Teaching Reliable, Secure and Survivable Distributed Control System Design

R. Lessard, J. Beneat

Electrical and Computer Engineering Department
Norwich University

Abstract

Distributed Control Systems (DCS) are deployed in power utilities as well as communication, transportation, and financial infrastructures. As demonstrated by power distribution grid failures, most recently in August of 2003, designing for reliability is an important need. In addition to inherent design weaknesses, critical infrastructures are potential targets of cyber-terrorism and protecting critical infrastructures against terrorist attacks is a national priority. DCS security and survivability need increased attention.

One of the Norwich University Electrical and Computer Engineering courses that address these issues is EE411 Microcomputer Based Applications. EE411 is designed to give computer and electrical engineering students a capstone DCS design experience applying concepts covered in earlier courses. They are introduced to "SCADAville", a municipal water system emulator modeled after a typical municipal water distribution system. The concepts of safety instrumentation and networking are introduced using Allen Bradley Programmable Logic Controllers (PLCs). Students come to understand the advantages and disadvantages of ladder logic code for digital controller reliability. In designing Distributed Control Systems that make any connection to the outside world, the system must withstand attack from disgruntled employees, hackers or cyber terrorists. The system must function well even when the attacker breaks through the security barrier. In the EE411 course, the concepts of redundancy, robustness, and resilience are developed and reinforced in the laboratories.

I. Introduction

The President's Commission on Critical Infrastructure Protectionconducted a year-long study concluding that cyber threats are a clear danger (risk) to all infrastructures[1]. Byers and Lowe[2] concluded that "The increasing interconnection of critical systems has created interdependencies we haven't been aware of in the past". The current trend with new technology with DCS components tied together directly over the Internet results in very cost effective distributed control systems (Wallace[3]).

The methyl isocyanate leak at the Union Carbide plant in Bhopal India that resulted in the loss of 3800 lives[4] has shown that industrial accidents have potential devastating effects. It is conceivable that an industrial cyber attack could possibly exceed the death toll of the 9/11 attacks. The terror effect on a society that has come to rely upon a computer-controlled infrastructure would be magnified even more.

The Norwich University Electrical and Computer Engineering (ECE) department was first granted funds by the National Security Agency (NSA) in the summer of 2003 to develop course materials to teach future engineers the principles for developing cyber-attack-resistant critical infrastructure systems. The material developed that summer by the team of students and professors consequently found application in the freshman "EE116 Professional Projects" course as well as the senior "EE411 Microprocessor-based Applications" course. The freshman course experience was reported at the 2004 ASEE Annual Meeting[5].

The EE411 course experience started in the fall of 2003 and was largely based upon a DCS simulator developed during that summer. The simulator is a set of LabVIEW programs that represent the elements of a municipality water distribution system. In order to simulate cyber attacks on the system, a set of three laptops were purchased and interconnected through a wireless access point to produce an isolated network. Ethereal[6] was used on one of the machines to monitor the User Datagram Protocol (UDP) traffic between the MTU and the RTU laptops. Attacks were generated using precompiled code such as UDP flooding as well as LabVIEW programs for Internet Protocol Address (IP) spoofing. During the summer of 2004 the ECE department was generously donated a set of four Allen Bradley PLC 5/20 systems and additional funding from NSA to refine the DCS emulator and design a realistic DCS water system test-bed. During the fall of 2004, the results of these efforts were used to teach the students how to design DCS systems that are reliable, secure and survivable. This experience is described in detail in the rest of this paper.

II. Microprocessor-based Applications (EE411)

EE411 is a 4 credit course with a 2 hour weekly laboratory experience. It builds upon earlier coursework in microprocessor programming as well as in higher level programming languages such as C++ and National Instruments LabVIEW, and in electronics design. It is required in both the electrical and computer engineering curricula. Unfortunately, the textbooks currently available do not adequately cover the material needed for the design of secure DCS systems, and the students must use industrial trade literature and published articles, and their own laboratory experiences to gradually develop the system. Much of the course is devoted to learning the techniques associated with Ladder Logic programming and industrial network application most widely applied in modern DCS designs. The students need to optimize the DCS design. The conflicting objectives are cost, profit, safety, survivability, and surety. The terms to follow are often found in the literature for the design of modern DCS systems but the definitions are still subjective. For purposes of this discussion, surety for instance is acceptable performance under an unusual loading, where an unusual loading could be a physical attack, a natural disaster or a cyber attack. Survivability includes: 1)Redundancy of the system components for more reliable operation, 2)Robustness which depends upon excess capacity and distributed intelligence in the system, 3)Resilience which depends upon the ability of the Remote Terminal Units to recover from attack as well as software which seeks viruses and destroys corruption, 4)Security which includes deterrence, detection, and defense against attacks. Security is introduced in this course with the help of a few articles and on-line seminars provided by the ISA society[7]. Resilience is covered by reading articles. Robustness, redundancy, safety, profit and cost are discussed as appropriate during the development of the SCADAville DCS design. Ezell[8] provides a framework for tradeoff analysis of these competing objectives. For instance it provides guidelines for securing the system depending on the probability of security measures being defeated during an attack. The attack/defense exercise during the final project gives a good opportunity to discuss security and surety as well as the "safety instrumented systems" aspects of the design. Students study these techniques later in the course when they better understand the concepts involved.

III. Laboratory Experience

The municipal water system model dubbed "SCADAville" shown in Figure 1 serves as the main focus for the laboratory experiments. Piston pumps are used to fill the water tanks. A reservoir needed for emergency situations such as a fire is also present. The valves serve as means to provide different pump speeds to represent actual situations (old pump stations versus modern ones). The system also relies on gravity to get water out of the reservoir, the same way it would be done in reality due to the elevation of the reservoir.

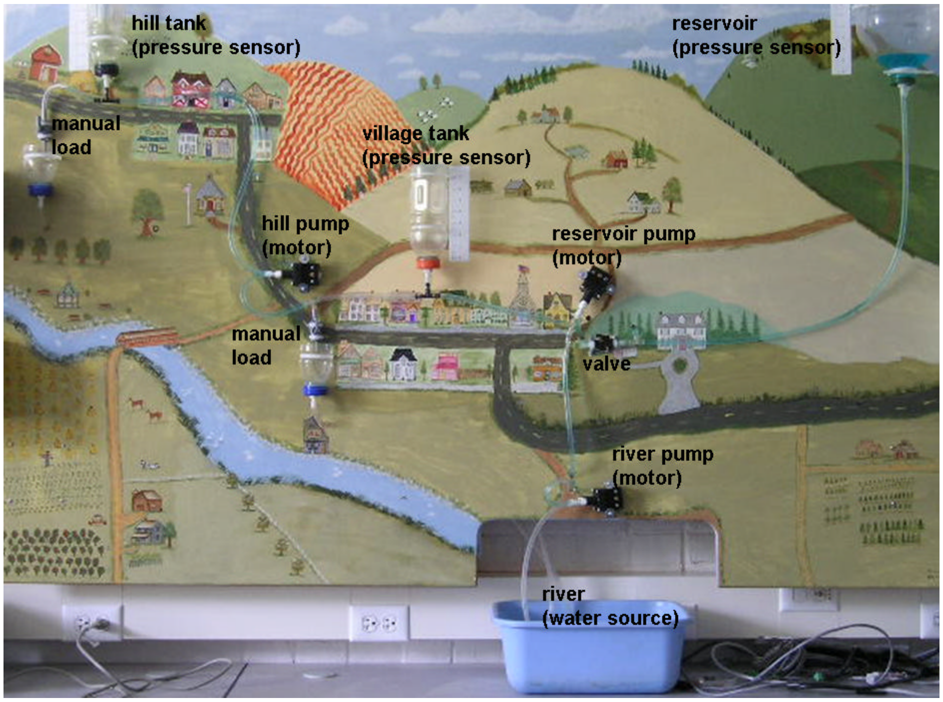

Figure 1: The SCADAville Municipal Water Distribution System Emulator.

Along with SCADAville, four PLC training systems are available to the students for the laboratory experiences. One of the PLC systems is shown in Figure 2. It provides several pertinent devices to illustrate the capabilities of a PLC system. AC input and output modules are connected to AC lamps and switches, DC input and output modules are connected to a thumbwheel and LED 7 segment display. Analog input and output modules are connected to a potentiometer and vu-meter.

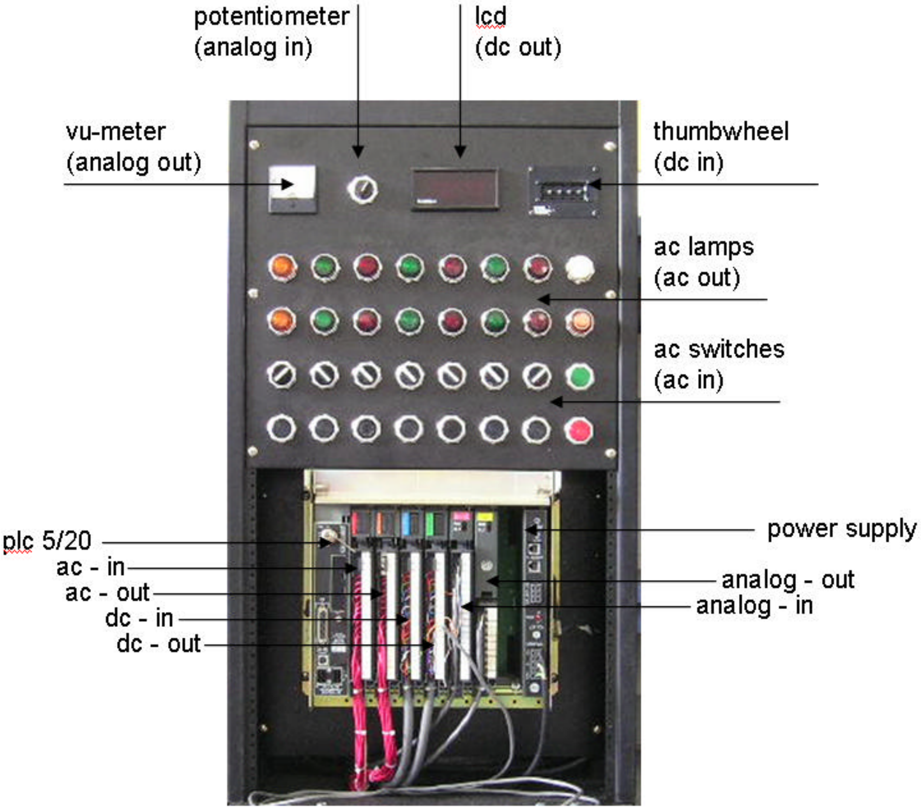

Figure 2: PLC5/20 Laboratory Station.

The first five laboratory exercises introduce ladder logic programming. In the first laboratory, students learn how to exercise the features of the PLC 5/20. The second laboratory has the student apply the concepts of the first laboratory to the control of a water pump/tank emulator circuit. Figure 3 shows the pump/tank emulator circuit.

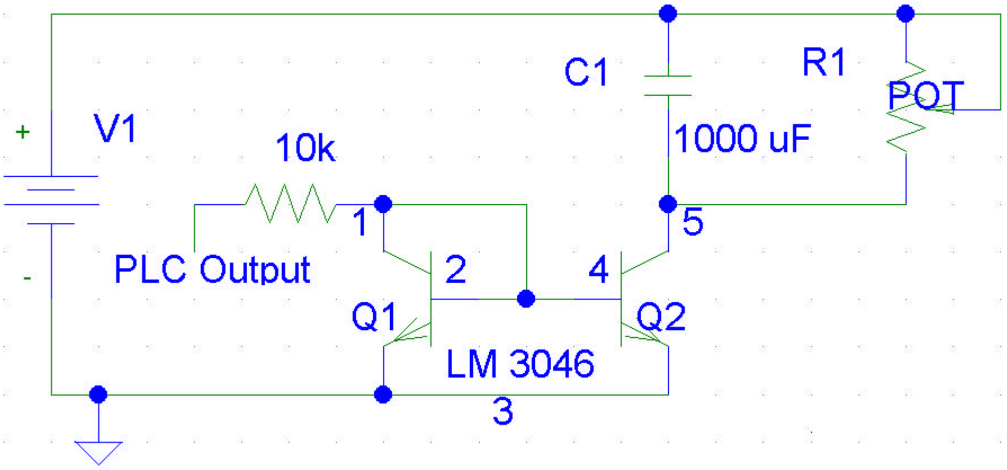

Figure 3: Pump Tank Emulator.

The capacitor represents the water tank, the charge Q on the capacitor the quantity of water stored. Hence the capacitor voltage represents the water tank level. Potentiometer R1 represents the drain on the tank by the customers. The pump is modeled by a current source realized as a current mirror. The current in the matched transistors of the LM3046 are controlled by the PLC output connected to Q1. The output voltage at the PLC output corresponds to the pumping rate. In this laboratory, the students would use an oscilloscope to monitor the capacitor voltage at node 5.

These first two laboratories lay down the model for the PLC as a robust and reliable controller. Here the students analyze and understand the advantage of the simplicity of the "scanning loop" software architecture. They use ladder logic to in effect configure the capability of their control system. The Computer Operating Properly "COP" mechanism of the PLC is the first "safety" feature of their design. This would prevent errant code from executing on their system. This would allow the control to revert to a completely electronic backup in the event the PLC failed "proper operation". This feature adds to the "surety" of the design. The robustness of the "scanning loop" architecture is a characteristic that makes the PLC both robust and reliable.

The third laboratory extends the simple emulator controller to encompass the operational features in a Distributed System Control such as using the PLC to set the Upper Trip Point (UTP) and the Lower Trip Point (LTP) of the process controller. They must demonstrate success with the emulator before controlling the actual SCADAville pumps. Their designing of a practical commercial version of the pump/tank controller allows for a more in depth understanding of how the control will revert to the electronic backup controller until the operator can get to the RTU and reset and perhaps reload the PLC. Here system "resilience" is discussed. The physical security issue at this point is provided by the relative isolation of the RTU. This is both an advantage and a disadvantage, and is further discussed at a later time when introducing cyber attacks.

In the fourth laboratory, the DCS network is established. The classical Master Terminal Unit (MTU) and Remote Terminal Unit (RTU) model as presented in Boyer[9] is used to guide the student in their design using the Allen-Bradley DH+ communications network. Here "survivability" issues are discussed. The DH+ is a proprietary protocol and is often though to be secure because it is assumed to be a company secret. However this is no longer true today when much information regarding popular proprietary protocols can be found over the Internet. On the positive side, DH+ is robust, reliable and simple to implement and allows data to be shared among peer level machines. The PLC-based MTU and each RTU are programmed to interact with the appropriate data items which are duplicated on each machine by a fast "scanning loop" mechanism. This allows for an attack on the MTU to be detected by the RTUs. It also allows for one of the RTU to take over the MTU function.

In the fifth laboratory, the students design a PC-based Human Machine Interface (HMI) for the PLC MTU designed in laboratory four. This HMI is designed using National Instruments' LabVIEW software. The command set for the DF1 protocol running over an RS232 connection is introduced and exercised. Student teams experiment with sample DF1 command strings. Once they understand how the protocol works, they are ready to complete the design. The students' HMI is designed to download the UTP and LTP values to the PLC MTU. It is also designed to upload the tank water level as communicated on the DH+ network in the previous laboratory. In addition, students must develop a more "functional" display of the water system shown in Figure 4 beyond the sample meter-switch-light LabVIEW HMI that was provided to them. The HMI is the entry portal for a network-based attack. This represents a key “survivability (security)” issue. Students learn how supervisory commands are communicated to the PLC MTU and assess the vulnerabilities of the system.

In contrast to the third laboratory where an isolated water pump and tank were being controlled, the sixth laboratory introduces the concept of controlling a system of tanks and pumps. During the laboratory preparation, the students develop a resistor/capacitor analog simulation model for the isolated pump/tank components. They then write the node equations for the network model that simulates the entire SCADAville plant as can be seen in Figure 4.

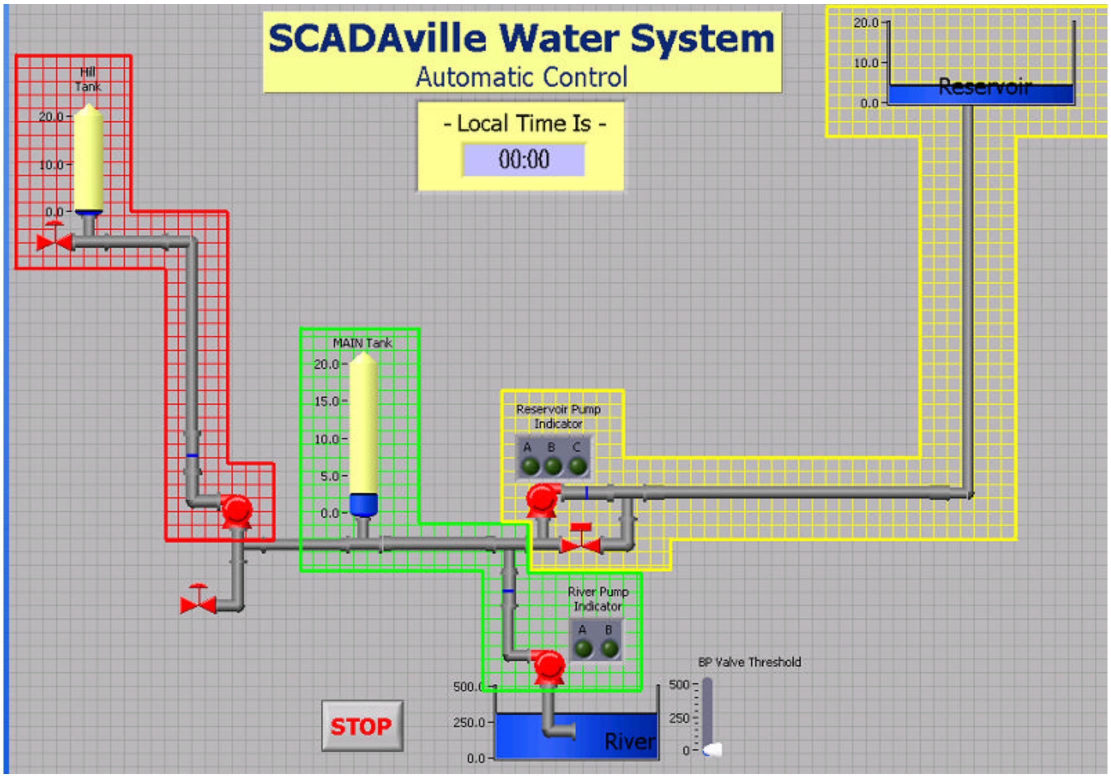

Figure 4: SCADAville DCS Control Panel.

They then write LabVIEW code to simulate PLC control of SCADAville. It was at this point in developing the course that we discovered that the Allen Bradley RSLogix software includes a tool to facilitate organizing the ladder code for a state machine design. This Sequential Function Charts (SFC) tool was used to produce the diagram of Figure 5 which organizes the PLC MTU code to sequence the pumps running on individual RTUs so that contention for resources will not be a problem.

Control of the SCADAville emulator hardware does not occur until the final project. No new issues of “safety”, “survivability” or “surety” are addressed at this point. This laboratory allows for reinforcement of the lessons from previous laboratory exercises.

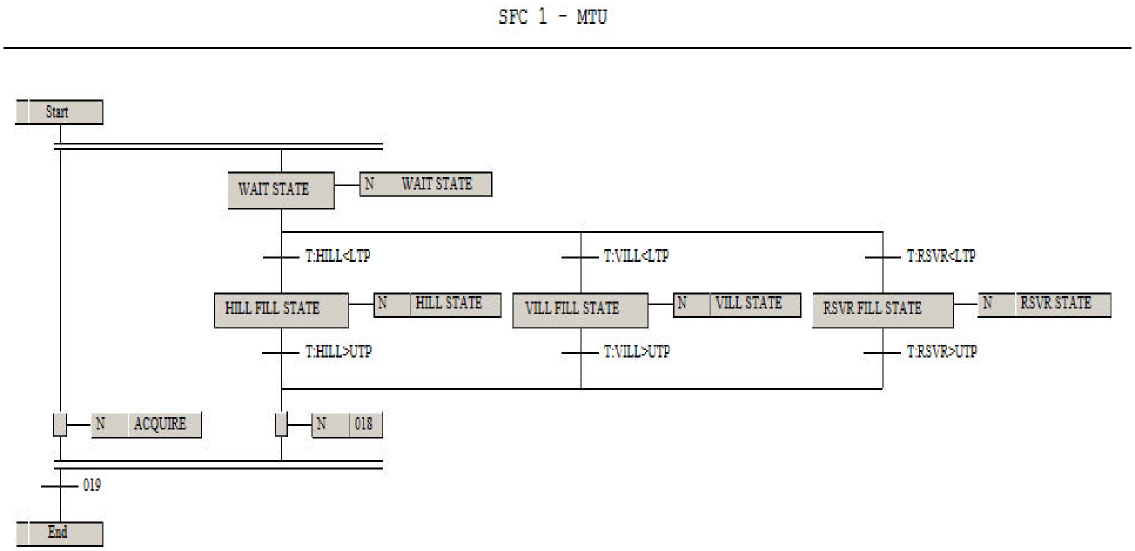

Figure 5: Sequential Function Chart (SFC) Diagram of SCADAville MTU.

In laboratory 7, students analyze the existing LabVIEW Datalogging and Supervisory Control (DSC) software to see how a PC-based industrial solution might work. They examine the design in light of the design objectives developed in the lecture section of the course. In the Pre-lab work, students apply “Risk Analysis” to understand system vulnerability to failure. They do not yet understand all the risks of their system to cyber attack at this point so component failure is discussed instead. Alarms and Security solutions for the commercial product are addressed. The commercial system using passwords and a hierarchical system of privileges is presented. The name of the National Instruments’ UDP type proprietary protocol that is used in this product is called Logos. Logos is used for Ethernet-based network communications. Again, the advantages and disadvantages of this protocol being proprietary are discussed.

Laboratory 8 is designed to have the students delve into the issues involved in modem communications such as the use of radio-based remote units in water utility DCS. To better understand system vulnerabilities, students study the physical characteristics of switched telecommunications and dedicated radio links. They use 1.DH+ running on proprietary Allen Bradley hardware. 2.DF1 running on RS232 between the PC and the PLC. 3.Logos and UDP running on an Ethernet-based network. They need to understand the basics of serial communication to design a “survivable” system. Here “redundancy” is discussed as it relates to “survivability”. Some systems backup the command center with a second system. Most large systems such a Walnut Hill in Massachusetts have several levels of backup communications. Communications is shown as a two-edged sword since the communication link is also the doorway used by the attacker.

Laboratory 9 is the final course project and lasts 4 weeks. The first week is designed to revisit the system simulator and emulator and complete any unfinished work. The second week is designed for the students to complete the design of an inter-dependent three zone controller that manages the contention for water resources. For example, they must propose a solution to the problem that if pumping water to the hill and village occurs simultaneously the village water pressure fails completely. The third week is used to complete the HMI for the entire system and control SCADAville using this interface. As originally designed, the fourth week was designed so that student teams would attack each other's DCS designs to uncover vulnerabilities. The notion of "safety instrumentation" is introduced as electronic controls can take over in the event of PLC system failures. If the PLC-based MTU is disabled in the attack, the RTU-DH+ network allows one of the RTUs to take over the MTU function. If an RTU determines that the shared DH+ data set has been corrupted, it can revert to a "safe" set of setpoints. While isolated controllers represent a sub-optimal solution to the total plant control, a temporarily acceptable solution is possible until the technician can visit the site and restore normal operation. On a higher level, "surety" is demonstrated as the student application level firewall protects against intrusions from strangers. However in a flooding attack, the RTU must abandon communications with the MTU and revert to "safe" control settings until reliable communications can be re-established. The laboratory handouts presented in this paper are available at: http://www.ece.norwich.edu/~lessard/

IV. Conclusions

The intent of the EE411 course is to educate students in the design of systems that are 1.Safe, 2.Survivable, 3.Sure. The PLC platform is a good tool to illustrate safety-instrumented systems. There are many industrial examples. Survivability is concerned with: 1.Redundancy 2.Robustness 3.Resiliency 4.Security. The DH+ peer-to-peer network architecture is well suited to the issues of redundancy and robustness of the design. Any one of the Remote Terminal Units could take over the function of the MTU if the MTU were disabled in the attack. If any of the Remote Terminal Units sense an unrecoverable system problem, it could revert to standalone control mode. While not being an optimal solution, control from isolated controllers would be better than total system failure. If the Remote unit fails, a preset electronic version would take over. If power failed across the system, then the units would be designed to reset to default setpoints and where necessary, reinitialize the modems.

The PLC control solution is a relatively expensive addition to the laboratory. It is well suited for illustrating some of the basic level instrumented safety, survivability, and surety design issues. During the course, the students visited the Northfield Vermont water treatment plant, and also witnessed Factory Acceptance Testing of the Manchester-New Hampshire water utility control system during a trip to LCS Controls in Rochester Vermont. In both cases, they saw the same equipment and software that they were using in the laboratory. This encouraged them to ask more in depth questions about design as it related to the issues of safety, survivability, and surety.

During the summer of 2005, the facilities are to be further improved, for instance with the addition of a closed Wide Area Network (WAN). However, a great challenge is the lack of suitable textbook material related to the new conflicting design objectives. A significant effort will be on improving the courseware for the best design practices of modern DCS systems including distributed intelligence and security features.

Acknowledgements

This work was made possible by the support of a grant from the National Security Agency (NSA Grant #MDA904-02-0214). The Allen Bradley PLC equipment and training of

Norwich personnel was generously donated by Mr. Randy Burgess (Automation Training Inc, Carmel IN.)

Bibliography

1. The Report Of the President’s Commission On Critical Infrastructure Protection, October 1997 http://www.tsa.gov/interweb/assetlibrary/Infrastructure.pdf

2. Byers, E. J., Lowe, The Myths and Facts behind Cyber Security Risks for Industrial Control Systems, VDE Congress, Berlin, October 2004.

3. Wallace, D. I., Pipeline and Gas Journal

http://www.undergroundinfo.com/PGJ/pgj_archive/Feb04/smart%20fields-02.04.pdf

4. Bhopal, Union Carbide, Incident Review, http://www.bhopal.com/review.htm

5. Lessard, R., Goodrich, R., Beneat, J., Fitzhugh, S., Supervisory Control And Data Acquisition Security Experience, 2004 ASEE Annual Meeting, Paper #1116.

6. Ethereal, A Network Protocol Analyzer, http://www.ethereal.com/

7. ISA Pre-Recorded Security Seminars, http://www.isa.org/Template.cfm?Section=Pre_Recorded_Topics&template=/TaggedPage/ArcSemSeries.cfm&SubICID=4336

8. Ezell, B., Risks of Cyber Attack to Supervisory Control and Data Acquisition for Water Supply, Masters of Science (Systems Engineering) Thesis, School of Engineering and Applied Science, University of Virginia, May 1998 http://www.riskinfo.com/cyberisk/Watersupply/SCADA-thesis.html

9. Boyer, S.A., SCADA Supervisory Control And Data Acquisition, 2nd Edition, 1999, ISA

Professor RONALD LESSARD is currently chair of the Norwich University Electrical and Computer Engineering department. He teaches microcomputer applications which have included autonomous robots and lumber drying control. His SCADA experience with remo te 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.

Professor JACQUES BENEAT teaches communications and controls in the Norwich University Electrical Engineering program.