Analysis of Protection Scheme Dependencies on Communications

Galina S. Antonova
ABB Inc., Canada

Eduardo Colmenares
ABB Inc., USA

Ilija Jankovic
ABB Inc., USA

Texas A&M Conference , Colleage Station, TX, USA, April 8th – 11th, 2013

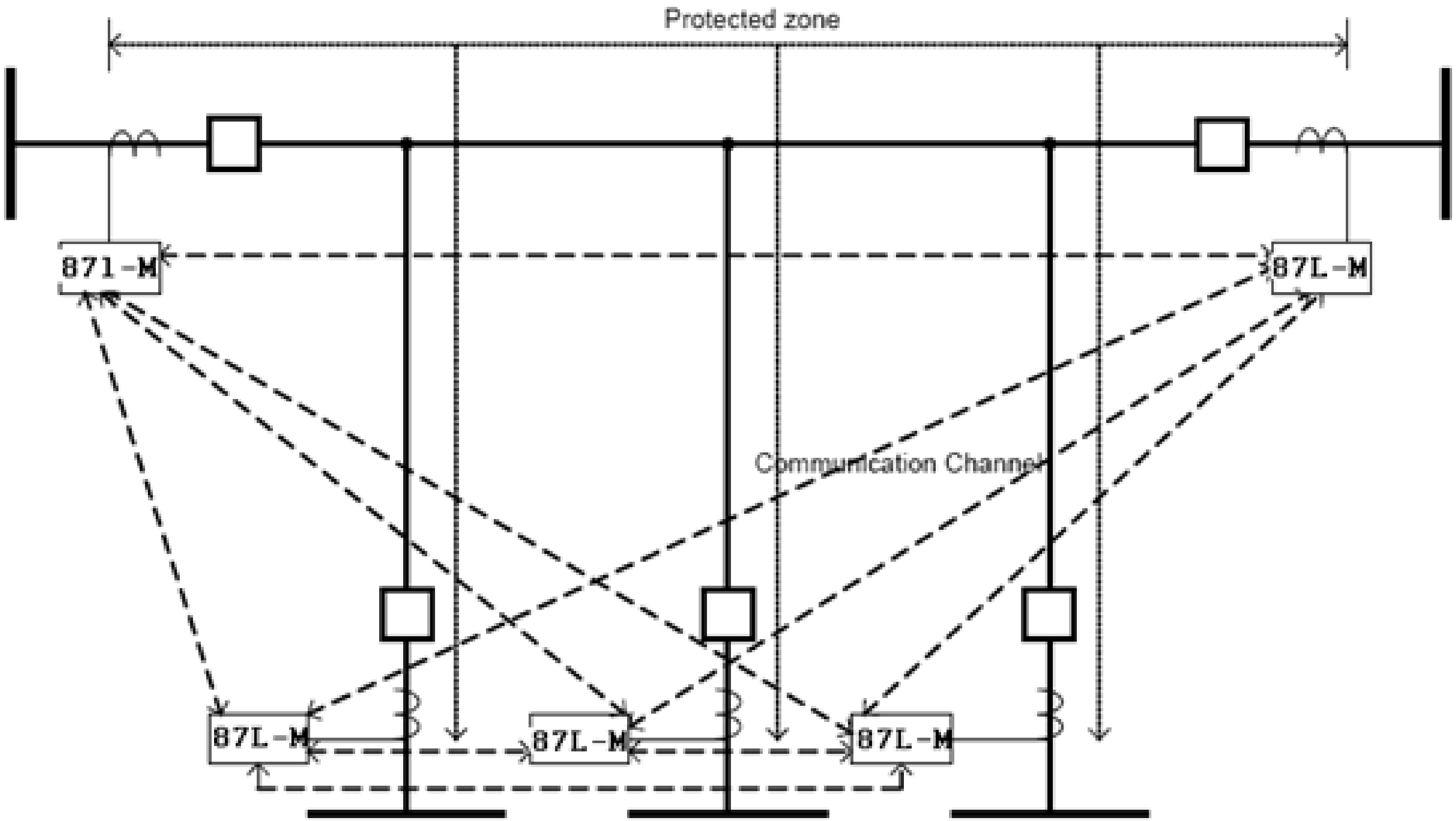
Outline

- The need to connect communications and protection
- Analysis of protection schemes dependencies on communications
  - Line current differential protection
  - Synchrophasor-based protection and control
  - Distributed generation related protection
  - Distance protection
  - Bus blocking scheme
- Conclusions

Introduction
The need to connect protection and communications

- Protection, control and communications often fall into responsibilities of different groups, with little or no communications and understanding
- This could have been sufficient for manually operated control and protection in traditional radial power systems
- Historically developments in communications lead to developments in protection, one can consider line differential protection
- On-going evolution leads to grids transformation into more diverse bi-directional systems with automated control and protection highly dependable on communications
- Lack of interactions and understanding between protection, control and communication engineers is no longer appropriate nor sufficient.

Line Current Differential Protection

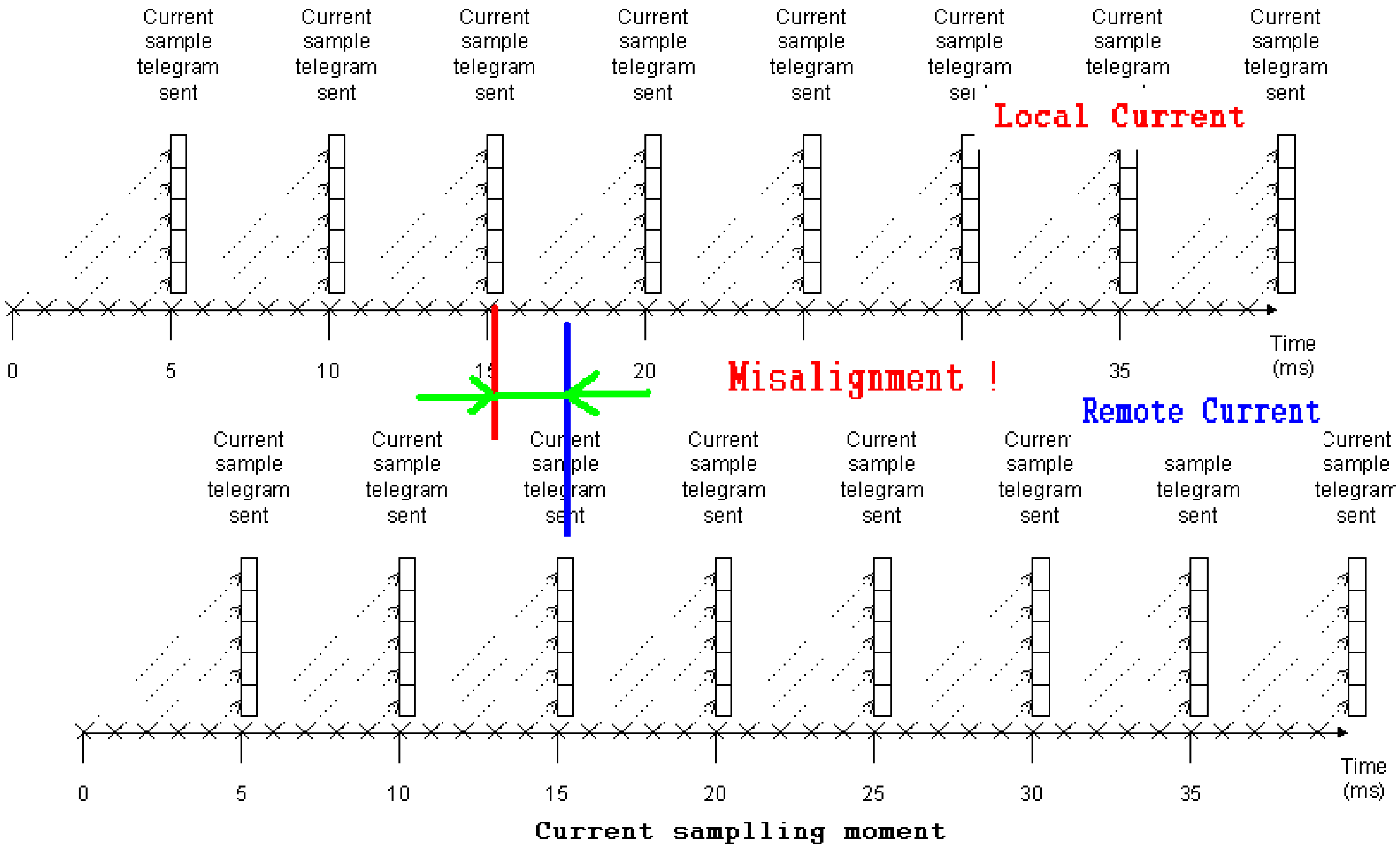


- Based on Kirchhoff's law for currents
- Uses synchronized current samples from 2 ends of the line
- 5 terminal system is shown
- Dedicated or multiplexed communication channels can be used

Line Current Differential Protection
Effect of Bit Errors

- Data corruptions in communication channel result in Bit Errors, and lead to discarding, i.e. loosing data
- Line current calculations can not be performed if data is not available
- Lost of one sample leads to operation delay of 1 sample period (e.g. 5ms)
- Lost of communication leads to blocking the protection scheme
- Rigorous requirements are imposed on Bit Error Rate (BER) of the communication channels used for line current differential protection
  - 10^{-12} - 10^{-9} during normal operation
  - 10^{-6} during disturbance
  - 10^{-4} when channel is blocked

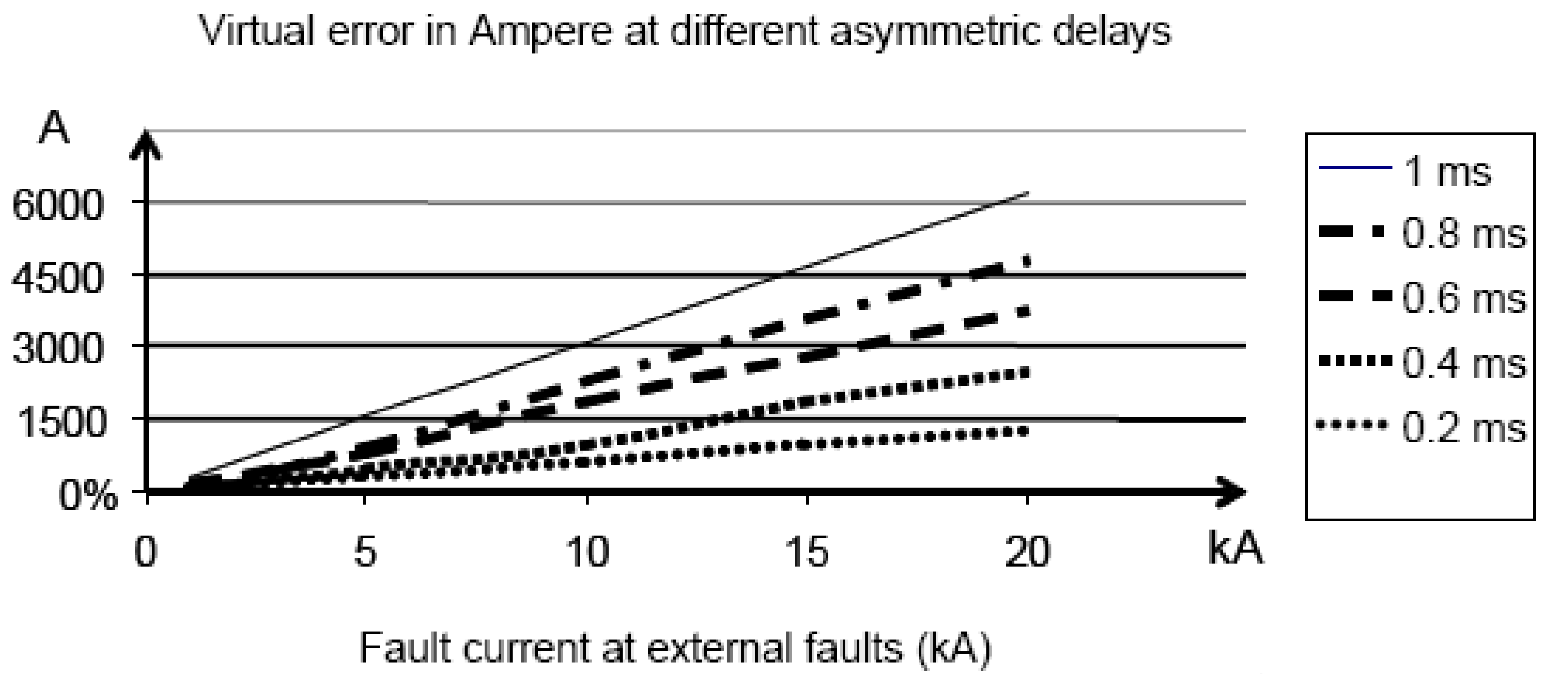
Line Current Differential Protection
Effect of Time Synchronization Error and Accuracy



Sum of currents at **the same time** is equal to 0

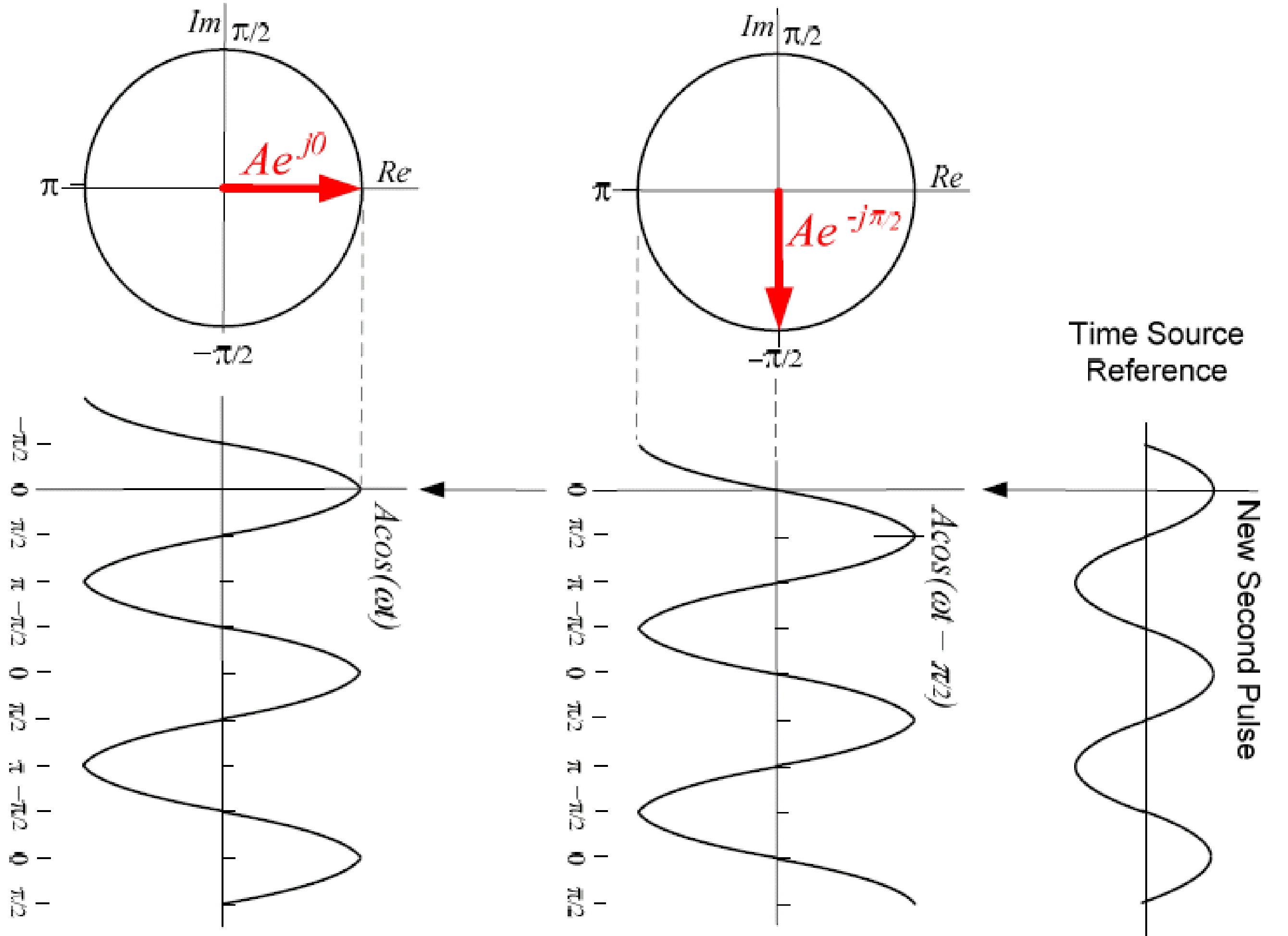
- Sample **times differ** => incorrect calculations and operation !
- Sample **times within expected range** => min operating current defined by time synchronization accuracy

Line Current Differential Protection
Effect of Delay Asymmetry



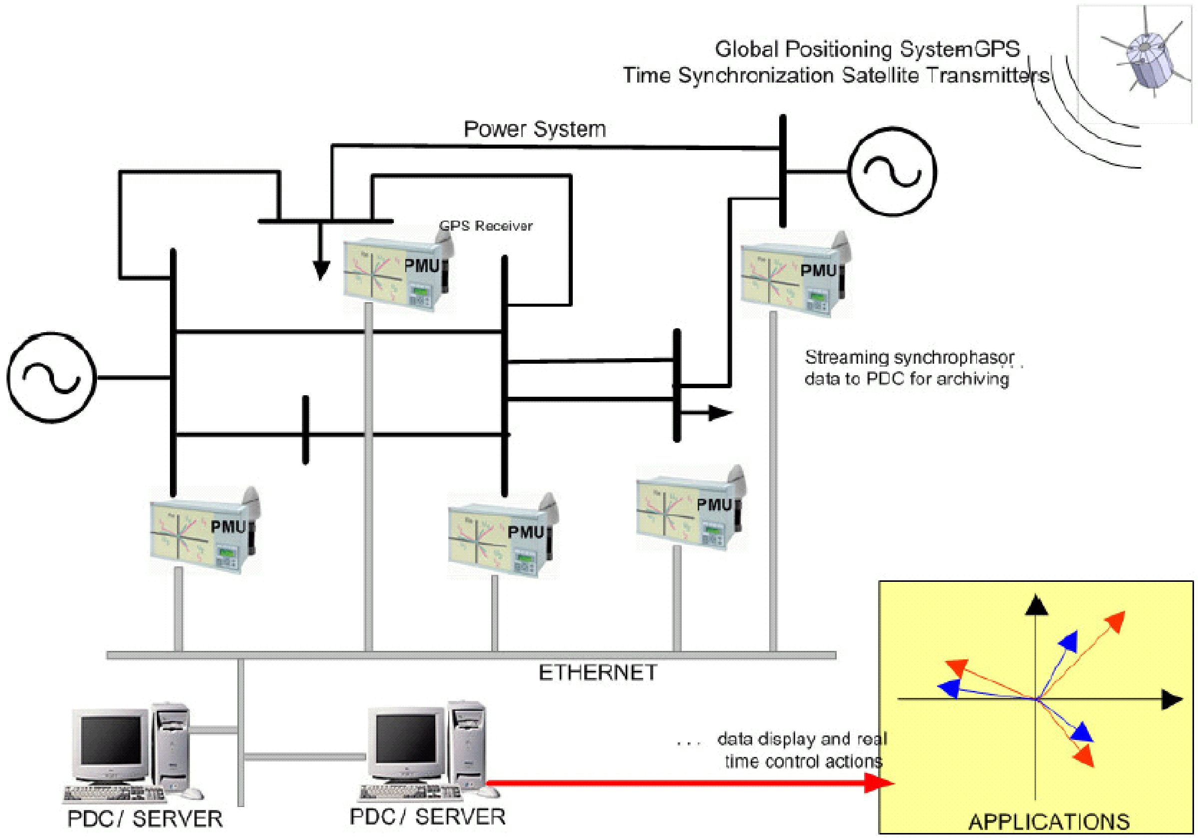
- If communication system is used for time synchronization, TX / RX delays assumed to be symmetrical
- Delay asymmetry translates directly into current measurement error

Synchrophasor-based protection and control



(a) $f(t) = A\cos(\omega t)$, $\theta = 0°$ (b) $f(t) = A\cos(\omega t - \pi/2)$, $\theta = -\pi/2$ (-90°)

Synchrophasor-based protection and control
Effect of one-way latency determinism



- Data is delayed by variable time prior to arrival to destination / application
- Telecommunication operators typically provide **average** not worst case delay
- Non-deterministic one-way latency can prevent correct calculations / decisions

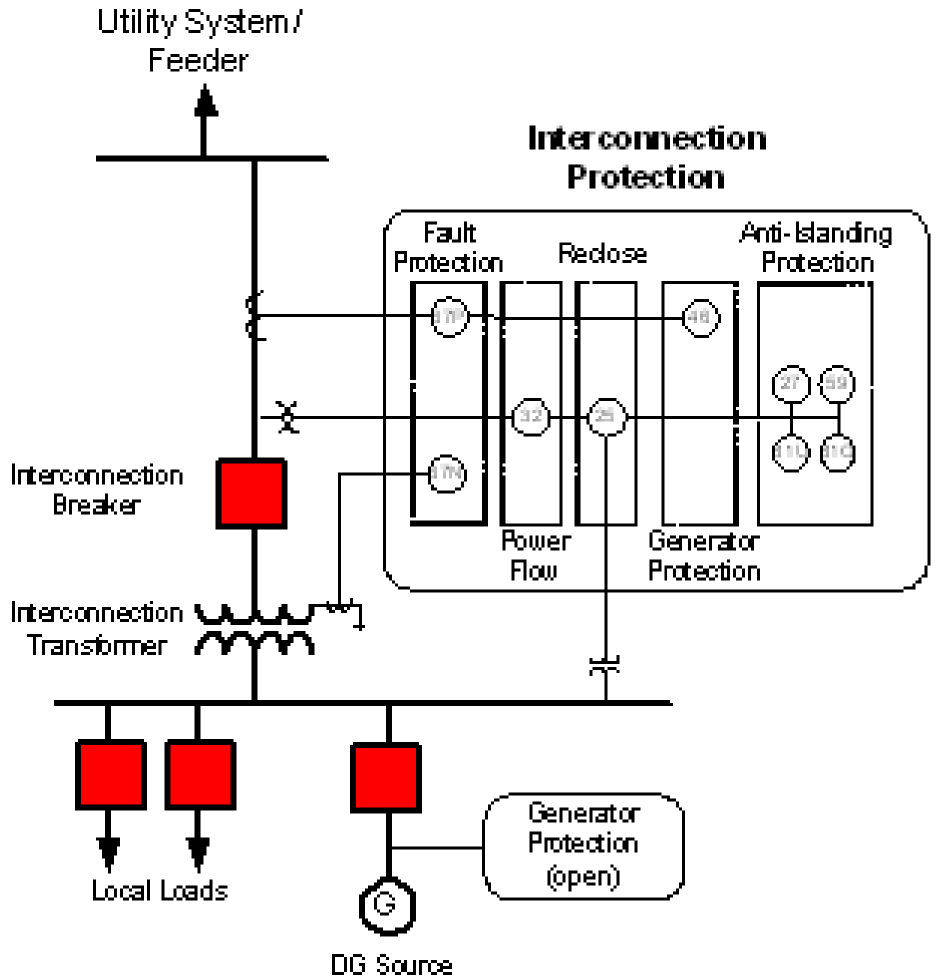
Synchrophasor-based protection and control
Effect of communication protocol

- Raw data are packed into telegrams or frames and packets for transmissions
- Protocols are the “rules” that define data exchange, what means what
- Reliable protocols, like Transport Control Protocol (TCP), establish a dedicated connection (connection-oriented) and use data receipt acknowledgements
- Non-reliable protocols, like User Datagram Protocol (UDP), don’t establish a dedicated connection (connection-less) and don’t confirm that data was received. They, however, can send same data to multiple destinations (multicast mode)

Synchrophasor-based protection and control
Effect of communication protocol

- Traditionally TCP has been used for synchrophasor data transmissions between one sender and one destination (unicast mode)
- Use of UDP is encouraged to enable multicast data transmissions, however UDP is not reliable and lead to data losses (not acceptable)
- Experiments and testing with UDP have shown that reliable no loss data communications is **possible** if end device buffers are specifically tuned
- Commands can still be transmitted over TCP (e.g. initiate / end data stream), while data can be transmitted over UDP
- New IEC 61850-90-5 Technical Report that specifies transmission of synchrophasor data over IEC 61850 systems only uses UDP

Distributed generation related protection



- Various protection schemes are used for systems with distributed generation
- These commonly include interconnection protection and feeder protection
- These schemes rely on communications to register DG presence, coordinate, etc

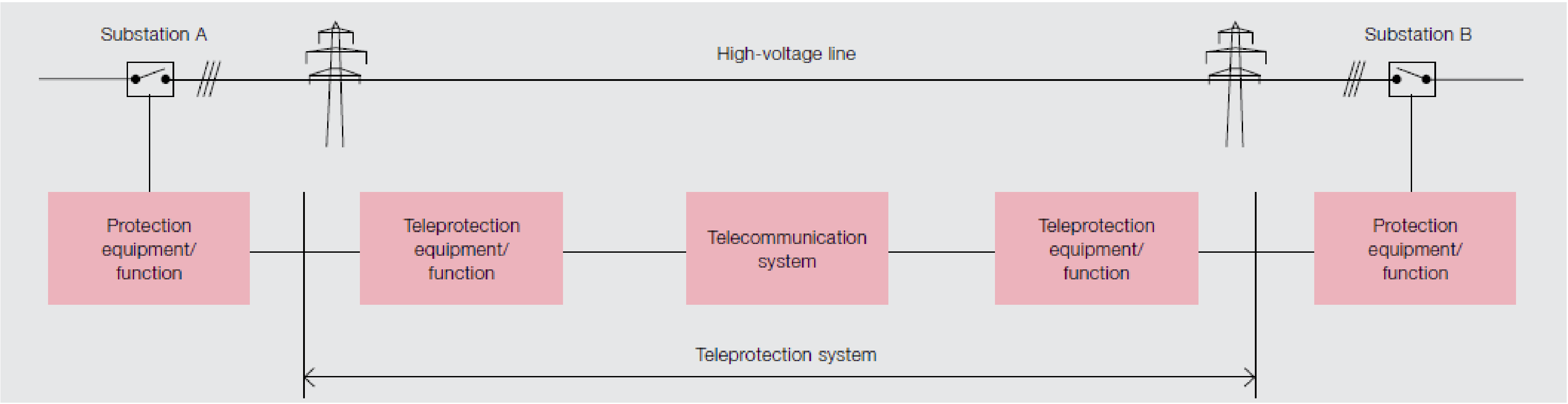
Distributed generation related protection
Effect of communication media

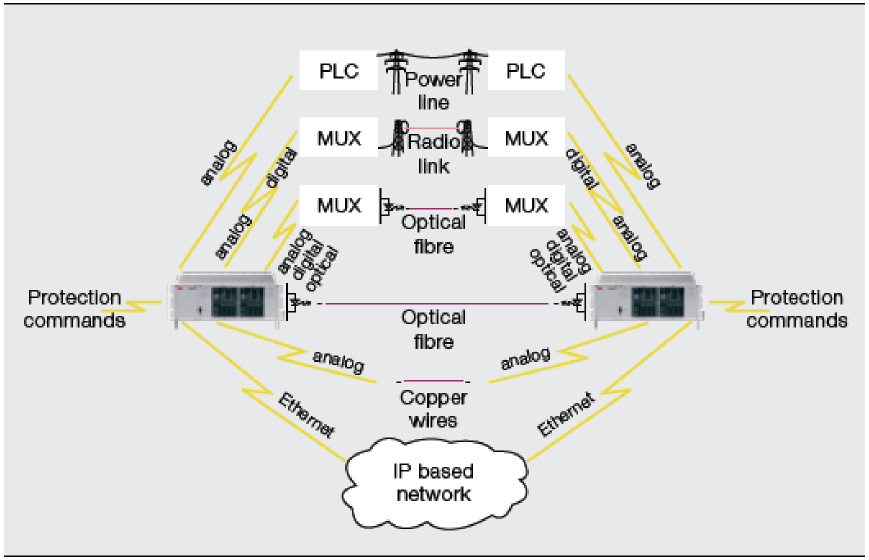
- IEC 61850 GOOSE messages could be used for coordination of protection schemes
- These short messages are mapped into Layer 2 Ethernet, use high priority and multicast mode (one message sent to many destinations)
- These messages can be transmitted over different media: fiber optic, electrical cable, or air (wireless)
- Testing conducted using WiMax wireless technology shown that some communication devices can not process GOOSE message “storm” without loosing data
- A specific older profile of WiMax technology was proven to work reliably

Distance Protection
Teleprotection Schemes

- Distance protection relays are the most common relays used for transmission line protection because it uses simple measuring principle.
- Distance protection can be performed without communications.
- In most cases, communication channels between the two ends are utilized to improve the performance of distance protection.
- Typically high voltage system faults are detected within 1-2 cycles, and are cleared within 5 cycles or 83 ms for 60Hz system.

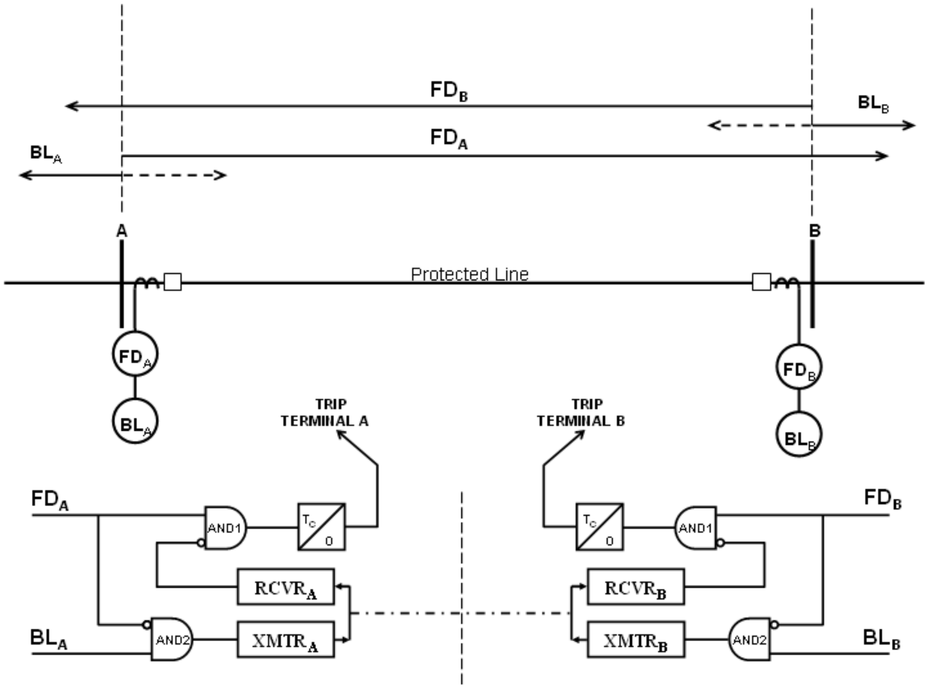
Distance Protection
Teleprotection Schemes





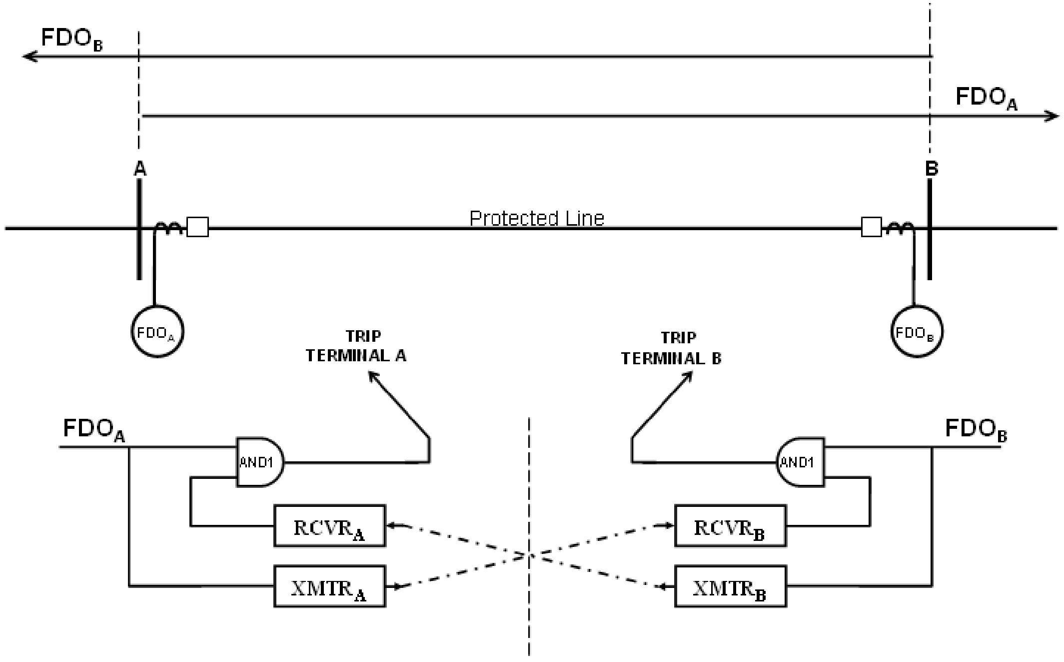
Distance Protection
Teleprotection Schemes

- There are two basic systems used for transmission line protection. The simplest is the directional comparison blocking (DCB) system. This system uses a blocking signal that is transmitted when the fault is outside of the transmission line protection zone, to prevent the remote end tripping for fault beyond the local terminal.



Distance Protection
Teleprotection Schemes

- Another system is the permissive system, which requires a signal from the remote end to give permission to trip for a fault. This system provides a continuous block or guard signal and shifts to a trip frequency to provide the permission. This is the frequency shift keyed (FSK) channel.



Distance Protection
Effect of communications performance

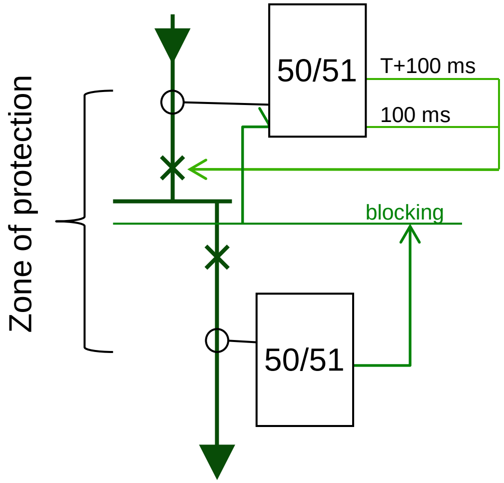
- Disturbances in the telecommunication channel must neither simulate a command at the receiving end when no corresponding command signal was transmitted (security), nor suppress a command that was actually transmitted (dependability).

- For digital channels:
  - Probability of an unwanted command, PUC, a measure of security, shall be less than 10^{-8}
  - Probability of missing command, PMC, a measure of dependability, shall be less than 10^{-2}
  - BER. The reliability of a protection command sent over a digital channel is related to bit errors.

Distance Protection
Effect of communications performance

Dependability	P_{mc} <	1E-02	1E-02	1E-03	1E-03	1E-04
Channel condition – Packet Loss Rate	PLR <	1%	2%	3%	10%	10%
Channel condition – Bit Error Rate	BER <	1.1E-05	2.3E-05	3.5E-05	1.2E-04	1.2E-04
Max. actual Transmission time	Tac ≤	4 ms	5 ms	6 ms	8 ms	10 ms

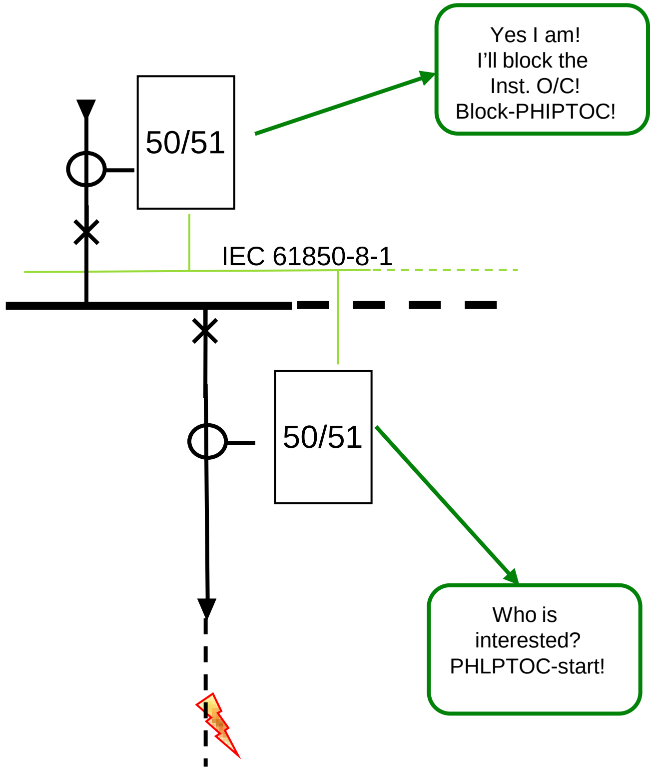
Bus Blocking Scheme



Delay setting with inst. O/C protection (conventional approach)	
Safety marginal, e.g. delay in operation due to CT saturation.	**20…40 ms**
O/C protection start delay + output relay's delay	**<40 ms**
Start delay with receiving relay + retarding time for the blocking signal *)	**<40 ms**
ALL TOGETHER	**100…120 ms**

- Traditional busbar protection is based on upstream blocking
  - Dedicated hard-wired signal paths needed
  - Signal path delay needs to be considered, input and output delay plus the delay in auxiliary relays
  - Changes in the protection scheme may require re-wiring
- Typically over 100 ms delay in the incoming feeder is needed

Bus Blocking Scheme
GOOSE message-based

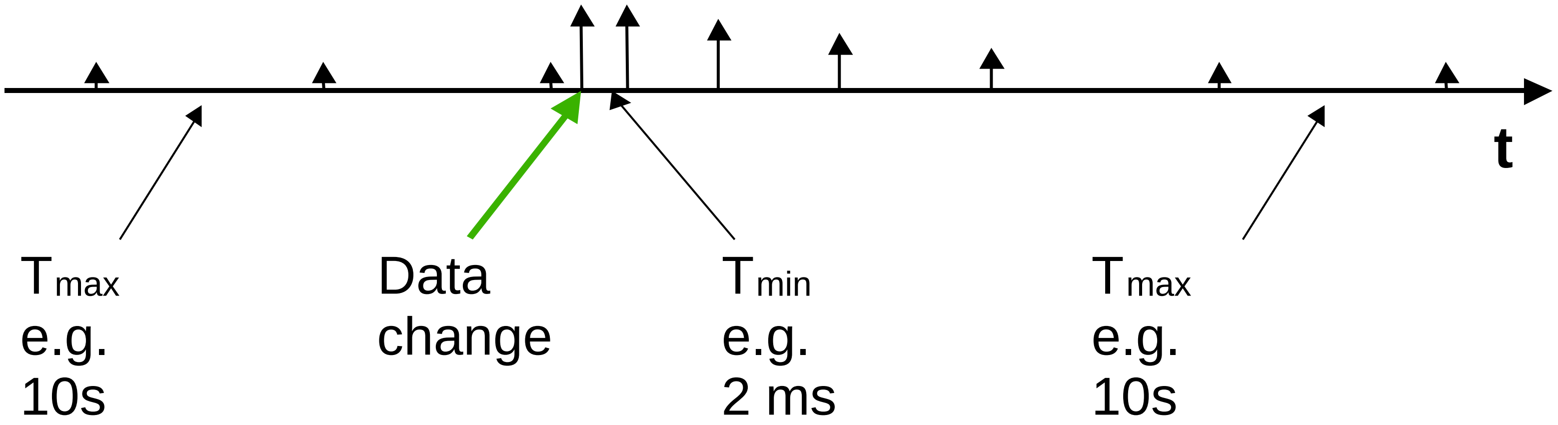


Delay setting with inst. O/C protection (GOOSE approach)	
Safety marginal, e.g. delay in operation due to CT saturation.	20…40 ms
O/C protection start delay	20 ms
Retardation time of inst. O/C stage blocking	5 ms
GOOSE delay (Type 1A, Class P1)	<10 ms
ALL TOGETHER	55…75 ms

Bus Blocking Scheme
Effect of communications performance

- Determinism
  - High-priority processing using Priority field in IEEE 802.1Q tag
  - Heartbeat and change-driven messages upon an event
  - Data multicasting (one to a group) and multiple re-transmissions
  - Bandwidth consumption should be taken into consideration when designing networks
- Redundancy
  - Rapid Spanning Tree Protocol (RSTP) ~5ms per network hop restoration time
  - Parallel Redundancy Protocol (PRP), no data lost
  - High-availability Seamless Redundancy Protocol (HSR), no data lost, typically used in ring topologies

Horizontal GOOSE communication
GOOSE data exchange



- The GOOSE communication link between the IEDs is supervised by sending data cyclically
- When data change is detected by an IED the event is immediately sent to the network multiple times to ensure reception of data
- In case of a timeout the application and the user are notified

Conclusions

- Evolving power grids become more dependable on communications, better interactions and understanding are required

- Dependencies of various protection schemes on communications were analyzed

- Effect of the following communication-related parameters was shows

  - Bit error rate
  - Time synchronization error and accuracy
  - Delay asymmetry, determinism of one-way latency
  - Communication protocol, media and profile
  - Probability of unwanted and wanted command

- Each of considered schemes deserves a separate in-depth investigation, further learning will benefit the industry