AMI Security

August 11, 2010

Luke Seewald

Version History

Version	***Date***	***Author***	***Description***
1.0	June 30, 2010	Luke Seewald	Initial Draft
2.0	Aug 11, 2010	Luke Seewald	Added Testplan details

Intellectual Property Rights and Copyright

Contents

Executive Summary

The AMR/AMI system introduces new security challenges to London Hydro. The operation of an external wireless network including communication points at every customer potentially opens the door to new security threats. These threats include denial of service, unauthorized use of assets, customer privacy issues and other unknown issues. Impacts of security failures may include interruption of operations, financial costs or damages, or public embarrassment and loss of company image.

This document presents a method for including reliable security concerns during the creation of this new network and integrating security postures into future ongoing London Hydro operations. The security problem is divided into the three stages of physical security, network security and applications security. Each separate stage is addressed through design and testing of physical assets and equipment and work procedures. Ongoing unmitigated threats or partially mitigated threats at all levels will be recorded to weigh against business planning operational impacts.

The security plan will be implemented in the three stages of implementation of internal procedures, independent internal audit, and external comprehensive threat assessment. Following initial implementation, a regular schedule of security reviews is recommended to ensure up to date technology, procedures, training, and that established London Hydro policies and work instructions are enforced.

This paper delineates projects from applications from technology platforms. Each of these items is required to have a person responsible for the security aspects. Aspects include physical access, network access and application access (including data). This includes the operation of contractors and external suppliers or partners. This person is in turn responsible to the London Hydro senior management security board. While this is a direct reporting responsibility and this paper outlines an integrated security system, security relies on the engagement of integrity driven and well trained staff.

AMI System. AMI systems consist of the hardware, software and associated system and data management applications that create a communications network between end systems at customer premises (including meters, gateways, and other equipment) and diverse business and operational systems of utilities and third parties. AMI systems provide the technology to allow the exchange of information between customer end systems and those other utility and third party systems. In order to protect this critical infrastructure, end-to-end security must be provided across the AMI systems, encompassing the customer end systems as well as the utility and third party systems which are interfaced to the AMI systems.[1]

Security is like Safety. Both are integrated operational mindsets which rely on leadership, equipment, procedures and continual review and improvement. While it not likely that security failures will result in injury or death, there are public privacy and public safety issues related to the prudent management of AMI (advanced metering infrastructure) and future Smart Grid technology operation. Additionally, safety issues are mostly about accident prevention while security must also include purposeful attacks. However, the manner by which an organization responds to these issues is similar. As such, effective security requires strategic inclusion by senior leadership. Despite the fact that much of utility security literature focuses on technological solutions to mitigate an internal threat this paper takes the position that leveraging employee trust and participation is the most effective way to create a safe and secure environment. The fact that London Hydro has health and safety considerations deeply embedded within the corporate strategy is expected to make the future adoption of security concerns easier. Also, as future smart-grid technologies are investigated, security is expected to take on an increasing strategic role at London Hydro and is a potential area to demonstrate the company's leadership within the industry.

Framework for AMI. This document presents a framework and method by which London Hydro's ICT (Information and Communication Technology) security concerns can be addressed. The scope of the paper is to include the internal and external IT infrastructure related to the mandated Smart-meter and AMI deployment. Additionally, the frameworks presented are created to be scalable and extensible to future technology deployments. The document provides:

a) the motivation and threats involved with deploying a complex external ICT network,
b) recommended frameworks and divisions for initial deployment and ongoing security evaluation, and
c) example documents, procedures and work instructions as templates for deployment.

The expectation is that if the operational elements presented within are implemented, London Hydro will be able to declare and deliver a best-in-class secure AMI system.

Threats. Threats to information systems include environmental disruptions, human errors, and purposeful attacks[2]. Information and communications systems are subject to serious threats that can have adverse effects on organizational operations, company image and reputation.

Cyberspace has been called the fifth domain of warfare, after land, sea, air and space[3]. Investment in security is comparable to the purchase of insurance to compensate for or mitigate downside risks. The recent deployment of Smart-meters and AMI systems to support the Ontario Government mandated TOU (time of use) billing and reporting requirements has introduced new risks for London Hydro. These threats include customer privacy issues, denial of service, unauthorized use of assets, and other unknown issues. The risk of a given attack is determined by the likelihood of a successful attack and the severity of the damage it may cause[4]. One main issue is confidentiality (privacy) of customer metering data over the AMI system, metering database, and billing database, to avoid serious breaches of privacy and potential legal repercussions. As well, the integrity of meter data is important, but the impact of incorrect data is not large. Additionally the availability of meter data is not critical in real-time but is required within a day or so to support supply management and financial considerations.

Customer privacy issues. In June 2010 the Ontario Information and Privacy Commissioner issued a report entitled "Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid." which outlines steps to protect customer (or ratepayer) personal information. Personal information is defined by the *Freedom of Information and Protection of Privacy Act (FIPPA)* and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). Failure to protect "recorded information about an identifiable individual" could bring public scrutiny and governmental review to focus on London Hydro's operations. Costs could include legal defense, fines or penalties, costs associated with re-implementing systems to meet privacy considerations. These issues impact legal, public relations and communications corporate functions. The overall objective is to maintain high levels of consumer confidence and public trust.[5] London Hydro's image of providing safe, reliable and economical service to the public could be at risk if there is a security compromise which impacts public trust. Other organizations may benefit if London Hydro is shown to not be reliable and trustworthy. Recent lateral example failure cases include an instance where personal health information of more than 80,000 people went missing.[6] Unauthorized release of Smart-Meter TOU information could support determining if a residence is occupied or support corporate marketing initiatives.[7] Other unknown applications could also make customer information valuable to outside parties. A systematic approach is required to identify vulnerabilities which could compromise privacy security. For example, while smart meters do not communicate any identifiable information, the flexnet ID which is used is printed on the front of the meter. Transmitted meter data when combined with separately acquired data could create an undesired disclosure of information. This in turn may define higher encryption requirements for data which does not actually contain personal information.

Denial of service. Operational impacts are very likely if unauthorized deliberate attacks on the ICT systems are successful. While internal change management processes are already in place to reduce the risk of accidental service outage, prevention and response to attacks is also required. Denial of service (DoS) is an attempt to make a computer resource unavailable to its intended users.[8] For London Hydro, this is where the desired service qualities of the AMI system are either degraded or prevented. Examples include preventing of IESO data transfer, lack of billing or business systems support activities, or maintenance activities. These service outages could be caused by tampering of a Smart-meter, RF interference of the Meter to TGB or

backhaul communication, virus, worm or other network attack. The cost of these outages may be external or internally attributed and may depend on outage severity and duration. Some outages may be difficult to diagnose and may take resources and people away from scheduled project activity. These types of outages are currently being recorded in the IS AMI FMEA (Failure Mode Evaluation and Analysis) spreadsheet.

Unauthorized Use of Assets. Some attacks may not have a detectable impact on London Hydro operations however pose a threat to the company. ICT networks have been known to be made use of for unauthorized activities. The cost of this may be theft of unutilized bandwidth for such applications as media file sharing. More severe scenarios include having London Hydro's ICT systems used for launching viruses, spam email bots or other illegal or undesirable initiatives.

Other Unknown Issues. Given that the technology today is relatively newly designed and implemented, there are many unknown security threats which may emerge as the AMI system becomes operational and is widely deployed. Meter tamper and electrical theft scenarios have not yet been recorded or assessed. HAN (Home area network) technology is not currently supported by London Hydro's Smart meter roll out. Sufficient flexibility will be required in the security plan to allow response to emerging issues.

Value of the Data. When deciding on how much resource should be put toward protecting the smart meter interval data it is necessary to question how much it is worth. This goes beyond the privacy and public security issues related to residential electricity profiling but rather seek to determine market value of the data. The market value can, in turn, be used to understand how much resource would be expended by an outside party to acquire the data. What additional insight or services could be created by an energy or market analytics company? How much would an individual residential, commercial or industrial consumer pay to access the web presentment or get the raw interval data? Would how much more would 15 minute interval data be worth than hourly data? How much less valuable is data which is one month delayed versus real-time consumption data? There is an opportunity for London Hydro to work with external parties to understand and realize the value of protecting the data.

Business Considerations. The commitment to provide AMI data reporting as mandated by IESO is to be fulfilled by this AMI system. However, security compromise or denial of service attacks may cause unacceptable RIS (read interval success) levels or data delivery service outages. Currently there are no consequences or financial penalties for data delivery outages. Because of this items such as redundancy, hot-standby swappable components, emergency service contracts, 24-7 hour outage, and disaster recovery are not considered. Availability and recovery will be considered best-effort and will be weighed against other business priorities.

Background Material. There are several basic security concepts which are presented to allow the background material necessary for the plan. These are presented to ensure a baseline of knowledge of security principles. The critical characteristics of information include the availability, accuracy, authenticity, confidentiality, utility, integrity and possession. The

components of an information system include all the involved hardware, software, data, people, procedures, and networks[9]. Basic principles include the following:

Need to know. This expression embodies the principle that only the minimum set of required information system components be made available to complete a task. This requires that there is clear task definition and an understanding of the ICT requirements for a defined task.

Ugo+rwx. This string is a networking concept from UNIX systems which controls file permissions attributes. The first three letters represent user organization as follows:

1) the 'u' represents an individual user which is authenticated by a username and a password.
2) the 'g' represents a group of users which can be defined to allow every member of that group various permissions. Users can be added or removed from groups my authorized system administrators.
3) The 'o' represents other or all users of a system. This can be used to enable common programs or publically available file permissions.

The second three letters indicate the types of permissions which are granted to users and include:

1) The 'r' represents the permission to read a file, folder or directory. Without this attribute, the user can not read a file or gain access to the information.
2) The 'w' represents the permission to write a file, folder or directory. Without this, an object is read-only.
3) The x indicates if a program can be executed.

The importance of this construct is to be able to define individual or groups of authenticated users and provide the desired kinds of access. With exception of time expiration, this construct frames the partitioning and allocation of user permissions.

This message will self-destruct[10]. This is a line taken from a security minded television series. It refers to messages which get destroyed after an expired time period. Time expiry can apply to physical security access, passwords, specific permissions, software licensing, data backup and oversight review procedures. Considerations of time expiry need to be assessed and implemented at the time of security granting such that there is no later neglect of security privilege removal. Using time constraints can reduce the security risk.

Secret or Top Secret. Security classifications are often used by government to segment information to be handled differently. The costs of time and resources to secure information can be managed in a way proportionate to the downside risk or impact of undesired information disclosure. The classification process itself provides value by doing risk analysis on individual security elements or on combination of security elements. Classification of security applies to information as well as to application access, network privileges and decision making authority. The following three classifications are used by the Ontario government[11] and are recommended for use in London Hydro:

a) **Unclassified.** Public information. Internal communications.
b) **Low Sensitivity.** Information that is only sensitive outside London Hydro. Generally available to employees and approved non-employees.
c) **Medium Sensitivity.** Information that is sensitive within the operations and is intended for use only by specific groups of employees.
d) **High Sensitivity.** Information that is extremely sensitive, of highest value to London Hydro or external partners and intended for use by named individuals (positions) only. Documents that can create an identity.

Elvis has Left the Building. When people leave the organization or transfer job function, this triggers a staff change event which needs to be considered in a security context. It is not appropriate to allow former employees access to operational systems in perpetuity. A staff change event may trigger the removal of login accounts, the change of passwords or physical locks, or more comprehensive change in the naming or configuration of sensitive systems. This concept may also be applied following system acceptance testing by vendors or contractors who have intimate knowledge of systems or equipment. In this case, once a system is installed or configured and the contractor is no longer involved, the system is re-configured, passwords changed, and documentation updated. This prevents vulnerability if supplier's information is compromised.

System Development Lifecycle Framework. As shown in Figure 1. The SDLF (System development Lifecycle Framework has been selected as a method to include security concerns across the AMI system. This model was selected due to its strengths in control, documentation, and ease of maintenance. Since the AMI system has been mandated and already mostly implemented, the rigidity and formality of the framework are of less concern. The AMI system is divided into sequential phases. Emphasis is on planning and implementation the security of the entire system at one time. This allows tight control is maintained over the life of the project through the use of extensive written documentation, as well as through formal reviews and approval/signoff by the user and security management occurring at the end of most phases before beginning the next phase[12]. These stages allow the overlay of management approvals, change management, data flow, and reconfiguration. It also allows the integration of security considerations (London Hydro's Security Information Management System (SIEM)) with other operational, performance and business lifecycle considerations.

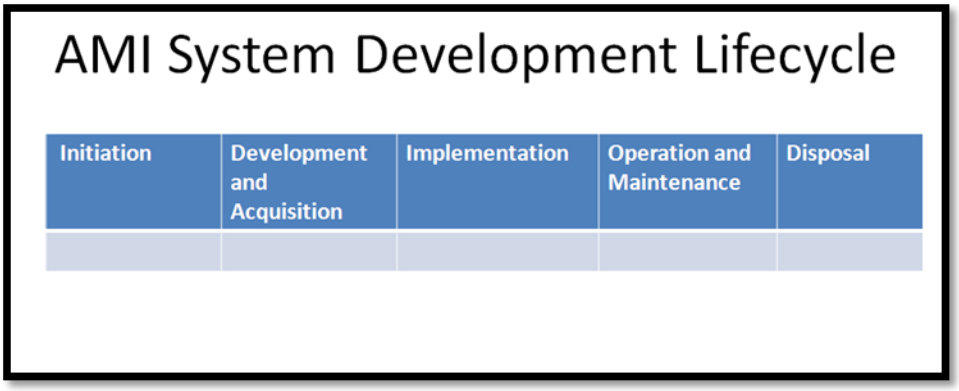

Figure 1. AMI System Development Lifecycle Framework Stages

Security Segments. While there are many types of security including physical security, personal security (i.e. safety), operations security, communications security, network security and information security. For simplicity and operational effectiveness it is recommended that the WBN and AMI system be segmented into the three segments of physical security, network security and application security.

Physical Security. For both internal and external ICT equipment, the physical access and security can be managed in a physical way. This segment includes the management of authorized access to equipment, enclosures, cabling, conduit, and associated authorization,

keys and review. London Hydro relies on contracted security company for monitoring company grounds and after-hours rounds. ID badges and electronic locks provide this security for internal purposes. However, external equipment may be in controlled areas, but open to external organizations, partners or suppliers such as the City of London or apartment building property managers. Physical security concerns relating to management of the AMI/WBN system shall include the following:

1) **Computer Access.** Physical access to London Hydro computer terminals is limited to authorized physical access. This access includes full time union and non-union staff, students or temporary workers, probationary workers, contract staff and support staff (such as facilities and janitorial services). This service is provided by contract security services and authorization is coordinated with department managers and employees.

2) **Internal ICT Security.** Physical access to internal ICT infrastructure server equipment which is contained in secure data center area. Given the sensitivity of the Data center and its importance in supporting operational business systems, including the AMI system, the following physical security considerations are recommended:
    a. Access to the RNI system and Data center shall be limited to required personnel.
    b. Director level approval is required for access to the data center.
    c. Regular work on installed equipment shall be performed remotely where possible.
    d. A periodic review of the access list be reviewed in context of work tasks.
    e. Access to the Data center be granted based on periodic expiry of access which can be renewed based on re-approval.
    f. Installation of security cameras within the Data Center.
    g. Sign in logbook or badge swipe recorder to log escorted access by guests or other parties.
    h. Intermittent testing of security procedures to ensure correct operation of security features.

3) **External ICT Security.** Physical access to external ICT assets requires different measures than the ones employed for internal ICT infrastructure as the assets are remote from operational staff, may not be on London Hydro property or may be located in shared facilities. The following physical security concerns are recommended for external IT infrastructure:
    a. Any access to external infrastructure including inspection, maintenance, upgrades, or other reasons be coordinated and logged centrally an include time, date, details of visit and names (an organization) of parties visiting the location.
    b. All assets be secured by lock and key. Were possible, separate chain fence cages shall be installed to secure Hammond/Server/TGB cabinets, power supplies.
    c. Keys which allow secure access to external AMI/WBN assets be centrally managed through facilities management and authorized by functional management.
    d. Security inspections be conducted with regular maintenance inspection schedules.
    e. Periodic re-keying, lock rotation or replacement be performed at a set time interval or following a personnel change event.
    f. The physical security of the AMI smartmeters is covered through the ongoing maintenance and operating procedures of the London Hydro metering department.

Network Security. The ICT network which supports the AMI and WBN requires controls to maintain secure and authorized use. The external IT and wireless nature of the AMI and WBN networks are particularly vulnerable to security issues because it is geographically distributed across the City of London. AMI smart-meter sensor and communications devices are in customer locations and are thus subject to tampering, interference and other possible external interventions.

AMI Platform. While the focus of this section is on network security, another way to look at the AMI system as it moves forward is that of a platform. Such a platform can enable an internally provisioned service level architecture (SOA) which could provide centrally managed service to internal or external organizations[13]. The AMI network is in effect a platform for different business applications which rely on information and communication technology to operate effectively. This is depicted in the diagram below. Currently, there is only one source of information (i.e. electric interval/delta measurements). In future there may be additional sources or applications depending on this AMI platform. In computing, a platform describes some sort of hardware architecture and software framework (including application frameworks), that allows software to run[14]. The security level of the network must be designed and tested commensurate with the requirements of the applications the network supports. If multiple applications are supported by a common network the application with the strongest security requirements dictate the minimum security requirements. Alternatively a network may be divided to separately support diverse applications. Also, the fact that multiple applications are hosted by the same platform shall not allow application security to be compromised. The principle is to avoid the weak link. The effort spent on protecting the various interdependent security objectives required for a system has to be distributed so that all mechanisms facing an attacker are of comparable strength[15]. Figure 2. depicts the AMI platform and application graphically. This division allows the security issues to be addressed from an end to end perspective as well as to divide the network into discrete components to define security for individual elements. This model also allows the definition of service agreements or platform requirements to be understood, documented and controlled. As additional security demands are made on the platform, the platform can adapt to changing requirements.

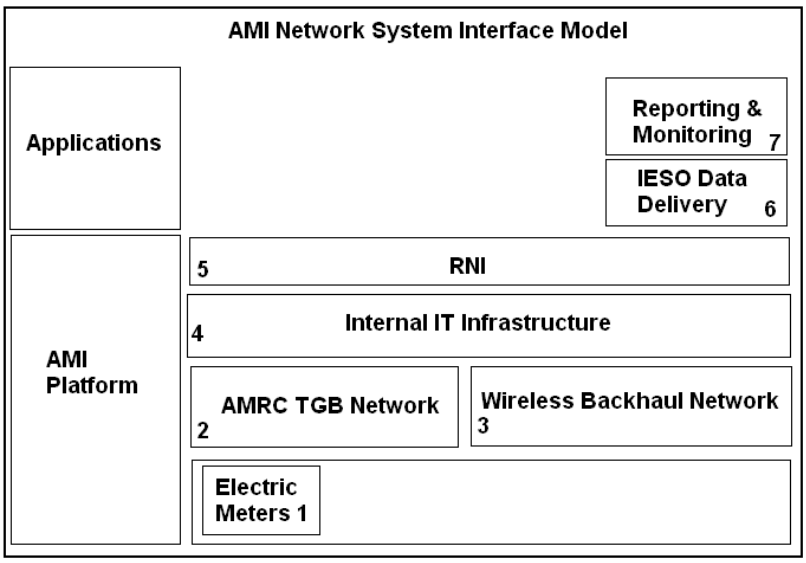

Figure 2. AMI Network System Interface Model

Network Element Security. The AMI system has been divided into 5 sections all of which have an essential role in supporting London Hydro's business applications. Security aspects for each section are further segmented below using the System Development Lifecycle Framework. The operation and maintenance phase is the focus of concentration. There are several common network security recommendations to all the sections of London Hydro's AMI system:

1) Password Management[16].

a) A particular user should be allowed one and only one password for a given computational resource. This means that the same password shall not be used for multiple systems or for personal uses.

b) The size of the password and the character set shall be strictly enforced.

c) The passwords shall be changed periodically and upon special events as required.

1) Assignment of AMI security custodian duties be formally assigned to include physical and device network/communication security[17].

2) Participate in Vendor and industry smart-meter security forums and report on latest risk and technology changes in the security industry.

3) Establish and maintain an available log of potential, temporary or permanent security compromise (loss of control[18]) including physical tampering, modification, signal spoofing, RF/Network interference, or transmission interception.

4) Establish and maintain security controls around internal operations support resources such as device documentation, security investigation and vulnerability reports, control of device administrator tools, equipment and resources.

5) Conduct periodic internal security review and include external audit expertise as required.

6) Reporting to London Hydro Senior Leadership security committee.

Electric Meters. The network security of the electric meters actually relies mostly on physical security measures (i.e. tamper seals and controlled inventory measures). Security measures related to the meters are important to deter energy theft, maintain the integrity and availability of reporting for billing[19]. Cisco Systems sees Fraud Prevention, and Privacy[20] to be two of the main threats to the electric utility industry. There are significant concerns about HAN (Home Area

Networking) with regard to authentication and security if London Hydro were to communicate with consumers' in home devices. This is not currently implemented, but such a service offering would be included in AMI network security lifecycle planning. The installed smartmeters are capable of 128bit encryption which is currently not enabled. The security decision making and operation of the meters is addressed by establishing several AMI common or specific recommendations. These include:

1) Participate in the Sensus security subcommittee activities to receive the latest meter security information.
2) Ensure the following Sensus Meter Encryption Parameters are set to the proper values:
    a. crypto.EncryptByDefault – set to True
    b. crypto.AllowUniqueKeyRotation – set to …TBD
    c. crypto.GroupKeyRotationPeriodDays – set to …TBD
    d. crypto.HanKeyRotationPeriodDays– set to …TBD
    e. crypto.SharedKeyRotationPeriodDays – set to …TBD
    f. crypto.UniqueKeyRotationPeriodDays – set to …TBD
3) Monitor Meter Tampers including meters which fail due to electronic failure (i.e. CMEP Meter Level Alarms)[21] This includes malfunctions, leaks, endpoint mismatch reports or bad reads. Suspicious incidents shall be logged in docushare and reported.
4) Manage UMKs (Upgrade Management Keys) or other license security solutions.
5)

AMRC TGB Network. Beyond the physical security considerations of the 9 TGBs are the network security concerns. Because the TGBs are the second half of the RF communication network with the population of smartmeters the TGB network security issues are closely related to that of the smartmeters. Here are some of the TGB specific security recommendations:

1) Ensure controlled user password access to the TGBs. Common team passwords are not sufficient to identify and authorize individuals and thus limit access to approved tasks.
2) TGB FlexNet uses a combination of shared, group and unique 256bit AES encryption keys. These keys must be verified and rotated regularly. Storage of the keys shall be securely stored.
3) Enable and manage SNMPv3 configuration and create applicable tgbuser.[22]

Wireless Backhaul Network (WBN). The WBN is a standards based (802.11a) 5.8GHz backhaul network. It uses point to point and point to multipoint microwave links. The network security is provided by the following:

1) The WBN is installed on towers and rooftops which are physically secure.
2) Several of the links use high gain directional antennas which prevent RF interference or intercept.
3) The system is closed and does not allow access from other than the approved set of 14 WBN nodes.
4) Data flows from wire connected TGBs to London Hydro internal infrastructure. There is some back channel and control, but the AMR/AMI traffic is predictable and uniform.
5) There are redundant paths built into the system to allow for outage and maintenance.
6) Currently the WPA2 128bit AES encryption key.

Internal AMI IT Infrastructure. The supporting Internal IT infrastructure supports much more of London Hydro's operations than just the AMI System. However, the Security of the Internal network must provide adequate security to protect the AMI system and prevent or mitigate any Cyber Incidents. NIST defines a Cyber Incident as: "An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional." Also, NERC has several CIP (Critical Infrastructure Protection) Requirements. These are in a further detailed section outlined below. It is well known that hackers or crackers can:

1) Crack passwords,
2) Probe systems, automatically uncovering known vulnerabilities, and
3) Capture, display and spoof selected LAN traffic.

It is up to London Hydro system administrators to actively impose barriers to effectively:

1) Prevent unauthorized access to system applications and data. Access to the AMI system (WBN, TGB, RNI) shall be controlled.
2) Protect the integrity of the data.
3) Protect the privacy of the AMI data.
4) Screen out viruses, Trojan horses, worms, bots and spyware.
5) Screen out denial of service traffic.

Security Tools and Technologies. The major tools used to protect London Hydro's networked systems include:

1) Firewall systems. In general, a firewall filters out unwanted traffic. It can prevent external computers from connecting to applications running at internal computers. Also a firewall can provide a barrier that hides the identities or the existence of internal computers[23]. Firewalls can provide router filtering, host filtering, application proxies and stateful screening. London Hydro's firewall can route traffic or datagrams based on a set of rules. Only authorized IP addresses, protocols, source/destination ports or initiation side are permitted. Firewalls may also be configured to provide network address translation (NAT) services.
2) Authentication Mechanisms. These are used to identify users reliably, protech passwords, and provide a way to detect whether a hacker has altered data stored on a disk or sent across a network. One method is to create message digests to authenticate users, verify data integrity and construct digital signatures.
3) Encryption. Encryption at several layers of the system may be implemented including using radius servers, using a public key encryption system or using SSH to secure smart meter data flow.

NERC CIP Requirements. While the NERC Requirements may not be enforced by London Hydro they provide a rigorous framework for organizing cyber security issues. For example: Standard CIP-003-2 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. The following NERC CIPs are particularly

applicable for London Hydro's AMI network[24]. Each contains requirements, sub-requirements, measures and information about compliance:

1) Standard CIP–002–2 — Cyber Security — Critical Cyber Asset Identification
2) Standard CIP–003–2 — Cyber Security — Security Management Controls
3) Standard CIP–004–2 — Cyber Security — Personnel and Training
4) Standard CIP–005–3 — Cyber Security — Electronic Security Perimeter(s)

Intrusion protection and Identification. The Internal network must also be capable of detecting and reporting any network intrusions. Figure 3. below illustrates the AMI network which shows the external infrastructure portion. If the wireless networks are not able to protect and secure the authorized functions the Internal IT infrastructure must be able to provide a defense in depth approach to protect the security of the RNI system and other London Hydro systems and applications.

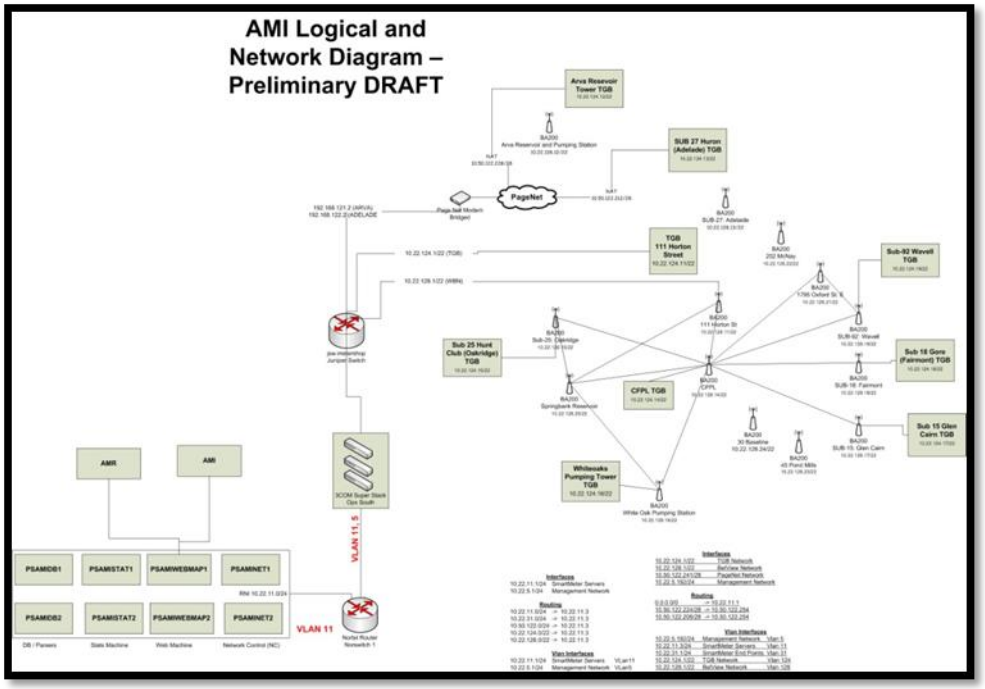

Figure 3. AMI Logical and Network Diagram

Sensus RNI System. The Sensus RNI (Regional Network Interface) is the most important AMI asset as this system contains all the combined meter data for the City of London. It also provides the central control of the smartmeter configuration and the services on which the applications depend. Of all the AMI network pieces, the RNI is the piece which requires the highest security. RNI security considerations include:

1) A member of London Hydro shall represent at the Sensus Security user group.
2) Data management for all applications is centralized for provisioning.
3) User account access is managed and reviewed.

AMI System Security Events. Security events are situations which trigger security related reviews or actions. Procedure documents for security events shall be described in separate documents in full detail. Examples of security events include:

1) An employee or contractor leaves or gets assigned to a project or AMI role.
2) A major security breach occurred.
3) A major system upgrade has happened For example, the last RNI software upgrade changed the user accounts and many of the related permission grants. These needed to be re-evaluated following the upgrade.
4) A pre-decided time interval has passed.
5) A new application is added to the AMI system.

Operational Security. The design and definition of London Hydro's business and operational applications can contribute to the overall security of the AMI/WBN network. The security of the applications is addressed through the chosen System Development lifecycle framework. Each application proposed to be supported by the AMI system needs to define the security risks, requirements and organizational structure. For example, an application security custodian role is defined for the application. The custodian role is likely to be the project manager of the business system within the functional organization. Security service level agreements are to be drafted and agreed upon between the application owner and the platform owner. Because security, like reliability and responsiveness, is a feature of IT systems that requires companies to weigh the level of protection against the amount they are willing to spend. Increasing security involves not only higher costs but also greater inconvenience. It is up to senior managers to assess those trade-offs.[25] These business decisions must be made early in the application definition stage. In addition to functional and system performance service levels the following security aspects shall be included. The following lists requirements for applications and is structured using the System Development Lifecycle Framework:

Initiation. The initiation stage of an application is important because concepts and ideas are still fluid and can be changed without additional cost. A draft concept description, list of requirements, use models or flowchart prototype can express the basic or minimum functionality can aid in expressing the concept. This can also allow the consideration of security concerns such as the following:

a) Who is going to look after the application security issues? Identify a permanent or intermediary internal security authority for the project.
b) What systems or information is needed? Create an Application Security Profile which contains a description of the data, network, platform or information required.
c) Who is going to use, support or maintain the application? Identify internal resources (i.e. IT infrastructure) to assist in security assessment and feasibility.
d) What security concerns are there? Conduct security classification of the data or information input, processed or outputted.
e) When is the application needed? Establish a security review schedule project plan.

Development and Acquisition. The application is further refined at this stage. The security considerations associated with the application also move from theoretical planning to implementing security controls an developing tests and procedures. These include:

a) Set security specifications which allows for practical testing of the application.
b) Select credible external parties including contractors, regulators or customers who meet security requirements. Security or trustworthiness shall be included in RFP requests.
c) Perform background checks on contractors, subcontractors or workers as required.
d) Ensure suitable NDA or contract clauses are in place to ensure or motivate security compliance.
e) Identify security risks during the build or engineering stages as well as for final end-build access.
f) Participation of outside (or inside) parties may be partitioned or segmented such that one organization or party does not have full specification of the entire system. Of course, architecture of the partitions must allow for lower level optimization flexibility and linear dependencies.
g) Procurement of external security design, audit or test expertise may be included at the development stage to provide input prior to implementation to strengthen security or to improve testability.

Implementation. During the operation stage the security concerns relate to managing the following security concerns:

a) Identify users who are permitted select authorized access.
b) Identify implementation staff with time limited authorization or build permissions which expire. For example a contractor VPN.
c) Control information release and controlled design and build documents.
d) Provide external protection or security while the system or application is being built. This can be done before and while it is being brought online and commissioned.
e) Following the implementation or at intermediate milestones, a security review may be held to ensure that all planned measures have been implemented and are operational and to review if un-anticipated functionality or operation requires review.

Operation and Maintenance. The steady state operation and maintenance of an application shall include the following security concerns:

a) Maintain a list of all permitted users of the system including a description of job or task function, information required when performing the job, and any formal permissions granted.
b) Maintain a list of all passwords, authentication keys or other access required.
c) Maintain a list of any application defects, error conditions, known security lapses or compromises.
d) Maintain procedures for adding or removing people from application access or permissions.
e) Reviewing security measures when upgrading or making fundamental changes to the application operation.
f) Periodic review of permissions and authorized access. (minimum once per year).
g) Conduct security rehearsals or refresher training to ensure skills are available.
h) Regular communication with vendors or suppliers to ensure awareness of known or theoretical security defects or events.
i) Any data or application backup or destruction/shredding is carried out in accordance with data classification.

Disposal. During this stage the following considerations apply:

a) Ensure decommissioning or disassembly does not impact security of other applications.
b) Platform support may also need security
c) Conduct end-of-life security review as part of decommissioning.

End to End Security Measures. In addition to piecewise security on application or system components there must also be an overall system security audit. Often this should be done by an individual or organizations which did not test the system components, but may require informational access understand how to test the system. Outside parties may be particularly suited to this Combinations of individual system component weaknesses, including human factors, may be exploited. Here are several tests which may support this:

***Staff centered review*.** In the above cases, the view has been about the application or platform and who has access. This review looks at a particular person and lists all the applications, access or system access they have to support daily duties. Job descriptions may be changed to ensure that no one person has access or control of all London Hydro's systems and that there are at least two person (primary and backup) on each system to allow for alternate access.

Alternate and backup system review. From a security perspective, if a system is compromised, a backup or fall-back system may be relied upon to maintain system or application availability. Use-cases can be employed to drive what-if scenarios to seed discussion or planning about backup or contingency systems[26]. Some extreme use-cases popularized in major motion pictures may be deconstructed and used to seed "what-if discussion"[27].

Exception handling. Unforeseen operational states may not be found until a system or application has received extensive in field testing. Consider any lockout scenarios or out of normal operations. Ensure special case scenarios are documented and assessed for security handling.

Security Testing Stages. The following three test stages are recommended:

1) Internal documentation and procedures included in application design requirements. The recommendations within this document largely outline this stage. Additionally included are the forms or records associated with incidents, inspections or other changes to the system.
2) London Hydro internal security audit and documentation. This is similar to ISO type audits which includes presentation of procedures and operation to an internally selected audit group.
3) External threat assessment and security audit.

London Hydro Organizational Structure. The following organizational roles are recommended for clear security responsibility within the organization:

1) AMI Platform prime. This role is responsible for the Information and Communication Technology security issues. This role can also be the business owner or manager of the equipment or system.

2) Application prime. This is the business application owner who is responsible for the security issues of the business application. Often this role coordinates the internal users and records permissions in relation to job functions.
3) Senior leadership Security form. This group performs the final review and oversight of the security strategy. It fulfills the risk executive function and includes the security issues.

Training and enforcement. Once the appropriate security measures are selected and agreed upon and approved a communication and training package is to be created. This package must clearly state the goals of the security program in place. New employees shall be provided with security concerns when trained on a system. Items to be covered during training include:

a) Reporting process if there is a witnessed or suspected security issue with respect to IT equipment: call helpdesk
b) Prudent use of IT equipment including transferring files offsite and use of portable hard drives and USB sticks for data transfer.
c) Password selection and management (i.e. same password for multiple services.)

AMI Implementation Project Outline. Due to the ongoing development of the AMI system and network three stages are proposed for the development and inclusion of security considerations. The staging of the testing allows for early testing of completed components to reveal risks and vulnerabilities while the system is in development. It also allows the organization to build up security expertise and awareness into the project.

1) **Phase I** – WBN and AMI internal infrastructure testing. Testing to begin in September 2010 upon completion of the internal firewall project.

a) Test of the WBN wireless network encryption. The WBN BelAir 802.11a radio currently uses a closed (non-access) 128 bit WEP encryption[28]. The network nodes are fixed members of the network set by wired TGB (AMRC) locations and radio repeaters. This standards based network provides the data backhaul capability to the AMR/AMI system. The testing of this network is performed through an external threat assessment and security audit. For the WBN this includes an infrastructure review, testing of encryption algorithm strength and wireless penetration testing. The infrastructure review includes a review of the security of the devices that make up the wireless network, access points, controllers etc… The encryption review includes an evaluation of the type and strength of the algorithm used to encrypt data on the wireless network[29].

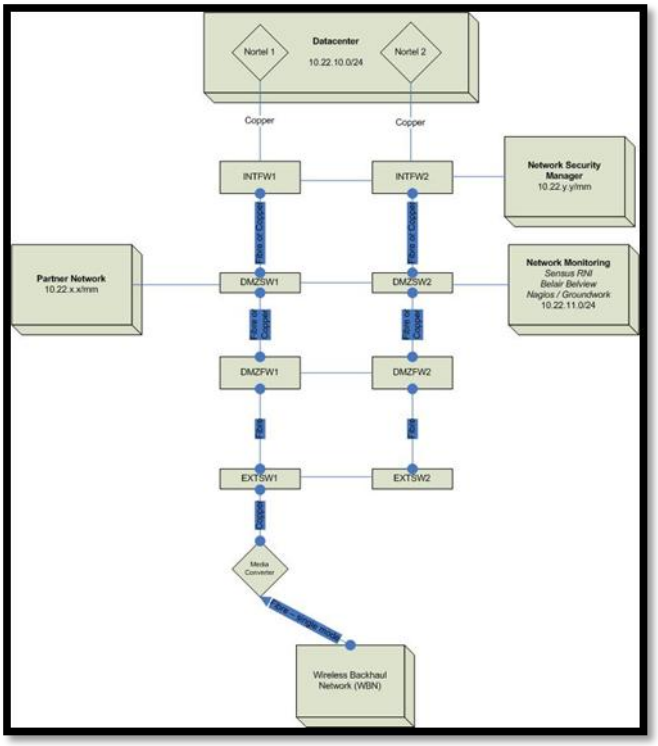

Figure 4. Logical Diagram of London Hydro's AMI Firewall

b) Test of the AMI internal Firewall system. Figure 4 shows the planned Firewall and DMZ (demilitarized zone) which has been designed to protect London Hydro's internal corporate network from the external AMI network. This project is to be implemented by London Hydro's internal network infrastructure group in the late August 2010 timeframe. Testing of this feature will be done through an external evaluation of the infrastructure security, authentication and authorization and an evaluation of the overall design. The Infrastructure Security review will include a review/assessment of the security of the devices that make up the access points and controllers etc… The authentication and authorization component reviews the authentication mechanisms that control access to the DMZ and internal network Access control mechanisms will be reviewed to determine what, if any, restrictions are placed on clients devices that are connected to the external network. Assessment of the overall design of the wireless network will be against industry and vendor best practices. Any recommendations will be made for any deficiencies discovered. From the data collected during the assessment phase, each piece is assembled, categorized and analyzed. The result is that all of the data is in a format which allows for the preparation of the final evaluation result.

Phase II – Testing to begin in Q1 2011

a) Test of the Smartmeter wireless network. Sensus 256bit AES wireless encryption is expected to be available in the Sensus RNI software version 2.0.6 or 2.1.0 in Q4 2010. This feature is recommended to be installed prior to security testing so that the latest operational version is the one to be evaluated. Due to the fact that the 900MHz is licensed and the data protocols are proprietary testing is expected to be internally evaluated in conjunction with the

vendor. External security consultants which London Hydro has used previously are not prepared to test and evaluate the technical security of these proprietary wireless networks. An additional service supplier or partner must be found which has the expertise and ability to provide such specialized testing. Similar to Phase I, testing of the smart meter network shall include an external evaluation of the infrastructure security, authentication and authorization and an evaluation of the overall design.

b) Test of the LH public internet web presentment security (Currently in Design/Development) This component is still in the early stages of project definition and project plan will depend on implementation. However, the above stated privacy concerns apply strongly to this area and it is recommended that security concerns be considered using the SDLC framework.

Phase III – Testing in Q2 2011

a) Full End-to-End testing of the whole AMI system.

b) Testing and Audit of approved security procedures (yet to be defined)

Appendix A: Additional Security Standards

AMI SRS v1.01

FIPS PUB 120-2 (ISO/IEC 19790:2002) – crypto

FIPS PUB 197 – AES

IEC/TS 62351-1 thru 6 – Power systems mgt

ISO/IEC 27001 thru 27002 – security & risk mgt, metrics

NIST SP800-53 – security controls

NIST SP800-52 – ICS security

SAS 70 Type II of hosted facilities

Appendix B: Acronyms used in this document

ICT (Information and Communication Technology)

Denial of service (DoS)

Freedom of Information and Protection of Privacy Act (FIPPA)

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

FMEA (Failure Mode Evaluation and Analysis)

IESO

CIP – Critical Infrastructure Protection (NERC)

References:

[1] IntelliGrid Use Cases (http://intelligrid.ipower.com/IntelliGrid_Architecture/Use_Cases/Fun_Use_Cases.htm)
[2] Ross R, et al., "Managing Risk from Information Systems". NIST, U.S. Department of Commerce, April 2008
[3] The Economist "Cyberwar: War in the fifth domain", The Economist, July 2010
[4] Naedele M, Dzung D. "Industrial information System Security" ABB Review, March 2005
[5] Information and Privacy Commissioner, "Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid", Ontario Information and Privacy Commissioner, June 2010
[6] Huber J. "Over 80,000 Ontario health records missing", The National Post, Dec 2009. http://www.nationalpost.com/related/topics/Over+Ontario+health+records+missing/2371723/story.html
[7] Spears J. "Privacy czar raises alarm on smart meter data", The Sun, June 2010, http://www.thestar.com/business/article/824450--privacy-czar-raises-alarm-on-smart-meter-data?bn=1
[8] Wikipedia "Denial-of-service attack" July 2010 http://en.wikipedia.org/wiki/Denial-of-service_attack
[9] Whitman M.E., Mattord H.J., "Principles of Information Security" Thompson course technology 2009
[10] The Economist "How to keep communications secret, This message will self-destruct, A new way of keeping private correspondence private" The Economist, Aug 2009
[11] Information Management Branch, Government and Program Support Services Division, Government of Alberta, "Information Security Classification", Government of Alberta, February 2005, ISBN 0-7785-3698-X
[12] Centers for Medicare and Medicaid Services, "Selecting a Development Approach", Office of Information Services, March 2008
[13] Ross R, et al., "Managing Risk from Information Systems". NIST, U.S. Department of Commerce, April 2008
[14] Gawer A., Cusumano M, "Platform Leadership". Harvard Business School Press, 2002
[15] Naedele M, Dzung D. "Industrial information System Security" ABB Review, March 2005
[16] Hughes J, "The Integrated Energy and Communication System Architecture, Volume IV: Technical Analysis Appendix A: Security", Electricity Innovation Institute Consortium for Electric Infrastructure to Support a Digital Society (CEIDS), (www.epri.com)
[17] EnerNex Corporation "Security Profile for Third Party Data Access" The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG), Version 0.20, January 2010
[18] EnerNex Corporation "Security Profile Blueprint" The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG), Version 0.20, December 2010
[19] IntelliGrid Use Cases (http://intelligrid.ipower.com/IntelliGrid_Architecture/Use_Cases/Fun_Use_Cases.htm)
[20] Cisco Systems "Securing the Smart Grid Whitepaper" Cisco Systems Inc. 2009
[21] Sensus Metering Systems "Extended CMEP File Format" Sensus Metering Systems 2008
[22] Sensus "TGB Network Management Users Guide" Solekai Systems, Rev 0.9.3 Feb 2010
[23] Telcordia Technologies, "IP Networks, Services and Applications Overview: Student Guide" Chapter 9, Security, Telcordia Technologies Learning Services, 2001
[24] NERC "Reliability Standards for the Bulk Electric Systems of North America" NERC, May 2009
[25] Ross J, Weill P, "Six IT Decisions Your IT People Shouldn't Make" Harvard Business Review, November 2002
[26] Carlin J, " A Farewell to Arms" Wired Magazine, May 1997 (http://www.wired.com/wired/archive/5.05/netizen.html)

[27] http://en.wikipedia.org/wiki/Live_Free_or_Die_Hard
[28] BelAir Networks "BelAir200 Wireless Multi-service Switch Router Data Sheet", http://belairnetworks.com/resources/pdfs/BelAir200_Data_BDMA20020-B02.pdf

[29] Digital Boundary Group, “London Hydro Wireless security Review & Assessment” July 16th 2010