Substation-to-Substation Applications 3

3.1 Line Protection Applications

Power system faults disrupt normal electrical power flow by diverting current through a short-circuited connection and collapsing power system voltage. Prompt and reliable clearing of power system faults therefore is of great importance in the design and operation of the power system.

- Removing faults as quickly as possible helps safeguard personnel in proximity to installations.
- Faults can cause severe operational disturbances resulting in collapse of power delivery and blackout for regions, and, in severe cases, even for several countries. Heavy reliance of modern society on electric power consuming devices for business activities, safety, lighting, heating, communication and many other conveniences make severe disturbances and blackouts unacceptable.
- Faults can cause damage and breakdown to power apparatus such as circuit breakers, transformers, and cables. The repair work or full replacement in case of destruction is very costly and may take considerable time.
- Transients due to faults in the power system can also adversely affect sources of generation and customer loads.
- Faults may have legal and financial consequences on manufacturers, held responsible for the consequences of device nonoperation (e.g., a breaker not acting correctly), and on power companies who may be penalized by the Regulation Authority or may have to compensate customers' nonsupply of power.

Electric power system generators, transformers, Busbars, and power transmission lines are monitored by Protective Relays which are designed to detect faults and consequently, to operate isolating devices in order to interrupt damaging fault current.

C. Samitier (ed.), *Utility Communication Networks and Services*,
CIGRE Green Books, DOI 10.1007/978-3-319-40283-3_3

The implementation of a Protection scheme must result in dependable operation of only those relays protecting the faulted unit, and at the same time must secure nonoperation of the relays during nonfault conditions and when faults occur on adjacent power system units. This balance is met only through proper protection scheme design, proper relay and equipment selection, and proper connection and setting of these relays and equipment to achieve appropriate sensitivity and coordination.

Protection performance requirements specify the balance between these conflicting goals of dependability and security.

- **Dependability** goals require maximum sensitivity and fast response time to detect and clear all faults quickly with very low probability of "failure to act" when a fault is present.
- **Security** goals require maximum selectivity and slow response time to minimize the probability of spurious operation leading to an unwanted action on a faultless circuit. Security is an issue during fault conditions as well as during normal, faultless conditions.

When protection schemes detect a fault on the equipment or line they protect, they signal (or "trip") isolating devices, called circuit breakers, to open, in order to isolate the faulty segment of the system and restore normal voltage and current flow in the power system.

When the protection scheme and circuit breakers operate properly, the fault is isolated within the required **fault-clearing time**. Protection applied on extremely high voltage systems, where fault-clearing times are most critical, typically detect faults and operate in about one to two cycles (or even less than one cycle in certain cases). Circuit breakers generally operate in one to three cycles. The combination of high-speed protection schemes and fast circuit breakers can interrupt a fault in about two cycles, although more common fault-clearing times range from three to six cycles.

Many protection applications require the real-time transfer of electrical measurements, signals, and commands between electrical substations to enhance or to enable the trip/operate decision.

A protection system must isolate the fault within a specified "fault-clearing time" of a few—typically 5 or 6 cycles (i.e., 100–120 ms at 50 Hz). This fault-clearing time includes the times for fault detection, protection decision including any signaling and isolating device operation.

Several protective relaying applications operate without any requirement for long distance communications, in particular those related to the protection of substation units (generators, busbars, transformers, etc.). Telecom services may be needed in this case, only to command a circuit breaker at a remote end if a local circuit breaker has been economized (Direct tripping) or exists but fails to interrupt fault-currents (Breaker Failure).

On the other hand, protection schemes for HV lines generally need real-time transfer of electrical measurements, signals, and command information with the protection device at the far end of the line to enhance or to enable the protection decision to operate and hence to meet fault-clearing requirements. In this case, communication may be the basis for fault detection (e.g. Current Differential Protection), or it may enhance time response and selectivity (e.g. Permissive Distance Protections), or still it may allow to command a remote isolating device (Circuit Breaker) for example when a local device fails to operate.

Teleprotection Signaling

If it were possible to set relays to see all faults on their protected line section and to ignore faults outside of their protected line section, then there would be no need for communication schemes to assist the relays. However, some protection relays, typically distance relays, cannot be set to "see" only the faults within a precise electrical distance from their line terminal. They are imprecise because of many factors including voltage and current transformer errors, relay operating tolerance, line impedance measurement errors and calculation tolerance, and source impedance variations. The primary relay elements used to detect line faults are therefore set to see or reach either short of the remote line terminal (this is called under-reaching), or to see or reach past the remote line terminal (this is called over-reaching).

The term "Teleprotection" refers to the communication interface of the Protection system (initially it applied to any protection scheme using telecommunications, now called telecom-assisted protection). Teleprotection signaling transforms the state information transmitted by the Protection Relay into a signal suitable for transmission over a telecommunication channel and restitution to the remote Protection Relay or remote Circuit Breaker in a secure and prompt manner. It may be integrated into the protective device, into the telecommunication access equipment, or more generally, it may constitute a stand-alone device.

This often supplements locally available data, confirming that a fault detected by at least one end, is in fact internal to the line, such that otherwise time-delayed operation may be accelerated.

In accordance with previously defined protection performance parameters, the operational performance of a teleprotection signaling system can be defined through the following parameters:

- **Security** is the ability to prevent communication service anomalies from restituting a Command at the remote end when no command has been issued. Security is expressed as the Probability P_{uc} of "unwanted commands" (command condition set at the receiving end for a duration longer than a specified limit). Security is related to the communication service integrity (error performance) and the Teleprotection Signaling system's error detection capability.
- **Transmission time** is the maximum time (T_{ac}) for the delivery of the command at the remote end, after which it is considered as having failed to be delivered. This is a constraint to the time performance of the communication service, not only in terms of nominal value but as a guaranteed limit.
- **Dependability** is the ability to deliver all issued commands at all times. It is expressed as the Probability P_{mc} of "missing commands" (issued commands not

arriving to the remote device, arriving too late or with a duration shorter than a specified limit). This sets a very severe constraint on the availability and error performance of the communication service, challenging such telecom service concepts as “errored seconds” and “degraded minutes” being counted in the available time of a communication service.

3.1.1 State Comparison Protection Schemes

State comparison protection schemes use communication channels to share logical status information between protective relay schemes located at each end of a transmission line. This shared information permits high-speed tripping for faults occurring on 100 % of the protected line.

The logical status information shared between the relay terminals typically relates to the direction of the fault, so the information content is very basic and generally translates into a “command”, requiring very little communication bandwidth. Additional information such as “transfer tripping” of a remote breaker (to isolate a failed breaker) and recloser blocking may also be sent to provide additional control.

These schemes are fundamentally based on comparing the direction to the fault at one terminal with the direction to the fault at the other terminal permits each relay scheme to determine if the fault is within the protected line section, requiring the scheme to trip, or external to the protected line section, requiring the scheme to block tripping.

Even if the communication requirements for state comparison protection schemes are considerably less stringent than for Analogue Comparison Protection schemes (described in the next section), the “command transmission time” is of great importance because the purpose for using communication is to improve the tripping speed of the scheme. Also, variations in transmission time are better tolerated in state comparison schemes than in the Analogue Comparison protection schemes.

Communication channel security is essential to avoid false signals that could cause incorrect tripping, and communication channel dependability is important to ensure that the proper signals are communicated during power system faults, the most critical time during which the protection schemes must perform their tasks flawlessly.

Communication for state comparison protection schemes must therefore be designed to provide safe, reliable, secure, and fast information transfer from one relay scheme to another. The communication scheme must—for the vast majority of protection schemes—also be able to transmit information in both directions at the same time. The amount of information required to transfer between relay schemes depends on the relay scheme logic.

The terminology used to describe these state comparison protection schemes is basically defined according to the *impedance zone monitored by the protection relay* as presented below:

- Directional comparison blocking schemes (also called Blocking Over-reach, BO)
- Directional comparison unblocking schemes (DCUB)
- Permissive over-reaching transfer trip schemes (POTT)
- Permissive under-reaching transfer trip schemes (PUTT)
- Direct transfer tripping (DTT).

Directional Directional Comparison Blocking (BO)

In a Blocking scheme, a fault detected by a time-delayed over-reaching relay (set directional into the line) is assumed to be internal to the line unless *blocked by the device at the opposite end* (Fig. 3.1). The blocking signal indicates that a fault external to the protected line has been detected. As the blocking command is used to prevent tripping, it is critical that the communication channel should be fast and dependable. However, when a blocking signal is transmitted the line is healthy and presents normal noise and attenuation conditions to a line-correlated communication channel such as power line carrier. Blocking schemes require only a simplex signaling channel and in this case they can be applied to a multiterminal line. If the Blocking signal fails to be received during a fault, tripping will still occur for faults along the whole of the protected line, but also for some faults within the adjacent line sections.

Directional Comparison Unblocking (DCUB)

This scheme was originally applied to frequency shift keyed PLC in circumstances where faults on the carrier phase can cause significant attenuation of the PLC signal. The scheme is basically a POTT scheme supplemented with monitoring of the PLC guard channel, such that a fault detection by the over-reaching element, coincident with the absence of either a receive signal or of the guard tone; is a sufficient condition to consider the fault to be internal to the line, permitting accelerated tripping (Fig. 3.2).

Permissive Over-reach Transfer Tripping (POTT)

A time-delayed forward directional (into the line) over-reaching relay is set at each end of the line. Over-reaching means detecting line faults on a distance longer than the protected line section. When the devices at all ends of the line see the fault as forward, then it must be internal to the line and accelerated tripping of the over-reaching element may take place. A phase-segregated POTT scheme provides additional security where single pole tripping is required (Fig. 3.3).

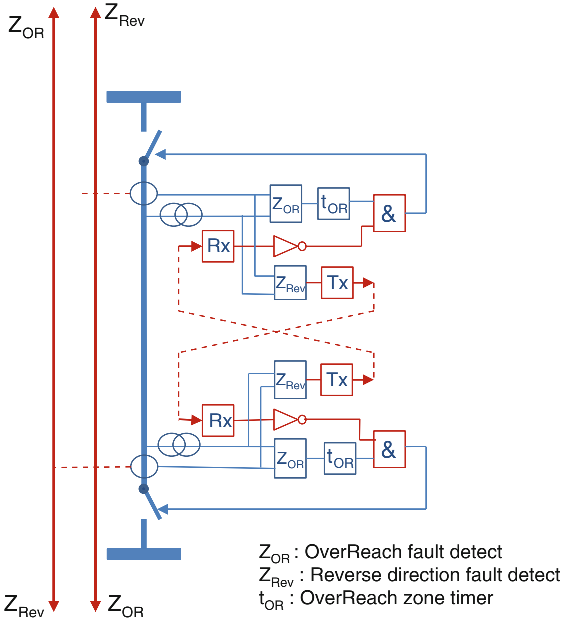

Z_OR
Z_Rev
Z_OR
t_OR
&
Rx
Z_Rev
Tx
Z_Rev
Tx
Rx
Z_OR
t_OR
&
Z_Rev
Z_OR
Z_OR : OverReach fault detect
Z_Rev : Reverse direction fault detect
t_OR : OverReach zone timer

Fig. 3.1 Directional comparison blocking scheme (BO)

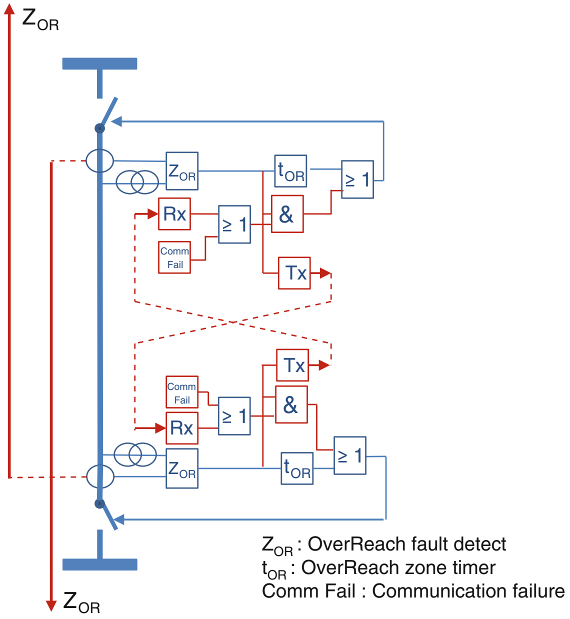
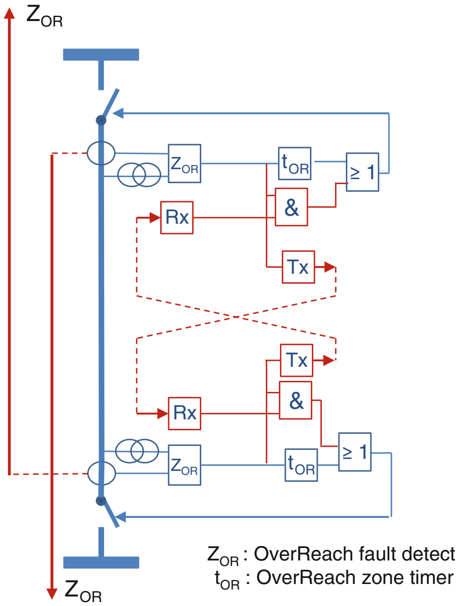

Z_OR
Z_OR
t_OR
≥ 1
Rx
≥ 1
&
Comm Fail
Tx
Tx
Comm Fail
&
≥ 1
Rx
≥ 1
Z_OR
t_OR
Z_OR
Z_OR : OverReach fault detect
t_OR : OverReach zone timer
Comm Fail : Communication failure

Fig. 3.2 Directional comparison unblocking (DCUB)

Fig. 3.3 Permissive over-reach transfer tripping (POTT)


Z_{OR}
Z_{OR}
t_{OR}
≥ 1
Rx
&
Tx
Tx
&
Rx
≥ 1
Z_{OR}
t_{OR}
Z_{OR}
Z_{OR} : OverReach fault detect
t_{OR} : OverReach zone timer

A Permissive Over-reach (POTT) relaying scheme requires a duplex signaling channel to prevent possible false operation due to spurious keying of the signaling equipment. This scheme may be more appropriate than a Permissive Under-reach scheme (PUTT) for the protection of short transmission lines due to greater resistive coverage. It should be noted that basic distance scheme tripping will still be available in the event of signaling channel failure.

Permissive Under-reach Transfer Tripping (PUTT)

In a Permissive Under-reaching scheme (Fig. 3.4), relays at the line terminations are set to detect faults over a distance shorter than the protected line section but longer than the middle of the line section A fault detected within a non-delayed under-reaching distance protection zone is definitively internal to the line: the Circuit Breaker local to the protection, may be tripped without delay. PUTT uses fault detection of this under-reaching zone to permit tripping of Circuit Breakers at the remote ends. If the protection at any of the remote ends receives the permissive transfer tripping command and has also detected the fault, but within a time-delayed over-reaching zone then accelerated tripping is permitted at that end (Zone Acceleration). The signaling channel is only keyed for faults within the protected line giving the scheme a high degree of security. If the signaling channel fails, basic distance scheme tripping will still be available.

Assuming that the Zone 1 is set to 80 % of the protected line, the faults in the remote 20 % of the line will be cleared via the Zone 2 time delay of the local relay if the remote terminal of the line is open.

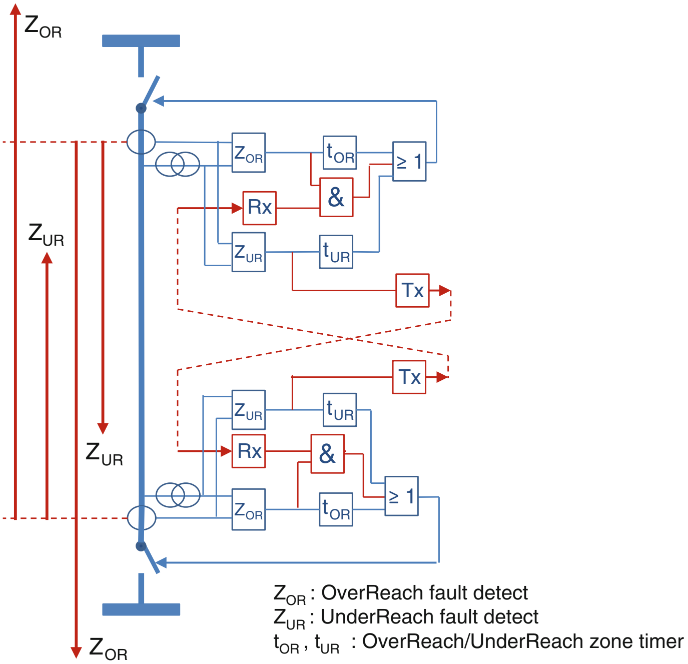

Z_{OR}
Z_{UR}
Z_{UR}
Z_{OR}
Z_{OR}
t_{OR}
≥ 1
&
Rx
Z_{UR}
t_{UR}
Tx
Tx
Z_{UR}
t_{UR}
Rx
&
≥ 1
Z_{OR}
t_{OR}
Z_{OR} : OverReach fault detect
Z_{UR} : UnderReach fault detect
t_{OR} , t_{UR} : OverReach/UnderReach zone timer

Fig. 3.4 Permissive under-reach transfer tripping

Direct Transfer Tripping (DTT)

In direct transfer tripping (or inter-tripping) applications, the command received from the far end is not supervised at the receiving end by any protection relay and simply causes Circuit Breaker operation. Since no local condition is available for checking the received command signal, it is absolutely essential that no stray unwanted commands are detected due to noise and error over the signaling channel. In other words, an inter-tripping channel must be very secure.

3.1.2 Analogue Comparison Protection Schemes

Analogue Comparison Protection is based on the transmission and comparison of electrical parameters between the ends of a protected line. The “analogue” values that are compared across the line are most commonly current samples, although other schemes such as pilot-wire or phase comparison have also been used (mostly in the past).

3.1.2.1 Current Differential Protection Schemes

The current differential protection, extensively used on HV transmission lines, compares the amplitude and phase of the local terminal currents with the amplitude and phase of the currents received from the remote terminal through a communications channel. It is applicable to any overhead line or underground cable at all voltage levels and is used in particular for the following:

- Very short lines and cables where the low impedance makes the adjustment of settings difficult for the use of Distance Relay.
- Multiterminal lines where the intermediate in-feeds modify the impedance seen by the Distance Relays, implicating that the observed impedance is not only dependent on the distance to the fault, but also on the in-feed from the remote terminals, making impossible an accurate measure of the impedance.
- HV Lines with only current transformers installed at each end (no voltage transformers).
- EHV transmission lines where series capacitors may create protection issues.
- Situations where immunity to power swings and current reversal is needed.

The currents at each line terminal are sampled, quantified, and transmitted to the remote end of the protected line for comparison. Current samples collected from a remote point must be compared with those measured locally at the same instant of time (synchronized sampling). Alternatively, the phase angles of the computed phasors are adjusted for the sampling skew and communication channel delays before comparison (asynchronous sampling). An error in sample timing and the associated delay compensation mechanism, results in a differential current that increases the risk of unwanted tripping.

Delay compensation in differential protection relies on the existence of a common time reference. Originally, and still in the great majority of installed and operational devices, this is achieved using a “ping-pong” technique to evaluate the “round-trip” transfer time and perform delay compensation assuming equal send and receive path delays. This creates a great sensitivity of the system to any time difference and therefore implicates the same routing for the two senses of communication. Moreover, considering the frequency of occurrence for this delay estimation, the communication medium must have a fairly stable propagation delay.

Modern protection systems can receive an external time reference such as a GPS clock to provide global time-stamping of samples, enabling them to tolerate switched networks. Once the system is synchronized, loss of GPS can be tolerated on a switched communication network using various techniques provided that the communication path does not change too often. There is, however, some reticence to render the protection system dependent upon an “externally provided” synchronization service such as GPS satellite.

New generation Current Differential Relays using IEC 61850 network interface and Precision Time Protocol (IEEE 1588v2) are expected to receive self-provisioned time coherence through the network which will perform the necessary ping-pong from switch to switch to determine the travel time from relay to relay. It is expected that precision time distribution will become by itself a critical "substation-to-substation" service in the future utility telecommunication network.

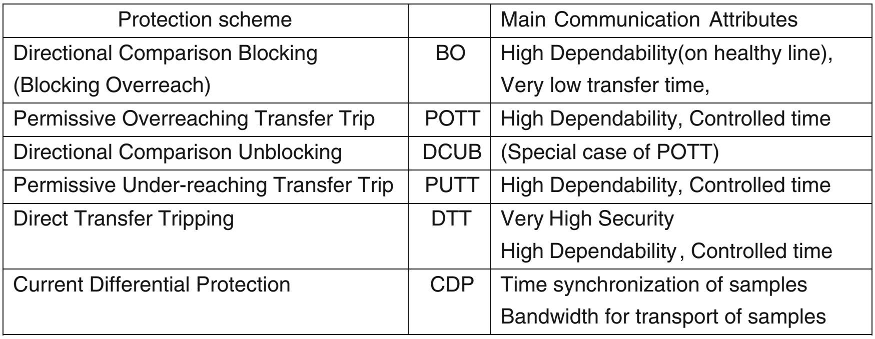
At present different fixed path and non-queued communications are used for Current Differential Relays. The instantaneous current sample values are converted to digital data and transmitted toward the other terminals at a rate of 12–60 samples per cycle over a communications channel of 64 kbps. Direct fiber and multiplexed communications are frequently employed. Packet-switched Ethernet communications with deterministic routing and time delay are presently being introduced. It must be emphasized that the availability of the current differential relay depends upon the availability of the communication channel. In general, the relay settings for current differential schemes are few and easy to compute, however, cable/long transmission line-charging currents and shunt-reactor applications in cables or overhead transmission circuits must be carefully studied.

There is always a finite time for the information from one end of the differential scheme to receive and process the information from the remote end and this will impact on the ability of the protection to trip. The longer the communications path and the delays in that path, the slower the overall trip time and this will become more critical as voltage levels increase. Typically, on EHV transmission systems total fault clearance times in the region of 3 cycles or less are required and given CB technology this would require unit operation in 1–1.5 cycles. This will have a direct relation with the maximum transfer time of the channel (including multiplexer, repeaters, network routing, etc.). Using differential protection requires an overall communications path delay <6 ms to achieve required fault clearance times.

Differential protection systems must have the capability of quickly detecting any loss of communications or inadequate quality of the channel in order to disable the differential scheme and employ another means of protection such as distance and over-current back up. This will indeed impact upon the achievable total fault clearance time considering the potential absence of teleprotection signaling to accelerate the back up protection. Generally, scheme designers would design mitigation strategies to reduce this risk, or use redundant communication paths/networks.

3.1.2.2 Other Analogue Comparison Schemes

Although the most commonly used analogue comparison schemes are Current Differential Protections, there are some older schemes such as AC pilot-wire relaying and phase comparison which may still be encountered as legacy applications in certain power networks. AC pilot-wire relaying is used for protecting short lines using independent metallic pilot-wires and as such do not interfere with the deployment or refurbishment of telecommunication systems. Phase Comparison Protection schemes compare the phase angles between the local and the remote terminal line currents and therefore require a communications channel to transmit and receive the necessary information. The phase comparison scheme has been very popular in the past because it had minimal communication channel requirements allowing the usage of Power Line Carriers. On the other hand, the sensitivity of the phase comparison relaying system is much lower than current differential relaying systems. Figure 3.5 provides a summary of line protection schemes described in this chapter and their communication attributes.



Protection scheme		Main Communication Attributes
Directional Comparison Blocking (Blocking Overreach)	BO	High Dependability(on healthy line), Very low transfer time,
Permissive Overreaching Transfer Trip	POTT	High Dependability, Controlled time
Directional Comparison Unblocking	DCUB	(Special case of POTT)
Permissive Under-reaching Transfer Trip	PUTT	High Dependability, Controlled time
Direct Transfer Tripping	DTT	Very High Security High Dependability, Controlled time
Current Differential Protection	CDP	Time synchronization of samples Bandwidth for transport of samples

Fig. 3.5 Summary of line protection schemes and their communication quality requirements

3.1.3 Protection Relay Communication in the IEC 61850

The following application groups have been considered in IEC 61850-90-1:

- Protection functions such as current differential line protection, distance protection with permissive and blocking schemes, directional and phase comparison protection, transfer tripping, predictive wide area protection, and substation integrity protection schemes.
- Control functions like auto-reclosing, interlocking, cross-triggering, generator or load shedding, out-of-step detection and topology determination of HV networks.

Whereas the timing requirements under normal operating conditions can be achieved within a substation, meeting the communication requirements for substation-to-substation applications such as protection relaying needs much more attention as to the WAN’s time predictability and hence guaranteed QoS.

IEC 61850 data model has been designed as a self-contained object model allowing the exchange of information without prior knowledge of the exchanging device. A client can retrieve information from, and explore logical nodes using only the elements given by the node and the knowledge of the standard data model. This abstract model is the basis for the i*nteroperability* which has been the goal of IEC 61850. At the same time, such a self-contained data model results in a great amount of data overhead which is not required if the exchanging parties have intimate knowledge of each other allowing them to exchange in a much more compact manner (e.g., trip signals). This has led to two architectural approaches from a communication point of view as shown in Fig. 3.6:

1. Gateway (or Proxy) approach—Corresponding gateway devices (at distinct substations) exchange specific signals and messages on behalf of IEC 61850 devices at each end. This is particularly useful where only low-speed

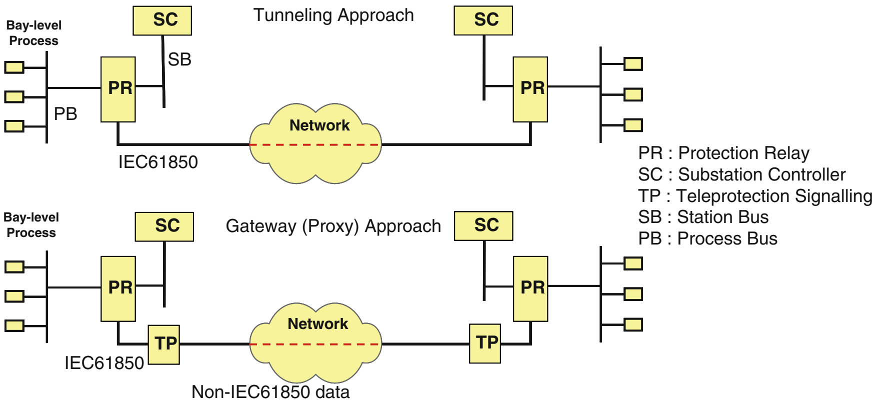


Fig. 3.6 Tunneling and gateway approaches in IEC 61850-90-1

communication channels are available. An IEC 61850-interfaced Teleprotection Signaling Equipment is typically in this category.

2. Tunneling Approach—Use high-speed communication links for direct transmission of 61850 messages from one substation to another substation.

3.2 System Protection Schemes

In many power delivery systems across the world the demand for electricity is fast approaching (and in some cases exceeding) the supply capability, while the operator still has the responsibility to provide a secure supply within statutory limits to its customers. Such increase in demand is pushing the grid to its stability limits which will ultimately result in the loss of supply or “black outs” as witnessed in recent years. Increasing the supply capability through infrastructure enhancement (e.g., new power transmission lines) has major economic and environmental implications. A mitigating approach is to implement strategies and corrective actions based on close monitoring of the variations of the power system parameters and a predetermined set of decision criteria. These systems are called System Protection Schemes (SPS), Remedial Action Schemes (RAS), or System Integrity Protection Schemes (SIPS). The following definition currently used for System Protection Schemes is given by the North American Electricity Reliability Council (NERC):

> An automatic protection system designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability. Such action may include changes in demand, generation or system configuration to maintain system stability, acceptable voltage, or power flows.

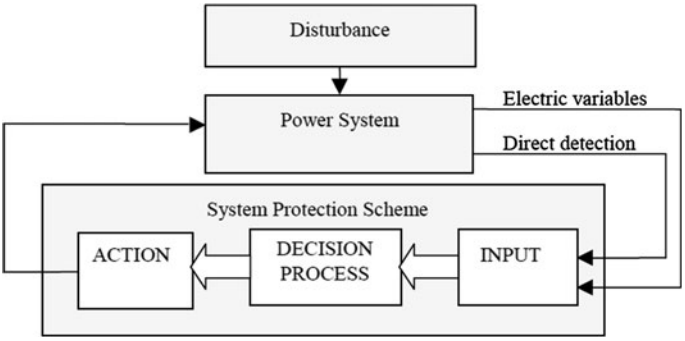


Fig. 3.7 General structure of a system protection scheme

System Protection operates over a wider portion of the grid (e.g., a transmission corridor) and a longer time (100 ms—few seconds) compared to Line and Unit Protections described previously. Typically it collects network condition information at multiple locations of a power system and undertakes system-wide automated actions such as load or generator disconnection.

Figure 3.7 shows the typical structure for a System Protection Scheme. The input to the system comprise electrical variables such as voltages, currents, and frequency measurements, but also control signals from power system stabilizers and FACTs as well as status signals from circuit breakers or tap changers. Typical actions associated to SPS decision are load shedding, generator tripping, etc.

3.2.1 SPS Applications

A large panel of power system applications responding to power system disturbance such as overload, power swing, and abnormal frequency or voltage can be implemented as System Protection Schemes. They comprise automated systems that protect the grid against system emergencies, minimizing the potential and extent of wide outages through automatic measures such as load shedding, generator shedding, or system separation. Some typical examples of System Protection applications are given hereafter together with operation time orders of magnitude in Fig. 3.8:

- Adaptive protection
- Generator control and rejection
- Load Rejection—Transmission line Removal
- Load Shedding (under-frequency or under-voltage)
- Out-of-Step Protection
- System split/separation
- Actions on Automatic Generation Control (AGC)
- VAR compensation

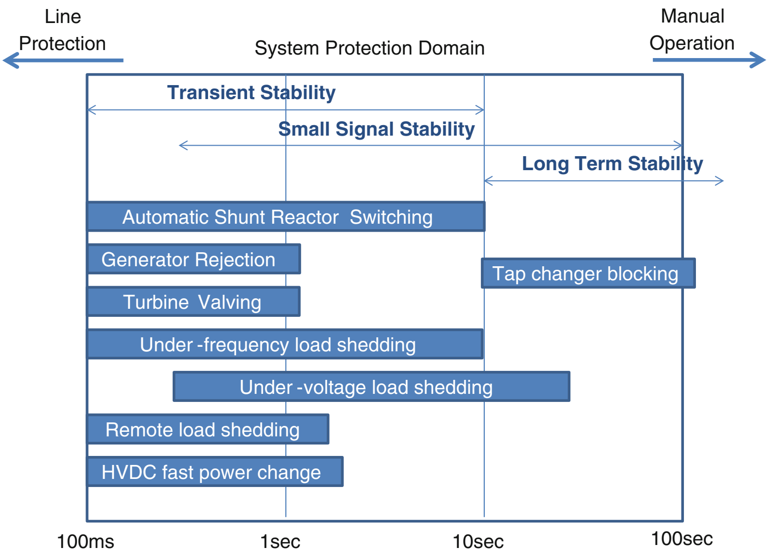


Fig. 3.8 SPS operation time frame related to power system phenomena

- Tap changer blocking
- Turbine fast valving/generator run-back
- Discrete excitation controls
- HVDC fast power change (Fig. 3.8).

3.2.2 SPS Architecture

The architecture of a System Protection Scheme can take different forms depending on the application:

- The system can be implemented with information capture, decision and action all located in electrical substations (reason why the section is inserted under substation-to-substation applications). In this case, a logic controller in one substation initiates actions across a subsystem. Reliability at the decision substation is a major design issue in this case. The decision and corrective action need secure reliable and prompt communication channels to collect remote information and to initiate actions.
- For more system-wide applications, the decision process can be totally or partially performed at a Control Center, and can initiate multilevel corrective actions. These systems are generally less time-sensitive automation applications covering stability issues in larger networks over one or multiple grids, and comprising multiple balancing authority areas. These systems are described under Substation-to-Control Center applications. The system can be composed

of a 2-level hierarchy: a lower level fast automation subsystem connecting substation sensing and actuating devices to a substation-based logic controller, and a higher level system-wide automation composed of a central platform and multiple subnetwork logic controllers.

- A System Protection Scheme can also be composed of sensing, decision, and actuating functions in the same substation together with a central coordinating platform which will adjust parameters and settings at each substation according to a wider set of situational information. An adaptive protection scheme is such a system, automatically making adjustments to protection relay settings in specific network conditions, typically to avoid cascaded tripping.

From an operational control point of view, two categories of SPS can be distinguished according to their respective control variables:

- **Response-based SPS** is based on measured electrical variables (e.g., a synchronized set of voltage phasors, frequency, etc.) and initiates actions when these variables are outside certain thresholds. Typical response-based SPS are under-frequency or under-voltage load shedding. Response-based schemes require fast exchange of large volumes of information. They require therefore extensive network communication capacity.
- **Event-based SPS** operates on detecting a combination of events (e.g., loss of several lines). Event-based SPS are faster than the response-based ones as they do not need to wait for the reception of out-of-tolerance measured variables at the decision node. Typical event-based SPS are generation rejection initiated by tripping across a transmission corridor.

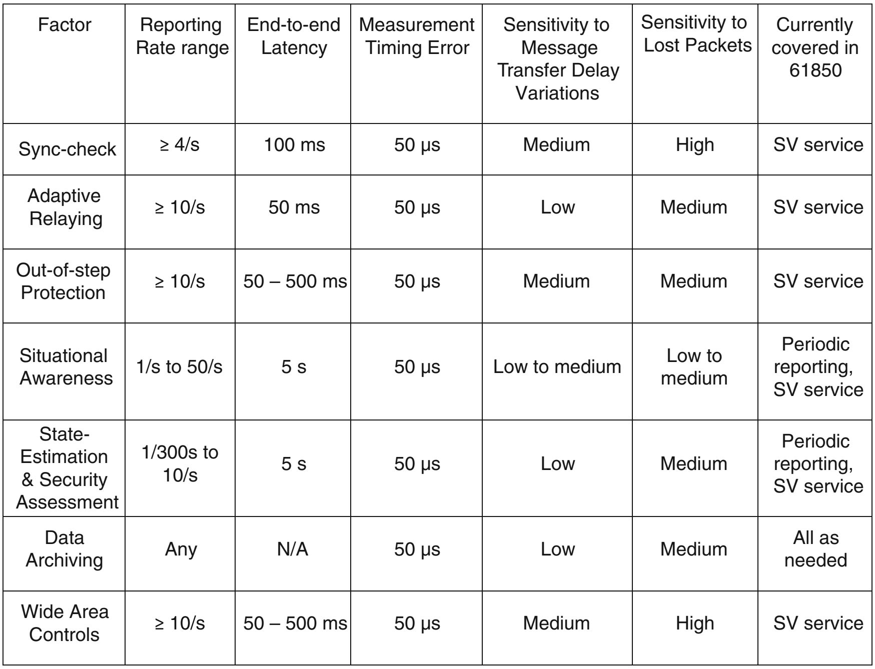
In all cases, implementing System Protection Schemes requires reliable, fast, time-constrained, and fully predictable communication network services. Response-based SPS, in the form of synchrophasor-based Wide Area Protection and Control requires fast collection of a coherent data set, as described in the following paragraph, to implement complex applications. Event-based SPS, implemented using teleprotection signaling equipment and simple combinatory logics is used as a way to implement protection systems responding to simpler but higher time constraint applications.

3.2.3 Wide Area Protection & Control (WAP&C)

Response-based system protection schemes capture electrical variables across a wide geographical area and from many different sites. Analytical algorithms use the collected data set in order to adopt an automated decision which can be more or less complex depending on the reactive or proactive nature of the application. The data set is generally composed of voltage and current values across the protected system. It must have high resolution (high sampling rate) to reflect the variation waveform information (vector measurements rather than scalar amplitude values). It must also be complete (no lost values) and coherent (a snapshot of all values taken at the same instant of time). Such a data set allows performing full-scale circuit analysis well beyond the State Estimation performed by the SCADA system. Complex transform-based predictive analysis can further allow proactive measures to maintain system stability.

These System Protection Schemes are known as Wide Area Protection & Control (WAP&C). This is an extension of the concept of Wide Area Monitoring Systems (WAMS), described in the next section, for implementing Closed Loop Applications automatically acting upon the grid in a time scale longer than Line and Unit Protection but shorter than SCADA (System Protection time scale).

WAP&C systems employ time-stamped voltage and current phasors (synchrophasors) with precise time synchronization across the protected domain. This allows accurate data comparison over a wide area or across the entire controlled system. Phasor Measurement Units (PMU) are data capture devices that in conjunction with GPS provide time-synchronized vectors. The standard IEEE C37.118 defines the coding of phasor information and the associated time-stamping. Phasor Data Concentrators (PDCs) receive phasor data from the PMUs and run decision algorithms for taking appropriate actions. They can also act as gateways towards higher level information processing at a Wide Area Monitoring and Control System.



Factor	Reporting Rate range	End-to-end Latency	Measurement Timing Error	Sensitivity to Message Transfer Delay Variations	Sensitivity to Lost Packets	Currently covered in 61850
Sync-check	≥ 4/s	100 ms	50 µs	Medium	High	SV service
Adaptive Relaying	≥ 10/s	50 ms	50 µs	Low	Medium	SV service
Out-of-step Protection	≥ 10/s	50 – 500 ms	50 µs	Medium	Medium	SV service
Situational Awareness	1/s to 50/s	5 s	50 µs	Low to medium	Low to medium	Periodic reporting, SV service
State-Estimation & Security Assessment	1/300s to 10/s	5 s	50 µs	Low	Medium	Periodic reporting, SV service
Data Archiving	Any	N/A	50 µs	Low	Medium	All as needed
Wide Area Controls	≥ 10/s	50 – 500 ms	50 µs	Medium	High	SV service

Fig. 3.9 Wide area protection and control applications

A high resolution capture and tight time imperatives (for prompt closed loop operation) imply high bandwidth and low latency deterministic communications. The completeness of data sets is to be assured through the reliability and integrity of the communication system. This cannot be fulfilled by an acknowledged exchange and retransmission upon error detection due to time imperatives of the closed loop system. Deploying Ethernet transport with controlled quality of service in the communication networks allows implementing many complex system protection schemes. The power system communication architecture standard IEC 61850 provides appropriate protocol stack and services for the information exchange in the WAP&C.

The time stamp precision can be achieved either through network-independent time distribution (e.g., GPS) or through a precise clock distribution service over a packet-switched network.

IEC 61850-90-5 describes how synchrophasors can be transmitted via IEC 61850. Sample transmission is based on the Sample Value (SV) service. For a communication outside the substation this service has to be tunneled across a broadband communication network. Additional event data can be communicated via GOOSE or MMS reports.

IEC 61850-90-5 describes the communication requirements for many protection schemes based on synchrophasors. Fig. 3.9 summarizes these requirements.