Cisco Connected Assets 2.0 Design Guide

December 2015

Cisco Validated Design

Building Architectures to Solve Business Problems

About Cisco Validated Design (CVD) Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit http://www.cisco.com/go/designzone.

Cisco Connected Assets 2.0 Design Guide

Preface

The Cisco Connected Assets solution is developed to easily connect different types of sensors, and leverage the capabilities of edge and cloud-based processing to provide business intelligence insights, to help the customers optimize operations and improve productivity efficiency. The initial focus of Connected Assets is targeting Site Asset Management (SAM). This solution will help operators to monitor the status of assets in remote sites from a central location and also control many aspects thus improve service response time and reduce OPEX.

Navigator

Chapter 1, "System Overview," introduces the Connected Assets CVD 2.0 solution. It also gives the list of use cases addressed by this CVD.

The second chapter, Chapter 2, "System Architecture (or System Design)," covers the end-to-end system architecture. It gives design considerations for various aspects such as network connectivity, security, requirement, and network operation center.

The next chapter, Chapter 3, "System Components," enlists Cisco and third-party components, both at the cell site and the network operation center (NOC).

Chapter 4, "System High Availability and Scalability" covers the system high availability and scaling aspects, it also gives the recommendation for server sizing, storage and network bandwidth requirement between each cell site and the NOC.

Document Objective and Scope

This design guide provides a comprehensive explanation of Cisco Connected Assets CVD 2.0 system design. It includes information about the system's architecture, possible deployment models, and guidelines for implementation and configuration. The guide also recommends best practices and potential issues when deploying the reference architecture.

Abbreviations

NOC: Network Operation Center

CAM: Cisco Asset Manager

ACP: azeti Control Panel

NOC: Network Operation Center

SG: Sensor Gateway

SAM: Site Asset Management

System Overview

This CVD 2.0 addresses the design and implementation details of Site Asset Management (SAM). SAM solutions can be used for various applications with remote site assets. Typical examples include the following:

- Cell towers
- Utility substations
- Oil and gas pump sites
- Remote ATM machines

A SAM solution for asset management applied to cell towers is detailed here as an example.

In the case of cell towers, the SAM Service can help the service provider secure, operate, and optimize their infrastructure. The wealth-creating ability of mobile telecommunications operators and tower companies, for example, depends on the cost, effectiveness and availability of their networks that are composed of thousands of remote and unattended base transceiver stations (BTS). The success of many operations in telecommunications and other industries relies on the remote monitoring of the performance of these costly assets.

BTS sites are exposed to certain hazards such as theft, destruction, harsh weather conditions or malfunctions of equipment. Having intelligence on the tower sites help to keep them up and running and prevents financial losses.

BTS often have a suboptimal performance level due to an inefficient resource allocation. Enhanced remote management capabilities are the basis for substantial cost savings as well as improvements in efficiency and utilization of given site infrastructure.

The Cisco SAM Services consists of a secure and manageable hardware and software solution. The solution offers energy reporting and management, remote monitoring and management, systematic actions from well-defined events, pre-defined NOC interfaces, and easy-to-use configuration to accelerate deployment.

When successfully deployed this solution provides a single view of all assets located at the site and detailed information on telemetry data. The solution is comprised of a combination of the functionality listed below:

- Site Security
- Advanced Analytics
- Environmental Monitoring
- Detailed Reporting
- HVAC Management
- Security Management

- Access Management
- Power Monitoring
- Multitenant Power Monitoring
- Energy Usage and Optimization by Asset-type
- Fuel Monitoring
- Data Visualization
- Other IoT sensors data with the capability of analytics, reporting and visualizations

Solution Use Cases

CVD 2.0 addresses the following use cases:

- Environmental Monitoring (Operational Continuity)
  - A number of environmental sensors, such as temperature, humidity sensors, as well as water intrusion, smoke detectors, and hazardous gas sensors are connected on the site. These sensors send real-time alarms to the NOC when there are threshold crosses.
  - The remote environmental monitoring help to gather fine-grained data on environmental parameters for further analysis.
  - Determination of optimal environmental settings.
- Security Management (Operational Continuity)
  - Surveillance of the whole tower site with the help of cameras and motion detection sensors, triggering alarms in case of unauthorized access
  - Detecting copper theft (earthing wire) thus increase the security of the tower site in case of a lightning strike
- Access Management (Operational Efficiency)
  - Keypads allowing keyless entry and logging access to the site
  - Provides work time-stamp control
  - Enables to remotely grant access to sites from the NOC
- Power Monitoring (Operational Continuity)
  - Monitoring the battery, the generator and the rectifier and provide their parameters
  - Predefined thresholds generating alarms to the NOC
  - Data and energy logging allows for detailed break down of energy consumption for comprehensive business analytics
- Multi-tenant Power Monitoring (Operational Efficiency)
  - Multi-tenant site operations, meaning that different Telco operators using one tower site and are paying only for the energy they have consumed.
  - Efficient use of already existing tower site infrastructure.
  - Detailed power consumption per tenant per tower site. Export to billing systems, and generating performance analysis reports.
- Fuel Monitoring (Operational Continuity)

  - Fuel level sensors help to determine when the next refill is due, as well as detects theft by tapping; therefore helping to prevent generator damage.
  - Constant tapping of minor amounts of fuel can be revealed using flow sensors in the fuel pipe to the generator, as well as door contacts on the fuel cap, which shows whether it has been opened besides scheduled refilling visits.

Partner Information

azeti Networks is a global provider of M2M technology for a variety of verticals. Cisco has partnered with azeti to provide an end-to-end solution for SAM for cell towers. azeti has pioneered the building of the sensor gateway (SG) and control products that interface with Modbus-7/based sensors. In the current projec,t azeti sensor gateway software (Site Controller) is used at the cell site and azeti control panel software is used in NOC.

Cisco Solution Unique Selling Points (USP)

- Highly scalable architecture can support asset management for thousands of remote sites.
- Secured WAN connectivity with advanced VPN options.
- Fog computing at the edge ensures the cell is operational even when the WAN link to the NOC is down.
- Faster response time to critical situations by executing actions locally at the remote site.
- Limited WAN bandwidth requirement by data compression and summarization at the remote site.
- Multiple WAN backhaul support, 3G/4G/LAN, with primary and backup options.
- Wide range and easily extendable Modbus TCP, Modbus RTU sensors support.
- Supports remote site surveillance with IP camera.
- Real time event notification to the NOC.
- Highly customizable reporting and analytics.
- Support for multi-tenant operations.

System Architecture (or System Design)

Major Architectural Requirements

This section describes the major architectural requirements of the Connected Assets CVD 2.0:

- The Connected Assets system needs to have a highly scalable and distributed architecture with thousands of cell sites geographically distributed across a wide region.
- Fog computing software residing at the cell site on the sensor gateway is responsible for local computing. It needs to have a reliable communication channel to interact with the central operations and analytics software hosted in network operation center (NOC). The sensor gateway can be hosted on IR809/829 or UCS-E.
- Intermittent low speed network connectivity between the remote cell sites and the central operations center is a tough challenge. The network architecture needs to take care of this problem.
- The architecture must leverage the available customer wired network while providing a backup on a wireless connection. The communication on both these media needs to be secured as it can pass through public Internet.
- The WAN link should have built-in redundancy; the primary link being Ethernet and the secondary link 3G/4G. Switch over from the primary to the secondary is triggered automatically when the primary link fails or the primary link quality degrades. On restoration of the primary Ethernet link, the WAN link should get restored back to primary.
- The cell site architecture needs to support interfacing with Modbus serial sensors and IP cameras. Both Modbus RTU and Modbus TCP sensors/adapters are supported. The preferred vendor for Modbus TCP adapter is B&R. The solution needs to collect various system and environmental parameters from the sensors, as well as support snapshot- based surveillance and future video surveillance.
- The Network Operations Center (NOC) for Connected Assets can be hosted in customer premises as stand-alone systems or in a public/private cloud.
- The overall solution needs to have an integrated user interface to manage different operations of the network including: configuration, monitoring and reporting (Fault, Performance and Configuration).
- The WAN link should be restricted to secure access, such as, IPSec tunnel and ssh.
- All features except for Modbus RTU are supported with a sensor gateway running on a Cisco UCS-E server.

End-to-End System Architecture

Figure 2-1 End-to-End Network Block Diagram

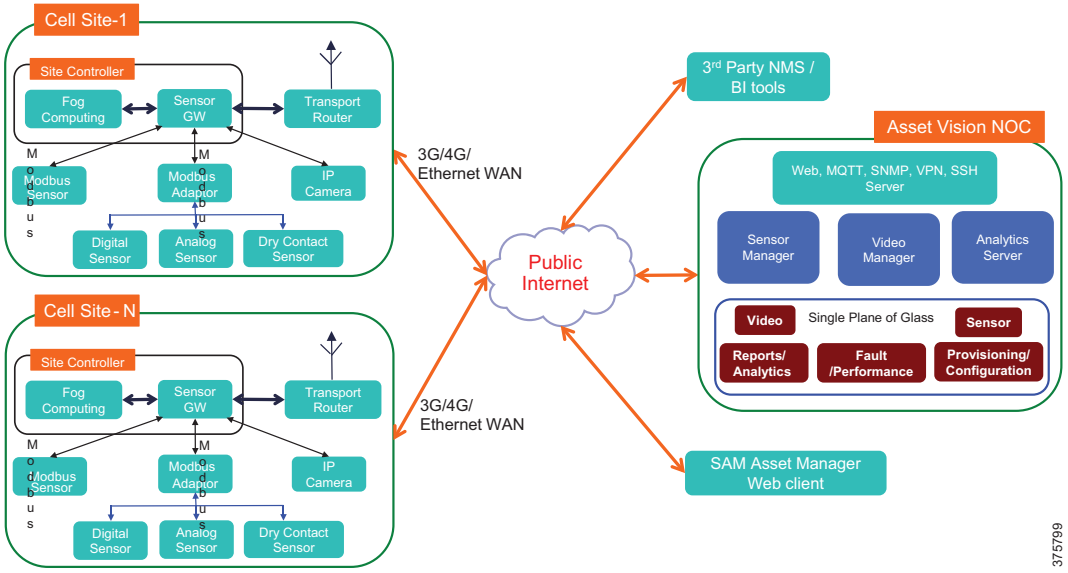
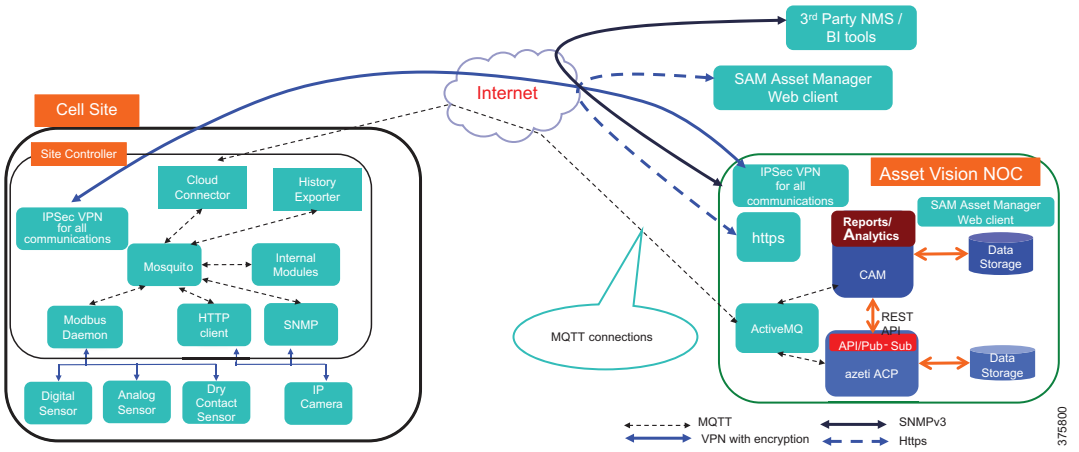


Figure 2-1 shows major functional blocks in the Connected Assets end-to-end system architecture. Multiple cell sites distributed geographically connect to the central NOC. As shown in Figure 2-1, the connectivity between the cell sites and the NOC can pass through the public internet. The functional blocks at the cell site are described in "Cell Site Architecture" and functional blocks at the NOC are described in "Network Operation Center Architecture".

End-To-End System Functional Blocks and Message Flow

The end-to-end message flow architecture is shown in Figure 2-2.

Figure 2-2 End-to-End Message Flow



In the NOC, the azeti Control Panel (ACP) and Cisco Asset Manager (CAM) are the front-end application servers. ACP provisions all sites and sensors. CAM query and gets configuration details from ACP using the rest API. ActiveMQ is the MQTT broker at the NOC end. PostgreSQL is the DB used by ACP.

ACP and CAM connect to ActiveMQ and subscribe to required MQTT topics. The cloud connector at the site controller is the MQTT client, which connects to ActiveMQ in the NOC. When required, the cell site to NOC connection is secured with a VPN tunnel. The site controller is the SG application at the cell site, which communicates with the sensors, does local processing and publishes the results to the NOC.

Mosquito is the MQTT broker and SQLlite is the DB used at the cell site. Various application processes at the cell site communicate with each other by exchanging MQTT messages via the Mosquito broker. Third-party NMS systems, Web clients and others hosted outside the NOC, communicate using one of the secured connections, such as, https, SNMPv3, https, and so on. Tomcat is the web server used in the NOC.

At the cell site Modbus daemon polls different sensors at regular intervals in a round robin fashion. The polling interval for each sensor can be configured. The collected sensor data is processed at the edge to check threshold crossovers. The threshold crossover events are published in real time to the NOC. Specific actions are taken locally based on different sensor data. The collected history records are published to the NOC at regular intervals.

IP cameras at the cell site are configured with a static IP address. Https is enabled on the camera; the session ID configuration is disabled. Communication to the camera is always initiated from the site controller over https. Only photos are taken; no live video streaming is supported. The trigger to take a photo is always initiated from the site controller to the camera with an http request. When the camera gets a trigger, it takes a photo and stores it in its local memory. The site controller gets the stored photo from the camera with an http request. At any given point of time, the camera needs to store only the latest photo. The collected photos are published to the NOC.

The cell site connects to the NOC using either a 3G/4G connection or Ethernet provided by the cell site operator. Appropriate routing, IP addressing and VLANs are configured for the communication to be possible. (Details are covered in “Cell Site Architecture”.)

Cell Site Architecture

Figure 2-1 shows a block diagram of various functional blocks at the cell site. This section describes these functional blocks and cell site network architecture.

Cell Site Functional Blocks

The functional blocks in the cell site include the following:

- Sensors: Sensors are transducers which sense or detect some characteristics of the environment and provides corresponding output. Different kinds of sensors supported by Connected Assets project are Modbus sensors and Non-Modbus sensors.
- Sensor gateway: Sensor gateways act as a gateway between sensor nodes and the end users, as they typically forward data from the end sensors to a central server. Typically, they are deployed on routers/switches that interface with the sensors.
- IP Cameras: IP cameras are deployed at the cell site for surveillance.
- Internet connectivity: Physical connectivity to the NOC.

Sensors Interface

This section describes the physical interface and communication protocol between the sensors and the sensor gateway.

RS485

RS485 is the physical interface between the sensor gateway and the sensors. RS485 is a serial interface. The key advantage of RS485 is it is simple and it can be used as a multi-drop communication link to connect multiple sensors. It offers data transmission speeds of 35 Mbps up to 10 meters and 100 Kbps at 1200 meters. A rule of thumb is that the speed in Mbps multiplied by the length in meters should not exceed 108. Thus, a 50 meter cable should not signal faster than 2 Mbps. RS485 electrical interface permit connecting up to 32 nodes. This number can be extended with repeaters.

It is preferable to have all sensors connected over RS485 to have the same serial communication parameters, such as, baud rate, parity, start, stop bits, and so on. However, different communication parameters for different sensors are allowed.

Modbus

Modbus is the communication protocol between the sensor gateway and the sensors. Modbus is a bus-oriented serial communication protocol. All communications are broadcast messages on the bus. It has one master and one or more slaves. The master always initiates the conversation by sending a query addressing a slave. Only the addressed slave responds to the query; all other slaves receive the request but they do not respond. A Modbus master can address up to 247 slaves and can address one broadcast address. Each slave can have a number of registers that the master can read/write. The stored data can be simple, discrete, or Boolean values, or can be of 16 bit unsigned value.

Modbus has the following three modes:

- Modbus ASCII
- RTU
- Modbus TCP

In case of communication over a serial interface, such as, RS485, the possible Modbus modes are ASCII and RTU. As the name suggests, Modbus ASCII packet carries data in ASCII format and RTU caries data in binary format.

Both Modbus RTU and Modbus TCP interfaces are supported. Modbus RTU is a prevalent sensor interface in the IOT industry. Modbus RTU sensors are inexpensive and are easily available in the local markets. The sensors can have Modbus natively or can interface via Modbus adapter. Sensors supporting Modbus interface natively are directly connected to the RS485 of the sensor gateway and they communicate using Modbus. Other sensors such as analog/digital/dry-contact sensors not supporting Modbus natively can be interfaced via Modus adapter.

Modbus TCP uses an identical command set, addressing modes and network representation as Modbus RTU. The same message that is transferred over RS485 using Modbus RTU is sent over a TCP/IP connection using Modbus TCP. This is a client and server architecture over TCP, where the client is the Modbus master and the server is the Modbus slave. The client queries the server over the IP network using the server IP and port 502. The server connects to the sensors and responds to the query. The set of sensors used with the Modbus RTU adapter can also be used with Modbus TCP adapter. For more information, refer to the following links:

http://en.wikipedia.org/wiki/Modbus

http://www.lammertbies.nl/comm/info/modbus.html

Sensors and Modbus Adapters

As discussed in the previous section, both Modbus RTU and Modbus TCP are supported. However, sensors with different interfaces, for example, analog sensors, digital sensors and dry contact sensors, and Modbus sensors can be connected to the sensor gateway. The sensors having Modbus RTU natively can be connected directly to the sensor gateway, whereas other sensors can be connected via a Modbus adapter.

The different Modbus adapters that interface with different types of sensors are described below:

Analog Modbus Adapters

These are adapters that interface between Modbus and analog sensors. One example of such an adapter is ADAM-4117-AE.

Digital Modus Adapters

These are adapters that interface between Modbus and digital sensors. One example of such an adapter is ADAM 4150-AE.

Dry Contact Modbus Adapters

These are adapters that interface between Modbus and sensors providing Boolean data. One example of such an adapter is ADAM 4150-AE.

Modbus TCP Adapter

The X20 series Modbus TCP adapter from B&R is tested as part of this solution. In this architecture, the site controller is the Modbus TCP master hosted on IR8x9. Similarly, the B&R X20BC0087 Modbus TCP bus controller is the Modbus TCP slave.

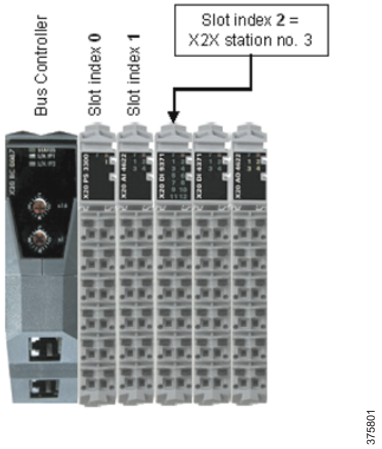
On one side X20BC0087 is connected to IR8x9 with Ethernet. The maximum distance between them is 100m, which can be extended with a standard Ethernet switch. On the other side, the X20BC0087 bus controller connects X2X Link I/O nodes. After it boots up, the bus controller detects all connected I/O modules, starts them and creates an internal image of the input and output data. The I/O data of I/O modules can be represented in different data types, for example, Word and bit.

X20BC0087 can support multiple interface I/O cards, such as Modbus RTU, digital, analog, Profinet, RS232/422/485, CAN bus, EtherNet/IP, and so on. Figure 3 shows an X20 controller with I/O cards.

For management support, the B&R FieldbusDESIGNER can be used for configuring the ModbusTCP bus controller and the connected I/O modules. The ModbusTCP Toolbox is available for system management and diagnostics.

The system has an IP rating of IP20 and has an operational temp range of 0 to 55^0 C.

Figure 2-3 X20BC0087 with I/O Cards



IP Cameras

IP cameras are connected to the POE port of a sensor gateway or an Ethernet switch. The sensor gateway communicates with the IP camera using https and controls its operations.

Real and Virtual Sensors

A real sensor is a physical sensor that measures some conditions, such as, temperature, humidity, door open, current, voltage, and so on. Virtual sensors are computed software derivation based on inputs from one or more real sensors. For example, a virtual power sensor can measure instantaneous power based on the physical inputs received from current and voltage sensors. Virtual sensors can be present at the cell site or even at the NOC side.

Sensor Gateway and Fog Computing System

Sensor gateways are middle devices between the end sensors and the NOC applications. Typically they are deployed on routers/switches that interface with the sensors. The capabilities of sensor gateways include types of interfaces supported to communicate with the sensors, local processing capability, capabilites to host third-party applications, and NOC interfaces supported, including data security. As the sensor gateway is close to the data collection point and it interfaces with often slow and intermittent links with the central NOC servers, data summarization at the sensor gateway is extremely useful and is an important feature. This capability is termed as edge computing of fog computing.

Fog computing extends the cloud computing and services paradigm to the edge of the network. Similar to cloud, fog provides data, compute, storage, and application services to end-users. The distinguishing fog characteristics are its proximity to the data collection point. Services are hosted at the network edge or even on end devices, such as, edge routers or access points. By doing so, fog reduces service latency, and improves QoS, resulting in superior user-experience. Fog supports densely distributed data collection points.

Three different models of the sensor gateway and fog computing devices are recommended to suit different requirements. A feature comparison of different recommended sensor gateway/fog computing devices namely IR809, IR829 and UCS-E is shown in Table 2-1.

Table 2-1 Sensor Gateway Feature Comparison

Features	ISR829	ISR809	ISR 4451 with UCS-E-180D M2
Serial Port	1xRS232 1xRS232/RS485 RJ45 instead of DB9	1xRS232 1xRS232/RS485 RJ45 instead of DB9	Not supported.
Serial port baud rate control from GOS	Not supported in the FCS.	Not supported in the FCS.	Not applicable.
LAN ports	4 LAN GE (POE) 1 WAN GE (SFP)	2 FE	Up to 48.
POE	Yes 802.3af MAX power: 30W	No	Yes Up to 48
3G	3G (HSPA+) (EVDO)	3G (HSPA+) (EVDO)	Yes
4G Support	4G(LTE) (Verizon, ATT, Global1, Global2, Sprint) Dual SIM support North America (AT&T and Canada), EU (-G SKU), and Australia (-Z SKU)	4G(LTE) (Verizon, ATT, Global1, Sprint) Dual SIM support. North America (AT&T and Canada), EU (-G SKU), and Australia (-Z SKU)	Yes (3G/4G LTE cellular card)
IP SLA supported	IP SLA supported	IP SLA supported	Yes
VM to run third-party applications	Supported	Supported	Yes
RAM	2 GB IOS: 700 MB GOS: 750 MB Hypervisor: 120 MB	2 GB IOS: 700 MB GOS: 750 MB Hypervisor: 120 MB	16 GB
SSD	No SD card 8GB eMMC No known read-write limit.	No SD card 8 GB eMMC No known read-write limit.	32 GB
CPU	Intel Rangley (2 to 8 cores, 1.25 to 2.4GHz)	Intel Rangley (2 to 8 cores, 1.25 to 2.4GHz)	Intel Xeon E5-2418Lv2 (2 GHz, 6 cores)
Site-to-Site VPN	Supported	Supported	Supported

Table 2-1 Sensor Gateway Feature Comparison

Features	ISR829	ISR809	ISR 4451 with UCS-E-180D M2
Management	Cisco IoT Field Network Director and Fog Director	Cisco IoT Field Network Director and Fog Director	Yes
Ruggedized	Yes IP54 IP67	IP30	-
Temperature	-40° to 167°F (-40° to 75°C)	-40° to 140°F (-40° to 60°C)	0 - 40C
Wi-Fi	2.4G/5G wifi	Not supported.	Not supported.

Fog Computing Considerations

- All events crossing the threshold are to be forwarded in real time.
- Set different water mark levels for thresholds. Different severity levels such as Critical, Minor and Clear, can be configured for different services. Refer to the Implementation Guide for details on configuring, thresholds and severity levels.
- History files compress before transmitting. History should be pushed every 5 minutes, when the connection is up. Preserve events and history data when the connection is down.
- All actions configured and executed locally; no connection to the server is needed.
- The polling interval is 500msec for low and normal priority services and 100msec for critical priority services (based on the baudrate and response delay from the sensor). Refer to the sensor data sheet.
- No change is needed in the polling interval or list of sensors polled based on the connectivity state to NOC.
- The Purge/Summarize history data is a low priority.

Transport Router

The transport router provides the physical connectivity between the cell site network and the NOC. Depending on the requirement, different alternatives for cell site routers are recommended namely, IR809/829/UCS-E. The cell site router needs to provide WAN connectivity, preferably with failover options. It also needs to provide a VPN connection with the NOC for a secured transport. The description for these deployment models along with their features comparison is given in a future section.

Interface between Cell Site Components and NOC

Sensor Interface

azeti SiteController is the sensor gateway software running on IR089/829. It is the single interface for all sensor communications between the cell site and NOC. MQTT is the messaging protocol used for this. Traps from the IP sensors (including cameras) are translated to MQTT messages and these MQTT

events are sent to NOC based on the configuration. To detect link failure between the sensor gateway and NOC, MQTT keep-alive can be set to 5 minutes. With this MQTT, a ping request is sent once in every 5 minutes (activity based) and a link failure can be detected.

Camera Interface

In CVD 2.0 there is no direct communication between the camera and NOC. All communications to the camera are routed via the sensor gateway. The sensor gateway also controls all camera operations.

Cell Site Network Architecture

IP Address and VLAN Considerations at the Cell Site

IR809/829 LAN interface and all cameras are to be on the same local subnet and VLAN. IPsec tunnel is set up from IR809/829 to the IPsec VPN server at the NOC. In case of 3G/4G, the dynamic IP address allocated by 3G/4G will be the IPsec tunnel end point IP address. In case of WAN, uplink the IP address configured at the IR809/829. This will be the IPsec tunnel end point IP address. In case of WAN, the IP address can be a public or private IP. However, reachability from the cell site to the VPN server needs to be ensured. The IPsec tunnel is always initiated from the cell site.

Cell Site Deployment Models

IR809 and IR829 are recommended as the preferred sensor gateway/cell site router devices for all deployment scenarios.

Three deployment models are recommended to suite to the needs of different cell sites. Different needs of the cell sites are as follows:

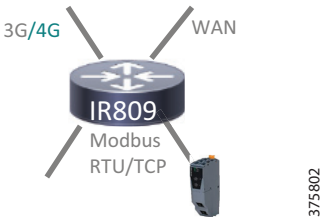
- Cell site having only Modbus RTU/TCP sensors
- Cell site having Modbus RTU/TCP sensors and cameras
- UCS-E used as a sensor gateway

The three deployment models are illustrated below. The first two are single box solutions and the third one requires an additional Ethernet switch to support POE for cameras.

Deployment Model-1

For the cell sites having only Modbus RTU/TCP sensors, IR809 can be used as the sensor gateway/ cell site router as shown in Figure 2-4. The Modbus RTU sensors can be connected to RS485 port and the Modbus TCP adapter can be connected to the Ethernet LAN port of IR809. The second LAN port of IR809 is used for WAN connectivity. Here, link failover is configured between the LAN link used for WAN connectivity and 3G/4G.

Figure 2-4 Deployment Model - 1: Sensor only Network with IR809



Deployment Model-2

For the cell sites having Modbus RTU/TCP sensors and up to two IP cameras can be deployed as shown in Figure 2-5. IR829 has four POE Ethernet ports with a maximum total power supply of 30.8W. Power allocated for a single 802.3af device is 15.4W, when no power negotiation happens through CDP. Thus, up to two cameras can be connected to 829 with POE. When more than two POE powered cameras are to be supported, an external switch such as IE-4000-4T4P4G-E is recommended.

Figure 2-5 Deployment Model - 2: Sensors and POE Powered IP Cameras

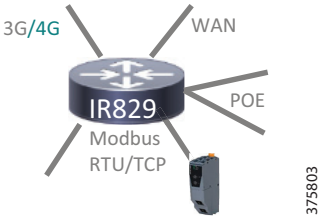


Table 2-2 summarizes the selection of different deployment models.

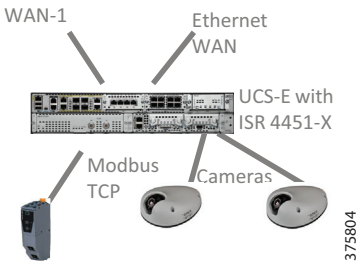
Table 2-2 Deployment Model Selection Matrix

Deployment Requirement	Recommended
Modbus RTU/TCP sensors only	Deployment Model - 1
Modbus RTU/TCP sensors with up to two POE powered IP cameras	Deployment Model - 2
UCS-E used as sensor gateway	Deployment Model - 3

Deployment Model-3

To cater to specific requirements the sensor gateway can be hosted on Cisco UCS-E servers as shown in Figure 2-6. UCS-E servers are housed within ISR 4000 or ISR G2 routers. Modbus TCP sensors can be connected to UCS-E over Ethernet. Due to lack of serial ports, Modbus RTU sensors are not used. The ISR 4000/ISR G2 routers support multiple WAN connectivity options.

Figure 2-6 Deployment Model - 3: UCS-E used as Sensor Gateway



WAN Connectivity

WAN Edge Router

The WAN edge router is the cell site router/gateway that connects the cell network to the service provider network and NOC. This could be the sensor gateway or an external router. Different connectivity options include 3G/4G and Ethernet. For Ethernet, the connection provided by the service provider at the cell site could be either L2 or L3.

WAN Connectivity Failure Detection

WAN connectivity failure is detected in multiple ways:

- MQTT keep-alive detects connectivity failure between the SG and the MQTT server in the NOC.
- For two-box-model, a transport router detects connectivity failure with the help of IPSLA.
- WAN Ethernet failure or degradation can be detected by configuring IPSLA in IR809/829. Ethernet is recommended as the primary WAN link and 3G/4G as the backup.

The following is the IP SLA recommended configuration:

- Type of operation to perform: icmp-echo
- Target address: VPN destination address
- Operation timeout (milliseconds): 5000
- Operation frequency (seconds): 5
- Verify data: No
- Life (seconds): Forever
- Reaction: timeout
- Threshold Type: X of Y
- Threshold CountX: 3
- Threshold CountY: 16

Network Operation Center Architecture

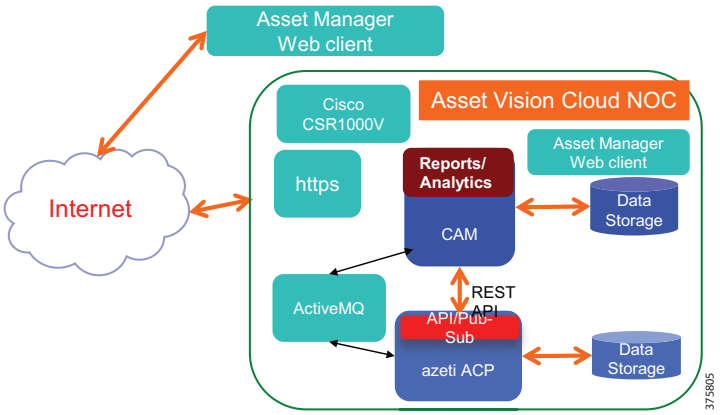
As discussed earlier, Connected Assets network operation center (NOC) can be hosted in a cloud or on customer premises. The following section describes the architecture for both of these.

NOC Cloud Architecture

The Connected Assets Network Operation Center hosted in a public or private cloud securely communicates with all sensor gateways at the cell sites. The functionality of NOC includes site provisioning, sensor data collection, monitoring the status of various parameters, generating alerts, and escalating alerts, presenting various fault/performance reports across sites to the operator. It is also responsible for providing North Bound Interface (NBI). Different servers responsible for this functionality include the azeti Control Panel (ACP) and Cisco Asset Manager (CAM).

Figure 2-7 shows components of NOC hosted in cloud. All applications in the cloud are hosted on VM. All servers have fixed IP addresses. The solution is tested using a Cisco cloud.

Figure 2-7 NOC Hosted in Cloud

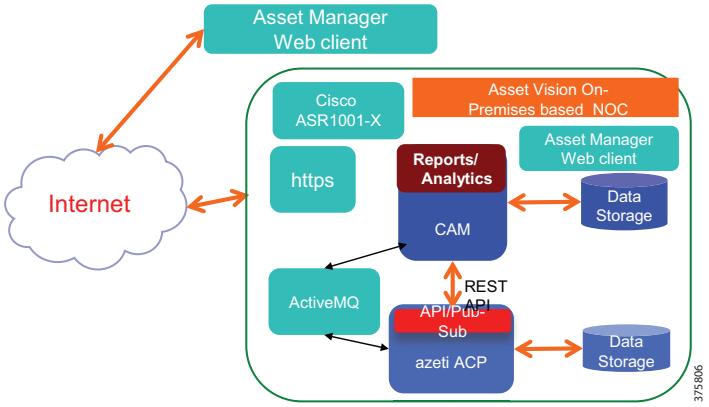


NOC On-Premises Architecture

Figure 2-8 shows components of on-premises NOC. All applications are hosted on VMs. Servers have fixed IP address. At the NOC side, VPNs are terminated at ASR1001-X.

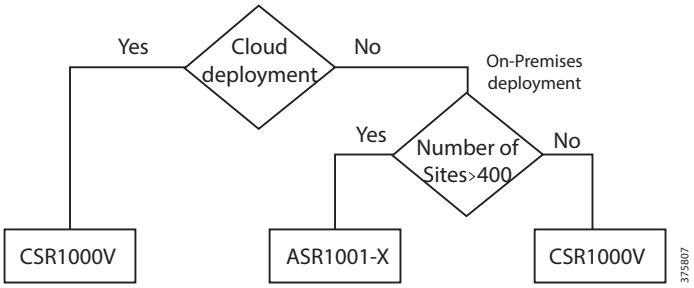
ASR1001-X has a crypto throughput of 8 Gbps. Each cell site has nearly a 50 Kbps crypto traffic requirement. Thus, a single ASR1001-X can cater to the requirements of 160,000 sites. For smaller deployments, up to 400 sites CSR1000V can be used, which matches its VPN termination limit. For larger deployments, ASR1001-X is recommended.

Figure 2-8 NOC Hosted On-Premises



Selection of the VPN terminator at NOC is shown in Figure 2-9.

Figure 2-9 VPN Terminator Selection



The only allowed communication channel between the cell site router and NOC is VPN tunnel traffic and ssh traffic. All other communications are blocked.

L3 IPV4 ACL: At the cell site router on the WAN link, the following ACLs are applied:

- Allow all traffic to and from TCP port 500 (IKE VPN NOC end point).
- Allow ssh from any source (for debugging purpose and for access from vendor site).
- Deny all other traffic (deny ip any any).

Connected Assets NOC Functional Blocks

- Communication Servers: Different interfaces are possible to communicate with the NOC servers. These interfaces include: Web (https), SNMP, VPN, SSH, MQTT, and so on.
- Network Operation Center (NOC): For the Connected Assets, can be hosted in a cloud or on customer premises. Various NOC applications such as Sensor Manager, Video Manager, Analytics Manager, and so on, are part of the NOC.
- North bound BI system: The Connected Assets NOC applications can interface with customer workflow/BI systems and NMS systems. Different NBI could be SNMP, MQTT, XML, and so on.
- Asset Manager Web Client: This is a user-friendly management console, where an operator can monitor, manager the entire network from a web client. The client presents information from all kinds of sensors and camera. It also visualizes various live fault, performance data, as well as, trend charts from historical data.

North Bound Interface

Customers can have different third-party business management systems (BMS) and NMS systems. The NOC needs to interface with these third-party systems. The possible NBI supported by the NOC includes SNMP, MQTT, and http.

Security Architecture

Security is one of the most important aspects, as the assets are spread over geography and are connected via public network to the central management station. However, if the cell sites and NOC are connected via a secured private network owned by the customer, then additional security measures could be optional.

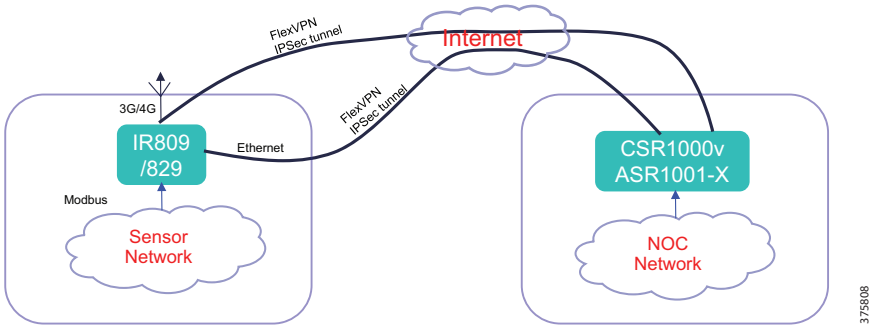
Network Security

When required, communication channels between the cell site and the servers in the NOC are protected by an IPSec tunnel. The recommended VPN server in the cloud deployment is Cisco CSR1000V router. For on-premise deployment, either Cisco CRS1000V or ASR1001-X can be the VPN server. All communications are authenticated and encrypted. When the Ethernet fails and the connection is switched to 3G/4G, a new tunnel is set up via 3G/4G. Tunnel creation is always initiated from the cell site by the cell site router IR809/829. Figure 10 shows IPSec tunnel end points.

FlexVPN is the recommended VPN model. FlexVPN is based on open standard based IKEv2 as the security technology, providing many Cisco-specific enhancements.

FlexVPN is the latest VPN model from Cisco. Some key advantages of FlexVPN are, it is designed to simplify the deployment of VPNs and it encompasses all features of various VPN models, such as, EZVPN, CryptoMap, and DMVPN. Cisco IOS-based routers, such as, ISR, ASR, CSR and others, support FlexVPN. Figure 2-10 shows the IPSec tunnel between IR809/829 at the cell site and VPN server at the NOC.

Figure 2-10 IPSec Tunnel End Points



Application Security

Cell Site Security

All communications to the cell-site are protected with a VPN. Access to devices at the cell site is authenticated with username and password. Direct access is available only via SSH.

Other Security Considerations

Security considerations, such as the maximum number of simultaneous MQTT client connections to be allowed by different MQTT brokers, is given in Table 2-3.

Table 2-3 Other Security Considerations

Server Location	Maximum Number of Client Connections	Subscription to Topics	azeti Support/Compliance
Mosquito MQTT broker at the cell site (sensor gateway)	20	All topics	Comply
ActiveMQ MQTT broker at NOC	1200	All topics	Comply Limit using the ActiveMQ configuration file.

QoS Architecture

Network QoS

Since the Connected Assets traffic passes through the public internet, no QoS parameters such as latency, jitter, packet loss, and so on, are guaranteed for the traffic. The desired network bandwidth is computed and that is to be provisioned to ensure smooth system operations.

Application QoS

MQTT Keep Alive

The keep-alive is a16-bit value measured in seconds. It is the maximum idle time permitted between control packets sent by the client including PINGREQ. The keep-alive value is defined during the connection setup. Server disconnects the client connection upon non-receipt of any control packet for 1.5 times the keep-alive time. The client can send PINGREQ at any time to determine the up status of the network and the server. A keep-alive value of zero turns off the keep-alive mechanism. In this case, the server is not required to disconnect the client on the grounds of inactivity. Typically, the keep-alive time is kept for a few minutes. The maximum value is 18 hours 12 minutes and 15 seconds.

Message Delivery Priority

No delivery priority can be guaranteed for different message types because the delivery is across the internet. Events are published on a separate connection and history on a separate connection. No out-of-band channel is supported by MQTT. All events are scheduled in FIFO.

The following is a reference link to MQTT:
http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html

Guaranteed Message Delivery (MQTT QoS)

QoS 0: At Most Once Delivery (Best Effort)

The message is delivered according to the capabilities of the underlying network. The receiver sends no response and no retry is performed by the sender. The message arrives at the receiver either once or not at all.

QoS 1: At Least Once Delivery (Guaranteed)

This quality of service ensures that the message arrives at the receiver at least once.

QoS 2: Exactly Once Delivery (Guaranteed and No Duplicates)

This is the highest quality of service, for use when neither loss nor duplication of messages is acceptable. There is an increased overhead associated with this quality of service.

Table 2-4 summarizes the recommended MQTT guaranteed delivery level for various message types.

Table 2-4 MQTT Guaranteed Delivery Levels Configuration

Message Type/Topic	Recommendation	MQTT QoS	azeti Support/Compliance
Ping requests	Best effort	QoS 0	Comply
Events	Guaranteed delivery No duplications Encryption	QoS1 (At least once)	azeti is using QoS1 for events. Duplicates are removed at the server.
History data	Guaranteed delivery No duplications Zipped file Encryption	QoS1 (At least once)	QoS1 used. Each history file zipped and separate message File/Record duplication checked at NOC.
XML upload (from NOC to device)	Guaranteed delivery No duplications File Integrity check Data correctness check	QoS1 (At least once)	QoS1 used. Each XML file separate message File duplication checked at device. Integrity of the file is checked with md5. File data validated by a process.

Protecting the Client from Storage Overflow during Server Link Down

Events older than a week are purged at the device.

History data files are zipped and published at a configurable interval when the connection is up. The interval configured as 5 minutes.

When the connection is down, the files are kept on a local disk/RAM uncompressed and data is never purged.

The history file is rotated on a daily basis and maximum of five copies are kept. Table 2-5 summarizes the log-rotation policy for various log files.

Table 2-5 Log Rotation Policy

Log File Name	Rotation Frequency	Maximum Log File Size (Based on Disk Space Requirement Computation)	Number of Copies
History	Daily	1 MB	5
Debug files	Daily	1 MB	5

SAM Asset Manager

The CAM user interface provides most of the network management functionality. CAM interfaces with ACP to provide these functionalities. Operations such as configuration, provisioning, fault, performance, and so on, are all supported by CAM. The user needs to access ACP for device logs and debugging related information.

The following are operations supported by CAM user interface:

"Configuration of all sensors and all sensor-related parameters (communication parameters, polling intervals, priority, and so on)

"Configuration of actions on device (actions-based events)

"Live alarm monitoring (events/alarms monitoring/alarm panel)

"Live performance monitoring (graphical and tabular performance data)

"Performance reports (analytics, summary charts, trend charts, correlation reports)

"Performance and fault reports across cell sites

"Performance and fault reports across sites and tenets (multi-site and multi-tenant)

"Camera photo viewing (recent and history)

"North Bound Interface (Alarms) - SNMP

Browser Requirements

Cisco SAM Services has a browser-based management console for configuration, operation, and reporting; it uses JavaScript. For the best user experience, it is recommended that an up-to-date browser with fast and efficient JavaScript support, such as, the latest version of Google Chrome or Mozilla Firefox, is used.

It is not advisable to use any versions of Internet Explorer, especially IE 8 and before.

Regardless of which browser is used, JavaScript needs to be enabled.

Remote Access

The Cisco SAM Services server is administered through a web interface. By default, both port 80 (HTTP) and 443 (HTTPS) are supported. For security reasons, it is highly recommend to open port 443 (HTTPS) only for remote administration and client connections.

Notification E-Mails

Cisco SAM Services can generate notification emails for fatal system errors, low resources, or if the license expires. To enable email notifications, the email account details needs to be configured. These settings are also used to send scheduled favorite reports or other sources via email.

Cisco SAM Services will email a notification if one the following events occur:

- The amount of devices exceeds the licensed number.
- The product is not licensed.
- A resource drops below its threshold.
- The service terminates unexpectedly (for example, crash, out of memory/disk space).
- A new update is available.
- An update is being installed.
- An update was successfully installed.
- An update failed.

In addition to those events this mail configuration is also used to send emails during the following:

- Sending System Notifications, for example, in policies or alerts
- Sending scheduled favorite reports

CAM Functionality - Reports and Analytics

Refer to CAM documentation for report generation capability and their dimensions (time and count-based reports, statistics-based reports, reports across cell sites, and so on). Define reports based on use cases. It is possible to view performance reports in graphical form, show previously stored reports, schedule report generation for standard and customized reports and view critical performance metrics.

The Cisco CAM Server can be hosted in a public or private cloud or can be hosted on the customer premises. CAM software is packaged with a PostgreSQL database to collect energy information about all devices.

Representative set of reports:

As mentioned, CAM is a generic reporting tool and customers can generate multiple reports suiting their specific needs. To show the flexibility, a sample set of reports that can be generated by CAM are listed below:

- Monitor site security

  - How many times the door was opened during a month?
  - How long was the site in an un-armed state?
  - How many failed attempts to open the door?
  - How many brute force attacks to open the door?
  - How many times was the door opened with keypad and opened from remote?
  - Report list of snaps taken by a cell site for a period of time.
  - How many man-down events noted in a year?
- Environmental monitoring and advanced analytics
  - What is the average, minimum and maximum temperature noted in a month?
  - What is the duration external temperature was outside the operating range?
  - Humidity monitoring, average, peak and minimum over a day/week.
  - How long was the air conditioner running?
  - Correlate environmental temperature and air conditioner power consumption.
  - Correlate power consumption with external temperature, air conditioner run time and system up time.
  - Define air conditioner maintenance schedule based on running hours.
- Power and generator monitoring
  - HVAC power source power quality report: voltage fluctuations, frequency fluctuations, power cut pattern and duration.
  - Generator run time during a month/week/day?
  - Generator fuel consumption report per day/week/month. Fuel refill alerts.
  - What is the rate of consumption of fuel per run time of the generator?
  - Number of times fuel leak/theft detected?
  - Generator power quality reports: Voltage, frequency.
  - Generator power consumption reports: Units.
  - Generator startup battery status report.
  - Generator maintenance schedule based on running hours.
  - Power consumption per asset type, such as, air conditioner and per equipment rack.
  - HVAC three phase load distribution.
  - Power theft detection.
- Multi-tenant reporting
  - Individual power consumption reports for each tenant in a site.
  - Individual power requirement and prediction reports.
- Statistics reporting
  - Number of threshold cross notifications.
  - Number of critical, major events reported in a month.
  - Network bandwidth reports, peak and average bandwidth.
  - Average storage requirement over a month.

- Cell link down events and duration report.

System Components

Cisco Products

A list of Cisco products used in Connected Assets CVD 2.0 solution is shown in Table 3-1.

Table 3-1 Cisco Components

Cisco Product	Software Release	Description
CIVS-IPC-6400E CIVS-IPC-7030E	CIVS-IPC-6xxx-V2.5.0-10.bin CIVS-IPC-7xxx-V2.5.0-10.bin	These cameras are tested as part of CVD testing. In general any Cisco IP camera with OpenAPI can be supported.
CAM	5.1	Sensor network monitoring, analytics and reporting tool. NOC software.
IR809G-LTE-GA-K9 IR809G-LTE-NA-K9 IR809G-LTE-VZ-K9		GA: Australia, Europe, Middle East, LATAM and APAC (depending on specific operator supporting bands) NA: LATAM and APAC (depending on specific operator supporting bands), USA (ATT), Canada VZ: USA (Verizon)
IR829GW-LTE-GA-EK9 IR829GW-LTE-GA-ZK9 IR829GW-LTE-NA-AK9 IR829GW-LTE-VZ-AK9		GA-EK: Global (Europe), LATAM and APAC (depending on specific operator supporting bands) GA-ZK: Global (Australia), LATAM and APAC (depending on specific operator supporting bands) NA-AK: LATAM and APAC (depending on specific operator supporting bands), USA (ATT), Canada VZ-AK: USA (Verizon)
IE-4000-4T4P4G-E		4 FE, 4 POE, 4GE combo uplink

Third-Party Products

A list of third-party products used in Connected Assets CVD 2.0 solution is shown in Table 3-2.

Table 3-2 Third-Party Products

Vendor Product	Release	Description
Sensors	Refer to Table 3-3	Modbus and non-Modbus sensors.
Site Controller	1.2.0	Sensor gateway software.
azeti Control Panel	0.3.12	Sensor configuration and provisioning tool. NOC software.
X20BC0087	2.3	MODBUS TCP (Base Module)
X20PS9400		Power Supply
X20DI9372		12x Digital Inputs
X20DO6639		6 Relays outputs (DO), 240 VAC
X20AI4622		4x Analog Inputs, 4-20MA or 0-10V
X20AP3131		AC Meter, 480 VAC, 50/60 Hz, 5A sec. current

Modbus and Non-Modbus Sensors and Applications

The list of Modbus and Non-Modbus sensors that are tested as part of CVD 2.0 are given in Table 3-3. However, in general any Modbus RTU/TCP sensors can be supported by the solution. Modbus sensors can be serially daisy-chained and connected to the serial ports. Non-Modbus sensors are connected to an adapter, which translates the received packets from analog/digital/dry-contact to Modbus over serial packets.

Typically, any sensor that can be connected to Modbus RTU can also be connected to Modbus TCP with B&R adapter.

Table 3-3 List of Modbus RTU Adapters and Sensors Tested with a Brief Description

Vendor	Product	Description	Remarks
Advantech	ADAM-4117-AE	Eight analogue inputs, analog to digital converter	RS485 MODBUS For example, quantization of voltage output of pressure sensor
Advantech	ADAM 4150-AE	Seven digital inputs, eight outputs	RS485 MODBUS For example, sense switch on and off state/dry contact output
Elkor	i-Snail-VC	AC current sensor	Analog input For example, monitor electrical load

Table 3-3 List of Modbus RTU Adapters and Sensors Tested with a Brief Description

Vendor	Product	Description	Remarks
Elkor	WattsOn-1100-MS16 0-120A	AC power meter Can monitor up to three single phase loads or one three-phase load	RS485 MODBUS output
Elkor	i-Snail-S	Current switched sensor, monitoring on/off state of a device	Digital input For example, detect electrical load on/off state
Elkor	MS160	Current transducer, for POC only needed one phase. Current measuring with clamped upper limit.	Connected to WattsOn
CE-Transducers	AD11B-34GS4-1.0/0 -50A*0-65V	DC multi-parameter monitoring (U,I,P,KWh)	RS485 MODBUS
CE-Transducers	CE-AU11-34MS3-0.2 /0-65V	1-element DC Voltage Meter	RS485 MODBUS
Comet	Magnetic door contact SA-200-A	Door contact, digital output	Digital input
Schneider Electric	NSYS3D6640P	Enclosure	
Comet	T3411	Temperature/Humidity Sensor	RS485 MODBUS
Infranet	WTSC-485 Wiegand to RS-485 Converter (for keypad)	Converter for the keypad	RS485 MODBUS
AST Sensors	AST 4510 - Pressure Sensor	Fuel level sensor	Analog input
HIDGlobal	Keypad Proxpro including Converter HIDGlobal 5355 WTSC-485	Security keypad	Weigand

System High Availability and Scalability

System Redundancy and High Availability

Redundancy for Communication Link

Different Deployment Models (IR809/829)

IR809/829 support IPSLA, hence a WAN link auto switchover can be supported. The IPSLA recommended configuration is described in a previous section. Thus, 3G/4G is configured as backup for Ethernet with auto switchover and reverting capability. In case connectivity to NOC via Ethernet fails, the system switches the connection to 3G/4G and reverts back when the connection via Ethernet is restored. The IP SLA is configured to monitor "icmp-echo" and switchover if 3 or more echo requests fail out of 16 requests, and revert back if less than 3 requests fail.

Redundancy for Server Applications at NOC

In CVD 2.0, redundancy/load balancing for the NOC applications (such as ACP, CAM, ActiveMQ, DB servers, CSR1000V, ASR1001-X, and so on) is not considered.

Scalability and Bandwidth Requirement

The system should support polling of up to 50 data points (services) from each serial port. A polling interval up to 500msec is supported without any event loss. Up to ten sensors with a polling interval of 100msec is possible. The CPU utilization should be below 90% and load average should be below 5. The system supports the network bandwidth and storage requirements shown in Table 4-1, without any impact on the performance and stability.

Table 4-1 Network Bandwidth and Storage Requirements

Number of events per day (services crossing threshold)	10	Maximum tolerable event latency in seconds	5	Photo interval in seconds	300
				History update interval in seconds	300

Table 4-1 Network Bandwidth and Storage Requirements

Types of messages	Peak Hour Messages per Second	Message Size in Bytes	Average BW Requirement (Kbps)	Number of Messages Stored in a Day	Storage per Day in MB	Storage per Month in GB for 1000 Cell Sites
ping	1	64	0	0	0	0
Events (threshold cross)	10	500	8	10	0	0
History update	1	3846	6			32
Photo from camera	1	20000	32	288	5.5	166
Total			46		7	198

Based on the computation shown in Table 9, the following bandwidth and storage requirements are recommended:

- The storage requirement at the NOC per month for 1000 cell sites is 200 GB.
- The storage requirement at the device to store data for one day when connectivity link is down is 7 MB. This does not include debug and log files.
- Downlink bandwidth requirement is minimal, since very minimal messages are sent in the downlink direction.
- Bandwidth requirement between the sensor gateway and NOC with 5 seconds allowed message latency is 46 Kbps.

Server Sizing Details

Storage space requirement for 1000 cell sites for one-month data storage: 200GB

Up to 500 web-clients connect in parallel to the webserver and MQTT.

Server recommendations for different size network deployment classified as small, medium and large are as follows:

- Small instance 8 GB RAM, 2 cores 100 GB
- Medium instance: 16 GB RAM, 4 cores 500 GB
- Large instance: 32 GB RAM, 8 cores 2 TB

Server Sizing and Bandwidth Recommendations

Based on the number of cell sites the network can be classified into three categories: small deployments up to 100 cell sites, medium deployments up to 500 cell sites and large deployments up to 1000 cell sites. A non-cloud based NOC is recommended for deployments larger than 1000 cell sites.

The server sizing in the cloud for three deployment categories is as follows:

Small Deployments

Server sizing in the cloud up to 100 cell sites, with a maximum of 10000 sensors total (see Table 4-2).

Table 4-2 Server Specification for Small Deployments

Server sizing for ACP	Two medium size servers (Medium size server: 16 GB RAM, 4 cores 500 GB)
Server sizing for CAM	VM-1 hosting one application server and one controller (1 Quad Core, 8 GB RAM, 250 GB disk space)

Medium Deployments

Server sizing in the cloud up to 500 cell sites, with a maximum of 50000 sensors total (see Table 4-3).

Table 4-3 Server Specification for Medium Deployments

Server sizing for ACP	Three medium size servers (Medium size server: 16GB RAM, 4 cores 500 GB)
Server sizing for CAM	VM-1: hosting one app server (1 Quad Core, 16 GB RAM, 500 GB disk space) VM-2: hosting one controller (1 Quad Core, 16 GB RAM, 100 GB disk space)

Large Deployments

Server sizing in the cloud up to 1000 cell sites, with a maximum of 100000 sensors total (see Table 4-4).

Table 4-4 Server Specification for Large Deployments

Server sizing for ACP	Three Medium size servers (Medium size server: 16 GB RAM, 4 cores 500 GB)
Server sizing for CAM	VM-1: hosting one application server (2 Quad Core, 24 GB RAM, 1 TB disk space) VM-2: hosting one controller (1 Quad Core, 16 GB RAM, 100 GB disk space each) VM-3: hosting one controller (1 Quad Core, 16 GB RAM, 100 GB disk space each)

Server Sizing for On-Premises NOC Deployment

The server sizing requirement for on-premises deployment are the same as cloud deployment. The UCS server selection for on-premises deployments is shown in Table 4-5.

Table 4-5 On-Premises Server Sizing and Selection

	Small	Medium	Large
CPU cores	12	20	28
RAM	40 GB	80 GB	104 GB
Disk	1.25 TB	2.1 TB	2.7 TB

The UCS-C220M3 LFF box has (UCS-CPU-E52660B) 20 CPU cores, out of which two CPU cores are reserved for the hypervisor. The remaining 18 CPU cores can be used by applications. Each box can have up to 512 GB of RAM. Up to four SAS drives with 1 TB (UCS-HDD1TI2F212) each are supported. With RAID5, three drives per box are needed. Thus, per box, 2 TB disk space will be available.

The requirements for the small and medium deployments can be met with a single UCS-C220M3 LFF box (considering 18 CPUs is acceptable). Large deployment will require two UCS-C220M3 LFF boxes. External SAN storage is not considered for the current phase.