WECC

# Communications Systems Performance Guide for Electric Protection Systems

Relay Work Group and Telecommunications Work Group

June 9, 2022

# **Table of Contents**

1.	Pu	Purpose			
2.	Ele	ectric	Protection Systems	3	
,	2.1.	Pro	tection System Architecture	4	
,	2.2.	Pro	tection Schemes and Functions	5	
	2.2	.1.	Binary Data Schemes	5	
	2.2	.2.	Encoded Data Schemes	5	
	2.2	.3.	Protection System Functions	6	
	2.3.	Perf	formance Considerations for Protection Systems	8	
	2.3	.1.	Protection System Reliability	8	
	2.3	.2.	Availability	9	
	2.3	.3.	Protection System Redundancy	10	
	2.3	.4.	Timing Considerations	10	
3.	Со	ommu	inications Channel Requirements	15	
	3.1.	Inte	rface Types	15	
	3.2.	Ban	dwidth	15	
,	3.3.	Qua	lity	15	
	3.4.	Late	ency/Delay	16	
	3.5.	Ava	ilability and Redundancy	17	
4.	Со	mmu	inications Design Practices	17	
5.	Re	comr	nendations for Protection Function Availability and Delay	19	
6.	5. Availability/Outage Reference Table22				
Di	sclaiı	mer		22	
Ve	rsion	n Hist	ory	22	



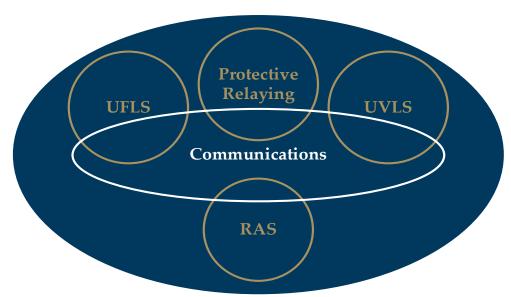
## 1. Purpose

This guide was prepared by the WECC Telecommunications and Relay work groups. It gives recommendations to communications system designers for communication circuits that support electric protection systems. It is not a detailed design specification, nor does it define hard requirements.

The guide was created in response to the recognition of potential relay timing problems arising from the application of digital communications and switching technologies. However, technology continues to develop, and this guide will be updated to address new problems as they arise. Since these performance standards are functional, they apply to all types of communications systems, for example, analog, digital, time division multiplex (TDM), packet.

# 2. Electric Protection Systems

Protection systems are used to isolate faulted parts of the system, protect the electric system from instability, and minimize equipment damage. Some protection systems operate in one substation or generation facility. Other protection systems operate over several locations. When the system includes several locations, communications channels are required to send information from one location to another. In this case, the communications channel becomes part of the protection system. This document is concerned only with protection systems that use communications channels. Figure 1 shows how this document categorizes protection systems.



#### **Protection System**

**Figure 1: Protection System Categories** 

The term *protective relaying* refers to traditional relaying schemes. A relay will sense a fault condition and assert a control signal to trip a breaker—isolating the fault and mitigating negative effects.



Underfrequency load shedding (UFLS) is a protection system that senses when frequency is lower than acceptable and directly acts to shed load to correct the frequency drop.

Undervoltage Load Shedding (UVLS) is a protection system that senses when voltage is lower than acceptable and directly acts to shed load to correct the low voltage condition.

A Remedial Action Scheme (RAS) is a scheme designed to detect predetermined system conditions and automatically take corrective actions, including adjusting or tripping generation (MW and Mvar), tripping load, or reconfiguring a system(s).

RAS:

- Meet requirements identified in the NERC Reliability Standards;
- Maintain Bulk Electric System (BES) stability;
- Maintain acceptable BES voltages;
- Maintain acceptable BES power flows;
- Limit the impact of cascading or extreme events.

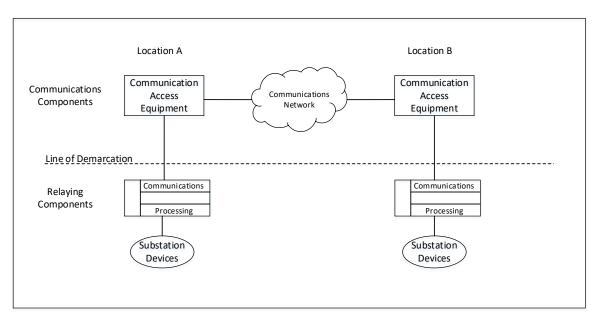
Communications are used to deliver information between sites. Examples of protection systems that use communications are Direct Transfer Trip (DTT), Permissive Overreaching Transfer Trip (POTT), Differential Comparison, and Telemetry.

#### 2.1. Protection System Architecture

In protection systems, relaying can occur locally, meaning the monitoring and tripping of the breaker reside at the same site; or remotely, meaning the monitoring may occur at one location, and the tripping of a breaker (or other action) may occur at another. Telecommunications technology becomes an essential part of the protection system in the remote case.

Figure 2 shows a protective relaying system, including all its major parts.





**Figure 2: Typical Protective Relaying Components** 

Substation devices include voltage transformers (VT) and current transformers (CT) and circuit breaker trip coils. The line of demarcation in Figure 2 is the boundary between communications components and relaying components of a protection system. Later, when we define the performance goals for communications, we will measure the performance at this line of demarcation. One confusing aspect of newer architectures is that modern relays may have an internal communications subsystem. For this document, the internal communications subsystem shown in Figure 2 is considered a relaying component.

## 2.2. Protection Schemes and Functions

Protection schemes are elements of a protection system and can be classified according to the way data is used. Two major groups are described below.

#### 2.2.1. Binary Data Schemes

These are protection schemes whose input to the communication system represents either of two discrete logic conditions (e.g., on/off for directional comparison blocking (DCB), guard/trip for POTT, line outage). There is no analog value or encoded data transferred from one location to the other.

#### 2.2.2. Encoded Data Schemes

These are protection schemes whose input to the communications system represents some type of analog value or time-sensitive, encoded information (e.g., phase comparison, current differential, megawatts).



#### **Communications Systems Performance Guide for Electric Protection Systems**

Prot. Scheme	Type of Scheme	Function Name	Description
	Direct	Direct Transfer Trip (DTT)	Direct circuit breaker tripping upon receipt of remote trip signal via communications
	Permissive	Permissive Overreaching or Underreaching Transfer Trip (POTT) or (PUTT)	Circuit breaker tripping is qualified by local fault detection and receipt of remote trip signal via communications
Binary Data	Blocking	Directional Comparison Blocking (DCB) or Unblocking (DCU)	Circuit breaker tripping is qualified by local fault detection and no receipt of remote block signal via communications
Ē	RAS	Remedial Action Scheme	An automatic protection system designed to detect abnormal or predetermined system conditions and take corrective actions other than or in addition to isolating faulted components to maintain system reliability.
	Phase Comparison	Phase comparison	Circuit breaker tripping is based on coincidence of local and remote waveforms representative of phase current
Encoded Data	Current Differential	Current differential	Circuit breaker tripping is based on coincidence of local and remote phase current waveforms
Enco	RAS	Remedial Action Scheme	An automatic protection system designed to detect abnormal or predetermined system conditions and take corrective actions other than or in addition to isolating faulted components to maintain system reliability

#### **Table 1: Protection System Types**

#### 2.2.3. Protection System Functions

A protection system often consists of several functions working together. A function is a single monitoring or control action. For example, a transmission line may be protected by a combination of DTT, POTT, and current differential functions. A RAS might include several monitoring functions (e.g., MW read, line outage, breaker status) and one or more control functions (insert reactive device, automatic generation control (AGC), etc.).

When analyzing protection system performance, we define performance recommendations that apply to each of these functions. The protection engineer may apply these functions to attain the desired overall performance of the protection system.



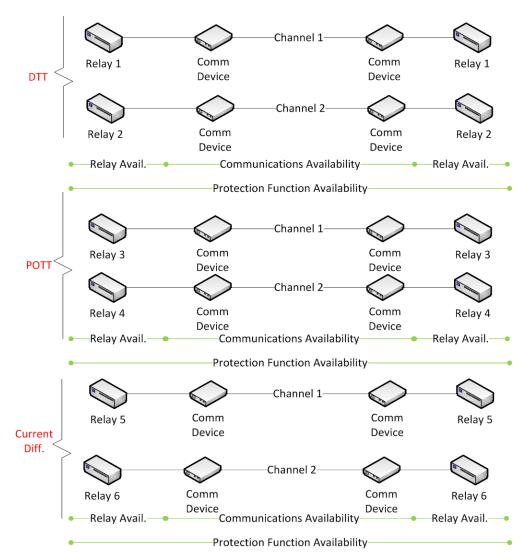


Figure 3: Typical Relaying Functions with Availability References



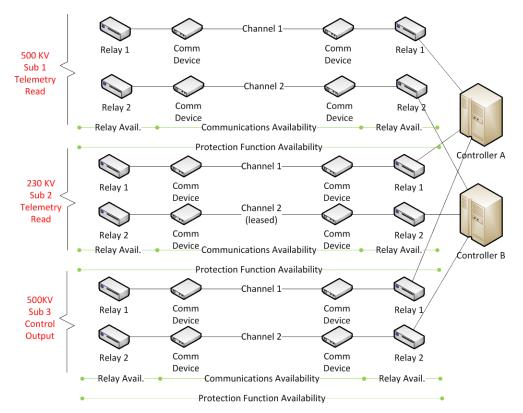


Figure 4: Typical RAS Functions with Availability References

## 2.3. Performance Considerations for Protection Systems

This section discusses the overall protection system performance. Also, the section separately identifies the performances of the communications components and the relaying components.

#### 2.3.1. Protection System Reliability

The Relay Work Group defines the components of protection system reliability as "dependability and security."

All parts of the protection system are considered, including relays, CTs, VTs, communications channels, all supply and control wiring, and station batteries. Note that communications channels include all communications equipment needed to deliver information from an initiating relay at one location to a receiving relay at another.

Two failure modes are considered: failure to operate, which is the defining characteristic of dependability; and unnecessary operation, the defining characteristic of security.

**Dependability**—The assurance that a protection system will respond to faults or conditions in its intended zone of protection.

Failure to operate means a failure of the protection system to clear a fault when it should.



#### **Communications Systems Performance Guide for Electric Protection Systems**

The dependability of a protection system can be affected by the communication component of the system. Consider a transmission line using a POTT scheme for high-speed protection over the entire length of the line. A failure of communication interface equipment at one terminal of this transmission line prevents the terminal from receiving the POTT signal from the remote terminal for an in-section fault. This results in loss of high-speed protection for the entire line.

**Security**—The assurance that a protection system will restrain from faults or conditions outside of its intended zone of protection. This term, as used here, should not be confused with the concepts of physical security or cybersecurity.

Unnecessary operations of a relay scheme are classified into two groups:

- 1. Unnecessary operation in a non-fault condition; and
- 2. Unnecessary operation due to a fault occurring outside of its primary protection zone, (i.e., external fault).

The security of a protection system can be affected by the communication component of the system. Consider the POTT scheme of the previous example functioning properly in all respects except for a loop back condition of the communication circuit at one terminal of the transmission line. An out-of-section fault detected by this terminal will cause the terminal to key POTT to itself resulting in an incorrect trip (overtrip).

In this guide, reliability of the communications system is a measure of overall reliability. Note that this is not the same measure of reliability or availability as used in path designs.

#### 2.3.2. Availability

Availability is the ratio of the time during which a protection system is functioning at or above its required performance levels and the overall time in a given period.

Unavailability is converted to availability by subtracting unavailability from 1 and converting to a percentage.

Unavailability is the percentage of time a protection system is unavailable due to failure and is dependent on its Mean Time Between Failure (MTBF) and Mean Time To Repair (MTTR). Unavailable time includes unplanned outage time, hardware failures, software failures, procedural errors, and may include other criteria as defined by the utility.<sup>1</sup>

<sup>&</sup>lt;sup>1</sup> For more details on the calculation of availability and unavailability, see WECC Telecommunications Work Group, "<u>Guidelines for the Design of Critical Communications Circuits</u>," March 10, 2016.



One paper<sup>2</sup> defines "protection system unavailability" at  $9.4 \times 10^{-2}$  for standard relays and  $1 \times 10^{-4}$  for relays with self-testing features.

Protection system availability is composed of the communications component and the relay component.

It is essential that the communications systems be designed to operate during transmission impairments (e.g., ground potential rise) that are likely to occur along with power system faults.

Table 2 in Section 5 gives some availability recommendations for protection functions.

#### 2.3.3. Protection System Redundancy

Redundancy is the duplication of critical components of the protection system and is used to improve availability by reducing or eliminating single points of failure. Redundancy also allows certain components to be taken out of service for maintenance without losing functionality of the protection system.

Predicting a system's availability is complex and has a margin for error. In certain cases, not all components are redundant (and independent); therefore, there are degrees of redundancy.

An availability analysis (required as part of a RAS evaluation) includes mathematical calculations combining the MTBF, which most often is calculated by the manufacturer, and MTTR of each component according to the physical topology of the system.

These calculations assume that all failures of redundant or parallel components are independent of one another. In reality, the redundant components are not completely independent but offer a degree of independence. Attention should be paid to physical and electrical separation between system components, as this separation affects the independence of these components.

#### 2.3.4. Timing Considerations

Protective relaying requires monitoring a condition at one location and, as a result, taking some action at another location. There are inherent time delays introduced at several points in the protection system.

As Figure 5 shows, the total delay time, or "end-to-end delay time," is the time between the detection of a condition at Location A and control action commanded at Location B. The relay detection time at Location A and the operation time of the breaker at Location B are not included in the end-to-end delay time.

<sup>&</sup>lt;sup>2</sup> See J.J. Kumm, M.S. Weber, E.O. Schweitzer, D. Hou, "<u>Assessing the Effectiveness of Self-Tests and Other</u> <u>Monitoring Means in Protective Relays</u>," Western Protective Relay Conference, October 1994.



Protection system designers will specify a required "clearing time" for a fault condition. This clearing time is specific to a certain transmission line and depends on many factors, which are not detailed in this document.

See Table 2 in Section 5 for performance recommendations.

**Detection time**—The amount of time required for the relaying equipment at the monitoring location to detect the abnormal condition.

**Message encoding time**—The amount of time required for the relaying equipment to create a change of state message for transfer to the communications access equipment.

**Message serialization time** — The time required to transfer the packet of information containing the change of state message from the originating relay to the communications access equipment.

**Communications system transit time**—The time required for the communications system to carry the information to the control location. Sometimes this is called propagation time.

**Frame Transmission time**—The time required to transfer the packet of information containing the change of state message from the communications access equipment to the destination relay.

**Message decoding time**—The time required for the relay at the control end to understand the meaning of the message and decide to take action.

**Action time**—The time required for the relay to assert the appropriate signal at the control location.

**Breaker operation time**—The time required for the circuit breaker to operate. This time (usually greater than two cycles) is **not included** in the total or end-to-end delay times discussed in this document.



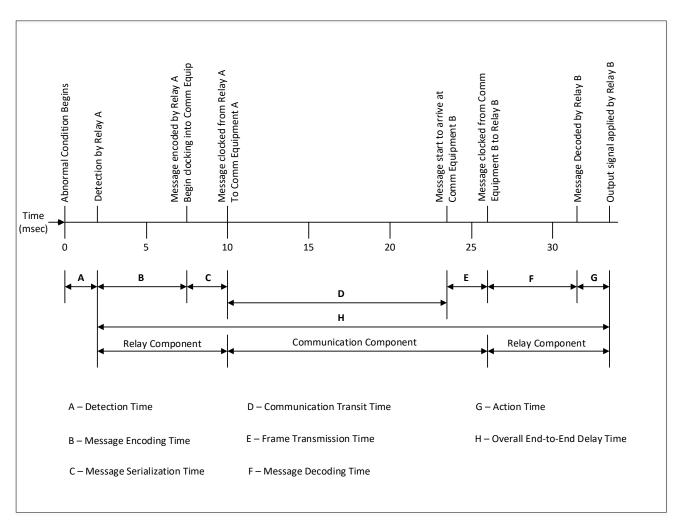


Figure 5: Protection System End-to-End Delay



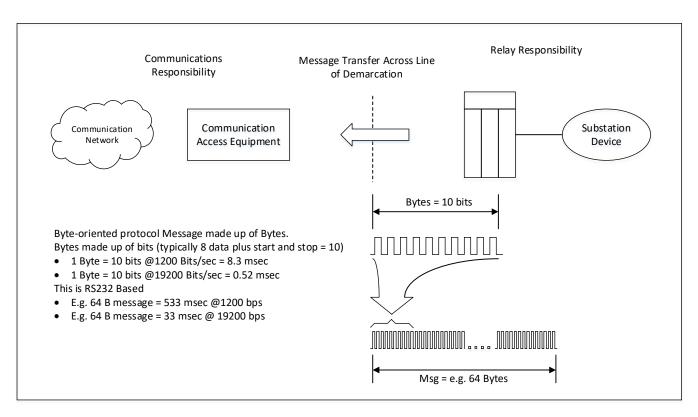
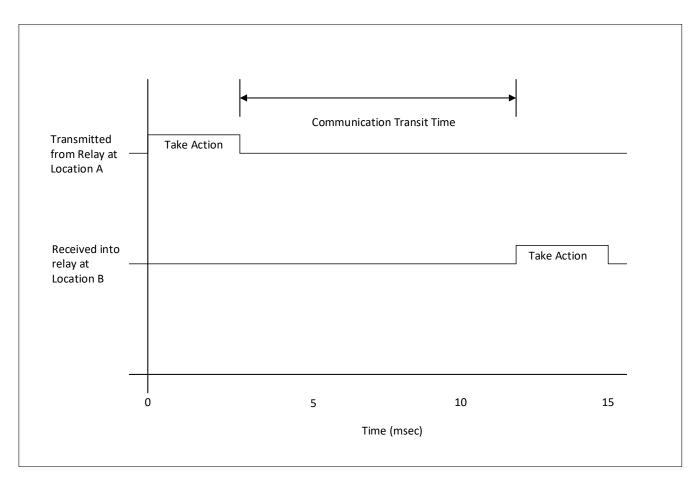


Figure 6: Message Serialization/Frame Transmission Time (direction dependent)







#### Figure 7: Communication System Transit Time

Some of these delays have a fixed component and a variable component. For example, the message decoding time will have a fixed component for the receiving relay to simply determine the meaning of the received message. In addition, this time might be lengthened to allow three consecutive "take action" messages to be received before deciding to take control action. Also, in an analog system, a trip action might only be executed after 50 milliseconds (ms) of valid guard tone followed by 5 ms of valid trip tone. This additional processing will increase the end-to-end delay but will decrease the likelihood of a false control action.

Communications system transit time will be the delay standard to which the communications infrastructure is evaluated.

Note that if the communications transit time could be zero, end-to-end delay would still be nonzero. For example, Schweitzer Engineering Labs (SEL) has measured the "back-to-back one-way data delay" for its devices using the Mirrored Bits ® protocol. SEL reports a delay of 12.5 ms for devices like 351 relays using 9,600 bps communications ports.<sup>3</sup>

<sup>&</sup>lt;sup>3</sup> Schweitzer Engineering Labs, Document AG2001-12, Appendix A



## 3. Communications Channel Requirements

The communications channel carries information from one location to another. Typically, this information is either analog (some form of modulated sinusoidal signal) or digital (electrical or optical 1s and 0s). Fundamental characteristics of a communications channel are discussed below.

The following sections will describe the fundamental characteristics of the communications channels used in protection systems. For each application, all these characteristics should be defined and agreed to by the relaying and communications responsible parties.

#### 3.1. Interface Types

Interface refers to the physical and electrical (or optical) connection point on the relaying components and the communications components. These interfaces must be compatible with each other. In some cases, an adapter is used to accommodate differences between the device interfaces. Some common interfaces are four-wire audio using screw terminals, digital RS-232 using a DB-9 connector, IEEE C37.94 using multimode fiber with ST connectors, and direct ethernet using fiber or copper.

#### 3.2. Bandwidth

Bandwidth is the capacity of a channel to carry traffic. Protective relaying generally does not require high bandwidths.

Audio signals produced by modems are usually carried via voice grade circuits having a frequency response of 300–3,000 hz. This is sufficient to allow reliable communications at up to 19.2 kbps. Digital channels used for relaying normally use bit rates of 19.2 kbps or less.

Ethernet interface services are becoming more common and typically operate at 10/100/1,000 Mbps.

## 3.3. Quality

The signal sent through the communications channel by the relay at Location A must be conveyed to Location B without a loss of information, i.e., the relay at Location B must be able to accurately decode the information it receives from Location A.

Sections 8.2 (Analog), and 8.3 (Digital), and 8.4 (Packet) of the "Guidelines for the Design of Critical Communications Circuits"<sup>4</sup> contain information regarding the required quality of analog and digital circuits.

The quality of analog channels is described using, for example, frequency response, signal-to-noise ratio, total harmonic distortion, or phase noise. For digital channels, bit error rate (BER), errored

<sup>&</sup>lt;sup>4</sup> WECC Telecommunications Work Group, "<u>Guidelines for the Design of Critical Communications Circuits</u>," March 10, 2016.



seconds (ES), severely errored seconds (SES), unavailable seconds (UAS), and jitter (bit timing variations) are often used. For packet channels, packet loss rate (PLR), ES, SES, UAS, and packet delay variation are often used.

## 3.4. Latency/Delay

This is a measure of how quickly signals propagate from one end of the communications channel to the other.

Table 2 in Section 5 defines the requirements for allowable message transit times through the communications components of an electrical protection system. The times contained in the table include the maximum end-to-end delay, and the division of this time into relay and communications components. Also, see Section 2.3.4 for additional timing considerations.

There are several aspects of the delay caused by communications transit time that are important to the protective relaying application. These should be discussed with the protection personnel for each application.

#### Magnitude

The delay introduced by communications transit time is measured from the output of the initiating relay to the input of the receiving relay. This delay includes signal propagation, data processing, and buffering associated with all communications components. The maximum delay for any protection scheme is dependent on the power system stability requirements. The protection engineer should provide the maximum delay allowable for the communications channel.

#### Variability

The communications transit time may not be constant over time. This variation may result from communications equipment processing, routing, or switching.

Solid-state encoded protective relays may be intolerant of variations in delay. Such variations in delay may result in protective relay misoperation. Some modern microprocessor relays use a digital messaging system that determines the delay while transmitting the data between the relays. These block relay operation on channel drop-out and do not restore operation until the delay is determined. They are tolerant of variations in delay but not tolerant of asymmetric delays, which we discuss below.

#### Asymmetry

The communications transmit time may be different in each direction. With Synchronous Optical NETwork (SONET) rings or networked communications systems, the forward and return paths used between relays may not be the same.

Some modern microprocessor relays use a channel-based messaging system to determine the end-toend delay while transmitting the data between the relays or a time-based synchronization to align data.



#### **Communications Systems Performance Guide for Electric Protection Systems**

Most relays can be set to block relay operation on channel drop-out and do not restore operation until the delay is determined or a predetermined number of good messages are received. Relays using channel-based messaging do not have an external time source and assume symmetry as if the end-toend delay were half of the measured loop delay. These relays attempt to align the remote terminal data to the local data with half the measured delay. An unequal end-to-end delay or asymmetry may result in relay misoperation. For relays using time-based synchronization, the free-running clocks of the relays are each phase locked to the external time, so they are mutually aligned. A high-precision clock is required to provide an absolute time for data alignment.

#### 3.5. Availability and Redundancy

Availability is the ratio of the amount of time the communications channel is performing at or above its required levels to the total time in a given period. The period for which availability is calculated does not include duration of planned maintenance or construction outages.

Unavailable time includes unplanned outages that are caused by failures of the communications equipment and power systems, radio path fades, fiber breaks, software outages, and procedural outages (worker error). Unavailable time does NOT include any planned outages.

The availability of the communications system must support the availability needs of the specific protection application. See Section 2.3.2 for a discussion of protection system availability. The concepts discussed in that section also apply to the communications components.

Table 2 in Section 5 contains availability and redundancy guidelines for four levels of system protection applications.

There may be a requirement for more than one relay-to-relay connection. In some cases, the parallel communications channels may use the same communications infrastructure. In other cases, completely independent communications paths are required ("fully diverse" is the term used in Table 2). For two communications paths to be "fully diverse," the communication system would be designed so that no credible single failure will cause loss of the protection function(s). In a system using redundant paths, unavailability of the protection function is only calculated when both the primary and standby channels are unavailable.

# 4. Communications Design Practices

Communications circuits that are components of protection systems are generally considered "critical communications circuits." The Telecommunications Work Group has created Guidelines for the Design of Critical Communications Circuits<sup>5</sup>, a document that provides design guidelines for many aspects of

<sup>&</sup>lt;sup>5</sup> WECC Telecommunications Work Group, "<u>Guidelines for the Design of Critical Communications Circuits</u>," March 10, 2016.



#### **Communications Systems Performance Guide for Electric Protection Systems**

communications systems, including buildings, towers, grounding, power systems, cables, microwave, and fiber optic transport systems. This document should be referenced by any designer of communications systems used for electric system protection.

Section 9 of the Critical Circuits document contains a method to calculate system availability. Although the intent of that method is to calculate the availability of a communications circuit, the method is valid for calculating protection system availability by extension.

One consideration not included in the Critical Circuits document is the end-to-end delay time. Section 2.3.4 above discusses timing considerations and describes the components that contribute to system delay. In the communications component (i.e., outside of the relay component), delay can be introduced by packet transfer between elements, signal processing in an element, and propagation time between elements.

A general design goal is to minimize delay time, but that is not always possible. Long fiber optic communications systems suffer from the relatively slow propagation speed of the optical signal. A rule of thumb would be to expect 1 ms of propagation delay for every 100 miles of optical fiber in the circuit.

Also, packet technology is becoming more common in communications systems. Where packet technology is deployed, the designer needs to consider the processing time required to examine and route the packet through the network, and the designer should investigate the packet processing delays of any communications equipment being used.

Finally, the designer needs to keep the needs of the specific protection application in mind while making design decisions. Working closely with the protection engineer will encourage this mindset.



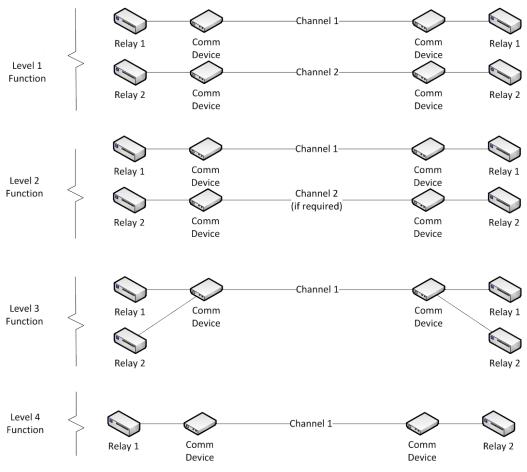


Figure 8: Typical Relay Topologies by Protection Level

# 5. Recommendations for Protection Function Availability and Delay

Table 2 captures recommendations for availability and delay performance for each function of a protection system. The table divides protection applications into levels to recommend a performance consistent with current best practices. The line of demarcation between the communications component and the relaying component is shown in Figure 2 in Section 2.1.



Level	Protection Application	Performance Recommendation for Each Function			
		Protection System	Communications Component	Relaying Component	
1	A BES transmission line or RAS; requiring critical clearing time <sup>6</sup> defined by the utility. Requires two redundant, fully diverse, independent communications channels.	Min availability 99.93% For combination of dual, diverse systems Max end-to-end delay 25.0 ms	Min availability 99.95% For combination of dual, diverse systems Max end-to-end delay 16.7 ms	Min availability 99.98% For combination of dual, diverse systems Max end-to-end delay 8.3 ms	
2	A BES transmission line or RAS; required to meet the reliability performance defined by the utility. Redundancy may be used to meet recommended availability.	Min availability 99.88% Max end-to-end delay 33.3 ms	Min availability 99.90% Max end-to-end delay 16.7 ms	Min availability 99.98% Max end-to-end delay 16.7 ms	
3	A BES transmission line or RAS; requiring improved security or dependency defined by the utility. Redundancy is typically not required to meet recommended availability.	Min availability 99.48% Max end-to-end delay 67 ms	Min availability 99.50% Max end-to-end delay 33.3 ms	Min availability 99.98% Max end-to-end delay 33.3 ms	
4	A BES transmission line requiring communications protection to satisfy power quality or other requirements of a given utility or customer.	Min availability 94.98% Max end-to-end delay 67 ms	Min availability 95.00% Max end-to-end delay 33.3 ms	Min availability 99.98% Max end-to-end delay 33.3 ms	

Table 2: Protection Function Performance Recommendations-Availability and Delay

Table 2 is intended to aid in telecommunications system design. The requirements of a specific application take precedence over the general recommendation of this table. For RAS, communication delays are based on the system studies and the overall requirements of the system. Reasonable efforts should be made to minimize communications delay. For Level 4 applications, consideration should be given to a design that is fail-safe (e.g., the line will trip upon loss of communications). Referring to Figure 5, the protection system max end-to-end delay H, is comprised of the Communications Component Max End to End Delay defined by D+E, the relay message serialization time, C, and the Relaying Component Max End to End Delay B+F+G.

<sup>&</sup>lt;sup>6</sup> Critical clearing time is the governing concept of the overall timing. The individual communications and relay components may be variable within this limit.



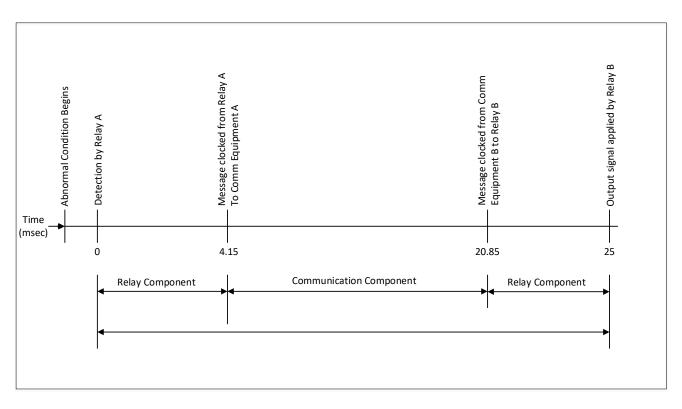


Figure 9: Example of Protection System End-to-End Delay Time



# 6. Availability/Outage Reference Table

Table 3 shows availability values found in Table 2 with the corresponding outage time.

Availability	Annual	Annual	24-hr outage
	Outage (min)	Outage (hr)	every x yrs
99.99%	52.6 min	0.88 hrs	27 yrs
99.98%	105 min	1.75 hrs	13.7 yrs
99.97%	158 min	2.6 hrs	9.1 yrs
99.96%	210 min	3.5 hrs	6.8 yrs
99.95%	263 min	4.4 hrs	5.5 yrs
99.94%	316 min	5.3 hrs	4.6 yrs
99.93%	368 min	6.1 hrs	3.9 yrs
99.90%	526 min	8.8 hrs	2.7 yrs
99.60%	2,104 min	35 hrs	0.68 yrs
99.50%	2,630 min	44 hrs	0.55 yrs
99.00%	5,260 min	88 hrs	0.27 yrs
96.00%	21,000 min	351 hrs	0.07 yrs
95.00%	26,300 min	438 hrs	0.06 yrs

#### Table 3: Availability versus Outage Time

# Disclaimer

WECC receives data used in its analyses from a wide variety of sources. WECC strives to source its data from reliable entities and undertakes reasonable efforts to validate the accuracy of the data used. WECC believes the data contained herein and used in its analyses is accurate and reliable. However, WECC disclaims any and all representations, guarantees, warranties, and liability for the information contained herein and any use thereof. Persons who use and rely on the information contained herein do so at their own risk.

## **Version History**

Modified Date	Modified By	Description
October 20, 2022	RRC	RRC Approved Document
September 7, 2022	EPAS	EPAS Approval, Recommend RRC Approval of Document
June 9, 2022	TELWG/RWG	Approved revised definitions and associated figures
October 22, 2013	OC	Approval of Guideline
August 20, 2013	TOS	Recommends OC Approval of Guideline
August 15, 2013	TELWG	Accepted Redlines
July 26, 2013	RWG	Approved Guideline/Redlines
July 11, 2013	TELWG	Approved Guideline
March 9, 2011	WECC	Added Tag

