SAND2006-5404C

Virtual Control System Environment: A Modeling and Simulation Tool for Process Control Systems

Erik Lee, John Michalski, Peter Sholander and Brian Van Leeuwen

Sandia National Laboratories
Albuquerque, NM, 87111
{ejlee, jtmicha, peshola,bpvanle}@sandia.gov

The development of tools and techniques for security testing and performance testing of Process Control Systems (PCS) is needed since those systems are vulnerable to the same classes of threats as other networked computer systems. In practice, security testing is difficult to perform on operational PCS because it introduces an unacceptable risk of disruption to the critical systems (e.g., power grids) that they control. In addition, the hardware used in PCS is often expensive, making full-scale mockup systems for live experiments impractical. A more flexible approach to these problems can be provided through test beds that provide the proper mix of real, emulated, and virtual elements to model large, complex systems such as critical infrastructures. This paper describes a "Virtual Control System Environment" that addresses these issues.

I. INTRODUCTION

The Virtual Control System Environment (VCSE) is a modeling and simulation tool for Process Control Systems (PCS) that is being developed to address the following issues in the *Roadmap to Secure Control Systems* [1]:

- Measure and assess security posture for facility providers. The goal is that by 2008, 50% of asset owners and operators can perform self-assessments of their control systems using consistent criteria.
- Develop and integrate protective measures for PCS. The goal is to provide "security test harnesses" for evaluating next generation architectures and individual PCS components by 2014.

The first goal is challenging because insufficient tools and techniques currently exist to measure risk. In addition, the threats are hard to demonstrate and quantify. A VCSE-like tool may help an analyst determine the robustness of a system's security posture by performing analysis on a modeled PCS and its controlled infrastructures. In most cases, an on-line operational system cannot be stressed by introducing attacks or failures to measure the system's resilience. In addition, the cost of building large-scale test beds may be prohibitive for many facility operators. As such, a modeling tool may be a practical and cost-effective solution for answering security-related questions for large complex systems.

With respect to the threat environment, further integration of shared telecommunications technologies into normal business operations has spawned increased levels of interconnectivity among corporate networks, control systems, other asset owners, and the outside world. This expansion of connectivity provides increased potential for cyber attacks, and new security measures are required to prevent potential attacks and mitigate the consequences of successful cyber and physical attacks. As such, the VCSE will support the analysis of cyber security measures and their impacts on system operation. (Note: This interconnection problem is not a current threat for nuclear power plants. However, planned upgrades to their digital control systems must not introduce this problem into those plants' control systems.)

The challenge for the second goal is that security upgrades are often hard to retrofit to legacy systems, may be costly, and may degrade system performance. Security solutions that are devised for legacy systems are constrained by the limitations of existing equipment and configurations. Analyzing the interactions and behavior between emerging security solutions and existing legacy control systems is critical though for identifying the introduction of any vulnerability into a proposed or upgraded control system's security solution.

I.A. Goals and Expected Benefits

A VCSE-like capability could enhance the security test harnesses used to evaluate next-generation control

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

systems by providing a mixture of real, emulated and virtual systems in those test beds. (Note: A "real" test bed uses the actual hardware and software components from a control system or network of interest. An "emulated" test bed runs real software binaries on virtual hardware. A "virtual" test bed simulates the actual hardware and software components. For example, the OPNET simulation tool is widely used to create and simulate large virtual networks.) A VCSE could also allow the combined analysis of system availability, system performance, and cyber security posture for critical infrastructures by using a mix of real, simulated and emulated systems, software and hardware in order to provide tradeoffs between cost, scalability, and accuracy. Each VCSE model or experiment would be populated based on expert opinion, facility operator documentation, vendor documentation, lab studies, and site assessments. The partitioning between real, emulated, and virtual entities in each model/experiment would be based on a particular assessment's goals. While this paper describes its potential application to bulk power generation and distribution, the concept is extensible to coupled infrastructures and manufacturing plants.

II. VCSE REQUIREMENTS AND USE CASE

This section provides a brief overview of several potential "use case" for a VCSE capability. All three use cases are traceable to the high-level requirements proposed in the Roadmap referenced in the previous section.

II.A. Augmented QA System / Security Test Harness

Figure 1 shows how a VCSE capability might be used to augment an existing Quality Assurance (QA) test bed, and also function as a security test harness. The business cases might be to:

- Test new hardware / software or software patches before deployment for PCS compatibility
- Reduce the cost of Quality Assurance (QA) systems by using a mix of real, virtual and emulated systems in the QA process

In this use case, the System Under Test (SUT) can be real hardware or real software binaries running in a Virtual Machine (VM). The need for accurate cyber security and functional compatibility testing is what drives the need for real and emulated systems in this use case. The virtual entities are then used for scalable and cost efficient models for the rest of the overall system.

In the simplified example shown in Figure 1, the cyber security question is whether the SUT uses ill-documented ports that are blocked by the existing or proposed Intrusion Prevention System (IPS). The "consequence of concern" is that blocking those information flows will imperil overall system availability.

II.B. NERC CIP Compliance

The North American Electric Reliability Council's (NERC's) Critical Infrastructure Protocol standard [2] is a voluntary standard whose compliance windows run from 2007 – 2010 [3]. The standard makes the following definitions:

- **Critical Assets:** Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.
- **Cyber Assets:** Programmable electronic devices and communication networks including hardware, software, and data.
- **Critical Cyber Assets:** Cyber Assets essential to the reliable operation of Critical Assets.
- **Electronic Security Perimeter (ESP):** The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.
- **Physical Security Perimeter:** The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.

The NERC CIP standard for ESP mandates that the "Responsible Entity" perform a cyber vulnerability assessment of the electronic access points to the ESPs at least annually. That vulnerability assessment includes, at a minimum, the following:

- R4.1. A document identifying the vulnerability assessment process.
- R4.2. A review to verify that only ports and services required for operations at these access points are enabled.
- R4.3. The discovery of all access points to the Electronic Security Perimeter
- R4.4. A review of controls for default accounts, passwords, and network management community strings.
- R4.5. Documentation of the results of the assessment, the action plan to remediate or

mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

The NERC CIP standard does not mandate the use of a VCSE-like tool during a facility provider's ESP vulnerability assessment. However, a potential use case is as follows:

- The CIP assessment identifies the critical cyber assets.
- Further risk assessment [e.g. 4,5,6] identifies an adversary's most likely attack paths.
- The proper mix of real and emulated nodes is used to provide ongoing assessment of and regression testing of those likely attack paths via the Security Test Harness Use Case discussed in the previous subsection.

II.C. Detailed Facility Analysis

There may also be VCSE use cases related to demonstrating how detailed process models, control system models, control center models, and network models can help the combined analysis of system availability, system performance, and cyber security posture for critical infrastructures as illustrated in Figure 2. It would again use a mix of real, simulated and emulated systems, software, and hardware in order to provide tradeoffs between cost, scalability, and accuracy. Figure 3 shows a simplified example of a power generation facility and its attachment to the bulk power grid.

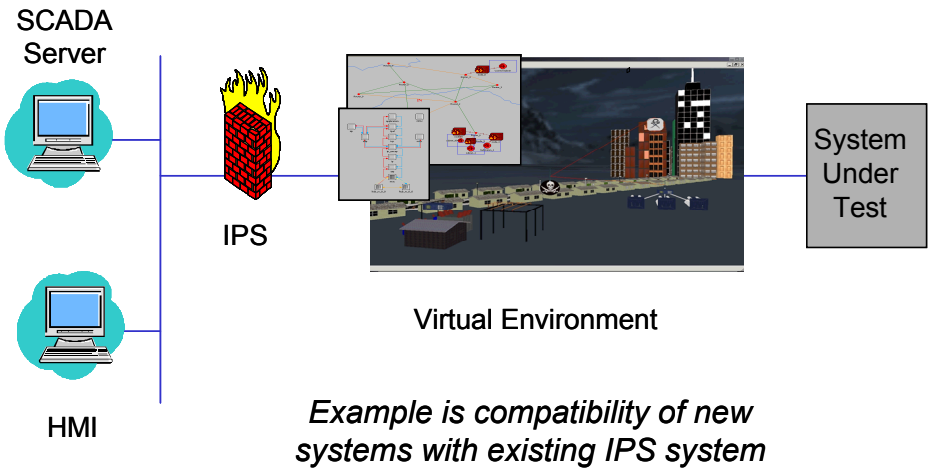

Figure 1. Augmented QA System / Security Test Harness Use Case

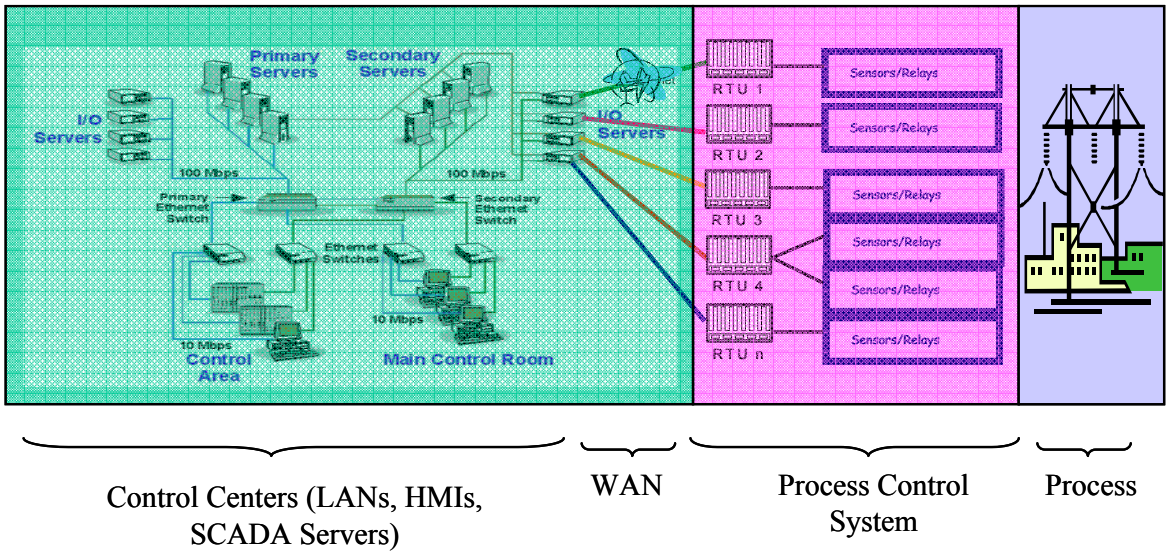

Figure 2. VCSE Application Model

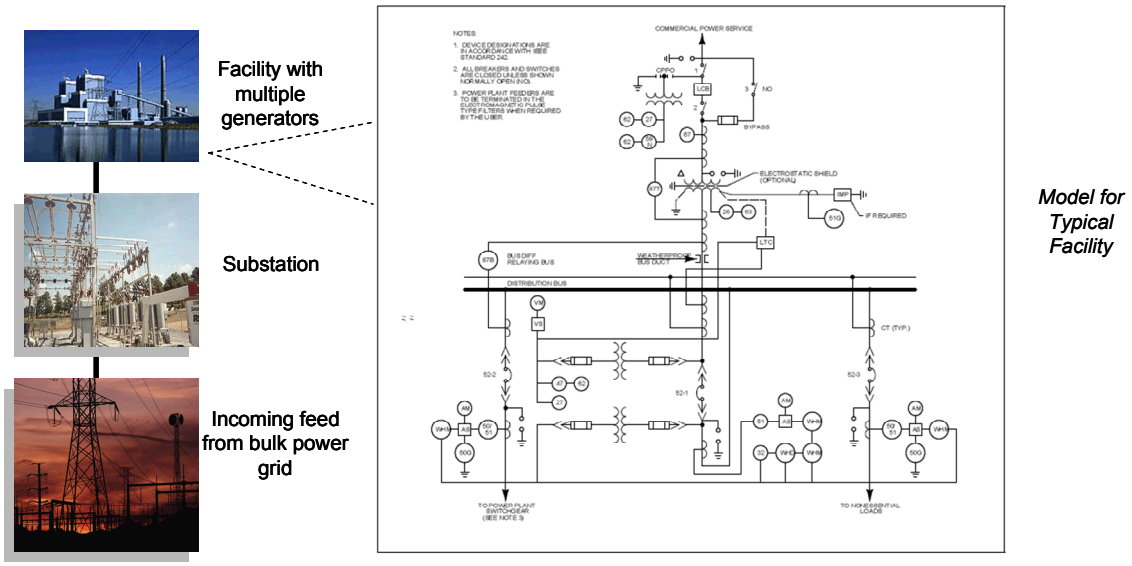

Figure 3. Detailed Facility/Device Analysis Use Case [7]

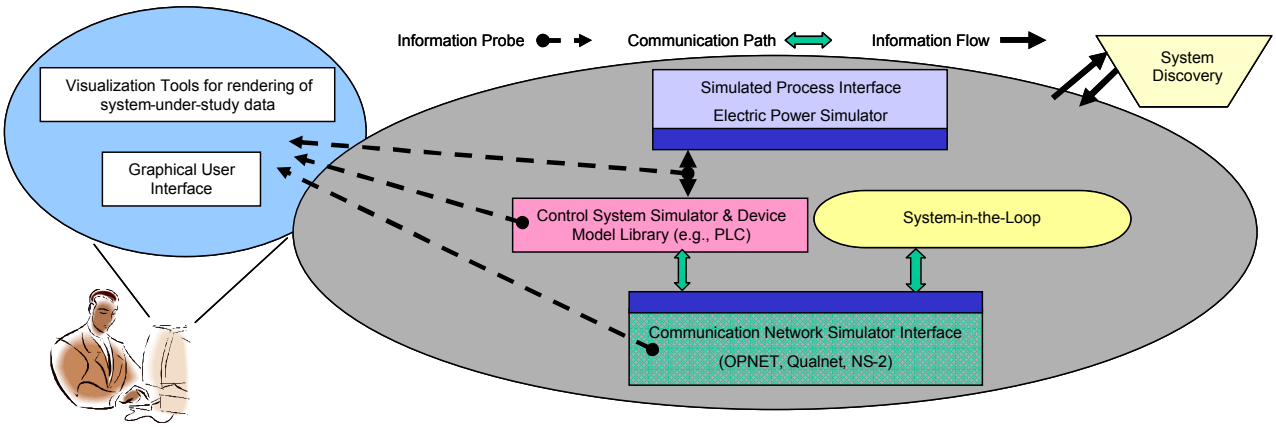

Figure 4: VCSE Architecture

III. VCSE ARCHITECTURE

There is a large body of existing tools for network simulation such as OPNET [8], QualNet [9], and ns2 [10]. Similarly, the PCS community has a rich body of engineering process models and other analysis tools for various infrastructures such as water distribution [11], oil/gas pipelines [12] and power generation/distribution [13,14]. So, the prototype VCSE focuses on:

- The rapid development of new models for control system element.
- Easy federation of real hardware/software with existing simulation, emulation, visualization and analysis tools; and
- Evaluating cyber security postures in large infrastructures.

These combined capabilities are lacking in existing tool sets for designing, developing and assessing PCS.

The high-level architecture of the VCSE Framework is illustrated in Figure 4, while brief descriptions of each module are provided in Table 1.

II.A. Communications Subsystem Modeling

The current VCSE software [15] provides a "proof-of-concept" modeling and simulation (M&S) environment that supports the analysis of PCS via a modular framework methodology. Its end goal is to employ an extensible modular M&S capability that will be federated (e.g., the DoD's High Level Architecture (HLA)) with real and emulated systems. This capability will use a

modular approach that supports interoperation with a network communication simulator and real/emulated network devices to represent the necessary communications network components. The modular approach will support easy integration of future models that will represent specific communication protocols associated with PCS (e.g. DNP3 [16] and MODBUS [17]). These models could be developed in either the selected network M&S tool or in the VCSE Framework. They could also be real software instances running on real/emulated hardware. Finally, they could also be real software binaries that run as "software-in-the-loop" wherein the modular framework is treated as another lightweight operating system port.

Another important feature of the VCSE's modular framework methodology is its "co-simulation" capability that supports the interoperability of multiple simulation tools operating in unison with real and emulated systems. In a co-simulation framework the simulators must also support integration with other simulators and their associated model libraries. At present, an interoperability capability has been demonstrated for the VCSE framework (described in the next subsection) and the OPNET Modeler network simulator. Work on co-simulation with other network simulation tools (e.g, ns2 and QualNet) is underway.

Developments included custom state machine development in OPNET to interface the communication protocol stack models to an application layer that interfaces to PCS devices in the VCSE. In addition, the VCSE interface included developments in process initialization, launching, and interleaving. A process control capability was developed that supports the interoperation of OPNET Modeler with the VCSE Framework. This process control resulted in OPNET Modeler operating as a *slave* to the VCSE Framework software in a master/slave configuration.

III.B. VCSE Simulator Framework

The VCSE modular framework provides a capability to perform analysis with the necessary modules to address the questions that a specific analysis is attempting to answer. In some cases, the analysis may require high-fidelity modeling of the PCS's control system devices, supporting network communications, and supporting security hardware/software. In these cases, the analyst will include a communication network simulator in the environment in order to provide scalability in the size of the test-bed. Real or emulated components could again be included where the highest fidelity (e.g., for detailed vulnerability and security testing) is needed. In the cases where network communications is not critical to the analysis no communication network simulator need be included. In this case, network communication might be assumed to be perfect with no communication delays or dropped messages. Alternately, operating system features (e.g., traffic control and queueing) might be used to model the expected delay and loss of the communications links.

Table 1: VCSE Module Descriptions

VCSE Module	Description
Visualization Tools for rendering of system-under-study data	Visualization tools that render architecture under study to allow visualization of the state of control system and controlled infrastructure, data traffic characteristics, etc.
Graphical User Interface (GUI)	Interface for tool user to build and execute simulation/emulation experiments.
Control System Simulator & Device Model Library	Control system and device model library.
Communication Network Simulator	An API for communication network simulator and protocol model library. Many network simulators include vendor specific model libraries.
System-in-the-Loop	Interface to incorporate actual systems (hardware/software) into VCSE-based experiments. This module supports experiments with both a real ,emulated and virtual parts.
Power System Simulator/Emulator	An API for tools that simulate the state of the physical system being monitored/controlled by the PCS under study.
System Discovery	An interface for tools used to discover the network and PCS under study. Creates a file that can be imported into the VCSE to help configure the real, emulated and virtual entities.

The VCSE modular framework uses an innovative *plug-in* approach that provides the interoperability capability for co-simulations and real/emulated systems. It also provides the means to create pure simulations with

models from supporting simulators and custom models created specifically for the VCSE.

III.C. Visualization tools

The VCSE Framework includes an interface to incorporate various visualization tools. The analyst can select how to represent the data to support answering system questions. Future developments will allow the analyst to place data collection probes and collect data throughout the system modeled with the VCSE. The goal is to use "real" visualization tools (e.g, Human Machine Interfaces for PCS) where fidelity is required or the cost of developing a detailed model is prohibitive. However, additional visualization tools are required for the virtual and emulated entities since those systems may allow additional information to be collected that is not possible with the real systems. A final goal is to have the virtual and emulated systems appear as real systems on the real HMIs.

III.D. Graphical User Interface (GUI)

Initial GUI developments include the necessary GUI parts to support the framework initialization and configuration. The current GUI supports the launching of the VCSE and dynamic loading of modules or plug-ins. More specifically, the GUI interface to dynamically link the VCSE with OPNET Modeler has been developed.

III.E. Control System Simulator & Device Model Library

Current developments of the VCSE Framework include an event simulation/scheduler engine. This simulation engine manages the discrete event execution of the control system simulation and interleaves its events with the external simulator (i.e., OPNET Modeler) if used. In the case of a co-simulation with OPNET Modeler, the VCSE simulation engine manages the execution of events in OPNET Modeler. (Note: the VCSE Team is also exploring co-simulations that use other network simulators such as *ns2*. The goal is to provide the VCSE end-user with a range of options for model fidelity, model complexity and tool cost.)

Current developments also included a number of very basic PCS device models. More specifically, generator functions, voltage sensor function, and limited RTU functions have been modeled. These models were created in a developed model-template that interfaced with the VCSE Framework.

III.F. Hardware-in-the-Loop Capability:

Current development also includes the employment of the OPNET Modeler System-in-the-Loop (SITL) feature to support the VCSE hardware-in-the-loop requirement. This capability merged actual hardware with the virtual environment through an IP interface on the computing platform.

III.G. Power System Simulator/Emulator Interface

Current developments include an interface that can merge a Sandia Labs developed steady-state power grid simulator with the VCSE. This interface module manages the data exchange, both presenting new control system state to the power grid simulator and reporting back the resulting power grid steady-state condition the simulated PCS. Future developments will interface existing commercial power system simulators to the VCSE framework.

The Sandia Labs developed steady-state power grid analysis tool is a steady-state power flow program that uses an iterative technique (Newton-Raphson) to solve for the unknown values in a power system using the known values. With initial known values for a system, a steady-state power flow simulation can provide the corresponding state the power system enters once it has stabilized. As known values change (e.g., load requirements, generator real power output) or as faults occur (e.g., a tree falling on a transmission line) the simulation can be run again to provide the new state of the power system.

III.H. System Discovery

Current developments are limited to investigating methods of creating the system of interest in the virtual environment. Future plans include import the system-of-interest topologies with XML files. Again, a key goal is to have automated discovery tools that can map real PCS and then help configure the VCSE experiments. This configuration includes the correct partitioning of the VCSE experiment's components into the real, emulated and virtual entities based on the analyst's desired tradeoffs between fidelity, cost and scalability.

IV. CONCLUSIONS

This paper described a Virtual Control System Environment (VCSE) whose programmatic goal is to provide the ability to analyze impacts of system vulnerabilities, estimate failure consequences, and assess performance impacts of alternative security solutions without risking disruption to critical operations. Its intended programmatic goal is to support an analyst in identifying operational impacts from cyber security deficiencies while not disrupting operational systems. It is also intended to help identify the cascading effects from a cyber attack, and in particular which threats and vulnerabilities pose the greatest economic risk. The goal is that the analyses can be configured in various types of

topologies (single device to full-scale) as well as in "hybrid" (hardware-in-the-loop) environments that provide control system vendors and infrastructure providers with the ability to test products prior to field installation.

V. REFERENCES

[1] U.S. Department of Energy, U.S. Department of Homeland Security, "Roadmap to Secure Control Systems in the Energy Sector," January, 2006. (http://www.controlsystemsroadmap.net)

[2] NERC Cyber Security Standards CIP-002-1 Through CIP-002-9, May 2, 2006, (http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html)

[3] NERC (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1, February 3, 2006.

[4] Amenaza Technologies, SecurITree software, http://www.amenaza.com/

[5] R. P. Lippmann and K. W. Ingols, "An Annotated Review of Past Papers on Attack Graphs", Technical Report ESC-TR-2005-054, MIT Lincoln Laboratory, Lexington, MA, 2005.

[6] J. Darby, J. Phelan, P. Sholander, B. Smith, A. Walter and G. Wyss, "Evidence-Based Techniques for Evaluating Cyber Protection Systems for Critical Infrastructures", IEEE MILCOM 2006, October 2006.

[7] Reference where this figure came from.

[8] OPNET Technologies, www.opnet.com

[9] Scalable Network Technologies, www.scalable-networks.com/

[10] The Network Simulator – ns2, http://www.isi.edu/nsnam/ns/

[11] U.S. Environmental Protection Agency -- Water Supply and Water Resources, EPANET 2.0, http://www.epa.gov/nrmrl/wswrd/epanet.html

[12] Stoner Pipeline Simulator, http://www.advantica.biz/Default.aspx?page=322

[13] Power System Simulator for Engineering (PSS/E) http://www.pti-us.com/pti/software/psse/index.cfm

[14] PowerWorld, http://www.powerworld.com

[15] E. J. Lee, J. M. Michalski and B.P. Van Leeuwen, "National SCADA Test Bed: FY05 Progress Control System Environment (VCSE)", SAND 2006-4083, July 2006, Unlimited Release.

[16] "A DNP3 Protocol Primer", DNP3 Users Group, March 20, 2005, http://www.dnp.org/

[17] "MODBUS Messaging ON TCP/IP Implementation Guide", Modbus-IDA, May 08, 2002, www.modbus.org