Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2015 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2015

Studying SCADA Organisations Information Security Goals: An Integrated System Theory Approach

Suhaila Ismail
University of South Australia, suhaila.ismail@mymail.unisa.edu.au

Elena Sitnikova
University of New South Wales, e.sitnikova@adfa.edu.au

Jill Slay
University of New South Wales, j.slay@adfa.edu.au

STUDYING SCADA ORGANISATIONS INFORMATION SECURITY GOALS: AN INTEGRATED SYSTEM THEORY APPROACH

Suhaila Ismail, School of Information Technology and Mathematical Sciences, University of South Australia, Australia, suhaila.ismail@mymail.unisa.edu.au

Elena Sitnikova, Australian Centre for Cyber Security (ACCS), University of New South Wales at ADFA, Australia, e.sitnikova@adfa.edu.au

Jill Slay, Australian Centre for Cyber Security (ACCS), University of New South Wales at ADFA, Australia, j.slay@adfa.edu.au

Abstract

Security awareness and its implementation within an organisation is crucial for preventing deliberate attacks or/and minimise system failures on organisation's system especially where critical infrastructure is involved including energy, water, gas and etc. This study is based on Integrated System Theory (IST) and focuses on measuring and assessing security goals including policies, risk management, internal control and contingency management implemented in 101 organisations that operate Supervisory Control and Data Acquisition (SCADA) Systems. The data collected were analysed using structural equation modelling to test the structural and measurement model. The major finding of this study is that organisational information security goals are strongly related to the key measurement indicators, which include items assessing security policies, risk management, internal controls and contingency management.

Keywords: SCADA Systems, Information Security, Integrated System Theory, Risk Assessment, Vulnerability Assessment

1 INTRODUCTION

The nature of interconnected and complex infrastructures critical infrastructure invites an array of risks and threats to these critical systems. Any risks or threats to these critical services will cause a substantial impact on the critical services provided energy, water, gas, transportation, emergency services, food, etc.

In the United States, the Executive Order on Critical Infrastructure Protection (CIP) by President George W. Bush in 2001 emphasized the continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. Protecting these systems is essential to the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services sectors (The White House 2001, pp.1-10). Critical infrastructures systems are created on a huge scale and are often interdependent and interconnected. A failure of any components in the critical infrastructure may result in the collapse of services and organisational coherence (Chunlei et al. 2011). Its complex nature makes it difficult to identify the dynamic behaviours of critical infrastructure sectors, but significant research has been done on mitigating risks to them. Several similarities were identified in the critical infrastructure systems, which are typically complex arrangements. They include cascading failures of interrelated infrastructures, for example, the failure of an electric company could eventually affect the whole infrastructure such as airports, transportation, telephone systems, etc. It is also difficult to determine boundaries between each infrastructure. Complex systems may be open and nested and any failure of an infrastructure could cause dangerous phenomena to appear elsewhere in the system (Cilliers, 2002).

According to Hentea (2008), a typical SCADA network layout comprises workstations, SCADA servers, Remote Terminal Unit (RTU), Programmable Logic Controllers (PLC), Port servers, workstations, as well as communication links that unite SCADA internal systems to any Corporate LAN. Hentea also noted that the following components that make up SCADA systems consist of: Programmable Logic Controllers (PLC), remote terminal units (RTU), intelligent electronic device (IED) or Process Automation Controller (PAC). Host computers are used as central points of interaction between people, databases and monitoring processes and creation of reports (Hentea, 2008). Figure 1 below illustrates a typical SCADA network as reported in the Industrial Control Systems Weekly Situational Awareness Report by the Critical Intelligence (Critical Intelligence Inc 2013). The layers in the figure illustrate how hardware and components are connected and interacts with one another. The sensors, actuators, PLC and RTUs are located at the remote locations to collect data. The SCADA layer consists of HMI, Historian, Engineering and other workstations. Historian is a subsystem that stores all the audit-logs of the activities conducted on SCADA systems (Mcnamee & Elliott 2011). Demilitarised Zones (DMZ) protect the SCADA systems from the corporate layer and the Internet if configured properly. This is achieved by ensuring secure access authentication devices, workstations, servers and databases.

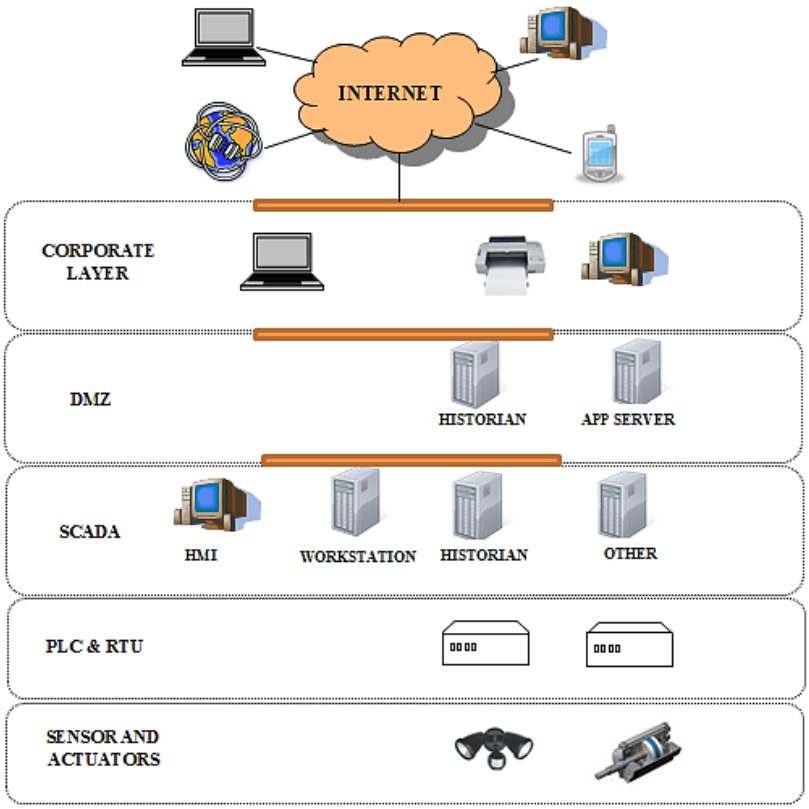

Figure 1: Typical structure and components in a Critical Infrastructure Environment (Adapted from Critical Intelligence, 2013)

There are different types of interruptions that can affect SCADA systems, in the form of either deliberate attacks or system failure. Both cause many problems for an organisation. An example of such failure of SCADA systems was an incident in Bellingham WA Gas Pipeline failed because the control systems did not function during database development on the pipes systems while the pipes were in operation. Because of this failure 237,000 gallons of gasoline leaked from a 16" pipeline that ignited and burned nearly 1½ miles along the local creek causing 3 deaths and 8 injuries (Ismail et al. 2014a; Miller & Rowe 2012; Tsang 2009).

This paper seeks to measure the information security goals within an SCADA systems organisation and the extent to which organisations are aware and implement information security mechanisms. Section 2 will briefly introduce the conceptual background of the study by highlighting the SCADA systems' vulnerabilities, and followed by a description of the theories often used in assessing security in organisations and the reasons for choosing Integrated System Theory for this research. Section 3 discusses the research methodology and respondents' demographics details that constitute much of the data collected. This is followed by section 4, which focuses on the data analysis and results of that analysis. This includes the assessments of the measurement and structural models adopted for this research. Section 5 concentrates mainly on a discussion of the data analysis. Finally, section 6 concludes the study.

2 CONCEPTUAL BACKGROUND

2.1 SCADA Systems Vulnerabilities

The growing demands for connectivity between corporate networks and SCADA systems have created the risks and introduced vulnerabilities. Private and confidential information is widely accessible to the public as well as individuals and corporations on the Internet, including structural maps networks, network systems configurations and names, etc. By obtaining this information, an intruder can then access and manipulate the SCADA systems for their own benefit. Insecure network designs may result from insufficient funds or lack of knowledge of the practitioners of the system (Fernandez & Fernandez 2005).

Research has shown that there are several vulnerabilities associated particularly with SCADA systems. SCADA systems have similar vulnerabilities with existing IT systems (Hildick-Smith, 2005), but due to their unique nature, there are exclusive vulnerabilities including: SCADA engineers' experiences are unlike those of IT personnel and the reality is they need to complement each other's tasks and skills in securing SCADA systems. In a normal IT organisation's operations, security patches are often deployed on the system regularly, but in SCADA organisations, the system would not be able to be patched rigorously due to its highly critical data and the requirement to be available without any interruptions. From the literature, as well as the interviews conducted with experts and SCADA practitioners (Ismail et al. 2014b), the use of a shared password by engineers operating the SCADA systems on the same site is a normal practise in order to ease day-to-day operations. This, however, creates risks especially in terms of authentication and accountability. Policies such as access control should be enforced in order to avoid unauthorised access to the critical systems. With increasing connections between remote locations, sites and offices sharing information can lead to vulnerabilities in the system. For reasons of cost and economic efficiency, engineers or SCADA practitioners should be able to remotely access systems and conduct their day to day operations without being physically at the remote locations. Due to the large amount of data involved in monitoring and controlling SCADA systems, real-time monitoring is another growing concern (Hildick-Smith, 2005; Rautmare, 2011).

According to Ismail, Sitnikova and Slay (2014a) and (Miller & Rowe 2012), a series of deliberate previous attacks has been directed at SCADA systems in order to gain confidential information, or access private networks and to deliberately cause denial of service. This can cause financial, economic and human loss. This paper recognizes the importance of assessing the security within SCADA organisations in order to prevent attacks or failure of their crucial services.

2.2 Relevance of Integrated System Theory (IST)

Within the SCADA systems environment, many studies have been conducted in assessing the vulnerabilities and risks organisations face, based on several theories such as, Integrated System Theory (Hong et al. 2003), Security Life Cycle Model (Creery & Byres 2007), Protection Motivation Theory (Workman et al. 2008), Institutional Theory (Bjork, 2004; Meyer, 2006) and Information Security Management Theory (Ericsson, 2010; Finne, 1998). An unconventional theory that applies theories across various sectors has also been applied to security risk assessments, and this is the Dempster-Shafer Theory of Belief Functions (Sun et al. 2006). In the case of SCADA systems and its complex nature, we believe that an integrated solution theory would be more applicable since it will cover all the important considerations within the SCADA environment.

This study adopts Integrated System Theory (ITS) because of its measurement indicators and components fulfil the research aims and objectives of this paper. The components are the implementation of security policy, risk management, internal control, information auditing, and contingency management in achieving organisational goals. Other studies have used the theory in terms of assessing the information security implementations and integrating components that address

the overall security issues within an organisation. This theory has previously been employed to examine the effectiveness of management strategies and lack of information security management theory. For example it was used in studies on the information security landscape in Malaysian Public Service organizations (Dzazali et al. 2009), information security governance in Saudi organisations (AbuSaad et al. 2011; Shahzad & Musa 2012) and improving information security in Taiwan (Hong, Chi, Chao, & Tang, 2006). IST provided the basis for the research framework concerning information systems security (Cannoy et al. 2006; Järveläinen 2012) where it underlined the importance of integrating security components within an organisation to ensure that information security and business continuity in inter-organisational IT relationships were effective. This also includes research papers on the financial impact of security (Hatzakis et al. 2010) and improvement strategies in electronic stock commerce (Ghotbi & Gharechehdaghi 2012; Kyobe 2008). Because of the wide application in other critical sectors mentioned above, this particular theory, Integrated System Theory (IST) is chosen to better access the overall security awareness based on the key measurement indicators. This research is also based a recent pilot study (Ismail et al. 2014b) that measured the alignment of information gathered through expert interviews, and pilot online surveys for SCADA systems practitioners from different organisations in different sectors of critical infrastructure. The survey questions were designed based on interviews conducted with experts who provided the critical factors to be considered during the information gathering process.

2.3 Integrated System Theory

In determining the security requirements (Igure et al. 2006) of an organisation, it is necessary to evaluate how organisations approach information sharing within the organisation (Bishop 1995) and the level of confidentiality of information. In order to ensure the security requirements are addressed, this study focuses on measuring the organisations' information security goals are achieved based on the components adapted from Integrated System Theory. Figure 2 below shows the Research Model that was adapted from (Hong, Chi, Chao, & Tang, 2003).

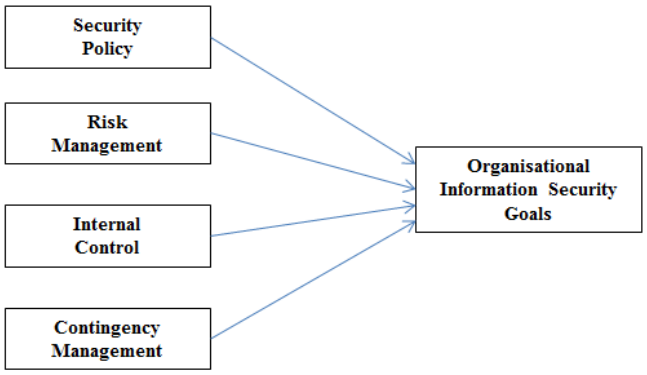

Figure 2: Research Model-Integrated System Theory (adapted from Hong et al., 2003)

- ***Security Policy***

  Implementing security policies is essential in organisations, especially organisations that are dealing with critical services. Security policy is a specific statement of what is and what is not allowed in terms of ensuring a system's security (Bishop 2003; Stouffer et al. 2011). Security policies are important for ensuring compliance to security practices in an organisation.

H1: The availability of security policies has a positive impact on the organisational information security goals

- ***Risk Management***

  Vulnerabilities in a SCADA system can occur due to mismanagement of risks, misconfigurations, poor maintenance on platforms hardware, operating systems and applications. Risk assessment serves to identify, quantify and prioritize risks against criteria for risk acceptance and objectives relevant to an organisation, specifically to those that employ SCADA systems. The outcome of a risk assessment could be used to determine the appropriate action required to manage the information security risks to the SCADA system networks, which will then lead to appropriately selecting the best security controls to implement (Ismail et al. 2014b).

H2: The ability to manage risks will have a positive impact on the organisational information security goals

- ***Internal Control***

  The third important component of Integration System Theory (IST) is control and auditing theory which suggests that each organisation measures the control performance of the implemented security control systems in their environment (Hong et al., 2003). Control is often regarded as preventing, detecting and correlating activities in the system in order to avoid illegal and unauthorised access and activities in their system (Ismail et al. 2014b). Stouffer at al. (2011) defines controls as management, operational and technical controls that constitute part of the informational system that protects the confidentiality, integrity and availability of the system and its data.

H3: The ability to implement Internal Controls has a positive impact on the organisational information security goals.

- ***Contingency Management***

  For the purpose of this study, participants from different organisations and cross-sectors are evaluated in terms of awareness and whether their respective organisations are implementing various measures in making sure the critical services that they are providing are continued even in events of disturbance. This is achieved by making sure that appropriate measures are taken when any unforseen incidents were to happen. Contingency planning normally includes documents in handling equipment's, restoring data, information on responsible personnel's for each tasks and emergency operations.

H4: Implementation of Contingency Management has a positive impact on the organisational information security goals

Table 1 below summarises the measurement items, mean and standard deviation for the key dimensions.

Dimensions/Questions	*Item*	*Mean*	*STD*
Security Policy			
My organisation has a specific and adequate documented security procedure	SP01	3.1683	.77549
My organisation has adequate guidelines in SCADA systems hardware/equipment maintenance	SP02	3.2970	.81908
My organisation has adequate policies for portable devices (hardware and software)	SP03	3.1188	.71116
My organisation has documented change management procedures	SP04	3.1980	.72138
My organisation has an appointed person in charge to manage security policies and procedures	SP05	3.0990	.84267
Risk Management			
Default platform configurations are used in my organisation	RM01	3.0297	.95347
Critical platform configurations are stored and backed up	RM02	3.4554	.70035
Data are stored on portable hardware drives and protected	RM03	3.2871	1.00336
Internal Controls			
My organisation implements a security assessment mechanism	IC01	3.0594	.79777
My organisation has appointed a person in charge (PIC) to conduct security assessments	IC02	3.1782	.81726
My organisation has specific plans to control and maintain security	IC03	3.1188	.73874
My organisation has a service acquisition strategy	IC04	3.2079	.94145
My organisation manages security training and awareness	IC05	2.9109	.82582
Contingency Management			
My organisation has adequate continuity of operations documentation	CM1	3.2079	.75255
My organisation has adequate disaster recovery documentation	CM2	3.0891	.82582
My organisation has installed intrusion detection software in my environment	CM3	3.0594	.97798
My organisation keeps track and ensures that all logs are maintained	CM4	3.2079	.87541
Organisational Information Security Goals			
My organisation implements adequate security policies for SCADA systems	OISG1	3.317	.8594
My organisation implements adequate security training and awareness policies	OISG2	3.0198	.83642
My organisation has procedures to provide adequate training on security architecture and design of the SCADA systems	OISG3	3.0396	.95834

Table 1: Measurement items, Mean and Standard Deviation

3 RESEARCH METHODOLOGY

To assist in achieving the overall objectives of this research, an online survey was created based on the National Institute of Standards and Technology (NIST) Guide to Industrial Systems (ICS) Security (Stouffer et al. 2011). The online survey was distributed to SCADA systems practitioners across several sectors within the SCADA systems community of organisations. The participants were identified by the experts from the industry which was interviewed during the first phase of this project (Ismail et al. 2014b), governing bodies as well as through various methods of selective sampling including communicating with the organisations through email and LinkedIn. A total of 118 practitioners from different organisations participated in the survey, but only 101 are used for the data analysis. Others were excluded due to their incompleteness. Table 1 shows the breakdown of the survey participants according to job role, department, and years of service, sectors and principal industry for the organisation. Most of the participants are the practitioners of SCADA systems. A high percentage is from the engineering department, which is consistent with the objective of the survey, i.e. to focus more on the practitioners (Ismail et al. 2014b) who run SCADA systems daily.

Information is also provided by IT personnel who ensure the security of the systems. 44.3% of participants have at least 1-5 years' experience, which is well reflected in the survey findings that are discussed in the following section. 75.7% of participants work in the private sector which reflects the fact that critical services are outsourced to private businesses, and thus emphasizes the importance of securing and monitoring the SCADA systems to ensure the integrity and safety of data. The three main critical services which are utilities industries, which include oil and gas (30.4%), electricity (21.7%) and water (13.9%) and these, are well represented. This will ensure that the data obtained from the survey can represent the level of security existing in critical services.

Demographics	***Category***	***Percentage***
Job Role	Senior Management	5.2%
	Middle Management	28.7%
	Team Leader	19.1%
	Staff	31.3%
	Contractor	7.8%
	Others	7.8%
Department	Administration	2.6%
	Engineering	62.6%
	IT	14.8%
	Facilities & Management	0.0%
	Emergency Planning / Management	0.9%
	Others	19.1%
Years of Service	Less than a year	7.8%
	1-5 years	44.3%
	6-10 years	24.3%
	10-15 years	11.3%
	More than 15 years	12.2%
Sector	Government	11.3%
	Semi-Government	13.0%
	Private	75.7%
Principal Industry	Construction & Manufacturing	15.7%
	Defense (Airlines & Aerospace)	1.7%
	Telecommunications	11.3%
	Utilities (Oil and Gas)	30.4%
	Utilities (Electricity)	21.7%
	Utilities (Water)	13.9%
	Transport	5.2%

Table 2: Respondents' Demographic Details

The comprehensive questionnaire consists of several sections. The first section is concerned with the demographics of participants. The second section focuses on the security policies implemented in the organisations, while the third section is about risk management implementations, in terms of platform, and network vulnerabilities identified in the organisation. Section four encompasses the management, technical and operational controls. The final section focuses on the issues concerning security of SCADA systems.

4 DATA ANALYSIS AND RESULTS

For this research, structural equation modelling is used to examine the data collected from the survey. The information retrieved was tested using the partial least squares (PLS) model. The first step in analysing the data was to assess the measurements of the said model by establishing the reliability and discriminant validity. The next step was to assess the structural model by testing the hypothesized paths (and the path coefficient, β) between the constructs, as well as determining the path significance

using t statistics values by conducting a bootstrapping method with 500 samples. This will be further explained in the following sections.

The measurement scale used in the survey is a Likert scale from 1-5 which ranges from: strongly disagree (1), disagree (2), agree (3), strongly disagree (4) and unable to rate (5). The information gathered were analysed and evaluated in SPSS 21.0. The psychometric properties of the constructs were assessed and by examining the internal consistency, convergent validity, composite reliability, and discriminant validity. Cronbach's Alpha testing (Cronbach, 1951) was also conducted to evaluate the constructs consistency and reliability. This is shown in Table 3 in the following section.

4.1 Assessments of Measurement Model

Assessment of the measurement model was done by conducting reliability and validity of the constructs namely; security policies, risk management, internal control, contingency management and organisational information security goals (OISG) based on the information collected through the online survey answered by practitioners of SCADA systems.

For the reliability of constructs test, we used the measurements of Cronbach's alpha using SmartPLS 3.1.6. It can be concluded that the reliability between the constructs is positive because it is higher than 0.7. If all the constructs are higher than the cut-off value of 0.7, this indicates that the constructs for the research have an acceptable level of internal consistency (Hair et al. 1998; Nunnally & Bernstein 1978). The independent variables for this research are security policy, risk management, internal control and contingency management, whereas the dependent variable is the OISG. The corresponding Cronbach's alpha values are 0.807, 0.769, 0.844, 0.710 and 0.860, respectively, as stated in Table 3.

Construct	***No. of items***	***Cronbach's alpha***
Security Policy (SP)	5	0.807
Risk Management (RM)	3	0.769
Internal Control (IC)	5	0.844
Contingency Management (CM)	4	0.710
Organisational Information Security Goals (OISG)	3	0.860

Table 3: Reliability of Constructs

We then evaluated the convergent validity assessments of the constructs by examining the correlation of constructs, and determining the factor loadings and average variance extracted. Convergent validity stipulates the degree of a construct correlation with another construct in the research model. For this test each indicator's factor loadings should be higher on their own constructs when compared to the other constructs in the research model (Anderson & Gerbing 1988; Rhee et al. 2009). On the other hand, discriminant validity specifies the degree to which the constructs is not correlated with another construct. The test that was done particularly to determine discriminant validity calculates the average variance extracted (AVE) which Fornell and Larcker (1981) recommended to be above 0.5, and composite reliability (CR) above 0.6 (Bagozzi et al. 1991) or above 0.7 (Hair et al. 2011). By determining the values of the factor loadings, AVE and CR are at an adequate convergent validity in each construct. Table 4 indicates the factor loadings for each corresponding indicator have the highest value and are in bold. Table 5 shows that the square root values of AVE for each construct are larger than the correlation with other constructs. The measures of the five constructs satisfy the conditions set for reliability and validity assessment. The validity test was conducted using Spearman's Validity test in SPSS.

Construct	*Item*	*SP*	*RM*	*IC*	*CM*	*OISG*
Security Policy	SP1	**0.859**	0.473	0.442	0.612	0.702
	SP2	**0.757**	0.387	0.373	0.520	0.536
	SP3	**0.685**	0.320	0.306	0.508	0.416
	SP4	**0.687**	0.427	0.317	0.589	0.376
	SP5	**0.748**	0.338	0.472	0.582	0.522
Risk Management	RM1	0.391	**0.808**	0.183	0.365	0.320
	RM2	0.517	**0.798**	0.217	0.460	0.348
	RM3	0.382	**0.873**	0.143	0.405	0.363
Internal Control	IC1	0.396	0.101	**0.820**	0.412	0.385
	IC2	0.502	0.275	**0.853**	0.403	0.414
	IC3	0.474	0.187	**0.780**	0.507	0.325
	IC4	0.388	0.266	**0.722**	0.352	0.272
	IC5	0.277	0.055	**0.740**	0.358	0.397
Contingency Management	CM1	0.528	0.372	0.363	**0.697**	0.431
	CM2	0.634	0.433	0.349	**0.780**	0.468
	CM3	0.419	0.252	0.373	**0.667**	0.342
	CM4	0.571	0.374	0.426	**0.775**	0.502
Organisational Information Security Goal	OISG1	0.598	0.425	0.399	0.503	**0.868**
	OISG2	0.563	0.187	0.393	0.509	**0.867**
	OISG3	0.693	0.466	0.438	0.582	**0.916**

Table 4: Factor Loadings for Convergent Validity

Construct	**CR**	**AVE**	***SP***	***RM***	***IC***	***CM***	***OISG***
Security Policy	.864	.562	**0.749**				
Risk Management	.867	.684	0.489	**0.827**			
Internal Control	.889	.616	0.529	0.350	**0.784**		
Contingency Management	.821	.535	0.677	0.473	0.525	**0.731**	
Organisational Information Security Goal	.915	.781	0.595	0.339	0.475	.0.507	**0.883**

Table 5: Composite Reliability, AVE, and Inter Construct Correlations (Using Spearman's Validity Test)

Note: CR= Composite Reliability, AVE= Average Variance Extracted, Bold diagonal values represent the square root of AVE.

4.2 Assessments of the Structural Model

The second phase is to ensure that the structural model is fit and adequate by conducting analysis using SmartPLS and SPSS software to test the hypothesis. PLS and bootstrapping test was conducted to identify each hypothesized path and estimate path significance using t values. A non-parametric bootstrap can be used in PLS path modelling to provide intervals for parameter estimates of shape, spread and bias of the sampling distribution of a specific set of statistics to test coefficients for their significance. Bootstrapping observes a sample as a representation of a population, in which the procedure creates a large, pre-specified number of bootstrap samples by randomly drawing cases from the original sample (Henseler et al. 2009). For the purposes of this study, the sample set of 500 was tested due to the nature and requirement of this research. All the hypotheses were tested and the results were supported by the findings.

Table 6 shows the hypothesized paths and their path coefficients, as well as the p-value and t-value, and the results of the findings. As stated in Table 6, the security policies implemented in organisations

significantly influences the institution's information security goals. The path coefficient from SP to OISG (β = 0.516, t=3.938, p<0.01). Thus, this findings supports Hypothesis 1. Hypotheses 2, 3 and 4 also have a positive relationship with OISG and the corresponding path coefficients; Risk Management to OISG (β = 0.058, t=0.602, p <0.05); Internal Control to OISG (β = 0.119, t=1.458, p<0.05) and Contingency Management to OISG (β = 0.129, t=0.995, p<0.05). These results support hypotheses 2, 3 and 4.

Hypothesis	**Hypothesized path**	**Path coefficient (β)**		**P-value**	**t-value**	**Result**
		Original	*Sample (Bootstrapping=500)*			
H1	SP → OISG	0.516	0.514	P < 0.01	3.938	Supported
H2	RM → OISG	0.058	0.057	P < 0.05	0.602	Supported
H3	IC → OISG	0.119	0.135	P < 0.05	1.458	Supported
H4	CM → OISG	0.129	0.125	P < 0.05	0.995	Supported

Table 6: Results of Hypothesis Testing based on Bootstrapping Technique

5 DISCUSSION

Drawing on Integrated System Theory, this research demonstrated the positive relationships between the measurement of security policies, risk management, internal controls and contingency management in organisations securing their SCADA systems. The analysis in section 4 has shown that the four hypotheses are supported, and therefore the overall research model is valid. Referring to Table 6 in the previous section, Hypothesis 1 proposes that the availability of security policies has a positive impact on the organisational information security goals. The findings suggest that most organisations are aware and are implementing security policies. The findings also suggest among all the other constructs, security policies have the highest percentage of t value, which indicates a high level of path significance. Most organisations have implemented specific and adequate security procedures, adequate guidelines in hardware and equipment maintenance, and adequate policies for portable devices (hardware and software) and have documented management procedures in place. They have also diligently appointed a person to manage security policies and procedures. With all the five items used to measure the security policies in organisations, a positive relationship was observed. The results also confirm that by evaluating the items within Risk Management (H2), Internal Control (H3) and Contingency Management (H4) were also proven to have a positive relationship with organisational information security goals.

H2 has the lowest path coefficient, which implies that some of the organisations that participated in the study are still using the default platform configurations, which is due to the complexity of the systems configurations. This opens up the possibility of future attacks on the system. This calls for efforts to increase the existing system and technology specific knowledge for the practitioners that are involved directly in the SCADA systems. On the other hand, most organisations believe that the critical platform configurations are stored and backed up, which is critical in the business continuity of services.

The organisations realise the importance of implementing a security assessment mechanism internally (H3), and the need to appoint a person in charge to conduct regular security assessments. It is important to note that not all the organisations assessed realise the importance of implementing security assessments within the organisations. Even though security assessments is deemed necessary and critical especially in the critical infrastructure environment, some participants believe that ICS/SCADA networks are isolated from office networks. This suggests that additional security mechanism measures are not always practical for industrial protocols. Another important issue is the

organisation's financial capability in procuring additional security measures or acquiring personnel's that are equipped with the proper knowledge of the complex SCADA systems security. .

H4, which refers to contingency management, is at an average where most organisations believe that they have adequate continuity of operations and disaster recovery documentation. Most organisational conflicts on the need to install an intrusion detection software are due to the nature of the system, which is in line with what was suggested by Hildick-Smith (2005). Although most organisations claimed that they keep track and ensure that all logs are maintained, several responses from the participants highlighted the fact that their workplace does not have sufficient monitoring and maintenance due to several factors. This include the fact that management is not aware and does not acknowledge the need for additional resources to ensure the system remains safe and secure.

One of the limitations to this research is the amount of participants in this study. Even though participants are practitioners from various sectors of the SCADA systems industry, there are several sectors that have a low percentage of participants, such as aviation and defence. A plausible explanation may be the high level of confidentiality that the industry demands. The defence industry is seen as one the most important economic sectors that has critical infrastructure and requires a high degree of confidentiality.

6 CONCLUSION

In this paper, we surveyed 101 SCADA systems organisations across several critical infrastructure sectors. The aim was to investigate the level of security awareness and implementation in conjunction with its organisational information security goals. Integrated System Theory was implemented in order to evaluate the important factors in the system that influences security awareness and implementation, by looking at: measuring the security policies, risk management, internal control and contingency management factors. The integration of all components shows an undeniable influence to the level of organisational information security goals.

Finally, our study confirms that the organisations that operate SCADA systems are aware of the need to implement and maintain a secure environment. Through the findings of the online survey, it is highly critical for organisations to conduct regular vulnerability and penetration tests, increase and develop training and awareness programs for both management, personnel, employees and practitioners of SCADA systems as well as providing training on security architecture and design of the SCADA systems.

References

AbuSaad, B., Saeed, F. A., Alghathbar, K., and Khan, B. (2011). Implementation of ISO 27001 in Saudi Arabia – Obstacles, Motivations, Outcomes, and Lessons Learned. In Proceedings of the *Australian Information Security Management Conference* .

Anderson, J., and Gerbing, D. (1988). Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach. *Psychological Bulletin*, *103*(3), 411–423.

Bagozzi, R. P., Yi, Y., and Phillips, L. W. (1991). Asessing Construct Validity in Organizational Research. *Administrative Science Quarterly*, *36*(3), 421–458.

Bishop, M. (1995). *A Taxonomy of UNIX System and Network Vulnerabilities*. Tech. Rep. CSE-95-10, Department of Computer Science at the University iof California at Davis.

Bishop, M. (2003). What Is Computer Security? *IEEE Security & Privacy Magazine*, *1*, 67–69.

Bjork, F. (2004). Institutional theory : A new perspective for research into IS / IT security in organisations. In Proceedings of the *37th Hawaii International Conference on Systems Sciences (HICCS)*.

Cannoy, S., Palvia, P. C., and Schilhavy, R. (2006). A Research Framework for Information Systems Security. *Journal of Information Privacy & Security*, *2*(2), 3-24.

Chunlei, W., Lan, F., and Yiqi, D. (2011). National Critical Infrastructure Modeling and Analysis Based on Complex System Theory. In Proceedings of the *2011 First International Conference on Instrumentation, Measurement, Computer, Communication and Control*, 832–836.

Cilliers, P. (2002). *Complexity and postmodernism: Understanding complex systems*. Routledge.

Creery, A. A., and Byres, E. J. (2007). Industrial cybersecurity for a power system and SCADA networks - Be secure. *IEEE Industry Applications Magazine*, *13*, 49–55.

Critical Intelligence Inc. (2013). *Industrial Control Systems Weekly Situational Awareness Report*.

Cronbach, L. J. (1951). Coefficient Alpha and the Internal Structure of Tests. *Psychometrika*, *16*(3), 297–334.

Dzazali, S., Sulaiman, A., and Zolait, A. H. (2009). Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. *Government Information Quarterly*, *26*(4), 584–593.

Ericsson, G. N. (2010). Cyber security and power system communicationessential parts of a smart grid infrastructure. *IEEE Transactions on Power Delivery*, *25*(3), 1501–1507.

Fernandez, J. D., and Fernandez, A. E. (2005). Scada systems: vulnerabilities and remediation. *Journal of Computing Sciences in Colleges*, *20*(4), 160–168.

Finne, T. (1998). A conceptual framework for information security management. *Computers & Security*, *17*(4), 303–307.

Fornell, C., and Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobserved Variables and Measurement Error. *Journal of Marketing Research*, *18*(1), 39–50.

Ghotbi, A., and Gharechehdaghi, N. N. (2012). Evaluating the Security Actions of Information Security Management System in the Electronic Stock Commerce , and Providing the Improvement Strategies. *Journal of Basic and Applied Scientific Research*, *2*(3), 3046–3053.

Hair, J. F., Black, W. C., Babin, B. ., Anderson, R. E., and Tatham, R. L. (2006). *Multivariate data analysis* (5th ed.). Upper Saddle River, NJ: Prentice Hall.

Hair, J. F., Ringle, C. M., and Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *The Journal of Marketing Theory and Practice*, *19*(March 2015), 139–152.

Hatzakis, E. D., Nair, S. K., and Pinedo, M. (2010). Operations in financial services - An overview. *Production and Operations Management*, *19*(6), 633–664.

Henseler, J., Ringle, C. M., and Sinkovics, R. R. (2009). The use of partial least squares path modelling in internatinal marketing. In *New Challenges to International Marketing (Advances in International Marketing, Volume 20)* p. 277–319, Emerald Group Publishing Limited.

Hentea, M. (2008). Improving Security for SCADA Control Systems.pdf. *Interdisciplinary Journal of Information, Knowledg, and Management*, *3*, 73–86.

Hildick-Smith, A. (2005). Security for Critical Infrastructure SCADA Systems. *SANS Institute*.

Hong, K.-S., Chi, Y.-P., Chao, L. R., and Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, *11*(5), 243–248.

Hong, K.-S., Chi, Y.-P., Chao, L. R., and Tang, J.-H. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*, *14*(2), 104–115.

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

Ismail, S., Sitnikova, E., and Slay, J. (2014a). Towards Developing SCADA Systems Security Measures for Critical Infrastructures against Cyber-Terrorist Attacks. In Proceedings of *ICT Systems Security and Privacy Protection* (428th Ed), p. 242–249. Marrakech, Morocco.

Ismail, S., Sitnikova, E., and Slay, J. (2014b). Using Integrated System Theory Approach to Assess Security for SCADA Systems Cyber Security for Critical Infrastructures : A Pilot Study. In *11th International Conference on Fuzzy Systems and Knowledge Discovery*, 1000–1006.

Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security*, *20*, 332–349.

Kyobe, M. (2008). The Impact of Entrepreneur Behaviors on the Quality of e-Commerce Security : A Comparison of Urban and Rural Findings. *Entrepreneur Behaviors and E-Commerce Security*, *11*(2), 58–79.

Mcnamee, D., and Elliott, T. (2011). Secure Historian Access in SCADA Systems. *Whitepaper*. Retrieved from http://galois.squarespace.com/storage/files/downloads/Whitepaper_SecureHistorianAccessInSCADASystems.pdf

Meyer, J. W. (2006). Reflections on Institutional Theories of Organizations, The Sage Handbook of Organizational Institutionalism, 788–809.

Miller, B., and Rowe, D. (2012). A Survey of SCADA and Critical Infrastructure Incidents. In *Proceedings of the 1st Annual conference on Research in information technology - RIIT '12*, p. 51, New York, USA: ACM Press.

Nunnally, J., and Bernstein, I. (1978). *Psychometric Theory*. New York: McGraw-Hill.

Rautmare, S. (2011). SCADA System Security. In Proceddings of *India Conference (INDICON),* p. 1–4. Annual IEEE.

Rhee, H. S., Kim, C., and Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, *28*(8), 816–826.

Shahzad, Aa., and Musa, S. (2012). Securing SCADA communication using hybrid cryptography. In *Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication - ICUIMC '12* , p. 1–11, New York, New York, USA: ACM Press.

Stouffer, K., Falco, J., and Scarfone, K. (2011). *Guide to Industrial Control Systems (ICS) Security*. US.

The White House. (2001) *Office of the Press Secretary*. Retrieved from http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html (accessed November 19, 2013)

Tsang, R. (2009). Cyberthreats, Vulnerabilities, and Attacks of SCADA Networks. *University of California, Berkley*. Retrieved from http://gspp.dreamhosters.com/iths/Tsang_SCADA Attacks.pdf (accessed January 6, 2013)

Workman, M., Bommer, W. H., and Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*, 2799–2816.