DOI: 10.21917/ijms.2016.0046

INFORMATION SECURITY ISSUES OF IDENTIFIED ASSETS IN AMR+ - GRID MONITORING AND ENERGY ACCOUNTING SYSTEM

P. Balakumar[1] and Goutam Kumar Kundu[2]
VIT Business School, VIT University, Chennai, India
E-mail: [1]balalabtheni@gmail.com, [2]gkk@vit.ac.in

Abstract

The Purpose of this article is to perform information security risk analysis, risk identification, risk prioritization and risk handling on the AMI grid monitoring and Energy Accounting system assets. Information security Risk analysis performed for the assessment of risk of information impacting confidentiality, integrity and availability and to its like hood and consequences. Critical assets identified based on the Threats, vulnerability and impact on the Information system due to the risks. Risks handled with risk treatment options for risks classified based on the likelihood and consequences. Risk assessment on the critical assets will identify the risks and risk prioritization will classify the risk to handle them to treat to address the Information security risks. Information security Analysis model method, risk classification & risk treatment can be adopted across other SMART GRID Systems. Creating such risk assessment will create a risk database and the risk handling will create risk treatment history to define predictive analysis of information security risks based on this data.

Keywords:

Utility Asset, ISRA, ISMS, SMART GRID, AMR, MEA

1. INTRODUCTION

In today's SMART GRID era Smart Grid systems and it's subsystems from generation, Performance monitoring, Automatic Meter reading, transmission, distribution, substation till end customer meter data possess smart technology. Smart technology involves SMART devices perform data transmission, automatic scheduling, performance adjustments, data storage etc., they are manufactured & later integrated to meet smart grid requirements. Each of these different manufacturers, suppliers, integrators inherits standard & proprietary protocols. Proprietary systems possess manufacturers or OEMs standard process. Utilities and OEMs mandates basic process requirements inherit Specific standards during development and undergo specific test certificates for these devices during supply, Installation and function to meet the performance requirements.

Among these systems Grid metering and Energy Accounting involves data collection from systems implemented a state run Power transmission company operating more than 1,00,000 ckt km in India, It's GM & EA consists of an Automated Meter Reading (AMR) system that will feed data to the Monitoring and Energy Accounting (MEA) System for each Open Access (OA) customers connected to the grid. The total number of Availability Based Tariff (ABT) metering points were close to 300 locations and the stakeholders included generation companies, the transmission utility, distribution circles, captive power plants, independent power producers, distributed power generation operators (for DG sets, mini-hydel) as well as EHT consumers in the state.

Solution involved customized AMR Client/Server, Data Concentration Units (DCUs) and MIS reports as part of the MEA system. Final energy accounting reports on various requirements like Unscheduled Interchange (UI), Auxiliary consumption, Reactive Energy Consumption, Scheduled Bilateral Exchanges, Inter regional, Inter and Intra state transmission losses.

Main solutions as part of their MEA:

1. Meter Data collection from remote meters
2. Meter Data import from xml files
3. Schedule Data from xls, txt files
4. Creation of Master Data base
5. Data Validation, Estimation and Editing
6. Configuration of various meter parameters like Meter Configuration, Virtual Meter Configuration, UI rate
7. GUI development for graphical display of ABT meter data's like Data trending, charts
8. Predefined reports generation
9. Report Generation Tool
10. Exporting report to user defined format like PDF, xls
11. Open access calculation
12. Tariff calculation - EC, CC realization based on Availability, UI charges, REC, Incentive calculation based on PLF, TSC
13. Security/ Authentication at various levels.

In recent years many reports relating to Information security management system, risks identification and classification methods, physical and logical security systems, threats and vulnerabilities, security frameworks, risk impact relation, risk management and response, have been published, Göran N et al. explained vulnerabilities and threats to the power utility system during its course of action and suggested the concept of using security domains for dealing with information security [2], Mina Sajjad et al. proposed an unified Risk management approach required for resource allocations, Identify best practises [3], Ericsson et al. proposed framework to baseline controls through risk assessment [4], Jian Guan et al. proposed diagraph model for risk identification, impact relation and to take specific and immediate action, such as temporarily raising the security at the control gateway, stopping traffic from the corporate network [5], Eric B. Ricea et al. defined a mitigating methodology by overlaying the worst-case attack execution, derived from the network simulations that can be applied as requirements for protective measures for this scenario [7], Jiaxi et al. proposed the probabilistic assessment and the integrated risk assessment, to assess the cyber security vulnerability applying Probabilistic risk assessment [8], G. Dondossol et al. published experimental data by conducting controlled experiments on power control test beds

in order to collect otherwise unavailable data related to cyber misbehaviors in power system operation [9], Friedrich Köster et al. proposed an assessment method and introduced central knowledge base that facilitates the intra-organizational collaboration [10].

Overall, the studies above identify important elements of Information security risks in smart distribution management system. Identification of critical assets within system, methods to classify the risk and assess their impact through controlled simulations, framework to mitigate risks, risk classification, prioritization and frameworks to manage information security risks.

In this paper, we applied holistic approach within system in identification of critical assets, risk prioritization, risk assessment to handle and treat the risk. This risk assessment and treatment method will provide risk database and enable to build predictive risk management system.

2. AMI COMMUNICATION ARCHITECTURE

AMI communication system is the major subsystem of MEA [10] [12] which collect data from meters using optical data collector interface & communicate the data through GSM/GPRS modem. Cluster of many such mater data is collected at the DCU/Industrial PC using GSM/GPRS Modems. The application in the Industrial PC invoked the meter specific proprietary APIs initiates the server end modem to dial the meter end modem. The dialing number for the modem was configurable and the same configured number was used by the API to call the meter end modem and the meter end modem was set to auto-answer mode.

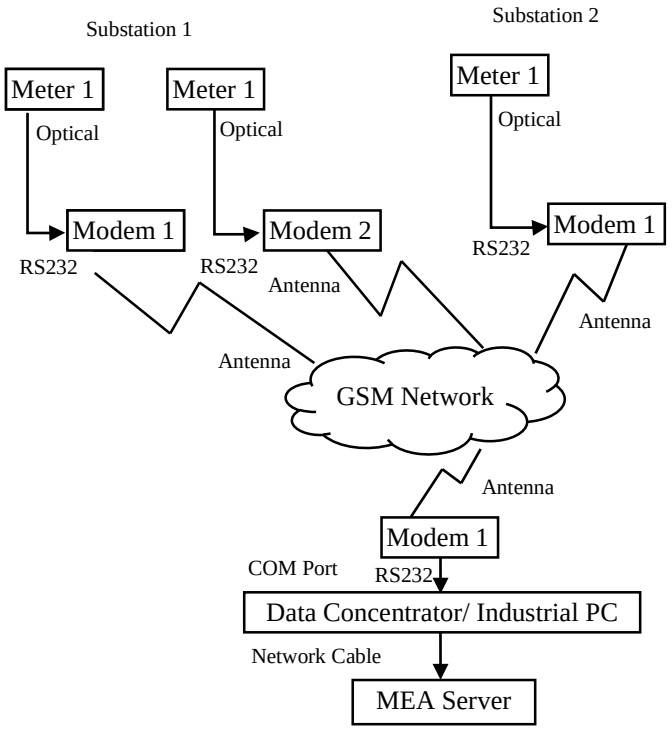

Fig.1. AMI Communication Architecture

The meter end modem is connected to the meter through the optical cable sends data fetch request and the collected the data from the meter whenever the data collection command was received from the server end modem. For this the server end modem and meter end modem were connected. All this dialing and data collection from meter were handled by the meter proprietary APIs as per the MIOS regulations. The meter end modem is physically connected to meter using Optical Cable. The server end modem is physically connected to the Industrial PC using RS232 communication cable. The server end modem and the meter end modem are connected over wireless GSM network at the time of data collection.

Existing functional AMI system and their subsystem including Smart meter, Modem, DCU, MEA server and GSM network installation, operation, management and their information security systems handled independently through OEM partners, service providers, Integrators and operators. By this independent management system lacks coordinated and integrated information security risk assessment, handling, treatment of risks and incidents between handlers adds vulnerabilities and threats in turn maximizes information security risk.

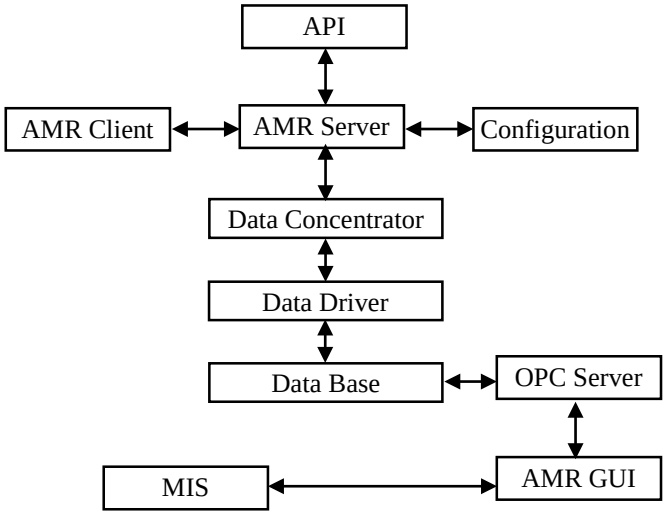

Fig.2. AMR Software Architecture

3. INFORMATION SECURITY RISK ANALYSIS

Detailed risk analysis is a time consuming exercise Risk assessment involves assessment of information security risk impacting, confidentiality, integrity and availability. Risk assessment should address likelihood and consequences. Risk analysis justifies selection of controls [3] [4] [6]. Detailed risk analysis should be done only for information systems which are very sensitive in nature as well as critical for business. The high level risk analysis will identify all such systems which should be subjected to this type of detailed work. Risk identification is identification of information risks, identification of risk triggered from process, opportunity, asset etc., and to identify consequence, impact and likelihood of information security risk. Identification of critical assets is important of risk assessment. Risk increases with the value of the asset. Same threat against a low value asset will cause less impact. Using Risk identification the threats to the assets, vulnerabilities that might be exploited by the threats, impact on the assets due to loss of confidentiality, integrity & availability is identified. Though risk prioritization the likelihood - Chance of something happening and

Consequence - outcome of an event affecting objectives to prioritize how large is the likelihood that a threat will occur? And how large is the consequence if threat occurs? Risk identified based on the likelihood & consequences. There is need to balance the business needs and the risks so that adequate protection is provided at an acceptable cost. The cost of protection cannot exceed the total value of the asset. Selection of controls should be done in a judicious manner such that the cost does not exceed the benefit. We should first check if the existing controls are adequate. If not what are the additional controls that are required to bring down the risk to an acceptable level. Risk handling can reduce the risk to a great extent but cannot totally eliminate it. The residual portion of the risk which remains is the net risk. Risk treatment options are risk reduction, risk avoidance, risk transfer and risk acceptance. Control objectives and controls are selected to meet the requirements identified by the risk assessment and risk treatment process. The selections takes into account that the criteria used while taking the decision of why the control should be applied that these are to reduce risk to acceptable level, meet legal requirements, meet regulatory requirements and meet contractual requirements.

3.1 STEP 1 - IDENTIFICATION OF CRITICAL ASSETS

Identification of critical assets based on threats to the information security assets, vulnerabilities that might be exploited by the threats, impact on the assets due to which loss of confidentiality, integrity & availability [2] [10] [12]

Risk Assessment started from the starting point of the data origin point

- Meter end
- Modem end (Master/Sender)
- Modem end (receiver/Slave)
- Data concentrator end/IPC
- Server end

These assets listed and the points that they interface possess high threats and vulnerabilities to the information system by their placement/location, accessibility, connectivity, interfaces, storage and control and integration with other systems in the network.

Meter collects data from the substation has its own limitation with the connectivity, interface, data storage & transmission. Meter is hardwired to the modem and collects the data & stores them for a limited time period and indexes with the next time frame block. Due to this limitation of data storage it possesses high threat. Meter is hardwired and has limited interface to the operator and also these systems were placed in jinxed location due to this it possess vulnerable to information security risk.

Modem is interfaced from meter through optical probe & redundant energy meter (Secondary meter) and it possess less threat to the information, but it is powered through a data concentrator unit (DCU) by which it collects data from the master (meter) and communicates to the Server end Modem. Due to this the DCU becomes critical and its operation becomes critical to collect the data through modem and transmit to the server end DCU and possess vulnerability and threat.

Modem end (receiver/Slave) possess similar threat and vulnerability like the Modem at the meter end. Here it possess additional risk on its availability to continuously ping and receive data packets transmitted from the meter end modem. Modem at meter end and Modem at the server end will need time synchronization, auto dialing, continues transmission & data receiving by ensuring data availability at the both ends.

Data concentrator/IPC collect data from the Modem and polls to the server. DCU is hardwired to the server. DCU has limited storage location and will be collecting data from multiple meters. Due to this limitation ensuring data polling to the server data base without any loss in the data from the meters is very critical. Server becomes more critical and must be ensured with continuous availability with power, memory, data backup and data loading.

3.2 STEP 2 - RISK PRIORTIZATION

Risk prioritization based on the availability & consequences due to loss of confidentiality, integrity and availability of these assets [12]. Based on the likelihood and Severity, the risks are classified by the below scales

3.2.1 Severity Scale:

i. Critical - Not able to operate and halts
ii. Very Serious - Operates but leads to part functional
iii. Serious - Operates leads but unpredictable
iv. Marginal - Operates with less data effects by which the situation is manageable
v. Negligible - minor risks

3.2.2 Likelihood Scale:

i. Frequent - More often the system is affected due to which non operational
ii. Moderate - Operational but has impulsive effect
iii. Occasional - Less impact to the system mostly operational
iv. Remote - has no adverse risk
v. Unlikely - Manageable

		SEVERITY				
		Critical (5)	Very serious (4)	Serious (3)	Marginal (2)	Negligible (1)
LIKELIHOOD	Frequent (5)	25 Operation not permissible	20 Operation not permissible	15 High priority	10 Review at appropriate time	5 Risk acceptable
	Moderate (4)	20 Operation not permissible	16 Operation not permissible	12 High priority	8 Review at appropriate time	4 Risk acceptable
	Occasional (3)	15 High priority	12 High priority	9 Review at appropriate time	6 Risk acceptable	3 Risk acceptable
	Remote (2)	10 Review at appropriate time	8 Review at appropriate time	6 Risk acceptable	4 Risk acceptable	2 Risk acceptable
	Unlikely (1)	5 Risk acceptable	4 Risk acceptable	3 Risk acceptable	2 Risk acceptable	1 Risk acceptable

Fig.3. Risk Prioritization

3.3 STEP 3 - RISK ASSESSMENT

AMR system is the critical subsystem of MEA has many identified & unidentified vulnerabilities [9] [16] and threats which will lead serious impacts on both technical & commercial grounds. Each identified unit has its own vulnerabilities & threats to the

systems. These vulnerabilities and threats of the units of the subsystems will be assessed to quantify the RPN and initiate the risk treatment plan to mitigate the ISR associated with them.

Table1. Risk Assessment

Asset	Risk	Severity	Likelihood	RPN
Meter end system (A)	1) Optical probe improper contact over the meter surface	2	2	4
	2) Optical probe connection damaged or disconnected to connect the GSM/GPRS Modem	4	2	8
	3) MODEM reset due to firmware update or incompatibility	5	3	15
	4) Modem isolated due to power failure	5	4	20
	5) Meter firmware corrupt	5	1	5
	6) Meter IR not intact with the Optical IR	1	1	1
	7) Low band level signal for Modem communication	3	4	12
	8) Modem data overload	3	3	9
Meter end system to server end system (B)	1) Meter end Modem not synchronized with the server end modem	5	4	20
	2) Incompatible Modem firmware installed or version mismatch	3	2	6
	3) Server end Modem signal loss due low band network	3	3	9
	4) Redundant data reader switch/lapse	5	1	5
	5) Multiple dialling and data polling lapse from the server end modem with the meter end Modems	3	5	15
DCU/Industrial PC end system (C)	1) Server end data driver over polling restart at the OPC server	5	5	25
	2) Automatic data update resulting to Industrial server automatic restart	3	2	6
	3) Data redundancy failure/corrupt	4	4	16
	4) Server switching during redundancy	4	5	20
	5) Time Synchronization mismatch between the industrial PC server & the MEA server	3	4	12
User control, data management, storage, update and retrieval (D)	1) Unauthorized access to the system	5	3	15
	2) Unauthorized installation & movement of the data driver, data folder and target files	5	2	10
	3) Unauthorized maintenance & restart	5	2	10
	4) Coping the data structure and overloading the server with the local backup	5	3	15
	5) Storing & retrieving unauthorized files	5	1	5
	6) Sharing user rights to the next level or unauthorized users	5	1	5
	7) Sharing classified & critical driver files	5	1	5

Likelihood and severity of the assets were assets on the basis of the experience with the operational system. In detail analysis on the testing of the individual system and its subsystems were assumed that they were designed & developed adopting required standards and process to meet the contractual requirements of MEA.

3.4 STEP 4 - RISK HANDLING

Impact analysis diagram clearly infers the impact of risk associated to the system and suggests us risk handling to take stern action plans by categorizing them with their values if Impact [7] [8] [14].

Mitigate - Plan and initialize alternate or standby plan with suitable controls to prevent such incidents with suitable preventive action

i. Manage - Manage the risks by using the tools and techniques with suitable corrective action plan
ii. Monitor - Monitor these risks so that they are not triggered
iii. Make do - Make to do so that the system is active with correction

Assessing the risk at different points/gates of data exchange it possess different level of information security risk with respect to the type of the asset, technology used, system it interfaces, operating & controlling methods.

Risk indicated within the RED band has High impact and certain to occur or incident and these risks are classified as critical risks. These risks will impact the critical information security management system in terms of process & value. Due to this impact the Information management system may collapse due to its impact.

Mitigation is mandate at all levels of the system to reduce the impact & Likelihood of this risk. Mitigation is planned by management system referring the controls stated in the SOA, in case there is an in adequacy and need to enact a control suitable for the management system.

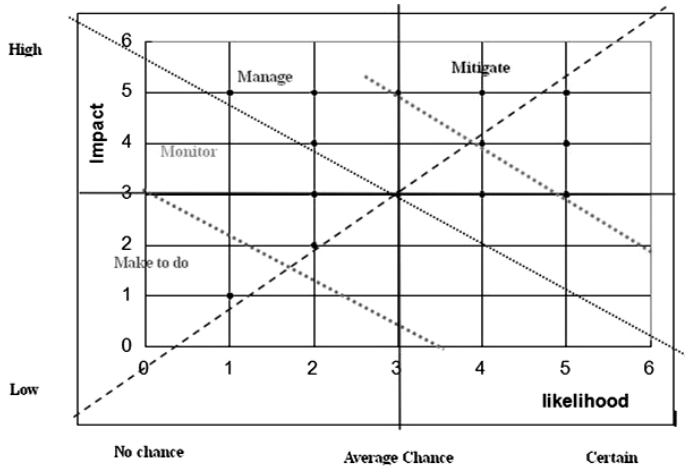

Fig.4. Impact Analysis

3.5 STEP 5 - RISK TREATMENT

Mitigation plan implied for identifies critical risks [24][26][27]

Table.2. Risk Handling

Identified critical risk with High Impact	Mitigation Plan suggested
Modem Isolated due to Power failure	Provide redundant Power supply with battery bank. The switching off modem must save the last data in it and have to send the last data out signal during switch over [ISO 27001:2013 - 11.2] BCP
Meter end Modem not synchronized with the server end modem	Synchronize the Modem with the upgraded firmware and available networks [ISO 27001:2013 - 12.4,12.5]
Server end data driver over polling restart at the OPC server	Server end data driver must be developed as per the end user requirement and the server data driver must restart within the limited time frame so that there is no data loss between the server end modem and the meter end modem [ISO 27001:2013 - 13.1, 17.2]
Data redundancy failure/corrupt	Data redundancy must have all the level of automatic switch over whenever there is blank output or invalid data passage between the file system drive [ISO 27001:2013 - 17.1, 17.2]
Server switching during redundancy	Server must be enhanced to be redundant with the file system, power backup and communication lines. BCP System.
Unauthorized access to the system	Define user controls, validate user controls with suitable control procedure [ISO 27001:2013 - 9.1, 9.2]
Coping the data structure and overloading the server with the local backup	Avoid copying the data files into the same driver or the target folder. Ensure with suitable control handling this system. Auditing, checklist monitoring will reduce this impact [ISO 27001:2013 - 14.2.6]

4. CONCLUSION AND FUTURE WORK

In this paper Information security risk assessment carried on the Grid Monitoring and energy accounting system of the smart grid system. Critical assets were identified and the severity & likelihood of the risks were assessed. Risk handled with risk treatment option with the assessed system. This method can be adopted as model generously across all other systems and sub systems of the Smart Grid systems will provide in detail risk management on the system. By performing this risk assessment and risk handling method with regular intervals will enable us to create risk table and risk handling table. By maintaining & updating risk table & risk handling table will create a database. This database can be used as a reference database in building predictive risk management system. Integrating and combining such many risk table and risk handling table with other system will enable us further to create enhanced predictive risk management system. With this Predictive analysis system Utilities, power generation, monitoring and distribution agencies can select system with less information risks to improve the efficiency of the installed systems, reduce legal & statutory implication and to benefit consumers.

REFERENCES

[1] ISO 27001:2013 - Information Security System Requirements, Available at: http://www.iso.org/iso/catalogue_detail?csnumber=54534.

[2] Goran N. Ericsson, "Management of Information Security for an Electric Power Utility-On Security Domains and Use of ISO/IEC17799 Standard", *IEEE Transactions on Power Delivery*, Vol. 20, No. 2, pp. 683-690, 2005.

[3] Mina Sajjadi and Babak Niknia, "Smart Power Grid Security Services: Risk Management Approach considering both OT and it Domains Case Study: Shiraz Power Distribution Company", *Proceedings of 22nd International Conference on Electrical Distribution*, pp. 1-4, 2013.

[4] Goran N. Ericsson, "Information Security for Electric Power Utilities (EPUs)-CIGRE Developments on Frameworks, Risk Assessment, and Technology", *IEEE Transactions on Power Delivery*, Vol. 24, No. 3, pp. 1174-1181, 2009.

[5] Jian Guan, James H. Graham and Jeffrey L. Hieb, "*A* Digraph Model for Risk Identification and Management in SCADA Systems", *Proceedings of International Conference on Intelligence and Security Informatics*, pp. 150-155, 2011.

[6] Mihaela Ulieru and Paul Worthington, "Holonic Risk Management Framework", *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, Vol. 1, pp. 209-214, 2005.

[7] Eric B. Ricea and Anas Almajalib, "Mitigating The Risk of Cyber Attack on Smart Grid Systems", *Proceedings of Conference on Systems Engineering Research*, Vol. 28, pp. 575-582, 2014.

[8] Yu Jiaxi, Mao Anjia and Guo Zhizhong, "Vulnerability Assessment of Cyber Security in Power Industry", *Proceedings of IEEE PES Power Systems Conference and Exposition*, pp. 2200-2205, 2006.

[9] G. Dondossola, F. Garrone and J. Szanto, "Supporting Cyber Risk Assessment of Power Control Systems with

Experimental Data", *Proceedings of IEEE PES Power Systems Conference and Exposition*, pp. 1-3, 2009.

[10] Friedrich Koster, Michael Klaas, Hanh Quyen Nguyen, Markus Brandle, Sebastian Obermeier and Walter Brenne, "Collaboration in Security Assessments for Critical Infrastructures", *Proceedings of 4th International Conference on Critical Infrastructures*, pp. 1-7, 2009.

[11] Xun Wang and Mary-Anne Williams, "Risk, Uncertainty and Possible Worlds", *Proceedings of IEEE Third International Conference on Social Computing, Privacy, Security, Risk, and Trust*, pp. 1278-1283, 2011.

[12] Robert K. Abercrombie, Bob G. Schlicher, and Frederick T. Sheldon, "Security Analysis of Selected AMI Failure Scenarios Using Agent Based Game Theoretic Simulation", *Proceedings of 47th Hawaii International Conference on System Sciences*, pp. 2015-2024, 2014.

[13] Gao Kunlun, Wang Yufei and Xu Ruzhi, "Study and Practice of Cyber security Situation Evaluation Method for Smart Grid", *Proceedings of International Council of Large Electric Systems*, pp. 1-14, 2014.

[14] Morteza Talebi, Chaoyong Li and Zhihua Qu, "Enhanced Protection against False Data Injection, by Dynamically Changing Information Structure of Microgrids", *Proceedings of 7th IEEE Sensor Array and Multichannel Signal Processing Workshop*, pp. 393-396, 2012.

[15] Dieter Fink, "A Security Frame work for Information Systems Outsourcing", *Information Management and Computer Security*, Vol. 2, No. 4, pp. 3-8, 1994.

[16] Clive Vermeulen and Rossouw Von Solms, "The Information Security Management Toolbox-taking the Pain out of Security Management", *Information Management and Computer Security*, Vol. 10, No. 3, pp. 119-125, 2002.

[17] Edson Dos Santos Moreira, Luciana Andreia Fondazzi Martimiano, Antonio Jose Dos Santos Brandao, Mauro Cesar Bernardes, "Ontologies for Information Security Management and Governance", *Information Management and Computer Security*, Vol. 6, No. 2, pp. 150-165, 2008.

[18] Rossouw Von Solms, "Information Security Management: Why Standards are Important", *Information Management and Computer Security*, Vol. 7, No. 1, pp. 50-58, 1999.

[19] T. Tryfonas, E. Kiountouzis and A. Poulymenakou, "Embedding Security Practices in Contemporary Information Systems Development Approaches", *Journal of Information Management and Computer Society*, Vol. 9, No. 4, pp. 183-197, 2001.

[20] G. Doukidis S. Smithson and G. Naoum, "Information Systems Management in Greece: Issues and Perceptions", *Journal of Strategic Information Systems*, Vol. 1, No. 2, pp. 63-75, 1992.

[21] M.M. Eloff and S.H. Von Solms, "Information Security: Process Evaluation and Product Evaluation", *Proceedings of 16th Annual Working Conference on Information Security*, pp. 11-18, 2002.

[22] Sharman Lichtenstein, "Factors in the Selection of a Risk Assessment Method", *Journal of Information Management and Computer* Society, Vol. 4, No. 4, pp. 20-25, 1996.

[23] A.M. Anderson, "Comparing Risk Analysis Methodologies", *Proceedings of 7th International Conference on Information Security*, pp. 301-311, 1991.

[24] D.J. Bodeaum, "A Conceptual Model for Computer Security Risk Analysis", *Proceedings of 8th Annual Computer Security Applications Conference*, pp. 56-63, 1992.

[25] Alison Anderson, Dennis Longley and Alan B. Tickle, "The Risk Data Repository: A Novel Approach to Security Risk Modelling", *Proceedings of the 7th International Conference on Information Security*, pp. 185-194, 1993.

[26] Richard Baskerville, "Risk Analysis as a Source of Professional Knowledge", Computers and Security, Vol. 10, No. 8, pp. 749-764, 1991.

[27] Janne Merete Hagen, Eirik Albrechtsen, Jan Hovden, "Implementation and Effectiveness of Organizational Information Security Measures", *Information Management and Computer Security*, Vol. 16, No. 4, pp. 377-397, 2008.

[28] E. Albrechtsen and J. Hovden, "Industrial Safety Management and Information Security Management: Risk Characteristics and Management Approaches", *Proceedings of the European Safety and Reliability Conference*, pp. 2333-2340, 2007.

[29] Installation site of MPPTCL.