A Gap Analysis of Cyber Security Training in the Smart Grid

Tim Yardley

A Capstone Presented to the Information Technology College Faculty
of Western Governors University
in Partial Fulfillment of the Requirements for the Degree
Master of Science in Information Security and Assurance

May 22, 2014

Special Thanks To

My Wife and Daughter for all their support,

The Department of Energy and DHS funded

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG),

and

The Information Trust Institute (ITI) at the University of Illinois Urbana-Champaign (UIUC)

Abstract

In this work, an analysis was conducted of the existing pedagogy and various bodies of knowledge that are utilized in cyber security training for critical infrastructure such as the electric power grid (smart grid). The project was implemented as a three phased approach. Phase 1 involved collecting the existing pedagogy, body of knowledge for training, and job requirements and competencies in this area. Phase 2 consisted of a gap analysis comparing the requirements of the industry compared to the existing training. Phase 3 focused on the detailed writeup of the gap analysis work.

The gap analysis discerned what exists both in approach and content in relation to workforce needs comparing coverage of topical areas and competencies in relation to job needs. It is intended that this gap analysis will be utilized in the future to determine areas of improvement and to develop an open training curriculum and platform that facilitates the rapid education of a wide variety of participants on important background and job focused aspects of smart grid cyber security. This future developed curriculum will consist of both presentations and hands-on training tools that will aid in the education of interested parties in research, industry, and government.

It was anticipated that the existing pedagogy and various bodies of knowledge have deficiencies that exist in comparison to the needs or ideal solutions for the target audience entering the workforce or changing career focus as the needs evolve. This hypothesis proved to be true, that there were existing gaps in the training material and areas of improvement. The details of this report cover that analysis and its conclusions.

Table of Contents

Introduction

With the mass modernization and investment efforts to secure the electric power grid, there remains a plethora of privacy and security related issues that both need to be understood and resolved by the emerging and adapting workforce. In terms of embracing these modernizations and developing workable solutions, cyber security training becomes both the instrumental tool and the key factor in the success of that effort. However, there is an observable deficit and training gap that exists in the workforce development training for cyber security. This project conducts a gap-analysis of the existing cyber security training pedagogy and bodies of knowledge that attempts to prepare the workforce for these changes.

Project Scope

This project conducted a gap analysis on the existing base of training material that exists for education of the new workforce intended to operate the modernized electric power grid. This included analysis of the pedagogy, bodies of knowledge, and syllabus' of a variety of existing training courses. These courses ranged from independent instructors to formal certification bodies that are targeting the smart grid cyber security training problem. In this project, the analysis focused on cyber security, but also considered the required prerequisite power system and computer knowledge that one must possess to effectively work on cyber security in the sector.

The goals of this project were to survey the existing work in this space and conduct the above mentioned gap analysis that aims to identify unaddressed needs to provide a more thorough and comprehensive body of knowledge for training in this space. This was intended to

reflect the needs of the electric power sector for cyber security training at various levels in the organization.

Defense of the Solution

The gap analysis approach is being undertaken as a means to identify what is and is not currently being addressed. This analysis will help reveal both the popularity and potential prioritization of topic areas for cyber security curriculum in this domain. By interfacing with the entities that have the positions to fill, this analysis will be compared against their needs and in the future lead to the creation of a comprehensive set of material that covers the existing topics and addresses the gaps that currently exist.

Further, the approach utilized in this project provides a multitude of benefits. First and foremost, the available training landscape is broad with varying topic coverage. To understand the coverage of each of those training opportunities and to determine which opportunities are needed to most effectively cover the desired training gaps is a cumbersome process for any utility to undertake. This project aimed to simplify that analysis by providing a coverage analysis of each of the opportunities and identifying what their strengths and weaknesses are in relation to being able to map to the needs of the sector.

The second important result from this work is the opportunity for derivative work. While a gap analysis is useful on its own, it does not provide the true benefit of a streamlined solution to the problem. This enables future work such as the intent to implement a modular and comprehensive training platform for this sector. While the deliverables of this project do not include the actual future training material, it does lay out a path that allows for the creation of said material.

Methodology Justification

The electric power grid of the United States has undertaken a monumental modernization and expansion effort, bringing in new technologies and working towards securing existing deployed technology. With this modernization, comes the need for a workforce that both understands the new technology and that can effectively and efficiently use that technology to advance the state of art in the grid. However, this new modernization also requires leveraging existing training or necessitates the creation of new training material to effectively carry out that workforce development.

While there are several approaches to training that have been created, there is a lack of easily accessible, comprehensive, and modularly adaptable training in this area. This project identifies the gaps in existing training approaches in comparison to job requirements and perceived needs in terms of technical competencies. It provides the basis to leverage that analysis as input to architect a future training curriculum that closes these gaps. The future training material created based on this analysis is intended to be openly released to the world for others to build upon when completed.

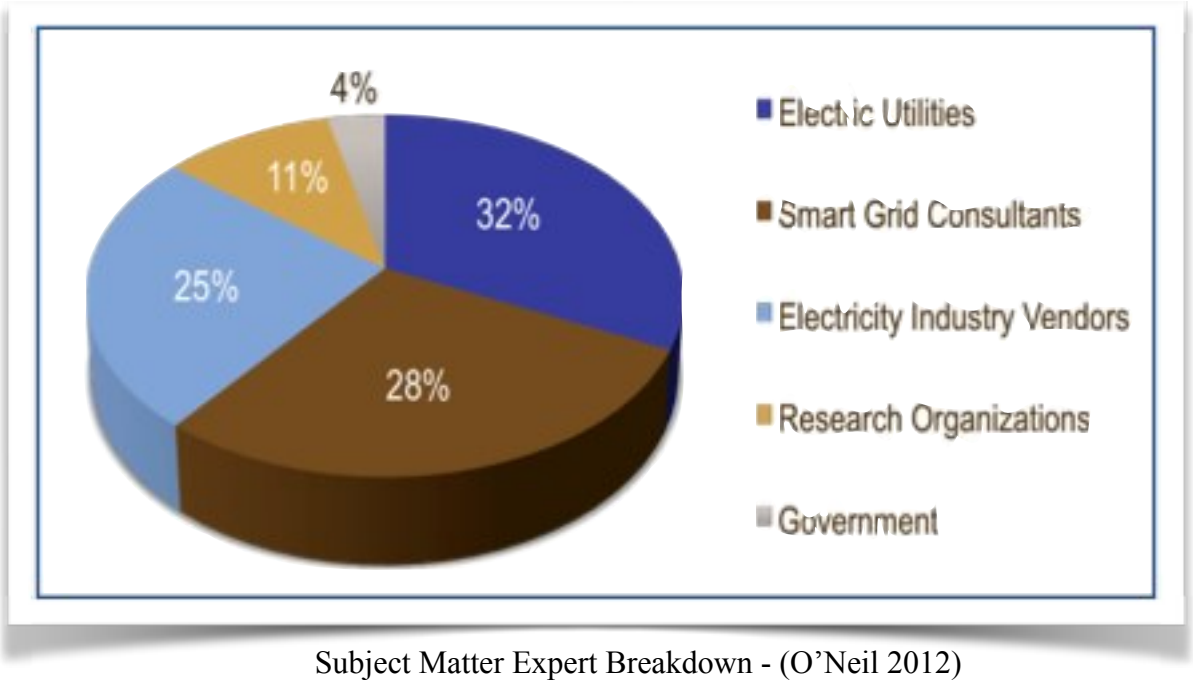
Organization of the Capstone Report

This report hypothesizes that there is a problem in that there is a lack of effective, accessible, and comprehensive training for the cyber security needs of the electric power grid. In the following discussion, causes, impacts, and various gap-based analyses will be conducted as a methodology by which to execute this project and determine if the hypothesis holds.

Assumptions and limitations of the project will be discussed along with the methodology before moving on to the analysis and results.

Systems and Process Audit

As a precursor to the project design and development, both a business process audit and a sector readiness ad-hoc analysis was conducted to determine the potential efficacy of the desired work product. It was determined through discussions with sector leaders, practitioners, and academics that the need for more accessible and comprehensive cyber security training for the electric sector is evident. This confirms the original hypothesis, and was further supported by external justifications and validations that this need does exist based on a subject matter expert survey (O'Neil 2012).



Subject Matter Expert Breakdown - (O'Neil 2012)

Audit Details

Having an effectively trained workforce is essential to nearly every aspect of any business. However, acquiring the necessary talent with the appropriate competency and sufficient

depth of knowledge in the area that the company needs can be overwhelmingly difficult. Many businesses will instead acquire talent that has a sufficient base and demonstrates potential, but is not necessarily sufficiently competent to carry out all specific job duties at hand. When businesses choose to do this, they often then put the new employee through a serious of training courses that help ramp up or hone the skills that are necessary to the business needs. Therefore, it is essential to have both this type of training available, and adequate coverage of the necessary areas of domain knowledge that map to the needs of the companies.

In the modernized electric power grid, along with many other sectors, these training opportunities are not necessarily offered at ideal times in the hiring cycle, or may not exist at all. This poses a fundamental problem to the hiring business in that they may only be able to effectively train new talent at particular periods of the year or through direct on the job training. On the job training has potentially drastic consequences in the case of failure due to the nature of critical infrastructure and it's overall importance to the operation of the nation.

Based on the report from O'Neil (2012), a panel of 28 subject matter experts were assembled to elicit job goals and tasks for cyber security roles. This produced over 500 tasks that were then assessed to determine criticality and competency requirements. These tasks were then classified based on the job roles (over 40) which were mapped to the functional roles identified in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. The tasks and roles where then combined with "vignettes" (over 109) which was defined as a terse statement that identified an incident or event that provides the context for a cyber security task. Those vignettes were then aggregated and distilled to form 13 master

vignettes. Those 13 master vignettes were then compared against a sub-selected set of three cyber security roles (Security Operations, Intrusion Analysis, and Incident Response).

The key takeaway from the O'Neil report was the development of a Critical-Differentiation Matrix (CDM) which is a matrix that aims to identify the the fundamental and differentiating tasks that should help predict job performance in a cyber security role. This identified 83 fundamental tasks across the 3 roles, with twenty tasks identified as indicators of competency for the six levels of expertise that were utilized. This CDM is referenced as a correlation aid for the training and job needs analysis and is a background consideration during each phase of the mapping.

Problem Statement

This project aims to verify and validate the cyber security training needs and coverage for the electric power sector. It is widely known (O'Neil 2012) that there exists no openly available, easily accessible, and comprehensive cyber security training that prepares someone with the requisite knowledge to effectively operate in a cyber security role in the modernized electric power grid. In order to effectively create such an open curriculum, one must understand the existing state of training and identify the necessary gaps to address for a comprehensive and modular solution. This project addresses that understanding and analysis and therefore attempts to solve the problem by identifying the coverage and corresponding inadequacies of the existing training when compared to the business needs.

The research methodology requires gathering information from the relevant existing training material and categorizing each topic area into a generalization of the material at hand. This is cross-indexed with various national initiatives that aim to indicate job priorities, areas of

responsibility, and areas of competency. In addition, training requirements were summarized from both job descriptions and discussions with those responsible for hiring cyber security experts in this sector. This information provides the basis of the cross-comparison to determine a needs-based gap analysis. Since no existing comprehensive pedagogy exists for this sector, this analysis could serve as the basis for the creation of a best practice based pedagogy and body of knowledge. This information further provides the basis by which to analyze the material and develop a fundamental understanding of both the existing covered body of knowledge and the gaps that are formed between what is available and what is perceived to be needed by the sector.

Problem Causes

Specialized training is traditionally a big-money business, focused on bringing a particular audience up to speed with the intended knowledge in a short period of time with both limited availability and hard-to-find expertise. This approach, while sometimes quite effective, does not put the training material into the hands of the broad general public instead limiting it to those that can afford to pay for the often costly training and attend in the particular timeframe of availability. Further, it necessitates the direct involvement of subject matter experts to actively teach the topic areas. In many cases, this material is just a derivation of prior material from another sector that is adapted slightly for the new domain. While adaptation can be effective, it is not an optimal solution for something as specific and critical as the electric power grid.

The existing training is well composed and built with particular needs in mind. Each of the organizations has done a great job of filling a particular niche, and moving the ball forward. However, there is still room for improvement and knowledge areas that could be covered in a way that results in more effective training.

In the future, this project will feed into work to change the training landscape by making self-standing and self-paced training that is widely available and easily modifiable. Further, it will focus on a modular approach that encourages use and extension to suit each target audience.

Business Impacts

Without effectively trained personnel in the necessary cyber security topics, the electric power grid of the United States could be left vulnerable to attack. Since the act of electrification has been so pivotal to the advances of society over the years, the impact of that capability going away would be catastrophic. Therefore, due to such great importance, the electric power grid is both a high-value target and a critical asset to adequately protect for the best interests of the nation. However, even with some of the most advanced cyber security protections in place, humans are still part of the loop and must both understand and effectively operate the cyber security mechanisms going forward. Failure to do either of those could result in either attrition of the protection mechanisms or complete failure in the ability to detect, defend, and respond to attacks on that critical infrastructure.

If businesses do not have training that is adequate for hiring and training the necessary workforce to address the cyber security of the modernized electric power grid, the consequences could be catastrophic. The electric power grid may fail, be vulnerable to attacks, or be insufficiently monitored resulting in attacks or intrusions going unnoticed with potential irreparable harm. As seen in various news sources, it is understood that other nations are likely interested in causing harm to the United States by attacking it’s critical infrastructure, making it even more vital to protect.

Without effective and efficient cyber security training in the relevant areas, the existing and emerging workforce will be inadequately prepared to detect and defend attacks against this critical infrastructure. While it is nearly impossible to actually quantify the potential incurred losses, those losses could come in the form of financial impact, business reputation, or even widespread loss of life through the failure to protect the critical infrastructure.

Since cyber security professionals are in short supply across many sectors, this analysis, and future body of knowledge and modular approach to training could be essential to widespread multi-sector addressing of this deficiency. Without such an approach, the many sectors that are relying on having adequately trained cyber security professionals may suffer.

Having accessible, effective, and well-positioned training also allows businesses to scale up their employees at will. If this material is tuned specifically to the types of needs that this domain, and its specific businesses have, the effectiveness of both existing and newly acquired staff is increased. This is further supported by the modularity of the intended future body of knowledge and coursework, as it would enable piecewise assimilation of the necessary material for rapid and effective competency improvement.

Further, by having the future material open, widely available, and designed in this modular way, businesses will have the ability to have more effectively trained staff that are better suited in carrying out their duties. In order to realize such material, this project's gap analysis is a foundational step towards the creation of said coursework and material.

By having adequately and effectively trained workforce, the companies and the nation as a whole are in better positions to detect and defend our critical infrastructure. This could result in both operational and capital expenditure savings by saving downtime, loss of critical function,

and minimizing operational or customer impact of a potential intrusion. While proper training goes a long way to being organizationally prepared, it does not prevent these types of attacks. It is assumed that the training could also allow the companies to leverage more complex security solutions that position the company in a more secure manner, potentially mitigating many attempted compromises and therefore thwarting attackers. The additional complexity (e.g., moving target defenses) could be possible with highly trained staff that possess the necessary competencies to effectively operate and interact with such security mechanisms.

Cost Analysis

Gathering the necessary information and applying the domain expertise to develop and expand the existing sector-based body of knowledge and core principles that are targeting the sector is a time consuming and human-capital intensive task. However, this is a critical step that companies need to utilize prior to training their workforce in this area. Without this analysis, companies may be training their employees inadequately or getting nominal value from the training expenditures they do undertake. Since training effectiveness is a very person-specific metric, it is difficult to analyze the efficacy of the training short of leveraging pre and post standardized testing or developing a job performance metric (JPM) such as that done by O'Neil (2012). However, standardized testing does not really exist for emerging topic areas like cyber security in critical infrastructure and therefore is not easily undertaken by the companies in this sector. Further, standardized testing encourages "teaching for the test" rather than necessarily acquiring true competence in a particular area, a constant struggle of standardized testing.

As part of this project, there are no capital or operational costs to a company or business. No hardware, software, staffing, or particular company expertise is needed to implement the

project solution. This is because the output of the project is a detailed analysis of the gaps in training compared to the needs of a company and is therefore informative rather than prescriptive. Future work will be to create open, modular training that fills those gaps, which does have costs involved if a company were to undertake its creation themselves. However, the intent is that the author and other interested parties will be creating that curriculum and releasing it openly and widely available to the world. As such, that implementation would also have no company incurred capital or operational costs inherent to its implementation.

The gap analysis that was done as the focus of this project is only one piece of the bigger puzzle and it doesn't provide the direct value itself. Instead, it is an enabler of value. To realize this value, the analysis must be leveraged and acted upon to create openly available curriculum that helps raise the bar of cyber security competency in this domain with the relevant areas of expertise for that competency. The creation of the curriculum is both a potentially arduous and time consuming task, however the author will be undertaking the actual creation of the material based on both past training efforts and in combination with a team of other interested parties following the completion of this analysis work.

To further state the importance of these tasks, the Department of Energy and Department of Homeland Security has commissioned several multi-million dollar efforts to explore the workforce development aspects of providing education and training in cyber security topics, specifically related to critical infrastructure such as the electric power grid. This includes initiatives spanning human resource hiring practices, education and training development, and analysis regarding certifications and accreditations that apply to this domain. These efforts have

been a bit silo'd in approach, and this project will augment them by providing a cross-cutting view of training versus needs, mapping to these initiatives.

Since the intent is to leverage this analysis to eventually create coursework in an open realm and then to release it widely, this output will help reduce the cost of training broadly and increase the availability of material that helps convey the appropriate body of knowledge and develop effective competency.

Risk Analysis

With any project, there are risks that may be encountered. One such risk is the failure to determine adequate source training material in this sector to feed into the analysis. If realized, this risk could result in setbacks to the project. However, a variety of training resources have already been uncovered to leverage in the analysis. These include standardized resources such as the GIAC GICSP (2103) program as well as academic courses and specialized training courses from various entities. Further, the author has strong connections to the sector that can be leveraged to garner further information surrounding needs.

Another risk is the availability of the requirements for jobs in this sector, however the O'Neil (2012) study and NICE framework include job listings across various operating domains of this sector and have distilled requirements and categories that can be leveraged. It is also possible that the hiring managers in this domain may not be forthcoming with the information about their needs or deficiencies in hiring cyber security professionals. This risk is also mitigated, as O'Neil (2012) has already undertaken a survey of this area and aggregated some relevant information that can be leveraged for this effort.

Another risk is that the job descriptions and perceived needs may not be comprehensive or that the interpretation of the coverage may be difficult, and therefore will require expansion leveraging the domain expertise of the author. Combining the collected information with the authors domain expertise will help further identify areas of education that are necessary to create a comprehensive body of knowledge that can then fill those gaps. This risk is therefore actually an opportunity for better results.

The final risk is that it is possible that the gap analysis of existing training will not uncover any significant gaps. While this is unlikely based on common knowledge and related work, there is still tremendous value in assessing the body of knowledges across various available training courses to derive a complete approach to training for this sector. Further, the future work of organizing that aggregated body of knowledge into a modular based approach provides intrinsic value for both operational efficiency and effective training. This is realized through being able to select only the areas where training is needed, and leveraging the self-standing and self-paced approach of the future modular training to educate the new workforce in less time and with more impact.

Detailed and Functional Requirements

There are several fundamental requirements that were necessary to execute this project. The first is familiarity with the ongoing efforts surrounding cyber security training and how they map to this sector. Since there is no single definitive resource for this information, it requires leveraging the author's subject mater expertise to appropriately survey the available work. After the known efforts are enumerated, a thorough understanding of what each effort undertook, and how that maps to the work at hand needed to be conducted. This understanding of data is not

tangible, but was required to appropriately address the gap analysis. From there, it was just a matter of executing the rest of the project plan.

Functional (end-user) Requirements

There are no direct end-users of the output of this project, as it is intended as a gap analysis that funnels into continued work of addressing the gaps. This work could be leveraged by training providers, certification bodies, or even hiring entities such as utilities to assess which training opportunities they intend to partake in for a given resource. Therefore, the gap analysis is useful to an end-user as a means to evaluate an existing training project or need against the identified global cyber security needs for a given sector.

In order for this to be effective, the output of this project needed to have an easy to discern compilation of topic area coverage, mapping to presumed responsibilities of jobs in the sector, workforce needs, and security role competencies. The tables that support the analysis is provided as appendices to this report.

Detailed Requirements

There are no technical, operational, or existing standards that have to be met specifically for this gap analysis. However, the gap analysis is designed to compliment the NICE (2011) framework and the (O'Neil 2012) certification report. If one were developing a certification program itself, it would likely need to be compliant with ISO/IEC 17024.

Existing Gaps

This project addresses gaps in several areas. First, there exists no known current analysis that surveys the currently available cybersecurity training and educational courses for this sector and analyzes the coverage of that training as it relates to defined job requirements. Second, the

training that does exist can be difficult to attend due to several factors, not limited to cost, training location and date availability, instructor availability, on-site versus off-site dissemination issues, and the opportunity for custom tuning/tailoring of the material to suite the target audience. It should be noted that each organization has varied priorities on any of those deficiencies, and while any one deficiency may not affect a particular company, the combination of these deficiencies does affect all companies that have been consulted.

Project Design

Scope

This project conducted a gap analysis on the existing identified base of training material that exists for education of the new workforce intended to operate on the modernized electric power grid. This included analysis of the pedagogy, bodies of knowledge, and syllabus' of a variety of existing training courses. These courses ranged from independent instructors to formal certification bodies that are targeting the smart grid cyber security training problem. There are definitely other courses that exist and that were not analyzed for various reasons ranging from lack of available material to adequately assess the course, or due to constraints on disclosure. Further, there are likely courses that are newly emerging and not well known to the general public yet. Any of those opportunities could be added to the tables to support the further analysis at a later date.

In this project, the analysis focused on cyber security, but also considered the required prerequisite control system and computer knowledge that one must possess to effectively work on cyber security in the sector. There are areas that are not addressed, such as the interplay of the

cyber-physical systems that are likely out of job scope requirements, but must be understood for deeper fundamentals and research.

The goals of this project were to survey the existing work in this space and conduct the above mentioned gap analysis that will identify unaddressed needs to provide a more thorough and comprehensive body of knowledge for training in this space. This was intended to reflect the needs of the electric power sector for cyber security training at various levels in the organization, with a focus on the working bodies rather than high-level management.

Assumptions

With billions of dollars having been invested into the modernization of the electric power grid, and the growing threat of attack and compromise of these systems, it is assumed to be essential that an effective and well trained workforce exist. It should be noted that the lack of effectively trained cyber security personnel is not limited to the electric sector. Various governmental agencies (e.g., DHS, DOE, and the White House) have indicated that there is a stark shortage of the personnel necessary for cyber defense and cyber operations across many government and private sectors.

It is justifiably assumed that this workforce does not yet exist and that there are gaps in the emerging curricula that facilities the training of this emerging workforce. There is a base assumption that their is a need for cyber security training for critical infrastructure, however this assumption is supported in the O'Neil (2012) report. It is also assumed that the existing material has limitations and therefore is insufficient in some way. This is also validated by the O'Neil (2012) report. These limitations could take many forms, such as inadequate coverage, requirement of being instructor led, format by which the course is given, venue or location, time

dedication, cost, or time involved in amassing the necessary knowledge by the attendees or even for qualified instructors. If the assumption that at least some of these limitations do not hold, then there could be less value to be provided by this project except to provide a basis through the analysis that then leads to the creation of an open, diverse, and modular training curricula.

Project Phases

The project was broken into multiple phases. In the first phase, existing material for cyber security education and training in this segment was identified. After this material was identified, it was cross-compared to determine areas of overlap and intersection between each subsequent available training options. Each generalized topic covered was analyzed in the context of necessary domain knowledge and then mapped to the identified competencies and requirements for the workforce in this sector. After the initial aggregated body of knowledge was created, gaps in the training coverage of that body of knowledge were identified. This involved discussions with industry experts, training instructors, academics, and sector consultants that helped understand the needs and the coverage of various pieces of training aiming to provide the maximum effectiveness, efficiency, and impact in the analysis.

Once a refined body of knowledge was created, the underlying concepts that are necessary to adequately understand each topic were identified and documented. An analysis was done and prior work leveraged to determine the necessary background topics that are prerequisite to any particular topic area, also known as foundational knowledge.

Future work will involve creating the necessary training material and hands-on training aids to assist in demonstrating competency in each topic area, the application of that area to the domain, and the behavior of that concept in relation to the larger picture of the system under

study in that domain. This material and training platform will not be created as part of this project, but this will lay the essential groundwork to allow for its future creation. It is intended that once this training material is created, it will serve as a foundation that can be leveraged for training a wide variety of entities, ranging from academia, industry, and government at various different levels of knowledge and understanding.

Timelines

The entire project was conducted in phases, however the timeline was compressed. Phase 1, information gathering, was intended to be done over the course of a month to acquire the necessary base material. Phase 2, analysis, was intended to be conducted over a period of two months to effectively analyze the acquired material and provide the base of the gap analysis. Phase 3, documentation and reporting, was intended to be done over the course of two months to effectively communicate the analysis and the expected outputs of the project.

Dependencies

The dependencies are ordered by phases. This means that each subsequent phase cannot be started until the prior one has fully, or at least partially, been completed. This linear progression is required to adequately cover the material at hand. Note, that the second phase of the project can be circular in nature, returning to the same material and revising as the analysis continued. The third phase could also require revisiting phase 2 as the documentation of the analysis may uncover additional insight or discrepancies.

Resource Requirements

No hardware, software, staffing, or particular company expertise is needed to implement the project solution. This is because the output of the project is a detailed analysis of the gaps in

training compared to the needs of a company. Future work will be to create open, modular training that fills those gaps, which does have costs involved if a company were to undertake it. However, the intent is that the author and other interested parties will be creating that curriculum and releasing it openly and freely available to the world. As such, that implementation also has no company incurred capital or operational costs inherent to its implementation.

Risk Factors

Since the project was set up in a phased approach and an appropriate preliminary audit and analysis was done before undertaking the project, there are no known risk factors that affect the project outcome. Adequate material was pre-identified, industry contacts established, and scoping put in place to ensure successful execution of the project.

If any of the core assumptions on time, material, or resource availability were to prove to be inaccurate, then the project could have taken longer than expected. However, since the core assumption violation is rooted in the author's availability, these potential risks are easily mitigated.

Important Milestones

There are three key milestones associated with the project. Successful acquisition of the source material should be completed by the end of the first month. Complete, or near complete, analysis of the material should be completed by the third month. The written documentation, analysis, and output for the project should be completed by the fifth month. At the half-way point for each of the phases, there should be measurable progress towards the end goal of each of those phases that is roughly represented by the appropriate marker in the timeline. For example, at 2 weeks in to phase 1, several sources should have been acquired with more pending.

Deliverables

In this project, the intended outcome is to shed light on various questions in this topic area, such as: 1) What are the perceived skills that are necessary for a cyber security position in this sector?; 2) What material exists to train towards those competency areas?; 3) What gaps exist in either the preparation for the existing material, or in the body of knowledge that is targeting these positions? For example, are there inherent assumptions that the current material makes that are flawed? If not, does the existing material provide the appropriate background information and cast the right context to apply the knowledge to this sector?; 4) What would a more comprehensive pedagogy that is tailored to effectively train the needed cyber security workforce in the electric power grid look like?

Methodology

In order to compare the needs of the sector to the available solutions, one must understand both the needs and the available solutions. From there, it is necessary to compare the needs against the solutions and to either qualify or quantify that comparison in a way that provides actionable output that can be leveraged by future efforts.

A common sense approach to this is to gather information about the needs of the sector and compare that to a survey of the available solutions. To gather the needs, one must look at surveys that have been conducted, or to research derivable needs via aggregation of job postings or other information available from hiring members of the sector. To survey the available solutions, one must first determine what solutions are available and to then acquire the outline, syllabus, and if possible the body of knowledge or actual training material that the solution utilizes.

Another approach could include just leveraging domain expertise to understand the space and execute the comparison. This approach could be biased and too limited in visibility or scope to adequately address the true sector needs. A final approach could be to produce and conduct a directed survey to gather these needs and information about solutions. While that could be effective, it is time consuming and only as good as the survey and the quantity and quality of the responses to that survey.

For these reasons, this project takes the approach of leveraging past work and adding domain expertise and inquiries for clarification to various needs or solutions. This combined approach should resolve limitations with each of the other approaches while maintaining an execution plan that remains both tractable and efficient. That execution plan can also be conducted in the allotted period, which is a key to success.

Approach Explanation

To approach this project, preliminary work was conducted to determine what base material was already out there. The O'Neil (2012) report provides necessary background on sector needs, including an appendix of job ads. This material was recently generated and is therefore sufficiently fresh to be used as a source of sector needs. For the solution space, research had to be done to see what is available and then work to obtain the necessary assets from each of those solutions. In some cases, the necessary syllabus and body of knowledge material was available on the web. In other cases, it had to be requested from the author or organization.

Once the material is obtained, it must be evaluated. There are several approaches that could be taken to analyze this material. One can compare each need to the solutions, mapping one to one between needs and solutions. This requires understanding what the need is and what a

corresponding body of knowledge would need to be to provide a solution. From this understanding, a mapping could be done. Another approach would be to categorize the needs and categorize the subjects in the solutions and then provide a mapping between the two. This abstracts the needs and solutions up a level, and provides a broader categorization to compare against, rather than the detail of a one-to-one comparison.

Approach Defense

There is value in both of the above stated approaches. For this effort, both methods are being undertaken. This will provide at least two ways the information can be leveraged, and provides the ability to re-reason about the categories and classify in a different way if deemed appropriate. Since this is a work product that is intended to be leveraged in future efforts, it needs to be flexible and adaptable to the needs of the future work.

Without this flexibility, there is still value in either independent solo approach. However, there is more power in providing both solutions. For instance, let's say a competency category is identified that deals with authentication technology. It is then determined that there are two solutions that cover that category. However, an organization that wants to evaluate which solution to choose is left without the supporting detail to say which one actually meets their needs, or what aspects of authentication technologies are covered in either solution. This means that the broad categories may be insufficient for someone to derive desired benefits from the analysis. However, organizations may not know what multi-factor authentication schemes are, such as RSA SecureID, and therefore may be better suited to have that technology summarized in a broad category rather than try to understand the details. These varied needs are therefore the

impetus behind doing the combined approach of providing both axis by which to evaluate the output.

Project Development

The development of this project is not a traditional development process. There is no code that will be generated, nor a system built. Instead, the work product is a set of documents that will allow an entity to build upon or leverage this work for other efforts or to evaluate against their own criterium.

Hardware

No hardware will be utilized for this effort.

Software

No software must be purchased or developed for this project.

Tech Stack

No layers of service will be provided for this project, as the output of the project is an analysis rather than a technological solution. This analysis provides the basis for a tangible deliverable of future training material. That training material may have hardware, software, or service layer requirements when that is undertaken.

Architecture Details

There will be no architectural elements of this project, including but not limited to the setup of any systems, networks, or demonstration platforms.

Resources Used

The only resources utilized for this project are both digital and physical copies of training syllabi, bodies of knowledge, and other related information. This is combined with existing work

that was analyzing the needs of and for certification in this sector. The analysis is a qualitative analysis that is conducted as a combination of digital and physical inspection, cross-correlation between the needs from existing work, and then cognitive analysis to determine the mapping of needs and requirements to an effective and comprehensive topic coverage mapping.

Final Output

The tangible output of this project is a combination of this report and its appendices that will provide the documentation of the gap analysis and the corresponding mappings to workforce requirements and competency areas. The training material that addresses that output is future work that is out of scope of the current project.

Intangibly, the analysis done here will benefit companies through potential increased efficiency in training their workforce and decreased costs by selecting the right training to meet the job requirements that personnel need to be trained for. These are intangible as they cannot truly be measured without a complete parallel analysis being conducted for any given employee. This assessment is difficult, if not impossible, to conduct because one a training path is selected for an individual, they cannot unlearn what they were just trained on and therefore cannot return to the prior state to see how their performance would compare if they took a different path. Further, job performance from one person to another cannot be correlated as each person is unique. One could use items like the Job Performance Metric (JPM) to assess individuals based on competencies, but again comparing two individuals is not a true correlation.

Quality Assurance

The analysis is to be spot checked through interaction with source inputs and subject matter experts in this sector. Once the analysis is complete and the project outputs are drafted,

they will be reviewed for completeness both internally and with external subject matter experts. This review process will help identify any missing areas of competency or areas that are identified as being superfluous to the intended goal.

Quality Assurance Approach

Quality assurance for this project is a bit subjective. The mapping of needs to solutions can be considered covered on a varied scale. For instance, one effort may go into great detail on a particular subject matter, while another may only spend a moment or two on that topic. Without reviewing the actual training material in depth (which may not be generally available), it is hard to quantify the amount of coverage. Therefore, if a topic is indicated as part of the outline, syllabus, or body of knowledge, then it is considered covered to some degree. If it is not indicated or could be derived using common sense of logical domain connections, then it is considered uncovered. For aggregated areas, they are considered covered if a sufficient amount of material is covered for that aggregated area. For instance, if an aggregated area consists of 5 topics, and only 2 are covered by a training course, then that aggregated area was considered inadequately covered.

The other area of quality control comes in the aggregated or generalized categorization of topic areas. While these mappings are likely straightforward, they will be reviewed to ensure that the categorization is considered accurate and sufficient to capture the intent.

These two approaches to quality control will help ensure the quality of the project. Failure to conduct quality control analysis on the outputs places the work in a position to fail its intended purpose. The intent is to provide a valid gap analysis and a mapping that is both usable and beneficial to both future work and for use by members of the sector.

Solution Testing

Since the work product is documentation of an analysis, there is no work product to methodically test. As such, no test cases or acceptance criterium are defined.

Implementation Plan

Without an analysis of the existing bodies of work, and a mapping of those existing efforts to the needs of the sector, training improvement cannot be accomplished. This project will serve as a foundational piece to help move the education and workforce development in cyber security forward for the electric power grid.

In doing so, this project will produce a complete analysis of the various bodies of knowledge for cyber security training in the electric power grid. Further, a needs assessment will be documented that provides the aggregated needs of cyber security positions in this space. This will be combined to produce a gap analysis. This analysis will serve as a blueprint for coursework material creation to educate towards that comprehensive body of knowledge.

The final output of the project will be that gap analysis and mapping, with insight provided from the precursory work that led to the creation of that aggregated and specialized body of knowledge. Upon completion of this project, that analysis can be leveraged to facilitate the actual creation of training material that can then be used to effectively and efficiently train the emerging workforce in this domain.

Strategy for the Implementation

There are few alternatives to the approach. For instance, one could conduct a body of knowledge creation blindly that looks to address the stated needs of the sector. While that may have merit, it ignores the prior work and pedagogy in this area and therefore attempts to re-

invent the wheel. Another approach would be to simply use a single source of training and map that to the needs of the sector, looking for gaps. While this may also provide merit, it is not comprehensive and does not adequately cover the fully available body of work. Further, this singular approach would not allow for training-to-training comparisons.

Therefore, a comprehensive approach is taken that maps existing work to needs, job roles, and competencies. This comprehensive approach provides extreme value while not being silo'd in one particular approach. It fairly identifies gaps, and determines mappings of training material to the corresponding needs of the sector.

Phases of the Rollout

Since there is not a delivered piece of hardware, software, or system, there is no rollout to be staged or scheduled. The project will provide documentation of the work produced and the corresponding documents themselves. These will be delivered with the final report.

Details of the Go-Live

Since there is no hardware, software or system being delivered. No go-live decisions need to be made.

Dependencies

The analysis of mappings to job roles, responsibilities, and competencies is dependent on the topic coverage mappings. These topic coverages are used as the input to determine the mapping to the aggregated areas. The NICE framework provides listings of various topics and how they map to the categories, although those topics are not a one-to-one mapping with the ones identified here. This is a result of the mappings here being domain specific rather than generalized up to broad cyber security in multiple domains.

Deliverables

The project provides an analysis that is formed on multiple axis: 1) a topical categorization, 2) a job responsibility mapping, 3) a cybersecurity workforce mapping, and 4) the NICE competencies mapping. This will provide a detailed gap analysis of those needs and mappings to determine what is not yet covered by the supporting material.

Training Plan for Users

Since no hardware, software, or system is being developed, no training will be created. The deliverables should be able to stand on their own and be utilized without the need for explicit training.

Risk Assessment

With any project, there are risks that may be encountered. Below is an itemization of those risks and their corresponding analysis.

Quantitative and Qualitative Risks

One risk is the failure to acquire adequate source material for cyber security training in this sector. This lack of sufficient material risk could result in setbacks to the project to determine more source material by which to draw conclusions.

Another risk is the availability of the requirements for jobs in this sector. Namely, there is the possibility that there have not been specific jobs posted, or that the job descriptions have been predominately high-level or lacking sufficient detail to compose a requirements list. It is also possible that the hiring managers in this domain may not be forthcoming with the information about their needs or deficiencies in hiring cyber security professionals if they need to

be queried directly. Further, these hiring managers may not be known or accessible in the timeframe needed to execute the project.

The final risk is that it is possible that the gap analysis of existing training will not uncover any significant gaps. While this is unlikely, there is still tremendous value add in aggregation of the body of knowledges across various training opportunities to derive a complete approach to training for this sector. Further, organizing that aggregated topical coverage into a future modular based approach provides intrinsic value for both operational efficiency and effective training. This could be realized through being able to select only the areas where training is needed, and leveraging the self-standing and self-paced approach of the future modular training to train the new workforce in less time and with more impact.

Cost/Benefit Analysis

The risk of a failure to acquire adequate source material for cyber security training in this sector and the risk of a lack of availability of the requirements for jobs in this sector could have shortfalls. The cost of a shortfall will simply result in a less comprehensive mapping and gap analysis. By having a less comprehensive canvas of material, the analysis may not cover material that is relevant to those that are assessing the value of utilizing a particular training opportunity. This could result in wasted expenditures to training staff in a less effective means, or in a way that does not meet the job requirements that are desired. Since there is no incurred costs to the companies for the use of this analysis, there is no drawback to a cost overrun on its production.

In the case that the gap analysis of the existing training does not uncover any significant gaps there is no shortfall to the entities using this analysis as the mapping to requirements would still provide tremendous value to the sector. Any gaps in the training are intended to map to

future efforts that will aim to fill those gaps and provide more effective training to meet the needs of the sector. Since there is no incurred costs to the companies for the use of this analysis, there is no drawback to a cost overrun on its production.

Risk Mitigation

The lack of sufficient material risk is mitigated in this project due to a variety of training resources having already been uncovered to feed into the analysis. These include resources such as the GIAC GICSP (2103) program, several training courses, and academic coursework. Further, the author has strong connections to the sector that can be leveraged to garner further information surrounding needs.

If the lack of sufficient material risk was not mitigated, more source material would need to be discovered. This could be done through interactions with various industry members or other subject matter experts. This provides the benefit of exposing other material, but has a drawback of acquisition of the necessary information for the newly discovered coursework. In most cases the necessary material is available online, but in other cases it has to be requested directly from the provider and that request cycle could result in setbacks.

The lack of exposure to job requirements is also mitigated, due to the O'Neil (2012) study which includes job listings across various operating domains of this sector. This is combined with the mitigation for the lack of forthcoming information from hiring managers, as O'Neil (2012) has already undertaken a survey of this area and aggregated some relevant information that was be leveraged for this effort.

Post Implementation Support and Issues

Post Implementation Support

Having accessible, effective, and well-positioned training allows businesses to scale up their employees at will. If this material is tuned specifically to the types of needs that this domain, and its specific businesses have, the effectiveness of both existing and newly acquired staff is increased. This is further supported by the modularity of the intended body of knowledge and coursework, as it enables piecewise learning of the necessary material.

Further, by having the material openly and widely available and designed in this modular way, businesses will have more effectively trained staff that are better suited in carrying out their duties. In order to realize such material, this project's gap analysis and body of knowledge creation is foundational to the creation of such coursework.

By having adequately and effectively trained workforce, the companies and the nation as a whole is in a better position to detect and defend our critical infrastructure. This could result in both operational and capital expenditure savings by saving downtime, loss of critical function, operational impact, or customer impact of a potential intrusion. While proper training goes a long way to being prepared, it does not prevent these types of attacks. It is assumed that the training will allow the companies to leverage more complex security solutions that position the company in a more secure manner, potentially mitigating many attempted compromises.

Post Implementation Support Resources

No direct resources will be provided to support the training or realization of training, however the source material is key to addressing those needs. As part of future work, the material will be developed and made openly available. This effort is out of scope of this project, but is

inherently intended to become a resource that others can build on and around to further their efforts.

Maintenance Plan

If one were to maintain the output of this effort, the tasks would be straightforward. One would first obtain the new course syllabus or body of knowledge. After careful evaluation and review, that new information would be added to the table that provides the mappings of coverage. Any changes to the covered material of this new course, or any of the existing courses would need to be re-evaluated to determine the changes in coverage and the implication on the mappings. This should be a generally trivial effort for any incremental changes.

Conclusion, Outcomes, and Reflection

Project Summary

In this project a detailed analysis was done to look at the available training courses for cyber security in the smart grid and map those to the corresponding needs, competencies, and responsibilities that exist in the sector. This analysis was intended to discover any existing gaps in the availability of material and the topics that are taught. Further, it was intended to look at the comparison of job responsibilities and needs to the current body of knowledge that is taught in the space. It was hypothesized that there exists a gap in this coverage, and that hypothesis was confirmed.

Training Analysis

In this project, several training or academic courses were identified as applicable to the matter under study. This includes the following, “Assessing and Exploiting Control Systems with SamuraiSTFU” (SamuraiSTFU), “ICS410: ICS/SCADA Security Essentials” (SANS),

"Understanding, Assessing and Securing Industrial Control Systems" (SCADAhacker), "Control System Cybersecurity Course" (Cybati), and Washington State University EE539 "Cyber-Infrastructures for the Smart Electric Grid" (WSU). These courses were selected based on their wide public visibility and have been established for a period of time that allows the material to mature. There are other courses that exist, some new to the field and some that have been around longer. For example, the Idaho National Lab SCADA training courses have been around for years, but are soon to no longer be available as the program is ending. Therefore, there is little value in providing an analysis for material that is going away.

The SamuraiSTFU course is offered in 3 variants, a 5 day, 3 day, and 2 day course. It has a penetration testing focus and attempts to assume no base knowledge prior to entering the course. It focuses on hands on testing using virtualized and real power system gear while following the NESCOR assessment methodology. It's objectives are to take an active red team assessment point of view and to explain ethical penetration testing, how to use various open-source tools, and to proceed with active exploitation of hardware, network, user interfaces, and service side vulnerabilities in the context of the Smart Grid. The course allows you to leave with a PDF of the material and the ability to purchase the demonstration kits that were utilized during the course.

The SANS ICS 410 course is a 5 day course that is geared towards the Global Information Assurance Certification bodies Global Industrial Cyber Security Professional (GICSP) certification. This course blends a mixture of attacking and defense to develop a foundational set of standardized skills and knowledge base. The general target of the course is workforce development, and it leverages a hands-on approach. The course utilizes virtualization

and recommends that a fundamental understanding of information security be present, or to take a corresponding SANS SEC301 Introduction to Information Security course.

The SCADAhacker course comes in 3 variants, a 5 day all inclusive course, a 10 day private course, or a 1 day intermediate course. The premise behind the SCADAhacker course is that the other existing courses focus too much on theoretical concepts or red team (hacking). It attempts to cover in-depth concepts of industrial control systems with demonstration and application of advanced security techniques. It targets end-users, asset owners, integrators, and vendors that are faced with the challenge of securing systems in this domain. It's emphasis is almost entirely on securing the systems and the principles behind it, rather than on attacking or exploiting the systems. It leverages approximately 25% of the time of the 5 day course for hands-on exercises. Students leave the course with a copy of the SCADAhacker reference library of standards and best practices, a catalog of software, access to download a library of virtual machines, the printed course material, and a copy of the book Industrial Network Security. The 10 day course is only given privately, an the 1 day course targets understanding the concepts of applying these techniques to professionals with a foundational understanding in industrial control systems, information technology, and cyber security.

The Cybati course has 3 variants, a 5 day, 2 day, and online distance learning course. The intent of the course is to understand the elements of, ethically assess, and proactively defend control systems. There is heavy use of hands-on exercises which are arranged in pods (teams of 2 people). This course focuses on cyber security topics, with active exploitation and exploration on real and modeled systems while providing additional base foundational skills like explanations of

ladder logic. The distance learning variant provides recorded videos lecturing on the topic material combined with hands-on exercises and is designed to be executed over a 6 week period.

The WSU course is an academic offering and is intended to provide an overview (breadth rather than depth) of fundamental principles of Smart Grid operation and control, Smart Grid technologies, and the interdisciplinary nature of these systems. The intent is to complete the course with several key areas covered: 1) the understanding of basic principles of smart grid components and operation; 2) understand the principles of communications, data management, distributed computing, and cyber security; 3) the ability to critically analyze interdependencies of related infrastructure for security; and 4) to apply interdisciplinary principles to build secure critical infrastructure for the smart grid.

For this analysis, all of the surveyed material had at least a syllabus. In the case of Cybati and SamuraiSTFU, the full course material was in possession of the author. In the cade of just syllabi being available, the mappings may be imperfect as some assumptions had to be made. Any invalid assumptions could result in slight inaccuracies on coverage, but shouldn't affect the overall quality in any major way.

In many ways these courses compliment each other. For instance, the WSU course provides background knowledge that is intended to instill understanding of the fundamental concepts. The SANS ICS 410 is designed to provide foundational core knowledge associated with ICS/SCADA systems and create a solid base that entities can utilize and that maps towards job responsibilities. The SamuraiSTFU course is an advanced course that looks specifically at the red (attack) based methodologies and is geared towards actual penetration testing and assessment. The SCADAhacker advanced course goes the opposite direction and focuses on

defense based approaches leveraging available software and hardware solutions and maps those solutions based on the assessment of needs for proactive (or reactive) defense. The Cybati solution is also an advanced course that looks deeper at items like regulation and control system context and impact while demonstrating the concepts through foundational application including some red (attack) approaches. All of these can work together in various ways, but it is likely impractical for any one entity to spend the time (and money) to attend all of these courses and then develop true competency in all of these areas in a short period of time.

Workforce Analysis

The DOE Secure Power System Professional (SPSP) Project (DOE SPSP) identified three specialized functional roles for cyber secure power engineers; 1) power system incident response, 2) intrusion analysis, and 3) security operations. It was determined that a secure power system professional is typically charged with doing the following.

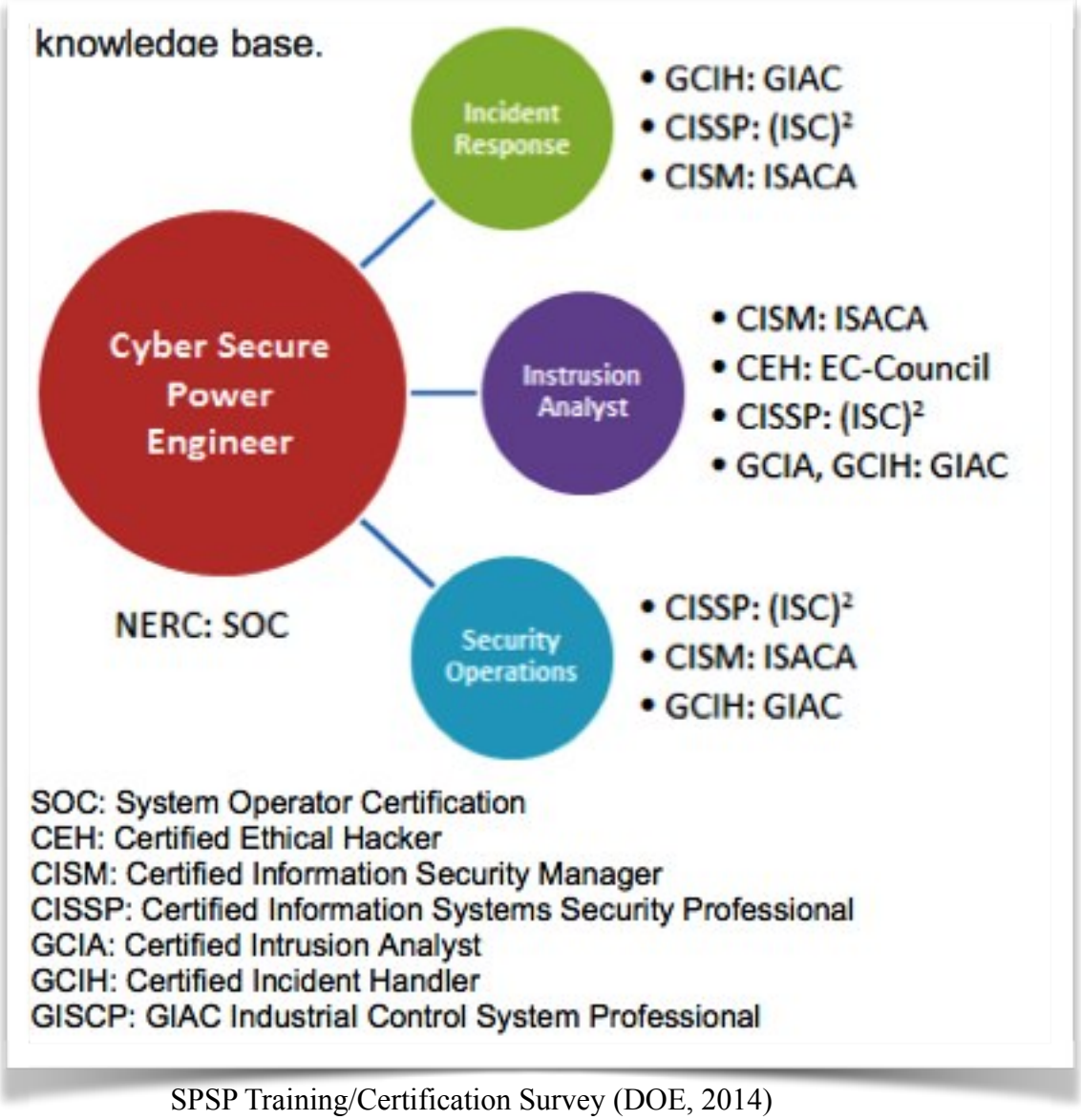
- *Power System Incident Response*: Respond to urgent situations by performing mitigation, preparedness, response, and recovery tasks.
- *Power System Intrusion Analysis*: Monitor networks, conduct traffic analysis, and detect intrusions due to malware, employee misconduct, sensitive data breaches, and other forms of external attacks.
- *Power System Security Operations*: Test, implement, deploy, maintain, and administer the infrastructure hardware and software required to effectively manage the smart grid network defense resources.

Within these functional roles, the initiative undertook defining responsibilities of those roles. As such, 11 responsibility areas were also identified:

1. Analyze Security Incidents
2. Assess and Manage Risk
3. Communicate Results
4. Develop and Manage Personnel
5. Identify and Mitigate Vulnerabilities

6. Implement Security Monitoring
7. Log Security Incidents
8. Manage Process and Procedures
9. Manage Projects and Budgets
10. Manage Security Operations
11. Respond to Intrusions

The SPSP initiative concluded that there were no existing education or training courses that truly encompassed the needs of the emerging professionals in this sector. In doing so, they looked at a variety of different professional courses and the corresponding certifications.



SPSP Training/Certification Survey (DOE, 2014)

Further, they also identified the qualifications of the ideal candidate to fill this cyber secure power engineering position. These qualifications would be intended as a base for job descriptions or evaluation of potential applicants and are detailed below.

Basic Qualifications:

- Experience working in utilities with cyber security expertise
- Experience in modern power system technologies
- Bachelor's degree in electrical engineering, industrial control systems, mechanical engineering, or other relevant fields
- Knowledge of SCADA and power system operations

Preferred Skills:

- Familiarity with smart grid vendors and expertise in smart grid security methodologies
- Expertise in computer networking. both standard and SCADA protocols
- Energy Management Systems (EMS)
- Control room operations
- Industry-adopted certificates (see diagram)
- Knowledge of and experience in cyber security detection, prevention and risk management of power assets
- Familiarity with industry codes and standards, especially NERC compliance

Desirable Professional Attributes:

- Motivated and team-oriented self-initiator
- Creative problem-solver
- Excellent communicator with good interpersonal skills
- Able to cope with a high-stress work environment
- Committed to maintaining credentials through professional development and continuing education

The NICE national cybersecurity workforce framework is broader, but still applicably defines several categories. Namely, it defines 31 speciality areas that then are organized into seven categories. Those seven categories are defined as follows:

Securely Provision: Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems (i.e., responsible for some aspect of systems development).

Operate and Maintain: Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

Protect and Defend: Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.

Investigate: Specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.

Collect and Operate: Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

Analyze: Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

Oversight and Development: Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.

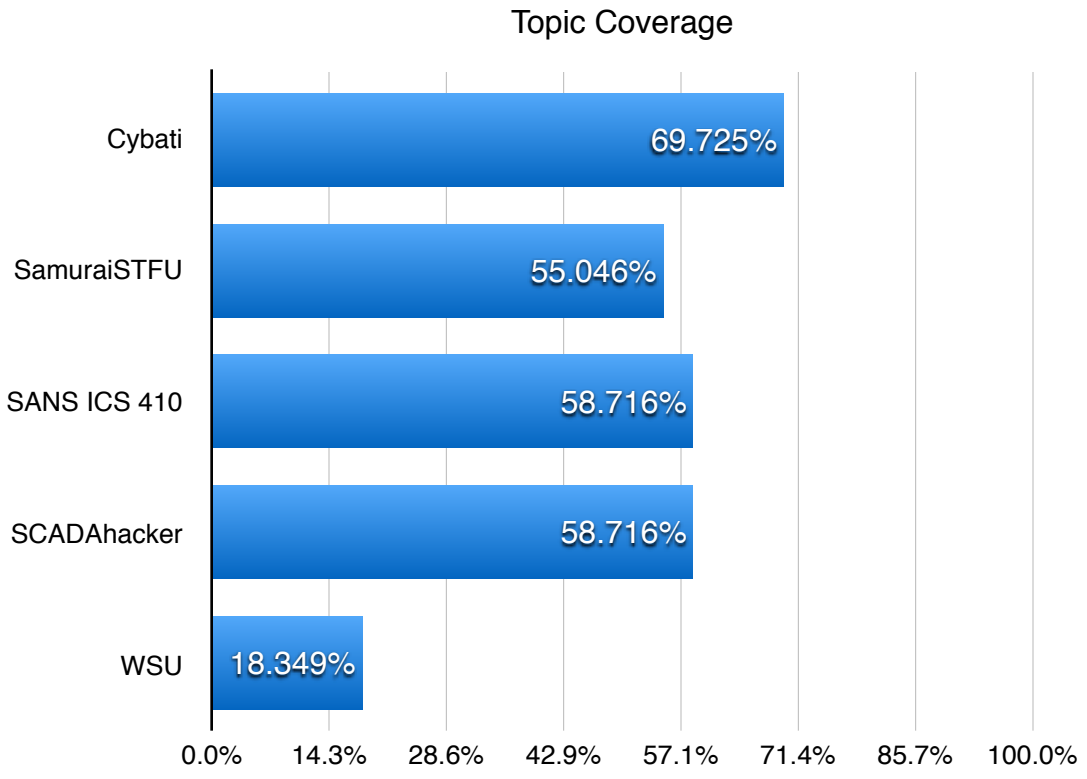
Deliverables

The project provides an analysis that is formed on multiple axis: 1) a topical categorization, 2) a job responsibility mapping, 3) a cybersecurity workforce mapping, and 4) the

NICE competencies mapping. These provide a detailed gap analysis of the needs and mappings to determine what is not yet covered by the supporting material.

Outcomes

The topics covered by the material were iterated at a medium to high-level and then a coverage analysis was done of each training material against the superset of topics. As illustrated in the chart, no single course covers all topics and the coverage is fairly sparse. Between each training course the topics covered also vary, which can be seen in Appendix A.

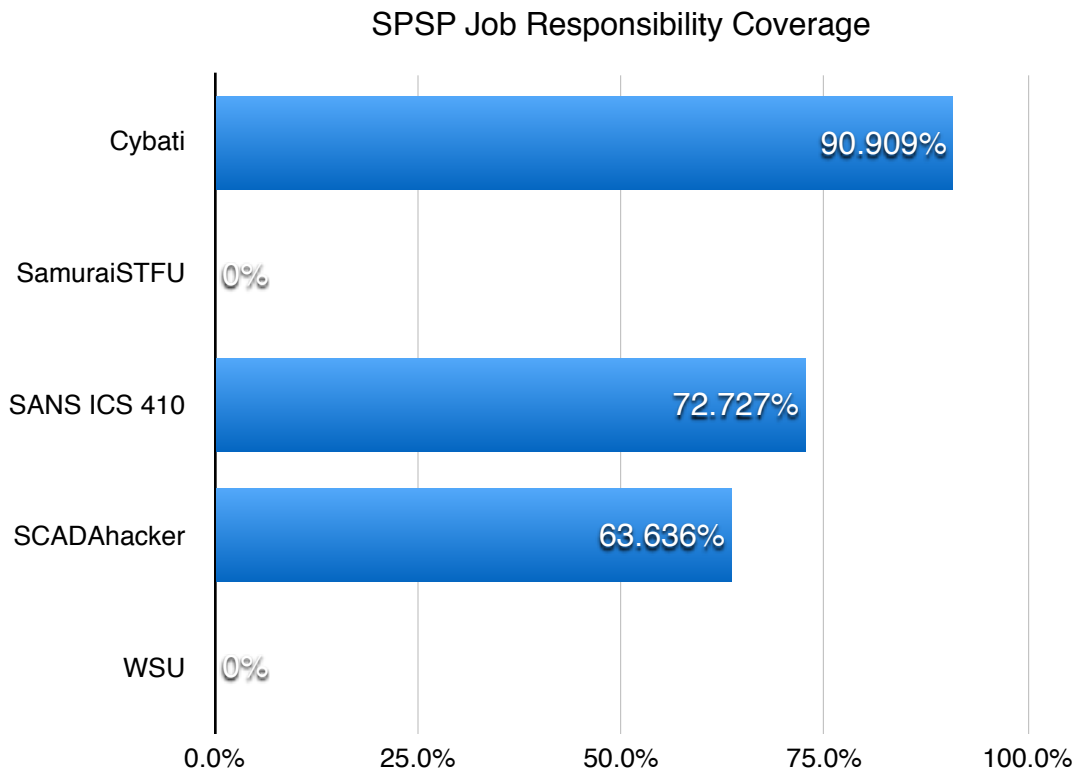


Each training course was also mapped to the responsibilities that have been defined from the SPSP effort which is intended to indicate typical responsibilities of a security professional in the smart grid domain. As evidenced in the chart, the coverage here is interestingly sparse. Some

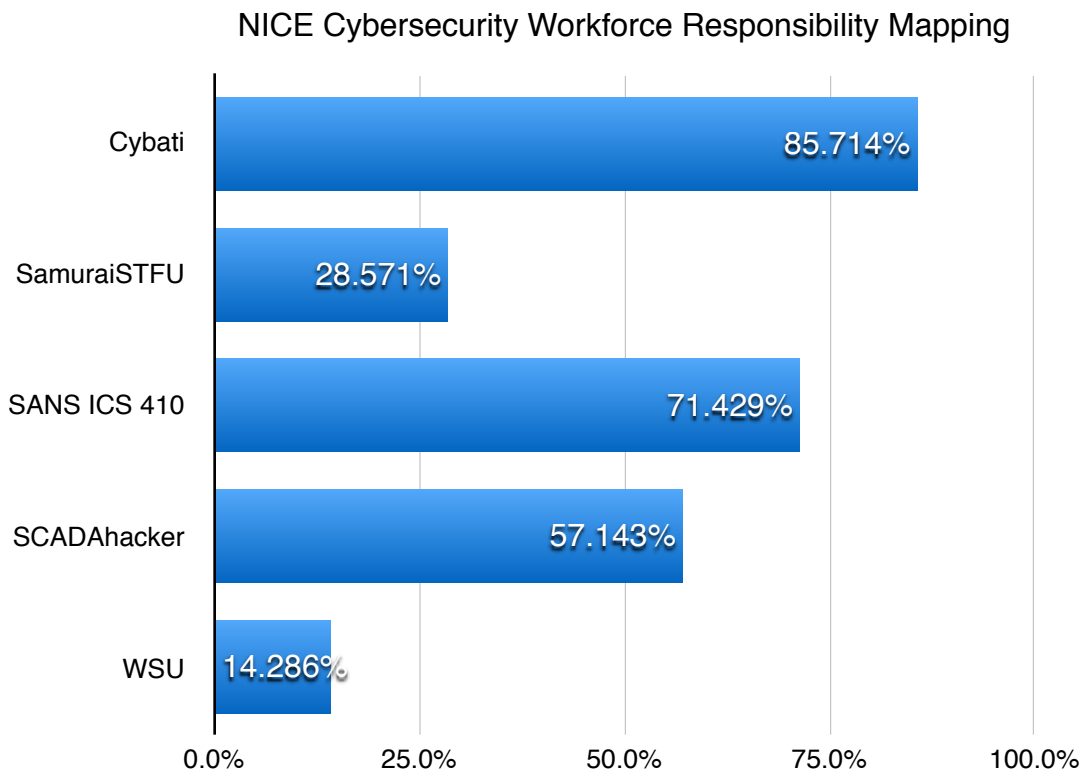
training courses have zero coverage of the topics areas that are considered to be mapped to cyber security positions in this sector (SPSP designation). There are various reasons for that mapping, which will be explained below.

In the case of SamuraiSTFU, this is because that training material focuses on red-team style activities that are focused on security assessment of critical infrastructure in the smart grid. As that is not a job responsibility that is typically undertaken by Secure Power System Professional's in the field. These responsibilities are normally undertaken by consultants, integrators, or dedicated security consulting firms.

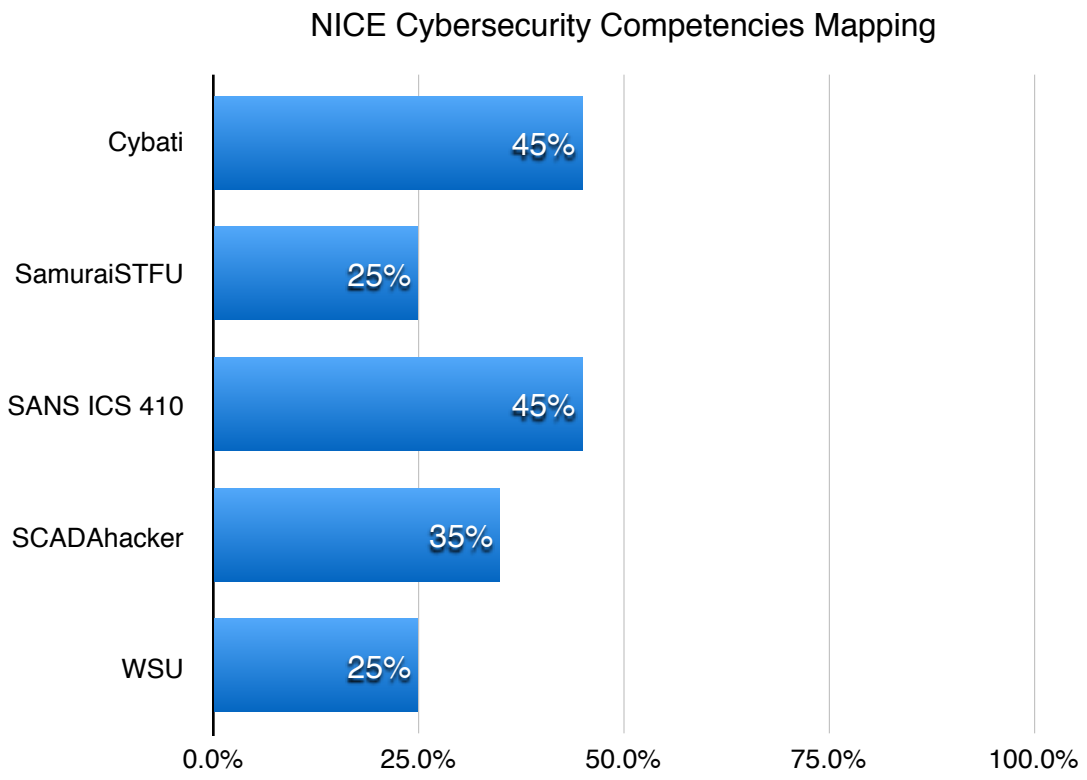
In the case of the WSU material, the material was intended to provide an introduction to the topic area and to educate about some of the underlying principles. As such, it is more theory based rather than the practical nature that is assumed for job responsibilities. This reflects negatively on this mapping, but does not discount the value of the material.



A further mapping is provided in the NICE framework with the Cybersecurity Workforce Responsibility Mapping. In this mapping, NICE looks broader across cybersecurity roles in several industries. Therefore, this is a more comprehensive mapping to potential responsibilities that a cyber security professional may need to have a basis in.



The last mapping is the competencies behind the responsibilities defined in the NICE framework. These competencies provide a cross-section of details that help determine the general mapping of smart grid security professionals to the broader cyber security topic areas. The coverage of each training course here, while sparse, is better represented than looking purely at the responsibilities.



Reflection

This analysis proved out the hypothesis that there is no single course that covers the full breadth of topics that is needed in cyber security roles for the smart grid. It further shows the gaps that were not covered at all by any of the courses as well as gaps in relation to the cyber security training of smart grid professionals in relation to the training for the broader topics of the cyber security domain across industries.

References

Anurag K Srivastava, Senior Member, IEEE, Carl Hauser, David Bakken, Senior Member, IEEE, and Min Sik Kim, Member, IEEE," Design and Development of a New Smart Grid Course at Washington State University," Power and Energy Society General Meeting, IEEE 2012, PP. 1-2.

Cybati. Control System Cybersecurity Course training syllabus. Retrieved on March 19, 2014 from https://cybati.org/education

Department of Energy. Secure Power Systems Professionals Project. Retrieved on March 19, 2014 from http://energy.gov/oe/downloads/developing-secure-power-systems-professional-competence-alignment-and-gaps-workforce

Depaul University. CNS 366: Critical Infrastructure and Control Systems Cybersecurity. Retrieved on March 19, 2014 from http://www.cdm.depaul.edu/academics/pages/courseinfo.aspx?Subject=CNS&CatalogNbr=366

G. Heydt, M. Kezunovic, P. Sauer, A. Bose, J. McCalley, C. Singh, W. Jewell, D. Ray, V. Vittal, "Professional resources to implement the "smart grid"", North American Power Symposium (NAPS), 2009, 4-6 Oct. 2009, Starkville, MS, USA

Global Industrial Cyber Security Professional - GICSP. (2013). Retrieved on March 19, 2014 from http://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

M. Crow, "Programmed for success: Educating tomorrow's workforce", IEEE power and energy magazine, vol. 8, issue 4, July-August, 2010

M. Kezunovic,"Teaching the Smart Grid Fundamentals Using Modeling, Simulation, and Hands-on Laboratory Experiments," Power and Energy Society General Meeting, IEEE 2010, PP. 1-6.

NICE-National Initiative for Cybersecurity Education. (2011). The National Cybersecurity Workforce Framework. Retrieved on March 28, 2014 from http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf

O'Neil, LR. Assante, MJ & Tobey, DH. (2012). Smart Grid Cybersecurity: Job Performance Model Report. PNNL- 21639. http://energy.gov/sites/prod/files/2013/05/f0/SGC-Report.pdf

P. Sauer, "Educational needs for the "Smart Grid" workforce", IEEE Power and Energy Society General Meeting, 25-29 July 2010, Minneapolis, MN.

SamuraiSTFU. Assessing and Exploiting Control Systems with SamuraiSTFU training syllabus. Retrieved on March 19, 2014 from http://www.samuraistfu.org/training-syllabus

SCADAhacker. Understanding, Assessing and Securing Industrial Control Systems training syllabus. Retrieved on March 19, 2014 from http://www.scadahacker.com/training.html

SANS. ICS410: ICS/SCADA Security Essentials training syllabus. Retrieved on March 19, 2014 from http://www.sans.org/course/ics-scada-cyber-security-essentials

Washington State University - WSU. CPTTS 539: Cyber-Infrastructures for the Smart Electric Grid course syllabus. Retrieved on March 19. 2014 from http://gradschool.wsu.edu/FacultyStaff/Committee/Documents/2013-14/Feb182014/ee_cptts%20539.pdf

Appendix A: Topic Coverage From Available Training

In this table, FALSE means that the area was not covered or perceived to be covered. If TRUE is present, then it was perceived that the area had some degree of coverage. Note, that to fully assess coverage, one would need a graduated scale or to define further subtopics to fully determine the efficacy of the material in that area. This secondary analysis was not possible in all cases due to the lack of the full training material for all opportunities covered.

The analysis of coverage in a particular area was a judgement call based on some combination of the analysis of the syllabus, training material, descriptions, body of knowledge, or certification tests. This mapping is the product of the thesis author, who is considered a subject matter expert in this domain, but used judgement based on the available material. Consider all of these mappings malleable and subject to interpretation, but mapped using the same criteria and assumptions throughout.

Topic Coverage

	Cybati	SamuraiSTFU	SANS ICS 410	SCADAhacker	WSU
1-day course option	FALSE	FALSE	FALSE	TRUE	FALSE
10-day course option	FALSE	FALSE	FALSE	TRUE	FALSE
2-day course option	TRUE	TRUE	FALSE	FALSE	FALSE
3-day course option	FALSE	TRUE	FALSE	FALSE	FALSE
5-day course option	TRUE	TRUE	TRUE	TRUE	FALSE
Academic Term	FALSE	FALSE	FALSE	FALSE	TRUE
Active Exploitation	TRUE	TRUE	FALSE	FALSE	FALSE
Assessment Methodology	TRUE	TRUE	FALSE	TRUE	FALSE
Assumes No Prior Knowledge	FALSE	TRUE	FALSE	FALSE	TRUE

	Cybati	SamuraiSTFU	SANS ICS 410	SCADAhacker	WSU
Assumes Prior Knowledge	TRUE	FALSE	TRUE	TRUE	FALSE
Attacking ICS Protocol	TRUE	TRUE	TRUE	FALSE	FALSE
Auditing and Analysis	TRUE	FALSE	TRUE	TRUE	FALSE
Automation	TRUE	FALSE	TRUE	TRUE	FALSE
Blue Team Skills	TRUE	FALSE	FALSE	TRUE	FALSE
Boot process, runlevels, and services	FALSE	FALSE	TRUE	FALSE	FALSE
Bus sniffing	FALSE	TRUE	FALSE	FALSE	FALSE
Business logic analysis	TRUE	TRUE	FALSE	TRUE	FALSE
Case Studies	TRUE	FALSE	FALSE	TRUE	TRUE
Cautions on ICS Security Assessment Process	TRUE	TRUE	FALSE	FALSE	FALSE
Certification available	FALSE	FALSE	TRUE	FALSE	FALSE
Communications	TRUE	TRUE	TRUE	TRUE	TRUE
Contingency and Continuity Planning	FALSE	FALSE	TRUE	TRUE	FALSE
Control Server Attacks	TRUE	TRUE	TRUE	TRUE	FALSE
Control System Background	TRUE	FALSE	FALSE	TRUE	TRUE
Controller and Field Device Security	TRUE	TRUE	TRUE	TRUE	FALSE
Cryptography Fundamentals	FALSE	TRUE	TRUE	TRUE	TRUE
Defending ICS Systems	TRUE	FALSE	TRUE	TRUE	FALSE
Demonstrations	TRUE	TRUE	TRUE	TRUE	FALSE
EEPROM password dumps	FALSE	TRUE	TRUE	FALSE	FALSE
Embedded device data extraction	FALSE	TRUE	FALSE	FALSE	FALSE
Enforcing Security Policy	FALSE	FALSE	TRUE	TRUE	FALSE
Ethical Disclosure	TRUE	FALSE	FALSE	FALSE	FALSE
External Resources or References	TRUE	FALSE	TRUE	TRUE	TRUE
Field Components	TRUE	TRUE	TRUE	TRUE	FALSE
Firewalls	TRUE	FALSE	TRUE	TRUE	TRUE

	Cybati	SamuraiSTFU	SANS ICS 410	SCADAhacker	WSU
Firmware analysis	TRUE	TRUE	FALSE	FALSE	FALSE
Firmware dumping	TRUE	TRUE	FALSE	FALSE	FALSE
Firmware exploitiation	FALSE	TRUE	FALSE	FALSE	FALSE
Follows assessment methodology	TRUE	TRUE	FALSE	TRUE	FALSE
Forensics	TRUE	FALSE	TRUE	FALSE	FALSE
Functional Analysis	TRUE	TRUE	FALSE	TRUE	FALSE
Hands-on Labs	TRUE	TRUE	TRUE	TRUE	FALSE
Hardware assessment	TRUE	TRUE	FALSE	FALSE	FALSE
HMI Attacks	TRUE	TRUE	TRUE	FALSE	FALSE
Honeypots	FALSE	FALSE	TRUE	FALSE	FALSE
ICS Applications Overview	TRUE	TRUE	TRUE	TRUE	TRUE
ICS Architectures	TRUE	TRUE	FALSE	TRUE	TRUE
ICS Attack Surface	TRUE	TRUE	TRUE	TRUE	FALSE
ICS Device Fragility	TRUE	TRUE	FALSE	FALSE	FALSE
ICS Drivers and Constraints	TRUE	FALSE	TRUE	TRUE	TRUE
ICS Governance	TRUE	FALSE	TRUE	TRUE	TRUE
ICS History	TRUE	FALSE	TRUE	TRUE	FALSE
ICS Network Capture	TRUE	TRUE	TRUE	FALSE	FALSE
ICS Overview	TRUE	TRUE	TRUE	TRUE	TRUE
ICS Protocols	TRUE	TRUE	FALSE	TRUE	FALSE
ICS Security Policies	TRUE	FALSE	TRUE	TRUE	TRUE
ICS Server and Workstation Technology	FALSE	FALSE	TRUE	TRUE	FALSE
ICS vs IT (OT/IT differences)	FALSE	TRUE	FALSE	TRUE	FALSE
Incident Handling	TRUE	FALSE	TRUE	TRUE	FALSE
Incident Response	TRUE	FALSE	TRUE	TRUE	FALSE
Industry Models	TRUE	FALSE	TRUE	TRUE	FALSE
Information Assurance in ICS	FALSE	FALSE	TRUE	TRUE	FALSE
Information Leakage	TRUE	FALSE	TRUE	FALSE	FALSE
Ladder Logic	TRUE	FALSE	FALSE	FALSE	FALSE

	Cybati	SamuraiSTFU	SANS ICS 410	SCADAhacker	WSU
Leverages real equipment	TRUE	TRUE	FALSE	TRUE	FALSE
Leverages virtual equipment	TRUE	TRUE	TRUE	TRUE	FALSE
Linux Hardening	FALSE	FALSE	TRUE	FALSE	FALSE
Linux Landscape	FALSE	FALSE	TRUE	FALSE	FALSE
Logs and Log Management	FALSE	FALSE	TRUE	TRUE	FALSE
Microsoft Systems	FALSE	FALSE	TRUE	FALSE	FALSE
Multiple architectures within a particular domain	TRUE	TRUE	TRUE	TRUE	FALSE
Multiple domains of critical infrastructure	TRUE	FALSE	TRUE	TRUE	FALSE
Network Behavioral Analysis	FALSE	TRUE	FALSE	TRUE	FALSE
Network Communications Attacks	TRUE	TRUE	TRUE	TRUE	TRUE
Network Components	TRUE	TRUE	TRUE	TRUE	TRUE
Network Fundamentals	TRUE	TRUE	TRUE	TRUE	TRUE
Online course option	TRUE	TRUE	FALSE	FALSE	FALSE
Open Source Intelligence (OSINT)	TRUE	TRUE	FALSE	FALSE	FALSE
Password Fuzzing / Cracking	TRUE	TRUE	TRUE	FALSE	FALSE
Password Management	FALSE	FALSE	TRUE	FALSE	FALSE
Patch management	FALSE	FALSE	TRUE	TRUE	FALSE
Pentesting circuits	FALSE	TRUE	FALSE	FALSE	FALSE
Physical Security and Safety Systems	TRUE	FALSE	TRUE	TRUE	FALSE
Process Flow	TRUE	TRUE	FALSE	TRUE	FALSE
Protocol Fuzzing	TRUE	FALSE	FALSE	FALSE	FALSE
Red Team Skills	TRUE	TRUE	FALSE	TRUE	FALSE
Red Team/Blue Team Drill	TRUE	FALSE	FALSE	FALSE	FALSE
Regulation Coverage	TRUE	FALSE	FALSE	TRUE	TRUE
Remote Device Attacks	TRUE	TRUE	TRUE	TRUE	FALSE
RF Analysis	FALSE	TRUE	FALSE	FALSE	FALSE
RF exploitation	FALSE	TRUE	FALSE	FALSE	FALSE

	Cybati	SamuraiSTFU	SANS ICS 410	SCADAhacker	WSU
Risk Assessment and Auditing	TRUE	FALSE	TRUE	TRUE	FALSE
Secure DCS Architecture	TRUE	FALSE	TRUE	TRUE	FALSE
Security Enhancement Tools	FALSE	FALSE	TRUE	TRUE	FALSE
Serial Communications	FALSE	TRUE	FALSE	FALSE	FALSE
Software assessment	TRUE	TRUE	FALSE	FALSE	FALSE
SQLi (Authentication Bypass)	FALSE	TRUE	TRUE	FALSE	FALSE
Standards and Best Practices	TRUE	FALSE	FALSE	TRUE	FALSE
Takeaway hands-on hardware (links or equipment)	TRUE	TRUE	FALSE	FALSE	FALSE
Takeaway hands-on tools	TRUE	TRUE	FALSE	TRUE	FALSE
Takeaway material	TRUE	TRUE	TRUE	TRUE	FALSE
TCP/IP lower-order functions	TRUE	TRUE	TRUE	FALSE	TRUE
TCP/IP middle-layers	TRUE	TRUE	TRUE	FALSE	TRUE
Teaches how to use openly available tools	TRUE	TRUE	TRUE	TRUE	FALSE
Teaches control system context	TRUE	FALSE	TRUE	TRUE	FALSE
Unix and Linux System Fundamentals	FALSE	FALSE	TRUE	FALSE	FALSE
Vulnerability Classes	TRUE	TRUE	FALSE	TRUE	FALSE
Windows Security Infrastructure	FALSE	FALSE	TRUE	FALSE	FALSE
Wireless Network Security	TRUE	FALSE	TRUE	FALSE	FALSE
Percentage	**69.7%**	**55.0%**	**58.7%**	**58.7%**	**18.3%**
Total Checked	**76**	**60**	**64**	**64**	**20**

Appendix B: Mapping of Training to SPSP Responsibilities

In this table, FALSE means that the responsibility area was not covered or perceived to be covered. If TRUE is present, then it was perceived that the area had some degree of coverage. Note, that to fully assess coverage, one would need a graduated scale or to define further subtopics of the training coverage to fully determine the efficacy of the material in that area. This secondary analysis was not possible in all cases due to the lack of the full training material for all opportunities covered.

The analysis of coverage of responsibilities in a particular area was a judgement call based on some combination of the analysis of the syllabus, training material, descriptions, body of knowledge, or certification tests. This mapping is the product of the thesis author, who is considered a subject matter expert in this domain, but used judgement based on the available material. Consider all of these mappings malleable and subject to interpretation, but mapped using the same criteria and assumptions throughout.

Responsibility Mapping

	Cybati	SamuraiSTFU	SANS ICS 410	SCADAhacker	WSU
Analyze Security Incidents	TRUE	FALSE	TRUE	TRUE	FALSE
Assess and Manage Risk	TRUE	FALSE	TRUE	TRUE	FALSE
Communicate Results	TRUE	FALSE	FALSE	FALSE	FALSE
Develop and Manage Personnel	TRUE	FALSE	FALSE	FALSE	FALSE
Identify and Mitigate Vulnerabilities	TRUE	FALSE	TRUE	TRUE	FALSE

	Cybati	SamuraiSTFU	SANS ICS 410	SCADAhacker	WSU
Implement Security Monitoring	TRUE	FALSE	TRUE	TRUE	FALSE
Log Security Incidents	TRUE	FALSE	TRUE	FALSE	FALSE
Manage Process and Procedures	TRUE	FALSE	TRUE	TRUE	FALSE
Manage Projects and Budgets	FALSE	FALSE	FALSE	FALSE	FALSE
Manage Security Operations	TRUE	FALSE	TRUE	TRUE	FALSE
Respond to Intrusions	TRUE	FALSE	TRUE	TRUE	FALSE
Percentage	**90.9%**	**0.0%**	**72.7%**	**63.6%**	**0.0%**
Total Checked	**10**	**0**	**8**	**7**	**0**

Appendix C: National Cybersecurity Workforce Framework Category Mapping

In this table, FALSE means that the category area was not covered or perceived to be covered with sufficient detail. If TRUE is present, then it was perceived that the area had some degree of coverage that could be considered sufficient. Note, that to fully assess coverage, one would need a graduated scale or to define further subtopics of the training coverage to fully determine the efficacy of the material in that area. This secondary analysis was not possible in all cases due to the lack of the full training material for all opportunities covered.

The analysis of coverage of categories in a particular area was a judgement call based on some combination of the analysis of the syllabus, training material, descriptions, body of knowledge, or certification tests. This mapping is the product of the thesis author, who is considered a subject matter expert in this domain, but used judgement based on the available material. Consider all of these mappings malleable and subject to interpretation, but mapped using the same criteria and assumptions throughout.

Cybersecurity Workforce Category Mapping

	Cybati	SamuraiSTFU	SANS ICS 410	SCADAhacker	WSU
Securely Provision: Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems (i.e., responsible for some aspect of systems development).	FALSE	FALSE	TRUE	TRUE	TRUE
Operate and Maintain: Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.	TRUE	FALSE	TRUE	TRUE	FALSE

	Cybati	SamuraiSTFU	SANS ICS 410	SCADAhacker	WSU
Protect and Defend: Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.	TRUE	FALSE	TRUE	TRUE	FALSE
Investigate: Specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.	TRUE	FALSE	TRUE	FALSE	FALSE
Collect and Operate: Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.	TRUE	TRUE	FALSE	FALSE	FALSE

	Cybati	SamuraiSTFU	SANS ICS 410	SCADAhacker	WSU
Analyze: Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.	TRUE	TRUE	TRUE	TRUE	FALSE
Oversight and Development: Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.	TRUE	FALSE	FALSE	FALSE	FALSE
Percentage	**85.7%**	**28.6%**	**71.4%**	**57.1%**	**14.3%**
Total Checked	**6**	**2**	**5**	**4**	**1**

Appendix D: NICE Competencies Mapping

In this table, FALSE means that the competency area was not covered or perceived to be covered. If TRUE is present, then it was perceived that the area had some degree of coverage. Note, that to fully assess coverage, one would need a graduated scale or to define further subtopics of the training coverage to fully determine the efficacy of the material in that area. This secondary analysis was not possible in all cases due to the lack of the full training material for all opportunities covered.

The analysis of coverage of competencies in a particular area was a judgement call based on some combination of the analysis of the syllabus, training material, descriptions, body of knowledge, or certification tests. This mapping is the product of the thesis author, who is considered a subject matter expert in this domain, but used judgement based on the available material. Consider all of these mappings malleable and subject to interpretation, but mapped using the same criteria and assumptions throughout.

NICE Competencies Mapping

	Cybati	SamuraiSTFU	SANS ICS 410	SCADAhacker	WSU
Capacity Management	FALSE	FALSE	FALSE	FALSE	FALSE
Computer Forensics	TRUE	FALSE	TRUE	FALSE	FALSE
Computer Languages	TRUE	FALSE	FALSE	FALSE	FALSE
Computer Network Defense	TRUE	FALSE	TRUE	TRUE	TRUE
Computer Skills	TRUE	TRUE	TRUE	TRUE	TRUE
Computers and Electronics	TRUE	TRUE	TRUE	TRUE	TRUE
Configuration Management	TRUE	FALSE	TRUE	TRUE	FALSE
Contracting/Procurement	FALSE	FALSE	FALSE	FALSE	FALSE
Criminal Law	FALSE	FALSE	FALSE	FALSE	FALSE

	Cybati	SamuraiSTFU	SANS ICS 410	SCADAhacker	WSU
Cryptography	FALSE	TRUE	TRUE	TRUE	TRUE
Data Management	FALSE	FALSE	TRUE	FALSE	FALSE
Database Administration	FALSE	FALSE	FALSE	FALSE	FALSE
Database Management Systems	FALSE	FALSE	FALSE	FALSE	FALSE
Embedded Computers	TRUE	TRUE	TRUE	FALSE	FALSE
Encryption	TRUE	TRUE	TRUE	TRUE	TRUE
Enterprise Architecture	TRUE	TRUE	TRUE	TRUE	TRUE
External Awareness	FALSE	FALSE	FALSE	FALSE	FALSE
Forensics	TRUE	FALSE	FALSE	FALSE	FALSE
Hardware	TRUE	TRUE	TRUE	TRUE	FALSE
Hardware Engineering	TRUE	TRUE	FALSE	FALSE	FALSE
Human Factors	TRUE	FALSE	FALSE	FALSE	FALSE
Identity Management	FALSE	FALSE	TRUE	TRUE	FALSE
Incident Management	TRUE	FALSE	TRUE	TRUE	FALSE
Information Assurance	TRUE	FALSE	TRUE	TRUE	FALSE
Information Management	FALSE	FALSE	TRUE	FALSE	FALSE
Information Systems Security Certification	FALSE	FALSE	TRUE	FALSE	FALSE
Information Systems/Network Security	TRUE	TRUE	TRUE	TRUE	TRUE
Information Technology Architecture	TRUE	TRUE	TRUE	TRUE	TRUE
Information Technology Performance Assessment	FALSE	FALSE	FALSE	FALSE	FALSE
Infrastructure Design	FALSE	FALSE	TRUE	TRUE	TRUE
Internal Controls	TRUE	FALSE	TRUE	TRUE	TRUE
Knowledge Management	FALSE	FALSE	FALSE	FALSE	FALSE
Legal, Government, and Jurisprudence	FALSE	FALSE	TRUE	TRUE	TRUE
Logical Systems Design	FALSE	FALSE	FALSE	FALSE	FALSE
Mathematical Reasoning	FALSE	FALSE	FALSE	FALSE	FALSE
Modeling and Simulation	TRUE	TRUE	FALSE	FALSE	FALSE