Risk Assessment Methodology Based on the NISTIR 7628 Guidelines

Robert K. Abercrombie
Frederick T. Sheldon
Computational Sciences and Engineering Division
Oak Ridge National Laboratory
Oak Ridge, TN 37831-6085
abercrombier@ornl.gov
sheldonft@ornl.gov

Katie R. Hauser
Margaret W. Lantz
1
Computational Sciences and Engineering Division
Oak Ridge National Laboratory
Oak Ridge, TN 37831-6085
khauser@hmc.edu
lantzmw@dukes.jmu.edu

Ali Mili
Department of Computer Science
College of Computing Science
New Jersey Institute of Technology
Newark, NJ 07102-1982
mili@cis.njit.edu

Abstract

Earlier work describes computational models of critical infrastructure that allow an analyst to estimate the security of a system in terms of the impact of loss per stakeholder resulting from security breakdowns. Here, we consider how to identify, monitor and estimate risk impact and probability for different smart grid stakeholders. Our constructive method leverages currently available standards and defined failure scenarios. We utilize the National Institute of Standards and Technology (NIST) Interagency or Internal Reports (NISTIR) 7628 as a basis to apply Cyberspace Security Econometrics system (CSES) for comparing design principles and courses of action in making security-related decisions.

1. Introduction

Complex systems (e.g., e-government, cyber physical systems) configured to deliver service or otherwise interact with a variety of parties or stakeholders are typically designed to balance functional and non-functional requirements. Stakeholders of such systems demand maximum reliability and security. We have developed an approach that allows analysts to estimate the security of a system in terms of the loss that each stakeholder stands to sustain as a result of security breakdowns [1, 2]. Stakeholder mission, in the context of our approach is defined by the set of stakeholder’s system requirements that must be satisfied [3].

Mission assurance is a full life-cycle engineering process that is an essential element of risk assessment [4]. Public and private operations do not differ significantly in their mission assurance needs; we all need cyber information operations that are reliable, available, survivable, and secure [5, 6]. We borrow from the methods used in securing organizations to improve our ability to provide accurate and timely assessments [7, 8]. Organizations typically use a risk assessment and management process to identify and mitigate risks to assure their organizational mission(s) [9]. Risk management provides a structured and transparent process to identify critical resources, estimate threats and vulnerabilities that may intersect to cause harm or increase the likelihood of undesirable events. Moreover, the process estimates the likelihood of security violations and evaluates tradeoffs among control measures used to mitigate the risks, and periodically revisits the analyses as needed. However, the quality of the analysis is a strongly dependent on the accuracy of the inputs to the process.

1.1 Risk Management State-of-the-Art

Organizations currently implement an Information Technology (IT) focused risk management process to identify and mitigate IT related risks to assure their organizational enterprise operates properly [10, 11]. The European Network and Information Security Agency (ENISA) has generated an inventory of risk management and risk assessment methods [12]. A total of 13 methods were considered. Each method in the inventory has been described through a template. The template used consists of 21 attributes that describe...
characteristics of a method. The inventory website also provides for the comparison of the risk management methods and tools [13].

Let’s consider critical infrastructures from the 11 sectors (agriculture and food, water, public health, emergency services, defense industrial base, telecommunications, energy, transportation, banking and finance, chemical and hazardous material, and postal and shipping), and 5 key assets (national monuments and icons, nuclear power plants, dams, government facilities, and commercial key assets). Vulnerability analysis of these infrastructures is well documented, using traditional techniques [14]. Notwithstanding, the electric power industry is applying similar techniques to SCADA (supervisory control and data acquisition) equipment [14], cyber threats, cyber security and the Smart Grid. Approaches are emerging that apply information security techniques easing the complexity of creating tree and graph structures, and deriving probabilistic defense graphs from network architectural models [15]. Further refinements have recently been reported [16] and additional methods have been applied dealing with enhanced dynamic decision making [17].

1.2 Need for Smart Grid Considerations

In September 2011, the DOE’s Office of Electricity Delivery and Energy Reliability published the Roadmap to Secure Control Systems in the Energy Sector [18]. The Roadmap synthesizes expert input from the control systems community, including owners and operators, commercial vendors, national laboratories, industry associations, and government agencies, to outline a coherent plan for improving cyber security in the energy sector. The plan provides a supporting framework of goals and milestones for protecting control systems for the foreseeable future (10 years): By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions. This is a bold vision that confronts the formidable technical, business, and institutional challenges that lie ahead in protecting critical energy control systems against increasingly sophisticated cyber-attacks [18].

The Cyberspace Policy Review, initiated by the White House, advised that “the Federal government should work with the private sector to define public-private partnership roles and responsibilities for the defense of privately owned critical infrastructure and key resources.” The review recommended that as “the United States deploys new Smart Grid technology, the Federal government must ensure that security standards are developed and adopted to avoid creating unexpected opportunities for adversaries to penetrate these systems or conduct large-scale attacks” [19].

1.3. Organization of Paper

This paper’s organization reflects the evolution of a series of activities. Section 1 introduces the subject domains of complex systems, and risk management, and introduces the current needs of the smart grid. Section 2 discusses the foundations of Cyber Security Econometrics (CSE) as a measure of Mean Failure Cost (MFC). Section 3 introduces the computational infrastructure that allows us to estimate the MFC using information about security requirements, system stakeholders and stakes, system architecture, and threat configurations. Section 4 provides an assessment of the capability of applying CSE to the Cyber Security Working Group (CSWG) five-step methodology. Section 5 applies CSE to the current series of cyber security related interfaces dealing with the Smart Grid and the Advanced Metering Infrastructure (AMI) as documented in NISTIR 7628 [20]. Finally Section 6 presents conclusions and Section 7 presents future research directions.

2. Cyberspace Security Econometrics System

Security metrics may be used as a basis for choosing security countermeasures and alternative security architectures that monitor and improve security in real-time during operation of the system. Characteristic qualities of an effective security metric should: (1) identify and measure properties necessary for decision making; (2) be measurable in a quantitative and repeatable way; (3) be supported by a system or process capable of accurate and repeatable measurement; and (4) be independently verifiable via an outside datum or reference.

Additional characteristics or qualities of effective security metrics or measurements: may be inexpensive, as a function of time and cost, to gather and determine; can be independently refereed or audited (in terms of compliance, accreditation and certification); and scalable between individual devices and computers to multiple devices and computers within an enterprise scale network.

Mean-Failure-Cost (MFC) embodies many of the characteristics of an effective security metric and may be utilized to quantify the impact of failures, interruptions, etc. as a function of failure cost per unit of time. Moreover, MFC may be used to determine and illustrate how much each stakeholder may stand to lose as a result of, for example, a security failure, a

1803
hardware failure or any other service disruption. MFC may be used within the framework provided by a Cyberspace Security Econometrics System (CSES) to design, implement and control a complex system.

The CSES provides many advantages over other known measurement/analysis systems or methodologies such as: (1) it reflects variances that exist between different users or stakeholders of the system [1]. Different stakeholders may attach different stakes to the same requirement or service (e.g., a service may be provided by an information technology system, cyber/physical, enterprise or process control system, etc.). (2) For a given stakeholder, CSES can highlight variances that may exist among the stakes attached to satisfying each requirement. For example, a stakeholder may attach or identify different stakes to satisfying different requirements within the overall system. (3) For a given compound specification (e.g., combination(s) of commercial off the shelf software and/or hardware), CSES can identify variances that may exist amongst the levels of verification and validation that are performed on components of the system (or specification). The verification activity may produce higher levels of assurance in satisfying some components of the specification.

The CSES follows a defined process [1]. The initial inputs (1) organizational mission (and components thereof), (2) value of its objectives and assets if uninterrupted, and (3) the components of the enterprise system that support each mission component, are determined by stakeholders.

The stakeholders, with assistance from subject matter experts, define the criteria of a quantitative value of an asset. For example, the criteria may include:

- Financial basis (e.g., operational cost of downtime per unit of time defined by hardware/software costs, facilities and staffing versus profit); which is the quantitative measurement to be used within the CSES.
- Stakeholder defined requirements; acceptable and unacceptable impact levels against the value related to information assurance tenets of confidentiality, availability and integrity may also be examined.

The CSES process includes three steps to derive the mitigation costs matrix [1]. CSES accounts for failure costs and verification (i.e., mitigation costs). CSES provides a:

- Framework for measuring the appropriate attributes that support the decisions necessary to (1) design security countermeasures, (2) choose between alternative security architectures, (3) respond to events such as intrusions or attacks and (4) improve security (including reliability and safety) during both design and operational phases.
- Comprehensive basis for choosing courses of action that have the highest risk reduction return on investment, i.e., reduce the most risks for the lowest cost.

With its focus on actual costs, its representation in terms of dollars per hours, and its focus on economic analysis, CSES is compatible with the spirit of Value Based Software Engineering [21]. CSES captures the different organizational mission needs for all stakeholders, including reliability and safety. CSES identifies information assurance controls and mitigation costs as an investment toward assuring mission success.

3. CSES: A Cascade of Linear Models – Stakes, Dependency, and Impact Matrices

In this section, we present the composition of the CSES model and motivate its application. From [1] we model our threat space. Specifically, the vector of mean failure costs (MFC, one entry per stakeholder) is given by the following equation:

\[ MFC = ST \ast PR, \]

where ST is the Stakes matrix and PR is the vector of requirement failure probabilities (one entry per requirement). The Stakes matrix is filled, row-by-row, by the corresponding stakeholders.

The vector of requirement failure probabilities is given by the following equation:

\[ PR = DP \ast PE, \]

where DP is the Dependency matrix and PE is the vector of component failure probabilities (one entry per component). Matrix DP can be derived by the system’s architect, in light of the role that each component of the architecture plays to achieve each security goal.

The vector of components failure probabilities is given by the following equation:

\[ PE = IM \ast PV, \]

where IM is the Impact matrix and PV is the vector of threat emergence probabilities (one entry by type of threat). Matrix IM can be derived by analyzing which threats affect which components, and assessing the likelihood of success of each threat, in light of natural
events or un-natural events (e.g., perpetrator behavior) and possible countermeasures.

By substitution of Equations 1, 2, and 3, we find the resulting equation gives us the vector of mean failure costs of all stakeholders as:

\[ \text{MFC} = \text{ST} \cdot \text{DP} \cdot \text{IM} \cdot \text{PV}. \]  

(4)

Utilizing a user interface, the Stakes matrix is filled by stakeholders according to the stakes they have in satisfying individual requirements; the Dependency matrix is filled in by the system architect (i.e., cyber security operations and system administrators) according to how each component contributes to meet each requirement; the Impact matrix is filled by analysts according to how each component is affected by each threat.

The remaining question is how to fill the vector \( \text{PV} \) that represents the probability of emergence of the various threats (natural or man-made) that are under consideration? This is done empirically, by simulating and/or operating the system for some length of time and estimating the number of threats that have emerged during that time and continue to be refined as the system evolves.

4. Application of the CSES to the Cyber Security Working Group (CSWG) Five-Step Methodology

Organizations typically use a risk management process to identify and mitigate risks to assure their organizational mission [9]. Risk management provides a documented, structured, and transparent process to identify critical resources, estimate threats and vulnerabilities (both natural and/or manmade) that may interact to cause harm (risks) to those resources. Moreover, the process estimates the likelihood of risk occurrence and evaluates tradeoffs among control measures used to mitigate the risks, and periodically revisits the analyses as needed.

The Smart Grid risk assessment process is based on existing risk assessment approaches developed by both the private and public sectors. It includes identifying assets, vulnerabilities, and threats and specifying potential impacts to produce an assessment of risk to the Smart Grid and to stakeholders and assets that make up the domains and subdomains, such as homes and businesses. Because the Smart Grid includes systems from the IT, telecommunications, and power system technology domains, the risk assessment process is applied to all three domains as they interact in the Smart Grid.

The following Sections 4.1-5 address each guideline methodology in detail (as excerpted from [22]), juxtaposed with the applicable concept within our defined CSE model for the smart grid.

4.1 Step 1: Selection of Use Cases with Cyber Security Considerations

Goal: Identification of Smart Grid use cases.

Description: Identification of Smart Grid use cases documents system interactions and behaviors that possibly occur during Smart Grid application scenarios.

Rationale: The use case set provides a common framework for performing the risk assessment, developing the logical reference model, and selecting and tailoring the high-level security requirements.

Outcome: This is a preliminary step, which provides initial input for assessing risk.

CSE Crosswalk: CSE provides this function by identifying the stakeholders’ mission requirements as related to their components and threat impact in a living document. As time goes on, the use cases may become cumbersome and unwieldy, yet the articulation of the relationship between the CSE matrices will remain stable.

4.2 Step 2: Performance of a Risk Assessment

Goal: Conducting the risk assessment on use cases.

Description: Risk assessment focuses on Smart Grid operations and not on systems used to run business operations.

Rationale: Each use case is reviewed from a high-level, overall functional perspective that includes identifying assets, vulnerabilities, threats and the specification of potential impacts.

Outcome: The output is used as the baseline for the selection of security requirements and the identification of gaps in guidance and standards related to the security requirements. Both bottom-up and top-down approaches were used in performing the risk assessment.

CSE Crosswalk: This step crosses the matrices developed with CSE, i.e., Stake, Dependency and Impact matrices. The existence with CSES allows for the Stakeholders, Architects, and Analysts to have input within their respective expertise and provides for the ongoing management of the results [1]. The NISTIR 7628 does not actually do this, but it does provide the data to populate the matrices. The bottom-up approach focuses on well-understood problems that need to be addressed, such as authenticating and authorizing users to substation intelligent electronic devices (IEDs), key management for meters, and intrusion detection for power equipment documented as respective Dependency and Impact matrices during
the Discovery and Evaluation phases [23]. In the top-down approach, logical interface diagrams developed for the six functional priority areas (Electric Transportation, Electric Storage, Wide Area Situational Awareness, Demand Response, Advanced Metering Infrastructure, and Distribution Grid Management) are to be dissected into the appropriate matrices.

4.3 Step 3: Setting Boundaries – The Beginnings of a Security Architecture


**Description:** The Smart Grid domain that is a high-level grouping of organizations, buildings, individuals, systems, devices, or other actors with similar objectives and relying on, or participating in, similar types of applications.

**Rationale:** This model focuses on a short-term view (one to three years) of the proposed Smart Grid and is only a sample representation. It can serve as a vehicle for identifying, organizing, prioritizing, and communicating security requirements and the security-related responsibilities of actors.

**Outcome:** The output of this analysis is a logical reference model that shows logical interfaces linking actors and suggests the types of information exchanged. The purpose of the logical reference model is to break down the Smart Grid and the domains into more granular detail, but not defining interface specifications and data types.

**CSE Crosswalk:** Referencing the CSES Foundations sections, the Stakes matrix identifies the Stakeholders with their representative missions (requirements). These requirements are further identified with their respective components to create the Dependency matrix by the Systems Architects [1]. This is an ongoing process that provides a foundation and reflects variances existing between different users or stakeholders of the system, their missions (requirements), components and threat vectors with mitigation consequences. The loss of confidentiality, integrity and availability impact levels can be mapped into the CSES and accounted for.

By using the CSES matrices, this layered approach to security should leverage existing power system capabilities that have been successful in assuring reliable supplies of power to consumers. Existing power system defenses and safeguards that protect against, or mitigate outages due to inadvertent actions and natural disasters may be used to address some of the cyber security requirements.

4.4 Step 4: High-Level Security Requirements

**Goal:** The development the high-level security requirements as applicable to the entire Smart Grid or to particular domains and interface categories.

**Description:** Determine the logical interface categories; Assess risk; and Select the initial set of baseline security requirements based on the logical interface categories.

**Rationale:** Organizations may use the CSWG’s set of high-level baseline requirements as they devise their cyber security strategies.

**Outcome:** Each of the high-level security requirements are assigned to one of three categories indicating where within an organization, operation, or function a particular requirement should be implemented.

**CSES Crosswalk:** CSES provides a similar definition for the requirements. However, the CSES is guided by stakeholders’ mission and thus the requirement can be mapped directly to an individual stakeholder. The nature of the Stakes and Dependency matrices allow for the natural grouping of the high level categories of (1) Governance, risk, and compliance (GRC) requirements, (2) Common technical requirements, and (3) Unique technical requirements, and expand on the logical interface categories, while providing the mechanism to conform to their naming conventions.

4.5 Step 5: Conformity Testing and Certification

**Goal:** Smart Grid Conformity Testing/Certification

**Description:** Smart Grid products are to be developed to conform to interoperability standards and undergo a rigorous conformity and interoperability testing process.

**Rationale:** In today’s standards environment, it is important to eliminate duplication of work activities related to Smart Grid standards as well as conformity testing.

**Outcome:** As a first step, this survey will address, in particular, conformity assessment programs assuring interoperability, cyber security, and other relevant characteristics.

**CSES Crosswalk:** CSES is designed to assist in risk management mitigation and guide the investment process. As such, it doesn’t address Step 5, except in a support role.

5. Real World Application Explained

The use of CSES for ranking a threat candidate may be obtained through a contextual semantic assessment. Contextual semantics may refer to the types of semantic information that may be inferred about words, objects, or concepts by the contexts the
concepts appear in, for example. A contextual semantics assessment engine may assess and in some instances automatically rate the meaning of a threat because threats or vulnerabilities that appear in the same context may share common contextual features. For example, a contextual assessment may weigh when a threat candidate develops or occurs. In a power distribution system, for example, a denial of service at a generator may result in a more significant threat (and therefore, may have a more significant effect) than if the denial of service occurred at single point of distribution (e.g., smart meter), because it may affect a larger population. A contextual semantic assessment would identify the denial of service and assess its effect.

Threat candidates may also be assessed through threat (e.g., failure) scenario (use of modeling to identify relevant threats or vulnerabilities) enumeration engines and predetermined criteria established by the defenders (e.g., the stakeholders) and known threat candidates. Historical records of known threats or vulnerabilities may also be used to identify the likelihood of a threat emerging just as factors that affect a machine’s performance and lifetime. This is shown by an assessment engine that recognizes that while each threat may be different, some share common features and manifestations when the threat materializes.

Utilizing the previous described matrices (Section 3), the stakes matrix is filled according to the predetermined stakes the stakeholders have in satisfying individual requirements; the Dependency matrix is filled (e.g., through a cyber-operation or through a processor) according to how each component contributes to meet each requirement; the impact matrix may be filled according to how each component is affected by each threat (e.g., a classical failure modes and effects analysis). Empirical data may be processed by a knowledge base engine and/or inference engine to fill the vector of threat emergence probabilities (PV) that represents the probability of emergence of the various threats or vulnerabilities that are under consideration. Empirical validation of the values of PV may occur by continually monitoring data sensors in relation to the assets at risk, countermeasures and concomitant impacts if compromised. This may result in a vector of mean failure costs of all stakeholders that may be represented from Equation 4.

The practicality and utility of the described systems and processes may be further shown when utilizing the documented interfaces from the NISTIR 7628. Following Title 44 of the U.S. Code [24], three security requirements are imposed upon the Advanced Metering Infrastructure (AMI) and Cryptographic Key Management Systems (CKMS), as follows:

- Confidentiality – ensure that only authorized parties are able to access cryptographic keys. A loss of confidentiality could result in unauthorized parties gaining access to any information that is protected by the key, including but not limited to personally identifiable information (PII) about a customer and customer energy usage data.
- Integrity – ensure that cryptographic keys are not altered by unauthorized parties. A failure of integrity may result in such consequences as power being shut off to a meter.
- Availability – ensure that cryptographic keys are available whenever needed. When availability is not met, possible consequences include power being shut off to a meter.

The Stakeholders for this Infrastructure Security example with the AMI and CKMS is based on [20] as follows:

- Public Power Utility,
- AMI Vendor,
- Cryptographic Key Management System (CKMS) Provider,
- Corporate Customer, and
- Residential Customer.

The monetary loss each stakeholder stands to lose upon violation of a given security requirement is documented as follows and is presented in summary form as Table 1.

For the stakeholders, the systems and/or processes identify:

- Public Power Utility – Given that there are 2,006 public utility companies in the United States and those companies serve a total of 20,940,561

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>No Req’t. Failure (NRF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utility</td>
<td>$762,044</td>
<td>$10,000</td>
<td>$10,000</td>
<td>$0</td>
</tr>
<tr>
<td>AMI Vendor</td>
<td>$762,044</td>
<td>$100,000</td>
<td>$5,000</td>
<td>$0</td>
</tr>
<tr>
<td>CKMS Provider</td>
<td>$762,044</td>
<td>$100,000</td>
<td>$200,000</td>
<td>$0</td>
</tr>
<tr>
<td>Corporate Customer</td>
<td>$31,140</td>
<td>$1,363</td>
<td>$1,363</td>
<td>$0</td>
</tr>
<tr>
<td>Residential Customer</td>
<td>$631</td>
<td>$3.82</td>
<td>$3.82</td>
<td>$0</td>
</tr>
</tbody>
</table>

Note: The NRF column represents the cost associated when no requirement fails and is provided for completeness (to explicitly denote this case).
customers, we take our example utility to have the average of 10,439 customers [25]. With respect to confidentiality, should the confidentiality requirement be violated, the utility stands to lose the cost required to mitigate the loss of customers’ personal information. The Ponemon Institute and Symantec report the direct cost of a data breach to be $73 per lost record in the 2010 Annual Study: U.S. Cost of a Data Breach [26]. With 10,439 customers, the utility then has a monetary loss of $762,044 with respect to confidentiality. With respect to Integrity and Availability each, we estimate that the loss to the utility per incident of outage is $10,000 on average.

- AMI Vendor – with respect to confidentiality the amount the AMI vendor stands to be liable for the same costs as the utility company; with respect to Integrity, we estimate that the stake of the AMI vendor in integrity is an order of magnitude greater than that of the utility; and with respect to availability, for the sake of the example, we estimate that the AMI vendor stands to lose $5,000 in the event of loss of availability.

- CKMS Provider – with respect to confidentiality, we estimate the same costs as the utility company; with respect to integrity, we estimate that the loss to the CKMS provider in integrity is an order of magnitude greater than that of the utility; and with respect to availability, we expect that the CKMS provider stands to lose the most with regard to availability (twice the amount of integrity), as it is responsible for creation and updating of keys.

- Customer (Corporate) – with respect to confidentiality, it is the loss of confidentiality that could result in corporate identity fraud. Card Protection Plan Group (CPPGroup Plc) reported in a 2011 white paper that small and medium companies in the UK who were victims of ID fraud lost an average of about £20,000 ($31,140) each [27]; with respect to integrity/availability, we suppose that a loss of integrity or availability could cause a power interruption for the customer. For a power outage of mean length, a commercial power customer’s average loss is $1,363, (value converted to 2012 dollars) [28].

- Customer (Residential) – with respect to confidentiality, the loss of confidentiality could result in theft of personally identifiable information (PII) and/or identity fraud amounting to an average Identity fraud cost to the consumers of about $631 [29]; with respect to integrity and availability, we suppose that a loss causes a power interruption for the customer. For a power outage of mean length, residential customers are expected to lose $3.82 (value converted to 2012 dollars) [28].

For purposes of this example for the components of the system, we take the Smart Grid Architecture Logical Interface Categories 13-18 relevant to AMI from the NISTIR 7628 [20] and summarize them in Table 2.

### Table 2: Advanced Metering Infrastructure related interfaces

<table>
<thead>
<tr>
<th>Component Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
</tr>
<tr>
<td>13</td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td>16</td>
</tr>
<tr>
<td>17</td>
</tr>
<tr>
<td>18</td>
</tr>
</tbody>
</table>

The dependency matrix (Table 3) assesses the architecture of the system in light of the role that each of the recited components of the architecture plays to achieve each security requirement. Whether a particular requirement is met or not may conceivably depend on which component of the system architecture is operational. In highly complex systems these operational components that play to achieve each system goal may be rolled up in a hierarchical process that may simplify the analysis and computations.

The resulting Dependency matrix is then populated as shown in Table 3. The qualitative ratings from NISTIR 7628 of High, Medium and Low were transposed to the numeric equivalent of 0.3, 0.2. and 0.1 respectively.

### Table 3: Dependency Matrix

<table>
<thead>
<tr>
<th>Requirements</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>.3</td>
<td>.3</td>
<td>.1</td>
<td>.3</td>
<td>.1</td>
<td>.1</td>
</tr>
<tr>
<td>I</td>
<td>.3</td>
<td>.3</td>
<td>.2</td>
<td>.2</td>
<td>.3</td>
<td>.3</td>
</tr>
<tr>
<td>A</td>
<td>.1</td>
<td>.3</td>
<td>.2</td>
<td>.1</td>
<td>.2</td>
<td>.1</td>
</tr>
<tr>
<td>NRF</td>
<td>.3</td>
<td>.1</td>
<td>.5</td>
<td>.4</td>
<td>.4</td>
<td>.5</td>
</tr>
</tbody>
</table>

Note: the NRF row represents the case when a component fails but does not affect the associated requirement. The NCF column represents the case when no component fails.

In determining the threats against the AMI system, we realized that a recognized group of individuals would be needed to validate the threats within this subject domain. The body that was selected was the National Electric Sector Cyber security Organization.
Resource (NESCOR). NESCOR is currently refining a
document that is the result from a collaborative effort
among the attendees of the NESCOR June 2011
workshop in held in Washington, D.C., where industry
experts, asset owners, and academia participated in the
NESCOR technical working group (TWG) 1. Additional
individuals are reviewing, revising and augmenting the
material produced at the June Workshop. The failure scenarios, impacts, and mitigation strategies were
developed from the “bottom-up,” rather than a top-down assessment of potential cyber
security events. The failure scenarios included in that
document are not intended to be a complete list of all possible failure scenarios [30]. Section 5.1 of the report
contains a set of failure scenarios in the domain of
AMI. From these scenarios, we extracted three specific
threats to the system, detailed below in Table 4. There
are, of course, many other potential threats to the
system, some of which are addressed in the NESCOR
report.

Table 4. Threat Description Details

<table>
<thead>
<tr>
<th>Threats</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMI-1</td>
<td>Wide use of same symmetric key</td>
</tr>
<tr>
<td>AMI-2</td>
<td>Creation of duplicate Access Point Name (APN)</td>
</tr>
<tr>
<td>AMI-3</td>
<td>Time-stamping falls out of sync</td>
</tr>
</tbody>
</table>

For the purposes of this example, we group all threats aside from the three below into the category ‘Other Threats,’ which we treat like a specific threat when filling out the IM Matrix. (For future reference, threat 1 stems from failure scenarios AMI.4 and AMI.5, threat 2 comes from AMI.17, and threat 3 comes from AMI.19 in the NESCOR document. There are a total of 29 AMI-related failure scenarios in the current version of the report, so there is strong potential for expanding our set of threats) [30].

Table 5. Impact Matrix

<table>
<thead>
<tr>
<th>Components</th>
<th>AMI-1</th>
<th>AMI-2</th>
<th>AMI-3</th>
<th>Other Threats</th>
<th>No Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>0</td>
<td>.3</td>
<td>.5</td>
<td>.1</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>.2</td>
<td>.3</td>
<td>.2</td>
<td>.1</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>.1</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>0</td>
<td>.2</td>
<td>.1</td>
<td>.1</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>0</td>
<td>.1</td>
<td>0</td>
<td>.1</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>.6</td>
<td>.1</td>
<td>.1</td>
<td>.1</td>
<td>0</td>
</tr>
<tr>
<td>NCF</td>
<td>.2</td>
<td>0</td>
<td>.1</td>
<td>.4</td>
<td>1</td>
</tr>
</tbody>
</table>

Note: the NCF row represents the case when a threat materializes but does not affect the associated component. The No Threat column represents the case when no threat materializes.

Using the details of the NESCOR failure scenarios and the NISTIR interface categories, we were able to gain a sense of how the three threats would likely affect the infrastructure. Further revision of the IM Matrix (Table 5) is undoubtedly necessary as failure scenarios are simulated and studied.

The impact matrix (Table 5) specifies the catalog of threats or vulnerabilities that may have been experienced at the AMI system. In this example, it comprises a subset of the AMI system. Table 5 also illustrates the probability of emergence of a subset of threats during operation. In some ways, the impact matrix represents a fault model that catalogs the threats or vulnerabilities that the AMI faces.

<table>
<thead>
<tr>
<th>Threat Vector (PV)</th>
<th>Probability of threat materializing during a day</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMI-1</td>
<td>0.005</td>
</tr>
<tr>
<td>AMI-2</td>
<td>0.005</td>
</tr>
<tr>
<td>AMI-3</td>
<td>0.03</td>
</tr>
<tr>
<td>Other Threats</td>
<td>0.16</td>
</tr>
<tr>
<td>No Threats</td>
<td>0.8</td>
</tr>
</tbody>
</table>

During our recent review of the 29 AMI-related failure scenarios, we do agree with the NESCOR TWG1 that information about potential cyber security failure scenarios is intended to be useful to utilities for risk assessment, planning, procurement, training, tabletop exercises and security testing. A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power. In our particular example we have concentrated on the AMI sub-domain.

Table 6. Probability Threat Vector

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Mean Failure Cost</th>
<th>Cost per day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utility</td>
<td>$22,368</td>
<td></td>
</tr>
<tr>
<td>AMI Vendor</td>
<td>$25,501</td>
<td></td>
</tr>
<tr>
<td>CKMS Provider</td>
<td>$29,664</td>
<td></td>
</tr>
<tr>
<td>Corporate Customer</td>
<td>$969</td>
<td></td>
</tr>
<tr>
<td>Residential Customer</td>
<td>$18.27</td>
<td></td>
</tr>
</tbody>
</table>

No threat materializing during a day is probably most likely as shown in Table 6. Since there are far more than three threats contained within ‘Other Threats,’ it is second most likely that one of these unspecified threats manifests. As the smart grid and AMI mature, the population of the Threat Vector will use empirical results to verify and validate these probabilities.

The Mean Failure Cost (MFC) is calculated by applying Equation 4 and results in the vector of MFC (one entry per stakeholder) developed by the systematic substitution of the successful analysis of the stakeholder’s requirements, components, and threats...
that cause failures, if and when they materialize and the MFC is shown in Table 7.

The MFC is in units of currency per time frame, e.g. dollars per day. The MFC gives stakeholders an estimate of their mean loss per unit time. Stakeholders can use the MFC to determine which security measures are worth implementing in their system and which are more expensive to implement than what the stakeholder stands to gain (by reducing his loss by means of the security measure).

6. Conclusions

As the nation continues to transform the electric power infrastructure, new risks and threats will evolve both natural and man-made. The three-volume report, NISTIR 7628 Guidelines for Smart Grid Cyber Security [20], presents an actionable initial analytical framework that organizations can gain insight and use to develop effective cyber security strategies and solutions tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities [22]. In this paper we addressed the application of the Cyberspace Security Econometrics System (CSES) specifically to the NISTIR 7628 in this context of the Smart Grid AMI components.

The Stakes matrix (Table 1) identifies the cost in US Dollars of how much the stakeholder stands to lose if the requirement (e.g., confidentiality, integrity and availability) is violated. In insurance terms, if someone is insuring their home, ST contains the value of their home (or the damage caused to their home by a hurricane, a flood, and earthquake and a fire) and MFC contains the yearly premium for their home insurance (according to the likelihood of each one of these calamities in a given year). The Dependency matrix represents how the requirements are dependent upon the proper operation of individual components of the overall AMI system with its interfaces. The Impact matrix relates component failures to threats. It represents the probability of failure of components given that a specific threat has materialized. While this example is illustrative of the technique of using CSES to understand the mean failure cost of a loss that may have been experienced within the context of AMI infrastructure, it is not, nor is it intended to be exhaustive. As shown, the Stakes matrix (Table 1) quantifies the variable in terms of financial loss, and represents the loss of service that the stakeholder may have experienced as a result of the failure. In Equation 4, the Stakes matrix (ST) is in dollars and PV is in 1/day, hence MFC is in $/day. We mapped the Stake, Dependency, and Impact matrices and the MFC described herein to the parameters set forth in NISTIR 7628 [20] and the NESCOR TWG1 Electric Sector Failure Scenarios and Impact Analysis Draft [30]. Further work in this area is ongoing by many respected experts. Their work will be the cornerstone for the asset owners to address risk management, risk assessment, planning, procurement, training, tabletop exercises and security testing. CSES as a decision support tool will aid in this endeavor, since a cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power. In our particular example we have concentrated on the AMI sub-domain.

7. Future Research

In the future, we plan to conduct a detailed analysis of failure scenarios and their associated impacts using the CSES approach that clearly delineates risk as a function of threat, vulnerability and consequence. The example described here only accounts for a small number of stakeholders, interfaces (components) and failure scenarios. There are currently 29 failure scenarios in [30] that need to be fully addressed, as well as additional requirements (e.g., no unauthorized access), and other functional requirements that are at risk (e.g., sustained operations), and interfaces (e.g., components among the other smart grid categories (e.g., control systems) of which there are 22 defined in NISTIR 7628 [20]. Our future analysis needs to comprehend the established electronic delivery systems threat models, detailed failure scenarios used by utilities, criteria and methods for prioritization of the failure scenarios. We also want to investigate threat mitigations, active defenders’ responses and courses of action.

8. References


