# Allegro & Harmony End-to-End Security

## 1. Introduction

The goals of a security strategy are simple: protect all points of entry to the network. As utilities move forward in development of Advanced Metering Infrastructure (AMI), they open themselves up to an expansive network with a number of elements requiring protection. This document presents an overview of the security elements within the Harmony / Allegro system.

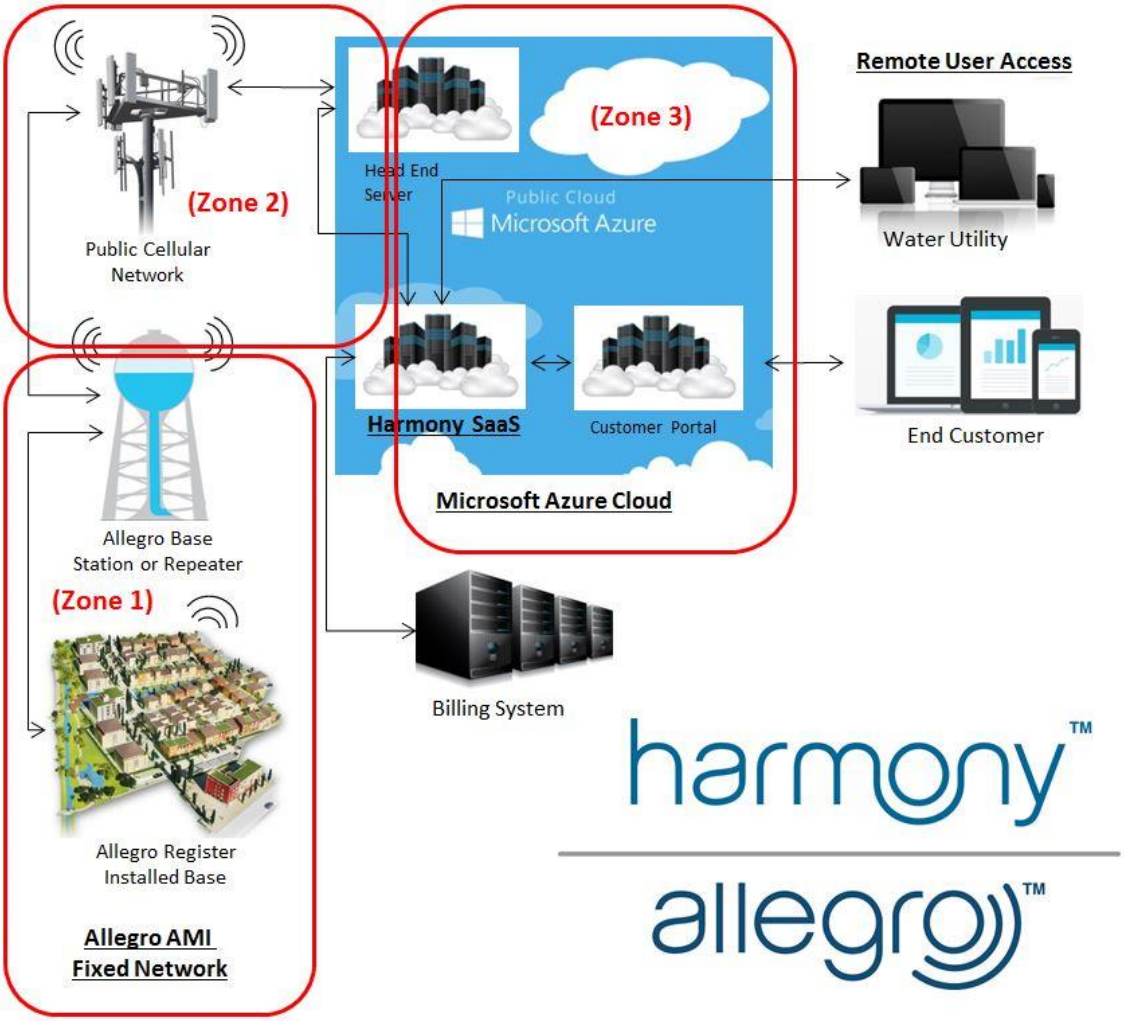


Exhibit 1

## 2. General Architecture

We can break the Allegro and Harmony Network into 3 Security Zones (See Exhibit 1 above):

- Zone 1: The Allegro RF Network – Any end unit at this zone can sense the Allegro network elements and potentially can register to the Allegro system.
- Zone 2: The Cellular Backhaul (APN) – This zone enables connection of the Allegro base stations to the Internet cloud, so any data that is received by the base stations can be delivered to the Harmony servers via the Internet cloud.
- Zone 3: Harmony Cloud Servers (MDM Head End & Microsoft Azure Data Storage) – This zone is a closed local network of all Harmony related servers.

Data that should be secured:

- All "set commands" and “get commands”, including meter readings

System modes that should be secured:

- Fixed Network
- Drive By
- Technician Operation

Threats that should be handled:

- Message Replay
- Registration / Authentication Attack
- Network Element Spoofing
- Data Eavesdropping
- Endpoint Key Theft

## 3. Zone 1: Allegro RF Network

The Allegro RF Network is a Wide Area Network (WAN) comprised of Endpoints, Base Stations, and Repeaters. Communication within this WAN is secured in a number ways.

**AES256 Encryption –** In symmetric encryption systems, 128-bit keys are considered very strong. The Allegro RF network easily meets the security requirements of water only systems along the Wide Area Network of endpoint to data collector.

**Time Windowed Commands –** The system first sends a notification of action message to the device; the subsequent action message must be received within a designated



Master Meter, Inc. | 101 Regency Pkwy, Mansfield, Texas 76063 | T 817.842.8000 | F 817.842.8100 | www.mastermeter.com

window of time, and it must contain elements that match those in the notification message, or else the action is rejected.

**Time Synchronous Network –** In the network security context, entropy refers to a degree of built-in uncertainty in how security provisions are applied. When security features are less predictable, they are harder to crack. The Allegro network is designed around assigning specific time slots for communication making the network much more difficult to compromise.

**Licensed Frequency –** A licensed frequency provides intrinsic security advantages since individuals can't purchase technology on these frequencies easily. Also, other than by the licensee, it is illegal to send or receive data on these frequencies.

**Physical Security –** A Base Station is generally installed at a water tower site, within a secured location. Often this is the same location that wireless telecom or paging systems are installed.

## 4. Zone 2: Cellular Backhaul

**Virtual Private Networks (VPNs) –** A VPN encapsulates the data being transmitted from the Allegro RF Network along the backhaul to the Head End Server located on the Microsoft Azure Cloud. VPNs authenticate both endpoints of the communication to prevent unauthorized users from accessing or reading the data. A VPN uses Transport Layer Security (TLS) or Secure Socket Layer (SSL) to encrypt transmissions at the transport layer.

**Private Access Point Name (APN) –** The Allegro Network has an established private APN with in the AT&T cellular network. This allows connecting the allegro base stations to the cellular network in a most secured way, using a local IP address which makes the base station unreachable to anyone other than authorized personnel.

## 5. Zone 3: Harmony Cloud Servers

Basic security measures found in the Harmony SaaS Cloud Servers:

- Firewalls
- Anti-Virus protection
- Self-Diagnostics
- Various other IP based security protocols

Additional measures securing the cloud data provided by Microsoft Azure Hosting:

- Design and Operational Security
- Identity and Access Management
- Encryption and Key Management
- Network Security
- Threat Management
- Monitoring, Logging, and Reporting
- Security Partners
- Penetration Testing

http://azure.microsoft.com/en-us/support/trust-center/security/

### 6. 3rd Party Network Security Verification

The Harmony SaaS Cloud Platform has been thoroughly vetted and certified by the largest Information Security & Infrastructure Solutions Provider globally – OPTIV (Formerly Fishnet Security).

A written statement is available upon request.

https://www.optiv.com/



Master Meter, Inc. | 101 Regency Pkwy, Mansfield, Texas 76063 | T 817.842.8000 | F 817.842.8100 | www.mastermeter.com