8-23-2010

Which Organisational Model Meets Best Practice Criterion for Critical Infrastructure Providers: An Examination of The Australian Perspective Based on Case Studies

Andrew Woodward
Edith Cowan University

Craig Valli
Edith Cowan University

Originally published in the Proceedings of the 1st International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 23rd August 2010

WHICH ORGANISATIONAL MODEL MEETS BEST PRACTICE CRITERION FOR CRITICAL INFRASTRUCTURE PROVIDERS: AN EXAMINATION OF THE AUSTRALIAN PERSPECTIVE BASED ON CASE STUDIES

Andrew Woodward and Craig Valli

secau – Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia
a.woodward@ecu.edu.au

Abstract

While it is recognised that there must be segregation between corporate and process control networks in order to achieve a higher level of security, there is evidence that this is not occurring. Computer and network vulnerability assessments were carried out on three Australian critical infrastructure providers to determine their level of security. The security measures implemented by each organisation have been mapped against best practice recommendations for achieving segregation between process control and corporate networks. One of the organisations used a model which provided a dedicated information security team for provision of security for the process control networks. One of the other organisations relied heavily on outsourcing for their IT security, and a third used in house corporate IT for their process control security. It was found that the organisation using a dedicated IT security team that worked within the process control group achieved the highest level of security when mapped to best practice. This paper concludes that best practice recommendations for critical infrastructure providers should also include guidelines for the organisational structure, and further, that dedicated IT security personnel be placed within the process control group.

Keywords: SCADA security, critical infrastructure protection, organisational model, operational technology, information technology

INTRODUCTION

Process control systems (PCS), of which supervisory control and data acquisition (SCADA) systems are a subset, are used by critical infrastructure operators to regulate and manage the operation of critical systems such as power, water and gas. In addition, these systems control everything from traffic lights through to large scale refineries and mining operations. All critical infrastructure providers also rely upon these systems for safety and reliability, through continuous monitoring and operation. These systems were originally designed around reliability and safety, and if they were network connected they were connected on isolated internal networks for the purposes of control and management; essentially a closed system. Typically in these situations security was not a consideration due to the isolated nature of the systems and their closed nature. It should be remembered that these systems were implemented also in an era when computing and information technology will also largely conducted in isolated installations or laboratories around the globe (Stouffer *et al*, 2008).

With advances in technology, we are becoming increasingly interconnected and interdependent on these connections for the full functioning of modern society. One of the main conduits and enablers for this has been the rapid expansion of the Internet. Correspondingly, as a result of the growth of the Internet there has been a convergence on the TCP/IP protocol suite as the dominant network protocol for business and industry (Steenstrup, 2010). This has seen many hardware and software vendors, including SCADA vendors, align their products with this kind of reality (Igure *et al*, 2006).

The increased interconnection of SCADA systems to corporate networks is a significant threat in itself, enabling and making them accessible to undesirable entities. Be it directed attacks, opportunistic scanning or malfeasant insiders (Jackson-Higgins, 2007), these once stand-alone systems are now vulnerable to a range of new attack vectors. While insider malfeasance may only account for some 20% of attacks against a system, the percentage of the costs related to insider attacks is nearer to 80% (Baker *et al*, 2009). The most infamous of the intentional insider attacks against a critical infrastructure provider is the case of Maroochydore shire. Their SCADA system was attacked by a person who had been employed to install the system after a request for employment was turned down (Smith, 2001). The attacker stole a laptop when he left which contained all of the tools and codes required to remotely operate the control system, and it took some time for the operators to locate the source of the issues he was causing. Additionally, most security measures are outward facing, and are not intended to detect against insider malfeasance. Insider attack must be a significant concern for CIPs, and gives further weight to the need for internal segregation between control system and corporate networks.

The research reported in this paper was based on the examination of a number of case studies conducted under the Federal Governments computer and network vulnerability assessment (CNVA) program. The CNVA program is an Australian Government grants scheme developed to help ensure the security of Australia's critical infrastructure (TISN 2008).

RECOMMENDED BEST PRACTICE FOR SECURING SCADA

This paper drew on a range of literature in order to create a composite, best practice list of features and strategies for securing process control systems, and as a guideline for measuring the compliance of an organisation against the organisational model. The first piece of literature used for this purpose is the NIST Guide to industrial control system security (Stouffer *et al*, 2008). This guide was produced by the National Institute of Standards and Technology (NIST), a United States Government Organisation, and the guide itself is put forward as recommended best practice by US-CERT. In addition to using the NIST guide as a reference point for determining effectiveness of the organisational structure, a range of other network security best practice measures have also been used including ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems (ISA, 2007), Idaho National Labs Control Systems Cyber Security – Defense in Depth Guide (INL, 2006).

Table 1: Common methodology used to assess the three organisations. Multiple other methods used for other CNVAs, components of assessment all align with NIST best practice.

Category	*Specific Measures*
Firewall	External
	Multiple
	Multiple (different vendors)
	Firewall rule sets configured correctly
	Firewall OS / firmware patched?
Network Segregation	DMZ between corporate and PCS
	DMZ between Internet and Corporate
	Logical segregation through VLANs and subnets
	Access Control lists on border routers
	Intrusion Detection
Remote Access	Secure authentication method
	Two factor authentication
	RSA token authentication
Documentation	Policies current
	Policy audited or enforced?
	Network topology diagrams current
	Network topology diagrams available

ORGANISATIONAL STRUCTURE TYPES

The structure of the three organisations in terms of their positioning of information security management, or provision of IT security services is given in figure 1. The structure represented as organisation 1 had a dedicated Information Security Manager as well as system administrators responsible for the security and operation of the process control networks embedded in the SCADA division of the organisation.

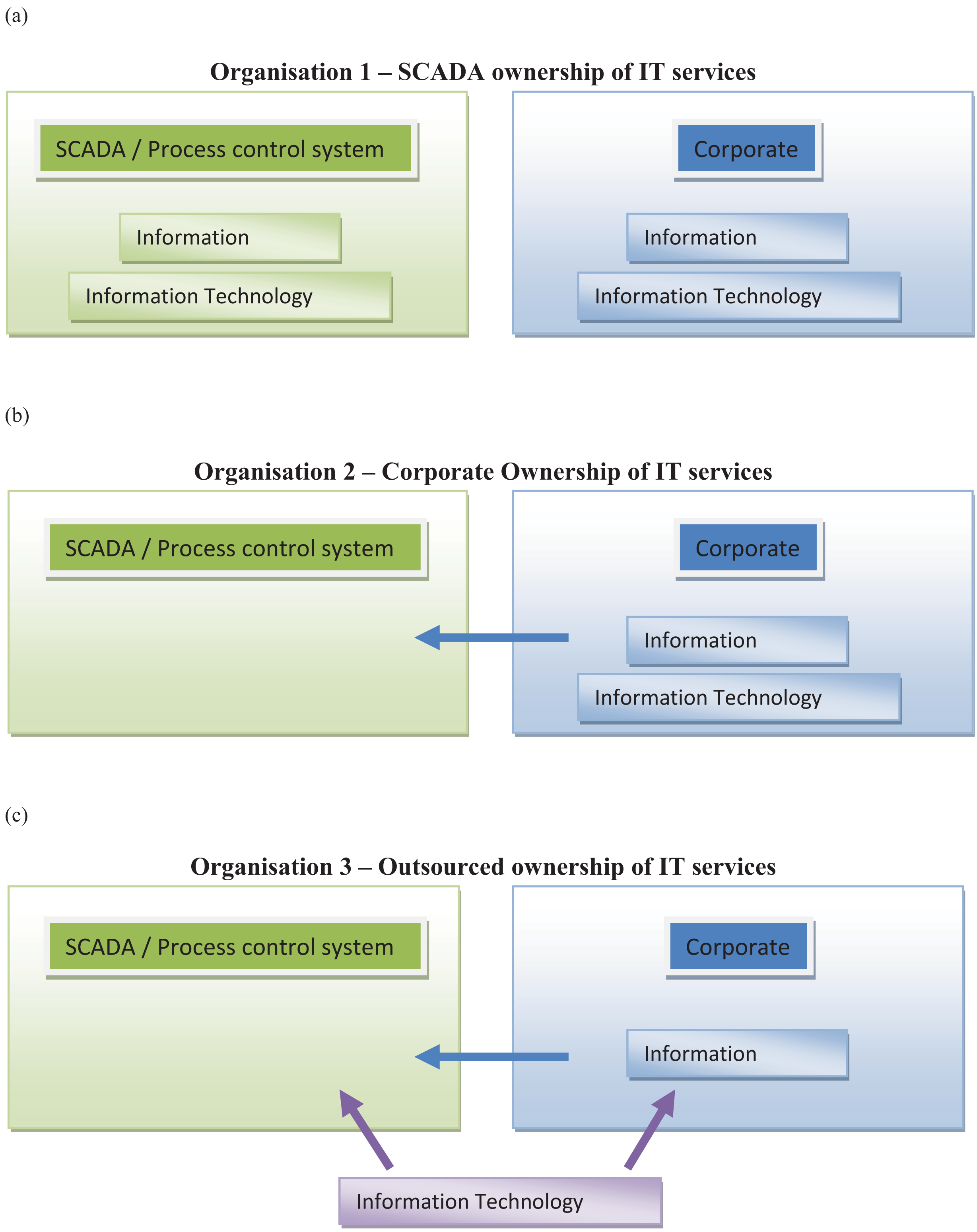
(a)
Organisation 1 – SCADA ownership of IT services
SCADA / Process control system
Information
Information Technology
Corporate
Information
Information Technology
(b)
Organisation 2 – Corporate Ownership of IT services
SCADA / Process control system
Corporate
Information
Information Technology
(c)
Organisation 3 – Outsourced ownership of IT services
SCADA / Process control system
Corporate
Information
Information Technology

Figure 1: Three different organisational models of placement of the information security (IS) team placement relative to SCADA / process control systems. (a) This organisation has a dedicated IS team in the SCADA section of the organisational

model in addition to the corporate IS team. (b) This organisation has no dedicated in house SCADA based IS team, and relies upon the corporate IS team to provide IT security for their control system infrastructure. (c) Organisation three out sources it's IT systems to a third party, but does still retain a corporate IS manager.

REPORTED ISSUES FROM THE CNVA CASE STUDIES

After establishing a baseline for what security measures a CIP should have in place, results of vulnerability assessments carried out on Australian CIPs was then examined. The organisations represented here were participants in a computer and network vulnerability assessment, a national program supported by the Australian Federal Government. The three organisations used for this paper were chosen as they were assessed using a common methodology, and given that other variables are not controlled, it is hoped that their relative overall security level should be comparable, The generic security issues found in the Australian CNVAs conducted using a common methodology can be summarised as follows.

Governance

All cases had significant issues with effective governance of the critical infrastructure assets. In this case we mean the assets to be both the corporate and SCADA networks of the organisations the authors examined. All organisations demonstrated poor delineation of corporate ownership and responsibility for the SCADA networks and in some cases the supporting information technology infrastructures.

Policy

As a result of poor governance structures within the organisations the policy structures also suffered. There was little evidence of any policy review, enforcement, auditing or existence of any policy implementation. Review of the policy documentation that was presented during the assessments revealed it was rarely current and was lacking in relevant details. The policy in some instances had not been reviewed or revised for several years. In some cases where there was the existence of a policy there existed approved procedures which were in direct contravention to the existing policy.

Un-Patched Hardware and Software

All of the assessments conducted found exploitable vulnerability as a result of un-patched hardware and software issues. Of particular concern were perimeter firewalls that had multiple exploitable vulnerabilities as a result of dilettante patching regimes. These firewall exploits were well known and had been known in the security community for up to five years. Due to the legacy nature of SCADA systems, all of the underlying supporting computer operating systems had significant vulnerability. Most of the operating systems examined in all assessments had long since reached end of life, and were no longer supported by the vendor. Most of the supporting applications in the form of SQL servers, network operating systems or specific SCADA applications were likewise no longer supported by the vendor.

Lack of Network Segregation and Segmentation

Assessments conducted so far have revealed networks that are severely compromised under the defence in-depth strategy. Several of the network architectures were based on flat 10.0.0.0/8 networks allowing for a reversal of the entire network including corporate and control systems. Penetration of perimeter controls would have allowed complete sight into the enterprises examined. This would allow the easy implantation of malcode such as packet sniffers or keystroke analysers into the network architectures.

Lack of Sound Authentication Mechanisms

Several of the installations provided generic logins to staff members for example username equals staff password equals staff. All of the systems reviewed had no reliable or monitored audit trial for systems access. That is no coordinated logging of even simple statistics such as logon or log off was conducted. These logins were provided mainly for expediency and were handed out typically as a result of the work environment trusting individuals. Given that 60 to 80% of losses sustained by successful I T. enabled crime or malfeasance is committed by insiders (Richardson, 2008), one could postulate this is an extremely unwise move on the part of management. Furthermore, some of the generic accounts uncovered in the examinations had root or admin level access to the entire IT infrastructure. This would allow any malicious individual the power to corrupt absolutely. The use of such simple and group based passwords also allows a substantial vector for the disgruntled employee to penetrate the system and wreak havoc with impunity.

Monitoring, logging, auditing

There was a complete lack of any substantive logging of network interactions with attendant monitoring and then subsequent auditing and review. This observation put all organisations in an invidious position with respect to the network based exploit and attack. This leads to the realisation that most of the organisations had no ability to answer fundamental questions such as have we been attacked? We got hacked – how did it happen? Inability to answer even these basic questions makes amelioration or reduction of any network borne threat a relatively impossible task.

In one organisation there was a logging of firewall connections but no actual review of these logs to determine any emergent threat, unauthorised connections or internal malfeasant activity. The net value of this type of logging is a completely negative proposition for the organisation. The organisation is wasting money logging data that was never intended to be examined.

It has been proven already due to the nature of SCADA systems that the use of intrusion detection systems and intrusion prevention systems can shutdown communications, which can have potentially catastrophic unintended consequences (Fink *et al*, 2006). If we cannot reliably implement and use intrusion detection systems or intrusion prevention systems to protect networks that run SCADA devices, the use of monitoring logging and auditing are fundamental tools and techniques in providing response against network based attack. In some cases the use of these is the first and last line of defence against attacks that would be perpetrated against networks.

COMPARISON OF ORGANISATIONAL STRUCTURE AGAINST SECURITY MEASURES

The results of the CNVA audits were genericised and summarised according to the criterion given in Table 1. These results were then categorised according to the organisation type as given in Figure 1, and ranked for their overall security posture. As can be seen in Table 2, Organisation 1 had a greater overall level of security than did the other organisation types. Whilst the majority of the measures are quite technical in nature, even issues such as policy and availability of documentation were areas of concern for organisations two and three.

Table 2: Evaluation of security audit results against a common best practice framework for three different organisational structures.

Criteria	*Organisation 1*	*Organisation 2*	*Organisation 3*
Firewalls			
External	Yes	Yes	Yes
Multiple firewalls	Yes	No	Yes
Multiple Firewalls (different vendors)	Yes	N/A	Yes
Firewall rule sets configured correctly	Yes	No	N/A
Firewall OS / firmware patched?	Yes	No	No
Network Segregation Measures			
DMZ between corporate and PCS	Yes	No	No
DMZ between Internet and Corporate	Yes	No	No
Logical segregation through subnets and VLANs	Yes	No	No
Access control lists on border routers	Yes	No	No
Intrusion Detection System	Yes	N/A	N/A
Remote Access			
Secure authentication method	Yes	Yes	Yes
Two factor authentication	Yes	No	No
RSA token authentication	Yes	No	No
Documentation			
Policies Current?	No	No	No
Network topology diagrams current?	Yes	No	No
Firewall and Access control rules available?	Yes	Yes	No
Policy audited or enforced?	Yes	No	No

The columns where an N/A is recorded were due to a number of factors. In some cases, it was due to the measure not having been implemented e.g. Organisation 2 did not have multiple firewalls at the boundary between corporate and the internet. Other N/A results were recorded because the outsourcing provider did provide this information e.g. the outsourcing provider at Organisation 3 was not able to produce current network diagrams.

DISCUSSION

The results presented here overwhelmingly support the notion that having dedicated information security and technology embedded within the process control division of a critical infrastructure provider leads to the best security outcome. However, it must be noted that this was an examination of four organisations, categorised into three types, and that it did not examine budgets or other factors which may have influenced this outcome.

The NIST Guide to industrial control systems security does discuss the formation of a team which consists of people from key stakeholders within an organisation, but the evidence presented here would seem to indicate that this does not go far enough. The NIST guide states that the IT department of an organisation can have vital input to protecting a process control network. In isolation, there is nothing wrong with this statement, but the reality is that IT departments do not have sufficient ownership of the process control systems, and as such there is a disconnect when it comes to protecting these systems i.e. the role of an IT security group, which is based in the corporate is to protect the corporate network. This is not a criticism, but simply a statement of their job purpose, and for this group to ignore their *raison d'être* would be negligent. There is then a paradox created when a group dedicated to protecting one part of an organisation is asked to assist in protecting an area which they do not have a direct interest in, and are then criticised when they do not give it their full attention. It is likely for this reason that those organisations using this model in order to provide IT security input for protecting their process control networks were observed to have a level of security which was inadequate when compared against the best practice guidelines.

Whilst it could be appropriately argued that the security issues found with organisations two and three may not be as a direct result of the organisational structure, there is certainly a case to support the structure of organisation one as being best practice. Noted in the assessments conducted on these organisations was a combination of lack of governance and or direct responsibility for the SCADA / control system. The result of this lack of responsibility was that the corporate or third party IT support groups had no direct ownership in these systems. As a flow on effect, this lack of ownership meant that there was a corresponding lack of understanding of the criticality of securing these systems from attack, and that the focus of their concerns from a security perspective was the computers on the corporate network segments.

Alternatively, some groups would argue that critical infrastructure protection (CIP) should be an organisation wide responsibility, and that there should not be a dedicated security team responsible for it. The NIST guidelines suggest that a dedicated team made up from all areas of the organisation should be responsible for securing CIP (Stouffer, 2008). Additionally, there are Gartner Reports suggesting that operational technology (OT) and information technology governance need to be converged (Roberts & Steenstrup, 2010). However, this paper paid more heed to business needs, with security a secondary consideration. Unfortunately, when the consequence of a security breach is loss of critical infrastructure, potentially for an extended period of time, security of the OT must take precedence. The reality, as found by examining the security of these organisations as reported here, is that a corporate IT security manager or agent is always going to put the corporate network first: it is the nature of the beast.

A recent report from Gartner highlighted the issue of where the information security officer should be located within a critical infrastructure provider:

> “Coordination and leadership for OT security is vital. To date, a chief information security officer (CISO) equivalent for OT security does not exist in most utilities, though a few innovators have already taken early steps in this area.” – Perkins (2009)

The evidence presented in this paper supports the preceding statement, given that only organisation 1 had a CISO equivalent in the OT structure of the organisation. The other organisations reviewed in the CNVA relied up on using the CISO from the corporate segment of the overall organisational structure.

The evidence presented in this paper would suggest that the structure of organisation where there are information security and technology personnel embedded in the control system structure of the organisation, and not reliance on the corporate division to provide these services, will lead to the best outcome from a security perspective.

CONCLUSION

Whilst there are arguments that CIP security is an organisational wide responsibility, the evidence presented in this paper suggests that the implementation of security needs to be based in the process control section of an organisation. Organisations that rely on in house corporate information security or information technology to provide security for their process control networks are not adequately protecting their SCADA / process control systems. Those organisations using a model which has IS / IT specialists working as part of the control system team achieved a higher level of security than those which did not follow this model. The reports supporting convergence do so from a management point of view, and not from a security perspective. As evidenced by the assessments carried out and presented here, this approach does not appear to be working, as security managed from the corporate side of the organisation was not adequate. The evidence presented here suggests that convergence does not lead to the best security outcomes, and that it is dangerous to impose a standard business governance model onto critical infrastructure providers.

One area not investigated here was the relationship between budget allocated to each section, and the impact this may have had on the security posture of the organisations that were examined as part of the CNVA process. It may be that budgetary restrictions had a role to play in any observed security issues, and this will need to be examined in any future research.

Further research in this area will examine a wider range of organisations to examine their level of security and to see whether this apparent connection between organisational structure and security level holds true across a wider sample.

REFERENCES

Aubert, M. (2004). *MCSE Guide to Microsoft Windows Server 2003 Active Directory*. Thomson Course Technology, Boston: Massachusetts

Baker, W. H., Hutton, A., Hylender, C. D., Novak, C., Porter, C., Sartin, B., et al. (2009). 2009 Data breach investigations report. Retrieved 5/7/2010, 2009, from http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Fink, R.K., Spencer, D.F. & Wells, R.A. (2006). Lessons learned form cyber security assessments of SCADA and energy management systems. Retrieved 14th July 2010 from http://www.inl.gov/scada/publications/d/nstb_lessons_learned_from_cyber_security_assessments.pdf

Igure, V.M., Laughter, S.A. & Williams, R.D. (2006). Security issues in SCADA networks. *Computers and Security*. **25(7)**: 498-506

Idaho National Laboratories (2006) Control Systems Cyber Security: Defense in Depth Strategies. Retrieved 10th July 2010 from http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf

ISA (2007). ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems.

Jackson-Higgins, K. (2007). SCADA state of denial. Retrieved 10th October from http://seclists.org/isn/2007/Apr/0068.html

Perkins, E. (2009). Evolving cybersecurity issues in the utility industry. Gartner Reports, ID: G00170025

Permann, M., Lee, K., Hammer, J. & Rhode, K. (2006). Mitigations for security vulnerabilities found in control systems networks. In Proceedings of the 16th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference, June 2006, San Jose California

Richardson, R. (2008). CSI Computer crime and security survey. Retrieved 14th July 2010 from http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf

Roberts, J.P. & Steenstrup, K. (2010). The management implications of IT/OT convergence. Gartner Reports, ID:G00174016

Smith, T. (2001). Hacker jailed for revenge sewage attacks. Retrieved 10th October 2008 from http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

Steenstrup, K. (2010). Operational Technology convergence with IT: Definitions. Gartner Reports, ID:G00200630

Stouffer, K., Falco, J. & Scarfone, K. (2008). NIST Special Publication 800-82 – Guide to industrial control systems (ICS) security. USA, National Institute of Standards and Technology

Trusted Information Sharing Network (2005). SCADA Security – Advice for CEOs. Retrieved 10th July 2010 from http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(427A90835BD17F8C477D6585272A27DB)~Supervisory_Control+and+Data+Acquisition+(+SCADA+)+-+Security+Advice+for+CEOs.pdf/$file/Supervisory_Control+and+Data+Acquisition+(+SCADA+)+-+Security+Advice+for+CEOs.pdf

Trusted Information Sharing Network (2008). *Computer Network Vulnerability Assessment Program*. Retrieved 11th October from http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/CIPPrograms_ComputerNetworkVulnerabilityAssessment(CNVA)Program