Proceedings of the 12th Colloquium for Information Systems Security Education
University of Texas, Dallas
Dallas, TX June 2 - 4, 2008

Developing SCADA Systems Security Course within a Systems Engineering Program

Jill Slay and Elena Sitnikova, *University of South Australia*

Abstract — This paper responds to the need to understand the nature of SCADA systems security concepts, their important role in the Australian nation's critical infrastructure protection and highlights the necessity of this as a specialist engineering course within a systems engineering program. It defines the nature of the field and the roles and qualifications of system engineering practitioners who serve in the field. It emphasizes the role of the specialist course within the tertiary program that produces potential systems engineering specialists with the knowledge required to achieve robustness and resilience of critical infrastructure systems and services.

Index terms — SCADA Systems Security, Critical Infrastructure Protection, Systems Engineering

I. Introduction

Supervisory Control and Data Acquisition (SCADA) systems are used for remote monitoring and control the nation's Critical Infrastructure (CI). In Australia, there are several CI such as electricity, gas, water, waste treatment, communications and transportation [1]. Researchers refer to protecting them as Critical Infrastructure Protection (CIP).

There are a range of potential threats to the Australian national CI: terror attacks, national disasters, accidents, poor management, inappropriate government polices and inadequate technology and systems designs. Similarly there are a range of services which make up the CI and there are interdependencies within them. For example, a cyclone has effect on both transport and the electricity infrastructure. So we find that we are dealing with interdependent and complex socio-technical systems of a multidisciplinary nature when we begin to expand on the role of SCADA within the Australian national CI.

Several papers have shown the application of Systems Engineering (SE) methodologies in Critical Infrastructure Protection (CIP) research. For example, Ibarra et all [2],[3] are using SE approaches for identifying the most critical elements of the transportation CI. Thus, researchers need to be knowledgeable in SE principles to be able to apply them to CIP research. Therefore, we can postulate that, to be able to understand concepts of critical infrastructure protection and security, systems engineering practitioners also need to be educated in the specialist course in the field of SCADA Systems Security.

Also in [1],[4],[5] some cultural issues that SCADA networks services are facing today are discussed and these highlight the gap between specialists with engineering skills and the specialists in network security with IT background who work in the field. We believe that providing education in SCADA SS will be able to help in filling this interdisciplinary knowledge gap.

Thus, the purpose of this paper is two-fold. The first aim of this paper is to discuss the role of SCADA systems in Australia and the need to secure them, and then to show the necessity of the SCADA SS course within a SE tertiary program.

The second aim is to propose SCADA SS graduate-level course outline. The course will aim to produce potential systems engineering specialists with the knowledge required to achieve robustness and resilience of critical infrastructure systems and services that may be threatened by man-made or natural disasters.

II. What is a SCADA System?

A SCADA system is used for gathering real time data, controlling processes and monitoring equipment from remote locations in automated systems. As described in [4] they can be used to automate processes such as:

- Electricity power generation, transmission and distribution,
- Oil and gas refining and pipeline management,
- Water treatment and distribution,
- Chemical production and processing,
- Railroads and mass transit.

Although SCADA is most popular in large automation networks for utility companies, these systems can be used for almost any automated process. Any company using assembly lines, such as a bottling factory, can also benefit from a SCADA system. Entire plants can be automated, making manufacturing more efficient and reliable.

Defence and Systems Engineering Institute,
University of South Australia,
Mawson Lakes, SA5095, AUSTRALIA
Email: jill.slay@unisa.edu.au, elena.sitnikova@unisa.edu.au

A SCADA network is essentially a collection of servers, clients and field devices connected together by a communication network. The process control and logic is controlled by master servers. The information used by the servers is collected via controllers/sensors. The clients are interfaces used by users to interact with the system. Servers are generally located in the main plant/station. They communicate with the controllers which can be located inside the plant or at remote locations. Programmable Logic Controllers (PLC) are placed onsite wherever equipment needs to be monitored or controlled. Essentially, a SCADA network can be very large and cover a hundreds of kilometres, especially in the case of utility plants where controllers need to be placed along power lines or gas pipelines.

The size and complexity of a SCADA network varies depending on the process that it controls, and also the size of the utility/business which runs it. The task will primarily affect the size and sophistication of the SCADA network. A typical electrical utility could have up to 50,000 data collection points in its network [6], whilst a simple bottling factory may only require one server and a small number of PLC's. Large companies are more likely to have extra connections and features on their network.

A larger SCADA network will generally include [7]:

- More than one server in the control system area.
- A HMI, Human Machine Interface, for engineers to interact with the system.
- A large number of PLC's (up to hundreds of kilometres away from the main plant).
- Remote connections for engineers, contractors or third party entities.
- A communications network for the devices to communicate over.

III. What is the Need to Secure SCADA Systems?

A. Threats to Critical Infrastructure – An Australian Perspective

Threats can take various forms that could be classified in two major categories:

- natural threats or disasters such as fires and floods; and;
- man-made threats such as terrorism, internet threats (viruses and worms), hackers attacks, technological errors.

SCADA systems are responsible, nationally and internationally, for controlling and monitoring power and utility plants. If these systems have security vulnerabilities, then they become a potential target to cyber attackers or terrorists. If terrorists can gain control of a SCADA system, they can then threaten the complete critical national power, gas, oil, water, sewage and IT and telecommunications infrastructure. The Australian situation is a complex one because of the unique nature of the Australian continent, vastness of the country and the remoteness of some of the power and utility plants and field stations. An example from South Australia and its electricity utility company ETSA illustrates this. The SCADA system provided to ETSA by its integrator provides coverage to over 178 200 square kilometres of networks. The networked SCADA system included 25 000 physical I/O points and over 100 000 tags. The system monitors daily data for currents, temperatures, various power variables, load shedding systems and fire alarms, to improve response time for network faults and increase security of the operation.

Most significant research in the area of SCADA system security, and also most statistical data, originates in the USA [8-12]. However, as described in [13] one significant example of a SCADA system breach is an Australian case which is widely quoted in research [14],[15] .

Maroochy Shire Council on Queensland's Sunshine Coast was experiencing some problems with its new wastewater IT system. Communications sent by radio link between wastewater pumping stations were being lost, pumps were not working properly and the alarms put in place to alert staff of the faults were not going off.

Initially it was thought there were teething problems with the new system. Eventually an engineer began to monitor every signal passing through the system and discovered that someone was hacking in and deliberately causing the problems. In time the perpetrator, Vitek Boden, was located, arrested, and gaoled. The former contractor used a laptop computer and a radio transmitter to take control of 150 sewage pumping stations. Over a three-month period, he released one million litres of untreated sewage into a 6 storm water drain, which in turn flowed to local waterways. The court commented that the attack on the system was motivated by revenge after the contractor failed to secure a job with the Council.

This case is used widely around the world as an example of the potential for damage should SCADA systems become insecure. (For example, it was cited in the US President's Information Technology Advisory Committee report on the efficiency of technical approaches to IT security.) At the time it was the only known successful attack on a SCADA system linked to public infrastructure. This case also has to be viewed in the light of more general Australian data on cyber crime, particularly network security breaches. The increase in electronic attacks on 127 Australian companies surveyed in 2003 [16] saw an average rise in financial loss of 20%

over 2002, bringing the average sum lost to approximately $116,000 per company surveyed. The survey also revealed that organisations which make up part of Australia's critical national information infrastructure (CNII) reported a greater loss, 50% compared to 42%, than those organisations which are not part of Australia's CNII. Other key findings in this survey showed that more organisations experienced electronic attacks that harmed the confidentiality, availability and integrity of network data or systems in 2004, than did in 2003. The increase reported was from 42% in 2003 to 49% of organisation surveyed in 2004. Most attacks were sourced externally (88%) but fewer organisations experienced external attack than in 2003 (91%). For the third consecutive year, infections from viruses, worms or Trojans were the most common form of attack reported, accounting for 45% of total losses in 2004. Other prevalent forms of electronic crime were fraud, followed by abuse and misuse of computer network access or resources.

B. The Need to Secure SCADA Systems

Much research has identified the SCADA networks as a potential "weak" point in a power utilities networks. SCADA systems are responsible for controlling and monitoring many of our power plants. If these systems have security flaws, then they become a potential target to attackers. Gaining control of a system can lead to the entire plant being shut down. According to Sandia National Laboratories, SCADA systems are used by 270 utilities in the U.S. This amounts to eighty percent of the nation's power [6]. This makes SCADA systems the most common system for controlling and monitoring utility plants. With so many plants using SCADA, this makes it vitally important to secure these systems from attackers.

Fernandez in [6] has given strong reasons for the need to secure the SCADA systems which control the critical utility infrastructures such as power, oil, gas and water. The authors emphasise the potential risks by looking at the financial loss caused by recent major blackouts across the world. Not only do they identify financial risks, they point out other factors which are affected by blackouts. For example, on the 25 August 2003, in the United States, more than 100 power plants were shut down. This led to 50 million people in the U.S. and Canada being affected. More importantly though, it lead to the closure of 10 major airports and also shut down the New York subway system. The loss of critical infrastructure such as Airports is a major risk which emphasises the need to protect the SCADA systems, especially if the cause is cyber terrorism.

Oman in [12] attributes the recent concerns to mainly be generated by political means. One of the factors identified is the recent increase in international and domestic terrorist activity against North America. There have been recommendations and documents developed by various U.S. government agencies. This emphasises that the government, in this time of terrorist threat, understands the importance of securing utilities that are crucial to the infrastructure of their country. The focus of his paper is on gaining remote access to the substations located at various points in the network and provides an example of how an "open" SCADA network can be penetrated by a potential intruder.

National Communication Systems [7] have identified that if a SCADA network is interconnected with the corporate network, then it is exposed to the same risks as those experienced in an attack on a conventional network. Companies may be under the false impression that a SCADA network is safe and lies on a separate network. However, once these networks are interconnected, then any attacker who breaches the corporate network has the ability to get at any device on the network, especially the SCADA system.

C. Cultural Issues that SCADA Systems are Facing Today

Security focus group from the Idaho National Laboratory (INL) and the New York State (NYS) of Cyber Security and Critical Infrastructure discussed a current situation that SCADA systems are facing today and released a set of guidelines that provide specific requirements for such systems [5]. The prime goal of those guidelines is to consider security of critical infrastructure systems in total as a system and to make a system more secure rather than paying separate attention to software and hardware security.

Historically, the role of SCADA systems creators was to detect physical failures to avert major power outages and manufacturing problems. They assumed such control systems (engineered 20 years ago) would be fully isolated, but in a modern world they are not isolated any more. The integration of SCADA systems with a steady stream of new technologies such as the Internet and wireless networks using a range of protocols means that critical infrastructure systems are seen as extremely vulnerable to cyber terrorist attacks.

According to INL's infrastructure protection strategist Michael Assante, while for many managers and engineers responsible for SCADA systems physical security has always been a priority and also for many of them information security is a new field, they have to understand the importance of CI systems' cyber security requirements, associated risks and thus make a deployment of proper security measures. This cultural issue is still to be overcome. Thus, training managers and engineers in the field will help to overcome this barrier.

In some other literature it has been also mentioned that SCADA system vulnerabilities can increase from a lack of communication between IT and engineering departments [1]. Slay highlighted in [4] that engineers are responsible for deploying and maintaining SCADA systems, whilst network security comes from an IT background. The gap between these two disciplines needs to be bridged to recognise, identify and mitigate against the vulnerabilities in these SCADA networks. Broader awareness and the sharing of good practice on SCADA security between utility companies themselves is a key step in beginning to secure the nation's critical resources.

IV. Developing SCADA SS Course in a System Engineering Program

Systems Engineering that defined in the INCOSE Technical Vision [17] is:

Systems engineering is a professional endeavor that leads to the engineering of a system of humans, organizations and technologies through knowledge management efforts associated with bringing the perspectives of all stakeholders to the associated issues to bear, such as to enable the appropriate: definition of the system to be engineered such as to achieve needed capabilities and fulfil requirements; development of the system through appropriate architecture, design, and integration efforts; and ultimate deployment of the system in an operational environment and associated maintenance and reengineering of it throughout a useful lifetime of trustworthy service to these stakeholders.

Systems engineering as a discipline was developed as means to address the design, implementation and operation of large, complex technical systems. SE is seen as inherently multidisciplinary in nature and over the years the problems it tackles have become more complex. The increase in complexity has been noted by Royal Academy of Engineering (RAEng) that suggests a number of multidisciplinary principles to maximize the success of creating systems that work. While the RAEng in [18] admits that engineers who design integrated systems and especially systems engineers are different from other engineers, they argue that every engineer has to *think* systems. By providing an education on CI and control systems security to engineers we are enhancing their capabilities to

- *think* of SCADA systems as a whole , and
- develop and service interdependent and complex control systems within the Australian national CI.

The SCADA SS course has both an inherent obligation and opportunity to influence the field in the academic systems engineering programs within the Defence and Systems Institute (DASI) at the University of South Australia (UniSA). To be credible, though, our initiatives must be based on understanding the academic settings, the programs structure and the scope and content of the course curriculum.

An approach for the SCADA SS course development has been proposed and is shown in Figure 1. First, we start with the identification of government and industry needs in engineering competencies for CI systems and services. Then two streams for existing SE and SCADA SS programs are required for information gathering and analysis following by identification of the topics for both streams. The next step is mapping identified topics with the required engineering competencies. The final step is to propose a curriculum for the specialist course - SCADA SS.

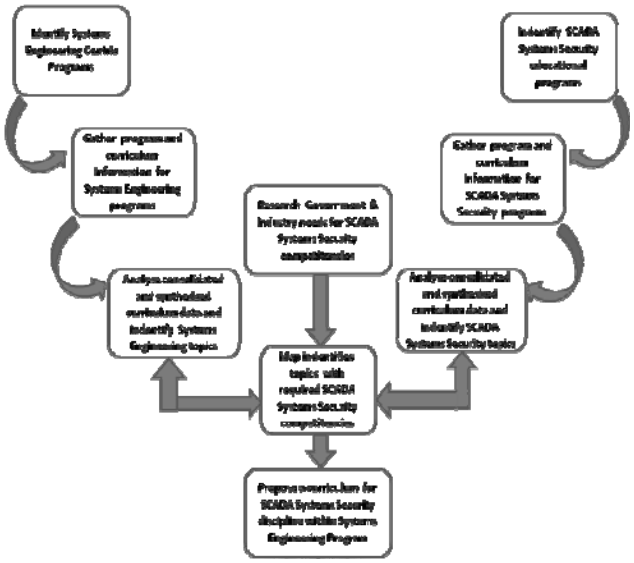

Figure 1: An Approach for the SCADA SS course development

A. Australian Government and Industry Needs in Engineering Competencies in Critical Infrastructure Systems and Services

In March 2004 the Australian Government outlined its CIP strategy for the first time. Since then, under government administrative arrangements through the Attorney General's Department (AGD) and the Department of Prime Minister & Cabinet (PM&C) (jointly responsible for the coordination of security related matters) a statement of principals for critical infrastructure protection has been provided and it outlines major tasks and responsibilities.

The Attorney-General's Department Trusted Information Sharing Network (TISN) was established in 2003. It is made up of 9 sector- specific Infrastructure Assurance Advisory Groups (IAAG) (energy, transport, health,

communications, food chain, water services, baking and finance, mass gathering) and Expert Advisory Groups (EAG) (CIP, IT security, SCADA Community of Interest) which provide advice on specific issues across IAAGs [19].

In some parts of Australia as much as 90% of the CI is privately owned. As such, the Government (both State and Federal) along with individual organisations, carries out CIP. The Federal Government admits that CIP is a multidisciplinary domain and is coordinating the blending of existing disciplines [20]:

- Law enforcement & Crime Prevention
- Counter terrorism
- Australian National Security and Defence
- Emergency management
- Business community planning
- Protective security (physical, personnel and procedural)
- E-security
- Australian national disaster planning
- Risk management
- Professional networking
- Market regulation, planning and infrastructure development

With a growing tendency towards cyber terrorism, effective e-security takes one of the major roles in SCADA systems defence. Therefore, the Australian Government's primary objective is to increase competencies of owners and operators of critical infrastructures by providing them with access to the world best practice on cyber security and training in industrial control systems security.

The Australian Government is seeking to achieve this objective by increasing competitencies in:

- Vulnerability of the critical infrastructure systems
- SCADA systems security technical issues
- Identifying and managing security related risks
- SCADA security public polices and security standards.

B. Systems Engineering Graduate Programs at the University of South Australia

There are two categories of tertiary academic programs that incorporate systems engineering: systems-engineering-centric and domain-centric systems engineering [21] At DASI, UniSA we have only systems-engineering-centric programs. This category includes only those basic- and advanced degree programs with a designated concentration (discipline-like focus) in systems engineering, where this field is the intended major area of the study.

DASI has many years of expertise in systems engineering any many years of successful running graduate courses within SE-centric category programs. The structure of DASI's SE graduate program is aligned with the layered framework proposed in [22] and shown in Figure 2.

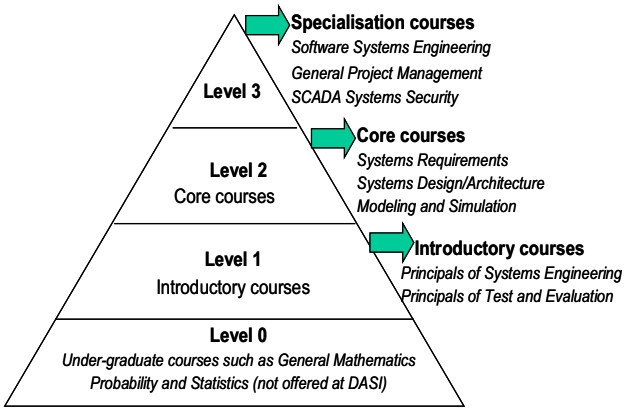

Figure 2: A Framework for a Systems Engineering Program at UniSA.

The role of DASI in the development of SCADA SS course is a very new one. However, those who are being prepared to work in this area have a required combination of expertise in systems and software engineering, forensic computing, control systems, critical infrastructure protection and IT security.
The SCADA SS course is going to be offered as one of the specialisation courses under Level 3 within a SE program.

C. Critical Infrastructure and Control Systems Security Programs

1) Training programs

The number of institutions providing training in SCADA security is very limited. Research of the courses available on the web showed that companies such InfoSec Institute and SANS (in incorporation with the U.S. Department of Homeland Security's (DHS) National Cyber Security Division (NCSD)) are offering such courses in US.

InfoSec provides 3 day courses which include classroom instructions in security architecture and implementation[23]. Labs are hand-on with common SCADA security components. At the end of the course participants are taking SCADA security Professional certification exam.

SANS is offering 2 programs with 2 courses each for students with different areas of SCADA security expertise[24]:

- SS1 Introductory SCADA Security Course (for people with no or limited IT background)
- SS2 IntermediateSCADA Security Hands-on (for people with IT background)
- SS3 Solution for Process Control Security (for people with no or limited IT background)
- SS4 Securing Control Systems and SCADA environments (for people with technical IT background)

Homeland Security had published Critical Infrastructure and Control Systems Curriculum draft version 1.01 that is designed to assist in teaching in the area of SCADA security public polices, technical issues and managerial principles.

2) Training Exercises & Workshops

The U.S. Department of Homeland Security's (DHS) National Cyber Security Division (NCSD) Homeland successfully executed cyber security exercise CyberStorm I exercise in 2006 and CyberStorm II in March 2008. Those exercises allowed participants (on a need to know basis) to respond to a variety of cyber and simulated attacks against critical infrastructures and to collaborate at the operational, policy and public affairs levels [25].

The Australian Attorney General department is paying significant role in training in the area and had delegated participants to attend five day International SCADA Cyber Security training and workshop provided by Homeland Security in INL in both 2007 and 2008. These are only available to the SCADA community of interest

D. SCADA Systems Security Course Outline[1]

The SCADA SS course is intended for engineers and managers serving in the field of CI and designed to teach a course in the policymaking and decision strategies, managerial and technical risks assessments and their mitigations required to achieve and sustain robustness and resilience of CI services that may be attacked by threats of any kinds. The knowledge gained during the course is aimed to be applicable for engineering practitioners from broad range of infrastructures, their technology systems, and kinds of threats to which they may be exposed. Despite the fact that the course materials are based primarily on the role and examples of SCADA systems in gas, water and cyber infrastructures, they can be customized to meet the needs and requirements of the particular circumstances.

[1] Curriculum designed with the use of materials provided by US Department of Homeland security – *Critical Infrastructure and Control Systems Security Curriculum*, Draft Version 1.0, Feb 28, 2007

The subject is inherently interdisciplinary, and thus, the course is also.

The aim of our course is to understand fundamental principles required to:

- understand a range of CI services and their interdependencies ;
- show an understanding of CI vulnerability;
- deal with "all threats", not only terror attacks, but national disasters , unintended accidents, poor management, results of inappropriate policy, inadequate technology and systems design.
- understand and demonstrate engineering approaches: design constraints, key technologies;
- effectively manage high-impact risk to CI services;
- design and implement public policies and business strategies that mitigate such risks;
- gain homeland security skills by using exercise learning techniques to assess and secure SCADA systems.

The syllabus includes the following topics:

- SCADA systems in the CI
- Vulnerability of the CI systems
- SCADA Security Methods and Techniques – engineering approaches
- Managing organisations and security related risks
- Overview and demonstration of a tool for self-assessment of security level in organisation
- Securing Networks for organisations.

Assessment

The pedagogical aspects of the course are based on Bigg's [26] theory of reflective knowledge. Thus a criterion-referenced assessment is employed. "Once you understand a sector of knowledge it changes that part of the world; you don't behave towards that domain in the same way again" (Biggs 1999).

Assessment will include:

- In-class activity (group exercises) 30%
- Post-class Essay 70%

Defining graduateness

In the past half decade the skills of Australian graduates have drawn much criticism with particular attention to the disparity between graduates' skills and industry demand [27]. In the United States the Accreditation Board for Engineering and Technology (ABET), like other engineering accreditation agencies outside the US, underlines the importance of having clearly specified objectives and graduate qualities which are reflected in the mission statements of educational programs and

embedded in the assessment of courses [28]. ABET, according to Felder and Brent in [28] underline the importance of not only being able to apply knowledge of mathematics, science and engineering but also the ability to communicate this knowledge effectively. At the University of South Australia (UniSA), these graduate 'end points' or qualities are addressed through a construct of seven Graduate Qualities which underpin assessment and curricula and listed below.

Table 1: The University of South Australia Graduate Qualities [29]

1	*A graduate of the UniSA operates effectively with and upon a body of knowledge in sufficient depth to begin professional practice*
2	*…is prepared for life-long learning in pursuit of personal development and excellence in professional practice*
3	*…is an effective problem solver, capable of applying logical, critical and creative thinking to a range of problems*
4	*…can work autonomously and collaboratively as a professional*
5	*…is committed to ethical action and social responsibility as a professional and a citizen*
6	*Communicates effectively in professional practice and as a member of the community*
7	*Demonstrates international perspectives as a professional and as a citizen*

The aim of our course development process is to provide a high quality learning environment that will prepare its students for life long learning. This means that while the graduate quality 1 (body of knowledge), is of primary importance, the method in which this knowledge is gained and applied is of equal importance and in fact to some degree defines graduateness. With this in mind, all assessment pieces define which graduate qualities are being developed. For example, if group skills are desired then group assignments which develop research skills in the course context are used. If individual report writing and information literacy skills are required then individual reports are requested. Students have to be taught, or are asked to review, report writing, information literacy or group skills simultaneously with the development of the body of knowledge in the required area.

In this course development there has to be a particular emphasis on the relationship between graduate quality 6 (effective communication) and the clarity of thought surrounding a body of knowledge. In students work, not only does effective communication reflect the disciplinary knowledge but it is commensurate with deep level of knowledge. In other words, the better a student is able to express this knowledge (simply, clearly, cohesively), the deeper the learning evident.

We have also chosen a focus on graduate quality 3 (problem solving, applying logical, critical and creative thinking) and graduate quality 5 (ethical action and social responsibility) so that the problem solving could be taught in the context of SCADA systems potential treats and risks investigations.

Limitations

At this stage, we are aiming to develop a course which will produce foundational knowledge in SCADA Systems security. This course is not intended to produce the specialist expertise in the field, but does lay the foundational knowledge in 'what is a SCADA system and what requires to secure it?' The purpose of the course is to focus on identifying high impact risks to CI services and effectively manage them; and also to use government polices, business strategies that mitigate such risks. Higher level knowledge and skills in the field will be developed in future developed courses.

CONCLUSION

The conclusion from a review of literature and evaluation of academic practice in areas of CI systems security is that there is an industry-based and social need to teach SCADA SS course

At the basis of the proposed course curriculum is the concept of using a specially designed approach, beginning with indentifying of the Australian Government and industry needs in engineering competencies for CI systems and services. This continues with examining streams for existing SE and SCADA SS programs followed by mapping identified topics with the required engineering competencies, and finishing by proposing a SCADA SS course outline.

SCADA SS course would be appropriate to industry and aims to produce specialists knowledge for the graduates required for CI systems security operations and services.

REFERENCES

[1] ITSEAG, *SCADA Security – Advice for CEOs : Executive summary,* viewed 27 Feb 2008 *<http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~20+JAN+SCADA+CEOCleaned.doc/$file/20+JAN+SCADA+CEOCleaned.doc>,*

[2] Ibarra, G., Stracener, J., Szygenda, S., (2007) *A Systems Approach to a Methodology for Identifying the Most Critical Links of a Highway Network*, CSER 2007 conference proceedings, Hoboken, NJ, USA, March 14-16 2007,

[3] Ibarra, G., Stracener, J., Szygenda, S., (2006) *Transportation in the Critical infrastructure: A Holistic Approach Using Systems Engineering Methodologies for Assessing Risk and cost Impacts Due to Highway,* Schafer School of Engineering press, Stevens Institute of Technology, Hoboken, NJ, ISBN-10: 0-9787122-0-X, Volume 1, pp. 55-71,

[4] Slay, J. Miller, M. (2006) *A security Architecture for SCADA Networks*, 17th Australasian Conference on Information Systems, December 2006,

[5] Lemos, R., *SCADA System Makers Pushed Toward Security,* viewed 2 March 2008 <http://www.securityfocus.com/news/11402>
[6] Fernandez, J.D. & Fernandez, A.E. 2005, 'SCADA Systems: Vulnerabilities and Remediation', *Journal of Computing Sciences in Colleges*, vol. 20, issue 4, pp. 160-168,
[7] NCS, 2004, 'Technical Information Bulletin 04-1', National Communications System, viewed 9 March 2008, <http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf>.
[8] Byres, E & Lowe, J, 2004, 'The Myths and Facts behind Cyber Security Risks for Industrial Control Systems', PA Consulting Group,
[9] Dzung, D., Naedele., M, Von Hoff, T. & Crevatin, M, 2004, 'Security for Industrial Communication Systems', Proceedings of the IEEE, 2005, vol. 93, pp. 1152-1177,
[10] GAO 2004 'Critical Infrastructure Protection – Challenges in Securing Control Systems', United States General Accounting Office, viewed 5 March 2008, <http://www.gao.gov/new.items/d04140t.pdf>,
[11] Katipamula, S., Hadley, M. & McKenna, T 2004, 'Evaluation of Symantec Security Products in an AREVA T&D-Implemented SCADA Environment using ICCP Communication Servers', Battelle Pacific Northwest Division, viewed 15 July 2005, <http://enterprisesecurity.symantec.com/Content/displaypdf.cfm?PDFID=804>,
[12] Oman, P., Schweitzer, E. & Frincke, D 2000, 'Concerns About Intrusions into Remotely Accessible Substation Controllers and SCADA Systems', CiteSeer, viewed 16 March 2005, <http://citeseer.ist.psu.edu/oman00concerns.html>,
[13] Slay, J & Miller 2007, 'The Maroochy Water SCADA Breach: Implications of Lessons Learned for Research', in Advances in Critical Infrastructure Protection. Springer, Boston, USA, pp. 73-82.
[14] PITAC 2005, US President Information Technology Committee, National Coordination Office for Information Technology Research and Development, viewed 8 March 2008 <www.nitrd.gov>,
[15] Hughes G., 2003 The Cyberspace Invaders, The Age, 22 June 2003,
[16] Auscert 2004, *Computer Crime Survey*, viewed 5 Feb 2005 www.aucert.org
[17] INCOSE (2005) INCOSE Technical Vision, Version 1.1, May.
[18] Royal Academy of Engineering, *Creating systems that work-Principles of engineering systems for 21th Century*, RAEng, 2007
[19] TISN home web page, viewed 14 March 2008 <http://www.tisn.gov.au/agd/WWW/TISNhome.nsf/Page/Business-Govt_partnership>
[20] TISN 2004, Critical Infrastructure Protection National Strategy, V.2.1, viewed 14 March 2008, <http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~National+CIP+Strategy+2.1+final.PDF/$file/National+CIP+Strategy+2.1+final.PDF>,
[21] Fabrycky, W., (2007) *Understanding and Influencing SE in Academia*, INCOSE *INSIGHT*, Vol. 10, No3, pp.7-8.
[22] Jain, R., Squires, A., Verma, D., Chandrasekaran, A., *A Reference Curriculum for a graduate Program in SE*, INCOSE *INSIGHT*, Vol. 10, No3, pp.9-11.
[23] INFOSEC, viewed 14 March 2008 <http://www.infosecinstitute.com/courses/scada_security_training.html>,
[24] SANS, viewed 14 March 2008 <http://lists.iinet.net.au/pipermail/scada/2005 December/000750.html>,
[25] CyberStorm info on web viewed 14 March 2008 <http://www.dhs.gov/xprepresp/training/gc_1204738275985.shtm>,
[26] Biggs J., *Teaching for quality learning at university: what the student does.* Buckingham, UK: Society for Research into Higher Education, Open University Press, 1999,
[27] J. Borthwick and R. Wissler, (2003), *Postgraduate research students and generic capabilities : online directions,* vol. . Canberra, Australia: Department of Education, Science and Training,
[28] R. M. Felder and R. Brent, (2003), *Designing and teaching courses to satisfy ABET accreditation criteria*, Journal of engineering education, vol. 92, pp. 7-25,
[29] University of South Australia, "Graduate qualities," vol. 2005: University of South Australia, 2005.