THE UNIVERSITY OF MEMPHIS | Center for Information Assurance

SMART GRID SECURITY WORKSHOP

Summary Report

March 25, 2022

The Center for Information Assurance (CfIA) successfully hosted the Smart Grid Security workshop on Friday March 25, 2022 on the University of Memphis campus. The hours of the workshop were from 12:00 pm until 5:00 pm. The purpose of the workshop was to cover various cybersecurity issues and their solutions to smart grid and power delivery systems.

A wide variety of topics related to Smart Grid security were represented, including but not limited to: Smart Grid security, Micro-grids, Renewable Energy sources, various cyber-attacks (Device attacks, Data attacks, Privacy attacks, Network Availability attacks, Communication networks, Demand Response, Smart Communication delays and its' mitigation technique, Power Quality, Reliability, Phasor Measurement Unit (PMU), Remote Terminal Unit (RTU) anomaly detection, and security and privacy policies). The workshop organizers offered both in-person and/or virtual attendance options.

The intended audience was IT Professionals, State employees, college students, and all persons interested in Smart Grid Cybersecurity and how to strengthen cyber resiliency. There was participation from various local, state, and federal including transitioning workforce. The participants were engaged for five (5) hours on Smart Grid Cybersecurity topics/ presentations with some real-world case studies, market-ready cyber security knowledge, and skills for career advancements. At the end of each speaker's presentation, there was time set aside for a question-and-answer segment.

The workshop was funded by the Department of Defense (DoD) under the NCAE-C-001-2021 Project Cybersecurity Education for Smart Grid Cybersecurity. All participants who fully participated at the workshop received a completion certificate.

Smart Grid Security Workshop Agenda

Date: March 25, 2022 Time: 12:00 pm to 5:00 pm.

Time:	Event:
12:00 – 12:10 pm	Welcome Remarks – Dr. Dipankar Dasgupta
12:10 – 12:15 pm	Participants Introduction
12:15 – 1:15 pm	Discussion on Smart Grid Cybersecurity – Dr. Hasan Ali
1:15 – 1:30 pm	Break
1:30 – 2:15 pm	Speaker – Dr. Stacy Prowell, Oak Ridge National Laboratory – Title of presentation: *Cautious Optimism.*
2:15 – 2:45 pm	Speaker – Mr. Chip Harris, Cybersecurity Administration at DMI.INC – Title of presentation: *Cybersecurity for Smart Grid Technology for I.T. and O.T.*
2:45 – 3:30 pm	Speaker – Dr. Sandip Roy, Program Director – Computer & Network Systems, NSF – Title of presentation: *Implications-Focused Cybersecurity Research for Power and Transportation Systems.*
3:30 – 3:45 pm	Break
3:45 – 4:15 pm	Presentation by Mr. Nathan Farrar, Undergraduate student, Electrical & Computer Engineering: “Impact Assessment of Cyber-Attacks on Inverter-based Micro-grids”
4:15 – 4:30 pm	Break
4:30 – 4:50 pm	Question and Answer / Discussion Session
4:50 – 5:00 pm	Workshop Closing Remarks – Dr. Dasgupta

An underlying objective for the workshop was “Advance your Career in the Cybersecurity related profession and opportunities at the University of Memphis”. There was a Pre-Survey and a Post-Survey given to all participants. (See Appendix A for a tabulation of responses).

Extracts from the Presentations:

The workshop’s welcoming remarks were given by CfIA Director, Dr. Dipankar Dasgupta. The participants were introduced. Afterwards, Dr. Hasan Ali, workshop organizer, presented on the topic: *“Cyber-Security Issues and Solutions to Distributed Energy Resources”*.

Synopsis: Dr. Ali began his presentation by giving a short description of a conventional power grid, and the issues associated with the grid in its current form. This was followed with the motivation of why smart grids are an important step for the power grid, and what can be accomplished with the adoption of smart grids. Dr. Ali then gave a discussion on distributed energy resources, followed by a visual depiction of how cyber-attacks occur on smart grids and distributed energy resources. Dr. Ali then discussed several different types of attacks that occur on smart grids and hybrid power grids, as well as the implications of the attacks. This was followed by a short discussion of the cyber security issues with Wide Area Measurement Systems (WAMS), including the Phasor Measurement Unit. He then discussed the importance of Photovoltaic (PV) energy in smart grids, as well as the necessity of including a battery storage device in solar networks. He discussed the specific cyber risks related to PV power generation and storage, followed by a control algorithm to detect, and mitigate cyber-attacks on PV systems. Dr. Ali concluded his presentation talk with reiterating that all businesses with an online presence are susceptible to cyber-attacks and that a proactive approach must be taken when managing cyber risk in smart and hybrid power grids.

After a short break, the next speaker was Dr. Stacy Prowell. His topic was: *“Cautious Optimism”*.

Synopsis: Dr. Prowell began his presentation with a recall to the winter storm in Texas that occurred in February 2021. The winter storm knocked out power to millions of customers and caused several hundred deaths in

the area. Thereafter, Dr. Prowell gave a short overview of the petroleum product supply in the gulf coast and east coast regions of the USA. This was followed by an explanation of ransomware, in which he explained how the ransoming is the last part of the cyber kill chain. He then presented an in-depth analysis of what types of firms are targeted by cyberattacks, how vulnerable firms are to cyberattacks, and how the invention of the internet and eventually IoT devices are responsible for the current state of cyber-crimes. He then discussed just how difficult and complex security is in the cyber realm. This was followed with a discussion on the incorrect assumptions coders and consumers make when relating to software and hardware development and utilization. He then finished his discussion by explaining why he is now cautiously optimistic that software and hardware suppliers, as well as consumers are beginning to take cyber security more seriously. Hence, the adoption of modern artificial intelligence algorithms may greatly reduce the risk and aid in prevention and mitigation of cyber-attacks.

The next speaker was Mr. Chip Harris. His presentation topic was: *"Cyber Security for Smart Grid Technology for I.T. and O.T"*.

Synopsis: Mr. Harris began his presentation by showing how much money is spent globally on cyber security from the year 2017 to the year 2026. Mr. Harris then touched on several different cybersecurity tools that when they are implemented effectively, can reduce the occurrence and the effect of cyberattacks. This was followed by a brief explanation of what a smart grid is with respect to IoT devices, and what types of cyber-attacks smart grid networks are facing. Mr. Harris then presented the challenges of a security control framework for identifying, protecting, detecting, responding, and recovering from a cyberattack on a network. This was then followed by a visual representation of the vulnerabilities of smart grids. Mr. Harris concluded his presentation by reiterating the importance of developing and maintaining a strong physical architecture for smart grids and the importance of cyber awareness.

The next speaker for the workshop was Dr. Sandip Roy.
Title of presentation: *"Implications – Focused Cybersecurity Research for Power and Transportation Systems"*.

Synopsis: Dr. Roy began his presentation by giving a brief explanation of his previous and current work experiences in infrastructure autonomy. This was followed by a discussion of why cyber security has become such a big concern in recent years, as well as the challenges to developing a secure system. Dr. Roy then segued into the primary focus of his presentation: the implications, and outcomes of cyberattacks. He used a bulk power system to explain how using physics, one can detect anomalous behavior of the system. A holistic risk approach was then used to detect the cyber risks of air traffic control and management. This was followed by a simulation of different attacks on an air traffic control and management system, as well as the emergency response system tasked with detecting cyberattacks. Dr. Roy concluded his presentation with a display of several axis that represent the challenges for cyber security, which include scale, time, goal, automation, and lifecycle.

After a short coffee break, the final speaker for the workshop was University of Memphis student Nathan Farrar. He presented on *"The Impact Assessment of Cyber-attacks on Inverter-Based Microgrids"*.

Synopsis: Mr. Farrar began his presentation by defining what a microgrid is, and how smart inverters are an integral part of the system. He then went into details of how detrimental a cyber attack could be on microgrid control systems if they should become compromised. Several different detection, prevention, and mitigation strategies were discussed including artificial intelligence, high-speed communication for wireless systems, and limiting "zero day" occurrences. Mr. Farrar concluded with how important it is for every person in the link, from suppliers to consumers, to understand just how important cyber security is, and to take every precaution when dealing with sensitive material.

Workshop Presenter's Biographies:

Dr. Mohd Hasan Ali, University of Memphis: Dr. Ali is currently an Associate Professor with the Electrical and Computer Engineering department at the University of Memphis. He leads the Electric Power and Energy Systems (EPES) Laboratory. His research interests include smart-grid and micro-grid systems, renewable energy systems, energy storage systems, load forecasting in smart buildings, electric vehicles charging

stations, and cybersecurity issues in modern power grids. He serves as the Editor of the IEEE Transactions on Sustainable Energy, IEEE Transactions on Energy Conversion, IEEE Power Engineering Letters, Frontiers in Energy Research, and the IET-Generation, Transmission and Distribution (GTD) Journals. Dr. Ali is a Senior Member of the IEEE Power and Energy Society (PES). He also serves as the Chair of the PES of the IEEE – Memphis Chapter.

Dr. Stacy Prowell, Oak Ridge National Laboratory: Dr. Prowell is a Distinguished Researcher with the Oak Ridge National Laboratory. He is the Chief Cybersecurity Research Scientist in the National Security Sciences Directorate at Oak Ridge National Laboratory. His research focuses on methods to secure the nation's critical infrastructure. He has developed technologies for automated reverse engineering of compiled software to detect vulnerabilities, to detect fileless malware remotely, and to detect attacks and compromises using timing and power side channel information.

Mr. Luther "Chip" Harris, Cybersecurity Administration at DMI.INC: Mr. Harris is the Ethical Hacker, Red Team Leader, Penetration Tester, and a Senior Cyber Security Administrator at DMI.INC. He currently works on network platform-based security technique experience and development of an enterprise IT (Malware Prevention) modernization plan.

Dr. Sandip Roy, Program Director, Computer and Network Systems, National Science Foundation (NSF): Dr. Roy is a Professor in the School of Electrical Engineering and Computer Science at Washington State University. His research is focused on developing secure and resilient autonomy for Cyber-enabled infrastructures. The research has led to tools and software that have been prototyped and deployed in several settings (e.g.: the Western U.S. Power Grid, and the U.S. Air Transportation System's Central Command Center). He is currently on appointment at the National Science Foundation, supporting the Cyber-Physical Systems and

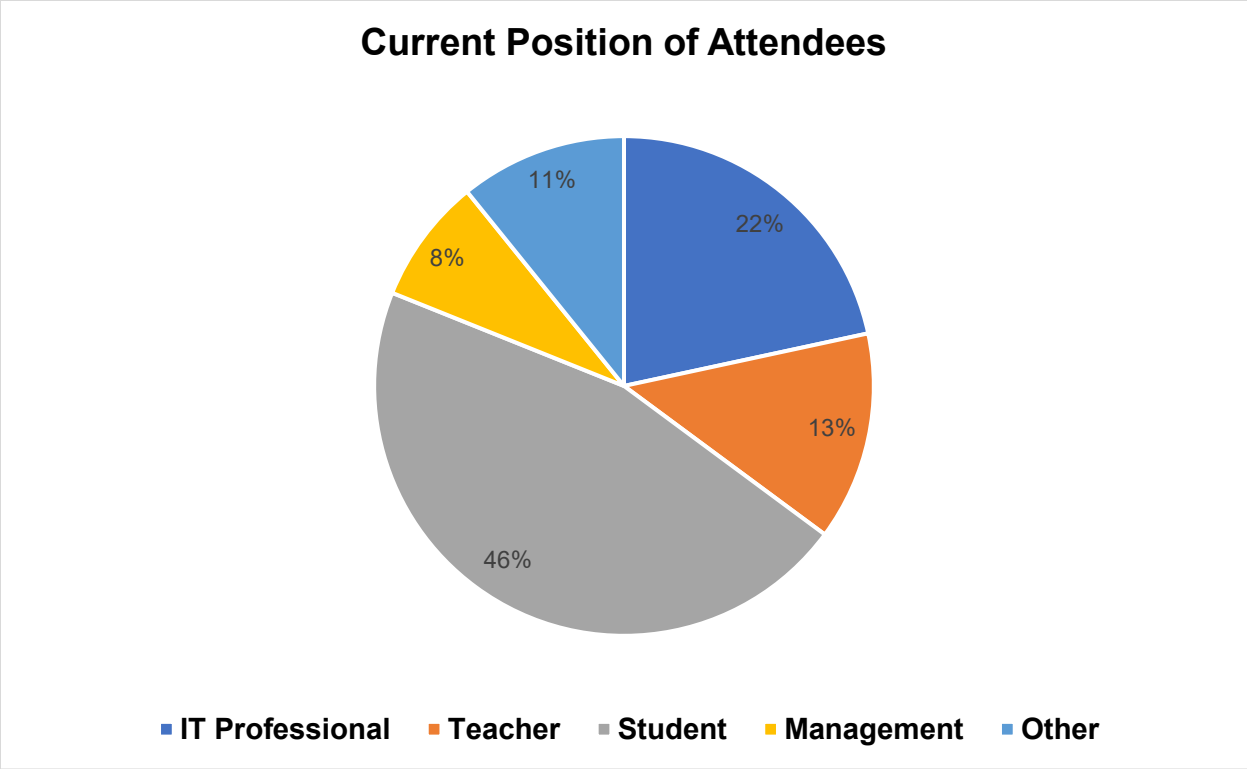
Smart & Connected Communities programs. He also holds a joint appointment at Pacific Northwest National Laboratories.

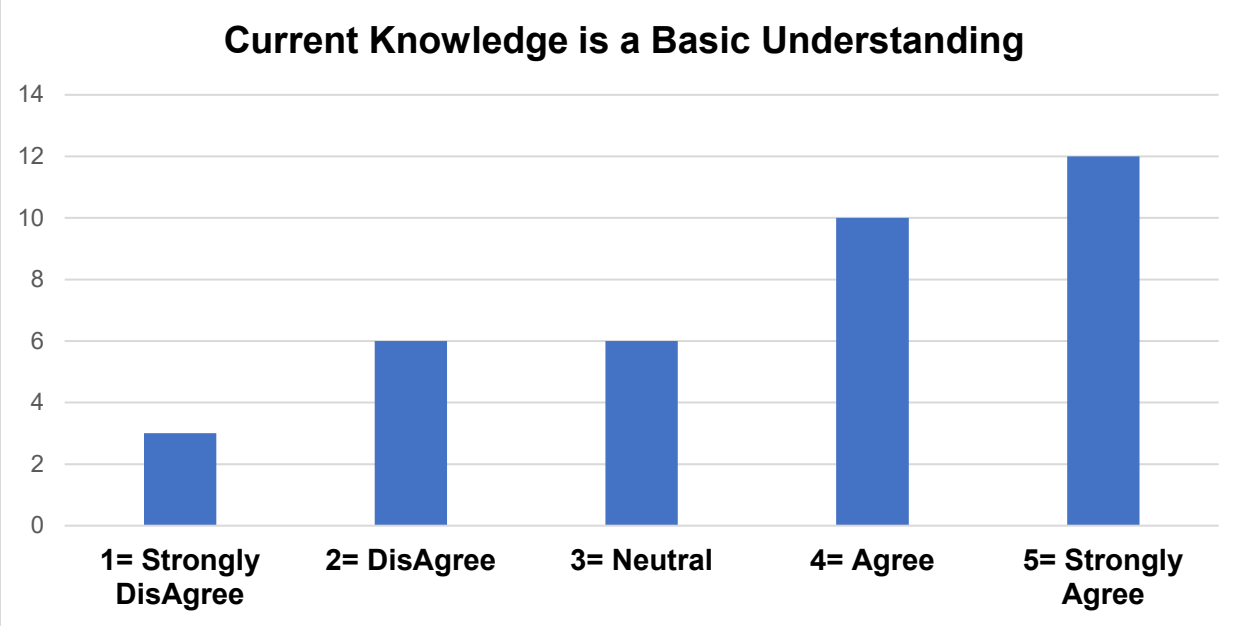
Mr. Nathan Farrar, University of Memphis: Mr. Farrar is an undergraduate student in the Electrical and Computer Engineering department. He will graduate in May 2022 and will start his Master's degree studies during the Fall 2022. His research interests include cybersecurity issues in modern power grid systems, smart grid, microgrid, and renewable energy systems.

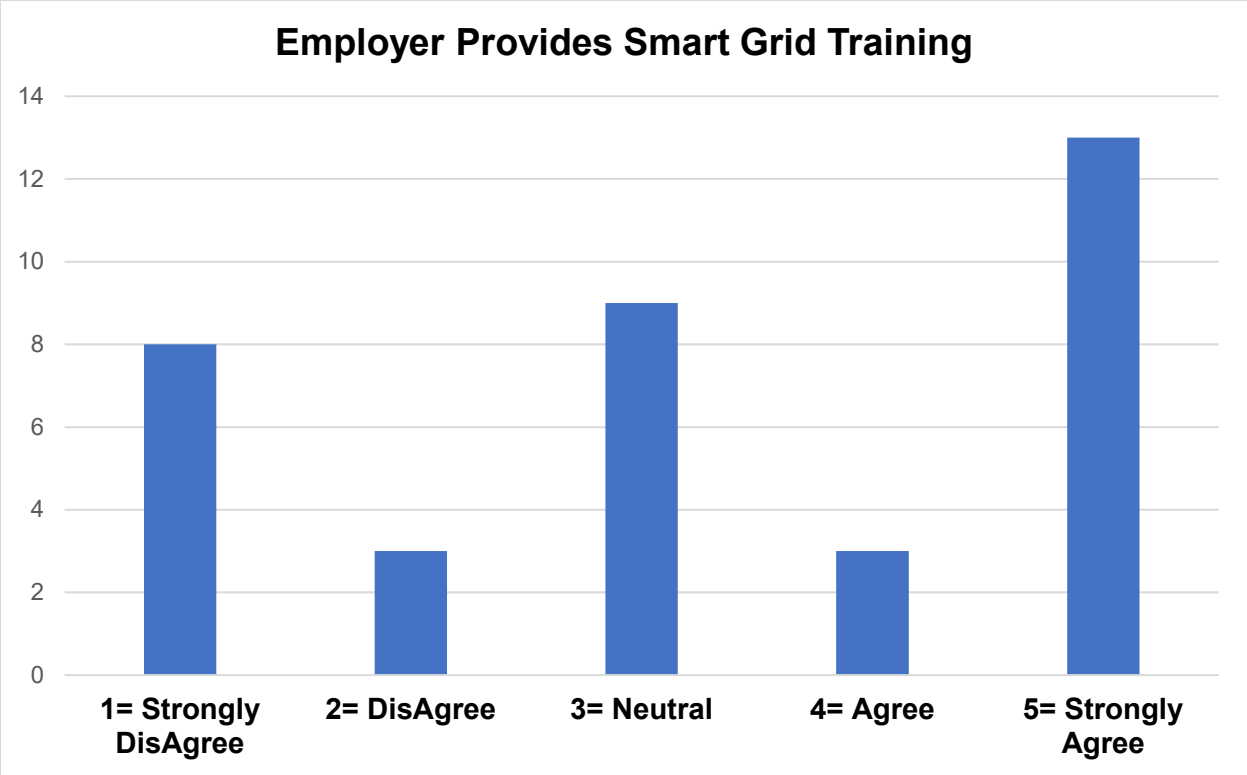
Appendix A: Smart Grid Security Workshop: Participant Data, Workshop Photo, and Feedback Response Charts.

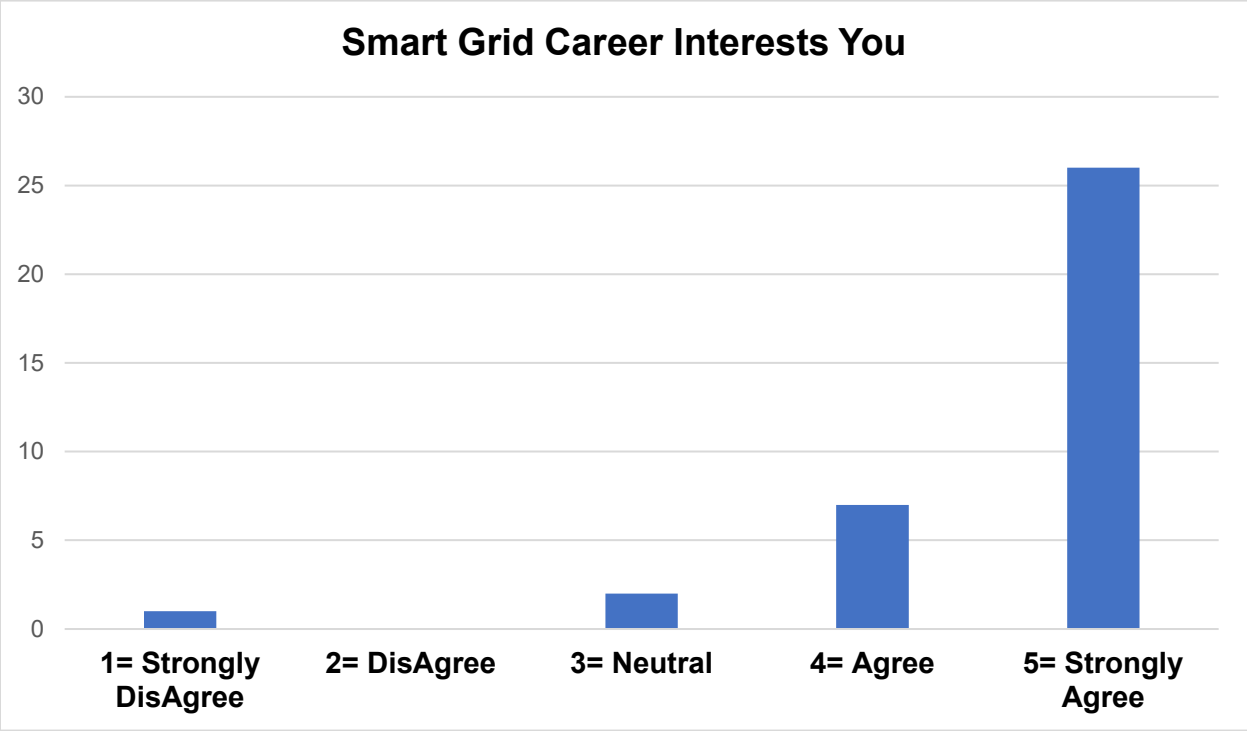
In summary, there were a total of 37 survey respondents (e.g., face to face and virtual).

A total of 84 people registered online for the Smart Grid Security workshop. There was a total of 18 face-to-face and 19 virtual attendees for this event. There were 3 walk-up participants. The following chart provides different categories of the professionals that participated.

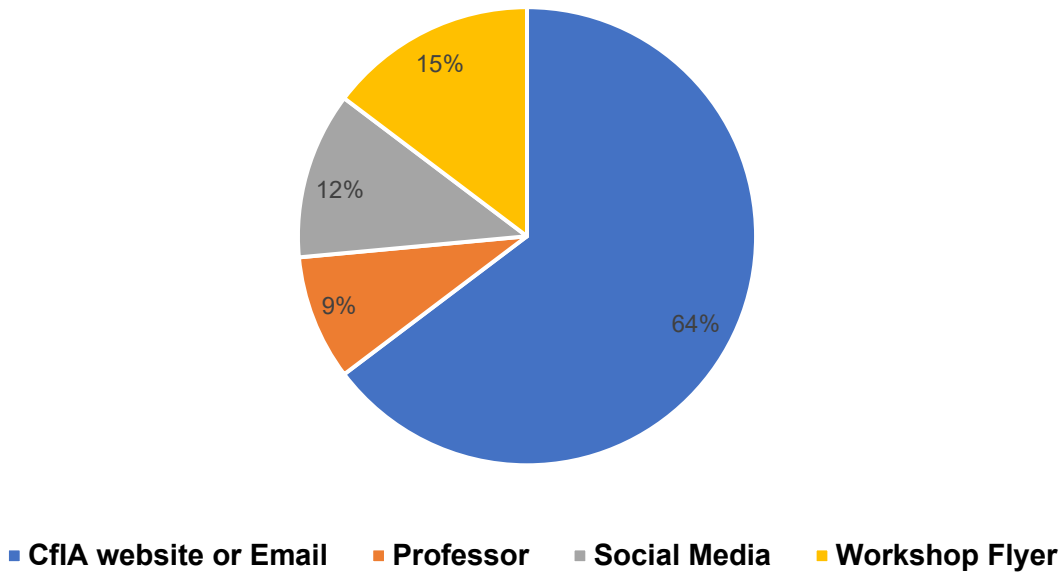

Current Position of Attendees
22%
13%
46%
8%
11%
IT Professional
Teacher
Student
Management
Other


Current Knowledge is a Basic Understanding
14
12
10
8
6
4
2
0
1= Strongly DisAgree
2= DisAgree
3= Neutral
4= Agree
5= Strongly Agree


Employer Provides Smart Grid Training
14
12
10
8
6
4
2
0
1= Strongly DisAgree
2= DisAgree
3= Neutral
4= Agree
5= Strongly Agree


Smart Grid Career Interests You
30
25
20
15
10
5
0
1= Strongly DisAgree
2= DisAgree
3= Neutral
4= Agree
5= Strongly Agree

How Did You Hear about this Workshop



Your Expectations of this Workshop