

EnergyAxis: Security by Design

A key competitive differentiator of EnergyAxis is its intrinsic architectural support for security. The strategy of designing security into the EnergyAxis System from the beginning has allowed Honeywell to add and enable security enhancements without costs or impact to system performance.

Honeywell takes a comprehensive approach to security to provide confidentiality, integrity, availability, and auditability within the utility's network. EnergyAxis features a robust, end-to-end security solution that provides protection against all types of security breaches and attacks. This multi-pronged approach includes these features:

- **Access** – Users receive their access privileges based upon their functional roles. The system also supports both media access control (MAC) and Internet Protocol (IP)-address access control lists. EnergyAxis controls access to the network at the end devices, the SynergyNet Routers, and the Connexo NetSense Advanced Metering Infrastructure (AMI) head end. Connexo NetSense supports role-based users, so that only users with certain levels of authority can perform specific tasks. Additionally, Honeywell recommends integration into Active Directory services that the utility employs.
- **Authentication** – Authentication limits transmissions on the network to authorized devices and personnel only. EnergyAxis currently uses sophisticated authentication techniques and enhances these techniques by utilizing unique keys for each device.
- **Encryption** – Encryption prevents unauthorized parties from reading data. EnergyAxis uses National Institute of Standards Technology (NIST)-approved encryption modes and algorithms including Advanced Encryption Standard (AES)-128. ANSI C12.22 key/seed security is enabled in the meter optical port, in all IP-based communications using our C12.22 application and controlled by Connexo NetSense for authorization and auditing. DTLS 1.2 is used for IP/HTTPS communications.
- **Monitoring and Reporting** – The utility receives notification in the case of a security breach. EnergyAxis provides security audit logging and reporting to allow early detection of any security issues. The Honeywell solution also enables the integration of third-party Intrusion Detection and Prevention systems.

The EnergyAxis System provides stringent security measures throughout the network at all levels. Honeywell engineers design and build the security features directly into the end devices, the radio communications networks, the SynergyNet Routers, and the network management system. Thus, full data protection exists in the endpoints and SynergyNet Routers as well as in transit.



Device Encryption from Manufacturing to the field

There are 5 steps to enable an EnergyAxis meter/device to work in the field and report back to NetSense. The process uses ANSI C12.22 for authentication and data exchange is always encrypted using AES-128. A few key notes – keys are never transmitted over the communication network and seeds are never transmitted in the clear.

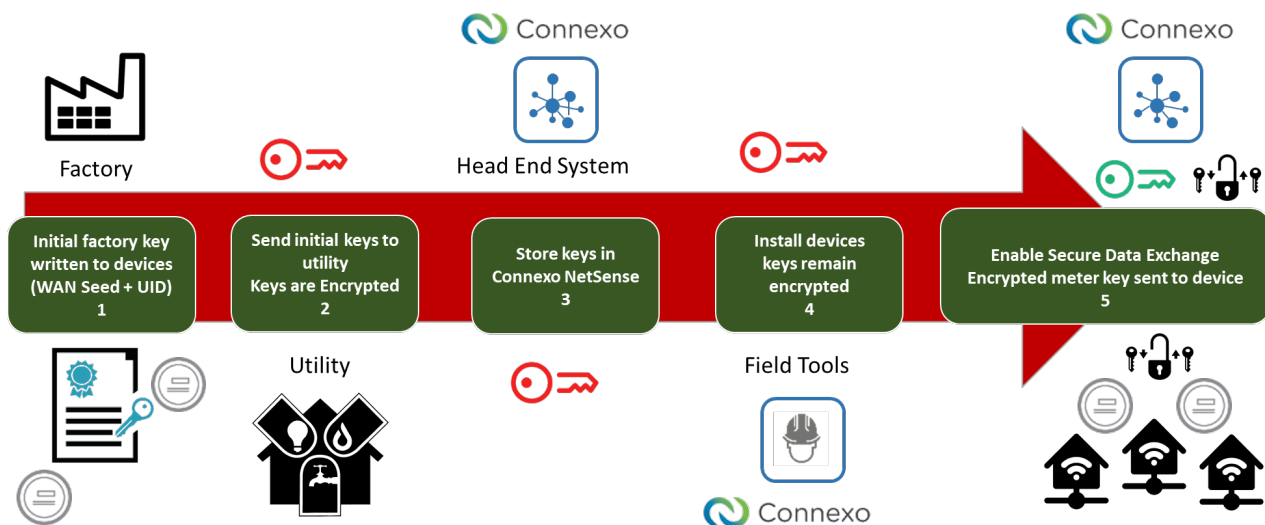
Step 1 (Manufacturing): Every EA device will have a network interface card (NIC). At manufacturing. Every NIC will in turn have its own unique encrypted identity consisting of a WAN Seed and Unique Internal Resource number or IRN.

Step 2 (Utility HQ - Remote): A manifest with encrypted initialization keys is sent to Utility.

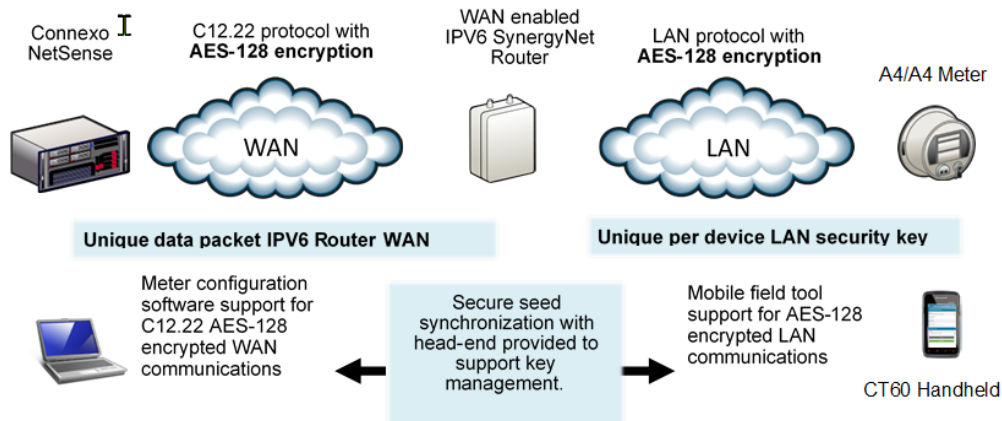
Step 3 (Connexo NetSense): The Connexo NetSense Head-End is setup and keys are stored in system.

Step 4 (Connexo FieldSense- On Site): Utility Field serviceman will replace old meter with new Honeywell meter and will use handheld to scan barcode on the meter to designate and confirm field installation and syncing installation status back to Connexo NetSense running on Utility's private network. At this point, keys remain encrypted – but meter is fully functional, recording consumption and now discoverable but not communicating reads back to NetSense yet- now waiting for NetSense acknowledgment.

Step 5 (Utility HQ-Remote): Once NetSense gets installation information, initialization process begins. NetSense will validate that NIC is trusted to operate on this system. Once authorized, the NIC will negotiate keys to secure that all application traffic is encrypted and move the meter to an active state.



AES-128/256 encryption and authentication on both LAN and WAN ends of the communications network. There are unique individual managed keys on each device. The auditing and logging of all system activities and data manipulation enhances information security. This guarantees nonrepudiation of all system information. The diagram below depicts day to day transactions of the EnergyAxis SynergyNet Network and where 2-way encryption delimiters take place both remotely and in the field.

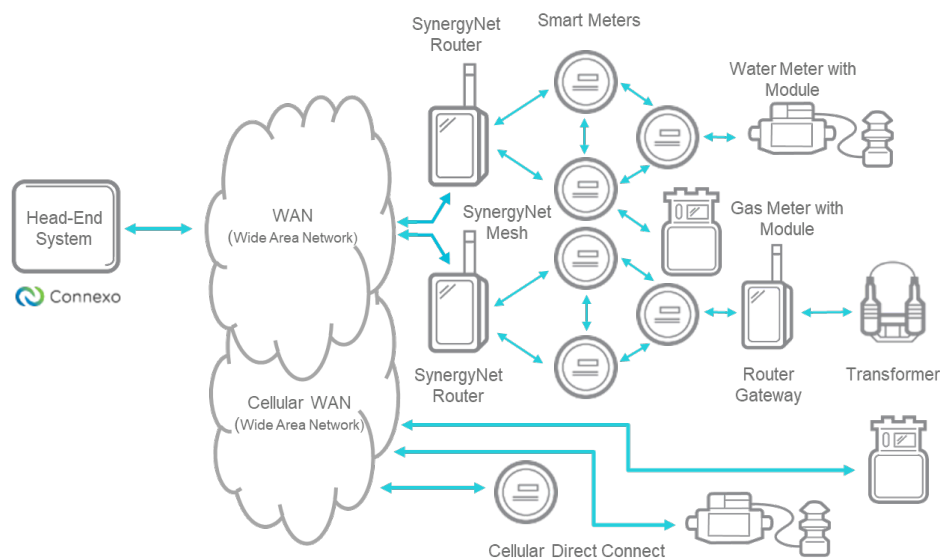


Device Security Key Policies

All Honeywell A4 meters now support management, cycling and recovery of A4 meter security keys directly from Connexo NetSense. Optionally, Connexo MeterSense (via handheld – on site) can also be used directly via optical port on a one-to-one basis for any individual device.

EnergyAxis Network Architecture

The Networking Architecture of EnergyAxis includes Honeywell Alpha Smart Meters (A4R/A4CI) that come in both residential and commercial & industrial formats. As mentioned, the EA network is not limited to RF Mesh and can use direct connect/cellular meters as well. All devices are completely autonomous and communicate meter data back to utility via the IPV6 SynergyNet Router all the way back to the Connexo NetSense head-end system.



Security in the EA Network Element Devices

Local access to the end devices (meters and distribution sensors) is possible via an optical port and remote access is possible via the EnergyAxis 900-MHz radio system. Access to the devices via the optical port requires an optical port C12.22 seed set. A valid seed set is necessary to read data from or configure the meter. The optical port seed

set is set per the customer's factory configuration. The utility can change the seed set using Honeywell's meter configuration software. The utility should maintain a policy of distributing seed sets for meter access on an as-needed basis only.

The SynergyNet 900-MHz local area network (LAN) uses a frequency hopping spread spectrum (FHSS) radio. FHSS systems usually work in unlicensed frequency bands where multiple radio systems may co-exist. FHSS systems also operate in critical applications where security is vital (such as military communications) because they enhance the security of radio transmissions. The inherent enhancement of security in FHSS systems is due to the pseudorandom nature of the radio communications. The EnergyAxis System transmits each packet of data on one of 50 available channels. The next data packet broadcasts on another channel in a pseudorandom channel selection process that provides immunity to eavesdropping, interception, and interference. The EnergyAxis hop sequence is per device (not common to all devices) increasing the difficulty in predicting the channel for the next packet in a communication sequence.

In addition to the secure transmission method provided by the FHSS radio in the end devices, there is further protection using authentication and using AES-128 encryption with unique keys for each end device. As part of the EnergyAxis system, we can configure them to only respond to properly encrypted data requests. For LAN communications, a unique, system-generated token (used only once) must be a part of each communication with a meter or device for authentication to occur. With added encryption, if an improperly encrypted request transpires, the meter will not acknowledge the request as valid and the meter will not comply with the request. The network identifies the attempt as an invalid radio access attempt. This combination of an FHSS system and AES-128 encryption prevents direct tampering.

Finally, additional security is provided within several standards included in our solution, including DLTS, VPN, and C12.22. Please refer to the SynergyNet Overview and the C12.22 document for more details.

AES-128 Encryption Benefits

Honeywell performed a thorough review of available encryption algorithms and specifically selected the National Institute for Standards and Technology (NIST) AES-128 encryption method for the EnergyAxis system.

Other NIST AES alternatives, including 192 and 256, result in much larger system latency and power consumption than AES-128. Implemented in software, each key size increase takes approximately 40% additional time (and therefore power), so if a software implementation of AES-128 takes 10 units of time, AES-192 would take 14 and AES-256 about 20. Simply put, if we encrypt all data communication packets, the latency due to encryption would be four times as much for a roundtrip communication to a smart meter with AES-256 versus AES-128. The meter would also consume double the power doing a single AES-256 encryption versus a single AES-128 encryption. For these negative attributes to be worthwhile, there would have to be a corresponding benefit.

For a given algorithm, longer keys provide a higher degree of protection against so-called "brute force" attacks, and so on the surface this might be a reason to choose a larger key. However, this does not seem to be the case for AES-192 and AES-256 versus AES-128. Recent analysis of those ciphers has determined that, in fact, AES-256 is weaker than AES-128. All three of the variants are still secure, even in light of this new advance, but using AES-256 provides no practical benefit. To mount a successful brute force attack on AES-128 on a machine that could somehow process a billion-billion iterations per second (far beyond even the fastest supercomputer today), it would take more than 10,000 billion years. For reference, physicists now estimate the age of the universe at less than 14 billion years. This is plenty of security, even for utilities with the very longest time view.

In short, 128-bit based encryption sufficiently addresses all commercial and top-secret government applications. However, complete end-to-end security requires more than simply adequate encryption algorithms. Key management (including key storage and distribution), sound software engineering techniques to eliminate

security hazards such as the kinds of coding errors that allow buffer overrun attacks, and a thorough and repeatable testing process are all also required for system security.

The EnergyAxis common security key management infrastructure (Security Manager GUI) reduces the complexity and cost of key management by enabling the security Administrator WAN to manage security keys and change WAN keys to meet utility security policy needs. Generation of new WAN security seeds by a NIST approved cryptographically secure random number generator at the Security Manager (i.e., RSA X9.31 PRNG Pseudo-Random Number Generator) is the means.

The EnergyAxis keys never leave protected environments.

Prevention of Tampering

Without the possibility of direct tampering, an adversary may attempt indirect methods of tampering such as packet replay attacks. In a packet replay attack, an adversary stores a radio transmission and replays the transmission later. One might attempt this type of attack to cause the system to respond in a way that changes control or billing parameters at the meter site. For example, an adversary might attempt to store load control or pricing commands to replay later. EnergyAxis devices have anti-replay mechanisms in each radio transmission to prevent the storing and replaying of messages later.

In addition to the security techniques to prevent unauthorized access, EnergyAxis devices have detection information to identify attempts to breach the device. The security detection information includes these pieces of information:

- Count of the number of invalid optical port access attempts (access attempts with an invalid password).
- Count of the number of invalid radio access attempts (access attempts with an invalid encryption key).
- Access-warning status flag appears if either the optical port or the radio invalid-access-attempt counts exceed a configurable threshold. We can configure the meter to immediately transmit an exception message when this status flag is set.
- A status flag to indicate a table write. We can configure the meter to immediately transmit an exception message when this status flag is set.
- The date and time of the last table write.
- If the meter leaves the installation site, a tilt warning transmits this information in the outage message. This differentiates an outage from a tamper event.

In addition, LAN devices (meters, SynergyNet Routers, etc.) cannot be reverse engineered. We lock the microcontrollers containing the firmware such that reading the firmware from the device is not possible. One can write the firmware, but certain provisos impede that strategy:

- Internal to the device is a section of firmware that cannot be overwritten (known as the boot loader).
- Regardless of whether an attempt is to write one section or the entire firmware image, the boot loader verifies the new downloaded section and the entire image must go through validation. In addition to satisfying all security requirements, one would have to have knowledge of the complete firmware image in order to attempt to modify or load a new image.
- The meter will not attempt to switch to a new firmware image prior to the validation of the new image.

To prevent end-point behavior monitoring (which is sometimes useful in an attempt to learn the behavior of the devices in order to use them to control other devices), the EnergyAxis system has built-in protection.

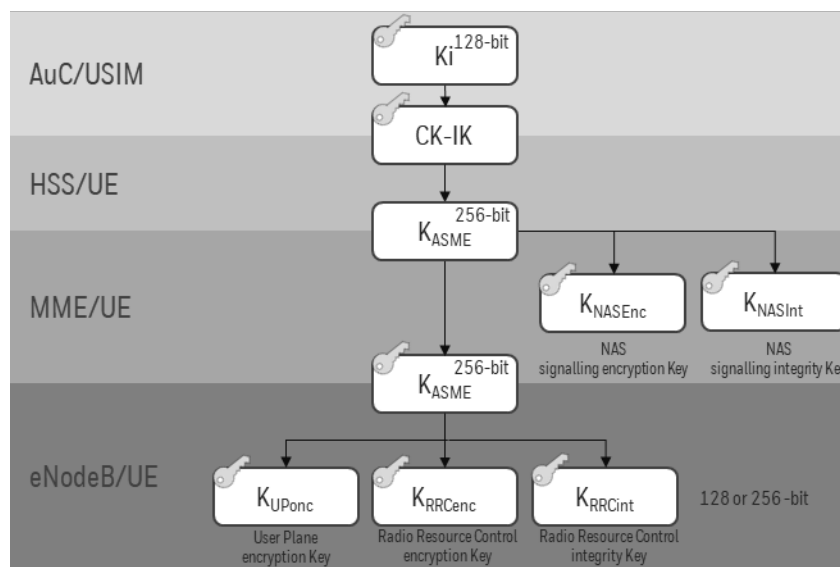
- When powered up, an endpoint device will send an event message such as a restoration message and it will request time from other devices, but it will not perform other communication tasks unless it is a command initiated by the SynergyNet Router.
- Metering data goes nowhere unless another device requests it.
- Firmware within the endpoints never initiates control messages to other network devices.

In extremely sensitive security situations, we can put the devices in locked mode, which electronically denies writes to any configuration table. When in the locked mode, EnergyAxis devices can only be unlocked if the device seal is broken (i.e., the physical packaging such as the meter cover is removed) and a Honeywell specific hardware and software technique is used to unlock the device.

Additional Security for Cellular Direct Connect Devices

Subscriber Identity Module

LTE-M meters like any LTE devices, require a SIM (Subscriber Identity Module) for activation, and all authentication. The SIM provides additional layer of security by the way key is transferred from SIM manufacturers to Key Authority (Network Providers).

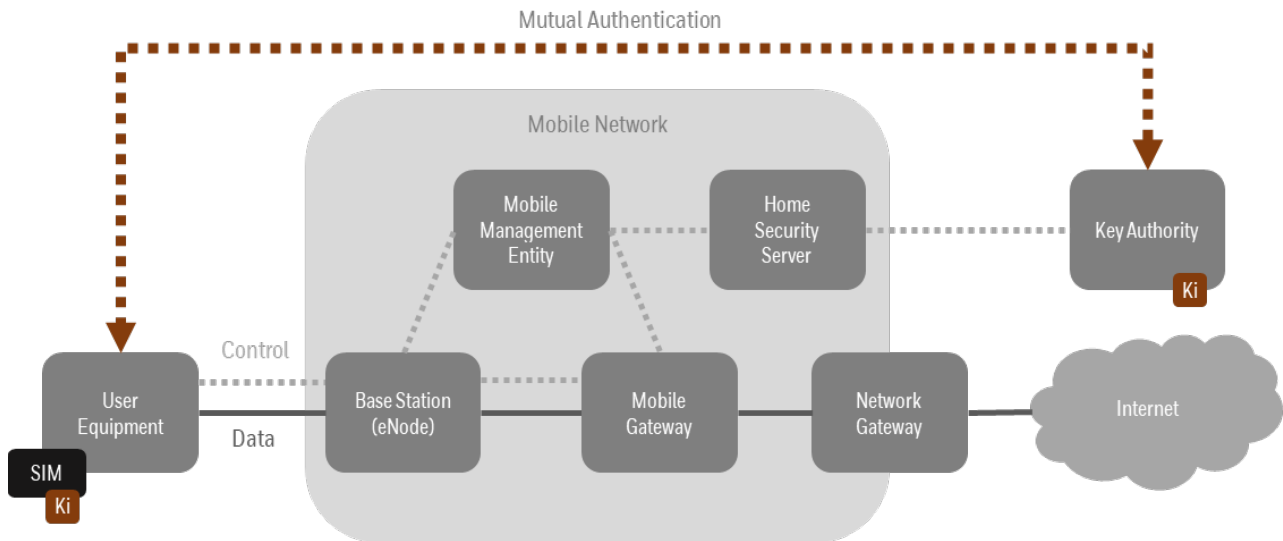


Key Generation Hierarchy

The master key (K_i) is never transmitted.

- It is generated by the SIM at manufacture
- It is transferred to the key authority
- Deleted by the SIM manufacturer

Security from Meter to Network



Elements in the core network have their own security layers. Keys are renewed regularly

- Mutual authentication between the UE and the network
- Regular derivation of keys for ciphering and integrity protection
- Encryption, integrity and replay protection of NAS signaling between UE and MME
- Encryption, integrity and replay protection of RRC signaling between UE and eNode
- Encryption of the user traffic between UE and eNode
- Temporary identities are used to avoid sending permanent ID over the radio link

Security of the SynergyNet Router

Typically, access to a SynergyNet Router happens via the WAN. The external connections are ethernet, and SD Card (for memory). A PC with ethernet connectivity can be used as local maintenance terminal to configure the router. Access is password protected.

The SynergyNet communication platform employs a comprehensive security approach that provides hop-to-hop as well as end-to-end security using symmetric keys and/or certificates.

Here are a few security mechanisms the platform supports:

- Secure VPN
 - Uses SSL/TLS (Secure Sockets Layer/Transport Layer Security) for security
 - Secures communication between Head-End-Systems and the SynergyNet Router
- Link Layer:
 - IEEE 802.15.4e security mechanisms based on CCM and AES; offers hop-by-hop security
- Transport layer:

- DTLS 1.2 offers end-to-end security for application flow
 - PANA/EAP/TLS for network admission
- Cipher suites for TLS/DTLS:
 - TLS_PSK_WITH_NULL_SHA256
 - TLS_PSK_WITH_AES_128_CCM
 - TLS_PSK_WITH_AES_128_CCM_8 (SHA_256)
 - TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 (SHA256)
- Cryptography:
 - Symmetric key cryptography
 - Public key cryptography based on security certificates

The security construct is policy driven, allowing the user to choose from various levels of authentication and encryption. Every link and every segment in the communication platform (WMN node – Router - NMS) is secure.

The communication platform allows for both network admission and for application security:

- Symmetric key cryptography
- Public key cryptography based on security certificates

The security credentials certificates for WMN nodes and Routers are configured in a secure environment during production. By employing security certificates, the production and deployment process are simplified, but it does require additional security measures during production for protecting the root certificate authority (CA):

- Special security for the appliance for signing the router and wireless nodes certificates
- Only designated personnel have login access to the appliance
- The access to the room hosting the appliances is restricted to the designated personnel
- Additional measures like video surveillance

The Router network admission process sits on SSL/TLS using security certificates and a NMS whitelist mechanism. The Router and NMS will mutually authenticate each other to prevent rogue Router from joining an NMS or a rogue NMS to hijack Routers. The WMN-node network admission process rests on PANA/EAP/(D)TLS using security certificates or PSK (Pre-shared keys) and an NMS whitelist mechanism. The WMN nodes, router and the NMS will mutually authenticate each other in order to prevent rogue wireless WMN nodes from joining an NMS and a rogue router/NMS to hijack a wireless WMN node.

Communication keys swap following the successful network admission process. A rogue node will not gain access to the network because it does not have valid security credentials. Without network admission, it will not get the communication keys and it will not be able to communicate with the other network entities.

Wireless link messages are both encrypted and authenticated assuring messages confidentiality and integrity. A rogue node will not be able to decipher, modify, or relay messages received over the wireless communication media.

Backhaul link messages are both encrypted and authenticated ensuring messages confidentiality and integrity.

The NMS configures the communication keys and the length of their life such that they change periodically and thus, assure both link layer security and application security.

The platform security policies are under control of the NMS and managed through user accounts and access control list. The NMS also includes accounting and reporting mechanisms of all operations executed by the users.

The WAN modem in the SynergyNet Router has password protection and supports Custom Access Point Nodes (APN) making the modem's IP address private and not exposed to the public internet. GPRS devices can be set up on custom APNs and made to appear as if they are from within the utility intranet so that the IP address is inaccessible from outside the corporate intranet.

LAN communications, to and from the SynergyNet Router, use the same FHSS 900-MHz radio as we described above. The security mechanisms, including AES-128 encryption, are the same as discussed for the EnergyAxis network element devices.

AES-128 encryption offers the following elements:

- Unique 128-bit crypto keys per WAN device
- Unique 128-bit crypto keys per LAN device
- Unique 128-bit re-keying keys per WAN and or LAN device during re-keying activities
- Built-in key management offering, providing the ability to securely change keys across the EnergyAxis system (WAN only in this release, with LAN support in the following), provide key recovery, and enable/disable encryption over the WAN and/or LAN
- Generation of crypto keys utilizing NIST approved processes

It is important to note that the SynergyNet Router does not accept LAN commands via the EnergyAxis 900-MHz radio that requests it to initiate LAN activity. Such commands may travel by and gain acceptance only via the WAN connection. This design feature denies an adversary any possibility of using a 900-MHz radio to control the SynergyNet Router's activities or gaining control access to the LAN.

LAN communications between the SynergyNet Router and meter as well as C12.22 communications from the Connexo NetSense AMI head end to the SynergyNet Router are session-less, requiring each communication to be authenticated prior to its being acted upon. WAN C12.21 sessions (Connexo NetSense AMI head end to SynergyNet Router) have a timeout, and the session expires if not kept open by communications (i.e., Connexo NetSense requested action).

Security at the Connexo NetSense AMI head-end

Password Management

Password management is managed via Microsoft Active Directory / LDAP. Microsoft Active Directory provides a standards-based solution to user policy management. Password strength, clipping levels, password expiry and other account and password policies are expected to be implemented using Active Directory service.

Access Level Controls

The Connexo NetSense AMI head-end resides within the corporate intranet and thus all security mechanisms that the utility has in place for its enterprise security are the primary mechanisms for securing access to Connexo NetSense. The network management system provides role-based access control: System Administrator, Meter Services User, Billing and communication and information system (CIS) User, Report Only User, and Security Administrator. Each user obtains access to the system via a unique username and password. User access depends on that person's assigned role.

- Reports Only users – Can only run reports and see their own activities in the activity monitor.

- CIS Operators – In addition to the above, the CIS users can perform some configuration functions such as meter setup, meter connect, and meter disconnect.
- Meter Services Users – Can perform more advanced functionality to the meter such as resetting event logs, manual demand resets, acknowledge meter alarms, etc.
- System Administrators – Have access to all functions and can create user accounts and monitor user activities across the system.
- Security Administrators – Can manage WAN and LAN security/encryption settings.

System User Monitoring

The Activity Monitor enables the system administrator to perform these important tasks:

- View log of each user's activities.
- View specific meter, account, etc., that were involved in the transaction and the parameters sent.
- Capture, log, and report every operation executed by a user from the web application. This includes timestamps and user IDs. Programmatic interfaces and batch operations archive in a similar fashion.

Security of Data between Connexo NetSense and Other Applications

If necessary, it is possible to encrypt device data transferred between Connexo NetSense and other enterprise systems using either a symmetric or asymmetric encryption algorithm. Honeywell uses the Optimal Asymmetric Encryption Padding (OAEP) scheme with Rivest Shamir Adleman (RSA) encryption, (RSA/OAEP) for the Asymmetric Cipher Algorithm and Triple DES (DESede) for the Symmetric Cipher Algorithm, for data exporting from Connexo NetSense.

Security of the LTE Core to AMI Head End (for direct connect meters)

Honeywell utilizes a private network to connect mobile network providers core network to AMI Head End System. The connection is based upon IPSec tunneling and utilizes encryption. The implementation employs private IP addresses which are not reachable (and thus are not subject to spoofing and attack) from outside systems. The meters IP addresses is only known to AMI Head End System.

Security by Design

We view cybersecurity as a never-ending pursuit to thwart an unremitting threat. Honeywell is committed to the continuous improvement of our security systems and solutions.

The Honeywell EnergyAxis AMI system provides far superior security over competitive offerings. The primary difference between Honeywell's secure network solution and others is the design. By design, we meticulously construct and implement the EnergyAxis system with security in mind.

EnergyAxis is not a conglomeration of third-party "secure" solutions. Our system is intrinsically secure. It is not bolted-together-parts secure.

Honeywell actively collaborates with customers and networking security consultants in performing penetration testing to validate our security coverage and to detect any exposures. Honeywell's goals are error free and secure data flow and communications.