Supervisory Control And Data Acquisition Security Experience

R. Lessard, R. Goodrich, J. Beneat, S. Fitzhugh

Norwich University

Abstract

Supervisory Control And Data Acquisition (SCADA) systems are deployed in power and communication utility, transportation, and financial infrastructures. These infrastructures are potential targets of cyber-terrorism and protecting critical infrastructures against terrorist attacks is a national and international priority. Norwich University's first year "Professional Projects" course sequence is designed to give computer and electrical engineering students their an awareness of the impact of technology on society. This is also their first experience with National Instruments' LabVIEW in an instrumentation and control application, and the SCADA system application illustrates the concepts of network-based computer systems. Students develop a SCADA system representative of a municipal water system using LabVIEW software and experiment with a simulated cyber attack. RoboLab-based programs for autonomous Lego Mindstorm robots to compete in intramural versions of the Trinity College Home Fire Fighting and RoboCup Jr competitions are used introduce LabVIEW programming techniques and the instrumentation and control issues they later apply to the SCADA problem solution. This experience also gives them a first understanding of an Artificial Intelligence_(AI) application. AI is beginning to find application in protecting SCADA systems against a cyber-based attack. The students complete a series of step-by-step instructions based on LabVIEW SCADA templates and laboratory documentation that were developed during the summer of 2003 under an NSA Grant. An attack simulation, limited to spoofing a rogue Master Terminal Unit (MTU) within the SCADA system, is conducted on the wired network. Development of an isolated wireless network used to further demonstrate denial of service, information tampering, and operating system (buffer overflow) attacks is discussed.

I. Introduction

A Supervisory Control And Data Acquisition_(SCADA) system is introduced for municipal water distribution system. Using commercial and affordable software, students develop a simple simulated version of a single pump/tank system that works over the network. A few vulnerabilities are discussed, and a simple demonstration is illustrated. The part that distributed artificial intelligence might play in protecting SCADA systems against cyber attack is also discussed. Robotic competitions earlier in the student experience were used to help the students understand the concepts of artificial intelligence.

Our society needs responsible and knowledgeable citizens. It is important for engineers to understand the impact of technology on society. The electrical and computer curricula at Norwich University hold that principle as an educational outcome. Norwich University also has been designated as a Center Of Excellence for Information Assurance. As such, the electrical and computer engineering department has been given grant money to support professors and students by the National Security Administration_(NSA) to develop materials to teach the engineering principles for developing cyber-attack-resistant critical infrastructure systems. Communications, transportation, finance, and utility distribution such as power and water are examples of critical infrastructure systems that are potential terrorists targets. One scenario postulated is that terrorists might detonate a dirty bomb in a large city and then disable power and emergency systems to hamper recovery efforts. Besides the immediate terror effect, a longer lasting perception of insecurity would ensue where Americans would feel that the core infrastructures of our modern society would be vulnerable for future attacks.

Currently, understanding the impact of technology on society is most explicitly taught in the introductory freshman year and the senior year courses. This paper addresses the introductory freshman experience called. The senior student experience will be discussed in a later paper. Robotics is used in the freshman course to introduce concepts of instrumentation and control, and artificial intelligence, as well as, the use of prototyping tools for hardware and software development. This is accomplished through the use of class competitions using an intramural version of the Trinity College Home Fire Fighting Robot as one model and RoboCup as another. The fire fighting robot competition is an autonomous robot competition where the robot searches a maze for the flame, extinguishes the flame and returns to the starting point. RoboCup pits two single robots or two teams in an autonomous robot soccer playing competition. The introductory engineering course sequence EG115 Professional Projects I and EG116 Professional Projects II meet once a week for the purpose of giving the students their first introduction to applications in computer and electrical engineering in a team oriented design experience.

We first introduced the SCADA system during the spring 2003 EG116 “Professional Projects” course. The laboratory exercise was revised during the summer and again tested during the fall senior level EE411 Microcomputer Applications course. In our first attempt at teaching the principles of designing SCADA system protection, too much time was spent on discussing the specifics of different types of SCADA system vulnerabilities. While the vulnerabilities need to be characterized, understanding the operating principles designed into the SCADA system command, communication, and control is the most appropriate thing we can do for engineering students.

II. Professional Projects

The EG115 and EG116 Professional Projects course sequence at Norwich University is designed to introduce freshmen engineering students early in their academic career to applications within their discipline. This provides the freshmen with a perspective on the reason for the mathematics, science, and engineering science courses that serve as the foundation of their knowledge. Since electrical and computer engineers take this course in common, applications in both disciplines are covered. Robotics is one application area that naturally draws significantly from both disciplines. They are introduced to robotics using the Lego Mindstorms[1] product that

is used as a rapid prototyping kit. Most students have experience earlier in their life with Legos. No additional learning is needed. MLCAD[2] is available as an intuitive drag and drop tool for producing engineering drawings. The robot programming software used is RoboLab. RoboLab[3] is a more powerful programming tool than that supplied with the Mindstorms kit. As illustrated in Figure 1, the students drag and drop program icons on the screen and connect them using a "wiring" tool.

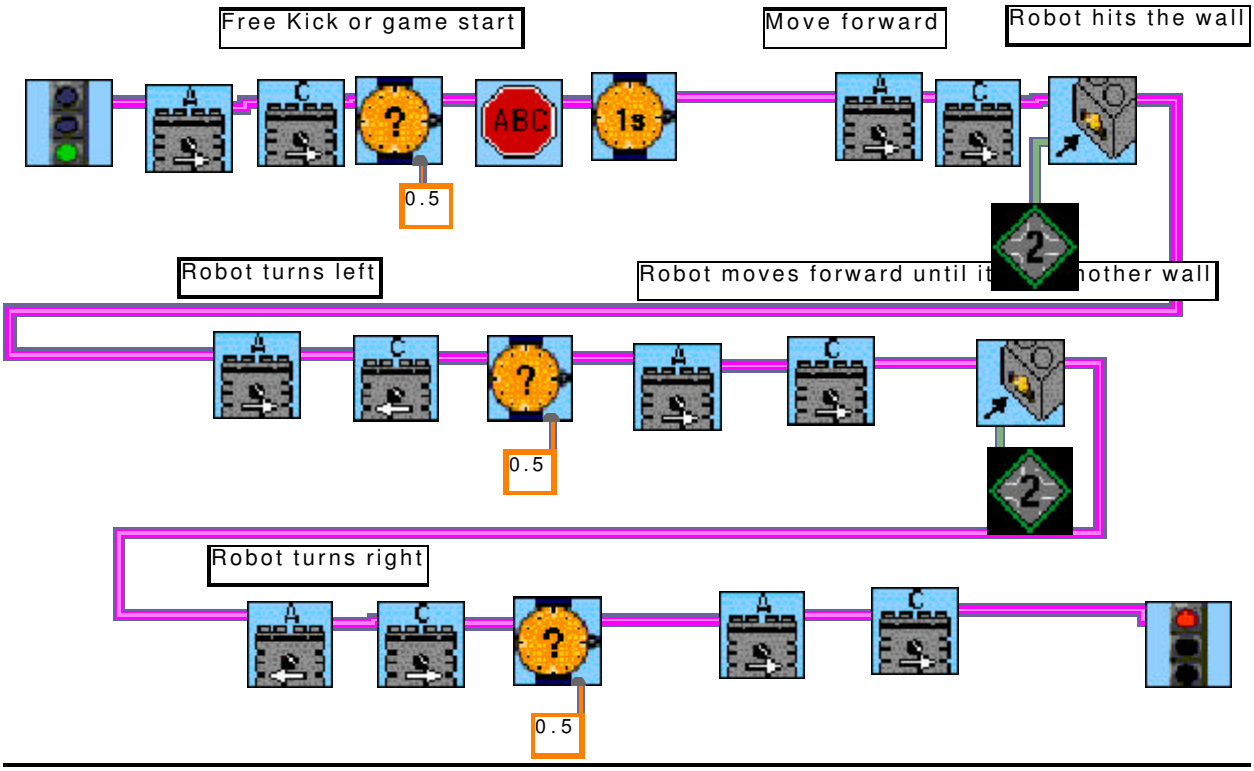

Figure 1: Example RoboLab programming screen.

Since RoboLab was developed as a LabVIEW Virtual Instrument, the groundwork is laid for the later part of the course where students are to use LabVIEW[4] as the main programming tool for the SCADA system simulation model. Early in the course, LabVIEW is also used to develop two virtual instruments. The first is developed to represent an oscilloscope while the other to represent a signal generator. To further lay the groundwork for the SCADA simulation model experience, the LabVIEW Web Publishing facilities are used to illustrate the control of a remote instrument over a network. SCADA systems form the basis of critical national infrastructure control systems for communications, transportation, and finance systems as well as the distribution of water and electrical power. Therefore, freshman students understand quickly the dangers posed by potential cyber attacks on these systems. Using LabVIEW[4] graphical programming language software, the issues involved in SCADA system vulnerability can be introduced with hands-on exercises. Using the LabVIEW DSC facilities that are designed for the development and simulation of SCADA systems, the experience for the students is very realistic. The example application chosen for teaching SCADA system operation and its vulnerabilities is municipal water distribution. The water system physics are naturally intuitive and allows the student to focus on other system aspects such as communication and control.

While the SCADA system simulation exercise we tested to date is sufficient to accomplish our educational outcomes, we feel that the student experience would be enhanced if a hardware simulator is used. In the freshman course, an R-C analog pump/tank simulator circuit was interfaced to the PC-based software through a National Instruments DAQPad unit. This analog circuit improves the sense of realism and teaches an additional lesson about analog devices and emulation. An emulator using pumps, tanks and water is currently under development to further enhance the student learning.

III. Laboratory Experience

A SCADA system involves multiple units therefore the introductory Water SCADA laboratory experience is organized as a class cooperative project. For an introduction to SCADA system organization see Boyer[7]. The most basic SCADA organization is a Remote Terminal Unit_(RTU) communicating with and controlled by a Master Terminal Unit_(MTU). Students at two laboratory stations decide which group will develop the MTU and which will develop the RTU. This laboratory provides you the basic concept of a SCADA system development using the LabVIEW DSC software tools. For an MTU the students are to (1) Build a Master Terminal Unit (MTU), (2) Build a Human Machine Interface (HMI), (3) Enable network communications by creating Tags (communication pointers) and pointing them at the RTU, (4) Manage alarms.

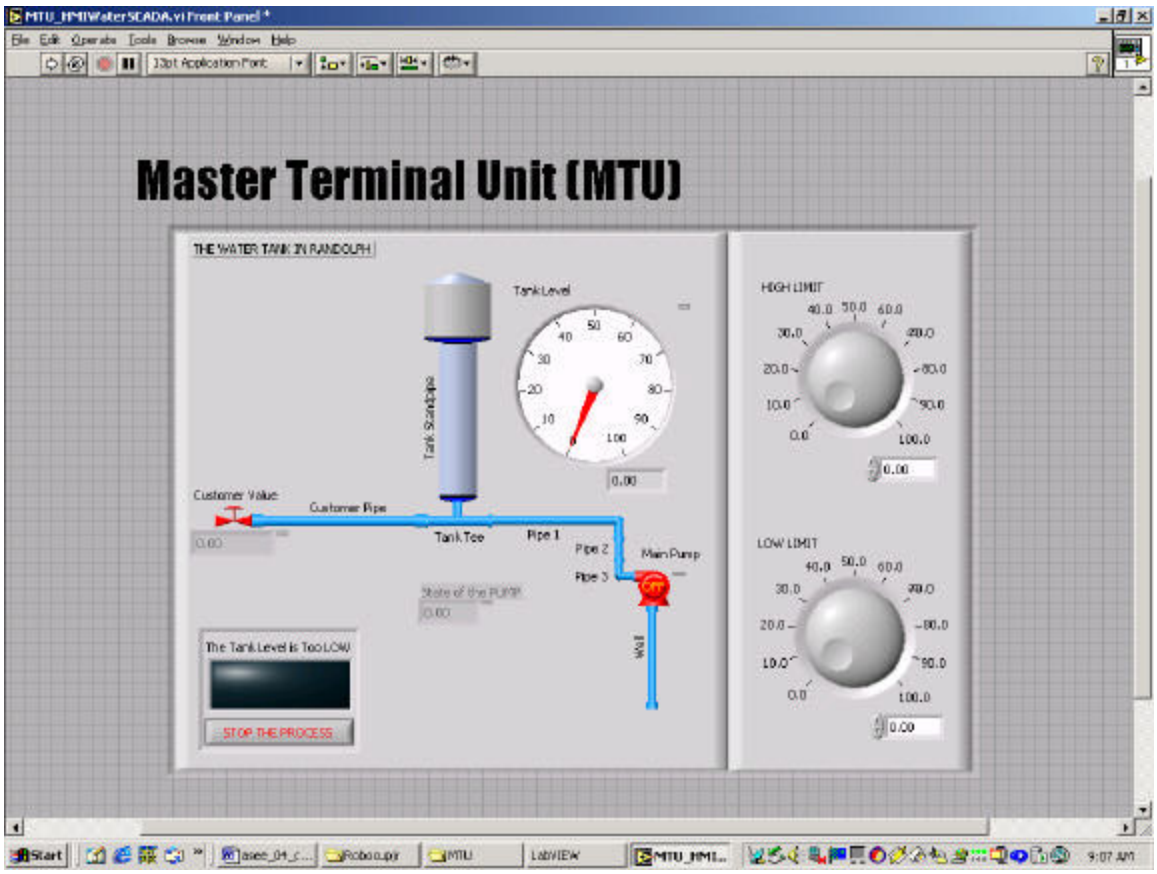

Figure 2: Example LabVIEW Front Panel

The RTU Team will do a corresponding set of actions for their unit. Communication between the two simulated SCADA system components is accomplished over the laboratory network. Building the MTU and HMI involves creating a front panel similar to that shown in Figure 2. Using pallets, students use drag and drop tools to place meters and knobs on the LabVIEW Front Panel.

The Front Panel is automatically associated with a block diagram that can be accessed in a "Block Diagram" window as shown in Figure 3. An icon appears in the block diagram corresponding to each front panel item. Students add icons in the block diagram to do the computation. The students then use a "wiring tool" in the "Block Diagram" window to interconnect the icon inputs and outputs to form their program. An execution control allows students to trace execution of their code. The resulting LabView program is often referred to as a LabVIEW Virtual Instrument or VI for short.

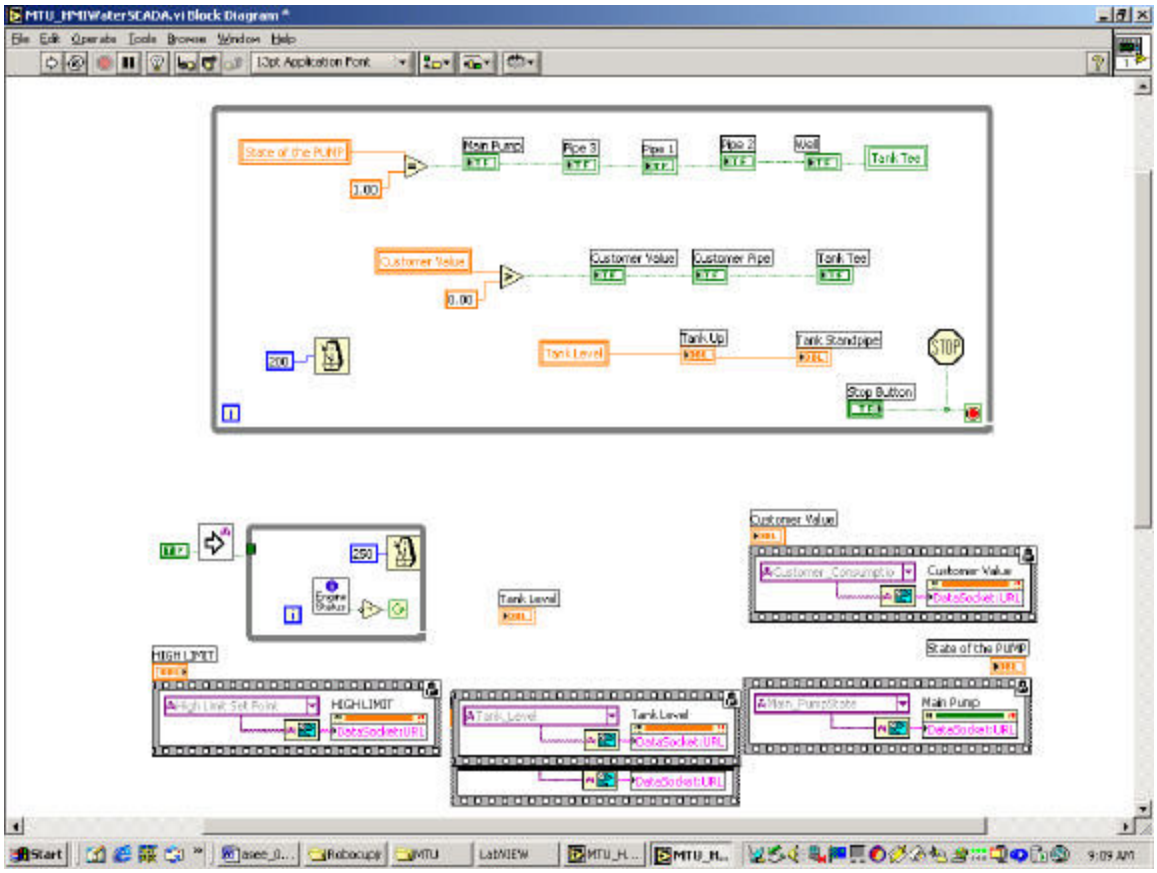

Figure 3: Example LabVIEW "Block Diagram"

Network communications in LabVIEW DSC is accomplished using a separate program running concurrently with the student-developed MTU or RTU Front Panel VI. This program is called a "Tag Engine". Transfer of communication packets between the MTU and RTU is accomplished through the use of the Tags specified by the students. A Tag is analogous to a pointer in C which in this case is an address of an input or output icon in the program executing on a machine elsewhere in the network. In the SCADA example, the tank display object on the front panel of

the MTU addresses the tank object on the RTU by use of a Tag. Developing network communications code is accomplished using a "Tag Editor". The "Front Panel" items are connected to the Tag Engine through the use of an HMI Wizard. The Tag Editor also allows the students to set alarm limits, an important feature for SCADA operation. Then after determining the tag addresses on the remote machine they are able to control the RTU VI from the MTU VI.

As a class project, a Cyber-Attack situation can be simulated using a second MTU to communicate with the RTU. This gives the students a tool to disrupt normal operation of their system. The second or rogue MTU can send zero setpoints causing the storage tank to empty and reducing water flow of the system to the customers to the capacity of the pump. The packets received by the RTU give conflicting commands. If the rogue transmits much more frequently than the MTU, then it effectively is in control. Actual attacks would likely use different tools but the key is to flood the target system with packets with malicious commands. For freshmen, the concept of switched network communications for remote data acquisition and control is an important concept to understand. It is also important that they understand how this communication might be disrupted. More detail on how this disruptive communication is actually accomplished is covered in the EE411 course. This will be the subject of a future paper.

IV. Results

The first time this introductory laboratory was tested on freshmen, the manufacturer-supplied LabVIEW DSC introductory "pump example" exercise was used. While the pump example was simple and intuitive, many of the DSC concepts were not explained in the exercise. Also, the students encountered some difficulty importing "Tags" over the network. This was their first experience working over a network and some confused locations on their machine with those on the remote. Based on this spring 2003 semester experience, this exercise was rewritten with the help of two students one of whom had taken the course. This exercise was subsequently tested in our EE411 Microcomputer Applications course with no problems. The students in the EE411 test were not confused about Tag addresses. The revised exercise is available at http://www2.norwich.edu/lessard Laboratory instructions are available under "Freshman_Intro_RTU.doc" and "Freshman_Intro_MTU.doc" and the starting LabVIEW code as "MTU_HMIWaterSCADA.VI", "RTU_WaterSCADA.VI" and "System_Calculations.VI".

V. Conclusions

The Lego Robotics hardware and software tools make introducing engineering principles with hands-on exercises both easy and enjoyable. More on Lego Mindstorms as a teaching tool is discussed by Patterson-McNeill and Binkerd[6]. The only problem is that students might spend too much time on their robotic and SCADA project to the detriment of their other studies. Using RoboLab to prepare the students to use LabVIEW also worked very naturally. Wang[5] discusses the RoboLab-LabVIEW intellectual connection in more detail. The details of protecting SCADA systems against cyber attack are daunting but the basic principles can be demonstrated effectively in a one-credit laboratory course using software simulation. We are developing our isolated wireless network demonstration using LabVIEW to control our physical water system emulator. PLCs are being donated by Automation Controls[8] to allow demonstration of a more widely used commercial system realization. Currently, the part artificial intelligence will play in

modern SCADA systems is not yet well defined. Concepts such as implementing expert systems and neural nets in switched communication network intrusion detection and prevention is being discussed in the senior level course and only mentioned in the freshman course.

Acknowledgements
We would like to thank Krenar Komoni and and Ilia Dormishev for their excellent job in converting the first version of the introductory SCADA laboratory into the much improved version which is referenced in this paper. We would like to acknowledge the support of the National Security Administration under NSA Grant #MDA904-02-0214.

Bibliography

1. Lego Mindstorms: http://www.lego.com
2. MLCAD: http://web.me.unr.edu/me151/spring_01/mlcad.htm
3. RoboLab: http://www.ceeo.tufts.edu/graphics/robolab.html
4. LabVIEW: http://www.ni.com
5. Wang, E., Teaching Freshmen Design, Creativity and Programming With Legos and LabVIEW, IEEE Frontiers In Education, October 2001, Session F3G
6. Patterson-McNeill, H., Binkerd, C., Resources for Using Lego Mindstorms, JCSC 16,3 March 2001, Pages 48-55
7. Boyer, S., SCADA Supervisory Control And Data Acquisition, The Instrumentation, Systems, and Automation Society (ISA), Research Triangle Park, North Carolina 27709, 1999.
8. http://www.automationtraining.com/

RONALD LESSARD
Professor Ronald Lessard is currently chair of the Norwich University Electrical and Computer Engineering department. He teaches microcomputer applications have included autonomous robots and lumber drying control. His SCADA experience with remote lumber drying control naturally lead to his most recent work for the NSA developing materials to teach engineers to develop systems that can be protected against cyber attack.

ROBERT GOODRICH
Robert W. Goodrich, PhD, PE, Associate Professor of Electrical Engineering, Norwich University. Formerly Director of Research at Northeast Utilities where he specialized in unconventional energy sources and power system planning. At Norwich, his primary interests are in instrumentation and control using National Instruments' LabVIEW.

JACQUES BENEAT
Jacques Beneat is an Assistant Professor of Electrical and Computer Engineering at Norwich University. He received a Ph.D. in Electrical and Computer Engineering from Worcester Polytechnic Institute (WPI), MA. He was a research scientist for over five years at the Center for Wireless Information Network Studies at WPI. His interests are in radio propagation and secure wireless communications.

STEPHEN FITZHUGH
S.L. Fitzhugh is currently the Computer Engineering Program Director at Norwich University. His current research interests include network traffic management, network and information security, and distributed control system security. He is a member of IEEE and ACM.