Communication Aspects in RePlan

Agreement no.:	PSO ForskEl 12347
Project Name:	Ancillary Services from Renewable Power Plants
Acronym:	RePlan
Duration:	2015 - 2018
Co-ordinator:	DTU Wind Energy

Document information

Document name:	Communication Aspects in RePlan
Document number:	
Contributors:	**Kamal Shahid**, Rasmus Løvenstein Olsen
Document type:	Internal
Dissemination level:	
Date:	
WP:	
Task:	

Content

Preface

This document provides highlights from the communication perspective in regards to communication scenarios, communication architecture and relevant properties of communication in smart grid scenario, focusing on the cases found in the project RePlan. An overview of standards and highly relevant protocols are found in this deliverable which is basically a summary of the existing standards, whereas also performance metrics are defined and discussed. Finally, an overview of challenges is provided in the last chapter of this report.

1 Scope of document

The aim for this document is to give an overall introduction to network issues and challenges that exist in the scope of RePLAN and related topics of smart grid. The purpose is not to give details of the ongoing research but to give non experts and insight into the issues that networking people are addressing as a help in communication (as in communication between people) between the different groups of people.

The document is continuously being improved as feedback is obtained as to ensure its objective is achieved effectively.

2 Typical Communication Scenarios

In the first chapter here we describe a few typical communication scenarios in power systems. These scenarios represent various data communications in the network infrastructure that provides intelligent support to energy management. Specifically, as the smart grid power systems are featured by automated bi-directional information exchanges in every phase of energy generation, distribution and usage. Figure 1 from [1] describes all these scenarios in one place.

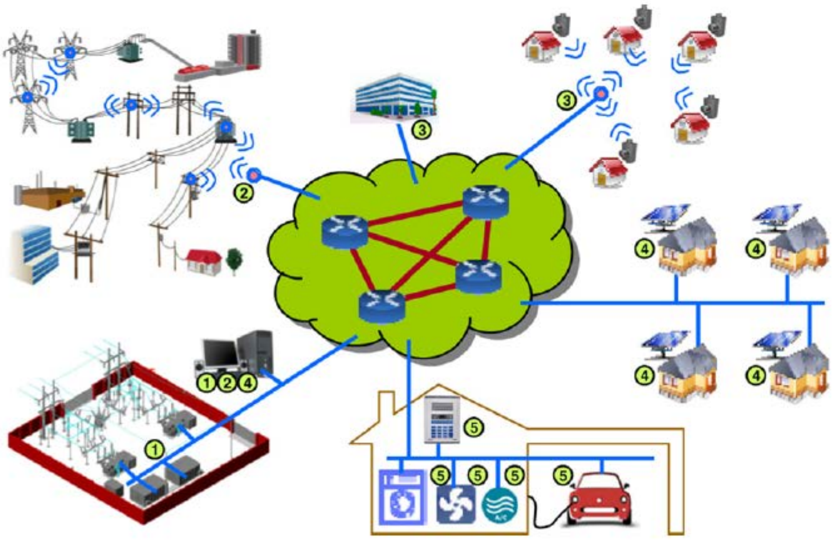


Figure 1 Communication Scenarios: (1) substation control, (2) power line monitoring, (3) automatic meter reading, (4) demand-response decisioning, (5) energy usage scheduling [1]

2.1 Substation control [1]

The electrical substation (Figure 1, case 1) is an important component in power systems. It changes the voltages on the electrical transmission lines and controls the power flow in the transmission system. A substation is a complex system composed of many elements such as transformers, capacitors, voltage regulators, and circuit breakers. Automated substation control will be implemented extensively in the smart grid systems to provide real-time monitoring and control through local area networks. The possible network technologies to be used in a substation include Ethernet and wireless LAN. To connect the various equipment in a substation, specialized sensors are attached to the equipment to take their status samples. The sampled values are then digitized and transmitted through the local area network to the control station in the substation. When the packet is received by the control station, a response may be made by the control station and a configuration message may be sent back to the electrical equipment.

2.2 Transmission line monitoring [1]

Electricity is transmitted and distributed from power generation plants to customers through power lines (Figure 1, case 2). The power lines may span over long distance and some segments may travel through less populated areas. Prompt detection of transmission anomalies is critical to ensure satisfactory power quality and service. One method of automated transmission line monitoring is to install sensors along the lines to collect the real-time status measurements. Each sensor is equipped with wireless communication capability to exchange data with neighbors. The real-time measurements are relayed through the sensors until they reach a measurement collection site, which is connected to the wide area networks for communications to the control office.

Sensors communicate with neighbors using wireless links, which are subject to interferences. It is therefore important to coordinate the sensor transmissions to ensure successful communications. Besides sending own measurements, some sensors also relay packets for others. The traffic loads on different sensors may be unbalanced, which should be considered in scheduling their transmissions. Sensors will higher loads should be allowed to transmit for longer time to maintain the communication network stability.

2.3 Automatic Meter Reading [1]

Facility companies need to read the electricity meter from each household for billing purpose. The traditional method is to send technical staffs to take the readings manually. With the deployment of communication infrastructure, meter reading can be automated and simplified (Figure 1, case 3). Electricity meters equipped with communication capability can send the meter readings automatically over the network to the facility companies. There are a number of advantages to replace the traditional meters with the networked intelligent meters. First, the billing cost is lowered. Facility companies do not need to send staffs for meter reading any more. Second, the billing process can be completely automated. The readings received from the network can be processed immediately to generate customer bills. Third, accurate and detailed usage information can be collected from customers. Readings can be made in periods shorter than the monthly billing cycle such that facility companies are able to analyze customer usages with improved data accuracy.

To read the electricity meters automatically, a facility company installs a reading collection device in each household subdivision. The meters send their readings to the collector through wireless links. As the collector location can be planned carefully, each meter communicates directly with the collector. A scheduling mechanism should be implemented to coordinate the transmissions from different meters to avoid transmission collisions. The collector then relays the readings through the wide area network to the facility company. The collector may either forward each reading as a separate packet or assemble a number of readings for group sending. Forwarding group readings reduces the communication overhead, but collection delays may be incurred. As meter readings are not sensitive to communication delay, it is acceptable to receive the readings with a delay of about a few seconds.

2.4 Demand-Response Decision [1]

In the smart grid power systems, electricity is generated distributive. Supplementary to large power plants, many households are installed with solar panels to convert sunlight into usable electricity. Wind turbines, small hydros and geothermal plants can also be constructed in regions with renewable energy resources to generate electricity. The electricity market will become diversified due to the participation of many small to medium sized suppliers. The communication infrastructure will connect all the energy suppliers and all the energy customers to provide a platform for energy trading

(Figure 1, case 4). The supply and demand of electricity change dynamically on the market due to the time varying properties of electricity generation and usage. Communications regarding the electricity availability and price are exchanged through the network for each supplier and each customer to reach a balance between the supply and the demand.

Each electricity supplier or customer publishes its amount of energy availability or demand through the wide area network. Different network access technologies may be used to connect the energy market participants. For example, a large business may have its own local area network through which its electricity usage information is sent out to the wide area network, and a household may access the wide area network through a dial-up phone line or a cable modem. The communications on the energy market are from multiple sources to multiple destinations, and each participant exchanges information with multiple others to look for the most favorable energy price. The path taken by a message consists of the segments in the access networks and the wide area network respectively. Because there are potentially many participants on the market, the communication delay perceived by individual packet may vary significantly. The smart grid users may expect a communication delay within a few seconds to catch up with the dynamic market states.

2.5 Energy usage scheduling [1]

The electricity price changes in the market as determined by the supply and demand. The price is usually higher during the daytime and lower at night. In the daytime, electricity is largely consumed by factories and all types of office buildings. At night, the demand for electricity decreases when factories and office buildings are closed. Accordingly, energy price varies at different times of a day. Customers can take advantage of the dynamic energy prices to reduce the energy cost by scheduling time flexible energy usages at the time of low energy prices. For example, the washer and dryer are used at night and the electric vehicle is charged at night. Home area networks can be deployed to connect the electrical appliances in a house to a scheduler, which activates each appliance at the appropriate time to minimize the cost of using electricity.

To schedule the energy usage according to the electricity price, the electrical appliances in a home are connected to a scheduling controller through a home area network. Usually, a wireless router is sufficient to set up a home network. The electrical appliances under scheduling may include washer, dryer, aircon, fan, light, and electric vehicle. These appliances can be connected into the home network either with wirelines or with wireless links. The scheduling controller requests electricity prices periodically from the energy market, based on which the controller determines an economic operation schedule to activate each appliance at appropriate time. The communications between the scheduling controller and the energy market and the communications between the controller and the electrical appliances do not have strict delay requirement. A delay of a few seconds is reasonably good to schedule energy usages.

2.6 RePlan Communication Case

As it is clear from the above discussion, in order to have coordination between the generation, distribution, and consumption of energy, smart grids greatly depend upon communication infrastructure, this dependency increases even more if the distributed power plants are based on renewable energy e.g. wind power, solar energy. Thus to achieve the goal of Danish government – converting the present energy system into an entire renewable energy integrated system by the end of 2050 – and coping with an increased number of ReGen plants in the system, RePlan project proposes an addition of Aggregator control unit between plant controllers and Transmission/Distribution systems. This control unit plays a role into the delivery of system services that are needed to ensure the system stability comprising both transmission and distribution level, namely ancillary services, as shown in Figure 2.

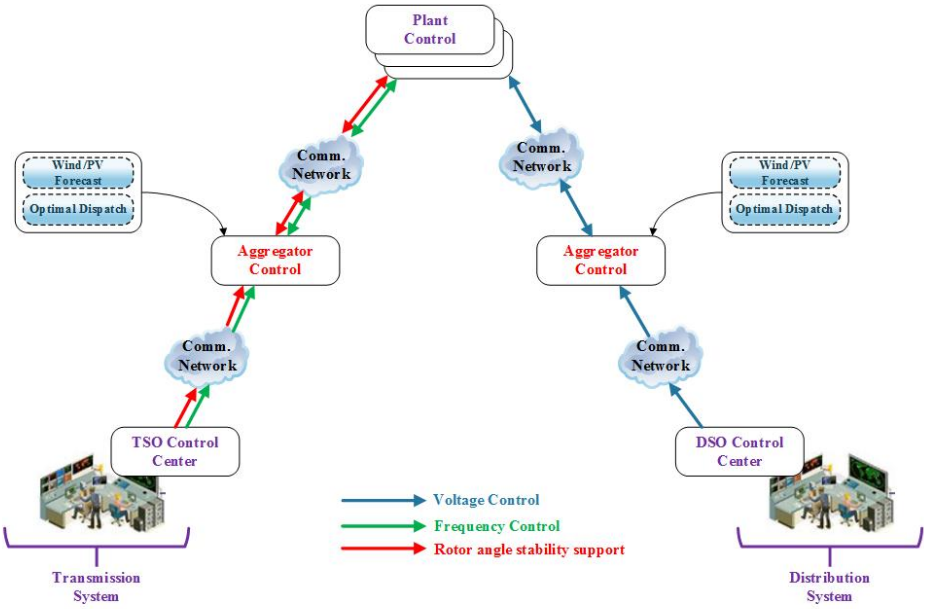


Figure 2 RePlan Communication Scenario

This model depicts how different assets in the RePlan scenario are connected together via a communication network. Each communication network has its own requirements that may differ from one another in terms of coverage range, distance covered, the maximum data rate, maximum delay allowed, and the information access strategies used.

However, to connect the plant control equipment in a substation, specialized sensors are attached to the equipment to take their status samples (e.g. voltage, frequency etc.). The sampled values are then digitized and transmitted through the network to the aggregator control.

The transmitted messages may be continuous data streams or isolated packets, depending on the particular controlling applications. A message generated by the sensor attached to an electrical equipment is processed by the network protocol stack and then transmitted on the network. The network may consist of a number of subnets connected through switches. Each switch on the path of packet transmission processes and forwards the packet. When the packet is received by the aggregator control station, a response may be made by the control station and a configuration message may be sent back to the plant control. As many plant control stations are monitored and controlled in a substation, all the communications share the network bandwidth.

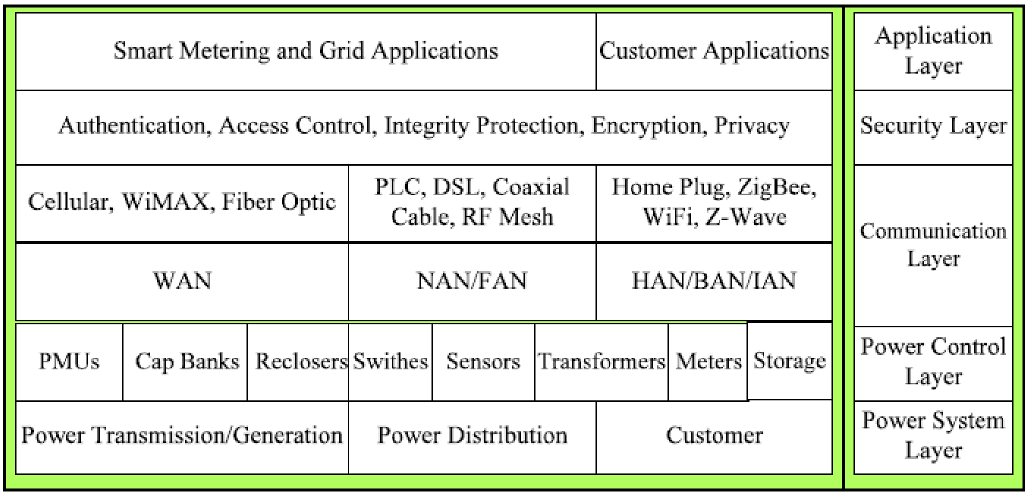
The delay requirements are determined by the type of measurements transmitted. According to [1], when the messages are used for periodic maintenance measurements, a maximum network delay of about 1 s is allowed. When the messages convey real-time monitoring, control information and are meant for a constant and continuous monitoring of important working states (such as voltage and frequency), the network delay should be limited to around 10 ms. In case that the messages carry urgent equipment fault information (reporting failures), the delivery to the control station should be within 3 ms. When the control station sends response messages, the delays should be comparable to those of the messages received by the control station.

3 Communication network architecture and various technologies for the Smart Grids

Smart grids are often characterized by the active use of information collected about the electrical grid to control assets in order to achieve some set objectives and in general consist of a power system layer, a control layer, a communication layer, a security layer and an application layer (See Figure 3). In general, a smart grid comprises:

1) A power system layer, which refers to power generation, transmission, distribution and customer systems;
2) A power control layer, which enables smart grid monitoring, control, and management functions;
3) A communication layer, which allows two-way communications in a smart grid environment;
4) A security layer, which provides data confidentiality, integrity, authentication and availability; and
5) An application layer, which delivers various smart grid applications to customers and utilities based on an existing information infrastructure.

For example, to enable a smart metering application, an electric grid must have the power system layer – which is an electric power distribution system that delivers electricity to customers; a power control layer – which is a smart meter that enables power consumption to be monitored; a communication layer – which is necessary to allow transmitting information from a customer to a utility or vice versa; and a security layer – which is necessary to address data privacy issues.



<table>
<tr><td colspan="5">Smart Metering and Grid Applications</td><td colspan="3">Customer Applications</td><td>Application Layer</td></tr>
<tr><td colspan="8">Authentication, Access Control, Integrity Protection, Encryption, Privacy</td><td>Security Layer</td></tr>
<tr><td colspan="3">Cellular, WiMAX, Fiber Optic</td><td colspan="2">PLC, DSL, Coaxial Cable, RF Mesh</td><td colspan="3">Home Plug, ZigBee, WiFi, Z-Wave</td><td rowspan="2">Communication Layer</td></tr>
<tr><td colspan="3">WAN</td><td colspan="2">NAN/FAN</td><td colspan="3">HAN/BAN/IAN</td></tr>
<tr><td>PMUs</td><td>Cap Banks</td><td>Reclosers</td><td>Swithes</td><td>Sensors</td><td>Transformers</td><td>Meters</td><td>Storage</td><td>Power Control Layer</td></tr>
<tr><td colspan="3">Power Transmission/Generation</td><td colspan="2">Power Distribution</td><td colspan="3">Customer</td><td>Power System Layer</td></tr>
</table>

Figure 3 The system multi-layer architecture of Smart Grid [2]

The communication layer is one of the most critical elements that enables smart grid applications. In the smart grid environment, a communication network can be represented by a hierarchical multi-layer architecture. Classified by data rate and coverage range, this architecture comprises:

- Customer premises area network, i.e., Home Area Network (HAN)/Building Area Network (BAN)/Industrial Area Network (IAN) – Not to be focused in RePlan.

- Neighborhood Area Networks (NAN)/Field Area Network (FAN).
- Wide Area Network (WAN).

Data rate and communication range requirements for these networks are summarized in Figure 4.

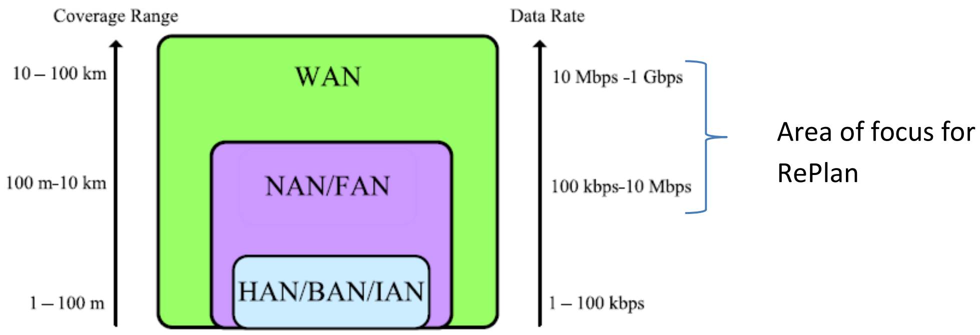
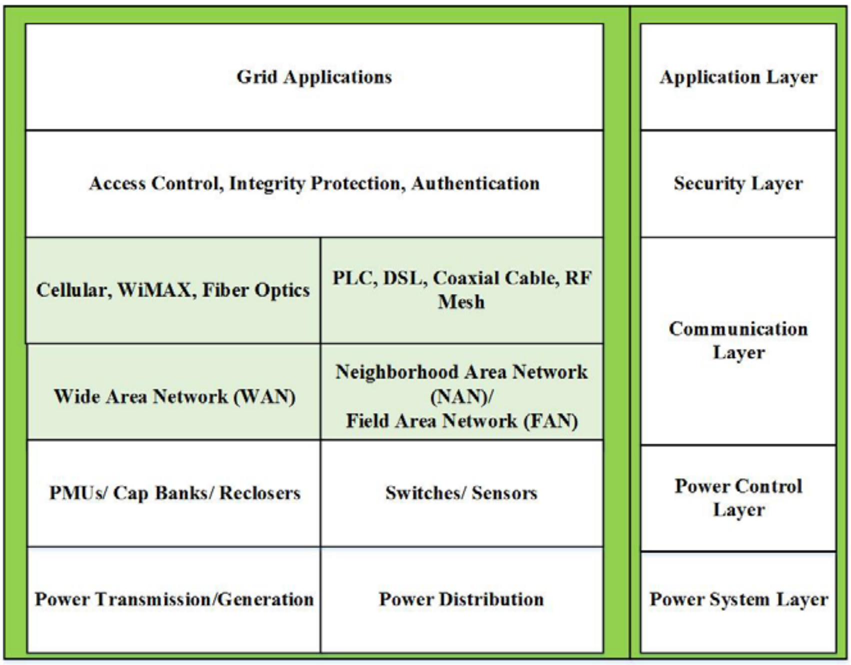


Figure 4 Data Rate and Communication range requirements for Smart Grid Communications hierarchy [2]

But since RePlan does not focuses on the customer applications, Figure 3 can be adapted as shown in Figure 5.



Grid Applications		Application Layer
Access Control, Integrity Protection, Authentication		Security Layer
Cellular, WiMAX, Fiber Optics	PLC, DSL, Coaxial Cable, RF Mesh	Communication Layer
Wide Area Network (WAN)	Neighborhood Area Network (NAN)/ Field Area Network (FAN)	
PMUs/ Cap Banks/ Reclosers	Switches/ Sensors	Power Control Layer
Power Transmission/Generation	Power Distribution	Power System Layer

Figure 5 The system multi-layer architecture for RePlan

In NAN/FAN applications, such as smart metering, demand response and distribution automation, data are required to transmit from a large number of customers/field-devices to a data concentrator/substation or vice-versa. Therefore, these applications require communication technologies that support higher data rate (100 kbps–10 Mbps) and larger coverage distance (up to 10 km). NAN/FAN applications can be implemented over ZigBee mesh networks, WiFi mesh networks, PLC, as well as long distance wired and wireless technologies, such as WiMAX, Cellular, Digital Subscriber Line (DSL) and Coaxial Cable.

For WAN applications, such as wide-area control, monitoring and protection, which require transmitting a large number of data points at much higher frequency (i.e., in a fraction of seconds) to allow stability control of a power system, communication technologies that support much higher data rate (10 Mbps–1 Gbps) and provide long coverage distance (up to 100 km) are therefore required. Optical communication is commonly used as a communication medium between transmission/distribution substations and a utility control center due to its high capacity and low latency. Cellular and WiMAX are also used due to their wide coverage range and high data throughput. Satellite communications can also be used to provide redundant communications at critical transmission/distribution substation sites as backup a communication mean in a remote location.

A comparison of various communication technologies that can support smart grid applications in terms of data rate and coverage distance is presented in Table 1.

Table 1 Comparison of communication technologies for the smart grid in context of RePlan [2]

Technology	Standard/Protocol	Max. theoretical data rate	Coverage Range	Network	
				NAN/FAN	WAN
Wired Communication Technologies					
Fiber Optic	PON	155 Mbps – 2.5 Gbps	Up to 60 Km		×
	WDM	40 Gbps	Up to 100 Km		
	SONET/SDH	10 Gbps	Up to 100 Km		
DSL	ADSL	1 – 8 Mbps	Up to 5 Km	×	
	HDSL	2 Mbps	Up to 3.6 Km		
	VDSL	15 – 100 Mbps	Up to 1.5 Km		
Coaxial Cable	DOCSIS	172 Mbps	Up to 28 Km	×	
PLC	HomePlug	14 – 200 Mbps	Up to 200 m		
	Narrowband	10 – 500 kbps	Up to 3 Km	×	
Ethernet	802.3x	10 Mbps – 10 Gbps	Up to 100 m	×	
Wireless Communication Technologies					
Z/Wave	Z-Wave	40 kbps	Up to 30 m		
Bluetooth	802.15.1	721 kbps	Up to 100 m		
ZigBee	ZigBee	250 kbps	Up to 100 m	×	
	ZigBee Pro	250 kbps	Up to 1600 m		
WiFi	802.11x	2 – 600 Mbps	Up to 100 m	×	
WiMAX	802.16	75 Mbps	Up to 50 Km	×	×
Wireless Mesh	Various (e.g. RF mesh, 802.11, 802.15, 802.16)	Depending on selected protocols	Depending on deployment	×	
Cellular	2G	14.4 kbps	Up to 50 Km	×	×
	2.5 G	144 kbps			
	3 G	2 Mbps			
	3.5 G	14 Mbps			
	4 G	100 Mbps			
Satellite	Satellite Internet	1 Mbps	100 – 6000 Km		×

As wireless technologies provide lower installation cost, more rapid deployment, higher mobility and flexibility than its wired counterparts, wireless technologies are recommended in most of the smart grid applications. Advantages and disadvantages of each technology have already been discussed in our previous study [3] in terms of their data rates and coverage ranges, and will not be repeated in this document.

4 Overall communication properties and performance metrics [1]

The communication infrastructure in smart grid undertakes important information exchange responsibilities, which are the foundations for the function diversified and location distributed electric power devices to work synergistically. Unsatisfactory communication performance not only limits the smart grid from achieving its full energy efficiency and service quality, but also poses potential damages to the grid system. To protect the smart grid and ensure optimal operation, the communication infrastructure must meet a number of requirements [4] [5]. All these metrics can be defined for different layers of the OSI model (see later in Chapter 6) and will thereby attain different values. This is therefore also reflected in the specific communication protocol and system when performance is measured, e.g. TCP performance is much different from UDP or Ethernet performance because of the protocol behaviors influence on the performance.

4.1 Network Latency

Network latency defines the maximum time in which a particular message should reach its destination through a communication network. The messages communicated between various entities within the power grid, may have different network latency requirements. For example, the protection information and commands exchanged between intelligent electronic devices (IEDs) in a distribution grid will require a lower network latency than the SCADA information messages exchanged between electrical sensors and control centers. Moreover, the messages exchanged can be event driven (e.g., protection and control related) or periodic (e.g., monitoring related). The network architecture and communication medium must support the diverse requirements. The network architecture will determine if the message sent from one communicating entity to the other will reach its destination in one or more hops. This will directly affect the latency. Similarly, the data rates supported by the communication medium also dictate how fast an entity can communicate an event observed or reply to a message received.

4.2 Data delivery criticality

The protocol suite used for a particular power system application must provide different levels of data delivery criticality depending on the needs of the application. This need may be decided at the time of connection establishment between two applications. The following levels of data delivery criticality may be used: (a) high is used where the confirmation of end-to-end data delivery is a must and absence of confirmation is followed by a retry. For example, this may be used for delivery of SCADA control commands for settings and changes of switch gear position; (b) medium is used where end-to-end confirmation is not required but the receiver is able to detect data loss, e.g., measured current and voltage values and disturbance recorder data; (c) non-critical is used where data loss is acceptable to the receiver. In this case reliability can be improved by repetitive messages. For example, this may be used for periodic data for monitoring purpose.

4.3 Reliability

The communicating devices in the power grid rely on the communication backbone in their respective domains to send and receive critical messages to maintain the grid stability. Hence, it is extremely important for the communication backbone to be reliable for successful and timely message exchanges. The communication backbone reliability is affected by a number of possible failures.

These failures include time-out failures, network failures, and resource failures. A time-out failure occurs if the time spent in detecting, assembling, delivering and taking action in response to a control message exceeds the timing requirements. A network failure occurs when there is a failure in one of the layers of the protocol suite used for communication. For example, a routing protocol failure might prevent a message from reaching its destination in spite of existence of a physical link. Noise and interference in the physical medium may also disrupt the communication. A resource failure implies failure of the end node which initiates communications or receives messages. Hence, there is a need to assess the reliability of the system in its design phase and find ways to improve it.

4.4 Security

In the future power systems, an electricity distribution network will spread over a considerably large area, e.g., tens or hundreds of miles in dimension. Hence physical and cyber security from intruders is of utmost importance. Moreover, if a wireless communication medium (like WiFi or ZigBee) is used as part of the communication network, security concerns are increased because of the shared and accessible nature of the medium. Hence, to provide security protection for the power systems, we need to identify various communication use cases (e.g., demand side management, advanced meter reading, communication between intelligent energy management (IEM) and intelligent fault management (IFM) devices, and local area communication by IEM devices) and find appropriate security solutions for each use case, for example, authorized access to the real time data and control functions, and use of encryption algorithms for wide area communications to prevent spoofing.

4.5 Time synchronization

Some of the devices on power grid need to be synchronized in time. The requirements for time synchronization of a device depend on the criticality of the application. Tolerance and resolution requirements for time synchronization are strict for IEDs that process time sensitive data. For example, phasor measurement units (PMUs) have the strictest need of time synchronization as they provide a real-time measurement of electrical quantities (voltage and current) from across an electricity grid for analysis, measurement and control [5]. Time synchronization can be obtained through a number of ways depending upon the resolution and jitter requirements. Precision time protocol (PTP) defined by the standard IEEE 1588 provides time synchronization with up to nanosecond precision over Ethernet networks. Global positioning system (GPS) and simple time network protocol (STNP) are other ways of achieving time synchronization.

4.6 Multicast support

The multicast concept is crucial for power system applications in which a message containing a given analog value, state change or command may have to be communicated to several peers at the same time [6]. Thus, instead of multiple individually addressed messages, a single multicast message is sent to a switch that forwards it to all outgoing ports. Receiving devices are simply configured to listen to a particular multicast address, thus making it possible to disregard unwanted network traffic, which is useful for IED devices to share protection related information with their peers.

5 Protocols and Standards

Many standards have been proposed to guide the development of next generation electric power systems. These standards cover a vast number of technical aspects of the power systems, including power equipment, electricity services, management automations and system protections. As the main focus in this document is the communication architecture for RePlan and its various aspects, the protocols and standards on the communication aspect of the electric power systems are presented next.

5.1 OSI Reference Model and Transport Layer Protocols

There are a number of protocols defined to handle data communication between terminals in an IP network (e.g. Internet). TCP & UDP are two of these protocols and lie in the Transport layer of the OSI reference model for communication (as discussed in WP1). Figure 6 shows different layers present in the OSI model with the sequence of arrangement and a brief functionality of each layer.

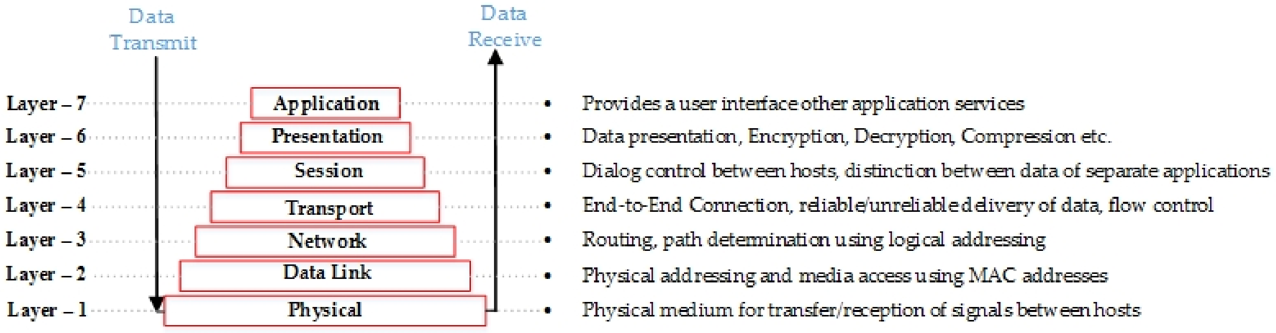

Data Transmit
Data Receive
Layer – 7
Application
Provides a user interface other application services
Layer – 6
Presentation
Data presentation, Encryption, Decryption, Compression etc.
Layer – 5
Session
Dialog control between hosts, distinction between data of separate applications
Layer – 4
Transport
End-to-End Connection, reliable/unreliable delivery of data, flow control
Layer – 3
Network
Routing, path determination using logical addressing
Layer – 2
Data Link
Physical addressing and media access using MAC addresses
Layer – 1
Physical
Physical medium for transfer/reception of signals between hosts

Figure 6 Open Systems Interconnection (OSI) Reference Model for Communication

5.2 Transmission Control Protocol (TCP)

All the layers below Transport Layer are unreliable and deliver the data (datagram) hop-by-hop. The IP layer delivers the datagram hop-by-hop and does not guarantee delivery of a datagram; It is a connectionless system. IP simply handles the routing of datagrams. If problems occur, IP discards the packet without a second thought, generating an error message back to the sender in the process. The task of ascertaining the status of the datagrams sent over a network and handling the resending of information if parts have been discarded falls to TCP. [7]

5.2.1 Communication in TCP

The communication in TCP takes place in three steps:

- Connection establishment
- Data transfer
- Connection termination

Thus, when a client wants to communicate to the server, a connection must be set up between the two devices that wish to communicate. This process, usually called connection establishment, involves an exchange of messages that switches both devices from their initial connection state (CLOSED) to the normal operating state (ESTABLISHED).

5.2.2 Connection Establishment

To establish a connection, each device must send a SYN (Synchronization) and receive an ACK (Acknowledgement) for SYN from the other device. Thus, conceptually, four control messages need to be passed between the devices. However, it's inefficient to send a SYN and an ACK in separate messages when one could communicate both simultaneously. Thus, in the normal sequence of events in connection establishment, one of the SYNs and one of the ACKs is sent together by setting both of the relevant bits (a message sometimes called a SYN+ACK). This makes a total of three messages, and for this reason the connection procedure is called a three-way handshake.

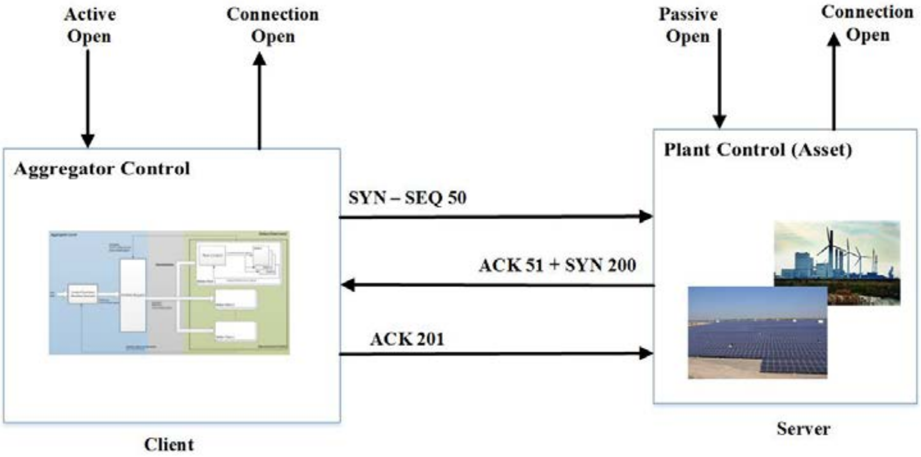


Figure 7 TCP – Connection Establishment

5.2.3 Data transfer

As soon as the connection is established, the client sends a request for the status update of the server. This transferring of request is straightforward, as shown in **Figure 8** below. For each block of data received by client's TCP, TCP encapsulates it and sends it to server with an increasing sequence number. After server receives the message, it acknowledges it with a segment acknowledgment that increments the next sequence number (and hence indicates that it received everything up to that sequence number). **Figure 8** shows the transfer of only one segment of information – one each way. In the same fashion, the server responds to the client’s request and finally receives an acknowledgement message by the client.

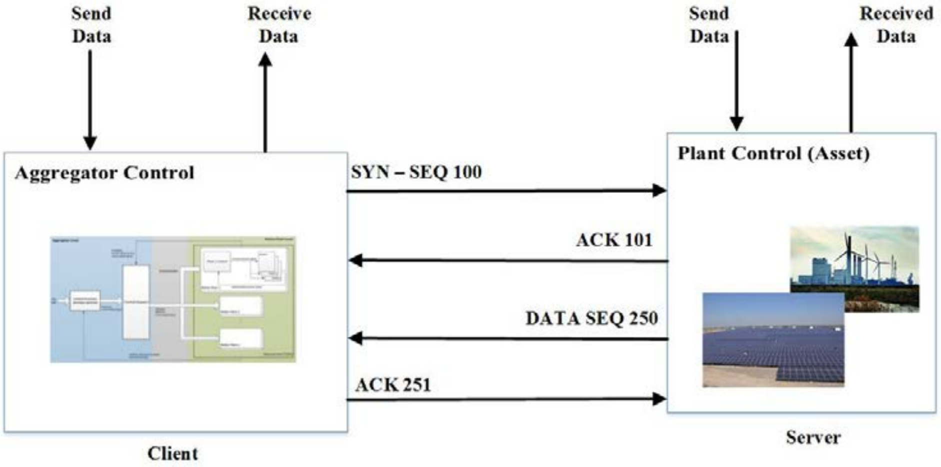


Figure 8 TCP – Data Transfer

5.2.4 Connection Termination

Now, to close a connection, client's TCP sends the request to close the connection to the server with the next sequence number. The server will then send back an acknowledgment of the request and its next sequence number. Following this, server sends the close message through its upper layer protocol to the application and waits for the application to acknowledge the closure. This step is not strictly necessary; TCP can close the connection without the application's approval, but a well-behaved system would inform the application of the change in state. After receiving approval to close the connection from the application (or after the request has timed out), server's TCP sends a segment back to the client with the FINISH (FIN flag) set. Finally, client acknowledges the closure and the connection is terminated.

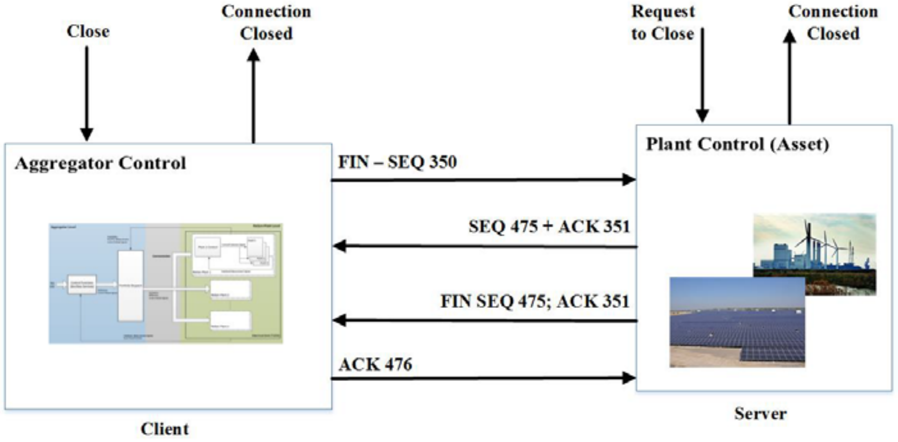


Figure 9 TCP – Connection Termination

TCP guarantees the recipient will receive the packets in order by numbering them. The recipient sends messages back to the sender saying it received the messages. If the sender doesn't get a correct response, it will resend the packets to ensure the recipient received them. Packets are also checked for errors. TCP is all about this reliability — packets sent with TCP are tracked so no data is lost or corrupted in transit.

TCP resides only on devices that actually process datagrams, ensuring that the datagram has gone from the source to target machines. It does not reside on a device that simply routes datagrams, so there is no TCP layer in a gateway (e.g. in routers). This makes sense, because on a gateway the datagram has no need to go higher in the layered model than the IP layer. This is shown in Figure 10.

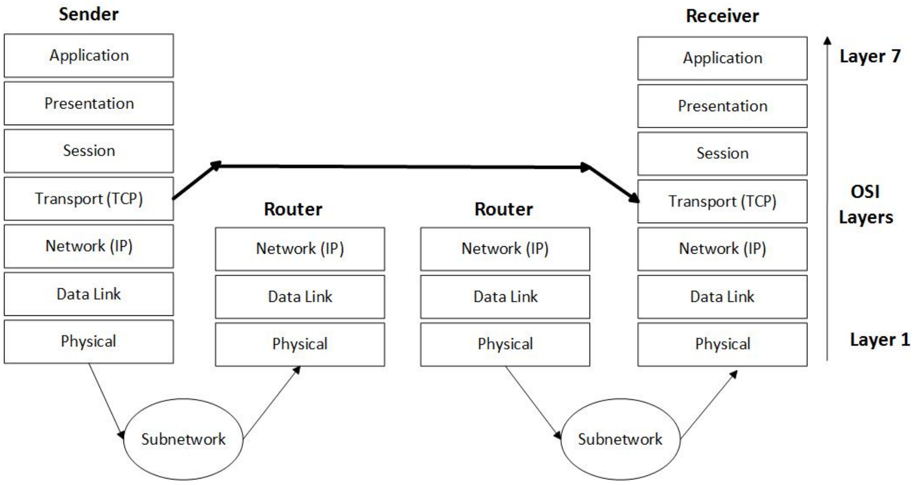


Figure 10 Reliable End to End Communication

5.2.5 Characteristics of TCP

TCP provides a communication channel between processes on each host system. The channel is reliable, full-duplex, and streaming. To achieve this functionality, the TCP drivers break up the session data stream into discrete segments, and attach a TCP header to each segment. An IP header is attached to this TCP packet, and the composite packet is then passed to the network for delivery. This TCP header has numerous fields that are used to support the intended TCP functionality. TCP has the following functional characteristics:

- **Unicast protocol:** TCP is based on a unicast network model, and supports data exchange between precisely two parties. It does not support broadcast or multicast network models.
- **Connection state:** Rather than impose a state within the network to support the connection, TCP uses synchronized state between the two endpoints. This synchronized state is set up as part of an initial connection process, so TCP can be regarded as a connection-oriented protocol. Much of the protocol design is intended to ensure that each local state transition is communicated to, and acknowledged by, the remote party.

- **Reliable:** Reliability implies that the data (stream of octets) passed to the TCP driver at one end of the connection will be transmitted across the network so that the stream is presented to the remote process as the same sequence of octets, in the same order as that generated by the sender. This implies that the protocol detects when segments of the data stream have been discarded by the network, reordered, duplicated, or corrupted. Where necessary, the sender will retransmit damaged segments so as to allow the receiver to reconstruct the original data stream. This implies that a TCP sender must maintain a local copy of all transmitted data until it receives an indication that the receiver has completed an accurate transfer of the data.
- **Full duplex:** TCP is a full-duplex protocol – it allows both parties to send and receive data within the context of the single TCP connection.
- **Streaming:** Although TCP uses a packet structure for network transmission, TCP is a true streaming protocol, and application level network operations are not transparent.
- **Rate Adaptation:** TCP is also a rate adaptive protocol, in that the rate of data transfer is intended to adapt to the prevailing load conditions within the network and adapt to the processing capacity of the receiver. There is no predetermined TCP data transfer rate – if the network and the receiver both have additional available capacity; a TCP sender will attempt to inject more data into the network to take up this available space. Conversely, if there is congestion, a TCP sender will reduce its sending rate to allow the network to recover. This adaptation function attempts to achieve the highest possible data transfer rate without triggering consistent data loss.

5.3 User Datagram Protocol (UDP)

5.3.1 Background and functionality

Unlike TCP, UDP doesn't establish a connection before sending data, it just sends. Because of this, UDP is called "Connectionless". UDP packets are often called "Datagrams". An example of UDP in action is the DNS service. DNS servers send and receive DNS requests using UDP. This protocol is similar to TCP that is used in client/server programs like video conference systems expect UDP is connection less and does not support acknowledgements, as shown in Figure 11.

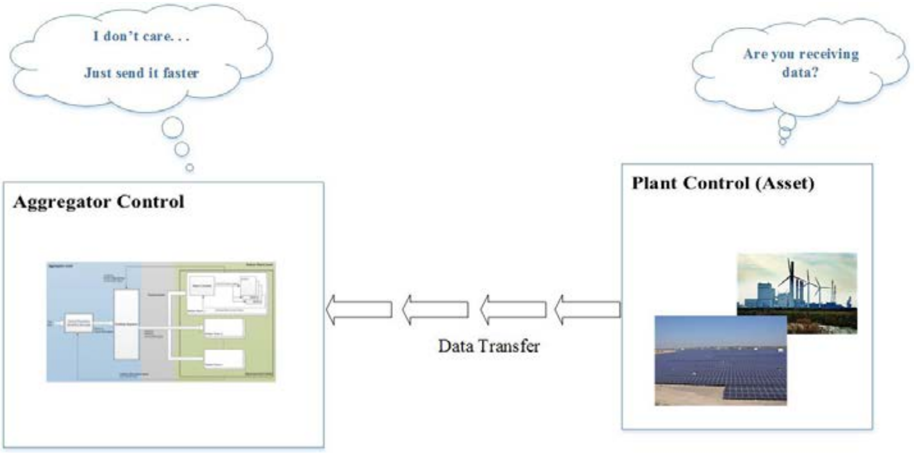


Figure 11 Data transfer with NO Acknowledgements

UDP is a connectionless and unreliable transport protocol. The two ports serve to identify the end points within the source and destination machines. User Datagram Protocol is used, in place of TCP, when a reliable delivery is not required. However, UDP is never used to send important data such as web-pages, database information, etc. Streaming media such as video, audio and others use UDP because it offers speed.

5.3.2 Why UDP is faster than TCP?

The reason UDP is faster than TCP is because there is no form of flow control. No error checking, error correction, or acknowledgment is done by UDP. UDP is only concerned with speed. So when, the data sent over the Internet is affected by collisions, and errors will be present.

5.3.3 Communication in UDP

In UDP connection, client set unique source port number based on the program they started connection. UDP is not limited to 1-to-1 interaction. A 1-to-many interaction can be provided using broadcast or multi-cast addressing. A many-to-1 interaction can be provided by many clients communicating with a single server. A many-to-many interaction is just an extension of these techniques.

5.3.4 Characteristics of UDP

The characteristics of UDP are:

- End-to-end. UDP can identify a specific process running on a computer.
- Unreliable, connectionless delivery (e.g. USPS)
- UDP uses a connectionless communication setup. In this, UDP does not need to establish a connection before sending data. Communication consists only of the data segments themselves.
- Same best effort semantics as IP
- No ACK messages, no sequence, no flow control
- Subject to loss, duplication, delay, out-of-order, or loss of connection
- Fast, low overhead
- Suit for reliable, local network
- RTP (Real-Time Transport Protocol)

5.4 Comparison between TCP and UDP

The User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) are the “siblings” of the Transport layer in the TCP/IP protocol suite. They perform the same role, providing an interface between applications and the data-moving capabilities of the Internet Protocol (IP), but they do it in very different ways. The two protocols thus provide choice to higher-layer protocols, allowing each to select the appropriate one depending on its needs.

Table 2 helps illustrate the most important basic attributes of both protocols and how they contrast with each other:

Table 2 Comparison of UDP and TCP

UDP Vs. TCP		
Characteristics/ Description	**UDP**	**TCP**
General Description	Simple High speed low functionality “wrapper” that interface applications to the network layer and does little else	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues
Protocol Connection Setup	Connection-less data is sent without setup	Connection-oriented, Connection must be established prior to transmission
Data Interface to application	Message is sent in discrete packages by the application	Stream-based; data is sent by the application with no particular structure
Reliability and acknowledgements	Unreliable best-effort delivery without acknowledgements	Reliable delivery of message all data is acknowledged
Retransmissions	Not performed. Application must detect lost data and retransmit if needed	Delivery of all data is managed, and lost data is retransmitted automatically
Features Provided to manage flow of data	None	Flow control using sliding windows; window size adjustment heuristics; congestion avoidance algorithms
Overhead	Very Low	Low, but higher than UDP
Transmission Speed	Very High	High but not as high as UDP
Data Quantity Suitability	Small to moderate amounts of data	Small to very large amount of data

5.5 Distributed Network Protocol (DNP)

The distributed network protocol (DNP) is a US based protocol that first appeared in 1998, which went through a number of revisions to become the current version (DNP3) [8]. Since protocols define the rules by which devices talk with each other, DNP3 is a protocol for transmission of data from point A to point B using serial communications. It has been used primarily by utilities like the electric companies, but it operates suitably in other areas.

The DNP3 is specifically developed for inter-device communication involving SCADA RTUs, and provides for both RTU-to-IED and master-to-RTU/IED. It is based on the three-layer enhanced performance architecture (EPA) model (see Figure 12) contained in the IEC 60870-5 standards [9], with some alterations to meet additional requirements of a variety of users in the electric utility industry.

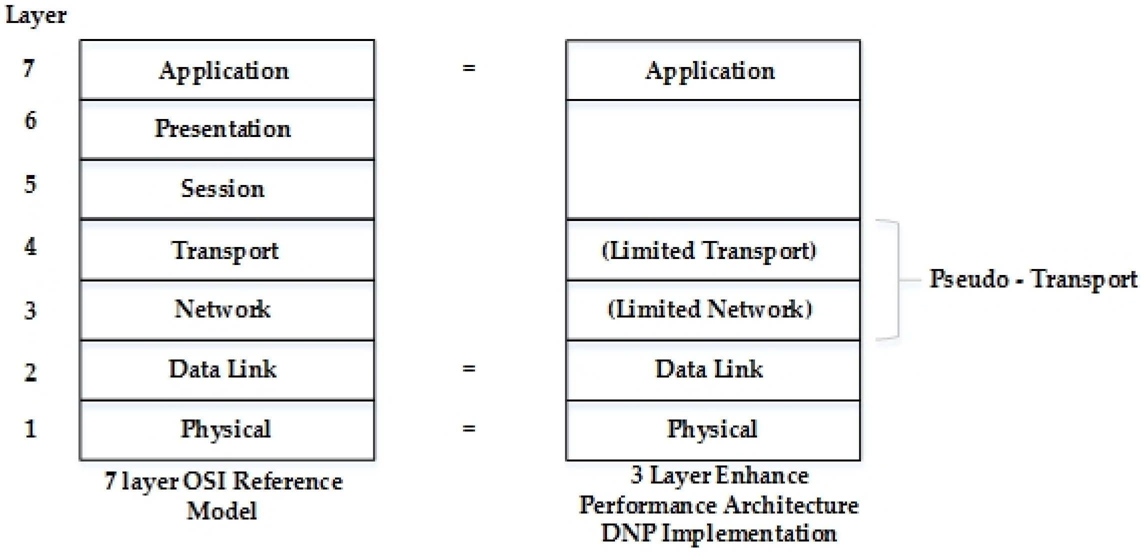


Figure 12 OSI 7 layer model versus EPA model [9]

5.6 IEEE standards

IEEE has proposed a number of standards related to the communications in power systems, including C37.1, 1379, 1547, and 1646.

5.6.1 IEEE C37.1

The IEEE standard C37.1 [10] describes the functional requirements of IEEE on SCADA and automation systems.

This standard provides the basis for the definition, specification, performance analysis and application of SCADA and automation systems in electric substations. It defines the system architectures and functions in a substation including protocol selections, human machine interfaces and implementation issues. It also specifies the network performance requirements on reliability, maintainability, availability, security, expandability and changeability.

5.6.2 IEEE 1379

The IEEE document 1379 [10] recommends implementation guidelines and practices for communications and interoperations of IEDs and RTUs in an electric substation. It provides examples of communication support in substations by using existing protocols. Particularly, it describes the communication protocol stack mapping of the substation network to DNP3 and IEC 60870-5. Processes are also discussed to expand the data elements and objects used in substation communications to improve the network functionalities.

5.6.3 IEEE 1547

The IEEE standard 1547 defines and specifies the electric power system that interconnects distributed resources. It consists of three parts: the electric power system [11], the information exchange [12], and the compliance test [13]. In the power system part, the standard specifies the requirements on different power conversion technologies and the requirements on their interconnection to provide quality electricity services. General guidelines are described to ensure power quality, respond to power system abnormal conditions, and form subsystem islands. The information exchange part specifies the requirements on power system monitoring and control through data networks. Important network aspects are described, including interoperability, performance and extensibility. Protocol and security issues are also considered in the standard. The conformance test part provides the procedures to verify the compliance of an interconnection system to the standard. As an electric power system is complicated in components and functions, the standard describes a variety of tests to guarantee an implemented system to work as expected.

5.6.4 IEEE 1646

The IEEE standard 1646 [5] specifies the requirements on communication delivery times within and external to an electric substation. Given the diversity of communication types, the standard classifies substation communications into different categories and defines the communication delay requirement for each category. For example, system protection messages are required to be transmitted within 4 ms and operation maintenance messages within 1s. Furthermore, it defines the communication delay as the time spent in the network between the applications running at the two end systems. Therefore, the packet processing time should also be considered into the delay such that the combination of processing and transmission times does not exceed the required delay bound. Since delays are introduced in both the end system processing phase and the network transmission phase, the standard discusses further on the system and communication capabilities required to deliver information on time, including for example real-time support, message priority, data criticality, and system interfaces.

5.7 NIST Standards

The National Institute of Standards and Technology (NIST) has also published standards to provide guidance to the smart grid construction. The NIST Special Publication 1108 [14] describes a roadmap for the standards on smart grid interoperability. It states the importance and vision of the smart grid, defines the conceptual reference model, identifies the implementation standards, suggests the priority action plans, and specifies the security assessment procedures. In particular, it presents the expected functions and services in the smart grid as well as the application and requirement of communication networks in the implementation of smart grid. The NIST report 7628 particularly [15] focuses on the information security issues of the smart grid. It explains the critical security challenges in the smart grid, presents the security architectures, and specifies the security requirements. Security objectives and strategies are discussed, including cryptography, key management, privacy and vulnerability analysis. The report 7628 aims to ensure trustable and reliable communications for the automated energy management in the smart grid.

5.8 IEC Standards

The International Electrotechnical Commission (IEC) has proposed a number of standards on the communication and control of electric power systems that are mostly used Europe. The standard 60870 [16] defines the communication systems used for power system control. Through the standard, electric equipment can interoperate to achieve automated management. The standard 60870 contains six parts, which specify the general requirements on the power system interoperability and performance. The standard 61850 [17] focuses on the substation automated control. It defines comprehensive system management functions and communication requirements to facilitate substation management. The management perspectives include the system availability, reliability, maintainability, security, integrity and general environmental conditions. The standards 61968 [18] and 61970 [19] provide common information model for data exchange between devices and networks in the power distribution domain and the power transmission domain respectively. Cyber security of the IEC protocols is addressed in the standard 62351 [20], which specifies the requirements to achieve different security objectives including data authentication, data confidentiality, access control and intrusion detection.

5.8.1 IEC 61850

Substation automation refers to the monitoring, protection and control functions performed on substation and feeder equipment. In the substation automation domain, the IEC 61850 and DNP3/IEE1815 are the most widely adopted protocols [21] [22]. While the DNP3 (Distributed Network Protocol, version 3) standard only provides communication specifications for low-bandwidth monitoring and control operations, the IEC 61850 standard covers almost all aspects of SAS including real-time, high bandwidth protection and control applications. Therefore, IEC 61850 is gradually becoming the dominant protocol in this field.

5.8.1.1 Overview of the IEC 61850 standard

The IEC 61850 standard is based on interoperable Intelligent Electronic Devices (IEDs) that interacts with each other, either within a substation (e.g. protection signals to circuit breakers) or on feeders (e.g. automated reclosers and switches along a feeder responding to isolate a fault). Although IEDs of several types and functionalities are defined in the IEC 61850 standard, the most common types include the breaker/switch IED, Merging Unit (MU) IED, and protection and control (P&C) IED [23]. The P&C IED is responsible for supervising the protection and control operations of its serving bay unit. The breaker/switch IED continuously monitors the state and conditions of the corresponding switchgears/circuit breakers, send status information to the P&C IEDs and receives trip/close command from the P&C IEDs. The MU IED collects the analog voltage and current signals from field CT and PT, converts them into digital format and then transmits to the P&C IEDs in the form of sampled analog values (SMVs).

The IEC 61850 communication architecture is comprised of three hierarchical levels – station, bay and process as shown in Figure 13. The process level includes various switchyard equipment such as

CT/PT, I/O devices, sensors and actuators. Bay level P&C IEDs and the station level contains the Human to Machine Interface (HMI) devices, station controller computers, etc. The standard defines two separate Ethernet subnetworks (called 'Buses') to facilitate QoS implementations. While the process bus handles the delay sensitive communication between P&C IEDs and switchyard devices such as breaker and switch IEDs, the station bus handles communication among different bay and with the station controller as well as communication with the external networks.

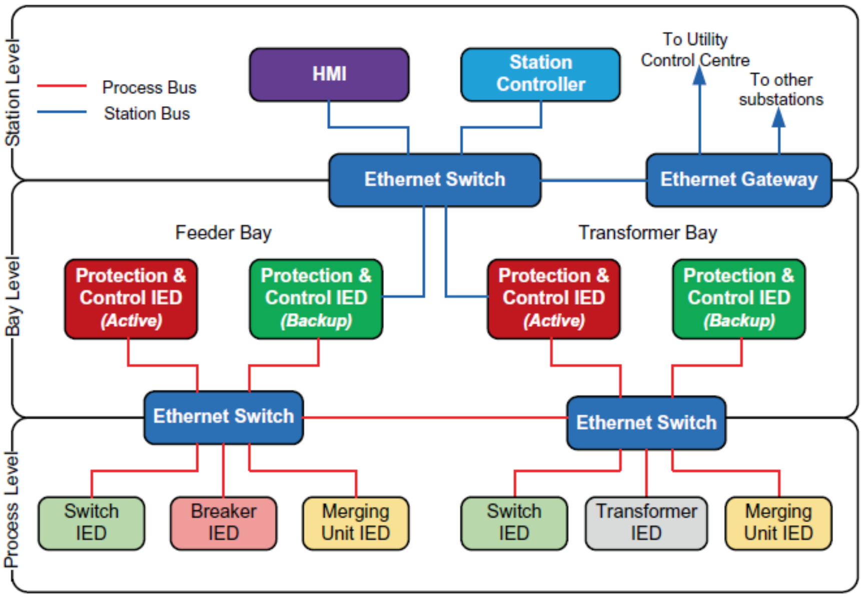


Figure 13 Architecture of an IEC 61850 based substation automation system. [24]

5.8.1.2 *IEC 61850 communication services and application types*

The IEC 61850 protocol is designed to run over standard communication networks based on the Ethernet and the IP standards. To differentiate among various applications and to prioritize their traffic flows, the standard defines five types of communication services:

1. Abstract Communication Service Interface (ACSI)
2. Generic Object Oriented Substation Event (GOOSE)
3. Manufacturing Message Specification (MMS)
4. Generic Substation Status Event (GSSE)
5. Sampled Measured Value multicast (SMV)
6. Time Synchronization (TS)

The ACSI services include querying device status, setting parameters and reporting and logging. All ACSI services are requested by the clients and responded by servers. The message exchange inside an ACSI application is similar to that of a FTP session where the application starts with a mutual handshaking followed by data exchange and connection termination.

GOOSE and GSSE services, together often called as Generic Substation Events (GSEs), are used to exchange event and status information (e.g., a binary change of state or an analog value crossing the reporting threshold) in real-time. While the GOOSE message may include several data types like analog, binary, and integer values, the GSSE message is limited to support only a fixed structure of binary event status data. The GOOSE messages use multicast services that allow simultaneous delivery of the same message to multiple IEDs. The IEC 61850 standard also specifies a retransmission scheme to achieve a highly dependable level of GOOSE message delivery [25]. The messages are sent immediately at the time of an event and then repeated with an increasing time interval from T_{min} to T_{max} as shown in Figure 14. The retransmission time gradually increases from T_{min} and eventually settles at T_{max}. The repetition with T_{max} continues forever, until a new event occurs and the repetition rate starts again with T_{min} [26]. Each message contains a TTL field after which the message is discarded by the receiver.

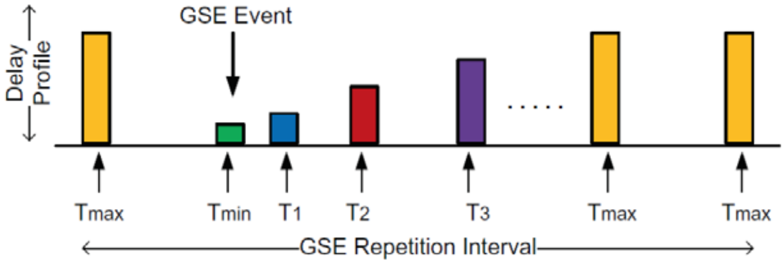


Figure 14 Repetition pattern of GSE Messages [24]

The SMV services are used to transfer sampled analog signals and status information from the MU IEDs via the process bus. The TS service is used to broadcast the system clock information to the IEDs to ensure measurement accuracy. The two most popular methods for time synchronization in SAS include the GPS and the IEEE 1588 Precision Time Protocol (PTP).

Since the raw data samples and GOOSE messages are time critical, they are directly mapped to the low-level Ethernet layer to reduce protocol overhead. The GSSE message uses its own protocol mapping called the GSSE T-profile. The TS service use broadcast communication using the UDP/IP transport layer. The rest of the ACSI services use the typical TCP/IP transport layer. The communication stacks mapping of the IEC 61850 services with the OSI (Open Systems Interconnect) layer is shown in Figure 15

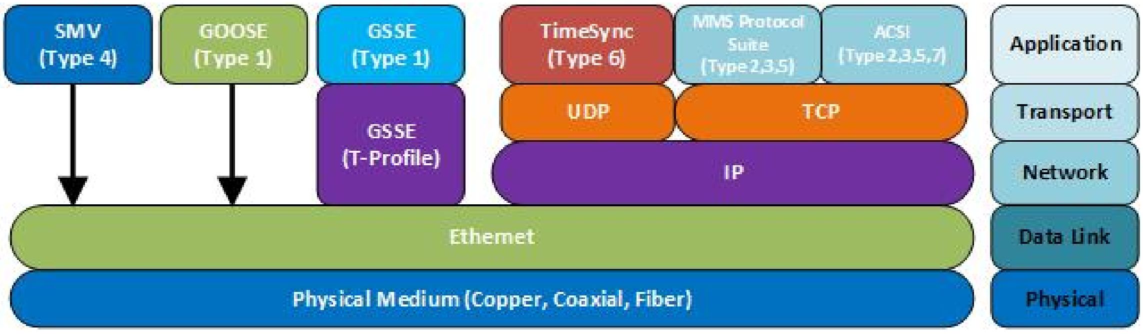


Figure 15 Communication stack mapping for the IEC 61850 messages [24]

5.8.1.3 Manufacturing Message Specification (MMS) [27]

MMS is an international application-layer protocol for exchanging or transferring information among real devices such as IEDs and the computer applications [28]. MMS plays an important role in mapping the services of abstract communication service interface (ACSI) models of IEC61850 to the lower level and vice versa so that all the IEDs respond in the same fashion from the network point of view. This is because services provided by ACSI in IEC 68150-7-2 cannot be used directly to make communication with another device over a network. Therefore, the objective of MMS is to specify how physical devices will operate when the messages are received to make the communication between the devices vendor independent. For example, services provided by MMS enable the MMS-compliant device to read the variables from different MMS-compliant devices because the MMS services (e.g., read, write) and messages exchanged are identical [29].

Using a range of services, MMS provides the ability to define and explore the functionalities and capabilities of IEDs for exchanging data between the intelligent devices and other utility applications. This can be better understood by a practical example by considering an analogy between MMS and telephone communication. For instance, a caller speaking in “French” language is assumed as an “MMS client” who wants to communicate with an international receiver in the China. The communication between the French caller and the China receiver is possible only if both understand a common language, French or Chinese. If not, then one of them has to use a local language translator, which is equivalent to a virtual manufacturing device (VMD) to ensure the correct delivery of messages between them. Therefore, VMD plays the role of language translator that provides an abstraction layer to hide the internal functionalities of real physical devices from the external environment. The main objective of VMD is to define the following three things:

- **Objects:** MMS objects are the variables defined in the server device (IED). These objects provide capabilities for accessing operational, control, and other parameters defined in a physical IED. In short, MMS objects enable the client application to see what is happening inside the IED.
- **Services:** Client device or application uses various MMS services such as Read, Write, Start, Stop, and so on to manipulate the objects or to obtain the status information of the objects defined in the physical IED.
- **Behavior:** When the client device sends a service request for an object to the server, the way the server responds upon receiving the service request is called behavior.

For exchanging the information between the IEC61850-compliant devices and applications, a client/server scheme is used in MMS for non-time-critical applications, which is a connection-oriented protocol. With the client/server scheme, a client application can perform read/write operations with an IEC61850 IED only after establishing a connection with the IED. Some of the advantages gained by connection-oriented protocol are as follows:

- It provides an acknowledgment message upon exchanging the information successfully,
- Because of the acknowledgment message, read/write/start/stop and other services are more reliable,

- It supports encoding and decoding of information from security point of view.

Moreover, the standard classifies application message types based on the delay requirements of the above six services.

Table 3 lists the IEC 61850 message types and their transfer time requirements.

Table 3 IEC 61850 message types and transfer time requirements [1]

Message Type	Application	Services	Transfer Time Requirement (ms)
1A	Fast Message Trip	GOOSE, GSSE	3-100
1B	Fast Message (other)		20-100
2	Medium Speed	ACSI	100
3	Low Speed		500
4	Raw Data	SMV	3-10
5	File Transfer	ACSI	>1000
6	Time Synchronization	TS	Accuracy
7		MMS	100

5.8.1.4 *Communication Requirements*

The IEC 61850 standard specifies the structure for application protocol data unit (APDU). Each APDU consists of one or more application protocol data unit (ASDU) with 6 bytes of header for each ASDU. The ASDU contains the data set (e.g., sampled values, status indication, ACSI data objects, etc.) based on their associated service types [30].

In order to calculate the communication traffic of a substation automation system, at first we need to identify the corresponding IEDs by examining the single line diagram of the substation. For example, let us consider the case of a small distribution substation whose single line diagram is given in Figure 16.

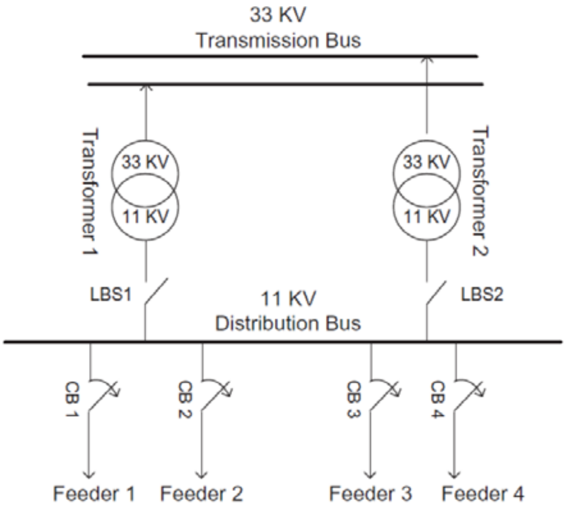


Figure 16 Small Distribution Substation – Single Line Diagram [24]

From the single line diagram, we can see that the substation has two transformer bays and four feeder bays. Each transformer bay contains a Load Break Switch (LBS) and each feeder bay contains a Circuit Breaker (CB). Thus, the total SAS should at least have six MU IEDs (for 6 bays), twelve P&C IEDs (1 + 1 redundancy) assuming that the LBS and CB communicates via their respective MU IEDs. To calculate the traffic load for different SAS applications, we assume the following parameters:

- **Sampled Data.** Each APDU generated by the MU IED of the transformer bay contains two ASDUs as it contains two data sets of voltage and current and the feeder bay contains only a single ASDU. Each data set consists of 8 sampled values (8 bytes each) and other status information adding up 32 bytes. Thus the total ASDU size is 96 bytes for this case [References]. Using the APDU structure in [References], the APDU size for sampled data in the transformer MU IED is 198 bytes (2 ASDUs with 2*6 bytes of header) and for feeder MU IED yields 102 bytes (1 ASDU with 6 bytes of header).
- **Protection and Control.** APDU size for Type-1 message (trip signal) is 50 bytes, Type-2 message (interlocking) is 150 bytes and Type-3 message (e.g., status indication, control, etc.) is 200 bytes [30].
- **File Transfer.** A 1 Mb file is transferred from each IEDs to the station controller in every 1h.

Protection and control of 1440 Hz for analog data, 250 Hz for medium speed messages and 10 Hz for low speed messages according to [31], the traffic load of each individual application is listed in Table 4.

Table 4 Types of traffic for the substation automation system in Figure 16. [24]

Application	Message	IED Type	Total IEDs	Packet Size (Bytes)	Sampling Rate (Hz)	Data Rate (Kbps)
Protection	1	P&C	6	50	1	2.34
Sampled Data	4	MU (trans.)	2	198	1440	4455.00
		MU (feeder)	4	102	1440	4590.00
Interlocks	2	P&C, MU	12	150	250	3515.63
Control	3	P&C, MU	12	200	10	187.50
File Transfer	5	MU	12	1 Mb	1/h	3.41
Total Traffic Volume						12.75 Mbps

The substation automation applications are strictly delay sensitive since they act as the triggering points for the underlying protection and control systems. Many of the time critical messages in substation automation applications contain a Time-To-Live (TTL) fields which implies that the message will lose its relevance if not delivered within the specified time. For example, the trip/close commands need to be delivered to the respective IEDs within 1/4th cycle time (4 ms for 60 Hz system, 5 ms for 50 Hz system) to perform the required actions. Hence, the IEC 61850 standard defines strict transfer time requirements for the SAS applications as listed in Table 4.

It is envisaged that in the future smart grid, the domain of substation automation functions will be extended out of the generation and transmission substations to the entire distribution grid [32]**. Since the distribution side of the grid covers a vast geographic area, it will be covered by several communication technologies which require the IEC 61850 messages to traverse through both wired and wireless links. Hence, end-to-end QoS guarantee in terms of latency and reliability are the key communication requirements here.**

6 Performance Definitions and Classifications

Timing is critical in smart grid communications, which is the most fundamental difference from other communication networks. Some types of information exchanges between electric devices is useful only within a predefined time frame. If the communication delay exceeds the required time window, the information does not serve its purpose anymore and, in the worst case, damage might be incurred in the grid. For example, in the common practice for power device protection, the circuit breaker must be opened immediately if the voltage or current on a power device exceeds the normal values. Such protection actions must be made within a time window as small as 3ms in order to be effective. In fact, IEEE and the International Electrotechnical Commission (IEC) have defined rigorous communication delay requirements in smart grid for different types of information exchanges. When we design and implement the communication infrastructure in the grid, these timing requirements must be satisfied. Obviously, overhead from communication protocols and technological physical performance and characteristics impacts the performance, but also the load of the network and computational resources at all entities involved in the communication (that is from A to B via all routers, access points, mobile masts etc.) all has an influence on the end to end performance which definitions and classifications must consider.

6.1 Delay Definitions

The communication delay in smart grid is defined as the time lapse between the sending of a message at the source IED and the receiving of message at the destination IED. It is measured end-to-end between the two applications running at the source and destination systems. An illustration of the delay definition is shown in Figure 17. As observed in the figure, the end-to-end delay is the sum of all the time pieces spent by the message during its processing and transmission at every traversed node: the source IED incurs some delay to format the message for transmission, each intermediate forwarding node adds in extra delay to process and relay the message, and the destination IED spends additional time to decode the message and present it to the application program.

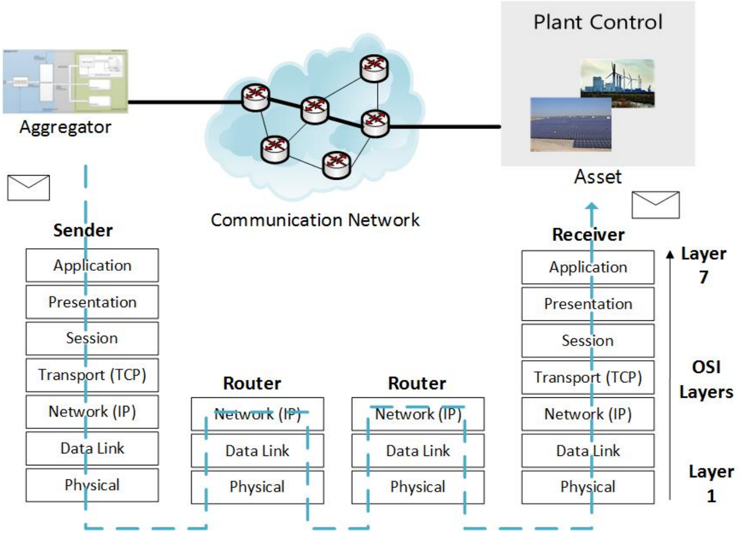


Figure 17 End-to-End Communication

As the electric power devices do not have communication capability by themselves, each electric device is attached with an embedded computer system to serve as the communication interface to the network infrastructure. The electric device and the embedded computer system together form an IED. The message processing steps within an IED are illustrated in Figure 18, in which a message containing the device status data is generated and transmitted through four modules in the IED: (i) the analog–digital converter transforms a status measurement into digital data, (ii) the CPU processes the measurement data, (iii) the setpoint structure stores the current measurement data, and (iv) the network protocol stack formats the message and sends it into the network. The time spent within an IED is part of the end-to-end delay as described in Figure 17 (above).

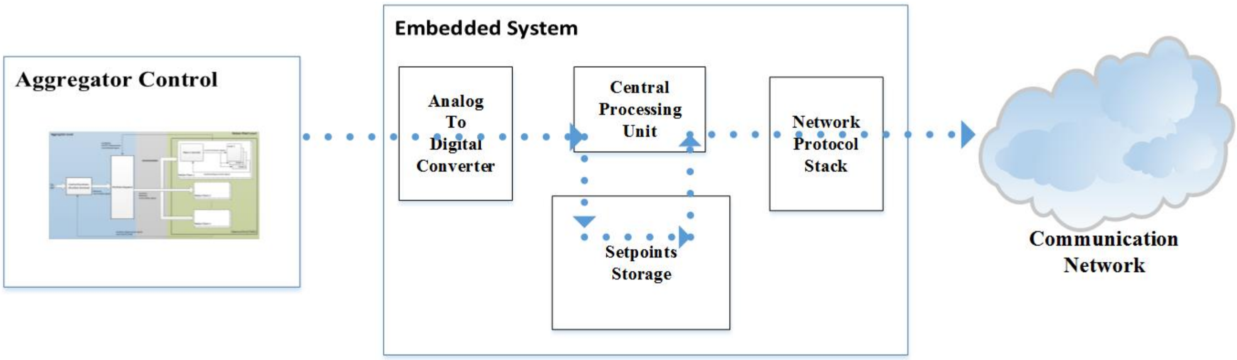


Figure 18 Processing time spend in IED device

6.1.1 Timing Classifications

IEEE classifies the message exchange events in power systems into several categories and requires the delays experienced in the communication networks be strictly less than these guideline values [5]. We summarize these delay categories in Table 5. Similarly, IEC has also specified the expected communication delays in different information categories [33], which we summarize in Table 6.

Table 5 IEEE 1646 Standard: Communication timing requirements for electrical automation [1]

Information Types	Internal to Substation	External to Substation (For RePlan)
Protection Information	4ms (1/4 cycle of electrical wave)	8 – 12ms
Monitoring and Control Information	16ms	1 s
Operation and Maintenance Information	1 s	10 s
Text Strings	2 s	10 s
Processed Data files	10 s	30 s
Program Files	1 min.	10 min.
Image Files	10 s	1 min.
Audio and Video data streams	1 s	1 s

Table 6 IEC 61850 Communication Network and systems in Substations: Communication requirements for function and device model [1]

Message Types	Definitions	Delay Requirements
Type 1	Messages requiring immediate actions at receiving IEDs	1A: 3ms or 10ms; 1B 20ms or 100ms
Type 2	Messages requiring medium transmission speed	100ms
Type 3	Messages for slow speed auto-control functions	500ms
Type 4	Continuous data streams from IEDs	3ms or 10ms
Type 5	Large file transfer	1000ms (not strict)
Type 6	Time synchronization messages	No Requirements
Type 7	Command messages with access control	Equivalent to Type 1 or Type 3.

It can be observed in Table 5 and Table 6 that the communication networks to be used in the smart grid are responsible for delivering a diversity of messages used in substation automations and some of them have critical delay requirements. The most time urgent messages are related to the most important system protection functions and require a delivery delay as small as 3 ms, which is measured round trip from the IED to the control station for problem alarming and back to the IED for emergency responding, as shown in Figure 19. It is paramount to guarantee the timely and reliable delivery of these messages within the specified delay windows. Note that these delay demanding messages are usually transmitted on the shared networks together with other less time critical but possibly rate intensive messages, so it remains a challenging research problem to guarantee the satisfactory delay performances of time critical messages.

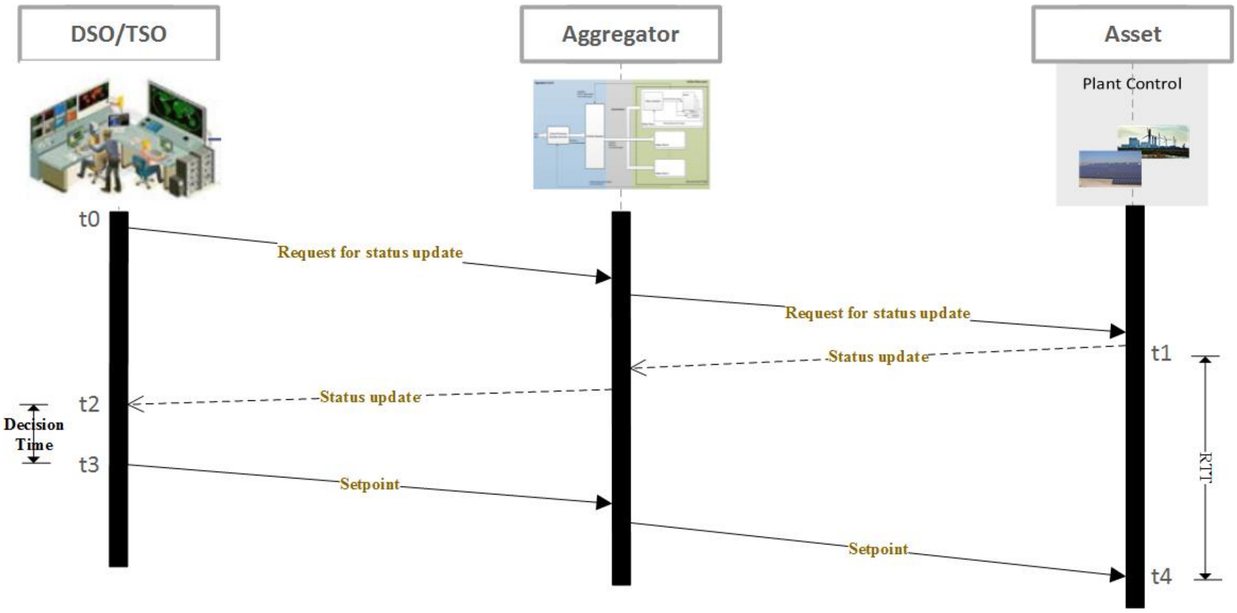


Figure 19 Urgent Message Delivery – Sequence Diagram

6.1.2 Latency

According to the Queuing theory, the busier a link gets, the longer packets have to wait. For instance, a 10 Gbps link running at 8 Gbps (80% utilization) means that on average, when a packet arrives, there are four others already waiting. At 99% utilization, this queue grows to 99 packets. Previously, when links were much slower, this could add a good amount of extra latency, but at 10 Gbps, transmitting 99 packets of an average 500 bytes is just a 0.248 milliseconds. Therefore, buffering in routers these days in the core of the network does not add a meaningful amount of delay unless links are massively oversubscribed i.e. 99.9% utilization or higher.

TCP uses a “slow start” mechanism to make sure it does not overwhelm the network. For a long transfer, the slow start portion is only a fraction of the total time, but for short transfers, by the time TCP gets up to speed, the transfer is already over. Since TCP has to wait for acknowledgments from the receiver, more latency means more time spent in slow start. Applications written by software developers with less networking experience may use simple “*open-transfer-close-open-transfer-close*” sequences that works well on low latency networks but slows down a lot over larger distances (or on bandwidth-limited networks, which also introduce additional latency).

For the reason of UDP and TCP the definition of delays is slightly different:

UDP delay is basically just attaching two port numbers to an IP packet, and thus the delay can be defined by delay at the network level (layer 3 delay), while for TCP it is a bit more complicated due to the – transmissions and acknowledge schemes, and thus can only effectively be defined at the transport layer as a function of network level delays. In any case the delay is defined by the start of the data transmission until the data has been received such that:

$$Delay := t_{receive} - t_{transmit}$$

In general, for TCP the Delay is a function of data size, packet loss probability and the end-to-end network conditions, whereas Delay for UDP is a function of only the end-to-end network conditions as long messages can fit inside on IP packet (i.e. less than or equal to 1600 bytes).

6.1.3 Jitter

It is the variation in the delay of received packets, which are sent in a continuous and evenly-spaced stream, as depicted in Figure 20. Network congestion, configuration errors or other problems with a system like improper queueing can cause jitter.

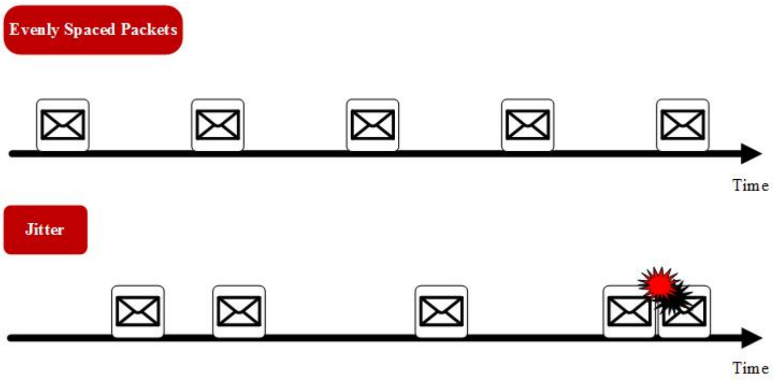


Figure 20 Jitter

Latency is typically caused by buffering of packets in routers and switches terminating highly utilized links. Sometimes a packet is lucky to get through fast, while sometimes the queue is longer than usual. For TCP, this is not a huge problem, although this means that TCP has to use a conservative value for its RTT estimate and timeouts will take longer. However, for (non-TCP) real-time traffic (e.g. audio and video), jitter is very problematic, because the real time information signals have to be received at a steady rate. Meaning, thereby, the application either has to buffer the "fast" packets and wait for the slow ones – which can add user-perceptible delay – or the slow packets have to be considered lost – causing packet-loss.

In conclusion, in networks that use multiple connections to the internet, it can really pay off to avoid paths that are much longer and thus incur a higher latency than alternative paths to the same destination, as well as congested paths with elevated packet loss.

Jitter can be expressed on an individual packet/message basis

$$Jitter := |Delay - avg(Delay)\ |$$

or by a statistical average

$$Jitter := \frac{1}{N}\sum_{i=1}^{N} |Delay_i - avg(Delay)|$$

But can also be defined in other ways for periodic updates, as the difference in periodicity as influenced by delays.

6.2 Packet Loss

Ideally, a network would never lose a single packet. However, in reality packets do get lost with some probability given as:

$$\boldsymbol{Packet\ loss := Pr(packet\ is\ dropped) = Pr(Delay = \infty)}$$

This loss of packets occurs due to the following two reasons:

Every transmission medium flips a bit once in a while, and then the whole packet is lost. If such an error occurs, the lost packet needs to be retransmitted. This can hold up a transfer. For instance, suppose we need to send data at a rate of 1000 packets per second on a 200 ms RTT connection. This means when the sender sends packet 500, packets 401 – 499 are still in flight, and the receiver has just sent an acknowledgment for packet 400. However, acknowledgments 301 – 399 are in flight in the other direction, so the latest acknowledgment the sender has seen is 300. So if packet 500 is lost, the sender won't notice until it sees acknowledgment 499 being followed by 501. By that time, it's transmitting packet 700. So the receiver will see packets 499, 501 – 700, 500, and then 701 and onward. This means that the receiver must buffer packets 501 – 700 while it waits for 500. (Remember, TCP delivers all data in the correct order)

Usually the above is not a problem. But if network latency or packet loss get too high, TCP will run out of buffer space and the transfer has to stop until the retransmitted lost packet has been received. In other words, high latency or high loss is not great – i.e. workable – but high latency together with high loss can slow down TCP to a crawl.

The second reason packets get lost is because TCP is sending so fast that router/switch buffers fill up faster than packets can be transmitted. When a buffer is full and another packet comes in, the router or switch can only do one thing: "drop" the packet. Because TCP cannot tell the difference between a packet lost because of a flipped bit or because of overflowing buffers in the network, it assumes the latter and slows down. In the above example, this slowdown is not too severe, as subsequent packets are continuously being acknowledged. This allows TCP to use "fast retransmit".

However, fast retransmit doesn't work if one of the last three packets in a transfer gets lost. In that situation, TCP cannot tell the difference between a single lost packet or the situation where the network is massively overloaded and nothing gets through. So now TCP will let its timeout timer count down to zero, which often takes a second, and then tries to get everything go again – in slow start mode.

6.3 Mismatch Probability

Lately, another metric has been included as often networks are used to transport dynamic data elements, the network delay and access method impacts the probability that information has changed. Therefore, an application layer metric, Mismatch Probability [34] was introduced in 2010, and following that worked on and analyzed for different purposes. The basic definition is therefore considering two communicating entities A and B:

$$mmPr := \Pr(Information\ at\ A\ \neq Information\ at\ B)$$

This can be observed in Figure 21.

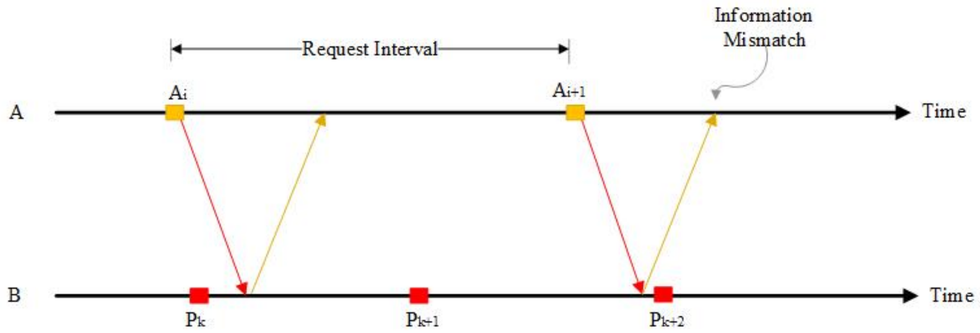
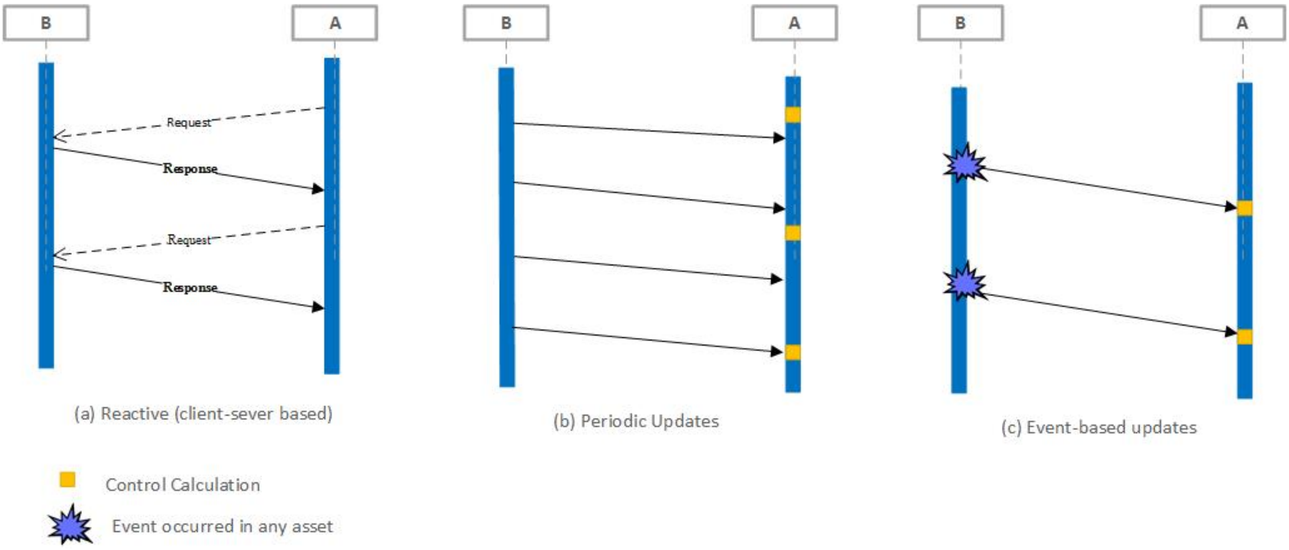


Figure 21 Mismatch Scenario

This metric is influenced by not only the end-to-end delay and information dynamics, but also for what access strategy is taken, which can abstractly be one of the following:

a) **Reactive:** A sends request to B to obtain information and gets the responding value, as shown in Figure 22(a). Potentially this can be cached which improves network traffic and access delay at the cost of increased mismatch probability.
b) **Proactive, Periodic:** B sends a message to A with an update periodically, as shown in Figure 22(b). The time period is strongly influencing the mismatch probability as well as the network traffic created.
c) **Proactive, Event Driven:** B sends a message to A with an update on certain pre-defined events Figure 22(c). The definition of the event is critical to the mismatch probability and the created network traffic.



(a) Reactive (client-sever based)

(b) Periodic Updates

(c) Event-based updates

Figure 22 Information Access Strategies. (a) Reactive (b) Proactive, Periodic (c) Proactive, Event Driven

The concepts provided in above discussion are added in the communication module developed for RePlan, as shown in Figure 23. This module will be helpful in optimizing the network requirement for RePlan once we get some specific input message types to be sent by the controller.

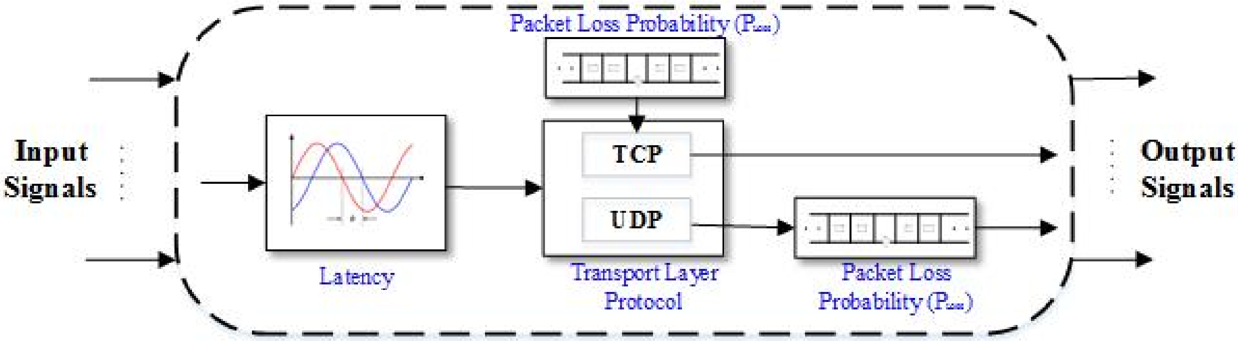

Packet Loss Probability (P_{loss})
Input Signals
Latency
TCP
UDP
Transport Layer Protocol
Packet Loss Probability (P_{loss})
Output Signals

Figure 23 Communication Module for RePlan – Block Diagram

6.4 Evaluating Enforcement Capabilities [1]

Under certain power system situations that affect massive number of devices, a large number of time critical messages may be generated, all with high delivery priority. It is necessary to understand the network capabilities in meeting the delay requirements of multiple simultaneous time urgent messages. Specifically, the research challenges exist in two perspectives.

- **Maximal Delivery Support**. When multiple time critical messages require simultaneous transportation and delivery, the available network processing and transmission resources should be carefully assessed and allocated such that maximal network support is provided to accommodate the delay expectation of each individual message. For example, if there exist multiple disjoint paths that can be used, the messages may be distributed over different paths to speed up their transmissions.
- **Support Capability Determination**. Given the limitation of network resources, such as the relay node processing speed and the link bandwidth, there exists an upper bound on the number of simultaneous time critical messages that can be delivered in time by the communication infrastructure. Evaluation of this network support capability limit is important and necessary as it determines the feasibility of simultaneous delay guarantees for multiple messages.

7 Research Challenges and Outlook [1]

Given the importance of communication networks in the smart grid management, many research efforts in [35] [36] [37] [38] [39] have been made in proposing and constructing various network architectures to connect the distributively located electrical devices for automated control. To achieve satisfactory communication delay performance, a number of open research problems must be addressed carefully.

7.1 Understanding Delay Components

The communication infrastructure in smart grid will incorporate many network technologies and assume a hierarchical and hybrid composition. Different types of networks are used to provide communication facilities to different portions or regions of the grid and they are interconnected to form the entire infrastructure. The delay experienced by a message consists of many components as the message travels within each subnetwork and through the interfaces between subnetworks. The various delay components can be generally categorized as follows.

- **Data Acquisition Delay**. The status measurements, such as voltage, current and temperature, are acquired periodically from the electric devices and converted from their original analogue formats into the digital representations. The digital information is then processed by the attached embedded system, which functions as a low-profile computer, for transmission through the communication networks. A data acquisition delay is incurred between the event occurrences, for example a voltage change, and the actual digital information capture.
- **Packet Processing Delay**. Data is transmitted through a communication network by following the specified network protocols. Different layers of packet headers and trailers are added, inspected, modified and removed along the transmission path taken by the packet. Each step in packet processing adds extra delay to the total time spent by the packet in the network.
- **Packet Transmission Delay**. The current link layer mechanisms append a data integrity check field to each data frame to detect possible data errors. Every intermediate node on the packet transmission path verifies the data correctness after receiving the complete data frame and before forwarding the packet to the next relay node. Transmission delay is incurred on each link for the sending and receiving of the data frame.
- **Medium Access Delay**. Multiple data sending nodes that share the same transmission medium, such as wireless spectrum and wireline cable, compete for the medium access in order to transmit their respective data. A node has to wait until its turn for transmission. Similarly, a packet in a node has to wait until all the other packets scheduled ahead have been cleared from the buffer.
- **Event Responding Delay**. For some types of IED status reporting messages, actions are required in response to the events. For example, a measured voltage exceeding the normal value should trigger a circuit breaker off command from the control station. The intelligent energy and fault management system residing at the action responsible node may spend some time in deciding what response to take.

A detailed analysis of all the delay components between any pair of communicating IEDs is required to understand the delay performances in the communication infrastructure. A comparison between the actual delay performances and the expected delay bounds is needed to evaluate the supportive feasibility of communication networks. Given the diversity of equipment and protocols used in the smart grid, accurate delay evaluation is a challenging research issue.

7.2 End-to-End Delay [1]

7.2.1 Reduction of end-to-end delay

In order to meet the strict delay requirements in the smart grid communications, efforts are required in three delay reduction perspectives, namely, choosing the appropriate network equipment, utilizing the fast communication mechanisms provided in the current network equipment and protocols, and designing new protocols to speed up the transmission of time urgent messages.

- **Network technology selection.** There are many different network technologies available for use, which have different communication capacities and delay performances. Selection of the appropriate network technology for each application scenario is the first step toward meeting the delay requirements. However, besides the delay requirements, many other consideration factors like the deployment convenience and equipment cost also affect the decision on network selections.
- **Network service mapping**. Some network technologies offer fast communication mechanisms to support time critical message delivery, for example the DiffServ service classes in the Internet and the coordination functions in the wireless LANs. As the smart grid communications consist of multiple delay classifications, each type of messages should be mapped to the corresponding delay service provided by the underlying network technologies. The mapping is determined by whether the chosen delay service meets the delay requirement.
- **New protocol design**. Due to many reasons, such as deployment convenience and equipment cost, high profile fast networks may not always be the best selection for particular application scenarios. When low speed networks are used, alternative network protocol design may be needed to improve the delay performance. Re-engineering of network protocols is possible by modifying and updating the protocol stack programs in network equipment, but the side effects of changing standard protocols must be fully considered, such as the compatibility problems.

The communication delay is defined in the smart grid from end to end including all the network segments traversed by a message. Therefore, it is also important to design and deploy simple network structures that involve the least number of intermediate hops to minimize the communication delay.

7.3 Reliable Communications [1]

Reliability and security are fundamental concerns in power systems. As the power systems provide electricity to almost every aspect of our lives, they must be operated in the normal functioning status in design conformance. By reliability, we require that system faults occur with minimum probability and, should some component go wrong, its impact to the whole power system is minimized and the dysfunctional component is restored to the normal working status in the shortest time. Security, on the other hand, addresses the power system malfunctions due to human reasons, such as intentional attacks and unauthorized alterations. Since the communication networks play a vital role in the intelligent and automated energy system management, their reliability and security issues are a critical part of the power system reliability and security, and thus need to be addressed carefully. More importantly, given the time urgency of some types of messages in power systems, it is challenging to find reliability and security solutions that meet the strict delay requirements at the meantime.

7.3.1 Research challenges in communication reliability

Communication networks are not deployed extensively in traditional power systems. As such, the existing research efforts on power system reliability have mainly focused on identification of reliability problems [40] [41] [42] [43], definition of reliability metrics [44], and evaluation of reliability models [45] [46] for power devices. Communication network reliability [47] [48] [49] [50] and its connection to the power system reliability [51] [52] [53] still stay in a primitive research stage. The research challenges in power system communication reliability can be classified into several categories.

7.3.2 Reliability Mapping

The communication networks in power systems are responsible for information exchange among distributed power devices to assist the functioning of management systems. The reliability of communication networks is hence coupled with the reliability of power management systems. Power systems cannot work correctly unless the communications among intelligent electronic devices are transported as expected. To determine the reliability requirements on the communication networks, it is necessary to understand the performance expectations on communication infrastructure from the power management systems first, and then map the communication expectations into the network reliability requirements. Given the diversified communication performance expectations from the energy management systems, multiple-class network reliability requirements should be defined correspondingly.

7.3.3 Network Reliability

Messages may be delayed, altered or lost during transmissions in networks. The communication networks should be designed and implemented by taking these possible transmission problems into account to ensure that each message reaches its destination correctly and timely. Many network problems can result in unsatisfactory message transmissions, including for example network congestions, protocol errors, and link disruptions. Message prioritization and resource reservation mechanisms may help mitigate network congestions to allow the most important messages to be delivered on time. To prevent protocol errors and link disruptions, periodic network maintenance checkups are needed to identify and locate possible network problems. Besides, early detection mechanisms are also needed to discover network connection problems such that they can be fixed promptly.

7.3.4 Communication Restoration

Communication problems can be largely reduced if the networks are carefully implemented and operated, but they can never be eliminated. Having backup communication solutions is always a good practice to improve the network reliability further. For every important end-to-end connection path, one or more alternative routing paths should be planned ahead of failure occurrences. The original and alternative paths should have minimum intersections to enhance the robustness of each individual path. Automatic failure detections and path switchings are needed to resume communications instantly at the time of disruption in the original path. Additionally, mechanisms should be implemented to retransmit the messages that are lost during the path transition intervals.

7.3.5 Reliability Responsiveness

For some types of messages in power system communications, there are critical timing requirements on their maximally allowed transmission delays. The communication network reliability should be inspected under these strict timing bounds. Therefore, the definition and evaluation of reliability are based on the corresponding timing requirements. For example, the power system protection messages must be correctly delivered within a time frame as small as 3ms. An acceptable reliability solution should hence guarantee that the retransmitted or rerouted messages reach the intended destination devices within 3ms from the time that the first attempted message is sent. Any delayed messages received after this 3ms time window do not serve the reliability purpose. Therefore, it is challenging to address the communication network reliability problem.

7.3.6 Reliability evaluation

The communication network reliability should be modeled and analyzed by defining quantitative reliability metrics, such as error probabilities and restoration delays. Understanding the specific reliability performances is necessary in order to predict the likelihood of network problem occurrences and allocate the limited network resources to the most important performance perspectives. Furthermore, the impact of communication problems on the power grid operations and services should also be evaluated. For example, analysis should be provided to estimate the possibility of equipment damages and the extent of service outages if certain types of messages cannot be delivered correctly and timely due to network reliability problems. As the communication networks assist in the power grid functions, the reliability evaluation of communication networks should be mapped back to the power grid ability in providing continuous electricity services without disruption.

7.4 Secure Communication [1]

Communication security is a research issue as important as the network reliability regarding the correct functioning of power system management. Different from reliability, security problems arise from malicious human behaviors and hence they are more challenging to solve. As the communication networks undertake the responsibilities for information exchange used in power management, they could become targets of attacks that attempt to distort the management functions. Attackers can possibly gain monetary benefits or simply cause impactful damages to the power systems. Therefore, it is imperative to protect the communication networks from cyber-attacks. The security problems in power systems have been discussed widely in the literature [54] [55] [56] [57] [58] [59] [60] [61] [62] [63] [64] [65] [66].

7.4.1 Security objectives in power system communications

In literature, information security problems can be classified into five general categories in respect to their objectives, namely, availability, integrity, confidentiality, authenticity, and non-repudiation. In power system communications, mechanisms to achieve information availability, integrity and authenticity must be provided, among which availability is the most critical requirement. The confidentiality and non-repudiation objectives may not always be required, depending on the particular communication scenarios.

- **Information Availability**. The communication networks should be able to perform communication functions as normal when attacks happen that attempt to block the information passage in the networks. Availability is the foundation of other security concerns. The communication networks must first guarantee message deliveries to their intended destinations and then protect the messages from other security threats. As the communication networks used in the smart grid will be a large-scale comprehensive infrastructure that involves a diversity of components and protocols, attackers may exploit the security vulnerabilities at various network nodes and protocol layers to deny the legitimate communications from network accesses and usages.
- **Information Integrity**. The messages transmitted in the communication networks in smart grid should be protected against unauthorized changes. The contents of these messages are related to power system measurements, controls and user data, falsification of which will endanger the smart grid operations. For example, an altered status measurement may miss a component failure alarm, a falsified control command may interrupt the power system functions, and an incorrect user data exchange may result in wrong operations in the energy management system. Mechanisms must be provided to verify the integrity of the information contained in the transmitted messages.
- **Information Authenticity**. Forged messages in the communication networks should also be discernable. False messages injected into the communication networks by attackers interrupt the normal power system operations in a similar way as altered messages. They convey incorrect information between distributed power devices and result in wrong management decisions. Therefore, the communication networks must have mechanisms that are able to verify the message genuineness, i.e., the messages are from the senders as claimed. Messages that do not pass the authenticity inspection must be ignored and, under certain cases, the actual sources of false messages should be identified.
- **Information Confidentiality**. Sensitive information transmitted through the communication networks should be kept confidential. Such information includes for example the user account and transaction data. Disclosure of user sensitive information may violate the user rights, cause user financial losses, and compromise the creditability of the power service providers. Methods should be used to prevent unauthorized users from accessing the sensitive information both during transmission and at storage. The degree of confidentiality protection should be commensurate with the secrecy period required by the protected data.
- **Information Non-Repudiation**. The non-repudiation objective refers to the fact that a user cannot deny the transmission of a message after the message has been sent. Non-repudiation is related to the information forensics. In the smart grid communications, most messages do not require assurance of non-repudiation.

7.4.2 Security solutions in power system communications

The importance of communication security has been recognized by the research community in power system communications. Solutions have been proposed to construct secure communication networks to support the smart energy management in the power grid. Specifically, the security solutions in the literature are observed in the following categories corresponding to the security objectives discussed above.

- **Denial-of-Service Defense**. All the information availability attacks interfere with the normal information exchanges by injecting false [67] or useless [68] packets into the communication networks. The false information confuses the packet recipients in recognizing the correct information. The useless packets consume a significant share of network bandwidth such that the legitimate traffic is knocked out in the network. Both types of attacks deny the information availability in the communication networks. Solutions to defend against the denial-of-service attacks rely on a careful discretion of the legitimate traffic from the attack traffic. An effective solution must be able to filter out the attack traffic to protect the legitimate information exchanges.
- **Integrity Protection**. To prevent messages from unauthorized changes during transmission, mechanisms are needed for the message recipients to verify the originality of the received messages. The integrity protection solutions rely on the established agreements between message senders and receivers on the use of message encryption keys [66] [69] [70] [71] [72]. The message senders use the encryption keys to compute a message digest for each message and the message receivers use the corresponding decryption keys to verify the correctness of the received message digest. The encryption and decryption keys can be either identical or asymmetric. Usually identical keys have lower computational overhead than asymmetric keys. In order to establish the encryption and decryption key pairs, key exchange protocols must be completed before the message integrity can be protected.
- **Authenticity Enforcement**. Message origins must be verified in the power system communication networks to prevent sophisticated attackers from impersonating legitimate power devices to transmit forged messages. The solutions to guarantee message authenticity are built on top of the mechanisms that require message senders prove their identities [73] [74] [75] [76, p.]. The identity proofs are usually presented in the form of demonstrating the knowledge of certain secrets that are known by the message senders. The secrets used for identification are usually the same message encryption keys used for integrity protection and therefore the authenticity enforcement schemes employ either the symmetric or the asymmetric encryption and decryption key pairs. Key exchange protocols are necessary in order to establish the key pairs.

In power system communications, the information confidentiality and non-repudiation are not always required. Except for certain types of messages, such as the customer transactions, messages do not need to be protected against unauthorized reading. There is also no requirement in most cases for the communication networks to prevent message senders from denying message transmissions. Most of current research efforts on the power system communication security are targeting the information availability, integrity and authenticity objectives, which are critically important in power systems.

Other than the five major security objectives discussed above, research efforts have also been reported in the intrusion detection systems [77], access control schemes [78], and communication anonymities [79]. Intrusion detection systems and access control schemes supplement the other security solutions to strengthen the power system defense against security threats. The communication anonymity, on the other hand, addresses the user privacy concerns while preserving the security requirements.

7.5 Summing Up on Research Issues [1]

The smart grid is a large-scale complex power system interconnecting an enormous number of power devices that are equipped with significantly diverse computation and communication capabilities. It is challenging to address reliability and security problems in the smart grid communication networks due to the network size and heterogeneity. Specifically, the research challenges exist in the following categories:

- **Requirements Mapping**. As stated in section 6.1.1, the communication networks in power systems transmit diversified classes of messages (see Table 5 and Table 6). Different types of messages may require different security protections. For example, the system control messages must be protected with information availability, integrity and authenticity, while the system status sampling data without emergency may only need integrity and authenticity and the availability requirement may not always be necessary, as occasional packet loss is acceptable. A careful classification of the message types and their mapping to the security objectives must be determined.
- **Minimum-Latency Solutions**. Security protection mechanisms for emergent messages must incur minimum latency to satisfy the message delay requirements. For the time critical messages, delivery beyond their acceptable delay windows renders the messages useless. The delays introduced by the security computations and protocol setups add on top of the message transmission delays and therefore they should be kept minimum. In general, computationally intensive security solutions provide strong protection but incur long delay, so a practical tradeoff between the security performance and the computational delay may be reached in the design of security solutions.
- **Security Evaluation**. Each security scheme used in the power system communication networks must be carefully evaluated on its strength. Typical evaluation metric is the computational time required for compromising the security scheme. The security strength should be sufficiently high such that it is practically impossible to compromise the scheme within a reasonable amount of time. For a security protocol design, every step in the protocol should be inspected to preclude any potential security holes. The security evaluation should also include an assessment of the possible equipment damages and service losses in case that the scheme is compromised.

Following table summarizes research challenges and their solution for RePlan:

Table 7 Communication requirements, challenges and solutions for RePlan

Research Challenges	Description	Solution
Reliability, availability and redundancy of communication infrastructure	• Communication infrastructure for control operations should use redundant heterogeneous communication links as	• Exploring reliable ICT • Specifying redundant interfaces between controllers and control-centers

	backup solutions to fault tolerance. • Guarantying the availability of communication infrastructure to “t” time unit/year with a mean time between failure (MTBF) equal to “t” time unit.	• Possibility of re-routing of information flow. • Further need for redundancy to be determined within test beds and simulations.
Integrity of End-to-End communication with minimum latency	• End-to-end integrity of control signal communications should be guaranteed through secure transport layer protocols.	• To be fulfilled by higher layers of the ICT architecture, • Further need to increase the integrity of end-to-end communication to be determined within test beds and simulations
Integrity of transmitted data	• Transmitted data/measurements/commands are protected against intentional changes • Integrity of transmitted data is preserved in all data exchanges	• Specific security measures are determined by security architecture.
Security of communication infrastructure	• The communication infrastructure for control operations should guarantee protection against intentional threats.	• Use of authentication, encryption and DDoS defense.
Controller to control-center communications	• Specifying the possible measures e.g. bandwidth, data rate	• To be determined once requirements for controllers are finalized through test beds and simulations.
Response Time	• The total response time of the closed control loop for any use case, from the start of the elaboration to the end of the set point actuation, depends on DER power electronics. • Depending upon the message type, it is of the order of “t” seconds	• General capabilities are given by ICT architecture design. • Performance analysis of KPIs to be determined by test beds and simulations.

8 References

[1] W. Wang, Y. Xu, and M. Khanna, “A survey on the communication architectures in smart grid,” *Comput. Netw.*, vol. 55, no. 15, pp. 3604–3629, Oct. 2011.

[2] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, “Communication network requirements for major smart grid applications in HAN, NAN and WAN,” *Comput. Netw.*, vol. 67, pp. 74–88, Jul. 2014.

[3] “D1.2 - Technical Feasibility of Ancillary Services provided by ReGen plants,” DTU Wind Energy E-0099.

[4] Adamiak, M, Patterson, R, and Melcher, J, “Inter and intra substation communications: Requirements and solutions,” 1996.

[5] “IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation,” *IEEE Std 1646-2004*, p. 0_1-24, 2005.

[6] V. Skendzic and A. Guzman, “Enhancing Power System Automation Through the Use of Real-Time Ethernet.”

[7] “Communication Networks/TCP and UDP Protocols.” .

[8] “IEEE Standard for SCADA and Automation Systems.” .

[9] G. R. Clarke, D. Reynders, and E. W. (B.Sc.), *Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems*. Newnes, 2004.

[10] “IEEE Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation,” *IEEE Std 1379-2000*, pp. 1–72, Mar. 2001.

[11] “IEEE Application Guide for IEEE Std 1547(TM), IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems,” *IEEE Std 15472-2008*, pp. 1–217, Apr. 2009.

[12] “Approved IEEE Draft Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected With Electric Power Systems.” .

[13] “IEEE Draft Standard for Conformance Test Procedures for Equipment Interconnecting Distributed Resources With Electric Power Systems.” .

[14] “NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.” [Online]. Available: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf. [Accessed: 26-May-2016].

[15] “NIST, Guidelines for smart grid cyber security.” [Online]. Available: http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf. [Accessed: 26-May-2016].

[16] “International Standard IEC 60870.” .

[17] “Intrnational Standard IEC 61850.” .

[18] “International Standard IEC 61968.” .

[19] “International Standard IEC 61970.” .

[20] “International Standard IEC 62351.” .

[21] “IEC 61850 Standard.”

[22] “IEEE Standard for Electric Power Systems Communications – Distributed Network Protocol (DNP3),” *IEEE Std 1815-2010*, pp. 1–775, Jul. 2010.

[23] T. S. Sidhu and Y. Yin, “Modelling and Simulation for Performance Evaluation of IEC61850-Based Substation Communication Systems,” *IEEE Trans. Power Deliv.*, vol. 22, no. 3, pp. 1482–1489, Jul. 2007.

[24] R. H. Khan and J. Y. Khan, “A comprehensive review of the application characteristics and traffic requirements of a smart grid communications network,” *Comput. Netw.*, vol. 57, no. 3, pp. 825–845, Feb. 2013.

[25] D. Hou and D. Dolezilek, “IEC 61850 – What It Can and Cannot Offer to Traditional Protection Schemes,” 2008.

[26] K. P. Brand, M. Ostertag, and W. Wimmer, “Safety related, distributed functions in substations and the standard IEC 61850,” in *Power Tech Conference Proceedings, 2003 IEEE Bologna*, 2003, vol. 2, p. 5 pp. Vol.2-pp.

[27] “Interoperable Framework for IEC61850-Compliant IEDs and Noncompliant Energy Meters with SCADA.”

[28] "Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3."

[29] Jan Tore Sørensen and Martin Gilje Jaatun, "An Analysis of the Manufacturing Messaging Specification Protocol."

[30] J. W. Konka, C. M. Arthur, F. J. Garcia, and R. C. Atkinson, "Traffic generation of IEC 61850 sampled values," in *2011 IEEE First International Workshop on Smart Grid Modeling and Simulation (SGMS)*, 2011, pp. 43–48.

[31] T. Skeie, S. Johannessen, and C. Brunner, "Ethernet in substation automation," *IEEE Control Syst.*, vol. 22, no. 3, pp. 43–51, Jun. 2002.

[32] S. Mohagheghi, J. C. Tournier, J. Stoupis, L. Guise, T. Coste, C. A. Andersen, and J. Dall, "Applications of IEC 61850 in distribution automation," in *Power Systems Conference and Exposition (PSCE), 2011 IEEE/PES*, 2011, pp. 1–9.

[33] "IEC 61850-5:2013 | IEC Webstore." [Online]. Available: https://webstore.iec.ch/publication/6012. [Accessed: 26-May-2016].

[34] M. Bøgsted, R. L. Olsen, and H.-P. Schwefel, "Probabilistic models for access strategies to dynamic information elements," *Perform. Eval.*, vol. 67, no. 1, pp. 43–60, 2010.

[35] Q. Yang, J. A. Barria, and C. A. H. Aramburo, "A communication system architecture for regional control of power distribution networks," in *2009 7th IEEE International Conference on Industrial Informatics*, 2009, pp. 372–377.

[36] K. Hopkinson, G. Roberts, X. Wang, and J. Thorp, "Quality-of-Service Considerations in Utility Communication Networks," *IEEE Trans. Power Deliv.*, vol. 24, no. 3, pp. 1465–1474, Jul. 2009.

[37] C. L. Chuang, Y. C. Wang, C. H. Lee, M. Y. Liu, Y. T. Hsiao, and J. A. Jiang, "An Adaptive Routing Algorithm Over Packet Switching Networks for Operation Monitoring of Power Transmission Systems," *IEEE Trans. Power Deliv.*, vol. 25, no. 2, pp. 882–890, Apr. 2010.

[38] M. LeMay, R. Nelli, G. Gross, and C. A. Gunter, "An Integrated Architecture for Demand Response Communications and Control," in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, 2008, pp. 174–174.

[39] L. A. O. Class, K. M. Hopkinson, X. Wang, T. R. Andel, and R. W. Thomas, "A Robust Communication-Based Special Protection System," *IEEE Trans. Power Deliv.*, vol. 25, no. 3, pp. 1314–1324, Jul. 2010.

[40] K. Moslehi and R. Kumar, "A Reliability Perspective of the Smart Grid," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 57–64, Jun. 2010.

[41] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal, "Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance," *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1922–1928, Nov. 2005.

[42] B. D. Russell and C. L. Benner, "Intelligent Systems for Improved Reliability and Failure Diagnosis in Distribution Systems," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 48–56, Jun. 2010.

[43] J. Eto, V. Budhraja, C. Martinez, J. Dyer, and M. Kondragunta, "Research, development, and demonstration needs for large-scale, reliability-enhancing, integration of distributed energy resources," 2000, vol. vol.1, p. 7.

[44] J. Haakana, J. Lassila, T. Kaipia, and J. Partanen, "Comparison of Reliability Indices From the Perspective of Network Automation Devices," *IEEE Trans. Power Deliv.*, vol. 25, no. 3, pp. 1547–1555, Jul. 2010.

[45] W. Zhao and F. E. Villaseca, "Byzantine Fault Tolerance for Electric Power Grid Monitoring and Control," 2008, pp. 129–135.

[46] Y. Wang, W. Li, and J. Lu, "Reliability Analysis of Wide-Area Measurement System," *IEEE Trans. Power Deliv.*, vol. 25, no. 3, pp. 1483–1491, Jul. 2010.

[47] Z. Xie, G. Manimaran, V. Vittal, A. G. Phadke, and V. Centeno, "An information architecture for future power systems and its reliability analysis," *IEEE Trans. Power Syst.*, vol. 17, no. 3, pp. 857–863, Aug. 2002.

[48] B. Yunus, A. Musa, H. S. Ong, A. R. Khalid, and H. Hashim, “Reliability and availability study on substation automation system based on IEC 61850,” in *Power and Energy Conference, 2008. PECon 2008. IEEE 2nd International*, 2008, pp. 148–152.

[49] M. G. Kanabar and T. S. Sidhu, “Reliability and availability analysis of IEC 61850 based substation communication architectures,” in *2009 IEEE Power Energy Society General Meeting*, 2009, pp. 1–8.

[50] M. S. Thomas and I. Ali, “Reliable, Fast, and Deterministic Substation Communication Network Architecture and its Performance Simulation,” *IEEE Trans. Power Deliv.*, vol. 25, no. 4, pp. 2364–2370, Oct. 2010.

[51] H. S. Yang, H. S. Jang, Y. W. Kim, U. S. Song, S. S. Kim, B. T. Jang, and B. S. Park, “Communication Networks for Interoperability and Reliable Service in Substation Automation System,” in *5th ACIS International Conference on Software Engineering Research, Management Applications (SERA 2007)*, 2007, pp. 160–168.

[52] F. Cleveland, “Enhancing the Reliability and Security of the Information Infrastructure Used to Manage the Power System,” in *IEEE Power Engineering Society General Meeting, 2007*, 2007, pp. 1–8.

[53] A. Z. Faza, S. Sedigh, and B. M. McMillin, “Reliability Analysis for the Advanced Electric Power Grid: From Cyber Control and Communication to Physical Manifestations of Failure,” in *Computer Safety, Reliability, and Security*, vol. 5775, B. Buth, G. Rabe, and T. Seyfarth, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 257–269.

[54] Dong Wei, Yan Lu, M. Jafari, P. Skare, and K. Rohde, “An integrated security system of protecting Smart Grid against cyber attacks,” 2010, pp. 1–7.

[55] G. N. Ericsson, “Cyber Security and Power System Communication #x2014;Essential Parts of a Smart Grid Infrastructure,” *IEEE Trans. Power Deliv.*, vol. 25, no. 3, pp. 1501–1507, Jul. 2010.

[56] G. N. Ericsson, “Information Security for Electric Power Utilities (EPUs) #x2014;CIGR #x00C9; Developments on Frameworks, Risk Assessment, and Technology,” *IEEE Trans. Power Deliv.*, vol. 24, no. 3, pp. 1174–1181, Jul. 2009.

[57] T. Sommestad, M. Ekstedt, and L. Nordstrom, “Modeling Security of Power Communication Systems Using Defense Graphs and Influence Diagrams,” *IEEE Trans. Power Deliv.*, vol. 24, no. 4, pp. 1801–1808, Oct. 2009.

[58] G. Ramos, J. L. Sanchez, A. Torres, and M. A. Rios, “Power Systems Security Evaluation Using Petri Nets,” *IEEE Trans. Power Deliv.*, vol. 25, no. 1, pp. 316–322, Jan. 2010.

[59] P. McDaniel and S. McLaughlin, “Security and Privacy Challenges in the Smart Grid,” *IEEE Secur. Priv.*, vol. 7, no. 3, pp. 75–77, May 2009.

[60] H. Khurana, M. Hadley, Ning Lu, and D. A. Frincke, “Smart-grid security issues,” *IEEE Secur. Priv. Mag.*, vol. 8, no. 1, pp. 81–85, Jan. 2010.

[61] L. Nordstrom, “Assessment of Information Security Levels in Power Communication Systems Using Evidential Reasoning,” *IEEE Trans. Power Deliv.*, vol. 23, no. 3, pp. 1384–1391, Jul. 2008.

[62] S. Sheng, W. L. Chan, K. K. Li, D. Xianzhong, and Z. Xiangjun, “Context Information-Based Cyber Security Defense of Protection System,” *IEEE Trans. Power Deliv.*, vol. 22, no. 3, pp. 1477–1481, Jul. 2007.

[63] J. Jaeger and R. Krebs, “Automated protection security assessment of today’s and future power grids,” in *IEEE PES General Meeting*, 2010, pp. 1–6.

[64] “Trust infrastructures for future energy networks - RWTH AACHEN UNIVERSITY Institute for Automation of Complex Power Systems - English.” [Online]. Available: https://www.acs.eonerc.rwth-aachen.de/go/id/dlmw/file/119014/lidx/1/. [Accessed: 06-Sep-2016].

[65] S. Clements and H. Kirkham, “Cyber-security considerations for the smart grid,” in *IEEE PES General Meeting*, 2010, pp. 1–5.

[66] A. R. Metke and R. L. Ekl, “Security Technology for Smart Grid Networks,” *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.

[67] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, May 2011.

[68] J. C.-Y. Chou, B. Lin, S. Sen, and O. Spatscheck, “Proactive Surge Protection: A Defense Mechanism for Bandwidth-Based Attacks,” *IEEEACM Trans. Netw.*, vol. 17, no. 6, pp. 1711–1723, Dec. 2009.

[69] D. Choi, H. Kim, D. Won, and S. Kim, “Advanced Key-Management Architecture for Secure SCADA Communications,” *IEEE Trans. Power Deliv.*, vol. 24, no. 3, pp. 1154–1163, Jul. 2009.
[70] M. Kim and J. J. Metzner, “A Key Exchange Method for Intelligent Electronic Devices in Distribution Automation,” *IEEE Trans. Power Deliv.*, vol. 25, no. 3, pp. 1458–1464, Jul. 2010.
[71] D. Choi, S. Lee, D. Won, and S. Kim, “Efficient Secure Group Communications for SCADA,” *IEEE Trans. Power Deliv.*, vol. 25, no. 2, pp. 714–722, Apr. 2010.
[72] I. H. Lim, S. Hong, M. S. Choi, S. J. Lee, T. W. Kim, S. W. Lee, and B. N. Ha, “Security Protocols Against Cyber Attacks in the Distribution Automation System,” *IEEE Trans. Power Deliv.*, vol. 25, no. 1, pp. 448–455, Jan. 2010.
[73] K. M. Rogers, R. Klump, H. Khurana, A. A. Aquino-Lugo, and T. J. Overbye, “An Authenticated Control Framework for Distributed Voltage Support on the Smart Grid,” *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 40–47, Jun. 2010.
[74] B. Daemi, A. Abdollahi, B. Amini, and F. Matinfar, “Digitally-Signed Distribution Power Lines: A Solution Which Makes Distribution Grid Intelligent,” *IEEE Trans. Power Deliv.*, vol. 25, no. 3, pp. 1434–1439, Jul. 2010.
[75] H. Chan and A. Perrig, “Round-Efficient Broadcast Authentication Protocols for Fixed Topology Classes,” in *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, Washington, DC, USA, 2010, pp. 257–272.
[76] Q. Wang, H. Khurana, Y. Huang, and K. Nahrstedt, “Time Valid One-Time Signature for Time-Critical Multicast Data Authentication,” in *IEEE INFOCOM 2009*, 2009, pp. 1233–1241.
[77] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J. C. Tan, “An Intrusion Detection System for IEC61850 Automated Substations,” *IEEE Trans. Power Deliv.*, vol. 25, no. 4, pp. 2376–2383, Oct. 2010.
[78] G. M. Coates, K. M. Hopkinson, S. R. Graham, and S. H. Kurkowski, “A Trust System Architecture for SCADA Network Security,” *IEEE Trans. Power Deliv.*, vol. 25, no. 1, pp. 158–169, Jan. 2010.
[79] P. Venkitasubramaniam and L. Tong, “Anonymous Networking with Minimum Latency in Multihop Networks,” 2008, pp. 18–32.