



Distributed Intelligence Platform (DIP) Reference Architecture Volume 1: Vision Overview

Authors

Name	Email	Role
Stuart Laval	Stuart.Laval@duke-energy.com	Emerging Technology Development
Bill Godwin	Bill.Godwin@duke-energy.com	Telecommunications System Architect

Revision History

For the latest revision of the document, please refer to the contacts above.

Date	Revision #	Reason for change(s)	Author(s)
08/18/2014	1.0	New	Stuart Laval, Bill Godwin
01/05/2015	1.1	Updated logo and figures 2-2, 3-1, 3-5, 3-6, 3-7, 3-9. Changed footer.	Stuart Laval

Table of Contents

1. Introduction.....	3
1.1 Document Context	3
1.2 Historical Perspective	3
1.3 Purpose.....	3
1.4 Objective	4
1.5 Operational Challenges Driving Distributed Intelligence Platform.....	4
2. Architecture Vision Statement.....	6
3. Platform Overview	8
3.1 Platform Vision.....	8
3.1.1 Hardware Considerations.....	9
3.1.2 Deployment Considerations.....	11
3.1.3 OSI Model.....	12
3.1.4 Connectivity	12
3.1.5 Computing.....	12
3.1.6 Field Message Bus Architecture	13
3.2 Hierarchical Application of Distributed Intelligence Platform Nodes	16
3.2.1 Network Definitions and Diagram.....	18
3.2.2 Node Tier Hierarchy Definitions	19
3.2.2.1 Tier 1	20
3.2.2.2 Tier 2	21
3.2.2.3 Tier 3.....	23
3.2.2.4 Tier 4.....	24
3.2.2.5 Tier 5	25
4. Software Considerations.....	27
4.1 Operating System.....	27
4.2 Node Element Management System.....	28
4.2.1 Firmware Management	28
4.2.2 Configuration Management	28
4.2.3 Network Management.....	29
4.3 IP Networking.....	29
4.4 Security Considerations	29
4.5 General Utility Protocol Support	30
4.6 Message Bus Protocols	31

1. Introduction

1.1 Document Context

This document is intended to be an overview of the distributed intelligence platform (DIP). It is Volume 1 of a four-volume set. This is the foundation that Volumes 2, 3 and 4 are built upon. Volume 2 addresses hardware functional requirements and associated deployment considerations. Volume 3 addresses software applications and associated data management. Volume 4 documents the comprehensive security requirements, but all of the volumes should be considered together in order to meet the end-to-end security capabilities of the DIP reference architecture. For the latest revision of each document, please email the contacts referenced on the title page.

1.2 Historical Perspective

Historically, the overall coordination and management of the electric power system has primarily been delivered through centralized management systems. This mode of operation has served the utility industry well for a number of years. However, with the evolution of more and more intelligent field devices generating massive amounts of data, along with the dynamic landscape of distributed generation, bidirectional load flow, and customer driven technologies such as electric vehicles and home automation systems, a new model employing both centralized and distributed information management is necessary to enable the effective management of the electric power system in this new environment. The need for distributed processing is also driven by the growing trend to support the integration of information technology (IT) and operational technology (OT) systems.

1.3 Purpose

A reference architecture is intended to help hardware and software developers accelerate the development and production of scalable products that integrate the capabilities of a number of previously discrete devices. Duke Energy additionally defines reference architecture as a starting point for utility product specifications as well as a stable functional target for suppliers to adopt.

The purpose of this document is to present a reference architecture for a distributed intelligence platform to serve as a blueprint to accelerate both the adoption of technologies and expedite the realization of their respective values as the grid environment evolves to its future state.

While standards and interoperability initiatives are underway, their collective outcomes are being narrowly applied, thereby limiting their benefits to the industry. This reference architecture provides a technology strategy that will holistically leverage standards-based solutions to realize these benefits consistently across multiple stakeholders.

1.4 Objective

An overall objective of an electric utility is to provide a more efficient, reliable, and maintainable electric power system and the development of enhanced information management systems is a necessary prerequisite to facilitate this. The goal of this document is to define the reference architecture for the Distributed Intelligence Platform (DIP), which will serve as an integral part of that enhanced information management system.

The objective of this reference architecture is to formalize and document Duke Energy's technology roadmap for enabling the operation and management of the electric power system in a non-invasive and affordable manner by employing open standard, interoperable, and distributed information systems. This platform will augment Duke Energy's legacy information systems infrastructure and allows seamlessly integration with future systems, equipment, and applications. The key platform attributes that allow for successful integration are standard communications via internet connectivity, interoperability via local data access, and distributed intelligence implemented on standardized and unified platforms providing security, analytics and network management. When implemented, this architecture will harmonize various central and decentralized systems, communicating in both synchronous and asynchronous manners resulting in increased business intelligence and operational efficiencies.

Interoperability is the key to helping utilities operate the electric power system more simply and cost effectively, while also enabling better service to customers. Historically, the integration of information systems in the back-office to achieve interoperability has been expensive and time consuming. The electric power system of the future will need to exchange information with different devices from many manufacturers locally in the field (outside of the central office) in order to achieve enhanced operational capabilities. In addition, traditional utility technologies, and the associated data, are often siloed as they typically utilize proprietary, prepackaged hardware, telecommunications, and software platforms that backhaul data to a centralized hub.

This reference architecture is intended to foster industry collaboration and evaluation of device interchangeability on remote computing devices or systems by further developing technology requirements to realize the benefits of interoperability. This is important because of the benefits it can provide for customers by enabling value-added services from the electric grid, and the benefits it creates for the company, making disparate systems work well together at a lower cost.

1.5 Operational Challenges Driving Distributed Intelligence Platform

Duke Energy's technology roadmap and Distributed Intelligence Platform (DIP) reference architecture are driven by a number of emerging challenges that are not adequately or efficiently addressed by traditional utility technologies and associated data that are often siloed in the proprietary, prepackaged hardware, telecom, and software systems. One of the key elements of the ongoing evolution of the electric power system is the accelerated deployment of Distributed Generation (DG) systems, such renewables (solar, wind), microgrids, and storage. The conventional information systems that were designed to support a few large primary generation facilities will be challenged to adequately support this evolving DG environment along with new consumption modes, which create new models for the generation, distribution, storage, and consumption of electric energy.

Other operational challenges include the need to support and manage:

- Bidirectional load flow
- Unified enterprise security
- Premise interaction (Home automation, thermostats, smart appliances, etc)
- Monitoring & diagnostics and grid optimization
- IT/OT integration
- Timely access to actionable operational device data in the field

In order to effectively address these operational challenges, the DIP reference architecture provides the following benefits that are not sufficiently met by the existing utility infrastructure:

- Reduced total cost of ownership (TCO)
- Scalable data and information management
- Near-real-time (sub cycle) response times
- Enhanced situational awareness
- Interchangeability
- Distributed control
- Greater energy efficiency

2. Architecture Vision Statement

In order to meet the efficiency, reliability, and environmental requirements of the 21st century, aging electromechanical analog devices comprising today's grid must be replaced with automated intelligent digital devices to enhance the ability to monitor and control the flow of electricity, to seamlessly integrate with distributed energy resources, and easily scale to handle millions (and potentially billions) of discrete data points in a secure, timely, and cost-effective manner.

Consequently, the modern grid must be able to adapt from proprietary, isolated, and single-function (a.k.a. siloed) centralized management systems to a multi-function and integrated distributed grid management systems that will simultaneously employ both decentralized and centralized systems in a highly coordinated manner. Figure 2-1 identifies select features and their respective differences between current and future states of the grid, the emerging challenges impacting these states and the 5-pronged strategy for meeting these challenges to maintain a safe, reliable, affordable and sustainable electric power grid. In summary, the goal of the Distributed Intelligence Platform (DIP) reference architecture is to address these identified emerging challenges by recommending an Internet protocol (IP)-based solution that can translate, contextualize, secure, and analyze information, independent of the hardware, software, or telecommunications implementations.

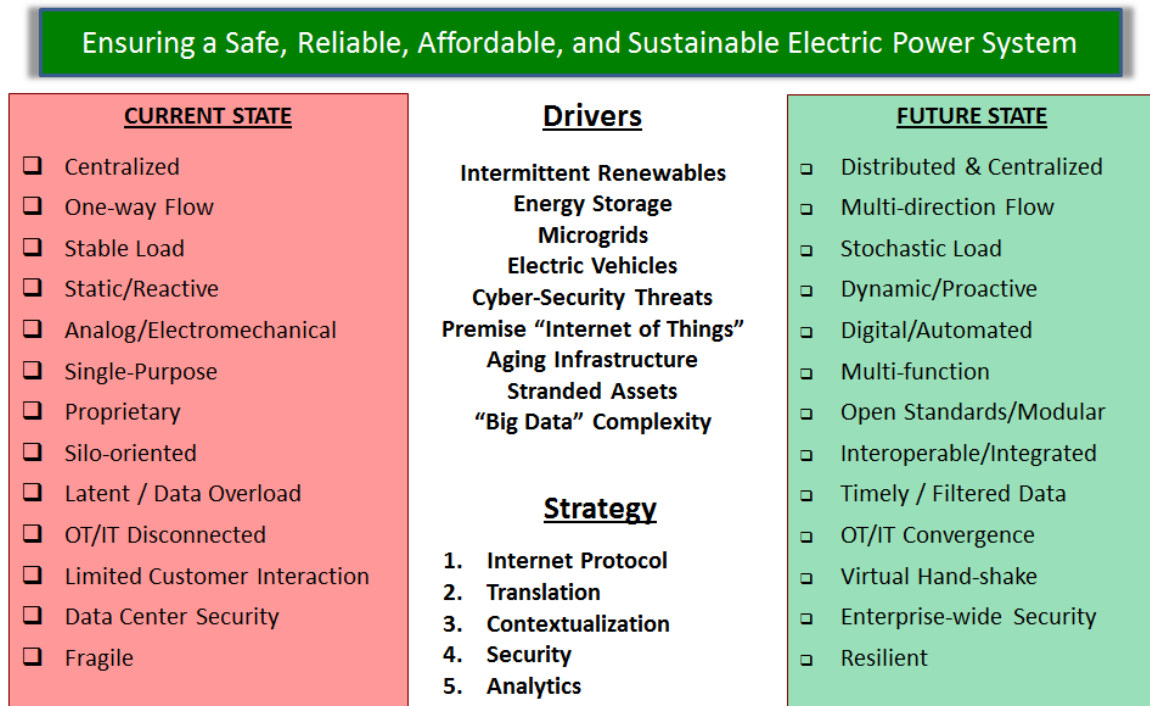


Figure 2-1: Current versus Future State of the Electric Grid

The core elements of the Information System network represented in Figure 2-2 consist of operational technology devices, two-way wired and wireless telecommunications, and logical software architecture elements. This network system should support the ability to quickly, reliably, and securely collect, organize, and analyze large volumes of data and develop actionable

information without overwhelming the centralized systems. An information system consisting of a hybrid, of both centralized and decentralized, processing systems can help provide this functionality. This distributed information system will help with processing, resolving, and delivering the large amount of actionable data needed to effectively manage and control the electric power system. In addition, it will be able to support immediate near real time decision making based on locally available information and also deliver appropriate trending and other actionable information to other information system. Distributed intelligence will allow the dynamic analysis of information and the relaying or sharing of important information, while discarding redundant or non-important information.

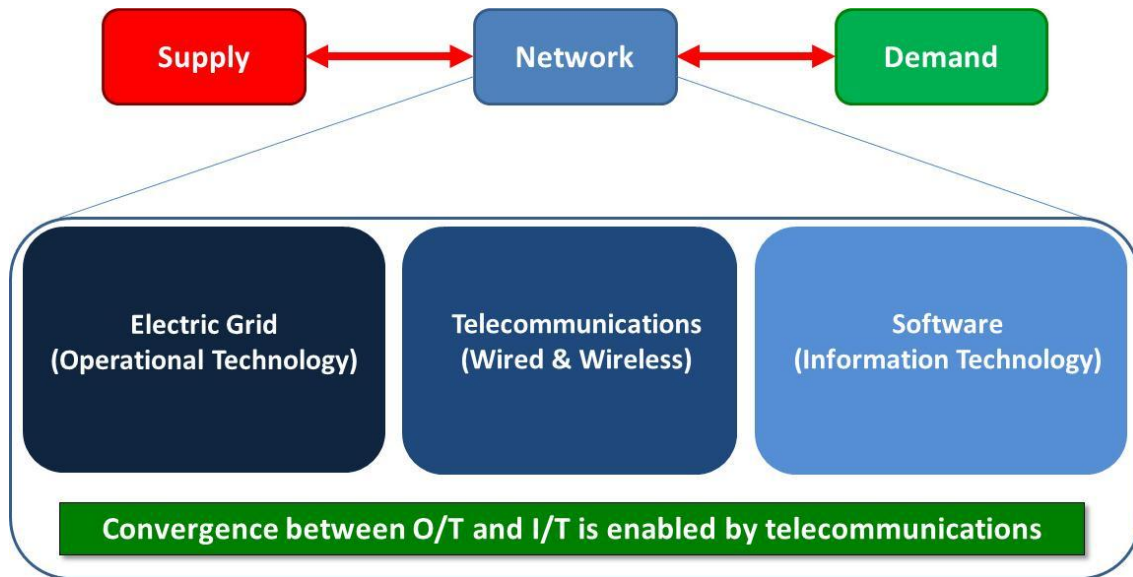


Figure 2-2: The Core Elements of Duke Energy's Smart Grid Architecture

3. Platform Overview

3.1 Platform Vision

Many of today's solutions for managing and controlling the electric power system are designed and packaged to perform a single function. They struggle to meet near-real-time speed requirements, necessitate extensive back-end integration effort, and often lack scalability. The electric power system of the future must employ multi-functional, standards-based, and modular systems to promote and allow interoperability, lower costs, and improved reliability by integrating and analysing multiple information sources based on their timeliness, location, and availability.

These new requirements demand an electric grid with “distributed intelligence” that has the potential to significantly increase the operational efficiencies of the electric power system resulting in benefits realization through additional cost savings by:

- Deferring capital infrastructure expansion
- Achieving improved operational performance
- Improving system response times
- More effectively managing the scalability associated with field devices
- Driving greater insight for more optimal decision making
- Streamlining the status monitoring and security of all communicating field assets
- Enabling workforce management to efficiently prioritize resources

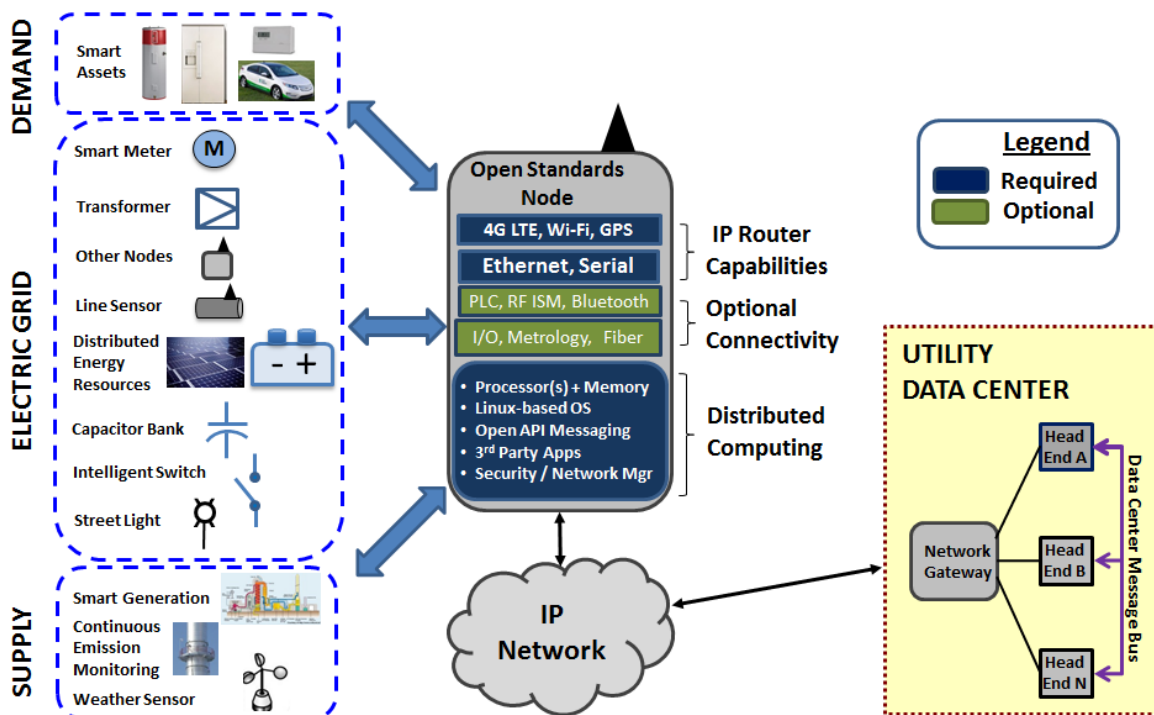


Figure 3-1: Duke Energy Distributed Intelligence Platform Node Architecture

The key enabler and chief catalyst to this Distributed Intelligence Platform (DIP) vision is a standards-based, modular communications system that can enable interoperability, scalability, enhanced security, and near-real-time resiliency at a lower cost and deliver better performance system-wide. Duke Energy currently hosts this DIP platform in the form of a physical and/or virtual component, known as a node ("*Node*"), that enables the "internet of things" for the utility, as depicted in Figure 3-1, to provide two complimentary functions: connectivity and computing.

The minimum base functional requirements of the DIP necessitate that every Node must:

- Utilize the IP network protocol
- Provide data aggregation, filtering, and prioritization of end points from multiple devices
- Support short-term storage of end-point data, audit information, and device diagnostics
- Provide routing, bridging and gateway capabilities to the IP-based networks
- Provide serial to IP conversion
- Support remote configuration and device provisioning
- Support required application level protocol translation between connected devices and back-office OT and IT systems
- Support open standards-based publish-subscribe messaging
- Enable third-party applications via standard APIs
- Allow integration of data from legacy assets
- Support distributed security functions
- Provide event reporting, health monitoring, and fail-safe mechanisms

3.1.1 Hardware Considerations

The node's hardware requirements are to be covered in great detail in Volume 2, but a fundamental understanding some of its key attributes are considered here. Table 3-1 represents the three types of packaging scenarios (i.e., internal, external, integrated) that Duke Energy envisions these packages will deliver the base functions of the reference architecture that meet past, present, and future grid configurations. As the grid evolves from the current to future state, one or more of these packaging scenarios may be required to satisfy each tier of the reference architecture in order to align with existing legacy apparatus, address present gaps in the infrastructure, and support future embedded components of new integrated hardware solutions.

	Past	Present	Future
Scenario	Internally mounted	Externally mounted	Integrated
Apparatus	Legacy Hardware	Stop-Gap Hardware	Future Hardware
Deployment Type	Brownfield (retrofit)	Greenfield (new product)	Software Upgradable (virtual)
Package Type	Hardened	Environmentally ruggedized	N/A

Table 3-1: Summary packaging scenarios

Since it could be decades before the existing legacy power systems infrastructure is replaced or upgraded with new hardware apparatus, there is a need to deploy hardened DIP Nodes as brownfield retrofit products inside existing cabinets of legacy capacitor-bank controllers, protective relays, or other intelligent electronic devices (IEDs) in order to deliver the functional requirements of the DIP without impacting or compromising the existing centralized SCADA or AML information systems. In addition, in areas on the electric power system where gaps exist with connectivity, monitoring, and/or control functionality, there is a need for environmentally ruggedized DIP Nodes, as a stop-gap greenfield product, to be externally mounted outside on poles or padmount transformers. Likewise, for the same gaps within the confines of an indoor substation control house or datacenter, there is a need to retrofit server racks with rack-mounted hardened DIP Nodes. Lastly, the main intent of this reference architecture is to ensure that manufacturers of power systems hardware devices and apparatus can incorporate and integrate the base computing and connectivity requirements of the DIP into their future product roadmaps and thus only requiring virtual software to interoperate and share data with other DIP Nodes on the distributed information system. It is important to note here that while the virtual node of the future may be implemented as a software or firmware module imbedded within the vendors apparatus, the physical networking interconnection interfaces of a Node may still require the use of an external communication module or fixture.

Duke Energy has identified the following package types:

- **Hardened:** Suitable for mounting inside an existing outdoor enclosure (i.e. IEEE 1613 compliant package)
 - Din-rail mounted or wall-mounted configurations
- **Ruggedized:** Suitable for mounting in outdoor enclosure for overhead and underground (i.e. NEMA 4+ compliant package)
 - Padmount configuration for underground
 - Polemount configuration for overhead
- **Rack-mounted:** Suitable for inside a substation control house or data center (i.e. IEC 61850-3 and IEEE 1613 compliant package)
- **Integrated:** New endpoint grid device that meets DIP requirements (e.g., sensor, meter, IED, Low Voltage power electronics, etc.)
 - Integrated as virtual software inside new apparatus products

Figure 3-2 depicts some of the various package types that are driven by the functional requirements to support the reference design architecture, which enables the platform flexibility for deployment in diverse operating environments and various installation locations.

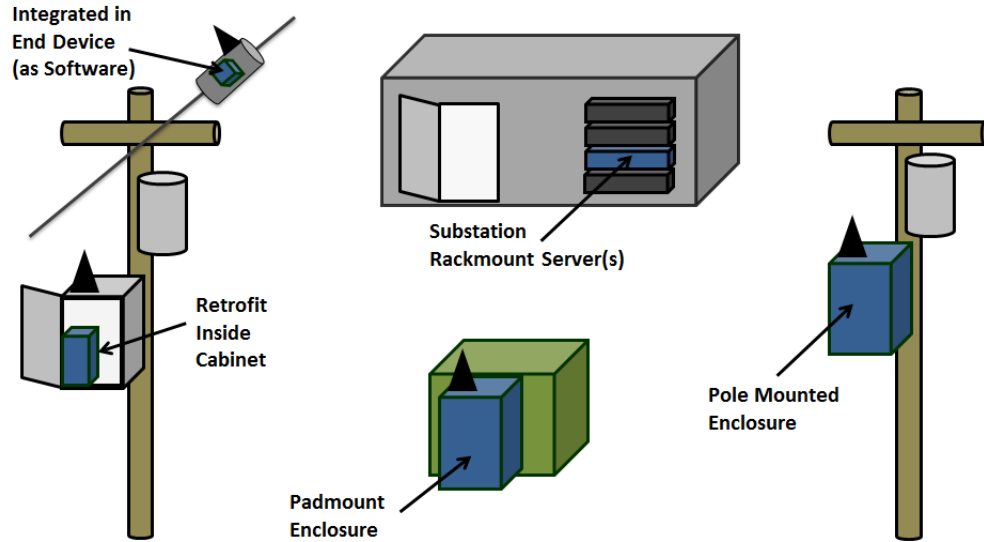


Figure 3-2: Several examples of packaging scenarios identified for reference architecture

A subset of packaging will also include options for chassis design to enable plug-and-play modular functionality for the middle to upper-tier family of nodes. A full description of the concept of tiers and their definition is included in Section 3.2.2. It is envisioned that examples of plug-and-play modules may include: modems, I/O cards, programmable logic controllers, power supplies, and expandable computing hardware. Figure 3-3 is a representation of the hardware described in proceeding sections.

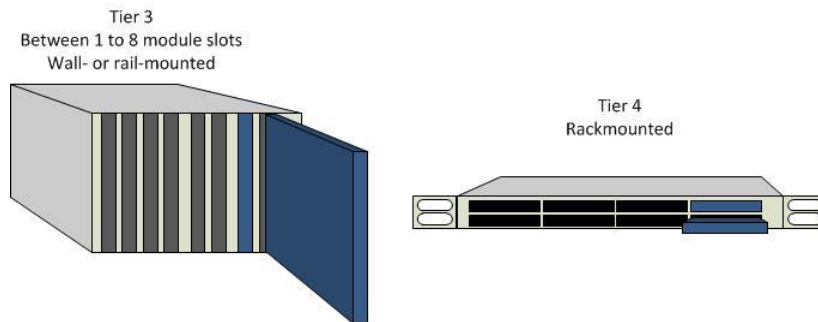


Figure 3-3: Modular Chassis Design

The package requirements for this reference architecture are defined to meet industry standards and Duke Energy's environmental, electrical, safety, and security requirements and support the best practices for hardware installations including the aesthetics, indicators (visual and audio), dimensions (size and weight), and color.

3.1.2 Deployment Considerations

The deployment considerations of the node is influenced by the packaging type and operational environment that it is to be installed in, ranging from an environmentally controlled data center to outdoor distribution pole-tops.

In a retrofit design that employs an internally mounted node, the periphery components (e.g., enclosures, mounting brackets, connectors, antennas) will need to be incorporated and tailored for the specific distribution grid asset. In an outdoor green-field design that employs an environmentally ruggedized NEMA 4+ enclosure, the main deployment considerations include the mounting bracket, the source of secondary power, and physical security.

For commercial applications, there is a wide array of deployment considerations (e.g., voltage at 480VAC) that the node manufacturer will need to consider. The antenna design is a key consideration to ensure the chosen wireless technology devices in the node can reliably transmit and receive in the targeted operating environment.

3.1.3 OSI Model

In Table 3-2, Duke Energy is using the OSI Model and Internet Protocol Suite (also known as the TCP/IP suite) as a reference to abstract and differentiate the connectivity and computing requirements.

Layer	OSI Model	Internet Protocol Suite	Protocols
7	Application	Application	HTTP, SMTP, DHCP, DNS, SSH, SNMP, TLS/SSL, XML, DNP, C12, REST, MQTT, DDS, AMQP, CoAP, Modbus, OCP
6	Presentation		
5	Session		
4	Transport	Transport	TCP, UDP, DCCP
3	Network	Internet	IPsec, IPv4, IPv6
2	Data Link	Network Interface	IEEE 802.3, 802.11, 802.15.4, 802.16, Bluetooth, MAC, PDCP, RLC
1	Physical		

Table 3-2: OSI Model and Internet Protocol (TCP/IP) suite with Associated Relevant Protocols

3.1.4 Connectivity

The Node serves as the router or gateway that can support directly connecting and interacting with various grid assets, process data, and share information with other nodes and assets through standards-based communications mediums utilizing the Internet Protocol (IP). The Node will contain the appropriate communications technologies to decouple the network interface (OSI Model Layers 1 & 2) from the higher layers (3-7), eliminating the need to accommodate unique device-specific connections.

3.1.5 Computing

The Node will collect, process, store, and distribute data from new and legacy grid assets or end points to support energy systems and applications, which enable distributed, tactical functions that are not currently achievable. The Node will contain the storage, processing, and an embedded Linux environment sufficient to seamlessly enable the fast data processing and secure exchange of information between disparate assets and systems on the network, effectively decoupling the application Layers 5-7 from networking Layers 3-4. It is also envisioned that a

Node will support the ability to directly interface and integrate with other nodes, independent of its tier. A full description of the concept of tiers and their definition is included in Section 3.2.2.

Figure 3-4 illustrates the various base and optional components required to support the multi-tiered node platform. The base hardware components define the minimum mandatory requirements for each tier. Depending on the manufacturer's preference or specific use-case for each tier, optional components can be incorporated into the node. The partitioned OS in the core processor and memory or separate apps processor and memory are required for decoupling the application Layers 5-7 from networking Layers 3-4.

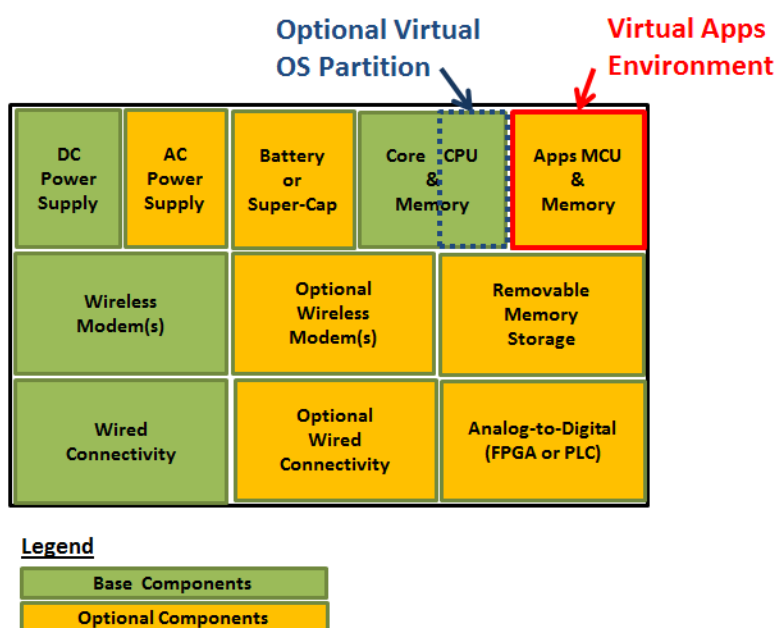


Figure 3-4: Configuration Hardware Components

3.1.6 Field Message Bus Architecture

The Distributed Intelligence Platform (DIP) is designed to extend the Enterprise Service Bus (ESB) concept to the edge (“last mile”) of the grid infrastructure and is designated as the Field Message Bus (FMB). The FMB, as depicted in Figure 3-5, is an open, standards-based, pub-sub interface that connects multiple disparate grid devices, telecom networks, and information systems. It is key to realizing the benefits of the distributed architecture by facilitating interoperability between heterogeneous OT, IT, and telecom systems. Unlike the ESB that resides in the datacenter behind head-end systems, the FMB enables distributed control and processing across various systems in a multi-tiered hierarchy, allowing for a cost-effective means of managing operational data. The FMB enables the integration of centralized control and distributed control systems. Since the value of operational data is determined primarily by its timeliness, location, and availability, the ability to analyze and process local data and to share other relevant information locally between disparate devices nodes and devices in the field is critical to effective decision making.

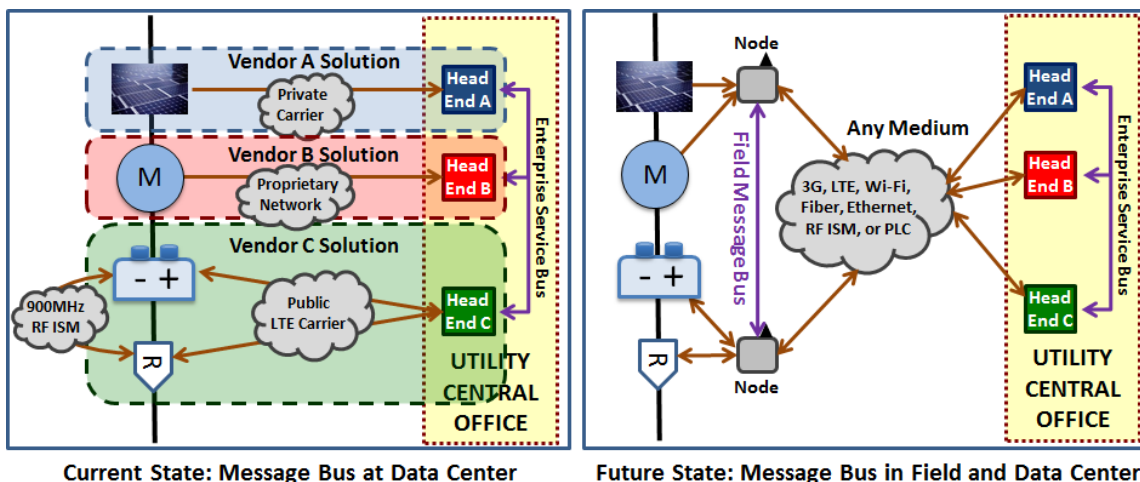


Figure 3-5: Duke Energy Distributed Intelligence Platform: Field Message Bus

Figure 3-6 illustrates the logical elements of the FMB's virtual environment that manages the flow of application layer data responsible for IT/OT convergence. This provides the interaction between application layer building blocks in the FMB stack. The translation component is a software adapter that filters data, converts the syntax of a protocol residing in a device endpoint to the message bus protocol, and conforms to a common semantic model (i.e., CIM). The value of the adapter is that it is constantly interrogating and discovering the connected OT systems or devices. The adapters and third-party use-case applications also comply with an open API ecosystem. Security at this level both provides additional encryption and controls the flow of operational data traffic.

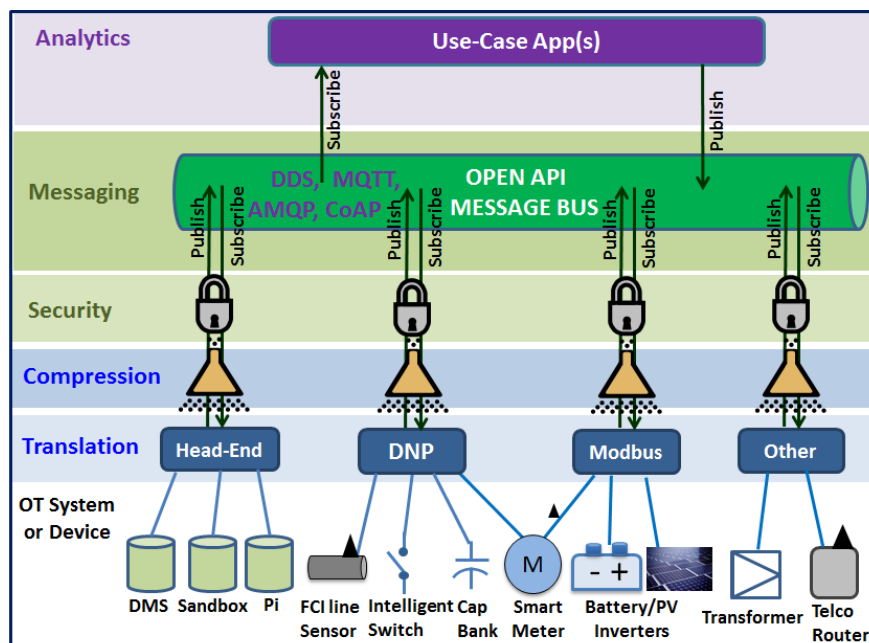


Figure 3-6: Duke Energy Field Message Bus Data Flow

Figure 3-7 illustrates the conceptual data and analytics model for the DIP reference architecture. The FMB allows contextualization and analytics to occur at the edge of the network. It handles the protocol translation at the device level, prior to contextualization, storage, and visualization, and allows for integration of data and analytics across devices. Finally, this allows for a unified, ubiquitous application of security across all enterprise verticals.

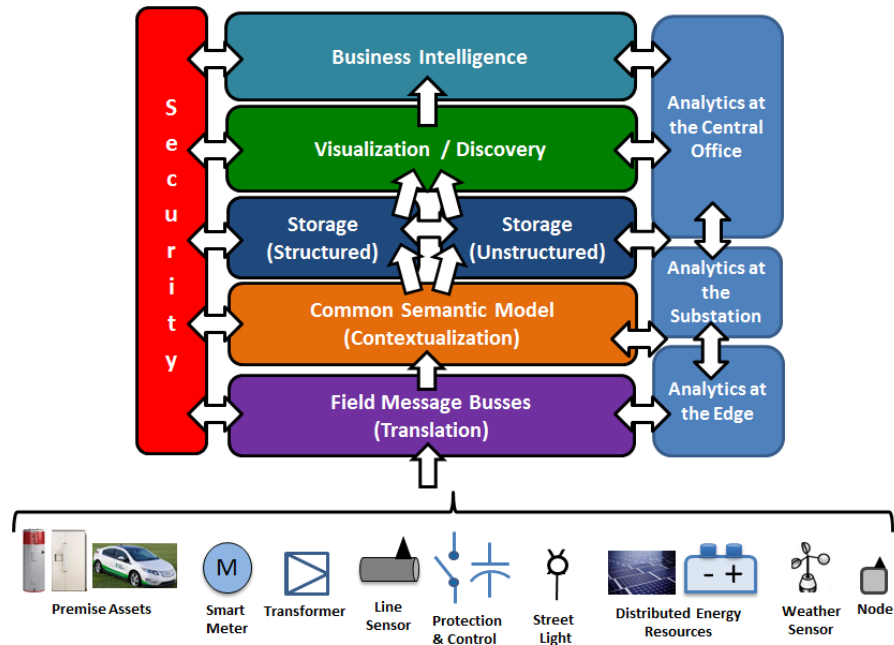


Figure 3-7: Conceptual Data and Analytics Model

Figure 3-8 illustrates the different building blocks of the architecture. This shows that the DIP reference architecture is protocol agnostic and modular with an open API.

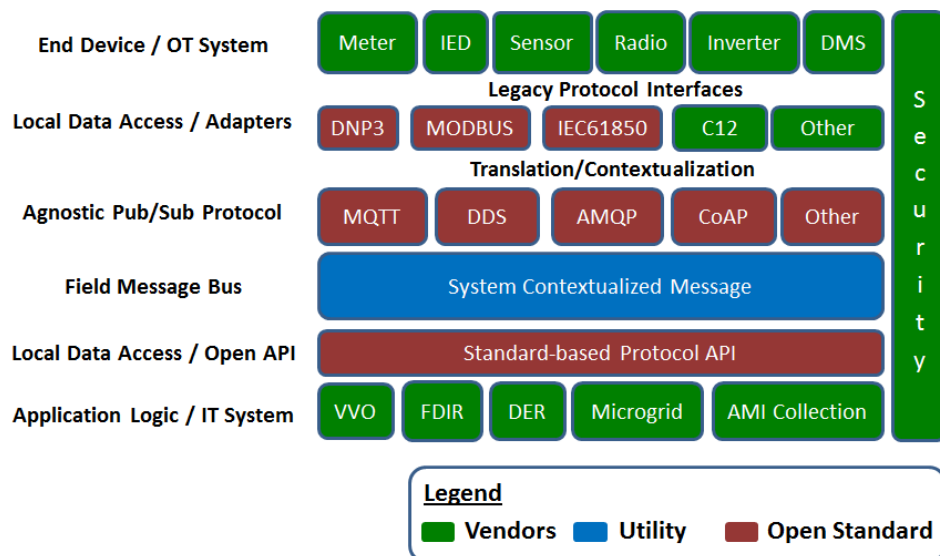


Figure 3-8: Duke Energy Field Message Bus Conceptual Building Blocks

Some of the key benefits and features of the Field Message Bus include:

- Secure end-to-end encryption
- Filtering, prioritization, compression, and translation of local real-time data
- Seamless peer-to-peer and broadcast information exchange of application layer data
- Separation of the physical, logical, and network layers of the OSI data stack
- Agnostic to programming language, OS, and message bus protocol
- Virtual field area network (FAN) cloud that handles and routes the message transactions
- Interoperability between different protocols, legacy systems, and IT enterprise systems
- Easy portability, reusability, and modularity of adapters, protocols, and analytics reduce the system development cycle time and validation efforts
- Simple, lightweight, and easy to implement open-source message bus protocol
- Better accommodation of lower latency requirements of critical operations (e.g., DERs)
- Migration path from centralized to distributed infrastructure
- Avoid “rip-and-replace” by translating legacy protocols to open standard API
- Support for communication protocol integrity (quality of service, persistence, and failover)

3.2 Hierarchical Application of Distributed Intelligence Platform Nodes

Node hierarchy is important for the DIP because it allows control functions to be initiated at the local level. It also offloads certain responsibilities from the centralized Distribution Management System or other centralized control systems and delegates these to lower level nodes. In essence, it gives lower level nodes their “marching orders,” and establishes their span of control and authority. This results in lower latency for certain delegated control functions because they do not always require individual instructions to be initiated from the centralized back office services.

From a logical, hierarchical point-of-view as illustrated in Figure 3-9, the distributed nodal architecture supports multiple tiers of Nodes that span across all network area domains, such as the Local Area Network (LAN), Field Area Network (FAN), and Wide Area Network (WAN). Even though from a transport perspective the data traffic is physically routed through the IP-based WAN via wired or wireless links, the application and logical information can be functionally shared peer-to-peer in horizontal and vertical ranking orders.

It is important to note that while it is envisioned there will be five tiers of nodes (Tiers 1 through 5), this hierarchy does not mean to impose a limit on inter-tier communications. Any tier level node can communicate directly with any other tier level node. The different tier levels relate to the capabilities and function of the nodes. This is described in much further detail in section 3.2.2.

As the power grid evolves and becomes populated with more intelligent devices and apps, the provisioning, monitoring, and diagnostics of these can be configured at higher tier node as opposed to the back office.

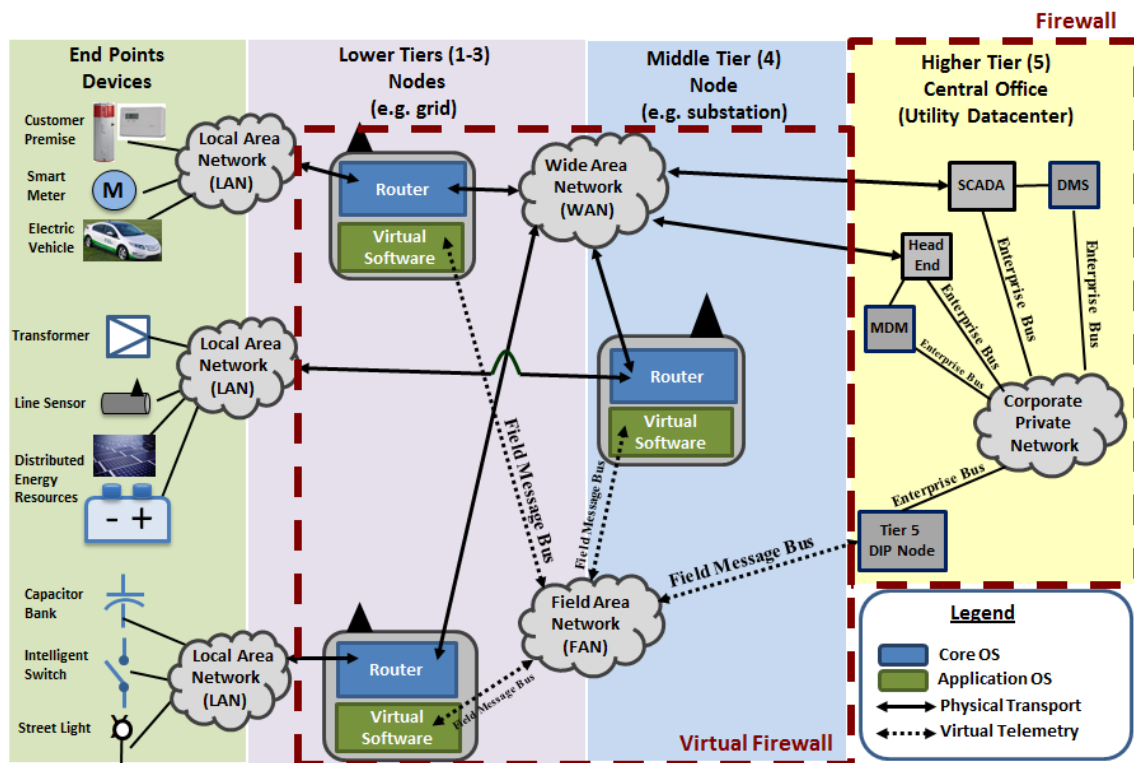


Figure 3-9: Duke Energy Distributed Intelligence Platform Vision: Node Hierarchy

3.2.1 Network Definitions and Diagram

Figure 3-10 below is an example of a hierarchy and structure of the various networks that is useful to illustrate the make up the DIP reference architecture. This figure does not intend to show all network systems or interconnections that may be employed by Duke to manage and control its electric power delivery system. However, it shows the major networks that will be used to interconnect the field devices, the DIP nodes, and the back office services.

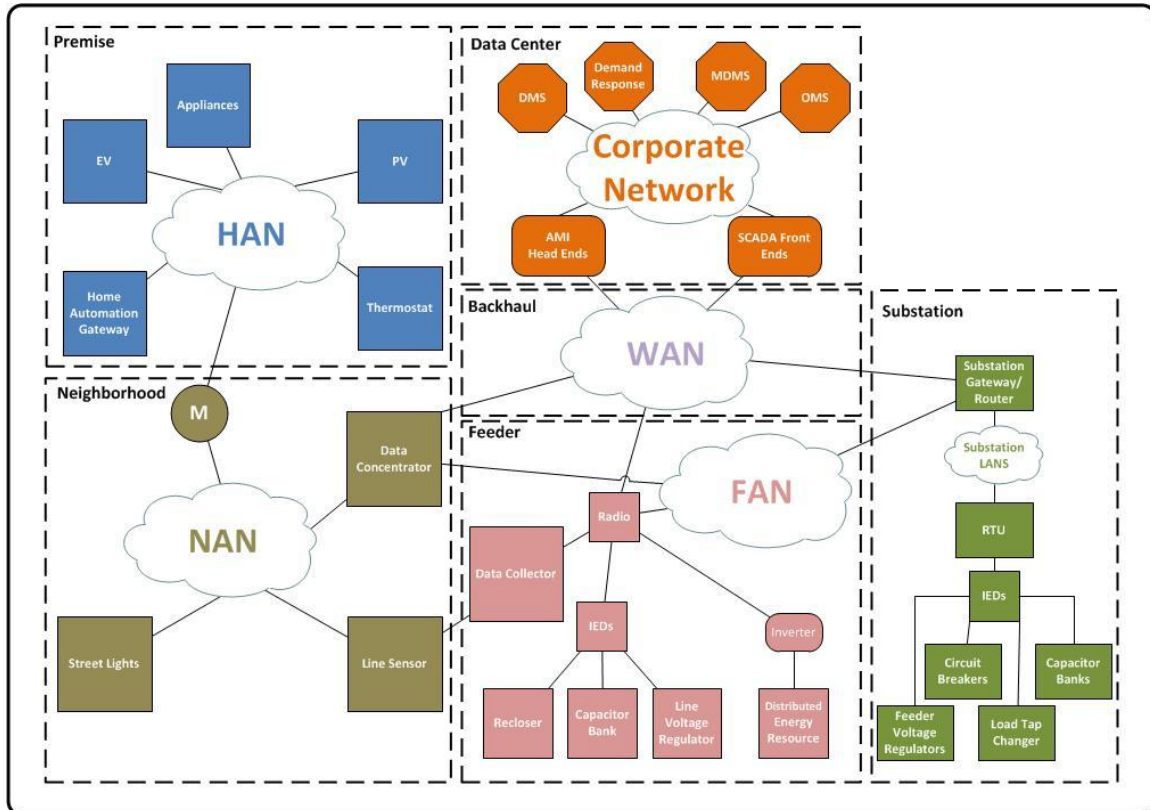


Figure 3-10: Connectivity of the Various Networks

Premise Network (HAN): This is the network that typically exist within a premise and serves to connect the devices and applications in and around the premise, such as smart appliances, PEVs, thermostats, home automation gateways, rooftop solar panels, inverters, energy storage, and load control switches.

Neighborhood Area Network (NAN): The NAN typically refers to a collection of individual and independent neighborhood area networks used to link together devices in small geographic areas or neighborhoods. Each of these individual NANs is then linked through a common Data Aggregation Point sometimes known as an Access Point or Cell Relay. The NAN may be used to connect with utility assets such as meters, streetlights, sensors, and grid monitoring devices. This network usually supports lower-bandwidth, higher-latency tolerant applications. It has the capability to connect upstream with the Field Area Network (FAN) or Wide Area Network (WAN) based on the application needs.

Field Area Network (FAN): This network is typically used to connect assets requiring lower-latency and higher-bandwidth applications, such as capacitors, reclosers, voltage regulators, distributed energy resources (DER), and distribution automation (DA) devices. It has the capability to connect to the NAN, Substation Network, or WAN based on the application needs.

Substation Network: This network exist in a substation and is used to connect devices in the substation, including voltage regulators, circuit breakers, transformers, energy storage, solar, weather stations, load tap changers, IEDs, programmable logic controllers (PLC), PMUs, and RTUs. This network may be composed of multiple logical networks to provide security partitioning from business applications and would connect with the WAN and FAN.

Wide Area Network (WAN): This network includes both wireless and wired technologies, and serves as the backhaul for all other networks. It is also the backbone that connects to the data center and other centralized services and the control centers.

Data Center Network: This is the back office network that serves to connect the WAN and centralized hosts and the enterprise service bus (ESB).

3.2.2 Node Tier Hierarchy Definitions

The primary driver for a multiple-tier hierarchy is the ability to manage a dynamic electric and communications infrastructure with constantly changing situational and operating requirements. Cost is also an important consideration for having a multi-tiered, hierarchical design. However, having the DIP reference architecture and node functionality also gives Duke Energy the flexibility to switch out nodes and other elements of the infrastructure as new devices and applications provide new economically beneficial value propositions to Duke Energy. A secondary driver is the ability to gradually augment and retrofit the existing legacy infrastructure without disrupting daily electric power system operations.

It is recognized that there is no “one-size-fits-all” Node that will accommodate all the existing and future cost, connectivity, hardware, and computing requirements of the DIP reference architecture. Therefore, Duke Energy has identified 5 levels of Nodes defined as tiers.

The Node tier classifications will adapt as digital technologies and network capabilities evolve. Every Node will contain the same minimum base functional requirements for all tiers as listed explicitly in Section 3.1. Based on today’s DIP reference architecture, the following tiers make up the Node hierarchy.

Their respective packaging types of the 5 tiers is summarized in Table 3-3.

Packaging type	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
Integrated	Yes	Yes	No	No	No
DIN-rail/Wall mount	Yes	Yes	Yes	No	No
Polemount	No	Yes	Yes	No	No
Padmount	No	Yes	Yes	No	No
Rackmount	No	No	No	Yes	Yes
Modular Chassis	Optional	Optional	Yes	Yes	Yes

Table 3-3: Summary of packaging requirements for multi-tier reference architecture

3.2.2.1 Tier 1

Basic Description: Tier 1 Nodes are targeted the lowest cost, support the least functional applications, while still meeting the minimum computing and connectivity requirements of the DIP reference architecture. This could eventually be used as an embedded feature inside new grid assets. Tier 1 Nodes requirements identified here also serve to establish the baseline requirements that the rest of the Tier Nodes will be built on.

The primary functions of the Tier 1 Node include local data access, direct interaction with the last mile endpoints, remote monitoring, protocol translation, IP conversion, and a common virtual environment for distributed security and third-party applications.

It is envisioned that the Tier 1 Node will primarily serve as the gateway between the HAN and NAN. However, for some last-mile or embedded applications, it can also serve as a NAN gateway to the FAN, or a FAN gateway to the WAN.

Figure 3-11 provides illustrations of example applications for the tier 1 node in a retrofit application and also embedded into new devices as a virtual piece of software. It should be noted in Figure 3-11 and Figure 3-12 that while the virtual node of the future may be implemented as a software or firmware module imbedded within the vendors apparatus, the physical networking interconnection interfaces of a Node may still require the use of an external communication module or fixture.

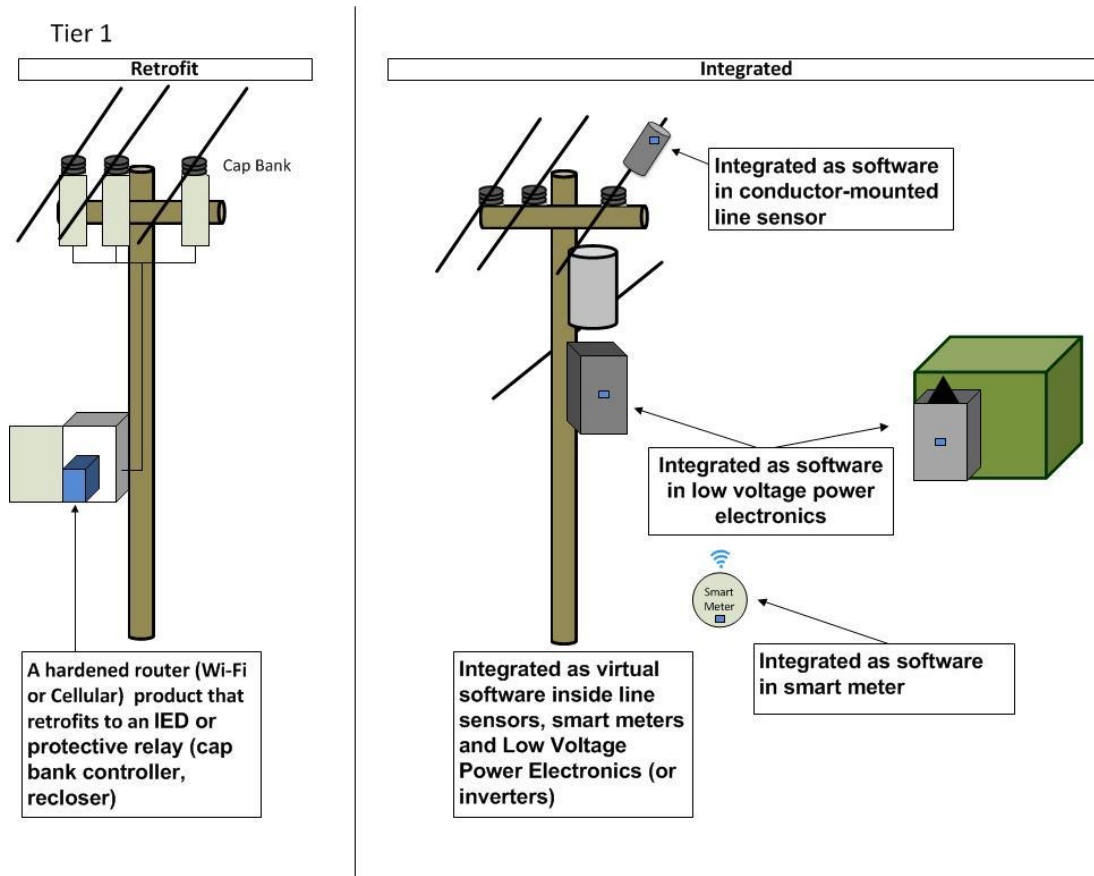


Figure 3-11: Examples of Tier 1 node applications for retrofit hardware or imbedded software

Below are the required feature sets for the Tier 1 Node:

- Required Communications
 - One of the following wireless mediums: Wi-Fi or Cellular
 - The following wired medium: Ethernet
- Optional Additional Communications:
 - Wireless: Bluetooth, Z-Wave, RF ISM, GPS, Wi-Fi
 - Wired: PLC, BPL, Serial, USB, Fiber
- Other optional capabilities:
 - Analog I/O, Digital I/O, Metrology, temperature

3.2.2.2 Tier 2

Basic Description: This Node will act as a data collector and cellular bridge targeting multiple devices, systems, and applications most widely deployed on the grid (i.e., meters, streetlights distribution sensors, etc.). This is a retrofit tool that can be used to bring IP communications to the legacy infrastructure, thereby providing access to the data previously locked or siloed within the devices.

Since the Tier 2 Node will initially be the most widely deployed, the volumes will drive the economies of scale for the platform. This builds the distributed computing foundation for the other Tier Nodes to leverage. The Tier 2 Node is the tactical workhorse of the platform, bearing the majority of the activities associated with data collection and management in the field.

The primary functions of the Tier 2 Node include an IP access point, broadband connectivity to the WAN, remote monitoring, protocol translation, IP conversion, locational coordinates, and local data access enabling a common virtual environment for distributed security and third-party applications.

The Tier 2 Node will primarily serve as the gateway between the NAN and FAN. This also unlocks peer-to-peer information exchange between all Tiers of Nodes. Furthermore, the Tier 2 Node will have the ability to manage the end points within its local area networks, which includes provisioning and configuration. It can also provide electrical measurement and sensing capabilities (PQ, PDM). Figure 3-12 provides illustrations of example applications for the tier 2 node in a retrofit, green field, and integrated embedded packaging types.

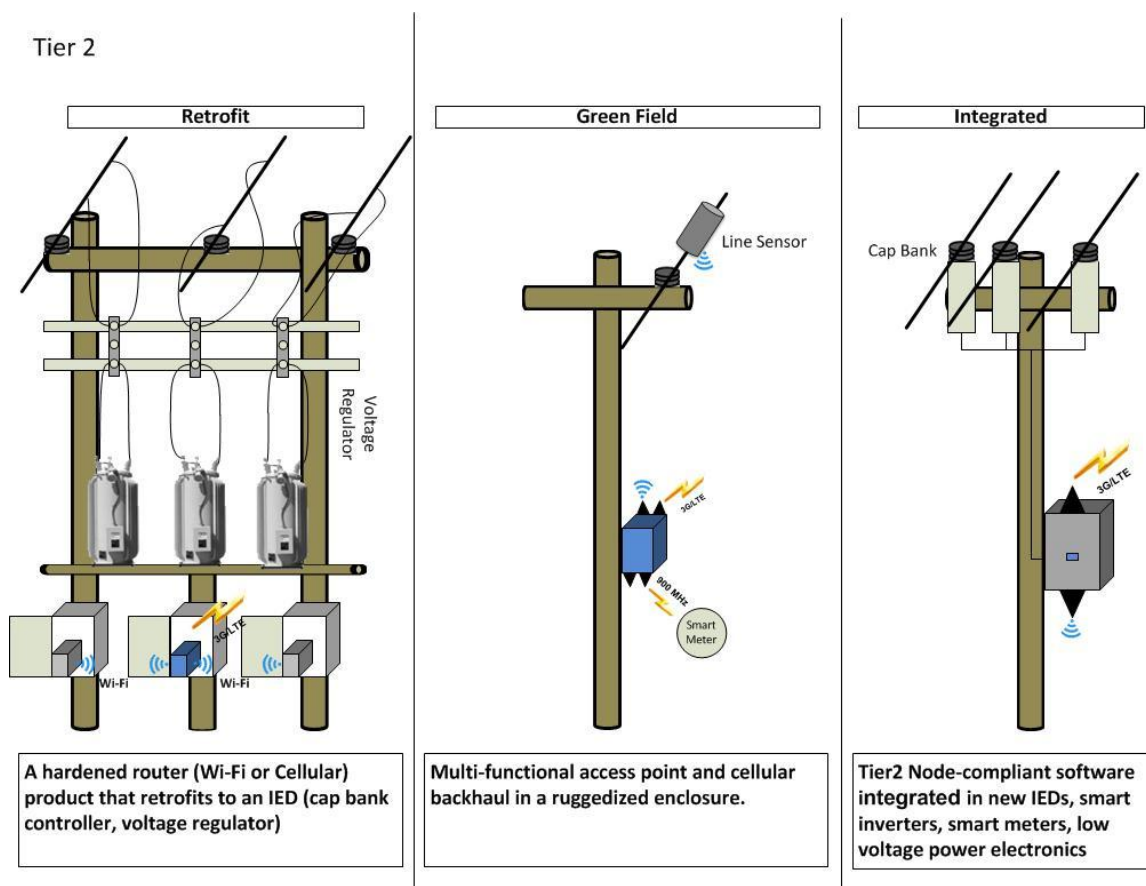


Figure 3-12: Examples of Tier 2 node applications for retrofit, green field, or embedded options.

Below are the required feature sets for the Tier 2 Node:

- Required Communications:
 - The following wireless mediums: Cellular w/ Assisted-GPS, Wi-Fi
 - Both of the following wired mediums: Ethernet, Serial
- Optional Additional Communications:
 - Wireless: Bluetooth, RF ISM
 - Wired: USB, Fiber, PLC, BPL,
- Other Optional capabilities: Analog I/O, Digital I/O, Metrology, Temperature

3.2.2.3 Tier 3

Basic Description: The Tier 3 Node is a field deployable, multi-purpose node with at least two of the following discrete features: upgradable computing hardware, communications, monitoring and control. It will inherit all the features of the Tier 1 and Tier 2 Nodes. It will be the data collector and may serve as the controller for critical FAN devices (i.e., DER, PMU, Grid Protection). It will also be a low-latency cellular router and host of third-party distributed applications for the FAN, WAN, and/or Substation Network. The Tier 3 Node has the option for IED operational capabilities. In order to support the multi-function capabilities, it will have a chassis that contains multiple modular card slots for plug-and-play optionality for radios, application server(s), I/O, PMU, and other peripheral device options. Figure 3-13 provides illustrations of example applications for the tier 3 node in a retrofit and green field solutions that require multi-function use-cases and plug-n-play modularity.

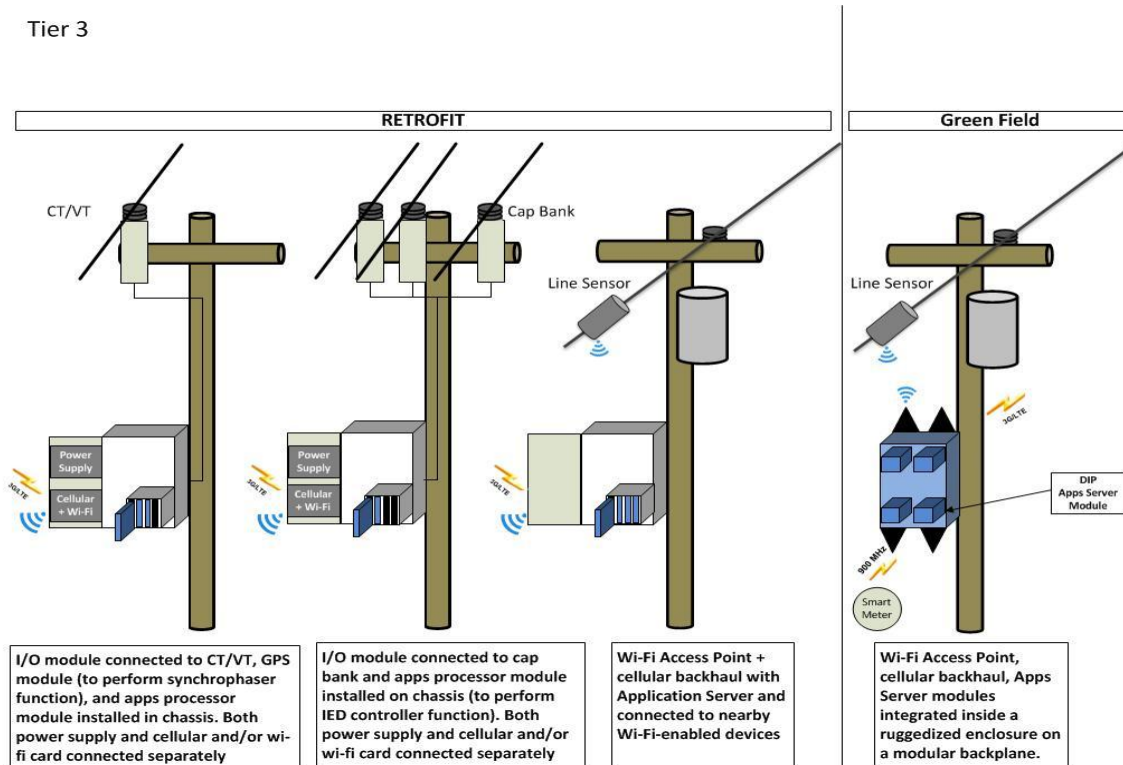


Figure 3-13: Examples of Tier 3 node applications for retrofit or green field options.

Below are the required feature sets for the Tier 3 Node:

- Required Communications
 - The following wireless mediums: Cellular w/ Assisted-GPS, Wi-Fi
 - If not embedded in the Node, a separate, external radio(s) is acceptable
 - Both of the following wired mediums: Ethernet, Serial
- Optional Additional Communications:
 - Wireless: Bluetooth, RF ISM, GPS
 - Wired: USB, Fiber, PLC, BPL
- Required Capability:
 - Modular chassis with multiple plug 'n play slots
 - Removable slot card with a third-party application processor and memory
 - One of the following slots cards: Analog I/O, Digital I/O, Metrology
- Other Optional Capabilities:
 - Analog I/O, Digital I/O, Metrology, temperature, sensors, PMU
 - Backbone routing (e.g. MPLS)

3.2.2.4 Tier 4

The Tier 4 Node will reside in the substation and inherit all the capabilities of a Tier 3 Node in a rack-mountable configuration. The primary function of the Tier 4 Node is substation automation and hosting the field message bus and security platforms that reside in the FAN. Its primary backbone backhaul is a broadband-wired router to the FAN, WAN, and/or Substation Network. It has cellular broadband, embedded or bolt-on, for secondary failover backhaul. The Tier 4 Node is the bridge to the data center and provides RTU and IED aggregation capability. Figure 3-14 provides illustrations of example applications for the tier 4 node in a retrofit rackmounted configuration at the substation control house.

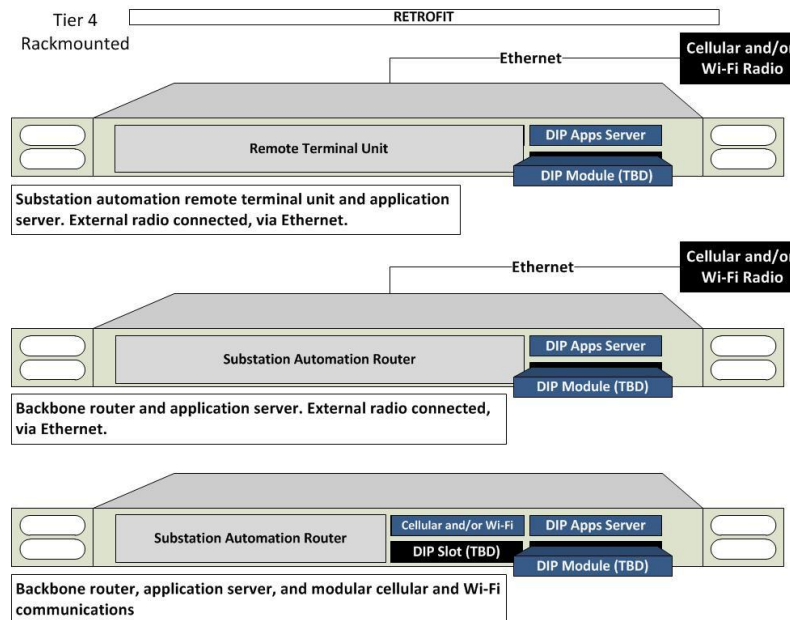


Figure 3-14: Examples of Tier 4 node applications for retrofit options at the substation.

Below are the required feature sets for the Tier 4 Node:

- Required Communications
 - Both of the following wireless mediums: Cellular w/ Assisted-GPS, Wi-Fi
 - If not embedded, a separate, external radio(s) is acceptable
 - All of the following wired mediums: Ethernet, Serial
- Optional Additional Communications:
 - Wireless: Bluetooth, RF ISM, GPS
 - Wired: USB, Fiber, PLC, BPL
- Required Capability:
 - Modular chassis with multiple plug 'n play slots
 - Removable slot card with a third-party application processor and memory
 - Backbone routing (e.g. Layer 2/3, MPLS)
 - If not embedded, a separate, external router is acceptable
- Optional Capabilities:
 - Both of the slots cards: Analog I/O, Digital I/O
 - Metrology, temperature, sensors, PMU
 - Programmable Logic Controller

3.2.2.5 Tier 5

It is envisioned the Tier 5 Node will reside in the centralized data center. The Tier 5 Node will be fully interconnected with the Tier 4 and other lower tier nodes in the field via the WAN, FAN, or other appropriate network services. The primary function of the Tier 5 Node is to function as a gateway between the centralized control systems and services and the lower level tier nodes along with their interconnected end devices. This can be accomplished by interconnecting the Tier 5 Node directly with the Data Center Enterprise Service Bus or directly interconnecting with any other centralized standalone security and control systems and services. The Tier 5 Node is not intended to replace any existing OT management or control system but is intended to functions as a gateway between these centralized services and the end devices in the field.

Below are the required feature sets for the Tier 5 Node:

- Network topology:
 - Primary functions:
 - Data center gateway to Enterprise Service Bus (ESB)
 - Broadband wired router to FAN, WAN, and/or Substation Network
 - Host of third-party centralized apps - TBD
 - Host of enterprise security application - TBD
 - Secondary function:
 - TBD
- Required Comms
 - Ethernet

Tier 5

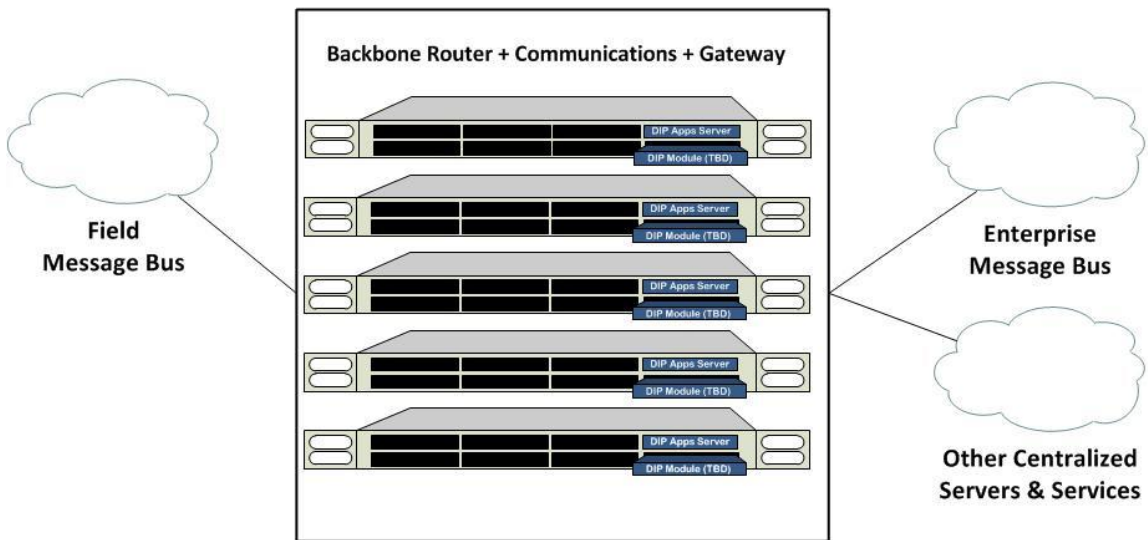


Figure 3-15: Examples of Tier 5 node applications for retrofit options at the substation.

4. Software Considerations

While the focus of this particular specification is on a DIP reference architecture vision, the symbiotic relationship between the software and the enabling hardware is such that software considerations have been included to ensure that the functions of the integrated nodes and tiers are understood. The intended focus in this section is on the software characteristics of the nodes themselves and not the applications intended to reside on the node. In addition, processes for managing, configuring, and upgrading the software elements and networking interfaces can be uniformly applied across the node platform. These major software considerations include the operating system (OS), element management system (EMS), device security, IP routing, and protocol support. Additional information concerning the software reference components can be found in a companion specifications labeled Volumes 3 and 4.

4.1 Operating System

In effort to cater toward a secure, open-source, economic, user-friendly, and flexible M2M application development environment, a Linux-based OS is mandatory for the distributed architecture to manage the core networking services and drivers as well as the virtual telemetry applications. It is also intended that the Node device's core OS will supervise the local databases and internal processing, filtering, and aggregation of raw data from many devices into "metadata" as well as executing local analytics to perform decisions and prioritize outbound traffic in the asynchronous message queue.

As displayed in Figure 4-4, the reference architecture is designed to separate the core applications in the core OS of the node from the virtual OS application environment(s) responsible for hosting the third-party software apps that include the open API field message bus, protocol adapters, enterprise security, and use-case specific analytics.

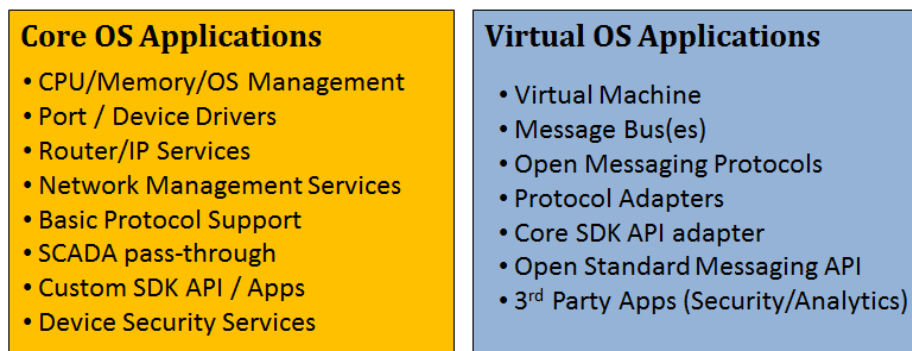


Figure 4-4: Example of separate Operation System (OS) environments

For cost and security reasons, Linux OS will be mandatory for the central OS requirements in the embedded node architectures in Tiers 1 and 2, while the upper-tiered devices, which contain a server-like processing capability, are flexible to accommodate alternative core OS environments. However, for the virtual OS environment, Linux is required for all tiers to ensure consistency in

the third-party application ecosystem and enterprise security that are developed to a common API. Table 4-6 exhibits these OS requirements for each tier of nodes.

Operating Systems	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
Linux core OS	Yes	Yes	Optional	Optional	Optional
Linux Apps OS	Yes	Yes	Yes	Yes	Yes

Table 4-6: OS requirements for the multi-tiered node reference architecture

4.2 Node Element Management System

In order to facilitate the safe and scalable deployment, firmware upgrading, and visibility of the internal data traffic within the DIP Node central OS environment, an Node Element Management System (NEMS) is required to perform the following functions and features:

- Verification of secure mutual authentication to all connected devices
- Remote administration for configuration and firmware upgrades to multiple devices
- Near-real-time data access, event-logging, and alert reporting
- Graphical user interface for geographic information and maps
- HMI interface to connected LAN devices and SCADA operational systems
- WAN/LAN telecom diagnostic information
- Publish data via standard protocols (i.e. MQTT, DDS, SNMP, etc.) to field message bus

The NEMS should be based on the ITIL and eTOM industry frameworks for systems management and operations. The NEMS is split up into three functions: firmware management, configuration management, and network diagnostics.

4.2.1 Firmware Management

The NEMS should provide authenticated remote firmware management capabilities that allow for revision control of device firmware (i.e., upgrades and downgrades) and image management for core processing, routing interfaces, and virtual applications. To efficiently download the contents of the firmware package, firmware upgrades should have the ability be split into partial package or component images.

4.2.2 Configuration Management

Configuration management is an important function of the NEMS. It must support configuration identification, change control mechanisms, reporting status, and auditing. Other crucial support functions include the configuration of network interfaces and the node internal database (e.g, management information base). With respect to the interfaces, the NEMS should support provisioning of network devices and authentication of LAN endpoints in the subnet. In regard to configuration of the internal database, the NEMS should provide visibility and accessibility to the local data residing on node with capabilities to publish and share data to the virtual OS environment hosting the open API field message bus.

4.2.3 Network Management

In addition providing OT support for field devices, the tier nodes will provide the capabilities to support the IT management functions in the field as well utilizing the commonly supported IT management protocol like SNMP. It is envisioned the tier nodes will relay and communicate the SNMP data packets and information between the interconnected networking devices and their respective Element Management Systems. The preferred management protocol is SNMP, but the tier nodes must be able to transport other management protocols as may be required to support legacy networking devices. Examples of the network management functions and the information that must be supported include the following:

- Performance analysis
- Statistics collection
- Fault Analysis
- Reporting
- Alarming
- Status information provision
- Automatic element discovery
- Unrecognizable element reporting/alarming
- Auditing and Reporting

4.3 IP Networking

The IP networking capability is part of the core networking services provided for node applications. The flexibility of the IP network and its routing capability is intended to support emerging technologies (e.g., IP-addressable premise devices).

Nodes will be able to support multiple independent IP sessions and the associated network routing, such as meter-to-cash “pass-through” data and simultaneous publishing of operational data to a separate field message bus.

4.4 Security Considerations

Though comprehensive security requirements for the Distributed Intelligence Platform will be detailed in Volume 4, there are some basic considerations to introduce related to the node’s device-level security features. The emphasis on standards in this specification is aimed to achieve mature integration with enterprise monitoring and management capabilities. This mature integration is vital to achieving a safe, secure and resilient solution that can be sustained at an adequate security level. The minimum recommendations for cybersecurity from the Energy Sector Control Systems Working Group’s document on Cybersecurity Procurement Language for

Energy Delivery Systems¹, NISTIR 7628, NIST 800-53, and NIST 800-82 should be carefully considered when developing and validating products that comply to the reference architecture. The intent of reference architecture is to position the security design and building blocks of DIP nodes with the appropriate technical definition and controls that can encourage the future discussions for compliance with NERC-CIP implementations.

To ensure the reference architecture provides appropriate device-level, network, and system security, the following features are mandatory:

- Secure IP and MAC authentication
- VPN tunneling over IPsec
- Key encryption management
- Physical Locks and anti-tampering mechanisms
- Isolation of core OS from application OS (e.g., hypervisor)
- A root account (i.e., superuser) should only be accessible to node manufacturer

Depending on what the node is connected to will dictate the level of trust perceived on the WAN.

4.5 General Utility Protocol Support

While the overall desire is to have an IP-based telecom network infrastructure, it is recognized that many utility or customer assets will continue to utilize other non-IP based protocols. To accommodate the diversity of the operational equipment on the grid, support for the protocols in Table 4-8 should be considered.

Protocols	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
MODBUS TCP	Optional	Yes	Yes	Yes	Yes
MODBUS RTU	Optional	Optional	Optional	Yes	Yes
DNP3	Yes	Yes	Yes	Yes	Yes
IEC61850	Optional	Optional	Optional	Optional	Optional
C12	Optional	Optional	Optional	No	No
SNMP	Optional	Optional	Optional	Optional	Optional

Table 4-8: Protocol considerations for the multi-tiered node reference architecture

Because of its market penetration, support for DNP 3 should be present at all tiers. In order to support distributed energy resources and legacy distribution automation, MODBUS TCP and RTU protocols should exist at Tiers 4 and 5. For substation automation, MODBUS TCP/RTU, and IEC61850 protocols are required to support at Tier 4. The C12 protocol is desired in the lower

¹ http://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf

tiered nodes for AMI applications. SNMP is desired as a legacy standards-based protocol to manage the existing router infrastructure.

4.6 Message Bus Protocols

The message bus protocols in Table 4-9 are recommended for the family of node tiers. MQTT is recommended in the lower tier that contain an embedded virtual environment. DDS is required in Tiers 3 and 4 due to the performance and security needs of critical operational controls systems (e.g., microgrids and substation automation). AMQP is envisioned as an option for enterprise service bus (ESB) applications. CoAP is also considered as a lower-tiered node messaging option for bridging to low-bandwidth NAN devices (e.g., AMI mesh).

Protocols	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
MQTT	Recommended	Recommended	Optional	Optional	Optional
DDS	Optional	Optional	Yes	Yes	Optional
AMQP	Optional	Optional	Optional	Optional	Optional
CoAP	Optional	Optional	Optional	Optional	Optional

Table 4-9: Message Bus Protocol considerations for the multi-tiered node reference architecture