Using Structured Assurance Case Approach to Analyse Security and Reliability of Critical Infrastructures

Kateryna Netkachova[12], Robin Bloomfield[12], Peter Popov[1] and Oleksandr Netkachov[1]

[1] Centre for Software Reliability, City University London, UK
{Kateryna.Netkachova.2, R.E.Bloomfield, P.T.Popov, Oleksandr.Netkachov.1}@city.ac.uk
[2] Adelard LLP, London, UK
{kn, reb}@adelard.com

Abstract. The evaluation of the security, reliability and resilience of critical infrastructures (CI) faces a wide range of challenges ranging from the scale and tempo of attacks to the need to address complex and interdependent systems of systems. Model-based approaches and probabilistic design are fundamental to the evaluation of CI and we need to know whether we can trust these models. This paper presents an approach we are developing to justify the models used to assure CI using structured assurance cases based on Claims, Arguments and Evidence (CAE). The modelling and quantitative evaluation of the properties are supported by the Preliminary Interdependency Analysis (PIA) method and platform applied to a case study – a reference power transmission network enhanced with an industrial distributed system of monitoring, protection and control. We discuss the usefulness of the modelling and assurance case structuring approaches, some findings from the case study, and outline the directions of further work.

Keywords: Assurance Cases·CAE Building Blocks·Critical Infrastructures·Power Transmission Network·Preliminary Interdependency Analysis.

1 Introduction

Reliable and resilient critical infrastructures are of vital importance to the society. Modern infrastructure components often depend on the information systems, which control their operation, monitor activities, provide real-time response to incidents and events. These information systems frequently become the target for cyber-attacks and can pose significant risks to the critical infrastructures (CI).

In this paper we present a systematic practical approach to justifying the models used to assure CI, taking into consideration the possibility of cyber-attacks. Building on the assurance case approach, we are creating a structured security-informed reliability case with the use of specially designed building blocks [1] that are based on the CAE notation [2,3] and provide means for developing a more rigorous justification in assurance cases. The analysis of dependencies between elements of critical infrastructures as well as the quantitative evaluation of reliability properties are performed using the Preliminary Interdependency Analysis (PIA) method and tool [4,5].

The proposed approach addresses three key issues: considerantion of security attacks on the critical infrastructures, system model and assumption justification, and quantitative evaluation of reliability properties for the system under attack. We use the results of PIA to support decisions about the critical infrastructure. The PIA approach deals with the stochastic properties and addresses the aleatory uncertainty. There are also epistemic doubts arising from our lack of knowledge of the world e.g. about the systems being modeled, the attackers. These types of doubts are interrelated and both need to be taken into account in the decision making. In this research we explore how combining the CAE Assurance Case approach with the PIA modeling allows us to do that.

Our approach is demonstrated with a specific case study – an advanced power transmission network – but it is not by any means confined to the power grids and can be used for a wide variety of industrial systems with complex topology and different functional, spatial and other stochastic dependencies between elements.

The paper is organized in the following way: In section 2 we provide a brief overview of the main approaches used. Section 3 introduces the case study. Section 4 demonstrates how the approaches are applied to the case study to create a structured security-informed reliability case. Section 5 summarises the key findings and Section 6 concludes the paper indicating the directions of future research.

2 Overview of the Approaches

2.1 Structured Assurance Cases

An explicit claim-based approach to reasoning about safety, security, reliability and assurance, influenced by the basic model of argumentation developed by Toulmin [6], has been in use for many years. There are various solutions to structure assurance cases [3], [7,8], and to increase rigour and confidence in them [9,10,11]. In this study we use a CAE approach, which provides an effective means for presenting and communicating cases. A graphical notation ASCAD [12] is used to describe the interrelationship of the claims, argument and evidence.

We extend the approach by developing a set of CAE building blocks that restrict the types of argument structures used in a case and help architect cases in a more systematic and rigorous way. Additional information on the building blocks including their definitions, application and guidance can be found in papers [1]. In this paper the building blocks are used to create a structured assurance case fragment for analysing reliability properties of power transmission system under cyber attack.

2.2 Preliminary Interdependency Analysis Method and Tool

Preliminary Interdependency Analysis (PIA) [4] is an analysis activity that helps to understand the range of possible interdependencies between the components of critical infrastructures. The objectives of PIA are to develop an appropriate service model for the infrastructures, and to document assumptions about resources, environmental impact, threats and other factors. PIA is used for both qualitative and quantitative assessment by accounting for both static (topology) and dynamic (behavioural) aspects of the

modelled systems. The key concept of the PIA methodology is representing the system components as continuous-time state machines.

The simulation of the state machines by the PIA tool produces series of events that are then aggregated by a subroutine to calculate the metric of interest. Typically, the metrics are various "loss functions", e.g. the number of failed components, the duration of non-working state of a particular component or a combined characteristic of many components' states. Statistical analysis of the metric data is enabled by repeating the simulation multiple times.

3 Case Study

The case study is based on a reference topology of a Nordic32 electric power transmission system. The network consists of 32 substations operating at different voltage levels: 400kV, 220kV and 130kV. Every substation is organised as a collection of bays. There are four different elements: a line, a transformer, a generator or a load. Each bay connects one of these elements with the bus bar of the substation. Bays also include protection and control units, which are responsible for switching on and off the connected elements. The control devices are typically used by operators or by a special purpose software (SPS) designed to undertake some of the operators' functions automatically and can both connect and disconnect the element from the bus bar. Each protection and control function (with respect to the individual bays) is available when the minimal cut set of equipment supporting the function is available. If the entire minimum cut set becomes unavailable, then the function itself also becomes unavailable.

A structure of the Nordic32 network and the architecture of one of the substations are shown in the Fig.1. Other substations have similar architecture but with a different number of bays. The figure is only meant to provide a high-level overview, detailed discussion of the components is not necessary to understand the rest of the paper.

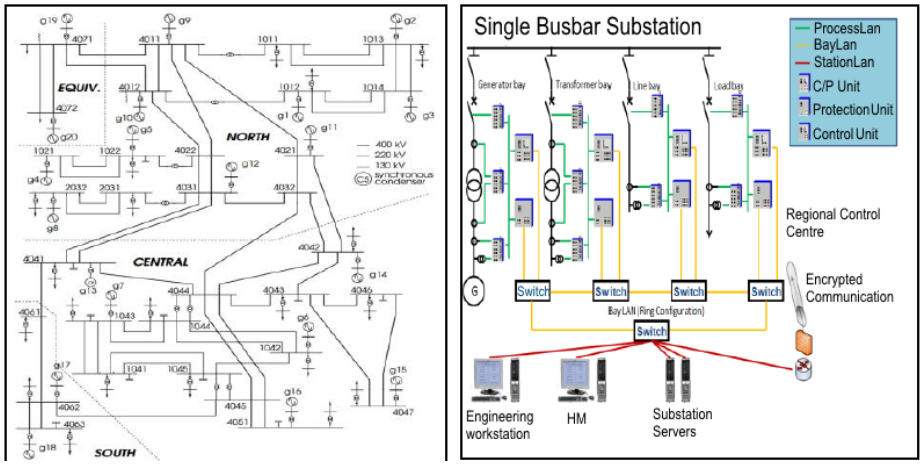

Fig. 1. Overview of Nordic32 system topology (left) and the architecture of a substation (right)

The substations are connected via a sophisticated information and communication technology (ICT) infrastructure, which includes a number of communication channels, control centres and data centres. Every substation has a Local Area Network (LAN), and a firewall protecting the LAN normally ensures that only legitimate traffic can pass through into the LAN from the rest of the world.

The modelled system can be studied with operational environment where only accidental failures are considered as well as those with cyber-attacks. In the later case, a model of Adversary is added in which the Adversary is tightly coupled with the assets. Further details about the case study and the various modeling assumptions can be found in papers [13,14].

4 Analysis of the Case Study

In this study, our main focus is on the system's reliability. We need to provide assurance that the system's critical reliability properties are satisfied – this makes our top level claim. In order to support the top claim, we expand it in a more detailed case using the CAE building blocks structuring approach and eventually demonstrate that the properties are satisfied by using the results from the PIA method and tool. The assurance case is created with the ASCE tool [15].

4.1 Establishing the Environment

As was mentioned earlier, we need to take cyber-security into account when assessing the reliability of critical infrastructures. Cyber-attacks can pose various risks and thus the top claim is too general to be demonstrated by a convincing argument that it is valid. We need to define the claim more precisely by making the adverse environment explicit and considering specific cyber-attacks. This is done by using a Concretion block, and the concreted claim states that "the critical reliability properties of Nordic32 are satisfied under specific design-basis attacks". The instantiated block is shown in Fig.2.

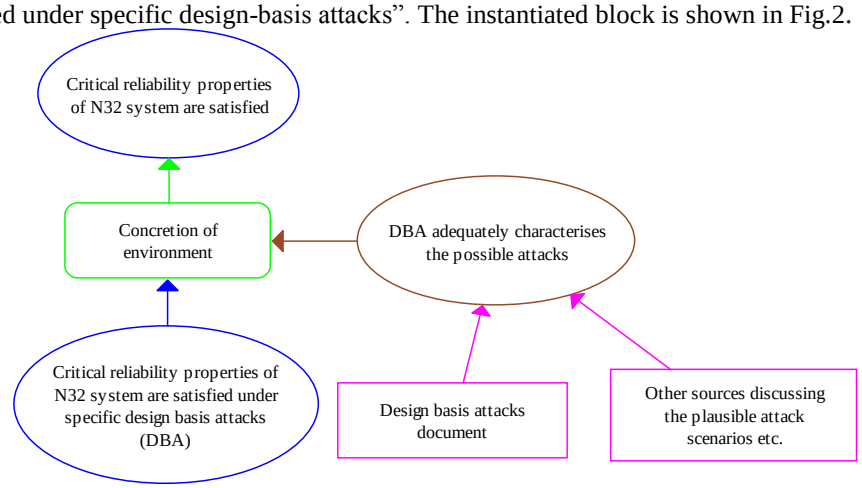

Fig. 2. Concretion making the attacks explicit in the claim

Making environment and attacks explicit in the claim highlights the need to consider various types of attacks, define them in terms of capability, frequency and justify that they adequately represent the possible attacks on the system. For our study, we analysed the effect of a single type of attack on system behavior: a cyber-attack via the firewall of a sub-station. The detailed model of Adversary and attack scenarios we developed are outside the scope of this paper and are described in recent publications [13], [16]. The justification of the models are performed in the side-warrant of the Concretion block. It can be supported by other documents and sources of attack information, e.g. scientific papers, insider knowledge, external expert analysis, and so forth.

At this point, the case could also be decomposed to consider each type of attacks in a separate branch. This could be useful if the case was going to be communicated to stakeholders who are particularly interested in different types of attacks, or if the case is likely to be changed in the future by introducing new types of attacks that could lead to different critical properties to be considered depending on the attacks.

4.2 Substitution of a Model for the Real System

Once the top claim is concreted, the case continues with a Substitution block. For most complex systems, especially the critical ones, it is impossible to perform live analysis. Instead, a model of a system operating in a simulated environment is constructed. Therefore, we substitute the claim about the real Nordic32 system under its design-basis attacks by a model M(N32) under the simulated attacks M(DBA). PIA is used as a platform to create the model. The substitution is shown in Fig. 3.

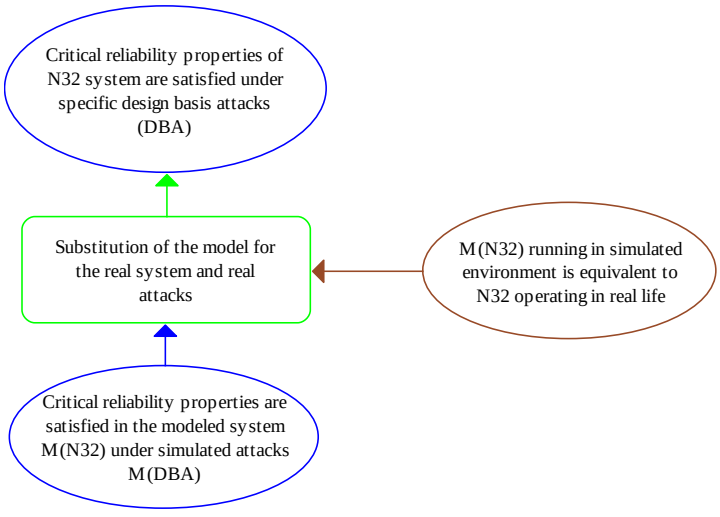

Fig. 3. Substitution of the model for the real system

When such a substitution is made, it is essential to justify that the model is adequate for the specific purpose it is being used for. We start with the side-claim stating that the

modelled system running in simulated environment is equivalent to the real system operating in real life. “Equivalent” is of course context dependent and will need further justification. Therefore, the side-warrant is expanded to justify that all the models adequately represent the reality and that the PIA simulation platform itself is trustworthy. Each model is analysed separately: the model of the system should adequately represent the actual Nordic32 system, the model of the usage should be realistic and the model of the environment should be adequate. The latter includes the models of attacks identified at the previous stage of the analysis, as cyber-attacks are part of the overall adverse environment. The justifications are presented in Fig 4, where the argument nodes of evidence incorporation blocks explain why the findings of the PIA report and research paper are taken as supporting the claim. There may also be further elaboration in terms of CAE, if needed. We used the IEEE research paper [16] as one of the evidence supporting the adequacy of the constructed models. The interaction of the models is considered within the validity of the platform as composing models together is part of the platform requirements. The expanded side-warrant structure with supporting evidence from PIA and other sources are shown in the Fig. 4.

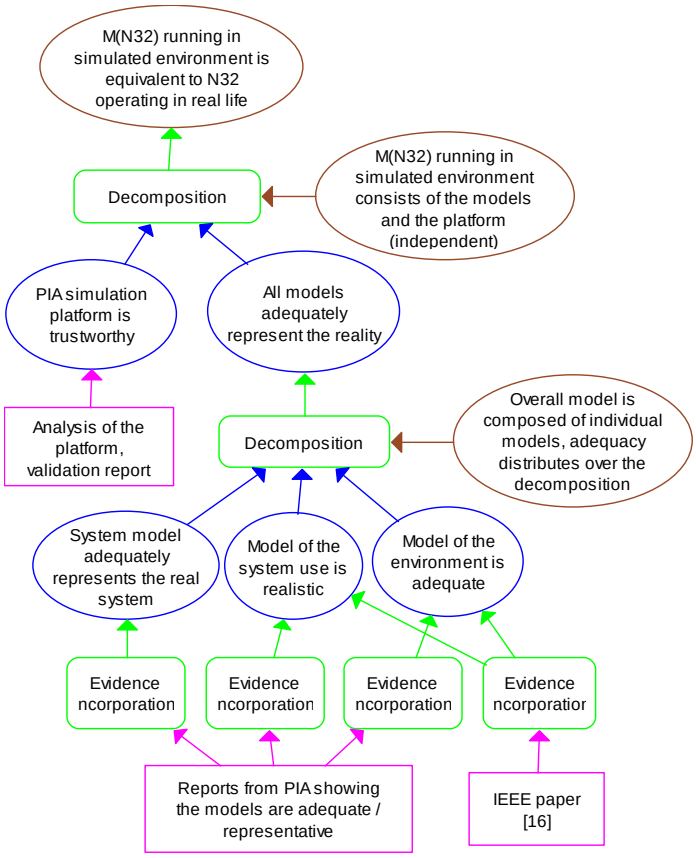

Fig. 4. Justification of the model

4.3 Analysis of Critical Properties

At this stage, we expand the case further by considering specific reliability properties that are to be satisfied. In our case, these are the properties important from the customer point of view, concerning the power loss and availability of the service to consumers. The system must ensure that all consumers are connected to the grid most of the time (consumers should have 99% or better availability of the supply) and the losses do not exceed 20% of the nominal value. The property values should be calculated for individual consumers, not the average one, otherwise some users could be disconnected all the time. The decomposition by the reliability properties is shown in Fig. 5.

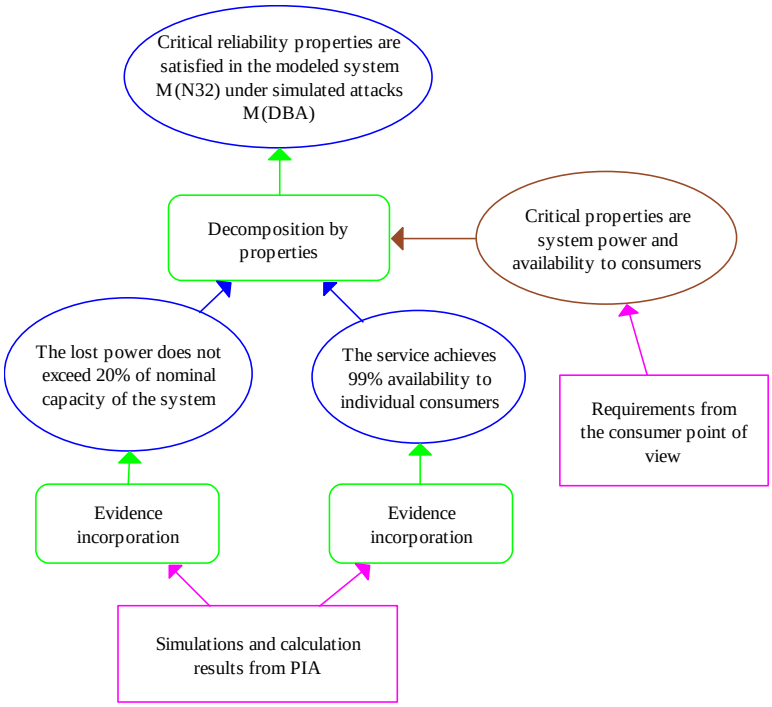

Fig. 5. Demonstration of the critical properties

We used PIA to perform the calculations and justify that the modelled system meets these reliability requirements under the identified cyber-attacks. The effect of cyber-attacks on the service provided by the system was measured using different rewards (utility function) linked to the supplied power. The length of a simulation run was selected be the equivalent of 10 years of operation. The details of our evaluation can be found in papers [13,14]. Evidence Incorporation blocks are used to feed the results from PIA into the assurance case. PIA results returned in the form of JSON file were additionally processed using special aggregation functions (linked to the argument nodes of the blocks) to demonstrate that they indeed support the corresponding subclaims.

5 Findings and Discussions

Overall, we found that structuring case method with the use of CAE building blocks, has enabled us to gain a clear understanding of the key issues that need to be addressed, identify the factors having the major effect on the analysis, and choose the best approach to achieving confidence in the results.

Some of the challenges and observations from our analysis are summarized below:

- Making environment and attacks explicit in the assurance case was essential for the analysis. As cyber-attacks have a great impact on the reliability, we needed to revisit the case study documents with the types of cyber-attacks toward the infrastructure. Some of the attack scenarios were identified by our in-house analysis and the assurance case challenged the justification of our decisions. Other sources discussing the plausible types of attacks also had to be reviewed to provide convincing evidence that they are relevant in a particular context and are indeed part of the security-threatened environment. We'll be continuing investigations into the specific adversary models that need to be considered. Ultimately, the critical properties will only be satisfied for the specific set of attacks so it is important to make an informed well-reasoned decision at this stage of assessment.
- Another crucial factor underpinning the success of analysis was the construction of an adequate model that represents the real system operating in its security-threatened environment. At this stage the assurance case required us to provide convincing evidence that the models of system, its usage and the environment are realistic. In doing so, it was identified that the usage model was not actually realistic and did not correctly represent the use of the system in real life. Specifically, the model of a load had a property defining the power consumed, and the property was set a constant value ignoring the natural fluctuations over time of the consumed power. In reality the power consumption is not constant and the model ideally should reflect this. The model is simplified since the fluctuations are managed by the power utilities, which are not part of the system model. Clearly, the model of the system must be scrutinized and the assumptions it is built upon – validated.
- In terms of the modelling platform (PIA tool), the assurance case also required us to conduct a thorough analysis and provide a validation report for PIA, which has been produced.
- The property evaluation part was substantial and took a considerable amount of time. The studied system is non-trivial, the model consists of more than 1500 state machines. With the chosen parameterisation we observed a significant number (~4000 to 32000) of events over a single simulation run of the system over 10 years of operation. Many of these events require power flow calculations, which take lots of time to complete. Similarly, following overloads or generator failures, active "control" is required to find a new stable system state, which is another time consuming process. As a result, a single simulation run takes approximately 5 min to complete and obtaining results with high confidence requires a very large number of simulation runs.

6 Conclusions and Next Steps

In the paper we presented an approach to analysing critical reliability properties of a power transmission system under cyber-attacks using structured assurance cases and preliminary interdependency analysis method and tool. The paper is centred on the case, which articulates how one should address cyber-attacks and perform the validation of the model before the evidence in support is supplied by the modelling tool.

We believe the presented approach provides a good overview of the important concerns and efforts in assuring the reliability of any complex industrial systems. It discusses the need to explicitly identify adverse environment considering various types of cyber-attacks, justify that the system model can be trusted and show that the model has the required critical properties. Coupled with the PIA method and tool, the approach provides support addressing both aleatory and epistemic aspects of the integrated security and reliability analysis. It can be used for a wide variety of systems and infrastructures.

The future steps will be taken to develop an integrated tool support for the PIA and ASCE assurance case tools. In parallel, we are developing the CAE Building Blocks methodology and resources further, looking into the composite blocks and how these are defined, linking to challenge and review checklists generated from the blocks and more support for the formal aspects of assurance cases. In terms of justifying critical infrastructures properties we have indicated where the case presented in the case study could be expanded for a real industrial system. This is a very active and growing area with a number of research trends on argumentation, confidence and model based approaches and we plan to continue our research in this direction.

Acknowledgement

We acknowledge support from the Artemis JU SESAMO project (grant agreement number 295354), FP7 AFTER project (grant agreement number 261788), and the UK EPSRC funded Communicating and Evaluating Cyber Risk and Dependencies (CEDRICS) project, which is part of the UK Research Institute in Trustworthy Industrial Control Systems (RITICS).

References

1. Bloomfield, R.E., Netkachova, K.: Building Blocks for Assurance Cases. In: IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW) 2014, pp. 186-191, doi:10.1109/ISSREW.2014.72.
2. Bloomfield R. E., Bishop P. G., Jones C. C. M., Froome P. K. D.: ASCAD – Adelard safety case development manual. London (1998)
3. ISO/IEC 15026-2:2011, Systems and software engineering — Systems and software assurance, Part 2: Assurance case. (2011)
4. Bloomfield, R.E., et al.: Preliminary Interdependency Analysis (PIA): Method and tool support. p. 56. Adelard LLP (2010)

5. Bloomfield, R.E., Chozos, N., Nobles, P: Infrastructure interdependency analysis: Requirements, capabilities and strategy. Adelard document reference: d418/12101/3, issue 1 (2009).
6. Toulmin, S. E.: The uses of argument. Cambridge University Press (1958)
7. Bishop P., R. Bloomfield: A Methodology for Safety Case Development. Safety-critical Systems Symposium 98, Birmingham, UK, ISBN 3-540-76189-6 (1998)
8. Kelly, T.: The goal structuring notation–a safety argument notation. In: Proc. DSN 2004 Workshop on Assurance Cases (2004)
9. Hawkins, R., Kelly, T., Knight, J., Graydon, P.: A New Approach to creating Clear Safety Arguments. Proc. 19th Safety Critical Systems Symposium (SSS 2011), p. 3-23. Springer, London (2011)
10. Littlewood, B., Wright, D.: The use of multilegged arguments to increase confidence in safety claims for software-based systems: A study based on a BBN analysis of an idealized example. In: IEEE Transactions on Software Engineering, 33(5), pp. 347-365. doi: 10.1109/TSE.2007.1002
11. Denney, E. W., Pai, G. J.: A Formal Basis for Safety Case Patterns. 32nd International Conference on Computer Safety, Reliability and Security (SAFECOMP 2013), LNCS 8153, pp. 21-32. (2013)
12. Bloomfield, R.E., Bishop, P.G., Jones, C.C.M., Froome, P.K.D.: ASCAD – Adelard safety case development manual. London (1998)
13. Netkachov, O., Popov, P., Salako, K.: Model-based Evaluation of the Resilience of Critical Infrastructures under Cyber Attacks. Paper presented at the 9th International Conference on Critical Information Infrastructures Security (CRITIS 2014), 13-10-2014 - 15-10-2014, Limassol, Cyprus (2014)
14. Netkachov, A., Popov, P., Salako, K.: Quantification of the Impact of Cyber Attack in Critical Infrastructures. In 1st International Workshop on Reliability and Security Aspects for Critical Infrastructure Protection (ReSA4CI 2014). 2014 Florence, Italy (co-located with SAFECOMP 2014): Springer International Publishing (2014)
15. Assurance and Safety Case Environment (ASCE) Help File. Adelard LLP, [Online]. Available: http://www.adelard.com/asce/ [Accessed: 29 June 2015]
16. Ten C.-W., Liu C.-C., Manimaran, G.: Vulnerability Assessment of Cybersecurity for SCADA Systems. In: IEEE Transactions on Power Systems. 23(4), p. 1836-1846 (2008)