Journal of Energy and Power Engineering 9 (2015) 199-213
doi: 10.17265/1934-8975/2015.02.010

Smart Meter Deployment Threat and Vulnerability Analysis and Response

Steven Dougherty[1] and Takaki Saitoh[2]

1. Cyber Security Architect, Energy & Utilities Global Center of Competency Global Business Services, Sacramento 95814, California, USA

2. Registered Management Consultant, Registered Professional Engineer Global Technology Services, Osaka 5340000, Japan

Received: November 04, 2014 / Accepted: December 02, 2014 / Published: February 28, 2015.

Abstract: Advanced intelligent or "smart" meters are being deployed in Asia. A result of deployment of smart meters, with associated equipment, is the electric power industry faced with new and changing threats, vulnerabilities and re-evaluate traditional approaches to cyber security. Protection against emerging cyber-security threats targeting smart meter infrastructures will increase risk to both the utility and customer if not addressed within initial rollouts. This paper will discuss the issues in SMI (smart meter infrastructures) deployments that pertain to cyber security. It will cover topics such as the threats to operations, infrastructure, network and people and organization and their associated risks. SMI deployments include not only the smart meter, but also the interfaces for home energy management systems as well as communication interfaces back to the utility. Utilities must recognize and anticipate the new threat landscape that can attack and compromise the meter and the associated field network collectors. They must also include threats to the WAN (wide-area-network) backhaul networks, smart meter headends, MDMS (meter data management systems) and their interfaces to CIS (customer information systems) and billing and OMS (outage management systems). Lessons learned from SMI implementations from North America, Europe and recently, Japan, will be discussed. How white-box and black-box testing techniques are applied to determine the threat impact to the SMI. Finally, organizational change risk will be discussed and how utilities have responded to re-organizing and developing a security governance structure for the SMI and other smart grid applications.

Key words: Smart meter infrastructure, cyber security, risk assessment, threat analysis, meter vulnerability, security operation center, privacy.

1. Introduction

As utilities in Asia rollout their SMI (smart meter infrastructures), the majority of benefits from SMI will be realized through the expanding capabilities of meter data management systems, as well as through functionality tied to specific SMI vendors at or above the head-end. Globally, several progressive utilities have begun to adopt true enterprise solutions which incorporate SMI data in conjunction of other data sources which will extract the most value from the adoption of new sensors and monitor devices, including the smart meters through subsequent grid modernization initiatives. With this further integration of SMI with the utility grid and information technology infrastructure, threats from cyber security incidents will have greater impact to a utility. Integration of SMI into the operation technology and information technology infrastructures expands and creates new threat vectors to reliability, safety, data integrity and customer privacy.

In the first wave of early SMI adopters, much work went into the initial architectures of SMI to protect from threats of regional disconnects by rouge hackers, prorogating worms and malware. Many of these new threats made the new wires and brought the attention of the regulators. Public and regulatory concerns for privacy protection over security brought encryption

Corresponding author: Steven Dougherty, architect, research fields: security & privacy (architectures and strategies and governance), risk and compliance for smart grid and AMI infrastructures. E-mail: sdougherty@us.ibm.com.

technologies into the field networks establishing secure channels for key exchange, secured meter control command and configuration. Utilities and the vendor community sought standardized approaches for efficient means of secure AMI (advanced meter infrastructure). Pioneering work in 2009 by the UCAIUG (Utilities Communication Architecture I International User Group) AMI-Sec Task Force [1] with Southern California Edison created a body of work on AMI Security Requirements and AMI Security Profile that was previously not available to the industry.

The work of the AMI-Sec Task Force was later adopted and incorporated into the United States NIST (national institute for standards and technology) NIST Internal Report (IR) 7628 guidelines for smart grid cyber security [2] as the major contributor to smart meter security. The work of the NISTIR was a collaboration of government, academics, industry, legal, and industry and technology vendors and consultants with Version 2 in development. Since the NISTIR, other utility specific standards have emerged addressing smart grid and smart meters including: the ENISA (european network and information security agency's) Smart Grid Recommendations for Europe and Member States [3] July 2012 and the ISA (International Society of Automation) with the the IEC (International Electrotechnical Commission) is producing the multi-standard ISA/IEC 62443 series for industrial controls cyber security [4]. The NERC (North American Electric Reliability Corporation) has established regulatory standards subject to audits and fines for violations protecting the North American bulk electric system for Canada, United States and parts of Mexico. NERC's CIP (critical infrastructure protection) [5] standards are specifically tailored for securing the grid leveraging recommended information security controls from NIST SP 800-53 [6] and ISO/IEC 27002 [7]. Current SMI deployments in North America are not impacted by NERC CIP but as autonomous load control systems become integrated with large SMI deployments, it is believed they will become NERC CIP regulated. Lastly, the standard and organization most recognized for information security, the ISO/IEC (International Organization for Standardization/International Electrotechnical Commission), released Technical Report 27019 Information Technology—security techniques—Information Security Management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry [8] in July 2013. ISO/IEC 27019 provides guidance for security management techniques for digital metering and measurement devices, e.g., for measuring energy consumption, generation or emission values.

It was once considered that standards should be constant and avoid revisions and updates due to the adoption process of the standard body and the investment by companies pursuing standard certification. Cyber security threats continually evolve, morph, and propagate as seen by the security community cross industries. Social media has accelerated the propagation of cyber security threats, their targets, and exploit techniques. Attempting to find the right framework and approach with constant changing threats has motivated the standards bodies to revise their standards with many accepting public comment on the revisions. A good case in point is the work with NERC CIP.

2. Applying Risk Management Models

NERC CIP was originally an "Urgent Action" item by NERC and its member utilities to address gaps and practices across the industry for cyber security. A team of volunteer member utility employees and industry consultants crafted the first versions and the focus was on asset identification and protection. Many utilities found ways to avoid CIP regulation by exempting their assets from the requirements with interpretations such as "the use of non-routable protocols". The results of NERC's self-certification request showed that only 29% of responding

generation owners and operators identified at least one critical asset, while about 63% of the responding transmission owners identified at least one critical asset. NERC expressed its concern with these results in a letter to industry stakeholders dated April 7, 2009 [9]. The industry was too focused on compliance and avoided the hard facts of cyber risk exposure to their systems. These situations lead many a utility executive to ask, "We are NERC CIP compliant, but are we really secure?".

Luckily for those living in North America, NERC and its member utilities have recognized current and past CIP versions have flaws. The emphasis was on asset identification and protection instead of a classic threat and impact approach to information systems. Realizing this gap, a risk impact approach has been adopted for Version 5 that will take effect in North America, April 1, 2016. Version 5 of NERC CIP addresses critical systems and their components in terms of high, medium and low impact to the grid.

The NERC CIP experience is a good lesson learned for SMI projects. A threat based risk and impact approach has been considered a best practice for security. ISO/IEC 27019 [8] summarizes this approach with: "It is essential that energy utility organization identify their security requirements". There are three main sources of security requirements:

(1) The results of an organization's risk assessment, taking into account the organization's general business strategies and objectives. Through a risk assessment, threats to the organization's own assets will be identified; vulnerabilities and likelihood of occurrence will be evaluated and potential impact estimated;

(2) The requirements which result from legislation and bye-laws, regulations and contracts which have to be fulfilled by an organization, and sociocultural requirements. Particular examples include safeguarding a reliable, effective and secure energy supply as well as the reliable fulfillment of the requirements of a deregulated energy market, in particular the reliable and secure transfer of data with third parties;

(3) The specific principles, objectives and business requirements placed on information processing, which were developed by the organization for supporting its business operations.

4.2.4.2 Assessing Security Risks

The necessary security measures or controls are determined by the methodical assessment of security risks. The cost of controls has to be balanced against the economic losses that may be incurred due to security issues. The results of the risk assessment facilitate the definition of adequate management actions and priorities for the management of information security risks as well as the implementation of the controls chosen to protect against these risks. The risk assessment should be repeated periodically in order to take all changes into account, which could affect the results assessed.

Following this guidance from ISO/IEC 27019, utilities must fully understand the threat landscape that they are operating within. A threat model that takes in consideration cyber security threats at the operations level, infrastructure level, network level and also human and organizational level. Cyber security threats are constantly evolving and adopting as illustrated by a recent incident, "Unable to breach the computer network at a big oil company, hackers infected with malware the online menu of a Chinese restaurant that was popular with employees. When the workers browsed the menu, they inadvertently downloaded code that gave the attackers a foothold in the business's vast computer network [10]". This exploit operated at multiple threat vectors targeting human/organizational vulnerabilities, infrastructure vulnerabilities and operational vulnerabilities.

A classic computer security observation that was made 15 years is so relevant regarding today's approach by the industry in applying security models. A valuable lesson learned will be gain by appreciating Dorothy E. Denning's, "The Limits of Formal Security Models", October 1999 National

Computer Systems Security Award Acceptance Speech [11]. Denning stated, "The lesson I learned was that security models and formal methods do not establish security. They only establish security with respect to a model, which by its very nature is extremely simplistic compared to the system that is being deployed, and is based on assumptions that represent current thinking. Even if a system is secure according to a model, the common (and successful) attacks are the ones that violate the model's assumption. Over the years, I have seen system after system defeated by people who thought of something new". To summarize Denning, "Systems are hacked outside the security model's assumptions".

IBM (international business machines) created a SMI threat registry to access SMI security requirements and designs with some of the initial SMI deployments in North America. The initial threat registry used 25 threat scenarios to test requirements and designs. As more and more attacks against the energy industry grew over the years, so did the IBM threat registry. These threats were outside current utility security models assumptions of the threat type, their target, motivation and how persistent they were. The energy security models did not address lateral penetration movement of the threats and the internal reconnaissance they conducted. Our most recent application of the threat registry used in Asia contained over 70 SMI [12] threats that a utility assessed against.

Japan's METI (Ministry of Economy, Trade and Industry) has recognized this issue by addressing it through their "Promotion of Information Security Countermeasures on the Fields of Power and Energy". We believe METI is correct in assuming that the Japanese power system information security will apply an international/industrial standard multi-purpose technology on the power supply regulations system. METI is developing a model for the power supply regulation system to prepare for unknown and inexperienced IT attacks [13]. METI's goal is the development of a model system that leads to an implementation of a security rating system and research on the effect of multi-purpose regulation system by the security countermeasures. We strongly encourage METI to include the evaluation and measurements of the use of mature, repeatable and continuous use of threat and risk management practices within their security model rating system.

As new and existing SMI projects emerge, we propose the use of threat models which simulate known and hypothetical attacks outside current models based on our recent experience in Asia, North America and Europe. We have found that the use of threat model enables the prioritizing of requirements and control designs through the use of threat impact and likelihood ratings. This approach creates a baseline to measure against and encourages the refresh of high risk threat evaluations annually whenever a new threat is discovered or when new or existing information systems undergo significant change.

3. When to Model

The SMI threat registry has over 70 threats categorized as operations threat, infrastructure threat, network threat and people/organization threat. Each threat was further categorized into a specific family or domain threat. They are:

- Administration threats;
- Audit threats;
- Cryptographic threats;
- Eavesdropping threats;
- Flawed implementation threats;
- Governance threats;
- Identification and authentication threats;
- Information system threats;
- Insider threats;
- Malicious code threats;
- Network threats;
- Operational threats;
- Physical threats.

Due to the length of a smart meter rollout, we have

found threat modeling should be conducted during the full lifecycle of the implementation. While the threat modeling should be inclusive of the total threat library, this paper will focus on critical threats and control tests during the following phases:

- Security in the SMI design consideration phase;
- Security in the SMI procurement work stream;
- Security in the SMI integration phase;
- Secure operations for SMI go-live.

The SMI threat approach and methodology commences with an initial threat, vulnerability and impact assessment against the initial SMI designs. The SMI conceptual architecture design documentation assists in framing the approach and identifying stakeholders. It is highly recommended to have detailed logical architectural design documentation available as it provides a good understanding of the components that will be modeled against for threats and risk exposure. The more specific physical architectural design documentation is required for the later stages of the model, i.e., the procurement work stream and integration phase.

In design consideration phase, the threat modeling process is done with no control treatment of risk in order to establish a threat baseline and define security requirements. We have found that facilitating TRA (threat and risk assessment) workshop across business units, functions and stakeholders creates a viable model that has fewer tendencies to capture biases and assumptions which also creates buy-in from the participants of the output. Typical stakeholders and participants would include the chief information security officer and appropriate staff, SMI project manager, SMI project owner, customer relations, risk and financial controller, operations, maintenance and dispatch, system management administrators, network and telecom engineers, lead SMI architect, and SMI vendors.

Once the cross functional team has been put together, the TRA team is briefed on the approach, definitions and criteria for the TRA. Typical workshops used the following definitions of risk characteristics: the TRA team gains a deeper understanding across business functions on the types of threats and impacts that can affect SMI. Impact level will vary across companies, within companies and across countries due to their regulatory environments and business risk profile. We recommend the use of an impact scale that is currently in place and used by the utility executive risk committee. Typically, impact is captured as catastrophic or very high, major or high, moderate or medium, minor or low and insignificant or very low in terms of financial, organizational, legal and human impacts. Below is a sample enterprise risk impact definition.

Once the TRA workshop team has ranked the threat impact, the participants then examined the probability of occurrence by assessing the motive, means, and opportunity of a threat. Each threat scenario uses a discussion starter and use case identifying how a threat might be applied to the smart meter infrastructure. A combination of low or high rating of the threat's means, opportunity and motive determines the likelihood probability of the threat. We define them as:

- Means—the skills, capability, tools and resources of a threat;
- Opportunity—does the threat have physical access to an asset? Does the asset have public facing network connectivity? Does the threat have the opportunities and knowledge of a trusted employee or contractor? Does the threat have the opportunity to dialogue directly (verbal/virtual) with a trust employee or contractor?
- Motive—is the threat a hostile nation-state, political activist, disgruntled employee or a criminal enterprise.

Based on the combination of motive, means and opportunity, likelihood probability was categorized for each threat as:

Once the threat impact and likelihood are determined, the threats are placed on a heat map for risk treatment evaluation and cyber security strategy

Table 1 Risk characteristic definition.

Risk characteristics	Description
Impact	What would result if a threat/vulnerability combination were to occur or were exploited (impact of occurrence)
Likelihood	How likely is the threat/vulnerability combination to occur (probability of occurrence)

Table 2 Impact definition.

Impact description	Impact definition
Catastrophic/very high	Exercise of the vulnerability: (1) may result in the very high costly loss of major tangible assets or resources; (2) will significantly violate, harm, or impede an organization's mission, reputation, or interest; (3) a disaster with potential to lead to the collapse of the organization; (4) multiple loss of life; incident(s) result in the inability to operate in a traditional manner; (5) jail term of any length for a director or officer
Major/high	Exercise of the vulnerability: (1) may result in the high costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; (3) long-term negative media focus and sustained concerns raised by stakeholders; (4) a critical event which, with significant management effort, can be endured; (5) multiple life injuries/isolated loss of life; incident(s) result in significant conditions or restrictions of operations; (6) criminal lawsuit commenced against the organization and its officers/directors
Moderate/medium	Exercise of the vulnerability: (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; (3) short-term negative media focus and sustained concerns raised by stakeholders; (4) a significant event which can be managed under normal circumstances with moderate effort; (5) isolated serious injuries; incident (s) result in changes in conditions of operations; (6) criminal action threatened
Minor/low	Exercise of the vulnerability: (1) may result in the loss of some tangible assets or resources; (2) may noticeably affect an organization's mission, reputation, or interest; (3) negative trending in more than one press release or social medium; (4) some management effort is required to manage the impact of the event; (5) reportable incident; (6) civil action commenced
Insignificant/very low	Exercise of the vulnerability: (1) may result in the loss of some assets or resources; (2) may affect an organization's mission, reputation, or interest; (3) one negative exposure in press or social media; (4) impact of event can be absorbed through normal activity; (5) minor non-reportable incident; (6) legal action threatened

Table 3 Likelihood ratings.

Likelihood ratings			
Motive	Means	Opportunity	Likelihood
Low	Low	Low	Rare
Low	Low	High	Possible
Low	High	Low	Unlikely
Low	High	High	Likely
High	Low	Low	Possible
High	Low	High	Likely
High	High	Low	Likely
High	High	High	Almost certain

development for the smart meter infrastructure. Below is an illustration of an untreated control SMI threat and risk heat map. Each threat is identified with a specific threat number. For example, threat number 1, "A threat agent may attempt to disconnect a large number of meters", is referred to as "T1".

The SMI TRA likelihood and impact heat map enables the stakeholders of SMI projects the ability to define threat based requirements and prioritize security investments based risk based assumptions. A traditional SMI architecture design through vendor based reference architectures, on paper, may seem reasonable in its mission to deliver services while meeting basic security requirements. But, with such an approach, a security architect or engineer may miss significant vulnerabilities or not considering threats in the design. One must also be cognizant of the one to many factors of SMI threats and mitigation. One threat agent may have many SMI vectors to exploit and therefore, many requirements and mitigating controls for one threat.

Table 4 SMI threat and risk heat map.

Likelihood	Impact				
	Very low/insignificant	Low/minor	Medium/moderate	High/major	Very high/catastrophic
Almost certain	T24		T54, T55	T2,T4, T8, T38, T45,	
Likely	T56	T6, T12, T13, T14, T27, T34, T36, T49, T63, T66	T5, T10, T16, T17, T21, T37, T41, T43,T60, T62, T67, T70	T7, T11, T19, T20, T28, T29, T33, T39, T40, T46, T47, T48, T51, T52, T61	T1
Possible	T25	T9, T15, T31, T32, T64	T18, T44, T58, T65	T22, T23, T26, T50, T68, T69	
Unlikely		T3, T3, T57, T65	T53, T59		T42
Rare		T35			

4. Security in the SMI Design Consideration Phase

We have found the use of a SMI TRA likelihood and impact heat map in the design consideration phase a very useful tool in validating security design requirements. One of the significant threats to SMI is "A threat agent may attempt to disconnect a large number of meters". Examining motive, means and opportunity, the threat source would be external and target the components with the capability to disconnect a significantly large number of meters. Therefore, the components targeted by this threat would be the SMI head end and field area network collectors/data concentrators. The primary threat source is external with internal source as a secondary. The primary vulnerabilities to enabling this threat are operational/administrative commands and spoofing as secondary. The primary assets to be protected are operational commands and firmware.

Some examples of security design requirements the design should focus on to mitigate this threat are as follows:

- Automatic mechanisms must be established which reduce the possibility to break or throttle a large number of SMI points as a result of errors or targeted attacks. The system shall, by default, be set up so that the switch and throttle functionality are only done per unit. There shall be limits on the number of points, number of operations per unit time and disclosed if the functionality can be authorized and executed by one person alone;
- It should be possible to control the integrity of the software which is installed and executed on all of the units in the data concentrators so that unauthorized changes are detected and reported. Units should be able to verify that the updating of firmware is authorized and that the firmware is unmodified and approved before it is updated;
- Commands, measurement data and other sensitive information which is transferred in the SMI solution must be protected against unauthorized inspection, injection or changing. The system shall utilize the strongest encryption that is appropriate within technical solutions and capacity/response times;
- The head end and data concentration system shall have implemented mechanisms for mutual authentication and authorization of meters and other units in the SMI solution prior to establishing connection between the units and the rest of SMI.

Another significant threat to SMI is "Network provides insufficient security to provide data integrity". Examining motive, means and opportunity, the threat source would be external and target the overall SMI to disrupt data integrity. The primary threat source is external with internal source as a secondary. The primary vulnerabilities to enable this threat are network and eavesdropping. The primary asset to be protected is the overall SMI.

Some examples of security design requirements the design should focus on to mitigate this threat are as follows:

- SMI interfaces shall not accept unauthorised or erroneous communications and are capable of handling (dropping) such communication without adverse effects on the operation of the equipment or the interface;
- The communication solution shall be able to search for unknown and illegal units that have been connected to the network;
- Commands, measurement data and other sensitive information which is transferred in the SMI solution must be protected against unauthorized inspection, injection or changing. The system shall utilize the strongest encryption that is appropriate within technical solutions and capacity/response times;
- The data concentrator system must be designed so that it is not possible for outsiders to introduce, read, change or delete information in any points. The data concentration system shall be designed so that it is not possible for outsiders to access control functions without permission.

Threat testing in the SMI design consideration phase is typically done through architecture design document reviews, vendor tech sheets and interviews with the architects and project managers. The SMI TRA tester evaluates proposed security controls to mitigate the threat. The SMI TRA tester should also evaluate the utility and SMI project team's capability to implement and operate the threat controls at this phase. A SCMM (security capability maturity model) assessment is recommended. The capability maturity model we used was based on the Carnegie Mellon University, Software Engineering Institute CMMI (capability maturity model integration) model [14] while other models such as the recent US Dept. of Energy's C2M2 [15] model can be used. We planned on using the SCMM assessment levels to quantify the SMI threat and risk treatment at a later phase so we used the following SCMM levels for the assessment.

From our experience with other SMI and smart grid projects, the SCMM assessment reveals critical areas of immaturity in the capabilities to detect and respond to SMI threats. A common area of immaturity of SMI projects are situational awareness of security events from the field and wide area networks. The SCMM process enables the utility to define organizational capabilities and requirements to detect, respond and recover from SMI threats. Many of these capabilities are new to utilities and energy companies. Performing these processes during the SMI design consideration phase allows a utility to develop the required maturity levels to manage and mitigate threats and risks as the project progresses to "go live".

5. Security in the SMI Procurement Work Stream

Procuring technology solutions for SMI is a process within itself that can take years of preparation, drafting, and evaluating. RFIs (request for information), RFPs (request for proposal), technology bake-offs and technology trials are common practices for SMI. SMI TRA output provides valuable assistance to utilities in the procurement process. SMI TRA output defines RFP requirements and responses to address the utility's concern with managing high impact and likelihood threats. The SMI TRA ensures security is built-in, up front and not a costly afterthought.

While nearly all the SMI threats in the SMI threat registry can be used for RFP requirement and responses, we are illustrating four threats that are typically classified as major impact and likely. Three threats are operations threats and one is an infrastructure threat.

The threat "Security in the Application Design does not meet requirements" is a flawed implementation operations threat. Lack of comprehensive security requirements at the application level usually makes this threat "likely and major impact" during TRA workshops. Traceability to security requirements is critical for RFP response evaluation by the procurement team. The procurement team should ensure that vendor responses address this threat through a RFP response requirement asking the responding vendor to describe, in detail, a

Table 5 Capability maturity level, description and value.

Capability maturity level	Description	Capability maturity value
Does not exist	Controls or program does not exist	0.5
Ad Hoc	Reactive with sporadic or inconsistent communication of issues and approaches to address them	1.0
Repeatable	Processes, tools and metrics are limited, not documented or consistent across the organization	2.0
Defined	Standardized and documented practices and processes	3.0
Quantitatively managed	Similar to defined, but processes and measures established to measure effectiveness	4.0
Optimized	Metrics are used for strategic planning and optimization. Processes and measures exists for analysis	5.0

response to: "Security must be safeguarded in the whole value chain of the SMI. The system shall be designed so that it safeguards end to end security between Meter nodes and all application interfaces. All of the components must be included in the same minimum security requirement and security must be addressed at all levels, both during development and production. Please explain in detail how your solution mitigates the threat: Security in the Application Design does not meet requirements".

Another flawed implementation operations threat that is constantly rated as "likely and major" is "The HAN (home area network) interface provides inadequate security to ensure security of data". Privacy risk, exposure of customer data, legal and regulatory risk at the SMI HAN can raise the impact level from moderate to major depending upon the utility's privacy laws and regulations. The procurement team should ensure that vendor responses address this threat through a RFP response requirement asking the responding vendor to describe, in detail, a response to: "All external equipment which shall be connected to units in the SMI must be authenticated before connection is allowed. Authorization to the external equipment and the user of the equipment must be checked before the operations can be carried out. It must be possible to remove/change authorization of such external equipment from the Head End, possibly via integration from the CIS (customer information system). External equipment is considered to be the end customer's HAN equipment such as display or controlled units and hand-held field equipment which is used by, for example, fitters in connection with installations/service and maintenance tasks in the field. This applies to connections via all accessible interfaces, including optical ports. Please explain in detail how your solution mitigates the threat: 'The HAN (home area network) interface provides inadequate security to ensure security of data'. The supplier shall describe how authentication and authorization of all external equipment/external connections is done".

"A threat agent may try to obtain key material from a meter" is a cryptographic operations threat. Secure meter design is critical to prevent theft, fraud and tampering. Service and communication ports, circuit boards, and encryption keys must be physically protected with mechanisms to detect opening of covers, shielding or tampering. One may find many examples of utility meters being reversed engineered to determine what type of processing chips are in place, how can one extract information from the circuit boards and can one alter the programming on the boards. Tutorials [16] and videos are available on the Internet describing how to open up a meter as well as indicating where the tamper and encasing opening alarm sensors are. Any attack that retrieves meter firmware provides advantages to an attacker. By reverse-engineering the meter firmware, an attacker could discover the meter's communication protocols, authentication methods, and the system's default security keys. While all meter manufacturers provides security features that prevents external access to on-chip memories, many are not robust to prevent a highly skilled, hardware hacker with EEPROM reader

tools. A common method of protecting the firmware from device programmer read access is done in the firmware with a security bit set to deny access at the time of manufacturing. This security bit can be overriding with electronic tools. Academic researchers and hackers have published the ability to recover encryption keys used for authentication and confidentiality through these methods. Compromised keys, especially global symmetric keys can be lead to a very large geographic security breach.

The procurement team should ensure that vendor responses address this threat through a RFP response requirement asking the responding vendor to describe, in detail, a response to:

"Mutual authenticating and authorizing of units in the SMI solution and the exchange of keys for securing communication channels shall be done with the help of unique security certificates belonging to the individual unit and these shall be included in a PKI regime delivered by the Supplier and administrated by the utility. Key management, issuance, renewing and revoking of certificates and keys should be an integrated and scalable part of the system to be supplied. All locations in SMI where keys and certificates are stored must be protected. It must not be possible to obtain encryption keys from all components of the SMI including meter, communication modules, and collector/concentrator by bugging or memory extraction of internal bus. Please explain in detail how your solution mitigates the threat: 'A threat agent may try to obtain key material from a meter'. The supplier shall describe how the encryption keys and security certificates etc for the individual components are generated, distributed and updated during daily operations and administration, as well as procedures for issuing and revoking of certificates".

We have shared three examples of operational threats and how they can be used to frame a detailed vendor RFP response. Our last example for security in the SMI procurement work stream is an infrastructure Information systems threat. Web services are increasing in usage for industrial control systems. Due to this increase in use, the threat "A threat agent is able to exploit a vulnerability in web services to gain unauthorized access" is rated "likely and major impact" during SMI TRA workshops by those stakeholders who have knowledge of web vulnerabilities.

The most common web application security weakness is the failure to properly validate input coming from the client or environment before using it. This weakness leads to almost all of the major vulnerabilities in web applications [17], such as cross site scripting, SQL (Structured Query Language) injection, interpreter injection, locale/Unicode attacks, file system attacks, and buffer overflows. Data from an external entity or client should never be trusted, since it can be arbitrarily tampered with by an attacker. Web-based attacks such as SQL injection and XSS (cross-site scripting) are the results of poor application design data validation requirements. While most design-level security flaws are discovered and mitigated during the modeling and architecture phases, most development and delivery security issues are introduced because of poor input validation and output encoding. It is critical that any user-supplied data goes through the appropriate validations. For example, all input must be validated through a validation control.

The procurement team should ensure that vendor responses address this threat through a RFP response requirement asking the responding vendor to describe, in detail, a response to: "Web-based attacks such as SQL Injection and XSS (cross-site scripting) are the results of poor application design data validation requirements. Please identify all instances of applications within your solution that utilize web-based user interfaces. Please explain in detail how your solution mitigates the threat: 'A threat agent is able to exploit a vulnerability in web services to gain unauthorized access'. The supplier shall describe how the solution application supports server-side validation

of all form fields, data type, data length and character ranges".

Leveraging the output from a SMI TRA during the SMI procurement work stream phase ensures that security is built-in, up front by framing vendor responses to specific threats. If the vendor has difficulty in explaining how their solution mitigates the threat, the utility should ask for clarification and whether mitigation will be in future releases.

Many of these SMI security requirements are new to utilities and energy companies. Performing these processes during the SMI design consideration phase allows a utility to develop the required maturity levels to manage and mitigate threats and risk as the project progresses to "go live".

6. Security in the Integration Phase

Most utilities conduct their SMI TRA in integration phase of a SMI project. There are many work streams to be integrated at the network, system, component and application level. During the integration phase, there are test environments, systems and devices to conduct black-box and white-box penetration testing. In the previous stages, the assessment and testing are conducted against architectural designs. In the integration phase, there are physical devices, components to test against. In penetration testing for TRA, white-box testing [18] refers to a methodology where a white hat hacker has full knowledge of the system being attacked. The goal of a white-box penetration test is to simulate a malicious insider who has knowledge of and possibly basic credentials for the target system. Black-box testing [19] refers to a methodology where an ethical hacker has no knowledge of the system being attacked. The goal of a black-box penetration test is to simulate an external hacking or cyber warfare attack. White-box and black-box testing have different purposes but they use identical tools and techniques.

The scope of white-box and black-box testing includes the smart meter, HEM (home energy management) devices, RF (radio frequency) mesh networks, PLC (power line carrier) networks, cellular networks, concentrators/collectors, back-haul WAN (wide area network) networks, MDMS (meter data management systems), and support and operations subnets that perform systems management infrastructure and monitoring. Firewalls, network switches and routers, and host systems that are potentially managed by workstations that reside within the utility's internal corporate network are in scope. Also in scope are general business internal networks containing file and Active Directory servers as well as administrative workstations. Hosts and services are manually reviewed by white-box testing to identify known vulnerability and potential attack avenues that an insider would have access to.

Tools used by the white-box and black-box testing include:

- portmapping tools such as NMAP will be used to discover active IP addresses and listening network services (TCP, UDP, and ICMP);
- SNMP sweeping tools, such as snmpsweep and snmpwalk will be used to detect SNMP services and any information about systems and devices provided by SNMP;
- general network vulnerability scanning performed using Nessus professional or Rapid 7 with custom policy based on what services and system types were discovered during the IP discovery. Disable password guessing checks on potential account lockout settings known or discovered. Black-box attacks will use the denial of service attack option;
- web based tools such as AppScan and Nikto are used to test any HTTP (web) based services discovered;
- database scanning tools such as Guardium or Appsec are used to assess any discovered databases running Oracle, DB2, Informix, MySQL or MSSQL;
- metasploit and fuzzing exploitation frameworks are also used.

Both white-box and block-box techniques will employ network traversal techniques as network and system access is gained to test access to protected network segments that may only be accessible from compromised systems.

It is important to note that a threat may be both external and internal, but cyber incident history has revealed that insider attacks have had the greatest impact on systems. We have 27 threats out of 70 that are internal threat as primary. The following are examples from the SMI threat registry that have internal threat as primary and were tested through white-box testing:

- "Inadequate network segregation/network"—test through portmapping, SNMP sweep and general network vulnerability scanning tools;
- "A threat agent reads SMI audit logs when it does not have authorization to read any audit logs or modifies/deletes SMI audit logs to hide other actions/audit"—test through database audit tools;
- "A threat agent leverages management software to access unauthorized data or take control of an application/infrastructure"—test through system management role base authentication and authorization review;
- "A threat agent may attack the system using test development software or other field tools/operations" —test through development and service tools role base authentication and authorization review.

Black-box testing simulates the attacks that an external threat would apply to the smart meter infrastructure. The extension of the SMI networks to the field and their components provides an attacker many more points of presence to attack via logically or physical. We have 43 threats out of 70 that are external threat as primary. The following are examples from the SMI threat registry that have external threat as primary and were tested through black-box testing:

- A threat agent may try to obtain key material from a meter/crypto—test through bus snooping exploitation tool (Bus Pirate) [20];
- A threat agent is able to inject date between a meter and collector/malicious code—test through hacking exploitation tool (KillerBee) [21];
- "A privileged SMI administrator or engineer work station is compromised through a spearphishing attack/administrative"—test through simulated spearphising email to privileged administrators for security awareness response.

When conducting the TRA white-box and black-box testing in the integration phase, the testing should be done via test and pilot environments. We have seen this conducted at the utility's test and demonstration locations as well as on vendor's test and demonstration locations. The SMI TRA white-box and black-box testing results should then be re-assessed against the SMI TRA Likelihood and Impact heat map to establish a "Control Treated SMI TRA Heat Map".

Once a "Control Treated SMI TRA Heat Map" is established by the white-box and black-box testing, the SMI threat model can now be quantified into a Risk Index based on the utility's SCMM assessment score to detect, respond and recover. The following quantified heat map illustrates the values assigned to each quadrant.

With the SCMM ranking determined for each threat, a quantified score and ranking is established to evaluate the risk treatment of likelihood and impact for each threat. For example, for a threat with a likely/high impact ranking of 56.25 divided by the Capability Maturity Value of Level 3 maturity, the risk index score would be treated to "18.75" low/minor. For a threat with an almost certain/very high impact ranking of 100 with a capability maturity value of level 5 (does not exist), the risk index score would be treated to "200" very high/catastrophic.

Each threat is then quantified with a risk index score by using the below scale: we have found that by establishing a SMI threat and risk index score, utilities are better able to under their risk exposure to SMI threats. We highly recommend the following ISO/IEC 27019 [8] recommendation, "The risk assessment

Table 6 Quantified threat heat man.

Likelihood	Impact				
	Very low/insignificant	Low/minor	Medium/moderate	High/major	Very high/catastrophic
Almost certain (1.0)	10 × 1 = 10	25 × 1 = 25	50 × 1 = 50	75 × 1 = 75	100 × 1 = 100
Likely (0.75)	10 × 0.75 = 7.5	25 × 0.75 = 18.75	50 × 0.75 = 37.5	75 × 0.75 = 56.25	100 × 0.75 = 75
Possible (0.50)	10 × 0.5 = 5	25 × 0.50 = 12.5	50 × 0.50 = 25	75 × 0.50 = 37.5	100 × 0.50 = 50
Unlikely (0.25)	10 × 0.25 = 2.5	25 × 0.25 = 6.25	50 × 0.25 = 12.5	75 × 0.25 = 18.75	100 × 0.25 = 25
Rare (0.10)	10 × 0.1 = 1	25 × 0.1 = 2.5	50 × 0.1 = 5	75 × 0.1 = 7.5	100 × 0.1 = 10

Table 7 Threat risk index scores.

Ranking	Score range
Very high/catastrophic	151-250
High/major	75-150
Medium/moderate	35-74
Low/minor	10-34
Very low/insignificant	1-9

should be repeated periodically in order to take all changes into account, which could affect the results assessed" combined with a SCMM to continually assess security capabilities and not just threats and risks.

7. Secure Operations for Go-Live

Once a SMI project goes into production and is live, utilities face the challenge of maintaining the security posture through the capabilities to detect, respond and recover from a threat. As stated earlier in the security in the design phase, a common area of immaturity SMI projects are situational awareness of security events from the meter to the head end.

Many of these capabilities are new to utilities and energy companies and are actual threats as they lack the governance model, the policies and staffing to maintain a secure SMI. We have 8 threats out of 70 that are governance and organizational. The following are examples of people and organizational threats from the SMI threat registry:

- Insufficient trained security personnel assigned to SMI project and operations/administrative;
- Lack of information security policies and procedures pertaining to SMI/governance;
- Personal and protected identifiable information is collected, transmitted and stored by the SMI infrastructure/governance;
- Lack of SMI cyber security and privacy governance model/governance.

Recognizing the organizational threats with SMI, a common best practice we have seen is to develop a cyber security strategy and roadmap to mature the utility's capability to detect, respond and recover from SMI threats. In addition to the development of governance, policies, procedures and staffing expertise, utilities are including SMI SOCs (Security Operation Centers) and CSIRTs (Cyber Security Incidence Response Teams) within their strategy and roadmap plans.

North American utilities with operating SMIs are establishing dedicated SMI SOCs to provide protection, deterrence, prevention, detection, reaction and recovery security services as a critical cyber security defence. The SOCs monitor SMI security source data and have security information event correlation of such reported events. The correlation is processed in a SIEM (Security Information and Event Management) application. The SOC should also be coupled with any SMI network and WAN NOC (Network Operation Center) to share event notification.

Several utilities in the USA and Canada have either

created or expanded on the concept of integrated NOC/SOC within their organizations. Some models include outsourced NOC/SOC through a WAN/telecom provider and a sourced managed security operation service. The NOC/SOC could also include the network monitoring service of a SMI RF mesh provider. The utility SMI SOC will have a SIEM data feed to the RF NOC, WAN NOC, Control Center and critical substations with the capability for mutual support in case of an incident, cyber or otherwise.

Staffing usually includes operations analyst(s) with 7 × 24 cover, system engineers, and incident analyst. To ensure sufficient staffing a number of items should be considered. The number and types of devices to be monitored, reoccurring tasks conducted by the monitoring team, and the amount of interaction with other teams needs to be accounted for. One must determine average number of events generated, investigated and escalated which affect staffing capacity. Evolving technologies can also have a substantial impact on staffing capacity. Some utilities that have major critical infrastructures within their service areas (military bases, major commerce zones-ports, financial centres) have expanded their SOC staffing to include: intel analyst, event analyst, vulnerability analyst, optimization analyst and forensic analyst. We have seen several utilities use NIST's Special Publication 800-61 rev2 [22] "Computer Security Incident Handling Guide" to model their CIRST (Computer Incident Response Security Team) and SOC staffing and job requirement descriptions to respond to the SMI threat "Insufficient trained security personnel assigned to SMI project and operations".

8. Conclusion

End-to-end threat and risk analysis with security testing should be performed during the entire SMI deployment lifecycle. Especially prior to go-live and then determined in frequency by threat and risk assessment for present and future testing. We recommend this type of assessment and security maturity capability assessment on an annual basis or after any major system upgrades or changes. Active vulnerability scanning should be performed on non-production systems and devices that are installed and configured for actual operation in testing or staging environments. The closer the testing and staging environments are to production, the more accurate the end-to-end security testing will be. The smart meter infrastructure systems to be tested should be configured for normal, expected operation. This should include all components from the HEM to the meter, SMI network, WAN, the head end, MDMS and up into the customer information systems.

References

[1] AMI Sec Task Force, OpenSG Users Group. 2014. "UCAIug: This Task Force Is Charged with Developing Security Guidelines, Recommendations, and Best Practices for AMI System Elements." Utility Contractor Association International user group. Accessed September 1, 2014. http://osgug.ucaiug.org/utilisec/amisec/default.aspx.

[2] NISTIR (National Institute of Standards & Technology Internal Report) 7628. 2014. "Guidelines for Smart Grid Cyber Security." Accessed September 1, 2014. http://csrc.nist.gov/publications/PubsDrafts.html.

[3] ENISA (European Network and Information Security Agency). Smart Grid Recommendations for Europe and Member States. 2014. "This Study Makes 10 Recommendations to the Public and Private Sector Involved in the Definition and Implementation of Smart Grids." European Network and Information Security Agency. Accessed September 1, 2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations.

[4] ISA/IEC (International Society of Automation/International Electrotechnical Commission) 62443. 2014. "Security for Industrial Automation and Control Systems." International Society of Automation/International Electrotechnical Commission. Accessed September 1, 2014. http://isa99.isa.org/ISA99%20Wiki/Home.aspx.

[5] NERC (North American Electric Reliability Corporation). 2014. "(North American Electric Reliability Corporation) Critical Infrastructure Protection Standards (CIP 001 thru

CIP 011).” Accessed September 1, 2014. http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[6] National Institute of Standards and Technology Special Publication 800-53 (NIST SP 800-53) Recommended. 2014. “Security Controls for Federal Information Systems.” Accessed September 1, 2014. http://www.nist.org/nist_plugins/content/content.php?content.18.

[7] ISO/IEC (International Organization for Standardization/International Electroctechnical Commission) 27002. 2014. “Information Technology—Security Techniques — Code of Practice for Information Security Controls.” Accessed September 1, 2014. http://www.iso27001security.com/html/27002.html.

[8] ISO/IEC TR 27019. 2014. “Information Technology—Security Techniques—Information Security Management Guidelines Based on ISO/IEC 27002 for Process Control Systems Specific to the Energy Utility Industry.” Accessed September 1, 2014. http://www.iso.org/iso/catalogue_detail.htm?csnumber=43759.

[9] US Senate Report 112-34. 2014. “Grid Cyber Security Act.” Accessed September 1, 2014. http://thomas.loc.gov/cgi-bin/cpquery/?&sid=cp112QuAhF&r_n=sr034.112&dbname=cp112&&sel=TOC_50340&.

[10] Nicole Perlroth. New York Times. 2014. “Hackers Lurking in Vents and Soda Machines.” Accessed September 1, 2014. http://www.nytimes.com/2014/04/08 /technology/the-spy-in-the-soda-machine.html?_r=0.

[11] Denning, D. E. 1999. “The Limits of Formal Security Models. National Computer Systems. Security Award Acceptance Speech.” Accessed September 1, 2014. http://faculty.nps.edu/dedennin/publications/National%20Computer%20Systems%20Security%20Award%20Speech.htm.

[12] Smart Grid Security: Threats, Vulnerabilities and Solutions. 2014. “Fadi Aloula , A. R. Al-Alia , Rami Al-Dalkya, Mamoun Al-Mardinia, Wassim El-Hajjb - Department of Computer Science & Engineering, American University of Sharjah, UAE (united arab emirates), Department of Computer Science, American University of Beirut, Lebanon.” Accessed September 2, 2014.

[13] METI (Ministry of Economy Trade and Industry). 2014. “Promotion of Information Security Countermeasures on the Fields of Power and Energy.” Accessed September 1, 2014. http://www.meti.go.jp/english/information/data/IT-policy/securityl.htm.

[14] Carnegie Mellon University. 2014. “Software Engineering Institute CMMI (Capability Maturity Model Integration).” Accessed Sept 1, 2014. http://sei.cmu.edu.

[15] US Dept. of Energy. 2014. “ES-C2M2 (Electricity Subsector Cybersecurity Capability Maturity Model).” Accessed September 1, 2014. http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity.

[16] Hardware Reverse Engineering. 2014. “Access, Analyze & Defeat, Joe Grand, Black Hat DC 2011 Workshop.” Accessed September 1, 2014. https://media.blackhat.com/.../BlackHat_DC_2011_Grand-Workshop.pdf.

[17] OWASP (Open Web Application Security Project). 2014. “Top Ten Most Critical Web Application Security Flaws.” Accessed September 1, 2014. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project .

[18] Wikipedia.org. 2014. “White Box Testing, Hacking.” Accessed September 1, 2014. http://en.wikipedia.org/wiki/White-box_testing.

[19] Wikipedia.org. 2014. (Black Box Testing, Hacking.” Accessed Sept 1, 2014. http://en.wikipedia.org/wiki/Black-box_testing.

[20] Dangerous Proto Types. com. 2014 “Bus Pirate.” Accessed September 1, 2014. http://dangerousprototypes.com/docs/Bus_Pirate .

[21] KillerBee. https://code.google.com/p/killerbee/.

[22] NISTSP (National Institute of Standards and Technology Special Publication). 800-61 rev.2. 2014. “Computer Security Incident Handling Guide.” Accessed September 1, 2014. http://www.nist.org/nist_plugins/content/content.php?content.42.