PikeResearch
Cleantech Market Intelligence

Research Report

# Utility Cyber Security
## Seven Key Smart Grid Security Trends to Watch in 2012 and Beyond

**Published 4Q 2011**

**Bob Lockhart**
Senior Analyst

**Bob Gohn**
Research Director

# Section 1

# EXECUTIVE SUMMARY

## 1.1 Seven Trends to Watch in Utility Cyber Security

Utility cyber security is in a state of near chaos. After years of vendors selling point solutions, utilities investing in compliance minimums rather than full security, and attackers having nearly free rein, the attackers clearly have the upper hand. Many attacks simply cannot be defended. Pike Research has observed a dawning awareness by utilities and vendors during the past 18 months of the importance of securing smart grids with architecturally sound solutions. There is hope.

However, cyber security solutions remain challenging to implement, especially as attackers gain awareness of the holes between point solutions. Security vendors have finally found time to focus on industrial control system (ICS) security, not only advanced metering infrastructure (AMI) security – although a few security vendors have focused on ICS from the outset. The utility cyber security market will be characterized by a frantic race to gain the upper hand against the attackers, while at the same time strong competitors attempt to outdo each other.

This paper looks at seven key trends in smart grid cyber security:

- One size doesn't fit all: cyber security investments will be shaped by regional deployments
- Industrial control systems, not smart meters, will be the primary cyber security focus
- Assume nothing: "security by obscurity" will no longer be acceptable
- Chaos ahead?: the lack of security standards will hinder action
- Aging infrastructure: older devices will continue to pose challenges
- System implementation will be more important than component security
- The top five most promising smart grid cyber security technologies

# Section 2

# SEVEN UTILITY CYBER SECURITY TRENDS TO WATCH

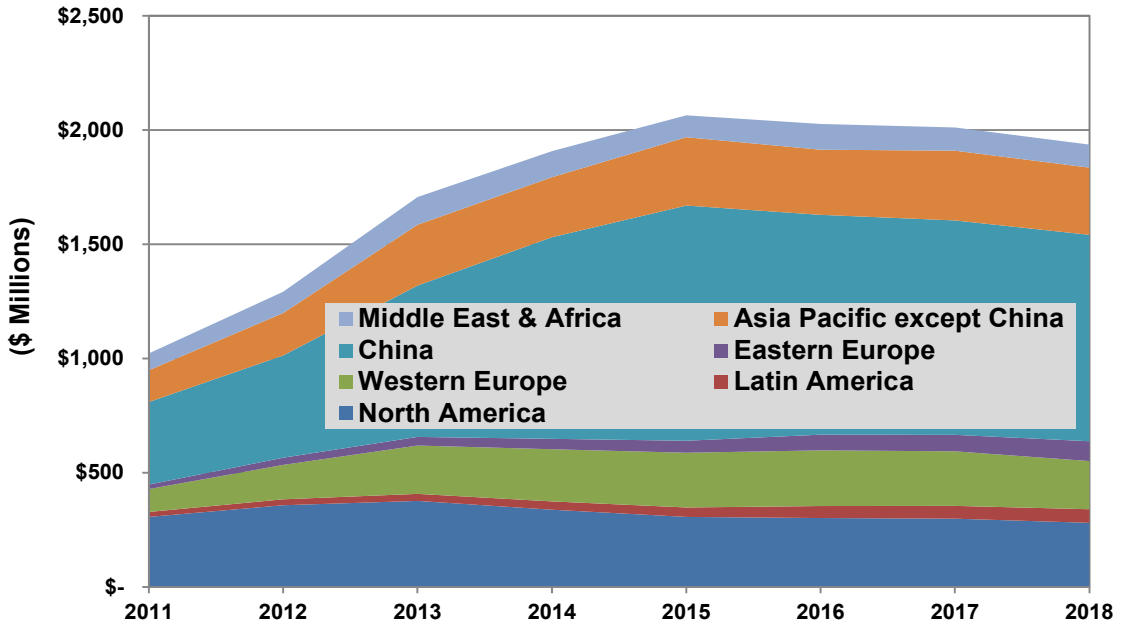
## 2.1 One Size Doesn't Fit All: Cyber Security Investments will be Shaped by Regional Deployments

The smart grid cyber security threat is clearly a global issue, with potential attacks coming from virtually anywhere, targeting anyone, and for a wide range of possible intents. But the underlying technologies differ by region, by segment, and by segment within a region. To cite examples at the extremes, smart meter adoption rates in North America have been quite a bit more aggressive than electric vehicle (EV) adoption rates in the Middle East and Africa, representing different cyber threat surfaces. Both adoption rates are likely to change throughout the forecast period as new markets open or reach saturation.

Obviously, investment in smart grid cyber security is directly related to smart grid technology adoption. Cyber security investment only happens when something needs to be secured. This makes it impossible to speak intelligently about smart grid cyber security at a broad brush stroke level, due to smart grid technologies' own variances within regions and segments. The following chart illustrates the diversity of smart grid cyber security investment throughout the world.

Chart 2.1, taken from Pike Research's recent report, *Smart Grid Cyber Security* (SGCS-11), shows our revenue forecast through 2018. The total revenue forecast is $14 billion, with a compound annual growth rate (CAGR) of 9.6%. The shaded areas in this chart show the diversity of investment by global regions.

***Chart 2.1 Smart Grid Cyber Security Revenue by Region, World Markets: 2011-2018***




*(Source: Pike Research)*

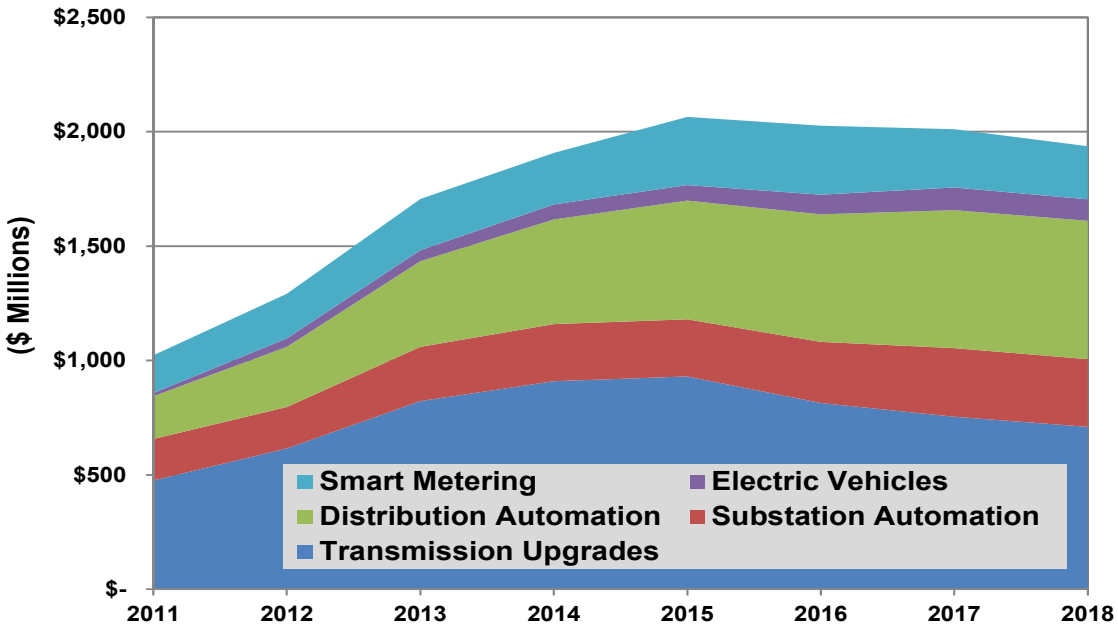
The overall revenue curve from this chart shows a plateau being reached in 2015, with a slight decline afterward. This reflects our assumption that smart grid deployments will increase throughout the decade, concurrent with price leveling, as cyber security technologies that are new today become more mainstream. Greater awareness of threats created by a connected smart grid, along with fines for non-compliance with regulations, such as the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP), have increased utilities' desires to deploy cyber security in their smart grids. As the utilities express more interest in smart grid cyber security, naturally, more vendors and products will arrive to accommodate that interest.

## 2.2 Industrial Control Systems, not Smart Meters, will be the Primary Cyber Security Focus

Pike Research forecasts that ICS security will grow faster and will generate more investment than smart metering security. Once again, this is a natural conclusion based on Pike Research's forecasts for smart grid technology investment. Pike Research's upcoming *Smart Grid Technologies* (SGT-11) report forecasts more investment in smart grid control systems – transmission upgrades, substation automation, and distribution automation – than in smart metering. Once again, we believe that smart grid technology investment will directly drive smart grid cyber security investment.

Chart 2.2, also from the Pike Research *Smart Grid Cyber Security* report, shows the same data analyzed by smart grid market segment, rather than by geographic region. Obviously, the overall curve is the same shape as Chart 2.1, because it is the same data, segmented differently.

***Chart 2.2 Smart Grid Cyber Security Revenue by Segment, World Markets: 2011-2018***




*(Source: Pike Research)*

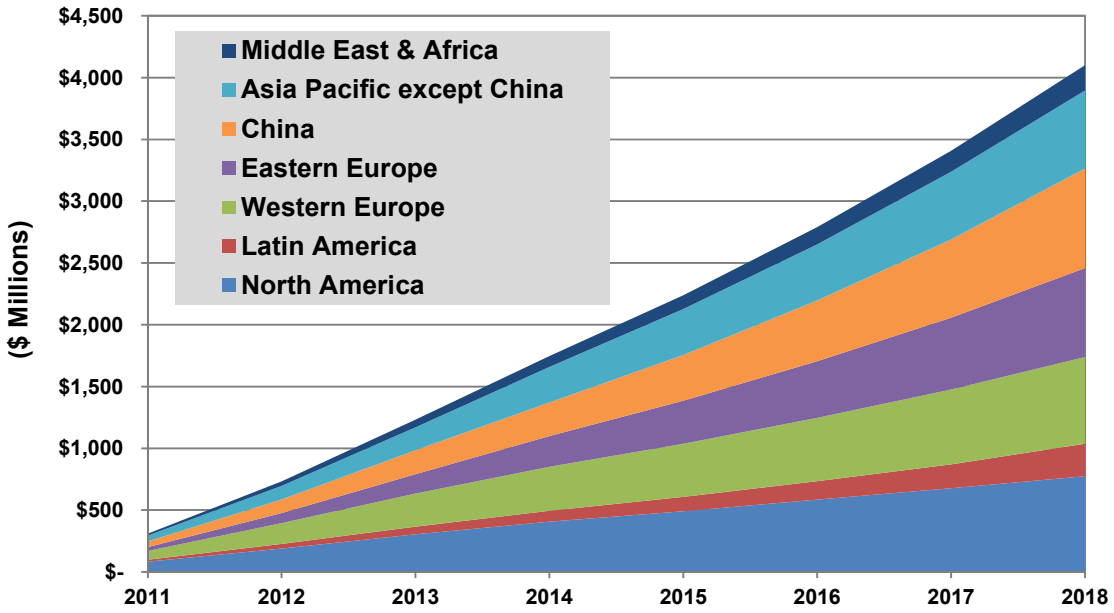
The shaded areas in this chart represent the five smart grid market segments. It is not surprising that the largest portions of investment are expected in transmission and distribution, two areas in which utilities have openly stated that they will invest. Transmission upgrades with smart grid technology can enable strategies like dynamic line rating, which can potentially reduce the amount of power that must be generated. Distribution automation can enable a number of promising technologies, such as demand response pricing and energy management. More intelligent distribution grid management can also enable utilities to deal more effectively with EV recharging, once EV adoption becomes more widespread.

## 2.3 Assume Nothing: "Security by Obscurity" Will No Longer be Acceptable

The discovery of Stuxnet during the summer of 2010 demonstrated that control networks are no longer secure simply because they are isolated from enterprise networks. Stuxnet also demonstrated that motivated attackers are willing to learn arcane technologies, such as the control sequences for a specific model of centrifuge.

Stuxnet was a mission and not simply a piece of malicious code. It was not detected until after it had accomplished its purpose and, most likely, evaded detection for more than a year after its release. Few utilities, vendors, or analysts are willing to discuss that even more sophisticated attacks may now be in process, which, so far, have completely evaded detection. However, that must be considered a probability, not merely a possibility.

***Chart 2.3 Cumulative ICS Security Revenue by Region, World Markets: 2011-2018***




*(Source: Pike Research)*

As we discuss in the *Industrial Control Systems Security* (ICSS-11) report, utilities, and especially their operations teams, have become more skilled and aware of control system cyber security issues during the past 12 to 18 months. Operations managers are now asking security vendors pointed questions. We believe that this will result in the appearance of more control systems security products. Chart 2.3, which depicts

cumulative revenues for 2011-2018, dramatically shows the forecast of increased control system security spending through the end of 2018. Even the less developed economies of Latin America and the Middle East and Africa show growth during this time.

The recently discovered Duqu malicious software has elements of Stuxnet, but may not be targeted at control systems. Regardless, it is a sophisticated information stealing attack with no clear idea yet as to how the stolen information will be used, if at all.

## 2.4 Chaos Ahead?: The Lack of Standards Will Likely Hinder Action

No enforceable smart grid security standards exist anywhere in the world for power distribution grids. The greatly discussed U.S. NERC CIP standards only apply to generation and transmission, though some of this has leaked into stimulus-funded distribution network projects. Other regulations or legislation may apply to specific situations, such as data privacy laws or payment card industry standards to protect customers' card data used in paying utility bills.

A number of well-written guidelines include the three-volume U.S. NIST Interagency Report (NISTIR) 7628, which covers smart grid cyber security strategy, architecture, high-level requirements, and data privacy. Additionally, NIST Special Publication 800-82 is a thorough examination of ICS cyber security issues. The U.S. and U.K. governments have co-published a document known in the United States as the Control System Security Program (CSSP) Recommended Practice: Improving Industrial Control Systems Cyber Security with Defense-In-Depth Strategies.

None of those guidelines is an enforceable standard and each takes great pain to point out that it is a series of recommendations, but not a baseline for audit or certification. At present, only the NERC CIP reliability standards have the teeth to result in fines for non-compliance. Even those standards are scoped to consider only critical cyber assets (CCAs). Identification of CCAs is, at best, labyrinthine.

This lack of enforceable requirements leads to a scene of mass chaos in utility cyber security. Many utilities – as with large companies in any industry – will only invest in cyber security when financial punishment for not investing is threatened, similar to failing an audit and being fined.

Utilities and vendors that would like to take action now to produce secure smart grids face a quandary: Which guidelines are going to survive? How is it possible to stake a direction now for cyber security and know with assurance that laws enacted several years from now will support that direction? The lack of clarity causes a number of utilities – and cyber security vendors – to take a wait-and-see posture. Those who choose to plow ahead now risk losing their entire investment if future laws invalidate their approach.

The definition of home energy management (HEM) solutions and the required home area networks (HANs) is in disarray as this paper is written. It is not clear what HAN approaches will prevail – whether customer data will travel via AMI wide area networks (WANs), consumers' Internet service providers (ISPs), or even dedicated HEM networks. This lack of standards makes selecting the right security solution for HEM an exercise in risk management and investment protection. It is not clear how to select a HEM security solution with any confidence that it will still be around in 2 years.

Finally, the lack of standards makes interoperability among smart grid technologies more challenging, since not all vendors will have adopted the same security approaches. Utilities are asking for interchangeable solutions, but the industry has not yet produced

interoperable solutions.

## 2.5 Aging Infrastructure: Older Devices will Continue to Pose Challenges

Smart metering systems are of recent enough vintage that all support modern communications protocols that protect information confidentiality and integrity. Whether proprietary or open protocols, most AMI systems have decent built-in cyber security. However, some supervisory control and data acquisition (SCADA) systems have been in place much longer than smart metering and may still have many devices running serial protocols, such as MODBUS, which has no built-in security features.

It is nearly axiomatic that SCADA devices will be replaced when their service life expires, not sooner (although possibly later). Security assessments are unlikely to result in a large-scale technology refresh, simply to replace old devices with better-defended modern devices. It is possible that a large-scale disaster caused – or not prevented – by inadequate cyber security could result in an earlier technology refresh. However, it is more likely that these older devices will be around until they are retired.

SCADA networks must support a mix of old and new, possibly for another 30 years until all the old devices' service lives have run their course. This coexistence of modern and legacy devices presents unique architectural challenges. The security architect cannot assume that a certain standard amount of cyber security is present on all devices. Old and new devices may need to communicate.

One approach to securing legacy SCADA devices is to insert a modern security device into the network, adjacent to the legacy device. Often referred to as a bump in the wire, devices like serial transceivers can integrate security functions, such as encryption and message digests. Those two capabilities used together can ensure data integrity and protect against man-in-the-middle attacks. However, these devices can, in some situations, introduce too much latency into control networks and installing the devices may require downtime on a network that has to be up at all times. Still, they can work in some scenarios and should be considered.

A second approach is to micro-segment the legacy devices into a single sub-network with protective barriers at the subnet boundary. These protective barriers can also integrate security functions, such as encryption and message digests. Again, the devices may introduce unacceptable latency to the control network, although the introduction of a single device, rather than many bumps in wires, could be less disruptive to the control network.

## 2.6 System Implementation will be More Important than Component Security

It is possible to have a system in which 100% of the components are secured, but the system as a whole is not secure at all. Cyber security works to protect a whole entity and attackers look for holes. The strongest adversaries are not going to waste time attacking a component device that is known to be a fortress. One cyber defense expert said, "Do not fear hackers. Fear engineers who hack." Security is only as strong as its weakest link and the best attackers know instinctively to look for that weak link.

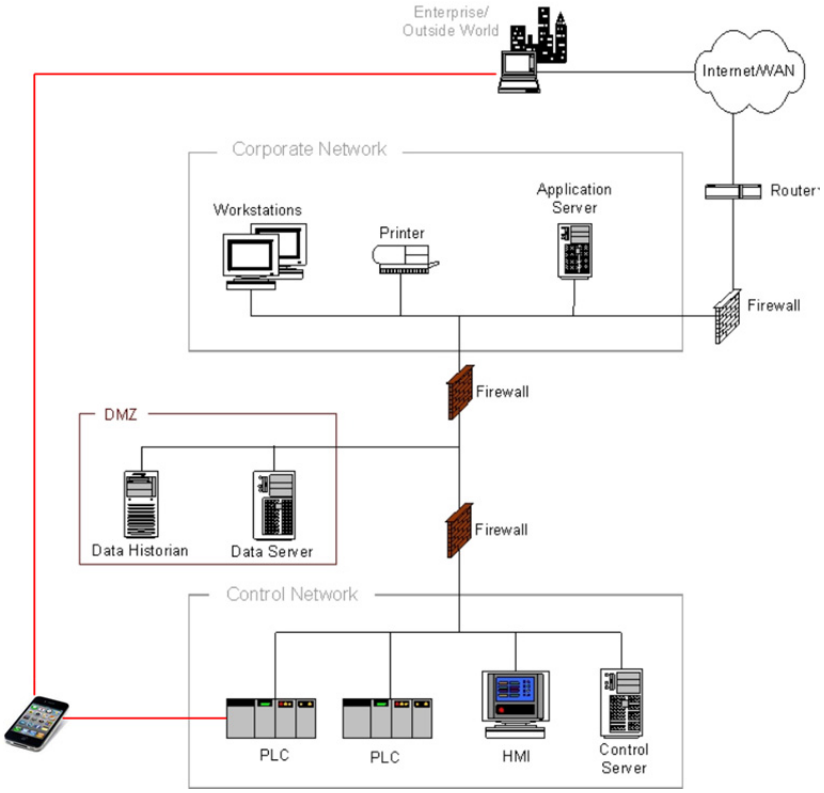
Implementation issues exist at the product and system levels. The best encryption algorithm in the world is useless if key distribution is not adequately secured. A sophisticated attacker will not attempt to brute-force attack a strong encryption algorithm, but will try to find the keys as they are being distributed, before the algorithm uses them.

At a system level, adequate security is nearly impossible without a cyber security architecture. This approach is commonplace in enterprise networks, but, as yet, rarely

seen in control networks. To be fair, some control networks have been built – perhaps congealed – over decades, so developing a security architecture could be a substantial backward looking research project. Once again, sophisticated attackers will look for holes in between secure components – things that architecture would address.

Figure 2.1 shows how a $60 piece of software can bypass an entire defense-in-depth implementation. This smartphone application allows direct communication between the smartphone and a Wi-Fi-enabled SCADA device. This direct access means that no protection exists unless a security architect has thought to include that in the plans.

***Figure 2.1 Paired-Firewall DMZ with Smartphone Directly Accessing SCADA Device***




*(Source: NIST Special Publication 800-82, with additions by Pike Research)*

## 2.7 The Top Five Most Promising Smart Grid Cyber Security Technologies

This section describes five cyber security technologies that can be the keys to protecting smart grids. A longer list is offered in the Pike Research *Smart Grid Cyber Security* (SGCS-11) report. As noted earlier, however, all security capabilities must be selected and deployed in the context of a security architecture, which considers the unique attributes of each smart grid.

### 2.7.1 Multi-Factor Authentication

The three factors of authentication are: something you know (e.g., a password), something you have (e.g., a smart card), and something you are (a biometric measurement). Multi-factor authentication requires the use of two or more of these authentication categories. A common example is withdrawing money from a cashpoint machine. You must use a cash

card (something you have) and enter a PIN (something you know), so it is two-factor authentication. Add a palm geometry scanner and it would be three-factor authentication.

Multi-factor authentication on control systems can ensure that stolen passwords are not enough to compromise the network. This can prevent many remote attacks against control systems, by requiring the user of the system to physically present the second factor – perhaps an access badge or a biometric scan – at the location of the control system.

Multi-factor authentication is also an effective defense against social engineering attacks, in which a remote person coaxes a password or other logon information out of an unsuspecting employee – usually via phone or email. Having just a password, but not the second factor, such as a security token, the attacker still will not have access to the control system.

### 2.7.2 Control Network Isolation

Network traffic from enterprise networks to control networks should be limited to the absolute minimum necessary to manage the control network. In some cases, traffic from enterprise to control networks can be eliminated altogether. One method to accomplish this is with a traditional demilitarized zone (DMZ) between the two networks, using firewall rules to restrict traffic into the control network. In extreme cases, such as nuclear generation plants, traffic from enterprise to control network can be eliminated completely using data diode solutions that prevent traffic flow at the hardware level.

### 2.7.3 Application Whitelisting

Application whitelisting is an alternative approach to preventing the execution of malicious software. In comparison to antivirus products (also known as blacklisting), whitelisting software records a list of permitted actions on a host and allows nothing else. Recent advances also enable whitelisting products to learn as they go and better protect the systems.

Whitelisting normally is faster and requires less compute power than blacklisting because it is only checking a small list of allowed actions, rather than a very large list of disallowed actions (the blacklist). This can be a good approach to securing embedded systems with limited computing muscle and possibly limited-life battery power.

Whitelisting requires few, if any, updates to the allowed actions list, whereas blacklists require daily or even hourly updates of the disallowed actions list. These updates can be logistically challenging to apply to embedded devices, chewing up yet more battery life and possibly requiring open communication channels that would not otherwise be needed and that present another attack surface for the control network.

### 2.7.4 Data Encryption

Data encryption makes data unreadable and, thus, prevents man-in-the-middle attacks against smart grid networks. Encryption is normally required by data privacy legislation to ensure that no personally identifiable information (PII) is accessed by unauthorized persons or enterprises. Asymmetric encryption (public and private keys) can provide authentication of the sender when the sender's private key is used for encryption. During later investigations, that same function can provide non-repudiation, as a proof of who actually sent the data. Many encryption products also have message digesting built in, which can indicate if any data had been changed without authorization during transmission.

### 2.7.5 Security Event Logging and Correlation

Security event correlation in control networks must support the primary security objectives of those networks: safety, reliability, and integrity. Unlike enterprise networks, these control system objectives cannot be achieved solely at the infrastructure level. Event correlation in control networks also requires a view into the data, rather than just its wrapper. Control system traffic that is perfectly formatted and follows all the rules of the network can still contain malicious set points or other data designed to destabilize a control network.

Securing a SCADA network is a highly contextual activity. Simply validating that servers, storage, communications, and endpoints are operating within security policies is not enough. SCADA security must also be aware of the types of actions that are legally occurring within those policies. This requires control system awareness that is built into the security products. Effective SCADA security needs inputs from application sources as well as infrastructure sources. Control system event sources, such as data historians, can provide this enhanced visibility.

As a result, control systems must be able to correlate the infrastructure level events, such as those from firewalls and logons, with those from the control devices themselves. Good correlation makes it possible to prevent incidents before they occur, by linking infrastructure-level and control-level events together and analyzing them.

# Section 3

## ACRONYM AND ABBREVIATION LIST

| | |
|---|---|
| Advanced Metering Infrastructure | AMI |
| Compound Average Growth Rate | CAGR |
| Control System Security Program | CSSP |
| Critical Infrastructure Protection | CIP |
| Critical Cyber Asset | CCA |
| Demilitarized Zone | DMZ |
| Electric Vehicle | EV |
| Home Area Network | HAN |
| Home Energy Management | HEM |
| Industrial Control System | ICS |
| Internet Service Provider | ISP |
| National Institute for Standards and Technology | NIST |
| National Institute for Standards and Technology Interagency Report | NISTIR |
| North American Electric Reliability Corporation | NERC |
| Personally Identifiable Information | PII |
| Personal Identification Number | PIN |
| Supervisory Control and Data Acquisition | SCADA |
| United Kingdom | U.K. |
| United States | U.S. |
| Wide Area Network | WAN |

# Section 4

## ADDITIONAL READING

**Smart Grid Cyber Security**

*System Reliability, Defense-in-Depth, Business Continuity, Change Management, Secure Telecommunications, Endpoint Protection, Identity Management, and Security Event Management*

http://www.pikeresearch.com/research/smart-grid-cyber-security

**Industrial Control Systems Security**

*Market Issues, Security Best Practices, and Global Forecasts for SCADA Security, Industrial Control Networks, Human-Machine Interfaces, and SCADA Telecommunications*

http://www.pikeresearch.com/research/industrial-control-systems-security

**Smart Meter Security**

*Event Correlation Improvements, Security Software on Meters, Identity Management and Authorization, Network Resiliency, Meter Worm Prevention, and End-to-End Data Encryption*

http://www.pikeresearch.com/research/smart-meter-security

**Electric Vehicle Cyber Security**

*Privacy, Compliance, Encrypted Communications, Resilient Networks, and Device Security: Market Analysis and Forecasts*

http://www.pikeresearch.com/research/electric-vehicle-cyber-security

**Smart Grid Technologies**

*Networking and Communications, Energy Management, Grid Automation, and Advanced Metering Infrastructure*

http://www.pikeresearch.com/research/smart-grid-technologies

**Smart Meters**

*Smart Electrical Meters, Advanced Metering Infrastructure, and Meter Communications: Market Analysis and Forecasts*

http://www.pikeresearch.com/research/smart-meters

# Section 5

## TABLE OF CONTENTS

# Section 6

## TABLE OF CHARTS AND FIGURES

# Section 7

## SCOPE OF STUDY

This white paper looks at some of the key issues for securing smart grids. Pike Research segments smart grids into: transmission upgrades, substation automation, distribution automation, EV charging infrastructures, and smart metering. This paper presents information previously published in a number of Pike Research reports and white papers, blending topics from several different research projects into a single viewpoint. For more details, we recommend the documents in the Reading List shown in Section 4.

## SOURCES AND METHODOLOGY

Pike Research's industry analysts utilize a variety of research sources in preparing Research Reports. The key component of Pike Research's analysis is primary research gained from phone and in-person interviews with industry leaders including executives, engineers, and marketing professionals. Analysts are diligent in ensuring that they speak with representatives from every part of the value chain, including but not limited to technology companies, utilities and other service providers, industry associations, government agencies, and the investment community.

Additional analysis includes secondary research conducted by Pike Research's analysts and the firm's staff of research assistants. Where applicable, all secondary research sources are appropriately cited within this report.

These primary and secondary research sources, combined with the analyst's industry expertise, are synthesized into the qualitative and quantitative analysis presented in Pike Research's reports. Great care is taken in making sure that all analysis is well-supported by facts, but where the facts are unknown and assumptions must be made, analysts document their assumptions and are prepared to explain their methodology, both within the body of a report and in direct conversations with clients.

Pike Research is an independent market research firm whose goal is to present an objective, unbiased view of market opportunities within its coverage areas. The firm is not beholden to any special interests and is thus able to offer clear, actionable advice to help clients succeed in the industry, unfettered by technology hype, political agendas, or emotional factors that are inherent in cleantech markets.

## NOTES

CAGR refers to compound average annual growth rate, using the formula:

CAGR = (End Year Value ÷ Start Year Value)$^{(1/steps)}$ – 1.

CAGRs presented in the tables are for the entire timeframe in the title. Where data for fewer years are given, the CAGR is for the range presented. Where relevant, CAGRs for shorter timeframes may be given as well.

Figures are based on the best estimates available at the time of calculation. Annual revenues, shipments, and sales are based on end-of-year figures unless otherwise noted. All values are expressed in year 2011 U.S. dollars unless otherwise noted. Percentages may not add up to 100 due to rounding.

Published 4Q 2011


1320 Pearl Street, Suite 300
Boulder, CO 80302 USA
Tel: +1 303.997.7609
http://www.pikeresearch.com