Providing Security for Smart Energy Systems: An Industrial White Paper

Meera Balakrishnan
Freescale Semiconductor

freescale.com

Abstract

Network connectivity in today's industrial entities, including electrical utilities, has exposed many digital communication and control aspects—from the office to industrial machines—to the threat of cyber attacks. When forward-looking improvements including smart grid, smart meters and other advancements are considered, security is of foremost concern. In fact, governments around the world have recognized the existing vulnerability and need to protect the grid infrastructure. To solve the problem, regulations and standards are being developed to ensure that the proper security steps are taken.

This white paper provides background regarding the increasing necessity for improved security, discusses the fundamental principles for improving security, including standards, presents two highly applicable use cases and explains a technical solution that implements requirements defined in key standards.

Need for Improved Grid Security

Attacks on computer systems from viruses, root kits, trojans, worms, keyloggers, bots and other malicious software have been the focus of hackers and cyber security experts for many years. With historically isolated industrial controls such as Supervisory Control and Data Acquisition (SCADA) systems and programmable logic controllers (PLCs) connected to the same networks, loss of service and physical damage can be caused from unauthorized access. In fact, the goal of the smart grid is network connectivity, so network security is fundamental to its successful implementation.

However, the global electricity grid infrastructure has experienced a rapid increase in the number of vulnerabilities since 2000, and the occurrences are growing. As one of the key assets of any nation, protection from the increasing number of attempted and successful attacks on the grid and its metering systems is (or should be) a national priority for all industrialized countries.

Increasingly, more dangerous attacks have occurred from sophisticated attackers, including foreign governments, as well as state run and financed attacks, hackers, cyber terrorists, organized crime, industrial competitors, disgruntled employees and careless or poorly trained employees. Perhaps the most well-known recent occurrence was the Stuxnet computer worm. Discovered in June 2010, Stuxnet was spread through Microsoft Windows® OS targeting Siemens' SCADA systems.

The motivation for stakeholders—from content owners, service providers and manufacturers to end users—varies, as shown in table 1. The bottom line is that the cost impact can be significant. At the 2011 London Conference on Cyberspace, British Prime Minister David Cameron reported that cybercrime cost the UK an estimated 27 billion pounds a year, and several other nations as much as U.S. $1 trillion a year globally.

Cyber Attack Impact

Asset	Stakeholder	Attack
Content – Media – Applications	Content owner	Piracy
Service access – Network – Enterprise	Service provider	Fraud
Intellectual property – Owned – Licensed	Manufacturer	Espionage
Personal data – Identification – Connections	End user	Privacy breach

Table 1. The impact on assets and stakeholders of cyber attacks. (Source: NIST)

As a result, governments around the world have taken steps to provide increased security and reduce the cost of cyber crime. United States government organizations active in standards and other areas include the North American Electricity Reliability Corporation (NERC) and the National Institute of Standards and Technology (NIST).

Designed to ensure the reliability of bulk electric systems in North America, NERC's Critical Infrastructure Protection (CIP) includes standards development, compliance enforcement, assessments of risk and preparedness. NIST developed and issued NISTIR 7628, Guidelines for Smart Grid Cyber Security and NIST Special Publication 1108: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.

Standards Developed to Provide Improved Grid Security

NERC's CIP Reliability Standards require compliance with specific requirements to safeguard critical cyber assets. CIP-002 through CIP-009 address physical as well as cyber security requirements for responsible grid entities. They provide the benchmarks for utility companies' measurements and certifications. Cyber aspects include the following:

- Identifying critical assets
- Identifying and training cyber security personnel
- Developing and implementing security management
- Defining methods, processes and procedures
- Securing the systems identified as critical cyber assets
- Reporting and response planning
- Establishing recovery plans

NIST's cybersecurity objective of confidentiality, integrity and availability (CIA) impacts the interactions of several entities as shown in figure 2. The basis of the interactions are the Internet, enterprise buses, wide area networks (WANs), substation local area networks (LANs), field area networks and premises networks. While confidentiality is least critical for power system reliability, it is increasingly important with the availability of online customer information and privacy laws that impose strict penalties for breach of privacy. The integrity for power system operation addresses requirements of the following:

- Authentication of the data
- No modification of the data without authorization
- Implementation of NISTIR 7628
- Known and authenticated time stamping and quality of data

Smart Grid Domains

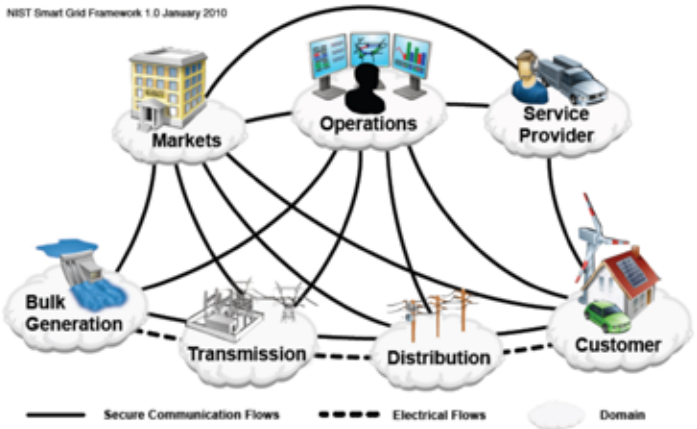

Figure 2. The interactions of different smart grid domains through secure communication and electrical flows. (Source: NIST Smart Grid Framework 1.0, January 2010).

In addition to establishing the requirements, NIST existing and developed standards identify critical security aspects such as data encryption and definitions for common understanding and implementation of solutions.

Root of Trust and Other Definitions

The fundamental step towards establishing a secure or trusted component or entry point to a network is a root of trust (RoT). The RoT verifies that the component is performing in an expected manner in the initial operation or engagement of the component or system. This established trust provides the first step towards improving security. In the Aberdeen Group report, "Endpoint Security: Hardware Roots of Trust," the analyst notes that over a 12-month period, companies that utilized a hardware RoT in their approach to security had 50 percent fewer security related incidents and 47 percent fewer compliance/audit deficiencies.

Other terms that may be unfamiliar to those addressing highly secure computer operation for the first time include:

- Anti-cloning provides a unique device ID and digital signing support and encryption
- High assurance boot is a security library embedded in tamper-proof on-chip ROM that prevents unauthorized software execution
- Secure clock provides reliable time source
- Secure communications ensure the integrity of data and information
- Secure debug protects against hardware debug (Joint Test Action Group (JTAG)) exploitation
- Secure storage provides a programmable ARM® TrustZone® protected region within on-chip RAM
- Trusted execution isolates execution of critical software from possible malware
- TrustZone is a trusted execution environment for security-critical software

See the appendix for more acronyms and glossary.

Two Use Cases Exemplify the Implementation of NIST Requirements

Use case 1: Smart meters

Smart meters, or the advanced metering infrastructure (AMI), have two-way communications between field area networks in the smart grid. As such, they can be a weak link in overall network security. In the NERC CIP assessment, there are several critical smart meter areas:

15—Interface between systems that use customer site networks such as home area networks (HAN) and building area networks (BAN)

17—Interface between systems and mobile field crew laptops/equipment

18—Interface between metering equipment

The NIST CIA impact level of low (L), medium (M), or high (H) for these critical areas is shown in table 2.

The high-level security aspects with unique technical requirements include the following:

- User identification and authentication
- Device identification and authentication
- Security function isolation
- Denial-of-service protection
- Software and information integrity

To meet these requirements, the silicon solution must provide the following:

- Crypto support
- Secure key
- Random number generator (RNG)
- Secure clock
- Trusted execution/hardware firewall
- Tamper detection
- Secure debug

Confidentiality, Integrity and Availability Impact Levels for Smart Meters

	Confidentiality	Integrity	Availability
15—Interface between systems that use customer site networks such as home area networks (HAN) and building area networks (BAN)	Low	Medium	Medium
17—Interface between systems and mobile field crew laptops/ equipment	Low	High	Medium
18—Interface between metering equipment	Low	High	Low

Table 2. CIA impact levels for smart meters. (Source: NIST 7628)

AMI system functions include measuring, communicating and using the data. Encryption techniques are defined for specific aspects of these functions. Smart meter encryption techniques include Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) that are even more stringent than techniques used in the banking sector. NIST applies additional requirements for smart meters, including unique credentials, a key management system (KMS) that supports an appropriate lifecycle of periodic rekeying and revocation, and more. The successful implementation of smart meter security is based on a hardware root of trust.

Use case 2: Data concentrator

In the AMI architecture, a data concentrator collects meter information and data for transmission to the utility. Figure 3 shows the process.

Security Process Between Smart Meter and Utility

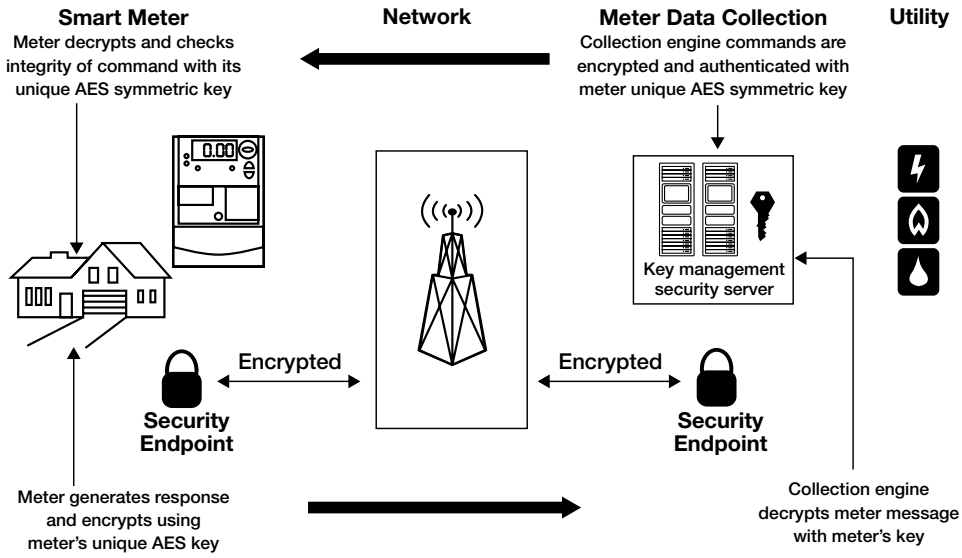

Figure 3. End-to-end security between the smart meter and the utility. (Source: FSL)

Mechanisms for the interface between the data collection system and the electricity meter (or a data concentrator and the electricity meter) include the following:

- Authentication of all command messages
- Encryption (AES 128) to ensure confidentiality of metering data using block ciphering and a unique symmetric encryption key for each meter
- Message authentication for meter data integrity provided via AES Galois Message Authentication Code (GMAC) algorithms

Each smart meter has a unique and secret unicast AES key with its default value set in the factory. When the meter has been installed and commissioned, a new operational key replaces the default value. A unique and non-modifiable master key encryption key (KEK) in each smart meter provides added security. The master key is used during the transportation of a new working key, during the commissioning or during the operational life of the meter.

Freescale Security Solutions

As a leading supplier of MCUs and MPUs for control and monitoring applications, Freescale has over 44 years of experience developing information security solutions. This includes the following:

- More than 150 security patents
- More than 5,000 man years and $1.7 billion invested to date
- More than 125 major equipment projects developed and produced

In addition, dedicated Security Technology Centers of Excellence and an extensive portfolio of cryptography and platform assurance intellectual property (IP) provide Freescale a distinctive position to address smart grid security issues. To meet NERC and NIST requirements, four different Freescale solutions address security in smart grid and other industrial applications. (Refer to table 3.)

Freescale Security Solutions

Security Features	QorIQ MPU	i.MX MPU	Vybrid MPU	Kinetis MCU
Trusted Execution	• Hypervisor secure and normal processor modes • Memory management • No execute feature (memory pages can be marked as non executable)	TrustZone secure and normal processor modes (i.MX53, i.MX 6)	TrustZone secure and normal processor modes	Non MMU—but security supported with memory protection unit
High Assurance Boot	Secure boot process supported by: • Security fuse processor • Internal boot • ROM security monitor	Authenticated boot, encrypted boot (i.MX 6)	Authenticated boot, encrypted boot	√
Secure Storage	√	Off-chip crypto protection On-chip, self-clearing RAM	On-chip zeroizable secure RAM	256-bit secure storage erased by tamper
Hardware Random Number Generation Ensures strong keys and protects against protocol replay	√	√	√	√
Secure Clock Provides reliable time source On-chip, separately powered real-time clock Protection from software tampering		On-chip separately powered real-time clock	On-chip separately powered real-time clock	Secure real-time clock with monotonic counter
Secure Debug	Permanent JTAG or challenge/response access	Three security levels and complete JTAG disable	Three security levels and complete JTAG disable	Multiple secure debug levels
Tamper Detection	Runtime integrity checker	Runtime integrity checking, physical tamper detection	Runtime integrity checking, physical tamper detection	Runtime integrity checking, physical tamper detection
Cryptography	Security acceleration AES, DES, 3DES SHA1/256, MD5, public key—RSA, ECC	Hardware acceleration for AES, MD5, SHA1/256	Hardware acceleration AES, DES, 3DES MD5, SHA1/256	Hardware acceleration AES, MD5, SHA1/256
Deep Packet Inspection Intrusion detection and prevention using signature detection and filtering techniques	√			

Table 3. Freescale security solutions at a glance.

QorIQ Family: The single-core QorIQ P1010 processor's trust architecture platform helps protect against software intrusion and software cloning with its advanced end-to-end code signing and intrusion prevention capabilities. Implementing the NIST 7268 system trust model, figure 4 shows the trust features in the QorIQ P1010 processor. Based on the e500 core, the P1010 includes security acceleration, security fuses, security monitor, internal boot ROM and external tamper detect blocks. These blocks and others combine to provide a variety of security options.

QorIQ P1010 Trust Features

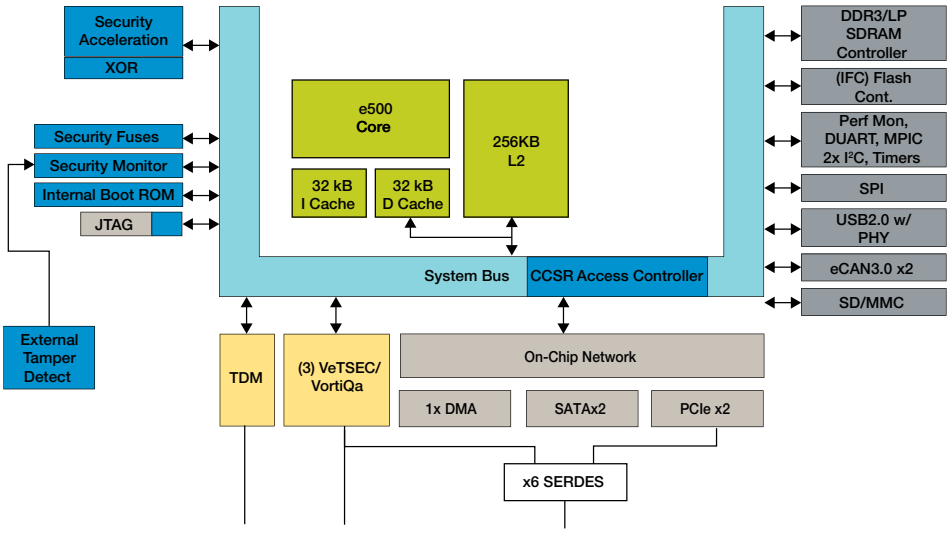

Figure 4. QorIQ P1010 processor trust features.

Figure 5 shows the trusted boot process of the QorIQ processor. The QorIQ processor uses an RSA public key to decrypt the signed hash and simultaneously recalculates the SHA-256 hash over the system code. If the decrypted original hash matches the calculated hash, the code is authenticated.

Code Integrity

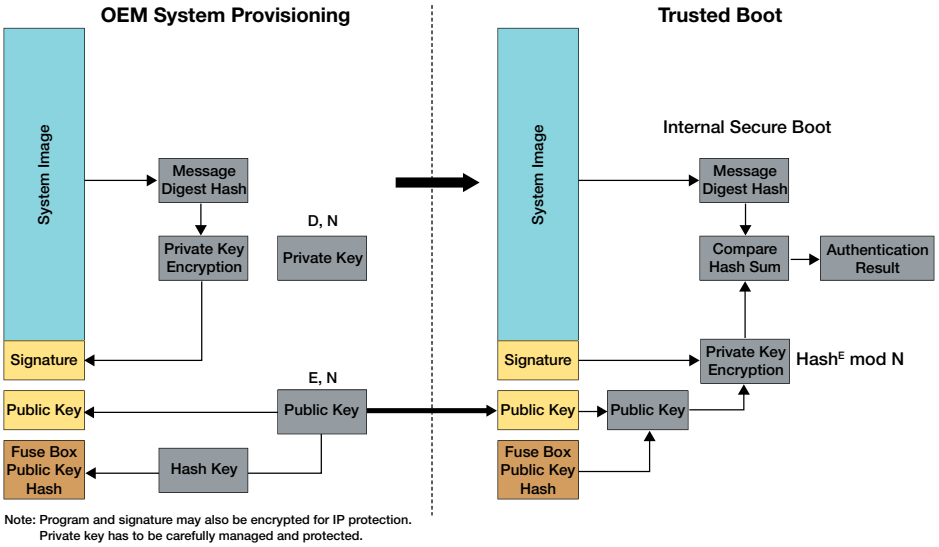

Figure 5. Code integrity through the trusted boot process.

The QorIQ family is ideally suited to solve the use cases mentioned earlier and many more. For example, the P1025 QorIQ data concentrator includes the following:

- 667 MHz/800 MHz dual-core P1025 QorIQ processor
- Capabilities for IEEE® 1588 time stamping and security acceleration

The P1025 includes additional features that address connectivity and security requirements in data concentrator applications.

Other Freescale security options for the smart grid include the i.MX and Vybrid MPUs and the Kinetis MCU. Vybrid MPUs do not have the deep packet inspection of the QorIQ, but they include a secure clock for a reliable time source. The on-chip, separately powered real-time clock provides protection from software tampering.

The i.MX processor includes TrustZone secure and normal processor modes as well as a secure clock, but does not have deep packet inspection. Finally, the Kinetis MCU does not have a memory management unit, but supports security with a memory protection unit and other security features.

Freescale security solutions feature robust tools and solid ecosystem partner solution support, including:

- Extensive tool suite of hardware and software available for customer evaluation
- VortiQa software tool suite for control center, monitoring control and home gateway applications
- Certified, third-party software suite

Securing the Grid and More

Increased grid infrastructure networking requires increased grid security. With efforts from organizations such as NERC and NIST, the specific requirements for increased grid security have been well defined. As a result, enabling technologies from many companies will ensure high security levels as smart grid systems, including smart meters and data concentrators, are implemented. Leveraging proven leadership in processing, control and security, Freescale security solutions provide the trusted, hardware-based foundation for a secure grid with comprehensive systems and software support.

Appendix

Additional terminology:

Hash is any well-defined procedure or mathematical function that converts a large, possibly variable-sized amount of data into a small datum.

RSA is an algorithm for public key cryptography named for Rivest, Shamir and Adleman, who were the first to publicly describe it.

For more complete acronyms and glossary, see Appendix I of NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References.

References:

Energy Grid: Safe From Cyber Attack?
news.discovery.com/tech/smart-grid-cyber-attacks-110901.html

INL/EXT-09-15500, “Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues”
inl.gov/scada/publications/d/securing_the_smart_grid_current_issues.pdf

NERC
nerc.com/files/CIP-002-1.pdf

Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security
smartgrid.gov/sites/default/files/pdfs/nistir_7628%20.pdf

NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements
csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid
csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References
csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

An Introduction to the QorIQ Platform’s Trust Architecture
element14.com/community/servlet/JiveServlet/previewBody/36481-102-1-218335/QORIQTAWP%5B1%5D.pdf

How to Reach Us:

Home Page:
freescale.com

e-mail:
support@freescale.com

USA/Europe or Locations Not Listed:
Freescale Semiconductor
Technical Information Center, CH370
1300 N. Alma School Road
Chandler, Arizona 85224
1-800-521-6274
480-768-2130
support@freescale.com

Europe, Middle East, and Africa:
Freescale Halbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
support@freescale.com

Japan:
Freescale Semiconductor Japan Ltd.
Headquarters
ARCO Tower 15F
1-8-1, Shimo-Meguro, Meguro-ku,
Tokyo 153-0064, Japan
0120 191014
+81 3 5437 9125
support.japan@freescale.com

Asia/Pacific:
Freescale Semiconductor Hong Kong Ltd.
Technical Information Center
2 Dai King Street
Tai Po Industrial Estate,
Tai Po, N.T., Hong Kong
+800 2666 8080
support.asia@freescale.com

For Literature Requests Only:
Freescale Semiconductor
Literature Distribution Center
P.O. Box 5405
Denver, Colorado 80217
1-800-441-2447
303-675-2140
Fax: 303-675 2150
LDCForFreescaleSemiconductor@hibbertgroup.com

freescale™

For more information, visit freescale.com/smartenergy

Document Number: SESECURITYSEWP REV 0