Chapter 11

Utilities

Mugoya Dihfahsih

Students No: 2100702353

Introduction

This chapter introduces the concept of the smart grid and explores some of the underlying IoT technologies that are transforming the way power is generated,

transmitted, and delivered. It includes the following sections:

Introduction to power utility industry

The GridBlock Reference Model

The Primary Substation GridBlock and Substation Automation:

System Control GridBlock:

The Field Area Network (FAN) GridBlock:

Securing the Smart Grid:

The Future of the Smart Grid:

- The three stages of the power supply–chain are generation, transmission, and distribution
  - Generation
  - Transmission
  - Distribution

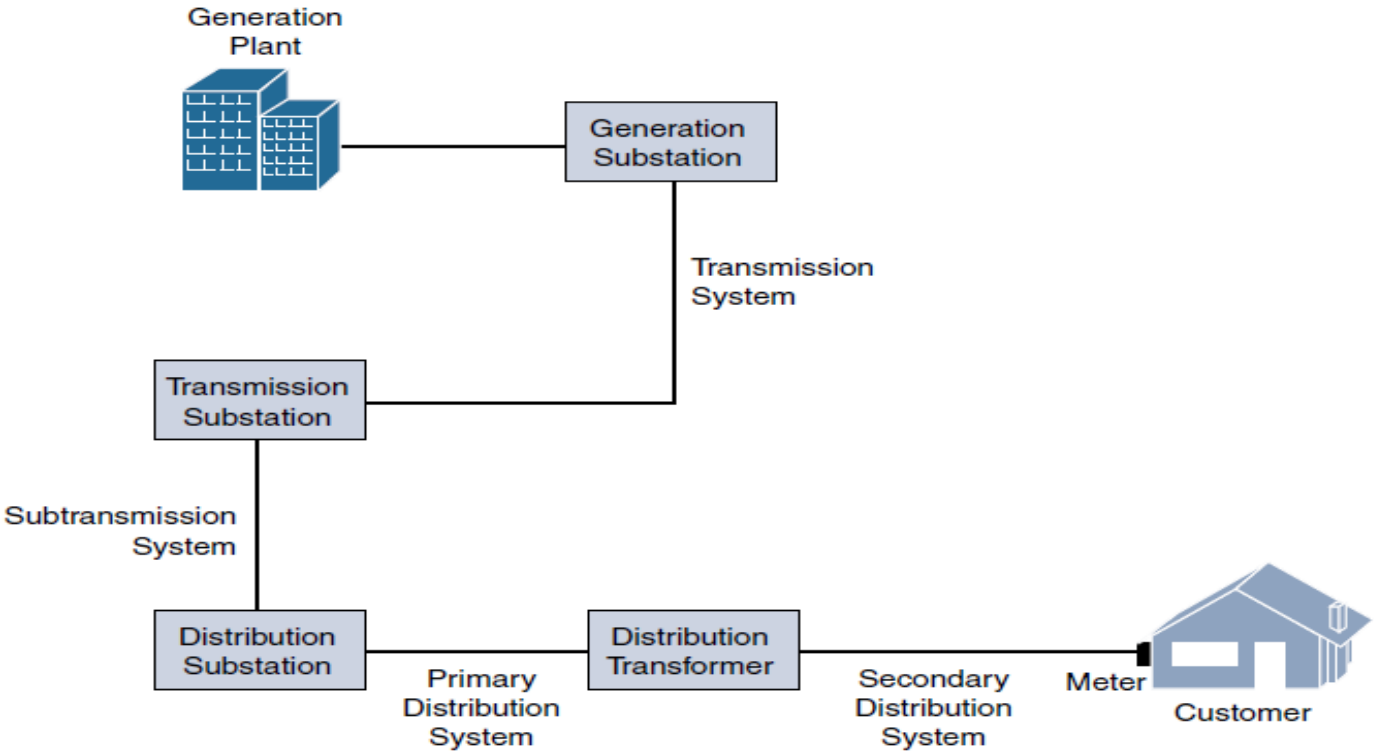


Figure 11-1 *Traditional Generation, Transmission, and Distribution Stages in a Power Utility Network*

Generation: Power generation is where the electricity gets produced. Power production typically includes nuclear, hydroelectric, gas, and coal pants. Once generated, high-voltage (HV) electrical power is sent through high-voltage transmission lines into the transmission system.

Transmission: Power transmission takes the HV power over long distances—typically 115 kV and above over distances of 50 km and greater. Transmission lines include aerial lines and also submarine cables that transmit HV electrical power over long distances underwater. The transmission system is responsible for connecting HV lines from generation stations to substations throughout the service area.

Distribution: Power distribution includes the part of the utility network from the substation to your home or business. This includes the medium-voltage (12.5 kV, for example) powerlines you see on poles around your neighborhood, including pad mount transformers.

The IT/OT Divide in Utilities

While OT networks are not as flexible as their IT counterparts, OT engineering departments have continually adapted to take advantage of newer technologies supporting the power grid.

OT engineers are always looking for better, more cost-effective ways to do things, and this often includes utilizing IT technology whenever possible.

Challenges of concern when IT and OT are interconnected

- How can network resiliency and redundancy be supported for mission-critical OT applications that keep the lights on?
- Who will support remote access to distributed systems on the grid that must transit both the IT and OT networks?
- How will security be governed in both the OT networks and the interconnection points between the IT and OT networks?
- Will change management be governed in the same way as it is for IT systems, or does the criticality of the OT applications require a new set of rules to ensure the continuity of business?

GridBlocks offers an easy-to-understand model for both novice and advanced users working in the utility space.

The model is forward-looking and is intended to be a generalized end-state reference framework that can help assist in deploying and designing end-to-end secure energy communications solutions for all aspects of the grid, thus facilitating a new and powerful foundation for utilities—the smart grid.

Benefits of GridBlocks reference architecture

- Details a flexible, tier-based model that supports incremental improvements to logical sections (tiers) of the grid
- Helps enable secure integration of both new and legacy technologies, improving overall manageability and visibility of network elements
- Builds on open standards, primarily IP, preventing vendor dependency and also supporting interoperability and thus promoting lower costs
- Provides a digitization roadmap for utilities, allowing them to modernize different parts of the grid in stages

The Primary Substation GridBlock and Substation Automation

There has been not so much progress in Electricity power industry as it is vividly seen in the telecommunication industry, nevertheless, one of the greatest progressive leaps in the past few decades in the electrical power industry has been the ability to connect devices and control them through telecommunications networks, and IoT is now taking this leap to a whole new level.

SCADA

SCADA is a system by which remote devices can be monitored and controlled by a central server. SCADA plays a critical role in the substation, allowing (as the name suggests) controls and data acquisition from remote devices, known as remote terminal units (RTUs) and intelligent electronic devices (IEDs).

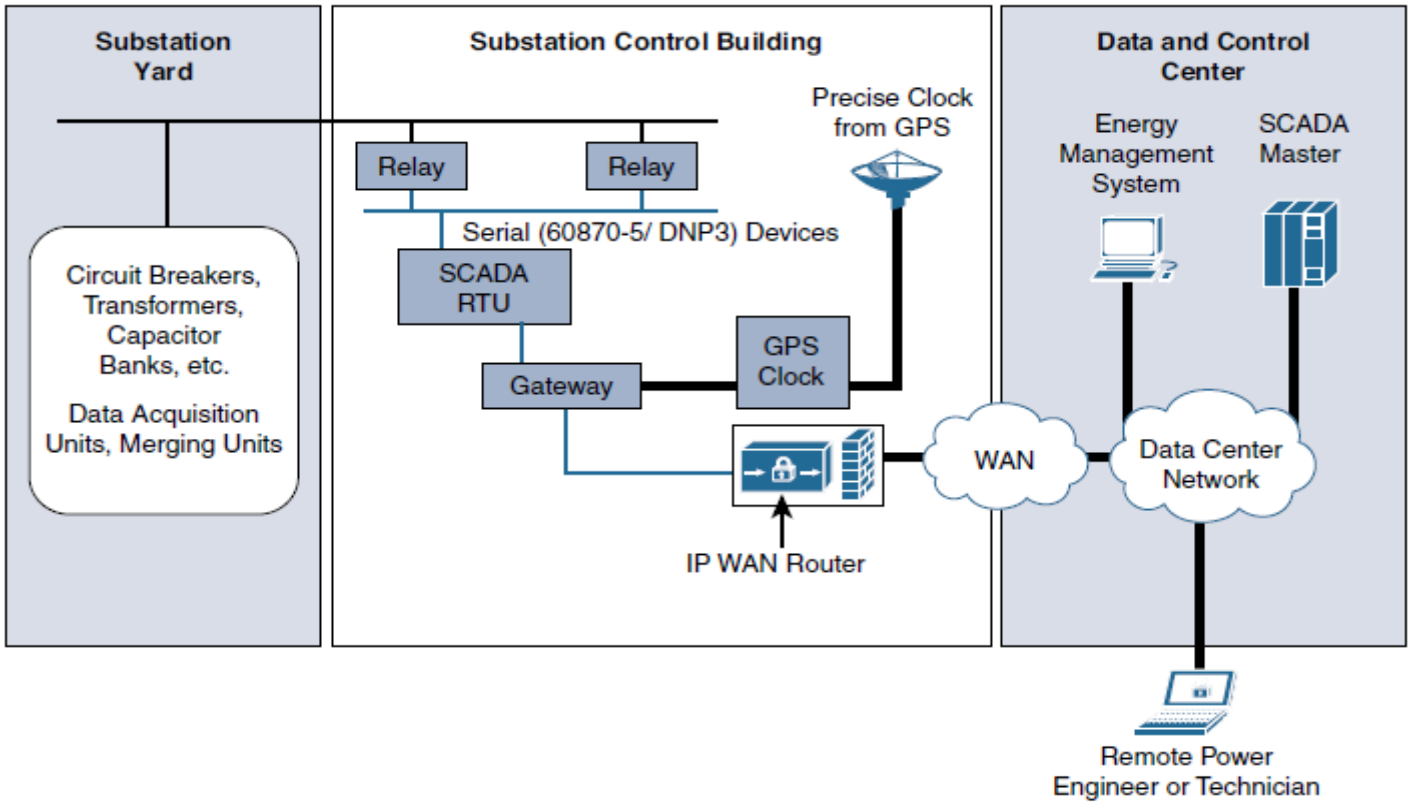
The intention of CSADA was to be a system in which an operator could manage remote industrial device from a central point (often a mainframe computer system).

Over time, remote WAN networks allowed SCADA

connectivity to extend to RTUs, but these connections were typically point-to-point

serial links that utilized RS-232

The legacy substation where the electrical relays are attached via serial (RS-232 or RS-485) connections to RTUs, which are in turn connected to a SCADA gateway device that is connected to the substation Ethernet network.



While we expect these legacy SCADA transport mechanisms to exist for many years to come, long term, traditional SCADA systems are being replaced by a new technology standard that natively takes advantage of Ethernet and TCP/IP: IEC 61850.

- **IEC 61850: The Modernization of Substation Communication Standards**

IEC 61850 was built from the ground up on modern standards and technologies and offers a host of new capabilities to IEDs in the substation

The inherent flexibility of Ethernet means that IEDs can easily communicate directly with one another and with other elements of the communications infrastructure.

Another key advantage offered by the flexibility of Ethernet is that interfaces are cheap and are being added by equipment vendors to all modern assets, which means unsupervised gear in the substation is now becoming a thing of the past.

- At station level there is communication with SCADA
- Station Bus interconnection between devices in the station level
- Bay level makes connection to power and current transformers.
- Process Bus has a collection of devices that effectively keep an eye on the overall function of their part of the grid.

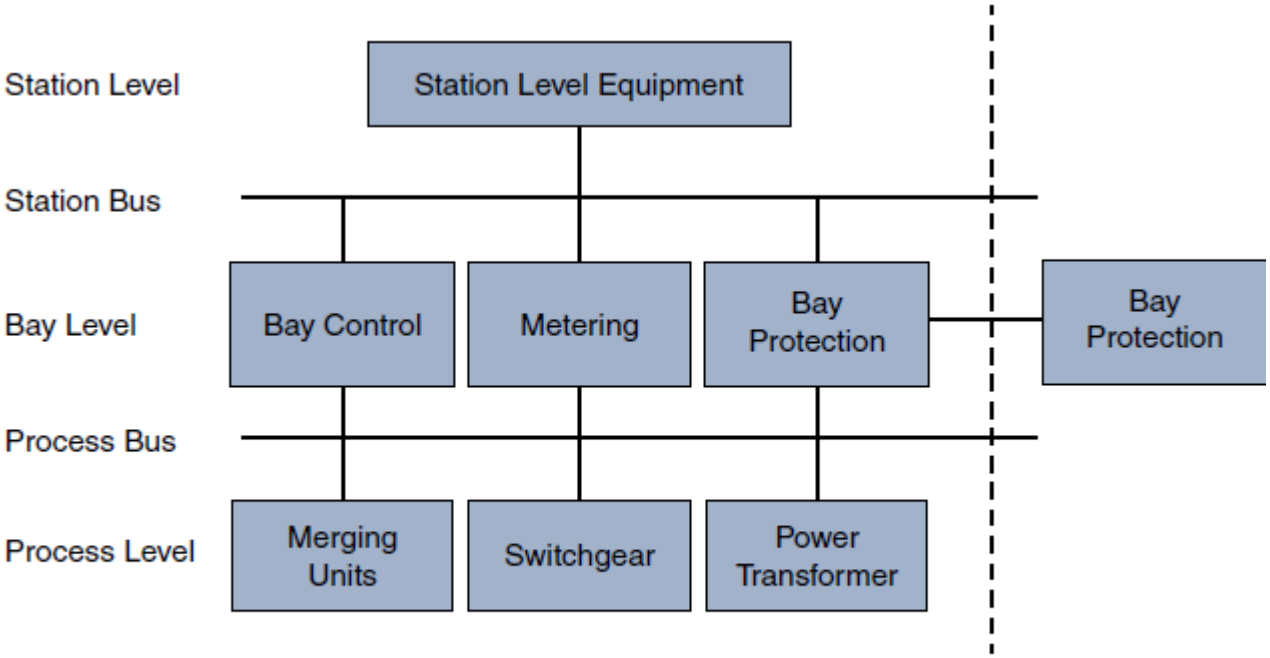


Figure 11-6 *Substation Automation Hierarchy*

Network Resiliency Protocols in the Substation

These protocols are designed to handle redundancy in the substations which can not be dealt using ITU and REP that are so stringent even to a single packet loss.

This is implemented in two protocols;

Parallel Redundancy Protocol - PRP is an IEC standard for implementing highly available automation networks which ensures that the network never loses even a single Ethernet frame, even in the event of a network outage.

High-Availability Seamless Redundancy – Unlike PRP, which relies on parallel network segments, HSR was designed for Ethernet ring topologies. HSR shares many similarities with PRP

One key constraint of HSR is that all intermediary switches in the ring must be capable of understanding HSR to remove the duplicate copy after the primary frame is switched on toward its destination.

System Control GridBlock: The Substation WAN

The WAN interconnecting the substations and the control center has become responsible for carrying applications that are intrinsic to the operation of the utility. This includes physical security systems,SCADA, and teleprotection

Protection according to IEC 60384, is defined as "the provision for detecting faults or other abnormal conditions in a power system, for enabling fault clearance, for terminating abnormal conditions, and for initiating signals or indications."

Teleprotection is the mechanism by which this information is transported over a network.

There are two common types of protection: **distance protection** and **current differential line protection**. Whatever the protection scheme, a communication system is always required between the relays

- **Distance Protection**

Distance protection monitors unacceptable variations in circuit impedance over a predetermined distance. If a relay sees a change in the impedance beyond acceptable thresholds, the relay determines that there is a fault on the line.

For a known line distance, the relay simply needs to measure the impedance of the line at key points, and then a calculation can show where the break is.

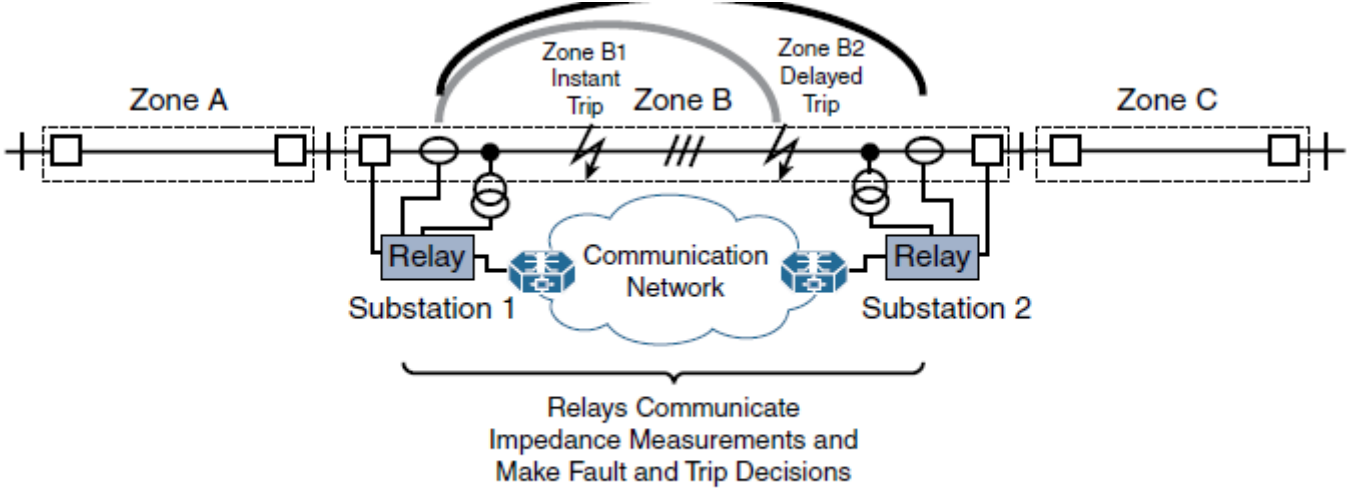


Figure 11-9 *A Sample Distance Protection Scheme*

If the measured impedance is different from what is expected, the relay can signal to the switch to either enable or disable a feeder line.

The relays measure impedance in the different zones and use this to isolate the location ofthe fault.

Current Differential (87L) Protection

Unlike distance protection, current differential protection compares current samples between two distant relays in different substations. For example, a nonzero differential in the current implies that there is a fault somewhere on the line that will cause the relays to trip.

For AC, timing is required for sync between the substations otherwise a false relay signal indicating power outage.

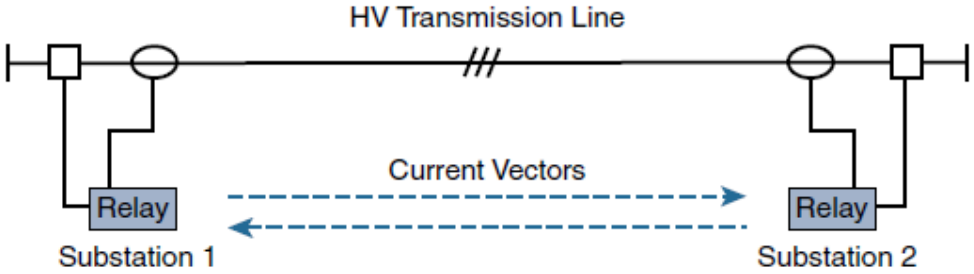


Figure 11-10 *Current Differential Protection Scheme for High-Voltage*

GPS-Sync is used to sync relays so that current is aligned, **channeled based sync** is also used to exchange timestamped messages between relays

Designing a WAN for Teleprotection

most modern utilities are now migrating to multipurpose packet networks such as MPLS to transport nearly all their applications, including teleprotection.

They are flexible, easy to scale, multitenant, and multiservice;

They are able to carry a host of different applications; and

They can even transport legacy protocols through channel emulation and tunneling services.

The downside of the IP-based WANS is that they don´t have support for predictable path with latency.

MPLS–Transport Profile (MPLS-TP), which brings capabilities for traffic engineering, automatic protection switching (APS), and Operations, Administration and Management

MPLS-TP transports a point-to-point pseudo-wire (a virtual circuit transported over MPLS) over a prescriptive label switch path (LSP).

Hop-by-hop LSP makes latency predictable and symmetrical,

and it also keeps jitter to a minimum

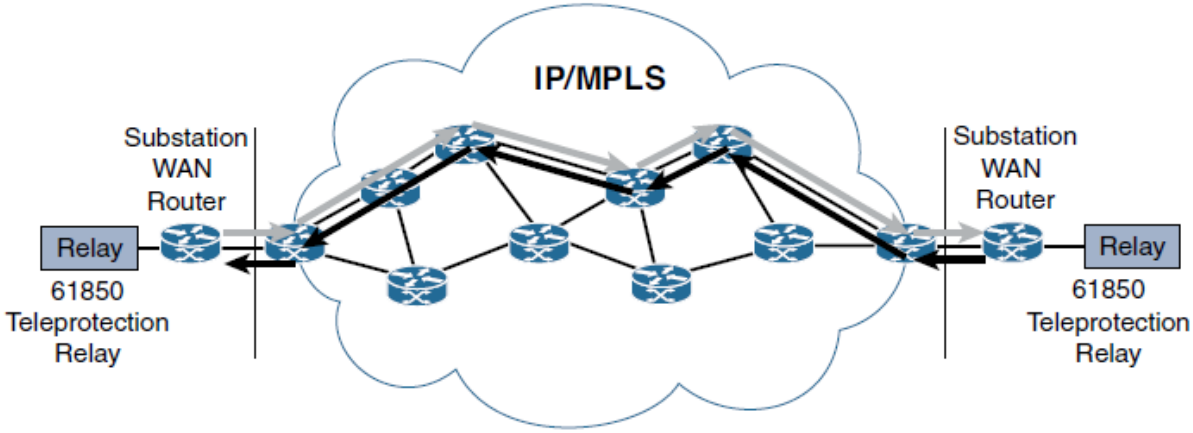


Figure 11-11 *Symmetrical Forward and Reverse MPLS-TP LSPs for Teleprotection Relays, Providing Predictable Latency and Jitter*

MPLS-TP also supports APS by identifying a known backup LPS path in case of a primary LSP failure.

MPLS-TP is that it supports end-to-end OAM. OAM allows for fault detection of the pseudo-wire at any point and is used as the trigger mechanism to fail over to a backup LSP.

MPLS-TP implements in-band OAM capabilities using a generic associated channel (G-ACh) based on RFC 5085 (Virtual Circuit Connectivity

The Field Area Network (FAN) GridBlock

The FAN is designed to enable pervasive monitoring and control of all utility elements between the distribution substation and the end customer.

The FAN GridBlock is built to be multiservice, meaning that it is not based on any vendor-specific, proprietary technologies that would limit its use to a single purpose, like so many legacy OT systems.

There exist modern standard alliances that such as Wi-UN and HomePlug that provide a common interface for all devices to ensure interoperability

It will soon be possible to have a fully functioning FAN network with various components supplied by different vendors, all using the same standards.

This flexible and open standards approach promotes multivendor plug-and-play capabilities with a well-understood framework for security, quality of service, resilience, and network management services.

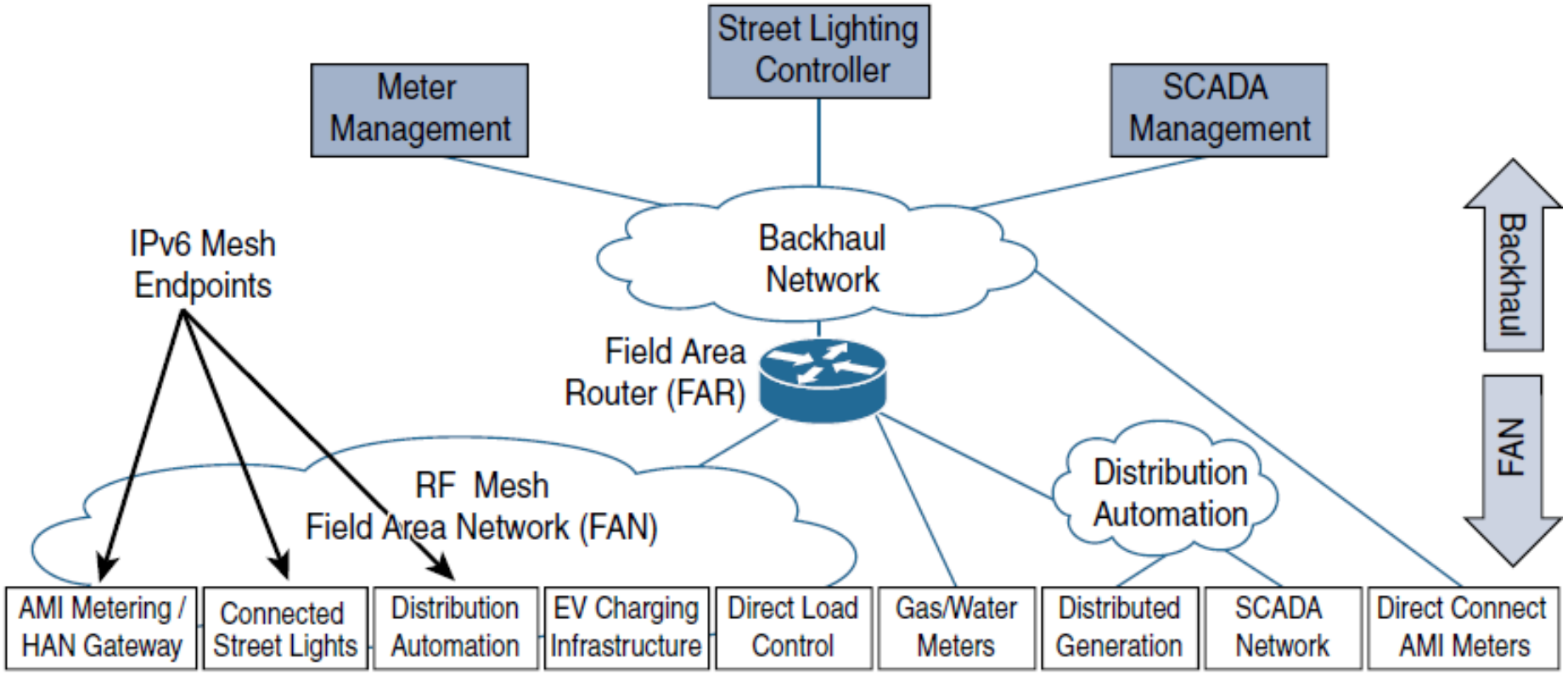


Figure 11-13 *The FAN Multiservice Grid Network*

- **The key advantages of the modern FAN**
  - Open and standards based:
  - Versatile endpoint support:
  - Flexible headend deployment options:
  - Flexible backhaul options:
  - Support for legacy applications:
  - Scalable:
  - Highly secure:
  - Stable and resilient:

The Application of FAN

- Advanced Metering Infrastructure
- Distribution Automation

- **Advanced Metering Infrastructure**

Smart meters are microprocessor-based sensors and controllers that exchange information such as device authentication, security, and management, using two-way communication processes.

This was intended to address the frequency of meter reading, meters were located in hard to reach areas so there was need for advancement in technology.

Benefits of Smart Meters

With the advent of smart meters, it is now possible to read meters several times per day. In the case of commercial and industrial (C&I) meters, readings can be done every few minutes to provide up-to-the-minute visibility into power consumption.

This has been extremely valuable for customers as they are now able to get highly accurate, per-month billing reports.

Customers can also view their power consumption on an hourly basis through a web portal

It´s now possible to remotely shut off a meter at will through a remote disconnect switch

In addition, most smart meters also come with an internal home area network (HAN) radio that is able to communicate with electrical devices inside the home, often through ZigBee.

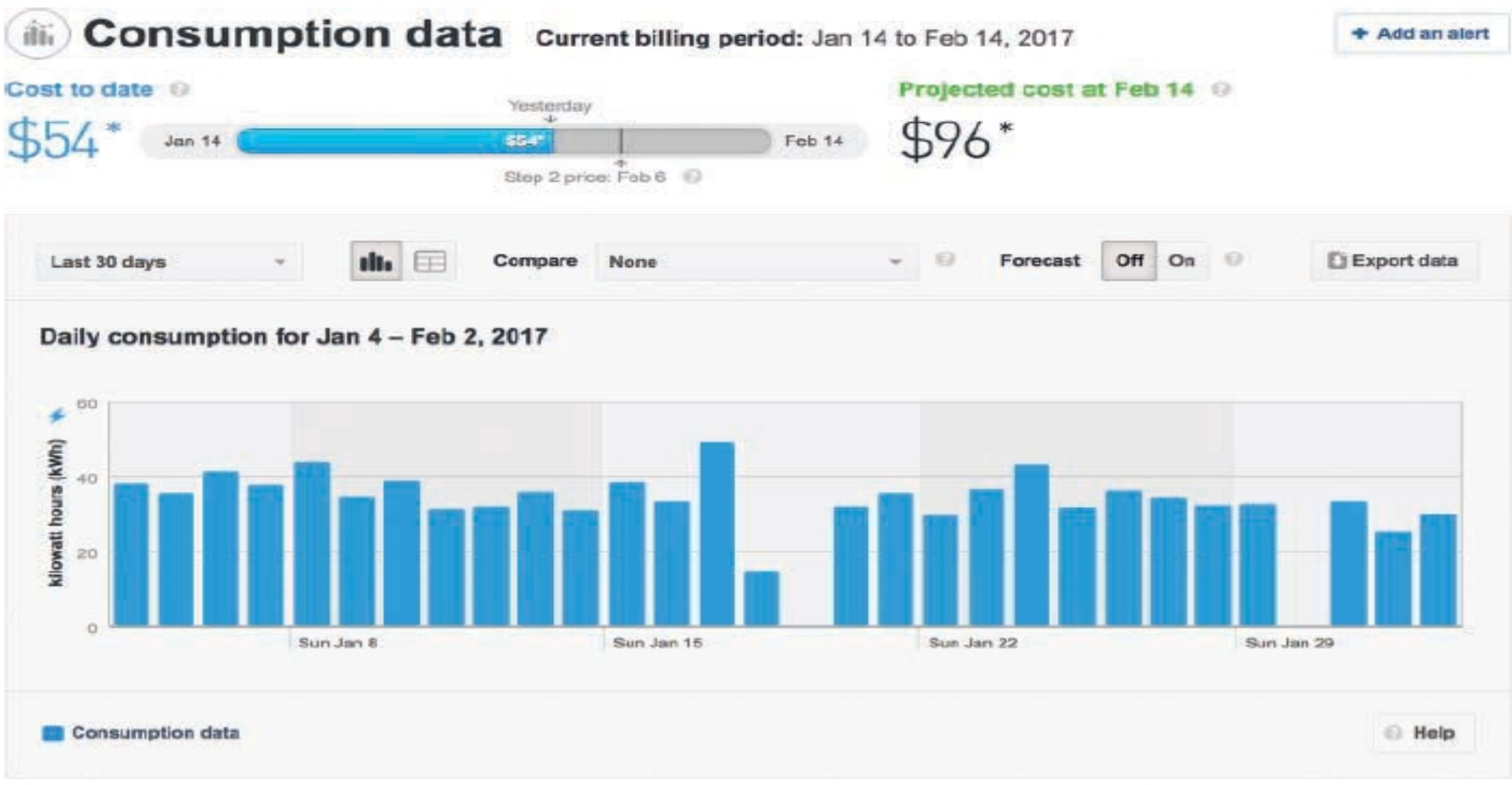


Figure 11-14 *A Smart Meter Web Portal Daily Report*

Each meter runs the IPv6 protocol stack and endeavors to find its place in the mesh through RPL.

But in this case the size of broadcast on the domain is not limited

The larger and denser the mesh, the further you are able to push it out into the neighborhood.

In a farm setting there maybe a hundreds of meters but there is only one meter with the upstream RPL link to a parent node leading to the FAR

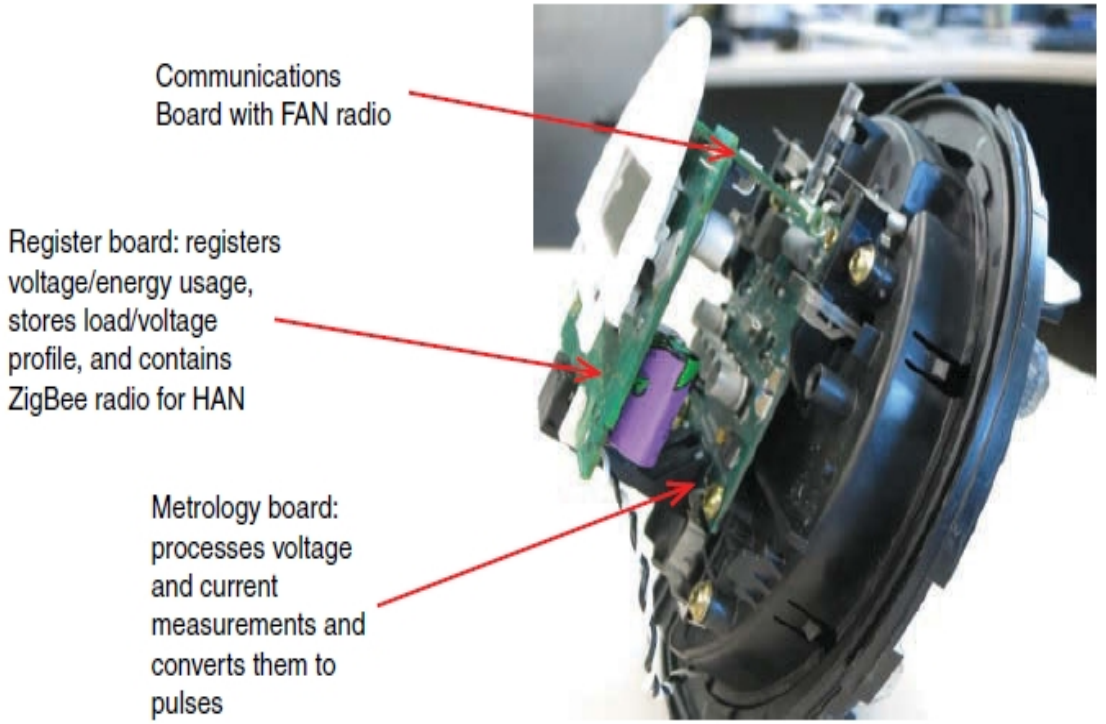


Figure 11-15 *The Anatomy of a Smart Meter*

- Other use cases of FAR
  - Demand Response:
    - If demand exceeds availability, something must give. For example, a large number of air conditioning units during a hot summer can tax a utility to the limit and may cause rolling blackouts.
    - The power is regulated and managed on less critical systems during peak periods so that the electricity can be available to customers throughout.
    - This involves deployment remotely controlled devices that turn off the flow of the electricity on certain devices during peak use periods.
    - In the past these devices were nothing but paggers that would receive signals from DR systems

Figure 11-17 An Electric Water Heater Connected to a FAN

- **Distribution Automation**

  - Electrical distribution devices include reclosers, load switches, and capacitor bank controllers. These devices all play key roles in electrical distribution grid services.
  - Due to the challenge of connecting distribution control and automation devices to a central network, they have, by and large, been designed to work as autonomous devices,in many cases with enough intelligence to operate without any supervisory control.
  - Deploying devices that sense grid operating environment has helped significantly improve the reliability and quality of electrical power in the distribution grid and has ushered in the age of DA

- Examples of how **FAN-based DA** is being used
  - **Distribution SCADA systems:**
    - When the SCADA endpoints are remote, the communications can be either aggregated at the substation and then sent back to the control center or sent directly to the control center, bypassing the substation altogether.
  - **Fault location, isolation, and service restoration (FLISR**
    - FLISR systems are designed to identify, locate, and diagnose problems so the utility knows instantly when an outage has occurred, and in some cases they even allow the circuits to self-heal.
  - **Integrated volt/VAR control (IVVC)**:
    - Volt/VAR systems are used in the distribution grid to monitor and control voltage levels during peak periods and help conserve electrical usage.
    - It is now possible to collect information from voltage sensors and use that information to adjust voltage-regulating equipment such as capacitor banks in real time.

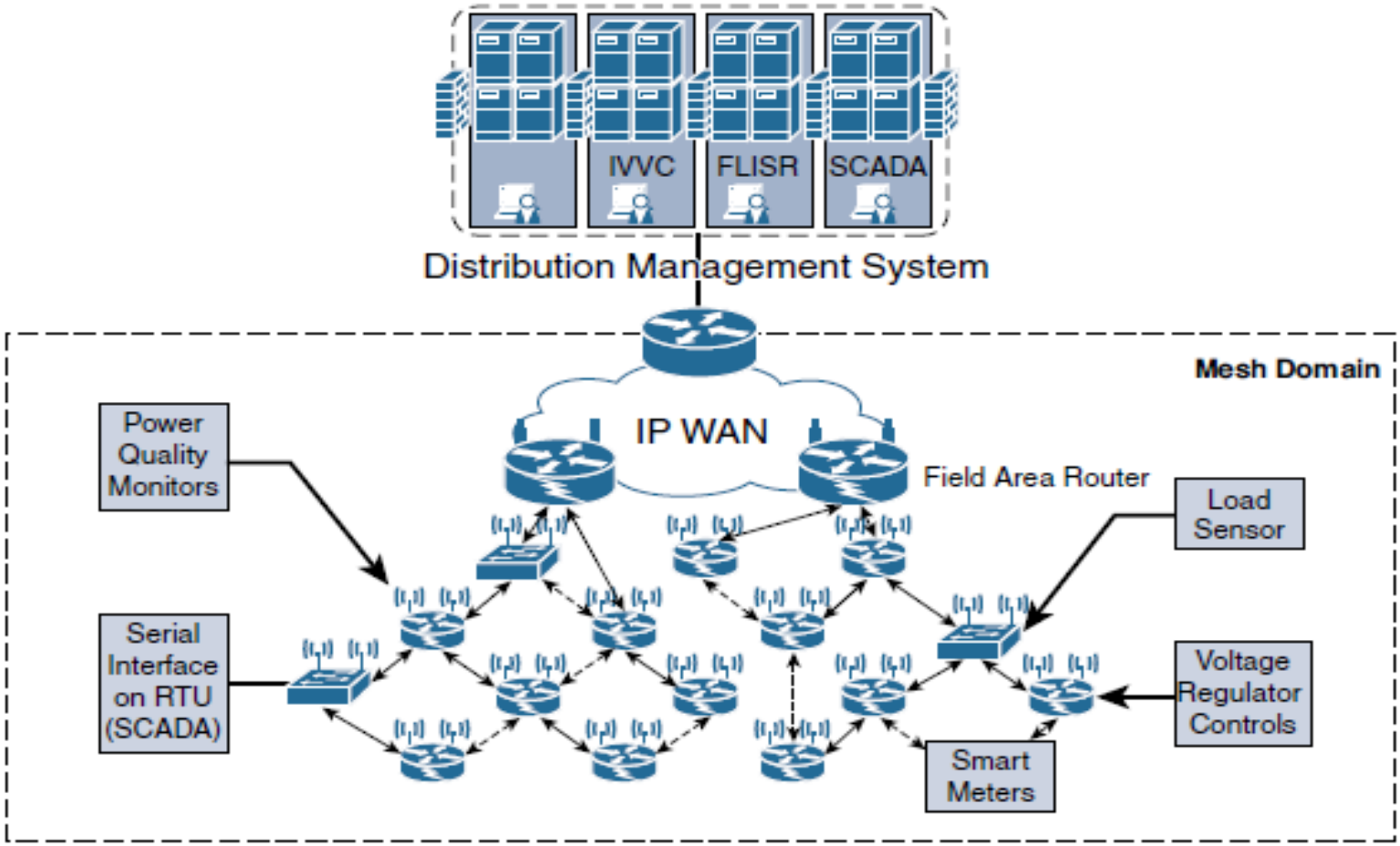


Figure 11-18 *Various DA Devices, Including SCADA, FLISR, and Integrated Volt/VAR Control Systems Connected Using a Single Multiservice FAN Grid Network*

Securing the Smart Grid

- Implementation of SCADA didn´t have in mind the security issue since SCADA connections to remote devices used dedicated serial links that were physically isolated
- The 2015 Ukrainian power attack, this cut power to 103 cities and towns (and affected 186 more) involved a sophisticated simultaneous attack on six power companies. Started as a malware on the computers but spread also to OT Systems.
- This was a wake up call for many industries that implemented SCADA IoT Network Architecture to rethink their design to include security.
- According to a Cisco Security Capabilities benchmark study, 73% of utility IT security professionals say they´ve suffered a security breach, compared with an average of 55% in other industries.

- **Different utility-based security architectures proposed**
  - **NERC CIP**(The North American Electric Reliability Corporation´s (NERC´s) Critical Infrastructure Protection (CIP)
    - It is a security model that was developed to protect bulk systems, and it continues to be one of the most important security subjects for North American utilities.
    - NERC CIP uses a risk-assessment security approach. Instead of using an exhaustive list of prescriptive recommendations and enforcing them through audits, NERC provides a clear vision of the security end state.
    - NERC CIP is primarily focused on establishing security policies, programs, and procedures.
    - Utilities need to properly identify what impact level each asset fits into, with levels defined as high, medium, low, or no impact at all.

NERC CIP v6 also requires intrusion detection/prevention systems (IDS/IPS) or some form of deep packet inspection (DPI).

The standard also mandates that an electronic security perimeter (ESP) be defined where assets within the EPS are protected by two distinct security measures, such as a firewall and an IPS.

The physical security perimeter (PSP) is defined, which includes other aspects, such as video surveillance and building access systems, and aims to protect the station against physical attack

A key aspect of NERC CIP is that an ESP must be established for all high- and mediumimpact

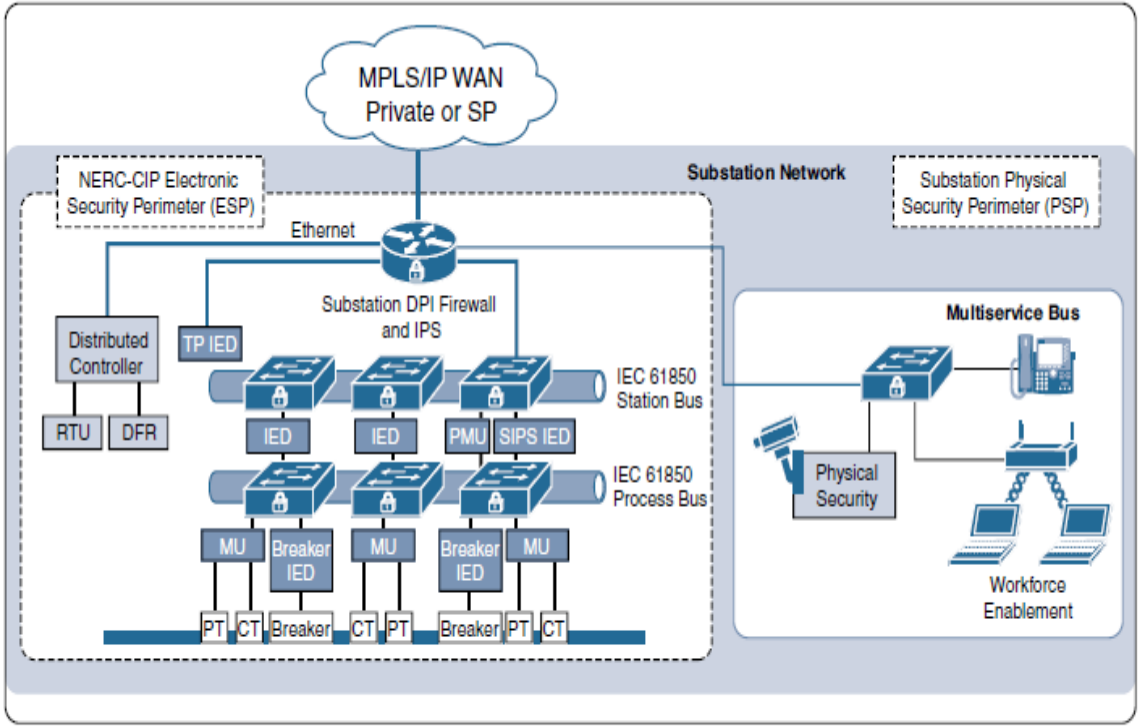


Figure 11-19 *A Primary Substation Network with NERC CIP v6 Electronic and Physical Security Perimeters*

BES cyber systems connected to a routable network, regardless of whether the segment containing the BES cyber system has external connectivity to any other network.

- Smart Grid Security Considerations

FAN security is aligned to the following principles:

■ **Access control:** FAN devices reside in generally insecure locations, so the devices themselves need to have highly secure access control. If a grid IoT endpoint were maliciously added to a FAN, it could be a backdoor to the network.

■ **Data integrity and confidentiality:** FAN devices need encryption. Last-mile FANs often use unlicensed wireless technologies that could be easily sniffed. Encryption at each layer of the stack is strongly recommended.

■ **Threat detection and mitigation:** One way threat detection and mitigation are accomplished is through the logical separation of the FAN headed components and systems from other critical systems in either the substation or the control center.

■ **Device and platform physical integrity:** The field area assets, such as the FAR, need to be physically secured as much as possible.

- **The Future of the Smart Grid**

  There still exist challenges that need to be addressed and these include;

  - Concerns about pollution emitted by generation plants,
  - Consumers´ insatiable appetite for more power,
  - The associated costs of constantly expanding the electric grid infrastructure,
  - The apparent fragility of an increasingly complex grid.

These challenges include requirements to incorporate electric power generated by inherently variable renewable resources, such as wind and solar, as well as integrated distributed energy

resources (DERs), such as solar photovoltaic (PV) cells that are installed and owned by the customer rather than the utility but sell power back to the utility grid.

Due to the ever increasing cost of electricity usage, people might resort to using alternatives like solar or generate their own.

The age of distributed generation and renewable energy builds a very strong case for the smart grid.

- There is need to have a reliable network system that is able to communicate between elements in the utility´s grid and IoT devices at the DER, such as the inverter or the smart meter.
- Another disruptive change we are seeing is the rise of EVs. As more and more electric cars are introduced, they will require more power from the grid, and there is also the potential to use these fully-charged car batteries as remote power storage units. There has to be conversion of power from DC to AC, this is another test on reliable communication in IoT network.