

Scalable Extensible Secured and Safe Smart Gateway Platform Solution for Smart Grid/ Energy and IoT

Vishwapathi Rao Tadinada¹ and Kwok Wu²

¹ Freescale Semiconductors, India
tv.rao@freescale.com

² Freescale Semiconductors, USA
kwok.wu@freescale.com

Abstract. IoT is here to stay, while the use of IPv6 is imperative to connect all devices globally via Internet, where security and networking safety is of primary concern.

This paper takes the example of the multi-billion dollar Smart Grid market and describes the security concerns for the applications in this market: Smart Meter, Data Concentrator, Sub Station Automation and the cloud-connected SCADA, Supervisory Control and Data Acquisitions network. For each of the segments/application the security concerns are analyzed and solutions to these concerns are proposed whilst addressing the IoT market opportunities. The four pillars of network security viz. Integrity, Availability, Confidentiality, Non-repudiation as specified by NIST SP 800 82 [1], NERC and IEEE are addressed in the proposed solutions. Apart from security; performance and scalability are given due importance and consideration both from software and hardware perspective in the proposed platform solution.

Freescale's M2M (Machine-to-Machine) and IoT end-to-end security solutions provided in this paper can be extended to other areas like smart energy, smart health, smart transportation, smart factory, enterprise and residential (smart home) and make connected intelligence a reality.

1 Introduction

This paper takes a closer look at the security concerns at the communication layer of the Smart Grid which is expected to be predominantly IP based network as shown in Figure 1. As the data is transmitted over Internet it has to be assured security in terms of Data Integrity, Confidentiality and Non Repudiation. All devices must be protected against denial of service attacks, cyber attacks, vulnerabilities and exploits. They should also be protected from malformed and bad traffic. Every IP address is susceptible to attacks and must be protected.

Smart Meters, Concentrators, Transmission line sensors are deployed out in the open and thus must be protected from physical attacks and tampering. Such attempts have to be detected with help of sensors and reported to the Utility. Trusted boot and secure architecture must be provided to protect against unauthorized or malicious firmware upgrade.

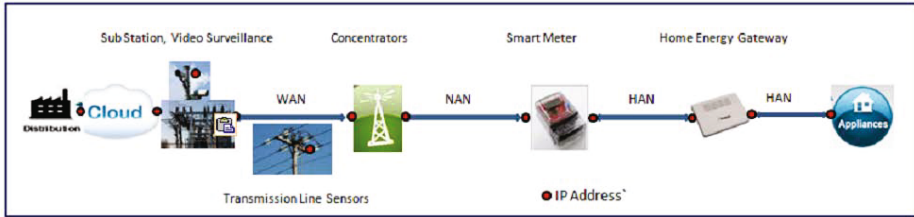


Fig. 1. End-to-End Security in the Smart Grid

Reliable two way communication is essential for effective functioning of the Smart Grid. Reliability and redundancy can be provided by having a mesh topology at the Concentrator. Additional reliability of communication can be achieved by having two WAN connections at the Concentrator and Sub Stations for load balancing and fail over. Reliability can be further enhanced by implementing RAID 5, Redundant Array of Independent Disks (<https://en.wikipedia.org/wiki/RAID>) on upstream device to protect loss of transient data.

This paper analyzes the security concerns across the Smart Grid hierarchy shown in Figure 2 and proposes platform solutions in form of Freescale hardware and software. Some examples of platform solutions covering various aspects of security discussed in this paper are:

1. Smart Meter: Low footprint IP Stack with 6LoWPAN, Firewall and IPSec-IKEv2 running on Freescale MC1322x.
2. Concentrator: IP Stack on Concentrator with 802.15.4 and 802.3 running on Freescale P1025 QorIQ.
3. Home Energy Gateway on Freescale MPC8308 with WiFi and Security Software.
4. Utility and Sub Station Servers with Security, Load balancer, virtualization software running on Freescale P4080 QorIQ.

2 Securing Communication on the Smart Grid

This section covers the various layers of Smart Grid Hierarchical Architecture, security concerns for each layer and platform solutions for each. Smart Grid security can be divided in the following segments/application blocks as shown in Figure 2:

1. Neighborhood Area Network- NAN (Smart Meter to Concentrator)
2. Home Area Network- HAN (Appliances to Smart Meter or Home Energy Gateway)
3. Wide Area Network- WAN (Concentrator to Sub Station/Utility)

Each of these layers is described in the upcoming sub-sections in terms of their typical deployment, network topology, communication technology, security

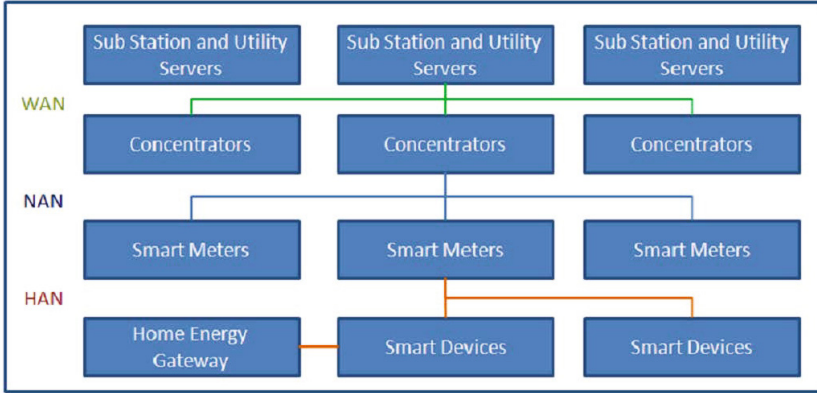


Fig. 2. Smart Grid Hierarchical Architecture

concerns for the devices in each segment and protecting the data that is being communicated. A platform solution detailing Freescale hardware and software addressing security issues is proposed.

2.1 Securing NAN (Metrology-to-Concentrator)

NAN, Neighborhood Area network that connects the Smart Meter to the Concentrator is perhaps the most challenging in terms of vulnerability and security solutions because of the following reasons:

1. Varied communication technologies options available: WiMAX, 3/4G, 802.15.4, PLC. Though multiple technologies are available, most of them are wireless and suffer the drawbacks of the wireless communication where the data can be sniffed and tampered with.
2. Low memory and other hardware resource constraints on the Smart Meter limit the feasibility of a robust security solution and restrict the options available for connection technologies.
3. Both Smart Meter and Concentrators are deployed outdoors and are susceptible to physical attacks

These factors make NAN the weakest link the Smart Grid and thus all factors impacting security need to be taken into considerations and addressed carefully.

This section takes 802.15.4 as example of communication between Smart Meter and Concentrators and discusses the security issues and demonstrates how they can be addressed. The same can be applied to other modes of communication.

2.1.1 Platform Solution for Smart Meter

Since adoption of IPv6 is inevitable, in this example 6LoWPAN/802.15.4 running on Freescale MC1322x is proposed as a platform solution. The IP stack can

be enhanced with rich security features integrating Freescale's VortiQa[2] Firewall, IPSec[3] and IKEv2 [4] as shown in Figure 3. However, since the flash and RAM on the board are less, light-weight version the security application to fit into sub 100 K ROM and sub 100 K RAM is used. Further, VaultIC from InsideSecure (<http://www.insidesecure.com/eng/Products/Secure-Solutions/Secure-solutions-products>) can be used to secure the keys and certificates on the Smart Meter.

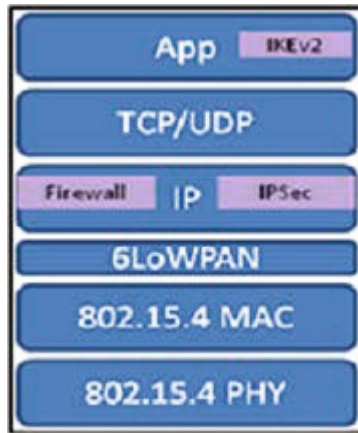


Fig. 3. IP Stack on Smart Meter with 6LoWPAN, Firewall and IPSec-IKEv2 running on Freescale MC1322x

2.1.2 Network Topology and IP Addressing: NAN

For NAN, the Concentrator is considered to be the focal point, 802.15.4 coordinator, a Full Functional Device (FFD) and the Smart Meter a Reduced Functional Device (RFD) with routing function. All Smart Meters in a given area or building are fully meshed with Concentrator as Coordinator. The Concentrator assigns DHCP v6 IP addresses to the *Smart Meters*.

2.1.3 Security on Smart Meter

Smart Meter comes preloaded with shared keys or certificates. Alternatively keys or certificates can be distributed in an out-of-band trusted mechanism. Since IP address at the Smart Meter is dynamically assigned Internet Remote Access Client IRAC, can be used for IKE exchanges. IKEv2 is used for Identity protection and for establishing Encryption and Authentication keys for the IPSec tunnel between the Smart Meter and Concentrator. This combination IKE and IPSec provides a secured NAN channel with data confidentiality and integrity. Sequence number in the IKE and IPSec help protect against replay and man in the middle attacks. Digital Signatures can be used for non-repudiation. Access policies or Access Control List can be configured on the Firewall to allow

only traffic from HAN to the Utility and vice-a-versa to pass through Smart Meter. Self traffic can be limited only to allow IKE, DNS, DHCP traffic from Concentrator to self and vice-a-versa. Since the Smart Meter is expected to be actively communicating with the HAN devices, ACL should allow traffic from HAN to Self and vice-a-versa. DoS/Cyber-Attack check can be enabled on the Firewall to protect the Smart Meter from well known attacks like Ping Flood, Syn Flood, LAND Attacks; Smurf Attacks. Any such attack detected should then be reported to Utility.

Freescale Secure Boot/Trusted Boot Architecture can be used to prevent malicious firmware upgrade. Freescale's Anti Tampering sensors can be used to protect from physical attacks and tampering. Security concerns at the Smart Meter and the suggested solutions are summarized in Figure 4

Security Consideration	Proposed Solution
Data Integrity/Authentication	VortiQa IPSec/IKEv2
Data Confidentiality/Encryption	VortiQa IPSec/IKEv2
Non-Repudiation	VortiQa IPSec/IKEv2
Reply-Man-in-the-Middle Attacks	VortiQa IPSec/IKEv2
Identity Check	VortiQa IPSec/IKEv2
Availability/Denial of Service	VortiQa Firewall
Access Control	VortiQa Firewall
Malicious firmware upgrade	Freescale's Secure Boot Arch
Tampering Physical attacks	Freescale's Anti Tampering Sensors



Fig. 4. Security Solution on the Smart Meter

2.2 Securing Home Area Network (HAN)

Home Area Network (HAN) has multiple smart automated appliances like HVAC (Heating, Ventilation and Air Conditioning), washing/dryer machines, smart plugs, lighting and multimedia connected to Smart Meter and/or Home Energy Gateway, then the Smart Meters from multiple households are connected to the data concentrator in the Neighborhood Area Network (NAN) for Advanced Metering Infrastructure (AMI). These appliances can be monitored and managed to use energy efficiently. This connected intelligence is provided by Freescale's Smart Energy Solutions.

As shown in Figure 5, all smart appliances are connected to the Home Energy Gateway communicating over wireless 802.15.4. The Home Energy Gateway in turn connects to Internet via 3G/LTE or DSL. Optionally it can act as an 802.11.x Wireless AP.

2.2.1 Platform Solution for Home Energy Gateway

Freescale offers a converged architecture networked Smart Energy Gateway on MPC8308 [5], offering seamless connectivity with TCP/IP, 802.11n and Zig-Bee. VortiQa Software offers Firewall, NAT, Intrusion Detection and Prevention (IDS/IPS), Application Identification/Monitoring System (AIS) and IPSec and IKE security services. Details of this solution are available at (<http://www.youtube.com/watch?v=ZlwivEjW2tk>)



Fig. 5. Home Energy Gateway on Freescale MPC 8308

2.2.2 Network Topology and IP Addressing

As shown in Figure 6, all smart appliances are connected to the Home Energy Gateway communicating over wireless 802.11.4. Smart metering connectivity is achieved via ZigBee SE 1 or MBus. Smart appliances are managed via ZigBee HA1.0.

On the WAN side the Home Energy Gateway connects to Internet via 3G/LTE or DSL using DHCP whereby, IP Address is dynamically assigned by the service provider.

Freescale wireless gateway can optionally act as an 802.11.x Wireless AP on the LAN side. The AP provide IP addresses to the LAN devices like laptops, tablets.

Freescale wireless Gateway also runs on P1010, i.Mx platforms with Trusted Architecture and Trusted Boot.

2.2.3 Security on Smart Energy Gateway

The remote monitoring, control and management of all in-home Smart Appliances happens through the Smart Energy Gateway. This data is sensitive and private and thus has to be provided security while traversing the Internet. This is achieved by establishing an encrypted secure channel for this traffic over the WAN. VortiQa IPSec/IKEv2 or SSL can be used to provide this. In addition to confidentiality this solution provides integrity, identity protection, non-repudiation and protection against replay and man in the middle attacks. Tight access control policies can be implemented using VortiQa Firewall to allow only authorized traffic to and through the gateway. DoS/Cyber Attack check can be enabled on the Firewall to protect the Home Energy Gateway and the internal network from well know D/DOS attacks. VortiQa AIS can be used to

control/rate-limit application traffic eg P2P, Social Networking Application. Security concerns at the Home Energy Gateway and the suggested solutions are summarized in Figure 6.

Security Consideration	Proposed Solution
Data Integrity/Authentication	VortiQa IPSec/IKEv2
Data Confidentiality/Encryption	VortiQa IPSec/IKEv2
Non-Repudiation	VortiQa IPSec/IKEv2
Reply-Man-in-the-Middle Attacks	VortiQa IPSec/IKEv2
Identity Check	VortiQa IPSec/IKEv2
Availability/Denial of Service	VortiQa Firewall
Access Control	VortiQa Firewall
NAT	VortiQa Firewall
Application Detection and Control	VortiQa AIS
Trusted/Secure Boot	Freescale's Secure Boot Arch
Anti Tampering	Freescale's Anti Tampering Sensors




Fig. 6. Summary of Security on the Home Energy Gateway

2.3 Securing WAN (Concentrator-to-Sub Station/ Utility Servers)

The communication between Concentrator and the Sub Station can happen on one of the several WAN technologies like WiMAX, 3G/4G, PLC. This communication is predominantly IP based and data travels over the Internet. This sensitive bi-directional data i.e. from the Smart Meter to Utility and vice-a-versa has to be protected from eavesdroppers to maintain confidentiality and integrity. As this link is critical to transfer real time data, to ensure reliability it recommended to have a fail over connection. Critical messages from/to the meter must be prioritized over other traffic. The transient data on the concentrator has to be protected in case of crashes. Further the Concentrator has to be protected from DOS attacks, bad traffic and unauthorized access. As in case of Smart Meters, since Concentrators are deployed outdoors they have to be protected against physical attacks and tampering.

2.3.1 Platform Solution for Concentrator

Freescale P1025 QorIQ[6] processor 667MHz/800MHz dual core device with memory up to 128 MB of NOR/NAND flash memory, Security Accelerator, running VortiQa Firewall, IPSec, IKEv2 and Application Identification Software can be used as a Concentrator as shown in Figure 7 delivering security and high performance.

This platform has 3G, WiFi, Zigbee WSN communication and 3 Giga-bit Ethernet capable ports to enable WAN/LAN communications and can communicate with Smart Metering devices via the industry standard Device Language Message Specification (DLMS) (IEC 62056). It offers Zigbee wireless connectivity to meters and 3G Broadband to Utility server. This device has energy efficient passive cooled design and has ruggedized, weather resistant construction.

2.3.2 Platform Solution for Sub Station/Utility Servers

Freescale P4080[7] QorIQ processor 1.5 GHz eight core device with Security Accelerator and Packet Matching Engine, running VortiQa Firewall, IPSec, IKEv2

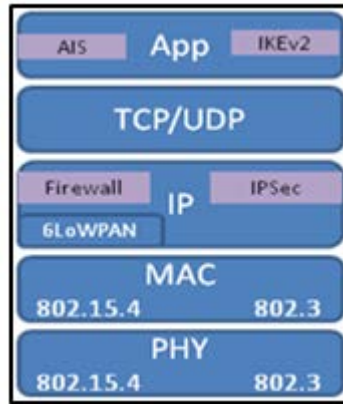


Fig. 7. IP Stack with 802.15.4 and 802.3 on Concentrator

and AIS-Application Identification Software can be used as a Utility Server. DPAA on P4080 delivers high performance with acceleration for the following functions:

1. Packet parsing, classification, and distribution
2. Queue management for scheduling, packet sequencing, and congestion management
3. Hardware buffer management for buffer allocation and de-allocation
4. Encryption (SEC 4.0)
5. RegEx Pattern Matching (PME 2.0)

These devices can be "clusterstered" at the utility to provide load balancing and failover for reliability and performance.

2.3.3 Network Topology and IP Addressing: WAN

The Concentrator's WAN interfaces get DHCP v6 addressed from the Sub Station. This connection can be 3G/LTE WiMAX, PLC. For greater reliability two links to the Sub Station can be provisioned using VortiQa Load Balancing and Fail Over (LBFO).

2.3.4 Security on the Concentrator and Utility Servers

Concentrator plays a key role in aggregating data form the Smart Meters within its area and propagating it upstream to Sub Station or Utility over the WAN link. This data traveling over Internet has to be encrypted for confidentiality and privacy. A secure IPsec VPN-Virtual Private Network tunnel can be established between Concentrator and Sub Station/Utility using VortiQa IPsec/IKEv2. Since IP address at Concentrator is dynamically assigned IRAC can be used for IKE exchanges. This tunnel provides data confidentiality, integrity, non-repudiation and protection against replay and man in the middle attacks.

ACL-Access Control List, can be configured on the Firewall to limit traffic from Home Area Network to the Utility and vice-a-versa to pass through Concentrator. ACL should allow traffic from Smart Meter to Concentrator and vice-a-versa to allow active communication between these devices. DoS/Cyber Attack check can be enabled on the Firewall to protect the Concentrator from attacks and report such attacks to the utility.

VortiQa AIS can be used to protect the Concentrator for bad and malicious traffic, AIS has a rich set of signatures to detect bad traffic, P2P application, vulnerabilities and exploits of protocols like HTTP, FTP, SSH. On detection of bad traffic action can be set to drop such traffic and inform utility.

Freescale Secure Boot/Trusted Boot Architecture can be used to prevent malicious firmware upgrade. Freescale’s Anti Tampering sensors can be used to protect from physical attacks and tampering..

Security configuration on the Sub Station and Utility server is pretty much similar to that on the Concentrator. In cases where the WAN IP address of the Sub Station is configured manually and known to the Utility server site-to-site IPSec can be configured instead of IRAC. Though most equipment including the surveillance cameras are in premise there are relatively well covered from physical attacks it is recommended to have anti-tamper sensors. Transmission line sensors are deployed on the transmission lines. Anti tamper sensors should be used on these sensors where the lines run above ground to detect and report attack.

Quality of Service (QoS) must be configured on the Concentrator, Sub Station and Utility server to prioritize critical messaging data over other traffic.

Security concerns at the Concentrator and the proposed solutions are summarized in Figure 8.



Security Consideration	Proposed Solution	
Data Integrity/Authentication	VortiQa IPSec/IKEv2	
Data Confidentiality/Encryption	VortiQa IPSec/IKEv2	
Non-Repudiation	VortiQa IPSec/IKEv2	
Reply-Man-in-the-Middle Attacks	VortiQa IPSec/IKEv2	
Identity Check	VortiQa IPSec/IKEv2	
Availability/Denial of Service	VortiQa Firewall	
Access Control and NAT	VortiQa Firewall	
QoS	VortiQa TM	
Application Detection and Control	VortiQa AIS	
Malicious firmware upgrade	Freescale’s Secure Boot Arch	
Tampering, Physical attacks	Freescale’s Anti Tampering Sensors	

Fig. 8. Security Solition on Concenretaoor

3 Summing It Up

The secure platform solutions proposed in this paper facilitate distribution grid automation which provides improved monitoring and visibility of a Utility company’s large distributed assets. Such remote monitoring capabilities serve as a key motivation for the Utility as it results in significantly improved ROI.

For example, AMI (Advanced Metering Infrastructure) with automated smart data concentrators and transmission line monitoring sensors can improve the business operations such as DR (Demand Response) to prevent brown-out and does not require significant behavioral change by customers. Benefits to the Utility company are: reduced downtime, faster service restorations, rapid identification of faults for preventive maintenance.

Figure 9 summarizes the Freescale’s Secure Platform Solutions for Smart Grid.

Freescale Secure Platform Solutions for Smart Energy				
Security Concern	Home Energy Gateway	Smart Meter	Concentrators	Distribution
	Proposed Solution			
Data Integrity/Authentication	IPSec/IKEv2	IPSec/IKEv2	IPSec/IKEv2	IPSec/IKEv2
Data Confidentiality/Encryption	IPSec/IKEv2	IPSec/IKEv2	IPSec/IKEv2	IPSec/IKEv2
Non-Repudiation	IPSec/IKEv2	IPSec/IKEv2	IPSec/IKEv2	IPSec/IKEv2
Replay Attacks/ Man in the middle Attacks	IPSec/IKEv2	IPSec/IKEv2	IPSec/IKEv2	IPSec/IKEv2
Identity Check/Data Source Authentication	IPSec/IKEv2	IPSec/IKEv2	IPSec/IKEv2	IPSec/IKEv2
Availability/Denial Of Service	Firewall	Firewall	Firewall	Firewall
Vulnerability and Exploit	Firewall+AIS	Firewall	Firewall	Firewall+AIS
Access Control	Firewall	Firewall	Firewall	Firewall
Unauthorized Firmware Upgrade	Secure Boot Arch	Secure Boot Arch	Secure Boot Arch	Secure Boot Arch
Anti Tampering	NA	Anti Tampering Sensors	Anti Tampering Sensors	NA
Hardware Platform	MPC 8308	MC1322x	P1025	P4080

Fig. 9. Secure Platform Solutions for Smart Grid

VortiQa[2] security software Firewall, IPSec, IKE runs on standard SMP Linux and is fully integrated with PowerQUICC III and QorIQ processor architectures to deliver optimum network performance under both normal and stressful network conditions. The software is optimized to leverage SoC hardware acceleration functions of the Freescale processors, such as the security (SEC) engine for VPN processing, pattern matching engine (PME) for IPS and the data-path acceleration engine for flow management to achieve high throughput and high session rate processing to meet the demanding security, performance and scalability requirements of the Smart Grid.

4 Conclusion

This paper has covered security concerns at various layers of Smart Grid and proposed end to end high performance security solutions viewing Smart Grid as a system. The four pillars of network security (specified by NIST SP 800 82, NERC and IEEE) are addressed in the proposed platform solution:

1. Integrity: Prevent unauthorized modification of information
2. Availability: Prevent DOS (Denial of Service)and Intrusion Prevention.
3. Confidentiality: Prevent unauthorized access of information
4. Non-repudiation: Prevent denial of action.

The secured M2M, IOT solution provided here is not limited Smart Grid, this model can be adapted and extended to other applications/markets like:

1. Gas and Water distribution
2. Health, Residential and Transport
3. Factory Automation
4. Securing Enterprise and Data centers

References

1. Stouffer, K.: Guide to industrial control systems (ics) security (2011)
2. Vortiqa software for networking equipment, <http://www.freescale.com.hk/files/32bit/doc/brochure/VORTOVRBR.pdf>
3. Kent, R.A.S.: Security architecture for the internet protocol, rfc 2401 (1998)
4. Kaufman: Internet key exchange (ikev2) protocol, rfc 4306, (2005)
5. Mpc8308 networked smart gateway reference design, http://www.freescale.com.hk/webapp/sps/site/prod_summary.jsp?code=RDMP8308NSG
6. Qoriq p1025 data concentrator reference design for energy management, http://www.freescale.com/webapp/sps/site/prod_summary.jsp?code=RDP1025DC&nodeId=0225E76A10&tab=Design_Support_Tab&site_preference=normal
7. P4080: Qoriq p4080/p4040/p4081 communications processors with data path, http://www.freescale.com.hk/webapp/sps/site/prod_summary.jsp?code=P4080