Cybersecurity for Electric Power Control and Automation Systems

Chee-Wooi Ten, *Student Member, IEEE,* Manimaran Govindarasu, *Member, IEEE,* and
Chen-Ching Liu, *Fellow, IEEE*

***Abstract*—Disruption of electric power operations can be catastrophic on the national security and economy. Due to the complexity of widely dispersed assets and the interdependency between computer, communication, and power systems, the requirement to meet security and quality compliance on the operations is a challenging issue. In recent years, NERC's cybersecurity standard was initiated to require utilities compliance on cybersecurity in control systems - NERC CIP 1200. This standard identifies several cyber-related vulnerabilities that exist in control systems and recommends several remedial actions (e.g., best practices). This paper is an overview of the cybersecurity issues for electric power control and automation systems, the control architectures, and the possible methodologies for vulnerability assessment of existing systems.**

I. Introduction

ELECTRIC power systems and automation systems include process control and supervisory control and data acquisition systems (SCADA) that operate safe, reliable, and efficient physical processes for the energy system [1]. These systems are connected via a highly automated network. A variety of communication networks are interconnected to the electric grid for the purpose of sensing, monitoring, and control. Computer and communication devices are widely installed in power plants, substations, energy control centers, company headquarters, regional operating offices, and large load sites. These devices and systems are increasingly networked and complex.

Computer, communication, and power infrastructures are interdependent in a power grid. The measurements and control signals acquired by SCADA are utilized in an energy management system (EMS) of the power grid to perform a wide range of system functions, including real-time control of the power grid. Failure of an important communication channel in the operational environment could result in an inability to control or operate important facilities, leading to possible power outages. Congestion of the communication networks could delay the transfer of power system data or control signals that may be critical in some scenarios [2].

Although the complex infrastructure provides great capabilities for operation, control, business, and analysis, it also increases the security risks including power system cybersecurity (PSC) threats and vulnerability. A cyber attack on the control center computer systems could lead to undesirable switching operations, resulting in widespread power outages. Another cyber attack scenario is to penetrate the substations and alter protective relay settings, which could result in undesirable switching actions. Currently the system may not have strong measures against cyber attacks and, therefore, vulnerabilities exist. Consequently, there is a growing demand to address these cybersecurity issues in a comprehensive and systematic manner.

SCADA protocols have advanced from point-to-point links to newer protocols and communication methods [3]. These newer methods allow for a higher level of redundancy and speed of transmission. An important issue is that the current practice has to be a hybrid of the original 1970s practices and today's standards. The reason for this is the expected life of SCADA devices. Since a device has to operate for 15–20 years, a wide variety of devices based on different technologies could end up in the field. Some may be "smart" devices with a processor onboard and others "dumb" with a hardwired set of tasks. Sometimes a site might be retrofitted and brought up to date, but in most cases that only happens when other maintenance work is required or the device is near the end of its lifetime. An understanding of the integration issues is important when both past and future SCADA protocols are involved.

Due to the technological changes over the last decade, the trend of protocols has been refined to be more flexible and accommodating to industrial needs, specifically in the open architecture with high-speed communications. The interoperability and maintainability of the standard protocols ensure communication security and stability. The interoperability also improves its interactions with other systems. However, these improvements may also lead to PSC vulnerabilities.

Various SCADA attacks through communication channels in the recent past have highlighted the extent to which the SCADA systems are vulnerable and the need to protect them against cyber attacks. Recent findings report the plans to disrupt the U.S. power grid [4]. In addition, the North American Electric Reliability Corporation (NERC) directives make it mandatory to undertake cyber security vulnerability assessment at the operator locations and to take corrective measures [5]. The NERC security document and the

C.-W. Ten is with the Electrical and Computer Engineering Department, Iowa State University, IA 50010, USA (e-mail: cheewooi@iastate.edu).

M. Govindarasu is with the Electrical and Computer Engineering Department, Iowa State University, IA 50010, USA (e-mail: gmani@iastate.edu).

C.-C. Liu is with the Electrical and Computer Engineering Department, Iowa State University, IA 50010, USA (e-mail: liu@iastate.edu).

1-4244-0991-8/07/$25.00/©2007 IEEE

ISO/IEC17799 standard [6] specify guidelines for cyber security in power systems.

The PSC vulnerabilities involve three main components, i.e., the computer, communication, and power systems. Attacks can be remotely targeted at specific systems, subsystems, and multiple locations simultaneously. These components are highly interdependent. Since the communication protocols are encapsulated with transmission control protocol / Internet protocol (TCP/IP), attacks using these facilities to degrade the systems may have catastrophic consequences. There is a threat to equipment design and safety limits that can potentially cause system malfunctions and shutdowns.

II. Evolution of SCADA System

The architecture of SCADA system has evolved through 1960s with the integration of new computing technologies into the grid environment. The evolution of SCADA system involves in three stages: (1) monolithic, (2) distributed, and (3) networked. The involvement of networking using TCP/IP has become prominent due to the economic, common deployment [7].

A. Monolithic

This is the earliest SCADA architecture using mainframe systems with redundancy by installing identical mainframe systems. It is a stand alone system with no connectivity to others. The communication of remote terminal units (RTUs) was implemented using vendor-proprietary protocol and equipment. Hence the limitation of functionality depends on the specific types of equipment and protocols.

B. Distributed

The distributed architecture of the SCADA system distributes the computing burden to a number of machines in a network. Each machine is configured with different functions and roles. The redundancy of each machine can be provided through other machines in the network. Comparing to the earlier systems, the communication protocols between the field and control center are similar. As a matter of fact, the system can still be limited by the vendors supporting the hardware, software, and peripheral devices.

C. Networked

The networked architecture has been widely used due to the nature of open system architecture that facilitates the compatibility to connect three party devices, even though some are still vendor-proprietary. Its major improvement is the open system architecture that utilizes the standardized protocols. This has been shifted from locally redundant systems to wide area networking (WAN) with the use of Internet protocol (IP) for multi-site control centers. This is used for disaster survivability that improves reliability of the facility housing the SCADA master by distributing the processes across physically separate locations.

Communication protocols have been advanced over time from point-to-point links to newer protocols and communication methods [6]. These newer methods have the advantages of greater redundancy and speed of transmission. As mentioned, an important issue is that the current practice has to be a hybrid of the 1970s practice and today's standards. An understanding of the integration issues is important when both past and future SCADA protocols are involved. Table 1 is a summary of the SCADA protocol evolution from 1970s.

Table 1: Evolution of the SCADA Protocols

Years	Protocols
1970s	No standard protocol: Point-to-point, hardwired remote control and tone telemetry
1980s	Proprietary and industrial protocols: Modbus, Modbus plus, and proprietary or vendor specific protocols
1990s	Open protocols: DNP by Westronics (GE); UCA by EPRI for EMS mainly in North America; IEC 60870 by International Electrotechnical Commission (IEC).
2000s	Promoting standard protocols: DNP primarily in North America. UCA merged into the main stream of standard protocols, IEC61850.

Due to the technological changes over the last decade, the trend of protocols has been refined to become more flexible and accommodating to industrial needs, specifically in an open architecture with high speed communications. The interoperability and maintainability of standard protocols ensure communication security.

III. Power System Cybersecurity Vulnerabilities

PSC vulnerabilities involve three main components, i.e., computer, communication, and power system [8-15]. Attacks can be targeted at specific systems, subsystems, and multiple locations simultaneously from remote. These components are highly interdependent. The security level indicates the severity of the damage that might be done if there is a penetration into the power system. At the level of computer systems, security is divided into three sub-categories, i.e., Internet, Intranet, or individual computers. The PSC threats arise from the various attacks discussed here. They represent the different attack types, mechanisms and other potential pitfalls that need to be considered in the design of a secure SCADA network.

1) *Cyber Attackers*: PSC threats to SCADA systems may arise from two sources, namely internal disgruntled employees and external malicious hackers. The threat from internal employees is real but not very likely as it would be easier to identify the attacker in most cases and the fear of the consequences would in itself reduce the likelihood of such attacks. However, it is still necessary to take preventive measures to avoid such occurrences. On the other hand, it is easier for an external hacker to launch cyber attacks and the

attack could go undetected, thereby making the SCADA systems more vulnerable.

2) *Targeted Cyber Attack Types*: Malicious attackers can launch targeted attacks such as sniffing packets at an Internet service provider (ISP) or carrier and then maliciously modifying the packets in the network to achieve the expected results. They could proactively exploit software bugs and other vulnerabilities in various systems, either in the corporate network or the SCADA network, to gain unauthorized access to places such as control center networks, SCADA systems, interconnections, and access links. Openly available vendor documentation for proprietary power systems control software also makes them vulnerable to software exploits. They could configure unauthorized access points to send false information to confuse the SCADA systems in order to trigger unwanted countermeasures. They could target RTUs, intelligent electronic devices (IEDs), uplink connections, and other physical entities to disrupt services. They could exploit the deterministic nature of the inter-center control communications protocol (ICCP) messaging protocol to achieve the desired effects on the SCADA network and the electric grid.

3) *Flood-based Cyber Attack Types*: Cyber-attacks that are based on denial of service (DoS) mechanisms, and others that spread due to viruses and worms by causing a traffic avalanche in short durations, can potentially bring down systems and cause a disruption of services. There is no well-known, fool-proof, defense against such cyber attacks in the computing literature. Various effective ad-hoc solutions have been adopted on traditional computer networks. If the access links that connect the SCADA network to the Internet are swamped by heavy traffic caused by such attacks, it could prove disastrous as the control and supervisory data (including alarms, IED data) flowing to the SCADA network could be lost in the network. The gateway or firewalls installed to monitor the incoming traffic could be overloaded by the large volumes of attack traffic. Thus the ability of the SCADA network to respond to actual failures can be significantly affected. Also, the traffic flood could contain malicious ICCP messages that could confuse the SCADA systems to a great extent.

There are many other avenues through which an attacker can execute a cyber attack in a manner that allows the attack to go undetected. Well-known techniques in computing literature, e.g., source address spoofing, or domain name system (DNS) cache poisoning, could also be tried but the impact of these attacks is currently unknown and needs to be studied in greater detail.

IV. SCADA System Security

This section provides a discussion of the SCADA system security with a broader consideration of existing SCADA standards. Salient features of the security solutions are also discussed.

A. *Escalating Cybersecurity*

The digital revolution has rapidly lowered the cost of computer peripherals. The Internet protocol enables the use of heterogeneous components that reduce the costs in SCADA communication and improve system performance, interoperability, and reliability. Merging of the computing technology using Ethernet, however, has resulted in network security issues for the SCADA systems. With the convenience of Internet and possible cyber-threat exposure, the attack can be executed through TCP/IP. In addition, commonly-used information technology (IT) security solutions may not be sufficient for the power grid environment due to the dependencies between information and power infrastructures. The vulnerabilities in the specific domain of power infrastructures must be considered.

The critical cyber assets in electric power infrastructures include (1) distribution management system (DMS), (2) substation automation system (SAS), (3) power plant process control system (PCS), and (4) control center. The first three are considered at the substation or regional level while the control center framework involves the system level. For maintenance purposes, these assets may be set up with a dial-up network. Wireless networks may be used for local communication. These access points may be used to exploit network vulnerabilities if network security is not tightly implemented and enforced.

B. *CIP 1200 and Other Standards*

NERC has constituted the compliance standard CIP 1200 for a power system to meet the network security requirements. This standard provides general guide lines about what to comply and alert, and training of the personnel. The guidance includes identification of physical and cyber parameters, and critical cyber asset; however, it does not provide system vulnerability assessment based on what is implemented. Some other SCADA security standards are available, e.g., BS7799 by British Standard Institute (BSI), IEC/ISO 17799, ISA TR 99.00.02, AGA12 by American Gas Association, and 21 steps by Department of Energy. Some of these standards provide guidance that include domain specific defense with examples [16].

C. *Salient Features of Security Solution*

One of the ultimate goals is to achieve an attack-proof network. Salient features of the security solution are discussed as follows:

1) Firewalls and IDS: Since the most important threat to the SCADA network may come from malicious attackers via the Internet, it is necessary to monitor the traffic flows from the Internet (IP network) to the SCADA network. It is proposed that firewalls and other Intrusion Detection Systems (IDS) be installed at the various ingress points (gateways) of the SCADA network to identify malicious traffic before it is allowed to enter. Although this would help to filter out some attacks, it may still be an inadequate defense action against attacks. Viruses and worms could swamp the systems with huge volumes of attack traffic. Hence, having only firewalls

and IDS at entry points may not suffice. This leads to the concept of the electronic perimeter.

2) Electronic Perimeter: It is proposed that a wider electronic perimeter be defined where cyber attacks can be filtered and unwanted traffic stopped before it reaches the gateway of the SCADA network [13]. This extended perimeter can be formed by multiple IDS devices across a wide area. Huge volumes of traffic can be handled by an extended perimeter as it would be possible to stop the attacks further away from the SCADA network. In addition, the IDS devices along the electronic perimeter could form an overlay network (i.e., a virtual private network over the Internet) and function in a distributed and collaborative fashion, supporting one another in tackling the attacks more effectively. The setup can be viewed as an electronic fence or protective perimeter-barrier that allows only legitimate traffic to reach the gateway of the SCADA network.

3) Domain-Specific IDS: IDS devices, along the electronic perimeter, can establish a baseline profile of the normal system behavior. In addition, a perspective on an intrusion can be developed by analyzing the emerging characteristics of the data such as patterns, clusters and trade-offs by looking for trends and cycles in the data flow. This would require domain-specific knowledge of the SCADA network and the associated communication devices in order to construct the IDS attack signature database. Identifying these attack scenarios and generating signatures that correspond to these situations is a significant challenge in itself and would need extensive and detailed analysis of the various attacks in the context of interconnected grids. However, once this is achieved, the observed behavior needs to be correlated to detect potential intrusions and filter the attack traffic. The solution of domain-specific IDS overlay network, along an extended secure cyber-perimeter, which functions in a collaborative manner, has the potential to tackle known cyber attacks to date in a fairly effective manner. It would follow the principle, “Stop the attack even before it reaches you.”

4) Secure Communication: The various communication links must be secured by adopting well-known security standards such as virtual private network (VPN) and IP security (IPSec) to provide authentication, data integrity and confidentiality for the data communication between the Internet or corporate network and the SCADA network. Also, DNS Security must be deployed in all DNS servers associated with the electric grid for validating the authentication and the integrity of DNS transactions.

5) Best Security Practices: Security practices such as computer operation and network management policies must be defined according to the NERC guidelines for procedures such as the choice of passwords and their expiry, use of a limited number of privileged computer accounts and disabling the rest, closure of unwanted communication ports and computers, enforcement of access control mechanisms, and frequent update of anti-virus signature databases. It is useful to evaluate the extent to which the corporate and SCADA networks can be logically and physically separated without affecting any functionality, in order to prevent a vulnerability in one network from making the other network also vulnerable.

6) Online Vulnerability Map Tool: It is also useful to develop a vulnerability analysis tool, to test whether the servers, hosts, routers, and devices that are part of the SCADA network are vulnerable to known attacks. This tool performs host/network vulnerability analysis periodically (through port scanning and other mechanisms) and provides a visual map of the vulnerability that alerts the operators/engineers to take appropriate remedial actions. The tool has to be flexible so that new attacks can be added to the repertoire any time. The tool acts as a security management technique, and complements the IDS techniques.

V. Power-Cyber Security Framework

NERC has developed cyber security standards and requirements for power grids to reduce the risk and improve the reliability of the bulk electric systems from any compromise of critical cyber assets of the grids [5]. It is difficult to deploy robust defense barriers against cyber attacks on control center networks, given the wide range of attack mechanisms, the centralized nature of the control, and the potential lack of coordination among various entities. To achieve the goal of a secure control center network and power infrastructure, a comprehensive strategy encompassing the policy, technical, and cost-benefit aspects of the emerging security needs must be developed. Towards this goal, our research focus is on the following tasks:

1. Threat and Vulnerability Assessment: This task is to develop a comprehensive understanding of all possible cyber threats and vulnerabilities to the electric grid and the various means by which the vulnerabilities can be exploited by malicious attackers.
2. Security Framework: This is to design a comprehensive security framework that encompasses the security policy, defense mechanisms and their deployment strategies, and best security practices.
3. Integrated Modeling of Attacks and Their Impacts: This is intended to model cyber attacks on critical cyber assets, using tools such as attack trees or Petri nets, and their impacts on the operational security of the power system. This step requires a deeper understanding of not only cyber security and power system operation, but also the cause-effect relations relating them.
4. Validation of Defense Mechanisms: This is to validate the defense mechanisms both quantitatively and qualitatively by deploying them in a controlled testbed environment and/or in a small-scale SCADA network before deploying them on a wide scale.
5. Cost-Benefit Analysis: This is to perform a detailed cost-benefit analysis and other economic feasibility studies of the proposed security framework and its various components before they are deployed.

Intrusion scenarios are formulated based on the common business practices. Various modeling tools have been proposed for the modeling and analysis of security attacks and defense strategies. In the rest of the paper, our work in modeling security attacks and defenses are discussed.

VI. Security Modeling and Evaluation

In this section, three methodologies of security modeling and evaluations are discussed. Although the metrics provided on each method varies, the common goals of security modeling and evaluations are fundamentally based on identification of attack objectives, and attack steps characterization. The methodologies include (1) *attack trees*, (2) *PENET*, (3) *integrated modeling of cyber and power security*, and (4) *SCADA testbed development and validation*.

A. Attack Trees

This is a methodology to evaluate the cybersecurity vulnerability using attack trees [17]. Attack tree is a multi-level hierarchical structure based on logical AND and OR operators. The top node is the ultimate goal with the grouping of different subgoals. The grouping can be composed with a number of attack leaves that are attributed with logic operators "AND" or "OR." This constitutes different intrusion scenarios. With this characterization, three vulnerability indices are introduced: *system*, *scenario*, and *leaf* vulnerabilities. This is determined from the power system control framework based on existing cybersecurity conditions. To evaluate the vulnerability indices in a systematic manner, the following steps are followed:

1. Identify adversary attack objectives.
2. Identify possible security vulnerability and construct an attack tree.
3. Determine the combination of intrusion scenarios with each cybersecurity condition on each attack leaf.
4. Compute leaf vulnerability with respect to the password enforcement and existing technological implementations, given that the cybersecurity conditions are determined.
5. Scenario vulnerability can be computed according to the combination of corresponding leaf vulnerability indices.
6. Finally, determine the pivotal attack, i.e., system vulnerability based on scenarios' vulnerabilities, and improve system security.

This framework can be extended to security investment analysis.

B. PENET

A new attack modeling framework based on Petri nets [18], called PENET, was developed whose goal is to significantly enhance the modeling capabilities of attack trees. PENET introduces useful concepts such as the dynamic nature of attacks, the reparability of a system, and the existence of reoccurring attacks [19]. Moreover, it attempts to find a balance between ease of use and representation power by providing a set of constructs, parameters, performance metrics, and a time-domain analysis of attacks. Time-domain analysis produces valuable output such as "time to reach the main goal" and the "path taken" by the attacker. This output helps to evaluate system survivability and defense strategies. This framework is implemented as a software tool, called PENET Tool, which lets users draw model diagrams of a given system through intuitive user interface, perform time-domain simulations and carry out security evaluations, and enable interactive ways to improve the survivability of the system.

C. Integrated Modeling of Cyber and Power Security

This is an approach in which it integrates both aspects of information security measures and power system operations that captures the attacks and the resulting consequences. A cyber attack modeled includes opening surrounding breakers in a substation using substation SCADA system that may cause loss of load. Petri net model are used to capture the relationship in two sub nets: *cyber-* and *power-nets.* The c*yber-net* models the attack and security measures in the information system, where the resulting impact in the power system is modeled in the power-net. The power-net formulation is based on the cascading events from power flow solutions where an attacked substation is simulated. Cascading events are simulated when lines are more than 105% overloaded. These overloaded lines are taken out of the system that may cause other lines to be overloaded in the system. The damage includes loss of load followed by the cascading overloads. The sequential cascading events are captured in the power-net where the transitions are "guarded" by the loading level.

The constructions of both nets are done automatically. By integrating both nets as a whole, system vulnerability can be evaluated in accordance with the security measures in the cyber-net and the loading level at the power-net. This integrated model enables analyzing each threat scenario according to the severity of the consequences. The basic model can be extended to capture economic aspects of the power system and carry out mitigation analysis.

D. SCADA Testbed Development and Validation

In order to evaluate the robustness of SCADA systems against electronic intrusions and other malicious activities, a realistic testbed needs to be developed comprising of SCADA devices, network devices, application servers, workstations along with emulators and simulators. This testbed can be used to conduct attack-defense exercises, which not only provides means to assess the security capabilities of the current system, but also to harden the system. Sandia National Laboratories [11] along with Idaho National Lab has setup a National SCADA testbed to create, test, and evaluate security solutions for power infrastructure. Similar effort with a goal of building a testbed platform have been undertaken to emulate the environment of an electric utility and study both attack and defense strategies.

VII. Conclusion

Cyber-power system security is a critically important issue today and for the future. In this context, several research challenges must be addressed, which include vulnerability assessment, security framework, modeling, and validation. This paper presented an overview of the research issues, ongoing research, and future areas of research. Specifically, the future work includes (1) integrated modeling techniques that capture the cause-effect relationship between cyber-physical systems, (2) metrics to quantitatively assess the survivability of the system and to carry out a security investment analysis quantifying the cost benefits, and (3) real-world data and testbed evaluations to validate the models.

Acknowledgment

The authors gratefully acknowledge the contributions of Srdjan Pudar, Mohammad Fraiwan, and the support of Electric Power Research Center (EPRC) at Iowa State University.

References

[1] C. H. Hauser, D. E. Bakken, and A. Bose, "A failure to communicate," *IEEE Power and Energy Magazine*, , Mar./Apr. 2005, pp. 47-55.

[2] Z. Xie, M. Govindarasu, V. Vittal, A. G. Phadke, and V. Centeno, "An information architecture for future power systems and its reliability analysis," *IEEE Trans. on Power Systems*, vol. 17, no.3, Aug. 2002, pp.857-863.

[3] K. P. Schneider, C.-C. Liu, and J.-P. Paul, "Assessment of interactions between power and telecommunications infrastructures," *IEEE Trans. on Power Systems*, vol. 21, no.3, Aug. 2006, pp.1123-1130.

[4] "Critical infrastructure protection report," Critical Infrastructure Protection GAO-05-434, Department of Homeland Security Faces Challenge in Fulfilling Cybersecurity Responsibilities, May 2005. [online]. Available: http://www.gao.gov/new.items/d05434.pdf

[5] "*Urgent action standard 1200 – Cyber security*", NERC directive, 2003.

[6] G. N. Ericsson and A. Torkilseng, "Management of information security for an electric power utility – On security domains and use of ISO/IEC17799 standard," *IEEE Trans. on Power Delivery*, vol. 20, no. 2, Apr. 2005, pp. 683-690.

[7] "Supervisory Control and Data Acquisition (SCADA) Systems," Technical Information Bulletin 04-1, National Communication System, Oct. 2004. [online]. Available: http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf

[8] "Understanding SCADA system security vulnerabilities," Symantec White Paper, 2005.

[9] T. Brown, "Security in SCADA systems: How to handle the growing menace to process automation," *IEE Comp. and Control Eng.*, vol. 16, no. 3, Jun./Jul. 2005, pp.42-47.

[10] "*Control systems cyber security awareness,*" US-CERT, Information Focus Paper, 2005.

[11] "The center for SCADA security," The Center for SCADA Security, Sandia National laboratory. [online]. Available: http://www.sandia.gov/scada/home.htm.

[12] B. Flynn, "*Advances in substation communications*", UTC 2005.

[13] "Cyber security standards," NERC. [online]. Available: http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html, 2006.

[14] M. Berg and J. Stamp, "A reference model for control and automation systems in electric power," Sandia National Laboratories. [online]. Available: http://www.sandia.gov/scada/documents/sand_2005_1000C.pdf

[15] "Direct generator communications – manual," NYISO May 2003

[16] A. Torkilseng and G. Ericsson, "Some guidelines for developing a framework for managing cybersecurity for an electric power utility," ELECTRA Report - JWG D2/B3/C2.01, no. 228, Oct. 2006.

[17] C.-W. Ten, C.-C. Liu, M. Govindarasu, "Vulnerability assessment of cybersecurity for SCADA systems using attack trees," *Proc. of the IEEE PES General Meeting*, Jun. 24-28, 2007.

[18] T. Murata, "Petri nets: Properties, analysis, and applications," *Proc. of the IEEE*, vol. 77, no. 4, Apr. 1989, pp. 541-580.

[19] S. Pudar, M. Govindarasu, C.-C. Liu, "PENET: A pragmatic method for attack modeling and validation," submitted for publication, 2007.