Intelligent Automation And Soft Computing, 2019
Copyright © 2019, TSI® Press
Vol.25,no.1,121–129

Cyber-security risk assessment framework for critical infrastructures

Zubair Baig[1] and Sherali Zeadally[2]

[1]School of Science, Edith Cowan University
270 Joondalup Drive, Joondalup, Western Australia 6027, Australia

[2]College of Communication and Information, University of Kentucky
315 Little Library Bldg., Lexington, Kentucky 40506-0224, USA
szeadally@uky.edu

ABSTRACT
A critical infrastructure provides essential services to a nation's population. Interruptions in its smooth operations are highly undesirable because they will cause significant and devastating consequences on all stakeholders in the society. In order to provide sustained protection to a nation's critical infrastructure, we must continually assess and evaluate the risks thereof. We propose a risk assessment framework that can evaluate the risks posed to the security of a critical infrastructure from threat agents, with a special emphasis on the smart grid communications infrastructure. The framework defines fine-grained risk identification to help quantify and assess exploitable vulnerabilities within a critical infrastructure.

KEY WORDS: Risk Assessment, Critical Infrastructures, Smart Grid Communications, Cyber Security, Threats

1 INTRODUCTION

A Critical Infrastructure (CI) is defined as a conglomerate of essential and irreplaceable services provided to a nation and its people. According to the US Department of Homeland Security (http://www.dhs.gov/what-critical-infrastructure), sixteen CIs are considered vital for the US economy, incapacitation of which may have severe consequences on the country's population and society at large. These CIs include: Chemical; Communications, Commercial Facilities; Critical Manufacturing; Dams; Defense Industrial Bases; Emergency Services; Energy; Food and Agriculture; Government Facilities; Healthcare and Public Health; Nuclear Facilities and Waste; Water and Wastewater Systems; Information Technology; and Transportation Systems.

Disruption of the operations of such CIs will seriously affect many of the important services that citizens, businesses, government agencies, and others rely on to conduct their daily operations and will very likely lead to catastrophic consequences. A threat is defined as a set of potential activities that when carried out against targeted resources will have a damaging effect (Bayne, 2002). Threats to a resource of a CI can originate from either its natural environment, inadvertent blunders, or from an adversary with a deliberate attempt to cause damage resulting in disruptions or financial losses. Some common threats to a CI include: natural disasters, human errors, system failures, adversarial malicious activities, and missing or ineffective controls. In contrast, risk is defined as the likelihood of a threat against a resource times the cost of the targeted resource (ISO/IEC FIDIS 27005, 2008). The risk posed to a CI's asset needs to identified and managed before the associated threat occurs and causes widespread damage to the infrastructure. Risk management is defined as the process of identifying and assessing the risk, reducing it to an acceptable level and implementing control mechanisms for risk containment (Harris, 2010). Resilience to risk exposure is a common goal of many governmental agencies working together to ascertain uninterrupted operations of a CI. Several resilience strategies, such as those presented in (Australian Government – Northern Territory, 2009) (Australian Government – Queensland, 2010) (Australian Government, 2015), have been developed both at the state as well as at the national levels of developed economies. Included in risk management is risk assessment which is

CONTACT Zubair Baig ✉ zubair.baig@csiro.au

associated with resource identification, vulnerability analysis, threat identification and estimation of possible damage through the occurrence of one or multiple threats. Identification of threats against all CI resources through a vulnerability analysis, is the first step towards risk assessment. The assessment process identifies acceptable and unacceptable levels of risk to a system, and helps develop and enforce policies that govern risk management. The risk management process is applicable to all three tiers of a CI, namely, organizational processes, mission/business processes and information systems (Ross, 2012). An integrated and holistic approach toward the assessment of risks posed to all CI assets, has not yet been considered by any of the above techniques. As part of this contribution, we propose a risk assessment framework for CIs and apply the framework for identifying and quantifying the risk to a smart grid communications infrastructure.

The rest of the paper is organized as follows. We briefly review some common risk assessment frameworks in Section 2. We present our proposed risk assessment framework in Section 3. We apply the proposed framework to assess the risk posed to a smart grid communications infrastructure in Section 4. Section 5 concludes the paper.

2 REVIEW OF RISK ASSESSMENT FRAMEWORKS

THE NIST SP800-30 standard (Ross, 2012) is a comprehensive guide for conducting risk assessments to meet the goals of information security. The guide defines four processes as part of risk management, namely, framing risk, assessing risk, monitoring risk and responding to risk. Furthermore, risk assessment is proposed as a step-wise implementation in the development of a risk assessment questionnaire for a CI, comprising the following questions:

- How to prepare for risk assessments?
- How to conduct risk assessments?
- How to communicate the results to key stakeholders?
- How to maintain risk assessments over time?

The risk model developed in the NIST guide to enable the risk assessment process describes threat sources, events, vulnerabilities exploited, and predisposing conditions (e.g., known bugs in a software deployed on a CI server), impact analysis, and calculated risk. Whilst the risk model may be applicable to both the organizational processes as well as to the underlying business processes and information systems, the exact implementation will depend on a CI's 3-tier infrastructure comprising information systems, organization-wide policies and procedures and business processes. Another observation worth making on the NIST SP800-30 guide is that the recommended guidelines do not consider security controls in an organizational network, and therefore do not provide any guidance on the risk assessment criteria to be adopted for judging the quality of security controls.

In 2013, the US President issued an executive order 13636, "Improving Critical Infrastructure Cybersecurity," (Obama, 2013). In order to enact the stated policy, NIST developed a voluntary risk-based cybersecurity framework (National Institute of Standards and Technology, 2016). The proposed framework incorporates risk assessment as an integral component to enhance the overall cyber-security of a CI. The framework considers risk assessment to include six steps: identification of vulnerabilities to assets, sharing of threat and vulnerability information with other sources, documentation of identified threats/vulnerabilities, analysis of potential business impact and likelihoods of occurrence, determination of risk and risk response recommendations. However, the risk assessment methodology described in (National Institute of Standards and Technology, 2016) does not provide specific details on critical infrastructure analysis and does not describe a holistic approach for assessing risks posed to the CI from both internal as well as external actors. But to quantify and accurately evaluate the risks faced by a CI, we need to consider these actors.

In response to the growing issue of malware penetrating the Korean CI, in (Heo et al., 2008), the authors proposed a framework for identifying the risk posed to the CI from the underlying communication network vulnerabilities. The framework proposed follows the ITU-T X.509 recommendation, which is an architecture to secure end-to-end data communications over a computer network. The risk posed by the individual threats is calculated based on three criteria, namely, the frequency of occurrence, the type of attack and the level of fatality. However, the interdependence between individual components of the CI and the resulting effect on the risk is not considered by the X.509 standard. Therefore, the scope of risk assessment of the proposed framework of (Heo et al., 2008) is limited.

The Astrolabe-based risk assessment methodology presented in (Bagheri and Ghorbani, 2007) models a CI as a complex network of socio-economic systems sustaining critical operations in society. The Astrolabe methodology comprises seven phases that may be adopted for risk analysis. These phases include: boundary specification of several perspectives such as the baseline for normal system operations, time frames for handling a threat and intention of the adversary; perspective identification and systems analysis wherein, the goals and objectives of the system are enumerated, along with an analysis and correlation of actions that the system performs; hazard identification which involves identifying the threats and analyzing the vulnerabilities in the system; consolidation of system-level perspectives of the threat landscape derived from various system components into one common perspective, to enable a complete analysis of the risks; and risk analysis based on all perspectives and interdependencies identified in the previous steps. One of the limitations of the proposed methodology is that the risk assessment only focuses on local feedback from individual components of the system without taking into consideration the organizational processes. Consequently, the Astrolabe-based risk assessment criteria do not provide a complete assessment of the risks that a CI faces.

The European Risk Assessment Methodology (EURAM) (Klaver et al., 2008) defines objectives to identify key elements for general risk assessment, enumeration of interdependencies and procedure definitions for information sharing to create trusted expert networks. The risk assessment process comprises seven steps similar to the NIST 800-30 framework presented above. These steps include: Holistic view of the CI, Holistic scope definition, Definition of risk assessment scales, Asset enumeration, Threat analysis, Identification of security risks/vulnerabilities, and Evaluation and ranking of risk. The applicability of the EURAM to a CI can be measured by the nature and type of risks identified. Whilst the severity levels of identified risk may be defined based on the EURAM, it is inadequate in terms of an in-depth analysis of the impact of a risk on the operation of the CI and subsequent effect(s) on stakeholders involved, including the potential for human life loss.

Risk assessment also depends on the analysis of the ever-changing threat landscape. The Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privileges (STRIDE) model (Wynn et al., 2012) developed by Microsoft is a six-step threat modelling methodology for identifying threats to software-based systems. The model uses a standard pre-defined template for system's information collection in order to ascertain the level of preparedness required to counter all the six threats comprising STRIDE. After the threats have been identified, countermeasures associated with each STRIDE category are implemented. Consequently, the system is redesigned with due consideration given to each threat type.

We summarize the main contribution of this work as follows:

- We propose an integrated framework for the enumeration and quantification of a CI's risk exposure.
- Our proposed framework provides: a better quantification of risk through three phases of assessment, identifies mitigation strategies and quantifies the overhead incurred through the adoption of risk management controls. The framework also quantifies interdependencies between individual components of the CI and quantifies the total risk.
- We present a case-study based on the smart grid communications infrastructure to demonstrate the operation of the risk assessment framework.

3 PROPOSED RISK ASSESSMENT FRAMEWORK

AS our review of related works revealed, the risk assessment strategy for a CI ought to be holistic in nature, encompassing all identified assets, exploitable vulnerabilities, threats and threat agents, and include interdependencies between the various components of the CI. In addition, we need to consider the likely occurrence of specific threats against key resources, as well as the overhead associated with the implementation of relevant and desirable controls to mitigate the impact of the risk. The risk assessment steps proposed in our framework include:

1. Risk identification.
2. Impact analysis.
3. Risk mitigation strategy.

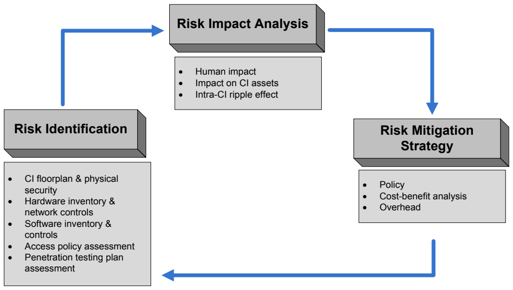

Figure 1: **Proposed risk assessment framework**

3.1 Risk Identification

A CI consists of several components that will vary based on the type of infrastructure. A thorough and descriptive inventory of all assets that constitute the CI is the foremost step to be taken when developing a risk analysis strategy. A framework that ascertains security for a CI is only effective when thoroughly complemented with the identification and recommendation on the deployment of security controls at the most appropriate positions in the infrastructure. The components of our proposed risk identification strategy for a CI include:

- **CI floorplan and physical security**: Essential information about the physical layout of the CI and all constituent components cannot be understated. Without such detailed information, the process of risk identification would remain incomplete. Particular components of a CI floorplan/layout would include information about the physical design aspects of the entire CI. For instance, an electrical power grid floorplan will include information such as the physical location of the power plant, the internal physical layout of the power plant including the physical entry points to the facility, location of each electricity generation and transmission device, transmission substation's location and interconnections, distribution substation's location and interconnections, and all the underlying data communication networks that facilitate the communication between various entities of the CI. The most appropriate approach is to represent the floorplan as a diagram with fine details on each of the above components.

The communication networks of a CI are exposed to adversarial threats that may exploit vulnerabilities of both the physical medium of communication as well as the protocol (and implementation) of the underlying network. Through a risk assessment of all boundary assets of a CI, relevant controls can be identified and recommended to prevent malicious attacks. In addition, during this assessment exercise, it is essential to identify the network security controls deployed and their respective configurations based on corporate-level security policies. These devices comprise firewalls, intrusion detection/prevention systems, proxy servers and traffic analyzers (such as data loggers) (Rahman and El-Shaer, 2013).

- **Hardware inventory and network controls**: A detailed inventory listing of each computing and/or control device that operates as part of the CI must be developed as part of the risk assessment procedure. The inventory should not be limited to specific components or locations as defined in the floorplan above rather should also comprise of complete details about device types, model numbers, version numbers, and year of manufacture, functions, and position relative to other interconnected devices. Depending on the domain of application, a CI typically comprises controllers such as Supervisory Control and Data Acquisition (SCADA) devices (Ralston et al., 2007) (Alcaraz and Zeadally, 2015), Programmable Logic Controllers (PLCs), remote control systems, telemetry systems, computing devices (servers inclusive), and other instrumentation components.
- **Software inventory and controls**: All computing devices that are deployed within the CI hardware run some type of software (including the Operating System (OS)) that must be inventoried. Software evolves with time and OS vendors regularly issue patches to fix bugs, errors or security vulnerabilities identified in their prior product releases. Such practice is also common with other software manufacturers. It is therefore mandatory to enlist all software types, version numbers and details on patches adopted or discarded. Such an inventory enables accurate identification of key vulnerabilities when the CI is holistically analyzed.

  Malware proliferation through a CI is a threat that was demonstrated through recent high profile CI attacks such as the Stuxnet worm (Zetter, 2014), which was only discovered by mere chance, and the lingering threat posed by the BlackEnergy Trojan program found in energy companies both in Europe and in the US (N-dimension solutions, 2016). Through the deployment of targeted malware detection programs for the diverse range of operating systems for all programmable CI devices, including Programmable Logic Controllers, Corporate Computing Devices and Bring Your Own Devices (BYOD) (Antonopoulos, 2011), malware threats can be contained. The act of preserving the operating system's state for potential rollback is referred to as backing-up, which is an essential outcome of software-control deployment (Elmasri, 2007). Software-based controls are also essential in controlling access to classified data items of a CI both through proper access control mechanisms as well as through policy-enforcement for preventing escalation of privileges for authorized users. As a result, data protection is ascertained. Identifying and categorizing data items of a CI alongside their respective levels of sensitivity and threats posed require the development of an efficient risk assessment strategy.
- **Access policy assessment**: Risk assessment must include policies governing access to the physical facility, access to hardware and software assets along with a categorization of access types as well as all anticipated actors (i.e., stakeholders involved). Therefore, after performing an asset inventory (including hardware and software), as well as a record of physical entry points to the CI facility(s), a careful analysis of the policy in place for physical access to the CI must be done. It is also essential to define the level of risk posed to a CI through a detailed analysis of the security policy in place for the CI as a whole. Policy enforcement for accessing a CI's resources and its impact on the security levels of the CI need to be analyzed in conjunction

with the deployed security controls. Risk can only be identified and evaluated if the mechanisms and governing principles for all deployed mechanisms are collaterally assessed. After checking whether all identified CI assets and controls follow the relevant access policies, the risk assessment outcomes can provide valuable feedback which can then be used to restructure and reconfigure specific vulnerable components of the infrastructure.

- **Penetration testing plan assessment**: In order to ensure that the above controls are in place and fully operational in protecting CI assets, a penetration testing plan needs to be developed, implemented and executed at predefined intervals against all computing resources. A set of attack vectors and variants once launched against target resources of the CI network would help identify vulnerabilities which would otherwise have remained exposed to the adversary. These attack vectors are typically launched against the CI assets sequentially and all successful outcomes are enumerated and are recorded on a scoring sheet. A live penetration test on an operational network would thus demonstrate all possible successful attack vectors that would be useful in developing the risk assessment framework.

3.2 Risk Impact Analysis

The list of risks against CI assets, identified through the mechanisms described in the previous subsection, must be quantified to determine the exact level of loss or damage. The following categories of risk impact to a CI are presented:

3.2.1 Human Impact

The risk assessed against a CI can be evaluated in terms of the anticipated number of human lives affected. Essentially the risk of injuries or loss of life as a consequence of a malicious attack must be weighed and pre-calculated. Subsequent application of the most relevant controls to reduce the risk to an acceptable level can therefore be made. For instance, the non-existence of a control to identify malware entering a power utility provider of a smart grid communications network would compromise one or more of its computing devices. Consequently, the malware may trigger disruption in the power supply by manipulating the generator or transformer switch operations, leading to a partial or even a total blackout of a city. The human loss foreseen through such an attack is through car accidents at traffic intersections, life-support patients losing access to power-dependent equipment and through stampedes in heavily populated areas of a city. The weighted risk for such a scenario can be defined as the likelihood of occurrence of such an attack and its effect on end-users.

3.2.2 Impact on CI Assets

The impact of a risk on a CI resource can be evaluated through a detailed enumeration of all CI assets, their respective functions, operational cost involved and loss incurred when asset is compromised, or disabled. Consequently, the risk assessment exercise can recommend effective security controls in order to reduce the risk to an acceptable range. If the value of an asset is $C, and the likelihood of a threat transpiring into an attack against the asset is set to L, the risk for this CI asset is estimated by: $R = N\_{C} * L$, where $N\_{\ C}$ is the normalized cost and $L \in \{0,1\}$. The total risk posed to a CI with A assets, with each asset $i \in A$ exposed to t_i threats, is given by:

$$R = \sum_{i=1}^{A} \sum_{j=1}^{t_i} C_i * L_j \qquad (1)$$

where C_i is the monetary cost of asset i and L_j is the likelihood of threat j transpiring into an attack against asset i and R is the total risk. The presence of a security control will reduce the risk posed by a given threat. We define the effect of asset type on the value of L_j in the following subsection.

3.2.3 Intra-CI Ripple Effect Analysis

Critical infrastructure services are interdependent to facilitate the sharing of knowledge and to coordinate contingency in the event of a malicious attack. Therefore, an interdependency relationship must be established among the various services offered by related infrastructures, as was proposed in (Aubert et al., 2010). The individual interdependencies between CI services are complex and hard to model. Several known mechanisms for identifying such interdependencies have been proposed in (Rinaldi et al., 2001) (Rinaldi, 2004). We model the likelihood of a threat to transpire into an attack by including the interdependencies that exist among the CI services. Consequently, the total risk would be best represented as follows:

$$R_I = \sum_{i=1}^{A} \sum_{j=1, j \neq i}^{A} \sum_{k=1}^{t_i} \max\left(C_i, C_j\right) * L_k * I_{i,j} \qquad (2)$$

where, $I_{i,j}$ is the level of interdependency between assets i and j, and , $I_{i,j} \in \{0,1\}$. The likelihood of a threat transpiring into an attack for a given asset $i \in$A, is correlated to the types and strengths of various security controls in place to protect the CI. Therefore, the quantification of risk (as given in Eq. (2)) represents the effectiveness of the security control towards reducing the threat level and the likelihood of the same threat to transpire into an attack. As such a timeframe for the quantification of the likelihood of a threat to transpire into an attack is not necessary in the context of CI security risk assessment. This is because a threat posed against an asset's vulnerability remains the same throughout the asset's lifecycle for as long as the vulnerabilities remain the same. The likelihood factor is also expected to remain constant for as long as the security controls are not upgraded or modified based on the current threats posed to the asset in question. As a result, the risk calculation defined in Eq. 2 is highly reliable, provided that the factors considered in its calculation are carefully determined beforehand.

3.3 Risk Mitigation Strategy

The level of risk against each asset of the CI is evaluated using the mechanisms described in the previous subsection. The risk is mitigated through the active deployment of security controls. In the presence of a security control, the likelihood of a threat developing into an attack is reduced by E_i, defined as the level of effectiveness of the control in place. E_i can further be quantified as follows:

$$E_i = \frac{Number\ of\ threats\ blocked\ for\ resource\ i}{Total\ number\ of\ known\ threats\ against\ resource\ i} \quad (3)$$

Over a defined period of time, the value of E_i can be estimated based on the number of threats that have been blocked against a resource i. Therefore, in the presence of security control(s) the total risk is best represented as follows:

$$R_C = \sum_{i=1}^{A}\sum_{j=1,j\neq i}^{A}\sum_{k=1}^{t_i}\max\left(C_i, C_j\right) * (L_k - L_K E_k) * I_{i,j} \quad (4)$$

By applying the appropriate mitigation strategies to reduce the risk to an acceptable level, the measurable overhead can be defined as an aggregate cost of resource procurement for risk control, personnel recruitment, and facility redesign. The attitude of CI stakeholders to risk management is essential in taking a decision on whether to accept the risk quantified based on Eq. 2 for a given scenario, or to make a limited decision based on the level of non-reliability of the quantification. This attitude will vary based on the criticality of the system being assessed for risks as well as on the variability of the parameters included in the risk assessment process. In the following section, we apply the proposed risk assessment procedure to the smart grid communications infrastructure.

4 CASE STUDY: SMART GRID COMMUNICATIONS INFRASTRUCTURES

THE Smart Grid (SG) communication architecture includes several heterogeneous components interacting with each other to exchange data in order to enable seamless and cost-effective power usage. The SG has emerged as a platform that allows user feedback into the electricity distribution process. Consequently, the requested power is supplied to the consumers at an adequate level of quality, whilst being cost effective, secure and reliable.

From Fig. 2, the following three communication networks can be identified:

1. Home Area Network (HAN): where household devices and the Smart Meter (SM) interact.
2. Neighborhood Area Network (NAN): facilitating SM to Data Concentrator (DC) communication.
3. Wide Area Network (WAN): facilitating communication between the DC and the centralized Utility Provider (UP).

Risk assessment of the SG requires a clear and robust representation of all vulnerabilities and threats (Knapp and Langill, 2014), existing security controls and policy enforcement criteria. Regulatory frameworks such as NIST smart grid cybersecurity framework (National Institute of Standards and Technology, 2014) recommend protection mechanisms for such systems. By enabling a robust identification of the risks, our proposed risk assessment framework helps provide a thorough security analysis of the SG communications infrastructure.

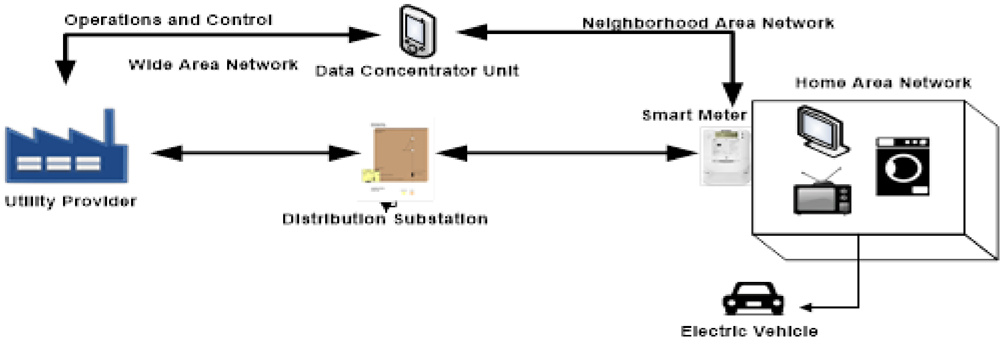

Figure 2. Smart grid communications infrastructure

A. CI floorplan: From the design layout of the SG communications infrastructure (Fig. 2), it is worth noting that physical entry points to the three communication networks , namely, HAN, NAN and WAN, can be curtailed through network-specific access controls. Thus, the risk arising from the threat of physical entry of an adversary to a facility and/or the household of a customer can be reduced to an acceptable level. For a UP or a DC facility, necessary access control through designated security inspection officers at entry points and multi-mode authentication systems for access to critical sections of the SG CI, such as server and data storage rooms, can be identified as controls. The HAN can only have a security guard on premise to make sure that the Smart Meter is only accessible to authorized personnel from the UP or to the household residents.

B. Hardware analysis: The SG infrastructure consists of an underlying communication network and a diverse and interconnected set of computing devices at various zones. Supervisory Control and Data Acquisition (SCADA) systems are computing devices with control capabilities that operate within the power grid substations. These devices are connected to the SG communication network and participate in two-way communications with centralized control servers. The automated nature of substation processes including power generation and distribution are thus at risk of a cyberthreat that may cause process disruptions by tampering with the SCADA functionality. A recent example where the SCADA system was compromised is the cyberattack that made use of the Stuxnet worm (ISO 15408-1, 2005) to cause variations in the nuclear centrifugal systems by injecting malware through open TCP ports on the SCADA devices. Smart meters are vulnerable to threats such as the remote control of these devices. The fundamental security goals of confidentiality and integrity of consumer and utility provider data, and uninterrupted availability of power resource access can be at risk if the smart meters are compromised. Therefore, a thorough assessment of the hardware and its resilience to hardware tampering attempts by the adversary, constitute the risk assessment plan. Manipulation of smart meter hardware can lead to energy fraud wherein household electricity usage can be modified by the adversary.

C. Software analysis: A thorough risk analysis of software (including operating systems) deployed on all computing devices of the smart grid, is enforced through our proposed framework. Risk assessment of software would include the identification of the operating system versions, patches pending and/or installed alongside an inventory of all installed software, protocol stacks supported by the operating system such as TCP/IPv4, number of ports left open on the computing device with appropriate justifications, and an analysis of all auxiliary software such as third-party information collection agents deployed on smart meters as well as those deployed on household devices such as smart TVs and refrigerators. Enumeration of all the above deployed software would embody the risk assessment exercise and would help deliver invaluable recommendations for reconfiguration and/or deployment of security controls required for risk mitigation or elimination.

D. Access policy analysis: The policy in place for role definition and access to all identified assets of the SG infrastructure is essential for facilitating the risk assessment process. Policies, by definition, can only be enforced if they do not encumber the end-user experience and are convenient when implemented. The policy that governs access to sensitive i.e., classified data and computing resources of the SG, must be defined and regularly updated after continuous feedback from all stakeholders (including utility providers' upper management, chief information security officer, security engineer, designated field employees and third-party contractor. By enumerating all risks posed to the SG through an analysis of policies that have been defined and implemented for each stakeholder involvement, we would ensure that the risks posed are indeed quantifiable and can be reduced to an acceptable level of tolerance.

E. Penetration testing plan analysis: A fully operational penetration testing plan would provide invaluable feedback on existing vulnerabilities of the SG. However, without a comprehensive plan in place, penetration testing may lead to disruption in routine activity of the SG causing operational concerns possibly critical in nature. Therefore, as part of our risk assessment framework it is essential to ascertain proper design and implementation of the penetration test plan. For instance, if a port scan and IP address enumeration task generate a large volume of network traffic packets against designated computing devices in the SG utility provider's network, the ingress and legitimate network traffic from data concentrators of a neighborhood area network may be inadvertently dropped, causing a Denial of Service (DoS). The risk posed through such a threat can be mitigated through effective disconnection of the network during testing periods for a predefined time interval.

F. Risk Impact Analysis: Based on the distinct assets of a smart grid communications infrastructure and their level of interdependency, a dependency matrix can be formulated. Table 1 shows the estimated level of dependency among the smart grid assets. We estimate the actual risk posed to the smart grid from several known threats that we have identified above, by using the risk computation equations (3 and 4) defined in the previous section. The resulting risk both with and without security controls in place were calculated for a specific scenario, and the corresponding values of E_i are presented in Table 2

Table 1. **Dependency matrix for the smart grid communications infrastructure.**

	Smart Meter	SCADA System	Communication Network	Data	Data Concentrator Unit	Utility Provider Facility (Servers)
Smart Meter	*	0	0.9	0.8	1.0	0.8
SCADA System	0	*	0.5	0.5	0	0.5
Communication Network	0.9	1.0	*	1.0	1.0	1.0
Data	0.5	0.5	1.0	*	1.0	1.0
Data Concentrator Unit	1.0	0	0.8	1.0	*	1.0
Utility Provider Facility (Servers)	0.8	1.0	0.8	1.0	0.5	*

Table 2. **Quantitative risk impact analysis based on predefined parameters**

Asset	**Asset Value ($)**	**Threat**	**Likelihood**	**Security Controls**	**(E_i)**
Smart Meter	100	Meter compromise, Physical tampering	0.8	Firewall	0.9
SCADA System	100,000	Malware	0.7	Firewall	1.0
Communication Network	50,000	Man-in-the-Middle/ Physical tampering/ Wiretapping	0.4	Data encryption, Tamper-resistant hardware	0.7
Data	50,000	Disclosure, tampering	0.7	Data encryption	0.7
Data Concentrator	10,000	Malware, Physical tampering	0.6	Firewall, Tamper-resistant hardware	0.7
Utility Provider Facility	150,000	Network sabotage, malware	0.5	Firewall, Intrusion Prevention System	0.8

The computed risk R_I, without any security controls in place, is 79% higher than the risk, R_C, with security controls in place.

5 CONCLUSION

WE have highlighted the importance of maintaining a critical infrastructure and ensuring that its operations are uninterrupted to support critical services offered to a nation. Risk assessment is an integral part of this effort and must be comprehensively and holistically addressed. We presented a framework that can identify and analyze the risks posed to a critical infrastructure. The three-step procedure is effective in identifying the most important and dependable recommendations for subsequent risk management. However, the proposed framework would only be as effective as the level of detail provided by stakeholders. Low-level identification of threats, threat agents and exploitable vulnerabilities, including physical assets as well as information resources, would ensure that the risk assessment procedure yields the highest benefit in safeguarding a critical infrastructure.

6 ACKNOWLEDGMENT

WE thank the anonymous reviewers for their suggestions and comments which helped us improve the content and presentation of this paper. Sherali Zeadally was partially supported by a University of Kentucky Research Professorship Award as well as an Edith Cowan University Silver Jubilee Visiting Professorship Award during this work.

7 REFERENCES

C. Alcaraz, and S. Zeadally. (2015). Critical infrastructure protection: requirements for the 21st century. International Journal of Critical Infrastructure Protection, 8, 53-66.

A, Antonopoulos. (2011, July 27). IT security's scariest acronym: BYOD, bring your own device. Network World. Retrieved from http://www.pcworld.com/article/236727/it_securitys_scariest_acronym_byod_bring_your_own_device.html

J. Aubert, T. Schaberreiter, C. Incoul, D. Khadraoui, and B. Gateau. (2010). Risk-Based Methodology for Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures. Proceedings of International Conference on Availability, Reliability, and Security ARES.

Australian Government – Northern Territory (2009). Framework for the Protection of Northern Territory Critical Infrastructure. Northern Territory Government: Australia.

Australian Government – Queensland (2005). Queensland Infrastructure Protection and Resilience Framework. Queensland: Australia.

Australian Government (2015). Critical Infrastructure Resilience Strategy. Australian Capital Territory: Australia.

E. Bagheri and A. Ghorbani. (2007). Risk Analysis in Critical Infrastructure Systems based on the Astrolabe Methodology. Proceedings of 5th Annual Conference on Communication Networks and Services Research.

J. Bayne. (2002). An overview of threat and risk assessment. SANS Institute.

D. Domingues, M. Parks, A. Williams, and S. Washburn. (2012). Special Nuclear material and critical infrastructure security modeling and simulation of physical protection systems. Proceedings of IEEE International Carnahan Conference on Security Technology (ICCST).

R. Elmasri (2007). Fundamentals of Database Systems. Pearson Addison-Wesley.

European Union Agency for Network and Information Security (2012). Smart Grid Security Recommendations.

S. Harris. (2010). CISSP. McGraw Hill.

J. Heo, J. Shin, W. Lee, and Y. Won. (2008). Risk Analysis Methodology for New Critical Information Infrastructure. Proceedings of the 3rd International Conference on Systems and Networks Communications.

ISO 15408-1:2005. Part 1: Introduction and general model – Information technology –Security techniques – Evaluation criteria for IT security.

ISO/IEC FIDIS 27005:2008. Information technology -- Security techniques-Information security risk management.

M. Klaver, H. Luiijf, A. Nieuwenhuijs, F. Cavenne, A. Ulisse, and G. Bridegeman, (2008). European risk assessment methodology for critical infrastructures. Proceedings of 1st International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA).

E. D. Knapp and J. T. Langill. (2014). Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Syngress.

N-dimension solutions (2016). What public power and cooperatively owned utilities need to know. Retrieved from http://www.n-dimension.com/blog/blackenergy-malware-poised-to-compromise-critical-infrastructures-what-public-power-and-cooperatively-owned-utilities-need-to-know/

National Institute of Standards and Technology (2016). Framework for Improving Critical Infrastructure Cybersecurity. NIST.

National Institute of Standards and Technology (2014). Guidelines for Smart Grid Cybersecurity. NIST.

B. Obama. (2013). Improving Critical Infrastructure Cybersecurity. The White House, Office of the Press Secretary: USA.

M. Rahman and E. Al-Shaer (2013). A formal approach for network security management based on qualitative risk analysis. Proceedings of IFIP/IEEE International Symposium on Integrated Network Management.

P. A. Ralston, J. H. Graham, and J. L. Hieb, (2007). Cyber security risk assessment for SCADA and DCS networks. ISA transactions, 46(4), 583-594.

S. Rinaldi, J. Peerenboom, and T. Kelly. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems, 21, 11-25.

S. Rinaldi. (2004). Modeling and simulating critical infrastructures and their interdependencies. Proceedings of 37th Annual Hawaii International Conference on System Sciences.

R. Ross. (2012). Guide for Conducting Risk Assessments NIST 800-30. National Institute of Standards and Technology (NIST).

J. Wynn, J. Whitmore, G. Upton, L. Spriggs, D. McKinnon, R. McInnes, R. Graubart, and L. Calusen. (2012). Threat Assessment and Remediation Analysis Methodology Description. MITRE.

K. Zetter. (2014, November 3). An unprecended look at Stuxnet, the world's first digital weapon. Retrieved from http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

8 NOTES OF CONTRIBUTORS

Zubair Baig is a Senior Research Scientist in Cyber Security with CSIRO/Data61, Melbourne, Australia. He is also an Adjuct Senior Lecturer in the School of Science at Edith Cowan University. His research interests include cybersecurity, machine learning, and digital forensics. Baig received a PhD in computer science from Monash University. Contact him at zubair.baig@csiro.au

Sherali Zeadally is an associate professor in the College of Communication and Information at the University of Kentucky. His research interests include cybersecurity, Internet of Things, networking. Zeadally received a PhD in computer science from the University of Buckingham. He's a fellow of the British Computer Society and the Institution of Engineering Technology, England. Contact him at szeadally@uky.edu