Report on Smart Energy Systems and Cyber Security*

Razgar Ebrahimy, Charles Morisset, Haris Patsios, Zoya Pourmirza
Newcastle University
first.last@ncl.ac.uk

July 2018

Abstract

Digitalization, real-time data, autonomous operation and ICT are all available to aid energy system integration, to provide more robust, reliable and on demand services to consumers and to enable producers a more flexible supply, utilizing various resources. However, with such tight integration the risks of systems failure is becoming even greater, specifically cyber threats against the energy systems. Newcastle University organised in April 2017 the First International Cyber Security Workshop in Smart Energy Systems gathering experts from academic institutions and industrial partners, from around the world, to discuss the current security risks to the smart energy systems, the current approaches and the possible future solutions. This document reports on the findings of this workshop.

1 Introduction

Globally, the energy systems are going through a rapid transition period of adapting renewable resources and information communication technologies (ICT) solutions into their current operations [1, 2, 3, 4]. Renewable energies help in reducing carbon footprints, cope with the increasing energy demands and ICT enables the energy systems to become more efficient, responsive and autonomous.

The role of ICT sector for the energy sector is becoming more prominent, vital and necessary for the sector operation. The transitions of energy sectors into smart grids has opened new opportunities to the energy providers to become more resilient, robust and cost effective. For the consumers, smart grids provide them with the ability to manage their energy consumption based on the time of usage and suggested time slots by their provider and in return consumers enjoy the remuneration schemes provided by the utility operators.

The rapid adaptation of ICT has also unveiled some of the unforeseen and critical risks that are associated with it that could potentially

*This report and the related workshop was funded by the EPSRC Project *HubNet: Research Leadership and Networking for Energy Networks*, EP/I013636/1.

jeopardize the entire operations of the smart energy systems (SES). The concept of connectivity and surveillance in all layers of the SES and the underlying networks at all times, with having access to the real-time data exchanged between the layers, is fundamental to the SES to operate in an efficient and effective manner. However, with a great degree of connectivity the risks of system failures resulting in triggering cascading failures are increasing [5]. This is when cyber domain is becoming very important to protect and defend to avoid, prevent and minimize any such failures that are caused by cyber domain.

In addition to the natural disasters and physical and mechanical failures, cyber security is another topic that has been of a great interest. The energy assets are among the most important and vital points to protect and defend in warfare, espionage and cyber-attack [USA-CIS]. The availability of the energy sector is so vital in all levels of the society that contemplating and facing a cyber-attack on any level of the energy systems could have catastrophic implications on both safety of the individuals and also to the operations of the dependent systems [6]. One of most recent cyber attack incident on the energy systems occured on December 2015 in Ukrain where over 25 local substations were affected and resulted in power outages with approximately 220,000 costumers affected [7].

In general, the energy providers are familiar, well prepared and resilient for sudden mechanical failures or physical disturbance to their assets that affect segment of their systems only. With the cyber-threats, utility providers are not so resilient against it. For instance in the power sector, if the cyber attack is happing in a large scale where the reserve capacity is not enough to compensate the service disruptions, operations [8].

This is why, cyber security solutions in the energy systems can not be based on a single task solutions but instead it should be a collection of solutions that bridges between the various systems that also provide insight and measure failure implication in all systems involved.
This report is prepared based on the insight, challenges and advise provided in the cyber security workshop NCl by a panel of experts from both industry and academia.
The remaining of this report is organized as follow, section 2 is providing and overview of current challenges, section 3 is about what the possible solutions could be. Section 4 focuses on the workshop held in Newcastle with the summary of the report followed in section 5. The appendix has three sections consisting of list of participants as A followed by the workshop agenda as B and the summary of the workshop as C.

2 Current challenges identified

Within the energy system engineers, industries, policy makers and regulators the importance of protecting the energy systems against cyber attacks and cyber failures is widely accepted. Nowadays, security in the energy systems refers to both its original definition on ensuring the security of supply and protecting it against cyber failures and cyber attacks. The energy systems are very resilient against physical and non-cyber related failures that can withstand huge interruptions which are not visible to the energy consumers[10]. However, the digital and cyber failures are

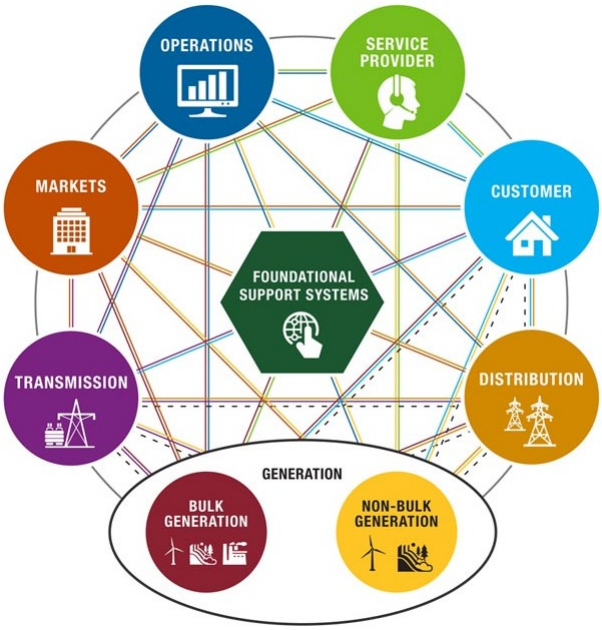

Figure 1: Smart energy systems (SES) domains and sub-systems [9]

relatively a new domain that could lead to cascading failures with a catastrophic impact on both the energy providers and the energy consumers. To this point, there are various challenges both in terms of providing technical solutions that protect the systems against the cyber attack and also the socio-technical aspect of it that includes the consumer as part of the solution. This is the reason the cyber security in the energy sector attract a diverse solutions from power engineers, cyber security experts, energy providers, energy market operators, social scientist, policy makers and solution providers.

2.1 Types of cyber attack in the energy sector

Energy systems are heterogeneous, complex, multi layered, interconnected, highly coupled and are dependent on various external factors to operate and therefore the threats vary in type, target and implications. The threats range from power system control command, market price information, consumer's meter data manipulations to the monitoring software [11].

In addition a variety of communication networks are interconnected with the energy systems to provide sensing, monitoring and control. These communications networks are associate with the supervisory control and data acquisition (SCADA) systems to manage the real time energy system and provide real-time control. It is not surprising that such systems can be targeted from various technological points of views. Some commonly threats known in the energy sector are, communication interception and network analysis, traffic modification and fault injection, authorization violation, spoofing of the utility systems and denial of the services by re-

source exhaustion and signal jamming [12] which are the indication to the extent that needs to be protected.

2.2 Risk Awareness and communication technologies

SCADA systems have been providing the monitoring and control mechanism to the energy sector and have enabled the operators to be more efficient and responsive to the system changes. Nonetheless, SCADA systems were designed to operate on the private network and to be totally isolated from the Internet. However, the shift in the energy sector to become technologically smarter and to become even more dependent on real-time data to enable demand and response management , means that SCADA systems also need to be integrated with the new technologies and in some point operate outside their private network. In addition, security has not been part of the initial design of early SCADA systems, meaning that they lack encryptions and authentications. Although, some of the newer types of SCADA systems such as remote terminal units (RTUs) are Internet enabled and provide some layer of security but the deployment of these advanced RTUs in the field is very limited due to the huge financial implication on the operators[13].

Monitoring and control in the energy sector is not a new task to the operators, in contrast it has been very well researched and investigated [14]. However, the resolution and depth of the monitoring and control has been relatively based of the transmission layer of the power systems with very limited ICT capabilities in the distribution layer. The visibility of the distribution network is very limited as not all the substation are ICT enabled (only up 11KV) and this limits the ability to control and monitor such assets remotely. In addition in terms of numbers, these asset constitute most of the nodes in the energy sector that can not be controlled or monitored remotely.

The emergence of smart grid in the power grid infrastructure with the objective to provide efficiency, reliability and safety based on available real-time data of the utility providers and consumers, has highlighted the importance of risk awareness and risk assessment tools in the energy sectors. With the modern smart grid systems, the risk assessments are no longer only limited to physical and mechanical failures but they also include the cyber failures and cyber attack implications on the system. For the utilities and solution providers the challenge is the ability to distinguish between possible stealthy cyber-attacks and more traditional failures[cite the workshop]. The ability to determine the cause is important because it paves the way for the next move to how to prepare and provide a response to such incidents while the risk levels are explained and visualized in a form understandable by system operator while still delivering the service to the consumers.

2.3 Cyber-security concerns in communication Infrastructure of Smart energy systems

Smart Energy systems contains a number of communication infrastrtructure such as Supervisory control and data acquisition (SCADA), Advanced

Metering Infrastructure (AMI), and Customer energy Management system (CEMS). Each of these communication infrastructures are vulnerable to cyber-attack from different perspectives.

In an electrical distribution grid, the SCADA (Supervisory Control and Data Acquisition) system that provides the communication infrastructure across the electrical grid from 11 kV to 132 kV is used as the intelligent monitoring system in place. SCADA systems are vulnerable to cyber-attacks due to: lack of active network monitoring and traffic monitoring, insufficient reporting capabilities of some connected devices, and Weak authentication scheme.

Advanced Metering Infrastructure (AMI) enables communication between energy consumers (customers) and the utility. AMI systems are vulnerable to attacks mainly due to lack of coordinated security policies and technologies amongst various components of the system.

Customer Energy Management System (CEMS) is an application service or device that communicates with devices in the customer home. It may have interfaces to the smart meter to read usage data or to the operations domain to get pricing or other information to make automated or manual decisions to control energy consumption more anciently. CEMS systems are vulnerable to cyber-attacks due to use of public communication systems, such as internet. Additionally, customer privacy is major drawbacks of such systems.

3 Possible solutions

In the available literature different types of solutions are suggested that tackle specific problems. Based on what is out there in can be infered that most of single solutions can only solve one problem or one type of attacks. Since there are variety of attacks that can be performed on the energy systems, solutions need to be combined and in some cased used in parallel with other techniques to gain the full advantages. The following are some of the possible solutions that can be adapted.

3.1 Specific security solutions

As mentioned earlier, the energy sector by nature is complex, interconnected, interdependent and heterogeneous. Therefore modeling such sector that includes all the layers with a detail representation of the networks, functionality and operation is a daunting task. This is why when modeling such system have been attempted, most focus has been to include few elements in the model and study the risk, behavior and failure implications in an abstract level. Or if the model includes the information communication technology (ICT) the models also include the availability of telecommunication as an element in the model with an abstract representation of the system. Though such models provide a very good insight to the operators in how to react to specific changes [15], recovering strategies [16, 17] or how to optimize the resource [18, 19] the operation for a specific conditions, the models lack the comprehensive visibility of the sector. And it is very important, for instance to be able to foresee the implication and ability to measure the consequences of a cyber attack in

case of a cyber attack on the energy system.

3.2 Co-modelling

Since modeling every possible outcome is almost impossible to envisage, one solution and strategy could be by utilizing co-modeling where you can have both the physical representation models, network and hierarchy and topology models along with cyber models .

In this case, co-modeling could refer to a various kinds of models that are modeled discretely but all run parallel to provide advise or help in mitigating the implications. The following are some examples to what the discrete models cold be;

1. Physical representation of the energy sector that include the network topology and power system analysis that reflect the physical property of the power systems,
2. The ICT integrations that includes the SCADA and telecommunication,
3. The real-time analysis of data generated from 1 and 2 for the ongoing operation of the system,
4. Threat models that include various types of attack vectors that can be tested on 1,2 or 3,
5. Risk assessment model that measures the implication of 4 on the operation of model 1

Though these are not an exhaustive list but rather some indications and directions to follow. The co-modeling idea is to models heterogeneous behaviour and combine them together, run some scenarios that fit all the individual models in order to provide a comprehensive solution .

3.3 Security response mechanisms

The cyber vulnerabilities within the smart energy sector are mainly based on two types; cyber vulnerabilities in the smart energy systems and cyber physical attacks on the smart energy sector [14]. The first refers to vulnerabilities that includes users as part of the system as well as protecting and enhancing the mitigation approaches. One suggestion by [14] is to educate the energy users about the risks of the smart energy sector so they become part of the solution rather than the weak link in the system.

Since the types of attacks on the smart energy sectors varies therefore the solution and protective mechanism should also reflect that and in this manner the response can be specific and to be built to fit the purpose.

There is a need for dedicated response mechanisms that can be triggered when an attack is detected, taking into account cyber and physical impacts. In the electricity market, [20] has already identified some of the main issues in this areas and provides a foundation for the future research in how to minimize the attack implications.

One method of protection against targeted attacks in the energy system that attempt to mitigate the the implications is using the blockchain technology. Blockchain is designed to eliminate the need of a third parties

in transactions in the middle to achieve peer-to-peer electronic payments [21]. Although blockchain has been designed to tackle financial issues however the idea of it is been applied in many branch of science. In the energy systems domain [22] has proposed a blockchain based data protection that eliminates the possibility of attack implications in a various power system layers. The framework utilizes the distributed security features of blockchain technology to enhance the self-defensive capabilities of the energy systems against cyber attacks.

4 Smart energy cyber-security workshop

In December 2015, a synchronized and coordinated attack compromised three Ukrainian regional electric power distribution

companies resulting in power outages affecting around 220,000 customer for several hours [23]. The cyber attack on the Ukrainian power system is the first known cyber attack that has been recorded. In addition the attack highlighted some serious flaws in the existing systems where the attackers inside knowledge about the system could increase the level of distractions and also sabotage the recovery procedures as it was the case with Ukrainian cyber attack. This attack was a motivation to organize an international cyber security workshop on 11 April 2017 hosted by the security and power system groups at Newcastle university to gather the views of both the industry and academic participants to aid in building and designing the next generation cyber attack protection tools.

5 Summary & conclusion

The energy sector is the backbone of today's living societies. There are great efforts in digitalization of the energy systems, and in addition we are at a period where legacy energy systems are integrated with newer and more renewable energy systems across the globe. Digitalization (eg. smart grid) of the energy systems enables the energy providers to become more efficient and optimize the generations and available capacity. However, digitalization means relying heavily on ICT technologies and integrating it with the existing and future energy systems. Digitalization provides numerous benefits and flexibilities to the energy systems but with some cost attached. Apart from the operational cost, ensuring that these systems are secure and resilient against cyber attacks is very crucial. For this reason cyber security of the energy system should become part of the current integration. Since the energy systems are complex and diverse we require different cyber security solutions that could fit various layers of the energy sector. It is not feasible to come up with a single solution that fulfills all cyber security concerns in the energy systems but instead it is an ongoing process that should involve all of the energy producers, users and regulators.

References

[1] Smart grid strategy the intelligent energy system of the future. `https://ens.dk/sites/ens.dk/files/Globalcooperation/smart_grid_strategy_eng.pdf`, May 2013. (Accessed on 05/05/2018).

[2] Nick Jenkins, Chao Long, and Jianzhong Wu. An overview of the smart grid in great britain. *Engineering*, 1(4):413 – 421, 2015.

[3] Accenture's Digitally Enabled Grid program. Forging a path toward a digital grid_global perspectives on smart grid opportunities. `https://www.accenture.com/se-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Forging-a-Path-toward-a-Digital-Grid_Global-Perspectives-on-Smart-Grid-Opportunities.pdf`, 2014. (Accessed on 06/12/2018).

[4] D. Connolly, H. Lund, and B.V. Mathiesen. Smart energy europe: The technical and economic impact of one potential 100 *Renewable and Sustainable Energy Reviews*, 60:1634 – 1653, 2016.

[5] B. Mukherjee, M. F. Habib, and F. Dikbiyik. Network adaptability from disaster disruptions and cascading failures. *IEEE Communications Magazine*, 52(5):230–238, May 2014.

[6] T. B. Rasmussen, G. Yang, A. H. Nielsen, and Z. Dong. A review of cyber-physical energy system security assessment. In *2017 IEEE Manchester PowerTech*, pages 1–6, June 2017.

[7] Defense Use Case. Analysis of the cyber attack on the ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, 2016.

[8] Ijeoma Onyeji, Morgan Bazilian, and Chris Bronk. Cyber security and critical energy infrastructure. *The Electricity Journal*, 27(2):52 – 60, 2014.

[9] Ieee smart grid domains - ieee smart grid. `https://smartgrid.ieee.org/domains`. (Accessed on 06/12/2018).

[10] Z. Bie, Y. Lin, G. Li, and F. Li. Battling the extreme: A study on the power system resilience. *Proceedings of the IEEE*, 105(7):1253–1266, July 2017.

[11] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli. Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2012.

[12] R. Berthier, W. H. Sanders, and H. Khurana. Intrusion detection for advanced metering infrastructures: Requirements and architectural directions. In *2010 First IEEE International Conference on Smart Grid Communications*, pages 350–355, Oct 2010.

[13] S. Sridhar and G. Manimaran. Data integrity attacks and their impacts on scada control system. In *IEEE PES General Meeting*, pages 1–6, July 2010.

[14] M. M. Pour, A. Anzalchi, and A. Sarwat. A review on cyber security issues and mitigation methods in smart grid systems. In *SoutheastCon 2017*, pages 1–4, March 2017.

[15] X. Liu, Z. Bao, D. Lu, and Z. Li. Modeling of local false data injection attacks with reduced network information. *IEEE Transactions on Smart Grid*, 6(4):1686–1696, July 2015.

[16] T. Kohler, J. P. Steghöfer, D. Busquets, and J. Pitt. The value of fairness: Trade-offs in repeated dynamic resource allocation. In *2014 IEEE Eighth International Conference on Self-Adaptive and Self-Organizing Systems*, pages 1–10, Sept 2014.

[17] C. Cameron, C. Patsios, P. Taylor, and Z. Pourmirza. Using self-organizing architectures to mitigate the impacts of denial-of-service attacks on voltage control schemes. *IEEE Transactions on Smart Grid*, pages 1–1, 2018.

[18] C. Zheng, D. Li, Y. Xi, and X. Wang. Hybrid modeling and optimization for energy management system of microgrid. In *2016 35th Chinese Control Conference (CCC)*, pages 10013–10018, July 2016.

[19] M. Carrasco, F. Mancilla-David, A. Angulo, J. Weston, and P. Papantoni-Kazakos. Proximal jacobian distribution optimal power flow in a distributed cyber-physical environment. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 7(2):319–328, June 2017.

[20] M. A. Mustafa, S. Cleemput, and A. Abidin. A local electricity trading market: Security analysis. In *2016 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, pages 1–6, Oct 2016.

[21] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[22] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong. Distributed blockchain-based data protection framework for modern power systems against cyber attacks. *IEEE Transactions on Smart Grid*, pages 1–1, 2018.

[23] Cyber-attack against ukrainian critical infrastructure. `https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01`. (Accessed on 05/05/2018).

A List of participants

List of the workshop participants		
Name	Affiliation	email
Luca Arnaboldi	Newcastle University	
Mustafa Asan Mustafa	University of KU Leuven	mustafa.mustafa@kuleuven.be
John Brooke	consultant	jmartinbrooke@gmail.com
Calum Cameron	Newcastle University	
Sara Cleemput	University of Leuven	
Stephen Cooper	Northern Power grid	Stephen.Cooper@northernpowergrid.com
Randle Cowcher	Northern Power grid	Randle.Cowcher@Northernpowergrid.com
Sarah Darby	University of oxford	sarah.darby@ouce.ox.ac.uk
Razgar Ebrahimy	Newcastle University	razgar.ebrahimy@ncl.ac.uk
Hasan J Uppal	University of Manchester	hasan.uppal@manchester.ac.uk
Cliff Jones	Newcastle University	cliff.jones@ncl.ac.uk
Kenn Keefe	University of Illinois	kjkeefe@illinois.edu
Jianing Li	University of Birmingham	j.li.6@bham.ac.uk
Jon Longstaff	Siemns	jon.longstaff@omnetric.com
Zofia Lukszo	TU Delft	Z.Lukszo@tudelft.nl
Charles Morisset	Newcastle University	charles.morisset@ncl.ac.uk
Haris Patsios	Newcastle University	haris.patsios@ncl.ac.uk
Ken Pierce	Newcastle University	kenneth.pierce@ncl.ac.uk
Peter Popov	City University London	p.t.popov@city.ac.uk
Zoya Pourmirza	Newcastle University	Zoya,pourmirza@ncl.ac.uk
Robin Preece	University of Manchester	robin.preece@manchester.ac.uk
Roy Proud	Newcastle University	
Michalis Smyrnakis	The Univeristy of Sheffield	m.smyrnakis@sheffield.ac.uk
Hongjian Sun	Durham University	hongjian.sun@durham.ac.uk
Phil Taylor	Newcastle University	phil.taylor@ncl.ac.uk
Aad van Moorsel	Newcastle University	aad.vanmoorsel@ncl.ac.uk
Yilei Wang	Newcastle University	

B Agenda

International Workshop on Cyber Security in Smart Energy Systems

Newcastle University, Devonshire building, room G21/G22 NE1 7RX

11th April 2017

Organisers: Razgar Ebrahimy, Zoya Pourmirza, Charles Morisset, Haris Patsios, Cliff Jones, Phil Taylor.

Agenda

10:15	**Registration and Coffee**
10:30	**Introduction** **Charles Morisset** - Lecturer in Security, School of Computing Science, Newcastle University **Haris Patsios** - Lecturer in Power Systems, School of Electrical and Electronic Engineering, Newcastle University
10:40	Newcastle University Power System Group – CESI **Phil Taylor**- Deputy PVC of Faculty of Science, Agriculture, and Engineering, Newcastle University, Director of the EPSRC National Centre for Energy Systems Integration (CESI), Siemens Professor of Energy Systems
10:50	Cyber security @ NCL **Aad van Moorsel**- Head of School of Computing Science in Newcastle University, Professor in Distributed Systems
11:00	**Session 1- Risks** What are the cyber-security risks in smart energy systems?
11:00	**Peter Popov**- City University of London, "Stochastic models for risk assessment in Cyber-Physical Systems: Achievements and Challenges."
11:10	**Zofia Lukszo-** Delft University of Technology, "Vulnerabilities and risks in smart grids."
11:20	Small groups discussion
11:50	**Break & Networking**

12:05	**Session 2 – Current Approach** Which threats types have the highest importance/implications, and what are the current practices to tackle them?
12:05	**Kenneth Keefe**- University of Illinois," Cyber-physical threat model in ADVISE of a smart grid system"
12:15	**Sarah Darby**- University of Oxford, "Energy and cyber security at different scales - user needs and perceptions"
12:25	**John Brooke**- Independent Software Consultant, "Cybersecurity issues in online modelling of Water Distribution Networks"
12:35	Small groups discussion
13:00	**Lunch & Networking**
14:00	**Session 3 – Solutions** What could be the practical solutions, both economically and technologically?
14:00	**Mustafa A. Mustafa**- University of Leuven," Secure and Privacy-friendly Peer-to-Peer Electricity Trading"
14:10	**Hongjian Sun**- Durham University, "Detecting bad data injection in Smart Grids"
14:20	**Michalis Smyrnakis**- Sheffield University, "A three actions game applied to a cyber-security problem"
14:30	Small groups discussion
15:20	**Feedback**
15:40	**Summary of the day**
16:00	**Closure**

C Summary of session

C.1 Risk session - workshop views

In this session the main arguments have been how to model and quantify risks in smart energy systems. There were different points of views in terms of what the risk is, depending on the fields of the experts in the workshop. It was quite evident based on the discussions that there was a general consensus around risk mitigations and what needs be done and how to evaluate the approaches. For instance it was pointed out that in order to capture the risks and the implications of risks in the SES it is vital to combine models that represents the cyber physical properties of the system as well as interdependent systems. Physical world model, control and instrumental model and any adversary or failure models, all need be studied and investigated in parallel to accurately represent the SES state when facing cyber risks. Interestingly it seemed that industries participants are very familiar and prone to failures and risks in their systems. They are usually expecting physical and natural failures in their systems on regular a bases and not surprisingly planning well ahead in how to react/recover and what do if that happens. However they have pointed it out that their main challenge with the new failures is, deciding whether a system failure is the result of cyber attack or its is one of the known causes already known by the industry. As an ongoing system monitoring and normal activity, they observe the power outages, systems destructions on their underlying systems on a daily bases. However to decide whether a fuse tripping in a cyber enable component is a physical or random failure or perhaps a consequence of a cyber-attack seem to be a challenging task from the industry point of view. Based on the smart grid architecture, it was argued that any risks or cyber threats could influence and jeopardise any layers identified in smart grid architecture model (SGAM). Each layer has different and diverse purposes and cyber-attack could influence the system at any of the levels with serious implications. For instance a cyber risk could target a business layer, component layer or communication layer. This means that there is a greater need for models that can include all of the layers in SGAM to enable us in identifying and tracing risks. Also it was pointed out in the discussions that such models might be very complex and in some points, not feasible to build because of the complexity, heterogeneity and interrelationships among all the layers of SGAM. Although based on another discussion some argue for using hazard and operability (HAZOP) as a known methods for evaluating the security of energy systems, since the method is used widely in the safety critical systems. However it was clarified that HAZOP is not able to provide enough insight for a complex, very large and interdependent system such as smart energy systems and instead suggested hybrid models that can capture emerging properties.

C.2 Current Approaches Session

In terms of what is out there to tackle cyber security in the energy systems, number of tools and solutions have been mentioned. Mobius developed by Illinois is one of the tools that is gaining high reputations for it is use in modelling the security of energy systems. Mobius could be used to test some adversary models on any given energy systems. The system analysts can design the adversary model with having some goals in mind

and perform simulation analysis of the system to see the likelihoods of security breaches in the system. It was claimed that the newer version of the tool is able to ease the process of system integrating and systems design in Mobius by enabling the tool to simplify the complicated tasks and still able to achieve similar results. Although it could be argued that given how powerful Mobius is, its focus is more on to advisory and informing the security analysts and it is not intended for everyone's use. Another interesting discussion of this session was (a talk given by Sara) about the security of the energy systems but from the user's prospective. She has highlighted some interesting points about the role of people in the smart energy systems and the lack of research into the human behaviour in the field. The argument was mainly based on the human perceptions and how they might use the technology for their own gains rather that the intended design principles. People are going to use technology the way they prefer and therefore they should be included in the way we analyse smart energy systems and incorporate the human behaviour into the design and analysis.