both qualitative and quantitative analyses. To properly perform the filtering and ranking of scenarios, many individuals with complementary expertise must be involved, including managers, engineers, and MIS experts, among others.

Within the risk assessment process, we have seen that numerous sources of risk associated with SCADA-CAD systems can be identified through the integrated HHM-CobiT process. The RFRM method then can be employed to reduce this large number to a manageable one.

Consider a terrorist-based failure, such as the GPS-Satellite Head-Topic in the Hardware/Software Sub-HHM, where the GPS-based SCADA system for the railways is affected. More specifically, a terrorist network collaborating with a rogue state launches a nuclear device that would detonate in orbit over the United States, thus disabling much of the GPS system, and consequently the evolving GPS-based SCADA system that controls the movement and safety of the railway system (among other dire consequences). In such not-unlikely scenario, the use of the intent and capability of the would-be attackers can serve a surrogate to the probability of an attack [Haimes et al. 2004a, b].

Risks to satellites and GPS may become unacceptable if the following conditions exist: (a) if credible intelligence indicates that terrorists have the capability to launch nuclear devices and explode them in orbit, (b) if the intent associated with such capabilities is sufficiently high, and (c) if the consequences from such attacks can be dire and catastrophic. In such a case, the trade-offs between efficiency (e.g., reliance on GPS for the railway system) and reliability, availability, and security may have to be reevaluated along with appropriate risk management strategies.

G. SUMMARY

The risks of terrorism to information technology and to critical interdependent infrastructures should not be underestimated for the following reasons:

- The economic efficiency gained by the introduction of information technology to our daily lives (e.g., computers, the Internet, wireless and cable-based communications, COTS systems, SCADA systems, satellites, GPS, and myriad uses of IT that span medicine, manufacturing, and transportation, among others, has also introduced numerous sources of risk.
- The availability of the same IT (coupled with the access to weapons of mass destruction) to the would-be terrorists has replaced the Cold War, for which the free world demonstrated resilience and achieved an ultimate victory, to a dangerous asymmetrical war.
- The already tightly interdependent critical infrastructures and major sectors of the economy have become dangerously more dependent on IT, especially on the Internet, GPS, and SCADA and satellite systems. Thus, the already vulnerable critical interdependent infrastructures are becoming even more at risk due to the threat of terrorism to these IT systems.
- The assessment of risks to intrusion and attacks by terrorists to SCADA systems can be achieved through two holistic methodologies—hierarchical holographic modeling (HHM) and control objectives for information and related Technology (CobiT).
- The risk assessment and management methodologies for addressing the above highlighted risks constitute a sample of the plethora of related risk-based methodologies available today.

REFERENCES

- Alberts, C. and A. Dorofee, 2002. *Managing Information Security Risks: The OCTAVE Approach*. Boston, MA: Addison-Wesley Publishing Co.
- Bailey, D. and E. Wright, 2003. *Practical SCADA for Industry*. Amsterdam: Elsevier.
- Boyer, S.A., 1999. *SCADA: Supervisory Control and Data Acquisition, Second Edition*. Research Triangle Park, NC: ISA.
- Bush, G.W., 2003. *The National Strategy to Secure Cyberspace*.
http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
- CobiT (Control Objectives for Information and related Technology), Third Edition, Information Systems Audit and Control Foundation. IT Governance Institute, Rolling Meadows, IL, 2000.
- DOE, 2003. 21 Steps to Improve Cyber Security of SCADA Networks. US Department of Energy, Office of Energy Assurance, Washington, DC. <http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf>, accessed January 29, 2004.
- DTRA (Defense Threat Reduction Agency), April 2001. Briefing, *High-Altitude Nuclear Detonations against Low-Earth Satellites*. Available at www.fas.org/spp/military/program/asat/haleos.pdf
- Dupont, D.G., June 2004. "Nuclear explosions in orbit." *Scientific American*, **290**(6): 100-107.
- Ezell, B.C., Y.Y. Haimes, and J.H. Lambert, 2001. "Risks of cyber attack to water utility supervisory control and data acquisition systems." *Military Operations Research*, **6**(2): 23-33.
- Giras, T., 2004. Research professor, Department of Computer Science, University of Virginia. Personal communication.
- Gnedenko, B. V., 1963, *The Theory of Probability*, translated from the Russian by B.D. Seckler, Chelsea Publishing, New York.
- Haimes, Y.Y., 1981. Hierarchical holographic modeling. *IEEE Transactions on Systems, Man, and Cybernetics*, **11**(9): 606-617.
- — 1991. Total risk management. *Risk Analysis*, **11**(2): 169-171.
- — 1998. *Risk Modeling, Assessment, and Management, First Edition*. New York: John Wiley & Sons.
- — 2004. *Risk Modeling, Assessment, and Management, Second Edition*. New York: John Wiley & Sons.
- — and P. Jiang, 2001. Leontief-based model of risk in complex interconnected infrastructures. *Journal of Infrastructure Systems*, **7**(1): 1-12.
- — and B.M. Horowitz (2004). "Adaptive two-player hierarchical holographic modeling game for counterterrorism intelligence analysis." *Journal of Homeland Security and Emergency Management*, **1**(3), Article 302.
<http://www.bepress.com/jhsem/vol1/iss3/302>
- — S. Kaplan, and J.H. Lambert, 2002. Risk filtering, ranking and management framework using hierarchical holographic modeling. *Risk Analysis*, **22**(2): 393-397.
- — B.M. Horowitz, J.H. Lambert, J.R. Santos, C. Lian, and K.G. Crowther. 2004a. Inoperability input-output model (IIM) for interdependent infrastructure sectors: theory and methodology. Submitted for publication to *Journal of Infrastructure Systems*.
- — B.M. Horowitz, J.H. Lambert, J.R. Santos, C. Lian, and K.G. Crowther. 2004b. Inoperability input-output model (IIM) for interdependent infrastructure sectors: case study. Submitted for publication to *Journal of Infrastructure Systems*.
- Helander, M.G., 1997. The human factors profession. In G. Salvendy (Ed.), *Handbook of Human Factors and Ergonomics, Second Edition*, p.6. New York: John Wiley & Sons.
- Hitachi- Rail.com, 2003, accessed December 11, 2003.
http://www.hitachi-rail.com/products/operation_and_management/SCADA/scada.html
- Kaplan, S. and B.J. Garrick, 1981. On the quantitative definition of risk. *Risk Analysis*, **1**(1): 11-27.
- — Y.Y. Haimes, and B.J. Garrick, 2001. "Fitting hierarchical holographic modeling into the theory of scenario structuring and a resulting refinement of the quantitative definition of risk." *Risk Analysis*, **21**(5): 807-815.
- Khodr, H.M., J. Molea, I. Garcia, C. Hidalgo, P.C. Paiva, J.M. Yusta, and A.J. Urdaneta, 2002. "Standard levels of energy losses in primary distribution circuits for SCADA application." *IEEE Transactions on Power Systems*, **17**(3): 615-620.
- Leontief, W.W., 1951. *The Structure of the American Economy 1919-1939, Second Edition*. Fair Lawn, NJ.
- Longstaff, T.A. and Y.Y. Haimes, 2002. A holistic roadmap for survivable infrastructure systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans*, **32**(2): 260-268.
- — C. Chittister, R. Pethia, and Y.Y. Haimes, 2000. Are we forgetting the risks of information technology? *Computer: Innovative Technology for Computer Professionals*, December: 43-51.

- — Y.Y. Haimes, and C. Sledge, 2002. "Are we forgetting the risk of COTS products in wireless communications?" *Risk Analysis*, **22**(1): 1-6.
- Lowrance, W.W., 1976, *Of Acceptable Risk*, William Kaufmann, Los Altos, CA.
- Mahoney, B., 2001. *Quantitative Risk Analysis of GPS as a Critical Infrastructure for Civilian Transportation Applications*, thesis, University of Virginia, Charlottesville, VA.
- — and Y. Haimes, 2001. *Quantitative Risk Analysis of GPS as a Critical Infrastructure for Civilian Transportation Applications*. Society for Risk Analysis Annual Meeting, Session M7 (Infrastructure & Risk), December, Seattle, WA
- NRC, 2002a. *Cyber Security Today and Tomorrow: Pay Now or Pay Later*. National Research Council, The National Academies, Washington, DC.
- — 2002b. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Research Council, Washington, DC.
- NYC, 2004. *Rail Investigations 1980 to 2004*. Collision/Derailment Data: Mainline and Yards, Office of System Safety, New York City Transit Authority, New York, NY.
- PCCIP, 1997. *Critical Foundations: Protecting America's Infrastructures*. President's Commission on Critical Infrastructure Protection, Washington, DC.
- Perrow, C., 1999. *Normal Accidents: Living with High-Risk Technologies*, pp 121-122. Princeton, NJ: Princeton University Press.
- Salvendy, G. (Ed.), 1997. *Handbook of Human Factors and Ergonomics, Second Edition*. New York: John Wiley & Sons.
- Sarter, N.B., D.D. Woods, and C.E. Billings, 1999. Automation surprises. In G. Salvendy (Ed.), *Handbook of Human Factors and Ergonomics, Second Edition*, p.1927. New York: John Wiley & Sons.
- Siemens, 2003. "Proprietary Networks still get the PLC user's vote", *Industrial Automation Insider*, February 2003, <http://www.siemens-industry.co.uk/systems/ai/IA030216.PDF> accessed July 7, 2004
- Solomon, B. 2003. *Railroad Signaling*, MBI Publishing Company, St. Paul, MN.
- Stanton, N.A., M.J. Ashleigh, A.D. Roberts, and F. Xu, 2003. Virtuality in human supervisory control: assessing the effects of psychological and social remoteness. *Econometrics*, **46**(12): 1215-1232.
- US Department of Commerce, Bureau of Economic Analysis, 1997. *Regional Multipliers: A User Handbook for the Regional Input-Output Modeling System (RIMS II)*. Washington DC: US Government Printing Office.
- US Department of Commerce, Bureau of Economic Analysis, 1998. *Benchmark Input-Output Accounts of the United States, 1992*. Washington DC: US Government Printing Office, 1998.