The Power of Hands-On Exercises in SCADA Cyber Security Education

Elena Sitnikova, Ernest Foo, Rayford Vaughn

The Power of Hands-On Exercises in SCADA Cyber Security Education

Elena Sitnikova[1], Ernest Foo[2], and Rayford B. Vaughn[3]

[1] University of South Australia
elena.sitnikova@unisa.edu.au

[2] Queensland University of Technology
e.foo@qut.edu.au

[3] Mississippi State University
vaughn@research.msstate.edu

Abstract

For decades Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) have used computers to monitor and control physical processes in many critical industries, including electricity generation, gas pipelines, water distribution, waste treatment, communications and transportation. Increasingly these systems are interconnected with corporate networks via the Internet, making them vulnerable and exposed to the same risks as those experiencing cyber-attacks on a conventional network. Very often SCADA networks services are viewed as a specialty subject, more relevant to engineers than standard IT personnel. Educators from two Australian universities have recognised these cultural issues and highlighted the gap between specialists with SCADA systems engineering skills and the specialists in network security with IT background. This paper describes a learning approach designed to help students to bridge this gap, gain theoretical knowledge of SCADA systems' vulnerabilities to cyber-attacks via experiential learning and acquire practical skills through actively participating in hands-on exercises.

Index terms: industrial control systems, SCADA, critical infrastructure, cyber-security, experiential learning, security laboratory, curriculum

1. Introduction

Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) are used for remote monitoring and control physical processes in many critical industries including electricity generation, gas pipelines, water distribution, waste treatment, communications and transportation. Increasingly today, these systems are being interconnected with corporate networks via the Internet. This makes them vulnerable and exposes them to the same risks as those experienced in cyber-attacks on a conventional network.

In recent years, research and education in the area of cyber security of ICS and SCADA systems has attracted interest within academic institutions. With the Australian Prime Ministerial directive recently announced by the Hon Julia Gillard and the launch of a new Cyber Security Centre [1], more researchers will begin to investigate the problem set associated with such systems and their critical roles in monitoring and control of Australian Critical Infrastructures. There is also a high industry demand in cyber security training for ICS and SCADA systems. However, many existing research centres are limited by the lack of testbeds or models capable of representing actual instantiations of ICS applications and an inability to observe an entire SCADA system. The reasons are usually high costs and limited space for such laboratories.

The Idaho National Laboratories (INL) SCADA Testbed Program is a large scale program dedicated to ICS cyber security assessment, standards improvements and training [2]. For several years Australian operators of critical industrial control systems have been attending one week training provided by INL in the US. The Australian government Attorney General's Department has subsidised attendance for selected attendees. This training which balances theory and practice is valuable. However from an Australian perspective the benefits are limited, because the time available limits the areas covered and it is a 'one off' opportunity, with substantial costs for the fortunate few attendees. These factors create an urgent need for locally based educational programs which aim to build awareness and relevant skills across the critical infrastructure industries. Local programs would also allow the curriculum to be customised, reflecting specific Australian directives and best practices. It would also cover a broader range of topics and delve more deeply into them. Local training capability also scales up better allowing an increase in the volume of students for a better return on investment.

This paper describes the authors' experience in designing and developing hands-on practicals in the two university courses listed below and their value in discovering vulnerabilities in SCADA systems. The cost of travelling overseas to undertake this kind of training is prohibitive, so locally offered courses such as these minimizes expenses and maximizes opportunities for operators to gain critical education in this area.

- COMP 5062 Critical Infrastructure and Process Control Systems Security (Masters level) course at the University of South Australia (UniSA)
    - At UniSA, hands-on practicals are presented during a one week intensive study workshop that balances the content of lectures with hands-on practicals delivered in our security laboratory set up temporarily on equipment provided by industry collaborators.
- Cyber-security 5 days training at the Queensland institute of Technology (QUT)
    - At QUT, the curriculum for a 5 day Cyber-security training is focused on providing education and local training for professionals working in the control system industry, as well as for graduates hoping to enter the field.

By way of background, researchers at both UniSA and QUT established a cross-institutional collaboration in 2011 when they first met at the Idaho INL training facilities. This initial connection was expanded internationally through strong collaborations with Mississippi State University (MSU) in the United States. This involved exchanges of faculty members, the establishment of SCADA laboratory facilities at QUT similar to the MSU laboratory and the exchange of virtual SCADA testbed software with UniSA. This collaboration has already resulted in several joint papers in the field [3,4] and plans for an international research and educational project between the three universities involved, MSU, QUT and UniSA.

The paper is organised as follows. Section 2 describes the needs of education in SCADA and ICS systems and highlights the challenges of educating both IT personnel and SCADA engineers. Section 3 examines tailoring reflective practice and active learning pedagogical approaches. In Sections 4 and 5 we provide details on the practical laboratories that we developed at QUT and UniSA and comment on the value that they provided to the students. Section 6 outlines some benefits, limitations and preliminary findings of how students responded to courses with a focussed on hands-on practical component. We conclude this paper by reviewing our contributions and future work.

2. The Need

According to an international commentator and INL's infrastructure protection strategist Michael Assante, for managers and engineers responsible for control systems, physical security has always been a priority [5]. For many also, IT security is a new field. They have to understand the importance of these systems' cyber security requirements, associated risks and thus deploy proper security measures. Assante in his testimony to the US government on process control security issues, criticises the last decade's considerable body of research in implementing yesterday's general IT security approaches into today's ICS and SCADA systems. He asserts it has "proven ineffective in general IT systems against more advanced threats". He also notes that as more technological advancements are introduced to ICS and SCADA, more complexity and interconnectedness are added to the systems, requiring higher levels of specialty skills to secure such systems. Training managers and process control engineers in the field will help to meet this skills need gap.

Other literature states that SCADA and process control systems vulnerabilities can increase from a lack of communication and/or trust between IT and engineering departments [6]. This is because very often SCADA networks services are viewed as a specialty subject, more for engineers than standard IT personnel. Control system operators are often mistrustful of IT maintainers because ICS has a 24/7 uptime requirement whereas IT maintenance often requires system outages. Previously [7,8,9, 10] authors have recognised these cultural issues and highlighted the gap between specialists with ICT engineering skills and the specialists in network security with IT background.

The gap between these two disciplines needs to be bridged to recognise, identify and mitigate against vulnerabilities in SCADA and process control systems networks. Broader awareness and the sharing of good practices on SCADA security between utility companies themselves is a key step in beginning to secure Australia's critical Infrastructure.

Industry-trained professionals and qualified learners, today often working in process control services and government organisations, bring to class their fundamentally different skills, objectives and operating

philosophies to the concept of security in an enterprise IT context. Thus, the authors are challenged to develop a curriculum that aims to address both discipline-specific engineering and IT issues and bridges the educational gap between IT network specialists and process control engineers, but within the post-graduate cyber security and forensic computing nested programs. To address these issues, the curriculum is designed to accommodate both process control engineers (with no or limited IT skills) and IT specialists (with no or limited engineering skills). This in itself is a difficult balance to achieve.

3. Learning and Teaching Aspects

3.1 Reflective Practice

Our students' diverse skill set has motivated educators at UniSA to implement a reflective practice approach to the hands-on exercises as a part of their assessment task. According to the literature, reflective practice enables students to: 1) understand what they already know; 2) identify what they need to know in order to advance their understanding of the subject; 3) make sense of new information and feedback in the context of their own experience and 4) guide choices for further learning [11]. Considerable literature attests to its benefits. In the mid-late 80s, researchers Kolb, Schon and Boud et al. [12-14] highlighted the major benefit of reflective practice as enabling learners to make sense of their practical experiences and develop critical thinking skills which are essential for decision making and problem solving, especially in the workplace. It has been argued [15] that reflection can be used as a tool to help learners through their studies by encouraging and fostering a deep learning approach. Unlike many other professions and disciplines, especially those in science, health and medicine, that have long adopted this pedagogical practice, engineering and ICT education have only recently begun to adopt this practice [16].

A reflective practice pedagogical approach has been introduced in the COMP 5062 Critical Infrastructure and Process Control Systems Security 4.5 unit course at The University of South Australia. Using well-structured hands-on practical exercises, students experience the technical details of what they have learned from the associated lecture topics. They then reflect on the skills gained, in the form of a written report by the end of the intensive week. Below, we discuss how hands-on practicals are aligned with a 4 step reflective practice process that enables students to

1) understand what they already know;

Prior to the intensive week, students have to complete a brief questionnaire on what they know about SCADA systems security. This allows instructors to identify students' backgrounds, work experience and knowledge in control systems. It also provides information for making informed decisions on how to form groups where diverse skills complement each other's skills to aid collaborative work.

2) identify what they need to know in order to advance understanding of the subject;

This step requires planning intensive week activities to balance theory and practice. Every daily session presents theory to students with active discussion, addressing focussing questions. This gives students knowledge prior to laboratory practicals.

3) make sense of new information and feedback in the context of their own experience;

The Intensive workshop is constructed to be informative and active, with timely feedback and support from instructors. Reflection on new gained knowledge is demonstrated during active participation in group discussions, oral presentations and written reports on the results from practicals.

4) guide choices for further learning

Building on knowledge during the intensive week, students reflect on comments and suggestions provided and then write their further assignment component - a SCADA Security Plan (SSP). The plan takes a form of the academic paper that includes a literature review on the topic and is based not only on theoretical scholarly knowledge, but also on the technical knowledge that students have gained.

QUT educators also implement a reflective practice approach to students' learning. For most of the courses there is an endeavour to ensure that there are three types of sessions. The intent is to provide a theoretical basis for the material, reinforce this with practical application and finally, encourage students to integrate the learning by actively reflecting on the sessions.

- *The first session* is a lecture type session where students are introduced to the theoretical aspects of the material. Students learn where issues fit into the bigger picture. Often, cyber security training courses

concentrate on particular vulnerabilities without teaching the background theory. This makes it difficult for students to adapt when faced with a new attack or other scenario.

- *The second session* is a practical hands-on exercise relevant to the topic. Some courses provide only theory or lecture based courses. These are good for awareness issues, but it is not until students successfully complete a hands-on exercise that the impact of the security issue hits home. The use of complex full system hands-on exercises such as a red team, blue team exercise is particularly good at providing an impact to students.
- *The third 'debrief'* session, occurs after the practical session. Here, the course instructor encourages students to discuss the impact of the previous exercise and relate it to their industry experiences. These open discussion sessions allow students to share their insights. Ideally, course instructors arrange for a break between the practical session and the debrief session. This allows students to reflect internally and synthesise the application of the hands on exercise that they have just completed. We have found in previous cyber security courses that the debrief sessions are often described by students as the most useful aspect of the course.

The authors next describe a set of hands-on exercises that are designed to help students to overcome the ICS/IT gap, gain knowledge through experiential learning of SCADA systems vulnerabilities to cyber-attacks and reflect this knowledge by actively participating in hands-on cyber security exercises.

4. Intensive Hands-on Practicals at UniSA

UniSA has developed a new Master of Science (Cyber Security and Forensic Computing) one and a half year full time equivalent program. It offers a pathway through a suite of nested programs including Graduate Certificates, a Graduate Diploma, Masters and possible continuation into PhD level program. These are designed to attract a diverse group of learners traditionally coming from two cohorts of industry practitioners: one with engineering (SCADA practitioners) and the other (ICT personnel) with IT background. It also enables industry-trained and qualified learners without undergraduate degrees, to gain the security qualification required though their access to tertiary study [8]. Within the program students have to complete eight core courses before they study a Minor Thesis 1 and 2. The COMP 5062 Critical Infrastructure and Control Systems Security course is one of the eight courses the program offers.

As the majority of these students are working and studying part-time, we need to accommodate their needs. To maximise flexibility, availability and convenience, the CICS course is offered to part-time students in online distance study mode (external class) – 1 virtual online class per course per week over 12 weeks plus one week half day intensive study in-class per course (15 hours).

The intensive face-to-face component is not mandatory for external students, but highly recommended. It is a cornerstone of the curriculum and it always occurs in week 4 of the study period. Students from both external and internal classes have an opportunity to attend a face-to-face workshop in Adelaide and participate in hands-on practicals, guest speakers' presentations and also networking opportunities among peers. During an intensive study week when students attend a half day face-to-face session at Mawson Lakes campus at UniSA, they attend lectures and guest speakers' presentations from industry, police, and law enforcement agencies. Students receive the majority of the course materials and hands-on exercises in class. Exercises are based on operational world situations run by industry practitioners. A brief overview of the intensive week is described in Table 1.

5. A Continuing Professional Education (CPE) training program at QUT

QUT has developed a Continuing Professional Education (CPE) training program teaching cyber security for industrial control systems. This course is mainly designed for control systems engineers to raise awareness of the impact of cyber attacks on the systems that are under their control. The course also caters to IT security professionals who wish to gain an understanding of control systems and the issues that face control system designers. The course is taught at a postgraduate level, as participants are mainly experienced engineers or IT professionals. Figure 1 (2-4) shows the QUT's laboratory module. The pioneer of the SCADA laboratory was Mississippi State University which first established the lab through support from the US National Security Agency and the US Department of Homeland Security. QUT purchased their lab from the same engineering company used by MSU to insure compatible configurations that will support future research experimentation between the two institutions.

As Control Systems become integrated with IT systems, engineers and IT professionals are now expected to understand the vulnerabilities and threats that affect industrial control systems under their protection. As a result they need to be familiar with general system exploitation techniques and tools that may be used against their system services and applications.

	Day 1	Day 2	Day 3	Day 4	Day 5
Short Lecture	SCADA control systems fundamentals	SCADA Specific Protocols Modbus and DNP3			
Practical Lab	Programming and testing of PLC.	Modbus Communications	SCADA Vulnerability assessment Part 1	SCADA Vulnerability assessment Part 2	
Lab Configurations	Virtual machine pre-installed with PLC programming software with emulation ability; HMI programming software with runtime ability, SCADA development and runtime software.	Virtual machine pre-installed with ModScan, MovServ software; Hex editor; Wireshark open source ; Hyper Terminal communication software; serial port capture, Modbus RTU parser	System is deliberately configured to be highly vulnerable with network in a "bad" condition. Different platforms are used (NT3.5, NT4, Win98) with un-patched software installed	System configured to be less vulnerable with network in a "good" condition. Tasks included: blue/red team exercise with red as attackers and blue as defenders. Students are provided with Backtrack software.	**Recap and the summary** Students present on what they have learned during intensive week. During this session students reflect on the knowledge they have gained during the week.
Task	Students have to write a PLC program starting from a single traffic light operation, adding later multiply traffic lights and include pedestrian lights and extending PLC program to include external control for emergency such as fire and ambulance. With SCADA running and its graphical control through HMI, students have exposure to detect PLC faults and fix them to ensure SCADA operates in correct way.	Students study Modbus RTU and Modbus TCP serial packets using ModScan and ModSim; forming of a Modbus packet to inject and manipulate of the traffic PLC.	The Blue/Red team exercise with red as attackers and blue as defenders of the traffic control system (Fig.1). Students are provided with Backtrack software.	The Blue/Red team exercise with Red as attackers and Blue as defenders. Students are provided with Backtrack software.	
Assessment	Worksheet completion with the comments /solutions demonstrated	Worksheet completion with the comments /solutions provided	Group presentations and discussions on Day 5	Group presentations and discussions on Day 5	

Table 1. A brief overview of the intensive week at UniSA.

This course aims to give an understanding of the fundamental concepts and major issues in the area of industrial control system cyber security. Students will be able to identify critical application and system service vulnerabilities and determine the information security implications of those vulnerabilities upon completion. The course introduces of a range of techniques for exploiting and mitigating the impact of threats and vulnerabilities to networks and systems.

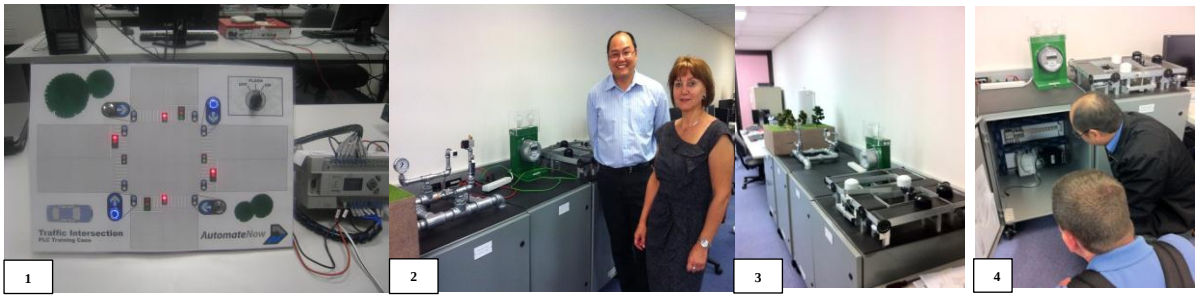

Figure 1. A SCADA Traffic Control System Lab at UniSA (1), Pipeline, Smart Meter and Conveyer Laboratory Simulators at QUT (2-4).

It is important to point out that this course discusses design and testing principles that produce secure applications. During this course techniques and tools are introduced that demonstrate how to exploit system services and applications. Each day of class consists of several information style presentations followed by a relevant practical exercise.

The course is an intensive five-day course delivered in one week. Students must travel to Brisbane to participate. The course has seen representation from students from a wide range of industrial sectors including transport, power, gas and water treatment. Students have travelled from all around Australia to attend the course even though a similar course is held in Western Australia.

The cornerstone of the QUT program is an 8 hour practical exercise. The course participants are divided into a blue team and a red team. The Blue team must defend a corporate network that is connected to a real industrial control system process. The Red team must attack and disrupt the industrial process. The QUT program employs small scale industrial process systems that use industrial PLCs to control them. These systems are also used to conduct research in the area of industrial control system vulnerabilities and the testing of mitigation strategies.

The following is a brief overview of day to day content included in the QUT's five-day course (Table 2)

Day 1	Day 2	Day 3	Day 4	Day 5
The first day begins with an introduction to cyber security and control systems. Definitions of threats and vulnerabilities are covered and a round up of recent security incidents is discussed. It culminates with a practical demonstration of a MODBUS control system being compromised.	The second day looks at common web application vulnerabilities such as cross site scripting, cross site request forgery and SQL injection. In the afternoon we look at authentication systems. The practical exercises involve demonstrating common password cracking strategies.	The third day looks at network vulnerabilities and exploit frameworks. We start the day by discussing network discovery techniques. The final section of the day looks at network mitigation strategies and the use of firewalls and intrusion detection systems.	The fourth day of the course is the key learning event for the course. The Red Blue team exercise is an eight hour event where the blue team must defend their industrial process from the red team.	The fifth day is a closing day where the students reflect on the week they have completed. Student from the red team and blue team give presentations that reflect on the processes and incidents that occurred in the Day 4 exercise. The instructors conclude the day by emphasising key points, as well as revealing any components of the Red Blue Team exercise that could have been handled better by the respective teams.

Table 2. A brief overview of the content of the CPE training program at QUT.

6. Discussions

Experience on running of hands-on practicals and the lessons we have learned could be categorised as benefits, limitations and observations.

Benefits. IT personnel together with control systems engineers have to encounter non-standard IT systems and learn how to protect SCADA and ICS and make them less vulnerable to cyber-attacks.

Limitations. Unlike QUT, UniSA does not have its own laboratory. For this reason academics rely on local industry practitioners to design, establish and run the lab once a year for a week. UniSA provides licences for required software, but hardware equipment is generously provided by industry collaborators.

Observations. At UniSA Students demonstrated good results (grades for hands-on practicals), they also summarised and reflected on what learned during the week during their oral presentations in class, but they were informally assessed by educators and fellow students. It would be better to include this activity in a formal submission with appropriate weighting.

One of the major goals of the course is the applicability of knowledge gained to students' work environments. We received positive feedback from students to this effect:

> *"It's been so much more than I expected - a good balance of technical along with practical skills that will hopefully help me gain employment" (Student #1, 2011, Adelaide)*

> *"The subject matter covered throughout the course was generally directly relevant to the industry I work in. The assignments were very helpful and relevant. Data collected during the first assignment and the report generated as part of the second assignment was able to link directly with issue within my own enterprise and been able to submit internally within the enterprise for further action". (Student #2, 2011, Adelaide)*

QUT Course Structure

The QUT training course has its origins in coursework adapted from normal coursework security classes that are offered to postgraduates and undergraduates. As a result the lecture presentations were quite theoretical and lengthy. There has been a concerted effort to streamline these presentations and to allow more time for students to explore and experiment in the practical exercises associated with each topic. This is also important for preparing students for the Day 4 Red/ Blue Team exercise.

Course Content

The content of the QUT training course is based on several classes that make up the undergraduate and postgraduate degree courses. This content previously had a strong focus on web vulnerabilities. While this has been very educational and interesting for students, the relevance to industrial control systems is less clear. It should be noted that some industrial control systems do employ a web interface. There are other relevant areas of security that have been previously omitted from early courses because of time constraints. These topics, such as the effect of social engineering and phishing attacks will be included in the next iteration. Also, basic introductions to malware functionality, operation and analysis will be included. These two main topics are more relevant to control system engineers, as they are the threat most likely to be encountered in their daily operations.

Red/Blue Team Exercise

The QUT course development team spent a large amount of time and effort in creating the Red/Blue Team exercise on the 4th day of the course, aiming to produce an environment as detailed and as realistic as possible. This complexity enables students to immerse themselves in the scenario and really invest in their tasks. Overall this has been a great success, with some students becoming too emotionally involved in the scenario. The many ingredients include a realistic corporate network and DMZ, physical separation of red and blue teams into their own areas, CCTV monitoring systems and localized VOIP communications. One of the key areas that has added to the realism of the exercise is the use of real control systems, combined to produce an industrial process that the Blue team must monitor and operate throughout the day. A complex sequence of events must be completed for one instance of the process to be completed. The Blue team is rewarded with points for every time the sequence is completed. The industrial process involves three of the simulators available at the QUT SCADA security research laboratory. These include a water reservoir, conveyer system, and gas pressure system.

While the Red/Blue Team exercise was successful, aspects of the exercise can be improved. Besides fixing bugs in the system, it is important that both teams are monitored closely. We employed CCTV cameras to monitor

the teams as well as network monitoring software, to ensure that Blue team servers continued to function. However the QUT development team realized that a closer monitoring of the network is required, in particular the monitoring of password changes by both the attacking and defending team. In the next course iteration, custom software will be used to monitor password files.

Another important aspect for the Red/Blue team exercise that links with monitoring students is that organisers should ensure that scripted events occur during the 8 hour length of the exercise. The Red Team should not be able to beat the Blue team in the first hour, but should not be stuck for hours on a particular problem either. The Red Team should have to meet a set of achievable goals within certain time restrictions. These do not necessarily need to match or oppose the goals of the Blue team. For example the Red team can be tasked with exfiltrating company secrets while the Blue team's main goal is maintaining the industrial process. Contingencies should be made by the course organizers to ensure that key learning outcomes are made for both the Red and Blue teams equally.

One option for running the Red/Blue exercise is to only have students participate as part of the Blue team as that is where industry will require them to operate. However since the teaching staff have set up the exercises and know all the avenues to access the Blue team network, the exercise would seem too artificial to the students. Ideally, past students should be invited back to play different roles such as the Red Team if they have participated originally as the Blue team. However this scenario is currently difficult, because students travel from all over Australia. It might be possible if the exercise were offered to local students in other award courses such as a Bachelors or Masters degree.

Experiences at UniSA and QUT have shown that large complex practical exercises for cyber security training have a deep impact on students' learning, enabling students to reflect on newly learnt theory and apply new skills and insights to following assignments and later to their workplaces.

7. Conclusion and Future Work

This paper has described two courses developed in two Australian universities – the University of South Australia (UniSA) and the Queensland University of Technology (QUT). From an Australian perspective, our work in developing courses in SCADA systems security aims to educate locally SCADA practitioners with engineering backgrounds and ICT personnel.. Establishing a local facility both to provide training and research into industrial control systems security should have substantial benefit. Establishing these course curriculum and practical laboratories in Australia gives more opportunity for local systems owners and operators to provide feedback so that local conditions can be more easily taken into account.
Another aim is a collaborative effort of two Australian universities - University of South Australia (UniSA) and Queensland Institute of Technology (QUT) towards an international project with Mississippi State University (MSU) in the United States. Plans are underway to engage our respective students in this project which will attempt to implement a trans-Pacific red team/blue team exercise.

Our future plans include expanding our research and education in the area of SCADA and ICS security by developing

- an external penetration hands-on exercise from the UniSA to a QUT laboratory;
- a remote vulnerability testing between laboratories in Australia (QUT) and United States (MSU);
- a working simulation model of ICS that provides accurate responses to sets of inputs (thus allowing some research experimentation to take place without using a physical laboratory)

8. Acknowledgements

The authors would like to acknowledge Mr Cameron Sands and Mr Ben McInerney of AutomateNow for their assistance in developing hands-on exercises for COMP 5062 course intensive week practicals at UniSA described in this paper and Dr Patricia Kelly from UniSA for editorial advice.

9. References

[1] Julia Gillard - Cyber Centre PMC's announcement (Jan 2013) http://www.theaustralian.com.au/national-affairs/defence/julia-gillard-announces-cyber-security-centre-warning-a-long-fight-lies-ahead/story-e6frg8yo-1226559907481, viewed 6 April 2013

[2] Common Cyber Security Vulnerabilities Observed in Control Systems Assessments by INL NSTB Program. Idaho national Laboratory. Idaho Falls, Idaho 83415. November 2008

[3] Morris, T., Vaughn, R. and Sitnikova, E.(2013) Advances in the Protection of Critical Infrastructure Improvement in Industrial Control System Security. Australasian Computer Science Week. January 29 – Feb 1, 2013. University of South Australia, Adelaide Australia.

[4] Vaughn, R., Morris, T., Sitnikova, E. (2013) Development and Expansion of an Industrial Control System Security Laboratory and an International Research Collaboration. 8th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW8). Jan 8-10, 2013. Oak Ridge, TN.

[5] Assante M. J., (2010), Testimony on Securing Critical Infrastructure in the Age of Stuxnet, National Board of Information Security Examiners , November 17, 2010

[6] ITSEAG, Achieving IT Resilience Summary Report for CIOs and CSOs http://www.tisn.gov.au/Documents/ITSEAG+Resilience+Paper+CIO+Report+(PDF).pdf, viewed 6 April 2012

[7] Slay J., Sitnikova E., (2008), Developing SCADA Systems Security Course within a Systems Engineering Program, proceedings 12th Colloquium for Information Systems Security Education, Dallas, US.

[8] Sitnikova E., Slay J., (2012), Pathway into a Security Professional: a new Cyber Security …. ADFC Richmond, Virginia, US

[9] Sitnikova E., Hunt R., (2012), Engaging Students through Reflective Practice Assessment within SSLS course, Orlando, US

[10] Foo, Ernest; Branagan, Mark; Morris, Thomas, "A Proposed Australian Industrial Control System Security Curriculum," *System Sciences (HICSS), 2013 46th Hawaii International Conference on* , vol., no., pp.1754,1762, 7-10 Jan. 2013

[11] Hinett, K (2002), *Developing Reflective Practice in Legal Education*, UK Centre for Legal Education.

[12] Kolb, D. (1984), *Experiential learning: experience as the source of learning and development*, Kogan Page, London.

[13] Schon, D. (1987), *Educating the Reflective Practitioner*, San Francisco: Jossey Bass

[14] Boud, D., Keogh, R. & Walker, D. (1985), *Reflection: turning experience into learning*, Kogan Page, London.

[15] Philip L.,(2006), Encouraging reflective practice amongst students: a direct assessment approach, GEES Planet Special Edition- Issue 17 http://www.gees.ac.uk/planet/p17/lp.pdf viewed 27th February 2012.

[16] Kaider, F., (2011), Introducing undergraduate electrical engineering students to reflective practice, proceedings of the 2011 AAEE Conference, Fremantle, WA.