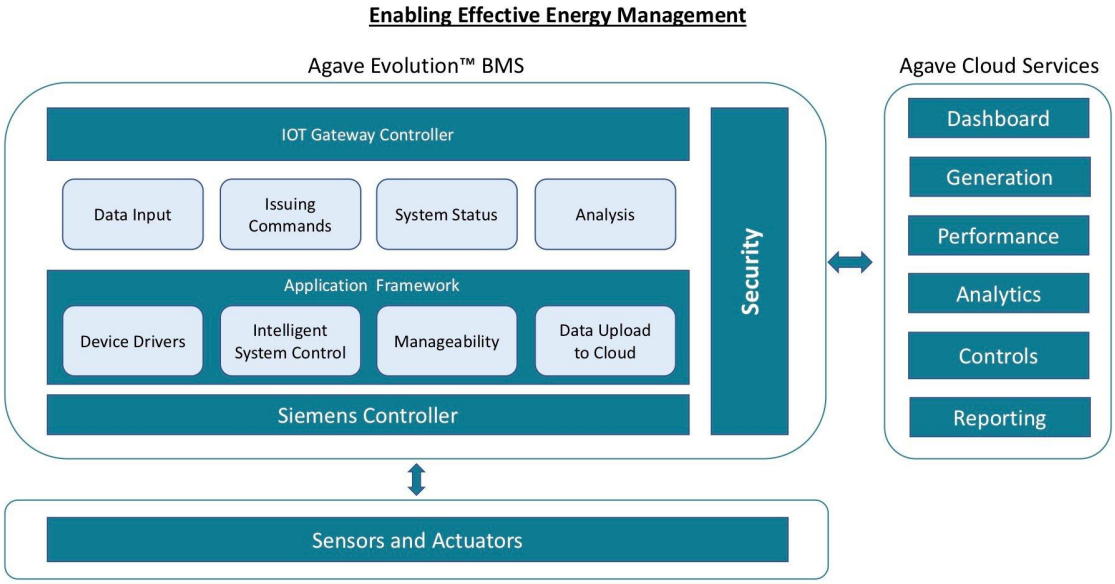
Architecture



Our Approach

Our approach is to minimize the cost of upgrading the BMS by utilizing the existing plant equipment and sensors. New modular IO controllers will be provided that replace the existing IO controllers installed in the existing cabinets. Wiring connections will then be made from the new IO controllers to the existing terminal blocks. Existing wiring from all sensors, pumps, valves, etc. to existing terminal blocks in control cabinets will be reused. This will provide substantial cost savings as well as keeping the system that onsite staff is familiar with.

Controller Specification

The cornerstone to our building management system is the SIEMENS SIMATIC-7 remote IO controllers. The SIMATIC range of controllers comprises Basic, Advanced, Distributed, and Software Controllers that offer impressive scalability and integration of their functions. Remote IO controllers allow digital and analog IO connections to be located near devices and communicated back to the central plant controller. IO modules can be easily added to the remote IO controller data bus for future expansion and scalability. SIEMENS SIMATIC platform is an industry standard with proven reliability in their equipment and software as well as support from vendors.

Remote IO Modules

Each existing cabinet will have a SIEMENS ET200SP control module with a power supply, and enough digital and analog IO to support at least the existing connection requirements. The IO modules allow interface to discrete inputs, discrete outputs, analog inputs, analog temperature inputs, and analog outputs. Each IO module is dedicated to a particular type of input/output to maximize signal integrity. IO modules come in standard 4, 8, and 16 points depending on the module selected. As a result, any spare IO will be identified for future expansion.

Individual remote IO controllers along with their associated IO modules will be provided at each of the existing control cabinet locations.

- Boiler Process
- Chiller Process
- Cogeneration
- Secondary Water Loop

Programming Logic Controller

There will be a SIEMENS SIMATIC S7-1500 PLC that will integrate all the IO modules and provide real time data to the IoT Gateway System for information and controls. The PLC will receive the information from the IoT Gateway System in order to sequence plant equipment via the remote IO modules. Ideally this would be located near the IoT Gateway System where all communications are currently truncated. Utilization of s PLC for plant sequencing and control provides increased system reliability void of viruses and instabilities that can be associated with Windows or Unix based platforms.

IoT Gateway System

An IoT Gateway System will be a PC-based system running SIEMENS runtime software for Human Machine Interface between the plant operator and PLC. The IoT Gateway System will include four (4) monitor screens to provide continuous visibility to each of the four major central plant areas. Screens will be provided to plant operators to provide an overview of each major central plant area, as well as, detailed equipment data acquisition and user control screens. User commands issued through the IoT Gateway screens are communicated to the PLC where execution of the control sequences and algorithms are carried out for enhanced reliability. In addition, the IoT Gateway System will manage long-term data storage of all parameters and commands.

Programming Tools/Design

SIEMENS TIA Portal will be used for the software development with code deployed on the PLC and the IoT Gateway System. This is an integrated development environment (IDE) that allows developers to provide a complete software project including data acquisition, data storage, sequencing logic, and user interface displays. The IDE provide compile time error checking to ensure that software loaded on the PLC and the IoT Gateway System are compatible and do not have potential errors as a result data register matching issues.

SIEMENS SIMATIC control platform has been refined for over 60 years. They have a proven history of reliability, backwards compatibility and future roadmap for growth as well as excellent customer support. Several organizations utilize this software platform providing end-users a wide variety of resources to access for their programming requirements. Programming support is available through Agave® Systems, SIEMENS distributors, and third-party programming vendors.

Users interface screens will utilize state of the art graphics design and be organized to provide plant operators a clean simple to use interface. The following user interface screens are included as part of this proposal.

- Site Plan
- Boiler Process
- Chiller Process
- Cogeneration
- Secondary Water Loop
- Equipment Specific Data Acquisition Pop-Ups
- Equipment Specific Controls Pop-Ups

Each controlled device will have representation on the overall plan screens. Each device will include a pop-up screen to provide a more complete view of all data acquisition parameters. Control screens will also pop-up to allow plant operators the ability select automatic or manual sequencing where appropriate, and issue manual override commands as needed for each piece of equipment.

SIEMENS Runtime License will be installed on the IoT Gateway System to allow it to communicate with the IO Devices.

Remote Data Storage

IoT Gateway System will include implementation of automatic data backup to prevent loss of data and provide quick disaster recovery procedures. Data will be uploaded to an offsite storage location (i.e Amazon Web Services or other secure location) to ensure availability of historical data. A stable version of the BMS software application will be backed up to the internet during software download. Together these measures protect against any potential virus, hardware failure, and damage to the local facility. Should any of these undesirable events occur, the user can restore operation of the IoT Gateway computer, download stable software version, restore local data image, and resume plant operations.

Security

Our security approach includes four basic strategies to prevent unwanted access from outside users while simultaneously allowing remote access. The first (1) strategy includes isolation of all devices associated with the BMS using a router to create a private network. This limits network traffic to authorized operations and unwanted communication that could negatively impact system response time. The second (2) strategy incorporates a VPN firewall to provide

security for accessing the private network, however remote access is not limited. Authorized users will be able to access the BMS only when they are able to authenticate a security key and provide issued username and password. The third (3) strategy includes password protection to access the BMS software remote user interface screens. This is a specific username and password allowing the system to track who has accessed the system and log what commands were issued. The fourth (4) strategy includes providing BMS sequencing and controls on a dedicated PLC separate from the IoT Gateway Screens. Several software services are offered on a PC-based platform making then susceptible to industry common viruses that can lead to undesirable consequences. The PLC is limited to the available software services that could allow unwanted access and limited to receive only certain types of commands from authorized devices.