SUBSTATION AUTOMATION PRINCIPLES

By

Michael J Bergstrom
## DOCUMENT CONTROL

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Author</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>16/10/2009</td>
<td>0.1.0</td>
<td>Michael Bergstrom</td>
<td>First release for initial review</td>
</tr>
<tr>
<td>25/11/2009</td>
<td>0.1.1</td>
<td>Michael Bergstrom</td>
<td>Added Earth fault O/C protection</td>
</tr>
<tr>
<td>07/12/2009</td>
<td>0.1.2</td>
<td>Michael Bergstrom</td>
<td>Added GPS time synchronization</td>
</tr>
<tr>
<td>16/12/2009</td>
<td>0.2.0</td>
<td>Michael Bergstrom</td>
<td>Added communications stuff</td>
</tr>
<tr>
<td>01/06/2010</td>
<td>1.0</td>
<td>Michael Bergstrom</td>
<td>First full release</td>
</tr>
</tbody>
</table>
CONTENTS

1 INTRODUCTION ..........................................................5
2 THREE-PHASE FUNDAMENTALS ..................................6
3 DEFINITE TIME OVERCURRENT PROTECTION (DTOC) ...........11
4 INVERSE DEFINITE MINIMUM TIME OVERCURRENT PROTECTION (IDMT) .................................................................13
5 DIRECTIONAL OVERCURRENT PROTECTION .......................16
6 LIMITATIONS OF OVERCURRENT PROTECTION ....................18
7 GROUND FAULT OVERCURRENT PROTECTION ......................19
8 DIFFERENTIAL PROTECTION PRINCIPLES .........................20
8.1 Through-fault Stability in Differential Protection .................21
9 THREE-PHASE TRANSFORMER CONNECTION TYPES .............24
10 DIFFERENTIAL PROTECTION FOR THREE-PHASE TRANSFORMERS .26
11 TRANSFORMER INRUSH CURRENT ....................................27
12 RESTRICTED EARTH FAULT (REF) PROTECTION ..................30
13 GROUNDING TRANSFORMERS ........................................31
14 ZERO SEQUENCE CURRENT ...........................................32
15 BUSBAR PROTECTION ................................................33
16 DISTANCE PROTECTION ...............................................35
16.1 Effect of arcing on distance protection ............................37
17 GENERATOR PROTECTION ...........................................38
17.1 Stator phase and ground faults .....................................38
17.2 Stator inter-turn faults ...............................................39
17.3 Rotor faults ........................................................39
17.4 Unbalanced loading ..................................................40
17.5 Overspeeding .........................................................40
17.6 Loss of excitation ....................................................40
17.7 Loss of prime mover ......................................................... 40
18 GPS TIME SYNCHRONIZATION ........................................... 41
19 THE OSI MODEL ..................................................................... 44
20 IEC 61850 .................................................................................. 46
20.1 The need to standardize communications within substations 46
20.2 Benefits of IEC61850 .......................................................... 46
20.3 Structure of the IEC 61850 standard ................................. 48
20.4 The IEC 61850 data model ............................................... 49
20.5 Mapping IEC 61850 to a protocol stack ....................... 51
20.6 Substation Configuration Language .............................. 52
21 REDUNDANCY IN INDUSTRIAL ETHERNET NETWORKS ....... 53
21.1 Network topology types .................................................. 53
21.2 Principle of redundancy in communications .................. 54
21.3 Redundancy requirements for automation networks ..... 55
21.4 PRP ..................................................................................... 56
21.5 HSR ............................................................................... 58
22 CYBER-SECURITY ................................................................... 62
1 INTRODUCTION

This guide outlines some of the principles used in modern substation automation protection systems, as well as some of the underlying theory.
Power for distribution is generally produced with three-phase generators. Ideally, as in a balanced system, each phase is of equal voltage and displaced from each other by 120°. The voltage at the terminals can be measured with respect to the neutral point (centre of the star) or with respect to the other phase voltages. A three-phase supply and its generated voltages are shown in Figure 1.

![Three-phase supply](image)

Figure 1: Three-phase supply

In a three-phase system, there are two possible sequences in which the voltages pass through their maximum positive values: A-B-C, or A-C-B. By convention, we define the sequence A-B-C as the positive sequence, where the vectors travel in an anti-clockwise direction. The sequence A-C-B, where the vectors travel in a clockwise direction is by convention the negative sequence.

The 120° angle between the three phases can be conveniently described by a complex operator 'a', where:

\[ a = 1\angle120° = -\frac{1}{2} + \frac{\sqrt{3}}{2}j \]

Further, we can derive:

\[ a^2 = 1\angle240° = -\frac{1}{2} - \frac{\sqrt{3}}{2}j \quad \text{and} \quad a^3 = 1\angle360° = 1 \]

Note that the operation –a does not turn a complexor through -120°. It turns it through -60° as shown below:

\[ -a = a \times (-1) = 1\angle120° \times 1\angle180° = 1\angle300° = 1\angle-60° \]

Thus we can derive the general equation: \( a^2 + a + 1 = 0 \)

Using the principles described above, it is possible to calculate following:

\[ V_{AB} = \sqrt{3}V_{\text{phase}} \angle 30° \]

where \( V_{\text{phase}} \) is the magnitude of the phase voltage with respect to neutral. Likewise:

\[ V_{BC} = \sqrt{3}V_{\text{phase}} \angle -90° \quad \text{and} \quad V_{CA} = \sqrt{3}V_{\text{phase}} \angle 150° \]

In each case, the line voltage is \( \sqrt{3} \) times the phase voltage in magnitude and leads the corresponding phase voltage by 30°.
Balanced star-connected load

Applying Kirchoff's law, \( I_N = I_A + I_B + I_C = I_A + a^2 I_A + a I_A = (1+a^2 + a)I_A = 0 \)

Therefore, if there is a neutral connection to the star point, the current in it will be zero for a balanced system. Sometimes the neutral wire is dispensed with; this is a three-wire system.

Balanced delta-connected load

In a balanced delta system, the magnitude of each line current is \( \sqrt{3} \) times the phase current and lags the corresponding phase current by 30°.

Unbalanced 4-wire star-connected load

With an unbalanced 4-wire star-connected node, the imbalance manifests itself in the flow of a neutral current, where:
\[ I_N = I_A + I_B + I_C = \frac{V_A}{Z_A} + \frac{V_B}{Z_B} + \frac{V_C}{Z_C} \]

**Unbalanced 3-wire star-connected load**

The unbalanced three-wire star-connected load is fairly difficult to deal with. One method is to apply the star-mesh transformation to the load and then deal with it as for an unbalanced delta-connected load. A second method is to apply Maxwell's mesh equations to the system. Both methods can be simplified by Millman's theorem.

Using Millman's theorem, the voltage of the load neutral point (N') with respect to the generator neutral point (N) is given by:

\[ V_{NN} = \frac{V_A Y_A + V_B Y_B + V_C Y_C}{Y_A + Y_B + Y_C} \text{ where } Y \text{ is the load admittance.} \]

Thus we have:

\[ V_{AN'} = V_A - V_{NN} \]
\[ V_{BN'} = V_B - V_{NN} \]
\[ V_{CN'} = V_C - V_{NN} \]

And:

\[ I_{AN'} = (V_A - V_{NN})Y_A \]
\[ I_{BN'} = (V_B - V_{NN})Y_B \]
\[ I_{CN'} = (V_C - V_{NN})Y_C \]
Unbalanced delta-connected load

With an unbalanced delta-connected load, the full line voltages equal in magnitude and separated by 120° in phase appear across each load phase.

The equations in this case are as follows:

\[ I_1 = \frac{V_{AB}}{Z_1} \]
\[ I_2 = \frac{V_{AB}}{Z_2} \]
\[ I_3 = \frac{V_{CB}}{Z_1} \]

**Note the use of parallelograms to resolve quantities in the phasor diagram.**

**Symmetrical components**

Any unbalanced three-phase system may be represented by a balanced set of positive sequence components, a balanced set of negative sequence components and a set of three currents equal in phase and magnitude. This is demonstrated in fig below.
Figure 7: Symmetrical components

The original unbalanced currents may be expressed in terms of A-phase symmetrical components as follows:

\[
I_A = I_{A+} + I_{A-} + I_{A0}
\]
\[
I_B = a^2I_{A+} + aI_{A-} + I_{A0}
\]
\[
I_C = aI_{A+} + a^2I_{A-} + I_{A0}
\]

The symmetrical components may also be expressed in terms of the unbalanced system as follows:

\[
I_{A0} = \frac{1}{3}(I_{A+} + I_{A-} + I_{A0})
\]
\[
I_{A+} = \frac{1}{3}(I_A + I_B + a^2I_C)
\]
\[
I_{A-} = \frac{1}{3}(I_A + a^2I_B + aI_C)
\]

The ability to break down an unbalanced system into symmetrical components gives us a very powerful tool for analyzing fault currents. In particular, where source impedance needs to be taken into account, this method must be used if the source is a synchronous machine or a transformer supplied by the synchronous machine. This is because in the case of a synchronous machine, the impedance to positive phase sequence currents is different from its impedance to negative phase sequence currents.

The main use of the symmetrical components method is therefore for the analysis of 3-phase networks under asymmetrical fault conditions.
DEFINITE TIME OVERCURRENT PROTECTION (DTOC)

Definite Time Overcurrent (DTOC) protection is one of the simplest types of protection. A DTOC protection device (IED) can be adjusted to issue a trip command at a defined time delay after it detects the fault current. It therefore has two adjustable settings; one for the pick-up current (the current at which the minimum fault current is defined) and one for the delay time (the time between the device recognizing the fault current and issuing a trip command). In a DTOC IED, the operate time is dependent on just these two settings and is independent of the level of overcurrent beyond the minimum pick-up current. The characteristic time/current curve of an ideal DTOC IED is shown in Figure 1. In reality the curve is slightly inverse, but for the sake of clarity, the idealized curve is shown here.

Figure 1: Idealized DTOC time/current curve

There are two basic requirements to bear in mind when designing protection schemes:

- The fault should be cleared as quickly as possible
- The fault clearance should result in minimum disruption to the electrical power grid

The second requirement means that the protection scheme should be designed such that only the circuit breaker(s) in the protection zone where the fault occurs, should trip. These two design requirements can be in conflict and this inevitably results in a compromise when using DTOC IEDs for a protection scheme of this nature, as will be shown.

Figure 2 depicts one phase of a three-phase feeder with two line sections AB and BC, and loads at all three buses. IED A controls CB A (circuit breaker A), providing protection for Bus A, while IED B controls CB B, providing protection for Bus B.

Figure 2: DTOC IEDs in a radial feeder

Consider a ground fault between B and C (Fault BC). The fault current flows from the source to the fault at BC, passing through line section A-B first. Our design requirements dictate that only CB B should open as this is the only circuit breaker that is required to open in order to isolate the fault. We also require that this circuit breaker open as quickly as possible, so the IED should react immediately...
and without delay. The problem is that the fault current also passes through CB A, which means we run the risk of shutting off the healthy section A-B. We therefore have to detect and isolate the fault before CB A has had time to react. The only way of doing this is by incorporating an intentional time delay into IED A, which is at least as long as the operate time of IED plus the rupture time of CB B.

From the above-described design principles and simplified example, it is clear that for a radial supply, the IED furthest away from the source should trip with minimum delay, whilst subsequent IEDs towards the source should incorporate appropriate increasing time delays to ensure they do not trip in response to faults covered by IEDs further down the line. This logic would yield our desired result, ensuring that the IED in the fault zone clears the fault before IEDs further up the line have time to respond.

DTOC IEDs are relatively simple and thus cost effective devices, and are used widely for protection schemes where the line is ‘electrically short’, i.e. the impedance does not change significantly from the power source to the end of the line. In this example, however, we shall assume that the line is ‘electrically long’, i.e. the impedance increases significantly from the source to the far end of the line. This means the nearer the fault is to the power source, the greater the fault current, as depicted by the curve directly underneath the line diagram in Figure 2. Although the scheme logic satisfies the criteria as far as fault localization is concerned, it is not desirable that the higher fault currents take longer to clear.

We can conclude that for ‘electrically long’ lines, DTOC IEDs are not the correct devices to use and we should consider using IDMT (Inverse Definite Minimum Time) IEDs for such cases.
4 INVERSE DEFINITE MINIMUM TIME OVERCURRENT PROTECTION (IDMT)

There are two basic requirements to bear in mind when designing protection schemes:

1. All faults should be cleared as quickly as possible to minimize damage to equipment
2. Fault clearance should result in minimum disruption to the electrical power grid.

The second requirement means that the protection scheme should be designed such that only the circuit breaker(s) in the protection zone where the fault occurs, should trip.

These two criteria are actually in conflict with one another, because to satisfy (1), we increase the risk of shutting off healthy parts of the grid, and to satisfy (2) we purposely introduce time delays, which increase the amount of time a fault current will flow. This problem is exacerbated by the nature of faults in that the protection devices nearest the source, where the fault currents are largest, actually need the longest time delay.

The old electromechanical relays countered this problem somewhat due to their natural operate time v. fault current characteristic, whereby the higher the fault current, the quicker the operate time. The characteristic typical of these electromechanical relays is called Inverse Definite Minimum Time or IDMT for short. There are three well-known flavors of this characteristic, as defined by IEC 60255:

- Inverse
- Very inverse
- Extremely inverse

The equations and corresponding curves governing these characteristics are very well known in the power industry and are summarized below. The characteristics of these three curves are plotted in Figure 1.

**Inverse**

The curve is very steep. The relay can operate at low values of fault current, but at high fault currents has a significant operate time. The inverse characteristic equation is as follows:

\[ t_{op} = T \frac{0.14}{\left( \frac{I}{I_s} \right)^{0.02} - 1} \]

**Very Inverse**

The curve lies somewhere between inverse and extremely inverse. The inverse characteristic equation is as follows.

\[ t_{op} = T \frac{13.5}{\left( \frac{I}{I_s} \right)^{1} - 1} \]

**Extremely Inverse**

The curve is very shallow. The relay does not operate at very low values of fault current, but operates very quickly at high levels of fault current.
\[ t_{op} = T \left( \frac{80}{I \left( \frac{I}{I_s} \right)^2} \right) - 1 \]

In the above equations:

- \( t_{op} \) is the operating time
- \( T \) is the time multiplier setting
- \( I \) is the measured current
- \( I_s \) is the current threshold setting.

The ratio \( I/I_s \) is sometimes defined as 'M' or 'PSM' (Plug Setting Multiplier).

The above three curves, plotted in Figure 1 are defined in IEC 60255 and are very well known, however with the advent of modern numerical IEDs, it is possible to define whatever inverse curve is required according to the more general equations:

\[ t_{op} = \left( \frac{T \beta}{M^\alpha - I} \right) + C \]

Where the constants \( \beta, \alpha \) and \( C \) are constants to be defined as required (\( C \) is the definite time adder, which is zero for the three standard IEC curves).

IEEE/ANSI standard curves differ slightly from the IEC curves in that the Time Multiplier Setting is replaced by a Time Dial Setting, plus there is a possibility of adding a further constant \( L \) into the equation thus the IEEE/ANSI standard equation is:

\[ t_{op} = \left( TD \frac{\beta}{M^\alpha - I} + L \right) + C \]

Figure 1: IEC 60255 IDMT curves
Table 1 Shows the constant values for a wider selection of standard curves:

<table>
<thead>
<tr>
<th>Curve Description</th>
<th>Standard</th>
<th>β constant</th>
<th>α constant</th>
<th>L constant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Inverse</td>
<td>IEC</td>
<td>0.14</td>
<td>0.02</td>
<td>0</td>
</tr>
<tr>
<td>Very Inverse</td>
<td>IEC</td>
<td>13.5</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Extremely Inverse</td>
<td>IEC</td>
<td>80</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Long Time Inverse</td>
<td>UK</td>
<td>120</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Rectifier</td>
<td>UK</td>
<td>45900</td>
<td>5.6</td>
<td>0</td>
</tr>
<tr>
<td>Moderately Inverse</td>
<td>IEEE/ANSI</td>
<td>0.0515</td>
<td>0.02</td>
<td>0.114</td>
</tr>
<tr>
<td>Very Inverse</td>
<td>IEEE/ANSI</td>
<td>19.61</td>
<td>2</td>
<td>0.491</td>
</tr>
<tr>
<td>Extremely Inverse</td>
<td>IEEE/ANSI</td>
<td>28.2</td>
<td>2</td>
<td>0.1217</td>
</tr>
<tr>
<td>Inverse</td>
<td>US</td>
<td>5.95</td>
<td>2</td>
<td>0.18</td>
</tr>
<tr>
<td>Short Time Inverse</td>
<td>US</td>
<td>0.16758</td>
<td>0.02</td>
<td>0.11858</td>
</tr>
</tbody>
</table>

Table 1: IDMT curve constants

Figure 2 depicts one phase of a three-phase feeder with two line sections AB and BC, and loads at all three buses. IED A controls CB A (circuit breaker A), providing protection for Bus A, while IED B controls CB B, providing protection for Bus B.

In this example, if we were to use DTOC IEDs, it would be necessary to program IED A with a delay time to prevent it from tripping before IED B. For a fault at AB, which is nearer the source and thus subject to a larger fault current, the IED A would trip only after an imposed delay, thus allowing the fault current to flow for a longer time than is desirable.

Use of an IDMT IED at A would alleviate this problem. For a fault at BC, IED A is prevented from tripping first not due to the set time delay but because of the IDMT characteristic. The fault current at this point is relatively low, so the operate time of IED A is relatively long, allowing IED B to trip first. However, for a fault current at AB, the IED trips quickly because the fault current is relatively high.

So now you can see that by using an IDMT IED at A, we can satisfy both of our desired criteria, namely that the IED nearest the fault is guaranteed to trip first AND the IEDs nearer the source trip quickly for faults, which are local to them.
5 DIRECTIONAL OVERCURRENT PROTECTION

The electrical power grid comprises a network of power stations, substations and transmission lines. As well as the simple single-end-fed radial system, there are other more complex systems such as double-end-fed power systems and parallel feeders in ring formation. In many cases, it is therefore not only necessary to know the magnitude of the fault current, but also its direction.

A double-end-fed radial system is shown in Figure 1. In this example, the line is fed from both ends. The protection zones are indicated by ellipses. The requirement is to open all breakers in any one protection zone where the fault occurs, but none of the others.

![Figure 1: Double-end-fed system](image)

In this example, it is impossible to set up an adequate protection scheme using non-directional protection devices. Consider a fault $F_{CS}$. As defined by the zones, only CBs 4 and 5 should trip. As CB 3 is in close proximity to CB 4, there would be no great difference in fault current flowing through these two circuit breakers, therefore IDMT IEDs would not be able to discriminate between them. The same situation applies for CB 5 and CB 6. This means that by using non-directional devices, CBs 3, 4, 5 and 6 would trip in the event of a fault at $F_{CS}$.

It is clear then that we need a device that is capable of detecting the direction of the fault current as well as its magnitude. Directional overcurrent protection devices can achieve this requirement, albeit at extra cost. Directional IEDs determine the direction of the fault current by measuring the voltage with a voltage transformer as well as the current with a current transformer, and establishing the phase difference. This section does not go into details of exactly how this is achieved, but it can be seen that it is possible to determine the direction of the fault current and base a tripping decision on this criterion.

Consider again a fault at $F_{CS}$. This time let us assume we have directional IEDs. If we configure the IEDs to trip for overcurrents only if the direction of the current flow is away from the bus, CB 4 and CB 5 will trip, but CB 3 and CB 6 will not.

To summarize: The overcurrent IED should trip whenever the fault power flows away from the bus, but should restrain whenever the fault power flows towards the bus.

There are other situations, which do not involve dual sources, where directional protection devices are necessary. One example is for a single-end fed system of parallel feeders. Figure 2 shows a situation where a fault on one of the parallel lines is fed from both the faulted line and the healthy one too.

![Figure 2: Parallel feeders in single-end-fed system](image)

This diagram shows that a fault current will not only flow from the source, through CB 4, but also from the source, through CB 1, CB 2, Bus B and CB 3. If non-directional IEDs are used, all circuit breakers will trip, thus isolating the healthy section of line between (1) and (2). This problem can be solved by introducing directional IEDs at (2) and (3). If the tripping direction is set such that they will trip when...
the fault is away from the bus, only the CBs in the required zone will trip. In the example above, CB 2 will not trip as the fault is flowing towards the bus. Directional IEDs are more expensive than non-directional ones. What is more, they necessitate the use of an additional voltage transformer. For these reasons, they should only be used when absolutely necessary. You can see by inspection that in this example, non-directional IEDs will suffice for positions (1) and (4).

Another example where directional IEDs are called for is in a ring main feeder system, as depicted in Figure 3. Such a system allows supply to be maintained to all loads in spite of a fault on any section of the feeder. A fault in any section causes only the CBs associated with that section to trip. Power then flows to the load through the alternative path.

The directional IEDs and their tripping direction are indicated by arrows in the diagram. The double-ended arrows indicate non-directional IEDs, as these will trip with currents flowing in either direction.

Figure 3: Protection of ring feeder using directional overcurrent IEDs
6 LIMITATIONS OF OVERCURRENT PROTECTION

The reach and operating time of overcurrent protection devices are dependent on the magnitude of the fault current, which is in turn dependent on the type of the fault (ground or phase) and the source impedance. Neither the type of fault nor the source impedance are predictable quantities, which means that the reach of overcurrent IEDs is also subject to variations resulting in loss of selectivity. This loss of selectivity can be tolerated to some extent in low voltage distribution systems, where the only objective is the continuity of supply to the consumer. However in EHV systems, loss of selectivity can result in grid instability and large disruption to the loads. Overcurrent protection devices should not be relied upon as a primary means of protection in EHV systems. Another protection philosophy called distance measurement should be used for this purpose. Distance measurement offers much more accurate reach, which is independent of source impedance and fault type.
7 GROUND FAULT OVERCURRENT PROTECTION

In a three-phase system, there are three types of ground faults:

- L-G: Single phase-to-ground
- L-L-G: Phase-to-phase-to-ground
- L-L-L-G: Phase-to-phase-to-phase-to-ground

By far the most common of these are single phase-to-ground faults. Consequently, this is the first and foremost type of fault that protection devices must cover.

Ground fault protection can be obtained by using a protection device that responds only to residual currents in a system. The ground fault IED is therefore completely unaffected by load currents or phase-to-phase faults. This is demonstrated by considering Figure 4.

![Figure 4: Residual ground fault current](image)

Consider a single phase-to-ground fault on the C-phase, as shown in the first of the two diagrams above. By inspection and applying electrical circuit theory, it is clear to see that the fault current (and only the fault current) is reflected in the phase C current transformer and that this current circulates through the IED and CT_C, causing the IED to trip.

If however, the fault does not go to ground as shown in the second of the diagrams, the fault current will not pass through the IED and therefore will not cause the IED to trip.

A phase-phase-ground fault will produce circulating currents such that the phase-ground component will circulate through the IED, whereas the phase-phase component will not. The same principle applies to phase-phase-phase-ground faults.

Typical settings for ground fault IEDs are around 30-40% of the full load current. If greater sensitivity is required, then Sensitive Ground Fault (also known as Sensitive Earth Fault or SEF) should be used.

This needs finishing
8 DIFFERENTIAL PROTECTION PRINCIPLES

Although nowadays differential protection is achieved numerically, in order to understand the principles of differential protection it is useful to analyze the ubiquitous electromechanical relay. Figure 1 shows a simple differential protection scheme, also known as a Merz-Price scheme.

![Simple differential protection diagram](image)

**Figure 1:** Simple differential protection

In this simple scheme, we can assume that under normal operating conditions, the current entering into the piece of equipment under protection is equal (or in the case of a transformer, proportional) to its exiting current. In this example we will assume that the entry and exit currents are equal. A circuit breaker either side of the equipment under protection is controlled by an overcurrent relay. Current transformers of identical types and turns ratio are installed on either side of the equipment. These current transformers induce identical secondary currents, because their primary currents are identical and they have the same turns ratio. By simple inspection of the diagram, it is clear to see that under these circumstances no spill current will flow through the relay, therefore no trip signals will be generated.

Consider a fault internal to the equipment. A large current would flow through the fault, thus the current exiting the equipment would rapidly reduce resulting in a reduced secondary current in CT B. This would cause a current to flow through the relay, which would be of a magnitude sufficient to trip the circuit breakers.

Now consider an external fault at F as shown in Figure 2.

![Simple differential protection with external fault diagram](image)

**Figure 2:** Simple differential protection with external fault

You can see that in this case, the current exiting the equipment, albeit large, is still the same as the current entering it, therefore the relay will not trip. This is exactly as how we want it, because faults external to the equipment are in a different protection zone and are protected within another scheme.

If the equipment to be protected is a busbar, or generator winding, for instance, it is clear that the exit current is the same as the entry current. If, however, the equipment is a transformer where the turns
ratio is not equal to one, the current entering will be different from the current exiting. In this case, the current transformers must be balanced with an equivalent turns ratio differential.

The differential scheme creates a well-defined protection zone, encompassing everything between the two current transformers. Any fault existing in this protection zone is regarded as an internal fault, while any fault existing outside this protection zone is an external fault. A differential scheme should therefore be able to respond to the smallest of internal faults, but restrain on the largest of external faults. In practice, this is difficult to achieve, especially for very large through faults, due to the non-ideal nature of the current transformers used to measure the currents. The term used to specify the system’s ability to cope with these imperfections is called Through-fault Stability. For a discussion on this aspect, see Through-fault Stability in Differential Protection.

In modern IEDs, the current in the current transformers do not directly control the operating coil which trips the circuit breakers, so the connectivity is not as it is shown in this example. In reality, the currents from the current transformers are simply input to the IED, where they are sampled and digitized. The differential operation is then carried out by the IED’s software.

8.1 Through-fault Stability in Differential Protection

With differential protection, everything between the protecting current transformers is in the protection zone and everything outside of the current transformers is outside the protection zone. We require the protection to operate only for faults within the protection zone. Further, we need this protection to be sensitive due to the low-current nature of some of the types of fault associated with the equipment within the protection zone.

In an ideal current transformer, its secondary current is either in phase or 180° out of phase with its primary current, depending on which way you define its direction. For the sake of convention, let us say it is out of phase by 180°. This is because the primary current induces a secondary voltage which lags the primary current by 90°, and this voltage induces a secondary current, which lags the secondary voltage by 90°. In reality the windings, cables, and components have real resistive components, which introduce a tangible phase shift. The exact amount of phase shift introduced by the real world is not possible to predict, therefore the phase shift of one current transformer will more than likely be different from that of the other. Furthermore, the magnitudes of the respective secondary currents will more than likely be slightly different too, even if they are nominally the same. This results in a small spill current \( I_{\text{spill}} \) (see Differential Protection Principles). This spill current increases as the magnitude of the primary current increases. This is best described in the form of the phasor diagrams shown in Figure 1.

![Figure 1: Spill current due to CT errors](image)

From this diagram, it is plain to see that for imperfect current transformers, the larger the primary current, the larger the spill current.

A fault outside the protection zone is likely to cause a very large current to travel through the transformer. This is known as a through-fault because we require that the transformer pass this fault current through. We do not want the differential protection to operate under these circumstances. The fault should be cleared by a protection scheme relevant to the zone in which the fault occurs.

The problem is that as this through-fault current in the primary goes on increasing, the discrepancies introduced by the imperfect CTs are magnified, causing the spill current to build up. Eventually, the value of the spill current will reach the pickup current threshold, causing the IED to trip. This is a case
of maloperation because an out-of-zone fault has caused the IED to trip. In such cases, the differential scheme is said to have lost stability. To specify a differential scheme’s ability to restrain from tripping on external faults, we define a parameter called ‘through-fault stability limit’, which is the maximum through-fault current a system can handle without losing stability. Figure 2 demonstrates the through-fault stability characteristic.

![Figure 2: Through-fault stability](image)

It is useful to define one further parameter with respect to stability. That is the stability ratio, which is defined as follows:

\[
\text{Stability ratio} = \frac{I_{\text{stab}}}{I_{\text{pickup}}}
\]

Differential protection is often used in the case of transformers and busbars. In the case of transformers, the turns ratio is not usually 1:1, therefore the turns ratio of the CT transformer on one side of the equipment will be different from that of the other side. This exacerbates the CT errors, making current differential protection unusable in its simplest form.

For busbars, the ‘equipment’ to be protected is simply a conductive busbar, so the entry and exit currents are the same, resulting in the use of current transformers either side with the same turns ratio. Although in the case of busbars the CTs are matched, busbars are subject to very high through-fault currents. This also means that simple differential schemes are not adequate.

In order to understand the principles of through-fault compensation, it is useful to analyze the electromechanical relay. For EM relays, the problems of through-fault instability can be overcome with the use of Percentage Differential Protection. This technique makes use of a further coil, split into two with a centre tapping, as shown in Figure 3.

![Figure 3: Compensation using restraining coils](image)
A detailed discussion of how through-fault stability is achieved using restraining coils is not considered necessary here, as these days IEDs do the job for us using software.

The way a modern IED achieves this is by using a transformer biased differential characteristic. Very often a triple slope characteristic is used as shown in Figure 4. Further details about this technique are described in the relevant product documentation.

Figure 4: Compensation using biased differential characteristic
There are four basic types of connection for a six-winding, three-phase transformer as follows:

- Y-Y (also known as Wye-Wye)
- Y-Δ (also known as Y-D or Wye-Delta)
- Δ-Y (also known as D-Y or Delta-Wye)
- Δ-Δ (also known as Delta-Delta)

To differentiate between the low and high voltage sides of the transformer, a standard convention has been adopted whereby lower case is used for the low voltage side and upper case I used for the high voltage side. The convention also requires that the low voltage side be called the primary and the high voltage the secondary, irrespective of the position of the transformer relative to the nearest generator.

Not only can the primary and secondary be connected as a star or a delta, each phase can also be reversed resulting in a large choice of possible connections. In reality, however, only a few of these are used, because we generally require that the phase shifts between the primary windings and their secondary counterparts be consistent. This reduces the common connection types to those shown in Table 1.

You will notice that the naming convention specifying the connection type in the first column also has a number appended to it. This number, called the clock face vector, represents the phase shift between the current in a high voltage winding with respect to its counterpart on the secondary side. The clock face vector is literally the position of the number of a standard clock face (Midnight, 1 o’clock, 6 o’clock and 11 o’clock), which is equivalent to a phase shift of 0°, -30°, -180° and +30° respectively.

The Main Group Number, or Vector Group is an IEC60076-1 categorization of the phase angles. For example, all connections with phase shift -30° are in group number 3.

<table>
<thead>
<tr>
<th>Connection type</th>
<th>Phase shift</th>
<th>Clock face vector</th>
<th>Main Group No.</th>
<th>Phase compensation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yy0</td>
<td>0°</td>
<td>0</td>
<td>1</td>
<td>Not required</td>
</tr>
<tr>
<td>Dd0</td>
<td>0°</td>
<td>0</td>
<td>1</td>
<td>Not required</td>
</tr>
<tr>
<td>Yd1</td>
<td>-30°</td>
<td>1</td>
<td>3</td>
<td>+30°</td>
</tr>
<tr>
<td>Dy1</td>
<td>-30°</td>
<td>1</td>
<td>3</td>
<td>+30°</td>
</tr>
<tr>
<td>Yy6</td>
<td>-180°</td>
<td>6</td>
<td>2</td>
<td>+180°</td>
</tr>
<tr>
<td>Dd6</td>
<td>-180°</td>
<td>6</td>
<td>2</td>
<td>+180°</td>
</tr>
<tr>
<td>Yd11</td>
<td>+30°</td>
<td>11</td>
<td>4</td>
<td>-30°</td>
</tr>
<tr>
<td>Dy11</td>
<td>+30°</td>
<td>11</td>
<td>4</td>
<td>-30°</td>
</tr>
</tbody>
</table>

Table 1: Transformer connection types

Reduces the risk of large fines due to non-compliance (1 trillion euros per second)
<table>
<thead>
<tr>
<th>Symbol</th>
<th>HV winding</th>
<th>LV winding</th>
<th>Winding connection</th>
<th>Phase shift</th>
<th>Vector group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yy0</td>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
<td><img src="image3.png" alt="Image" /></td>
<td>0°</td>
<td>1</td>
</tr>
<tr>
<td>Dd0</td>
<td><img src="image4.png" alt="Image" /></td>
<td><img src="image5.png" alt="Image" /></td>
<td><img src="image6.png" alt="Image" /></td>
<td>0°</td>
<td>1</td>
</tr>
<tr>
<td>Yy6</td>
<td><img src="image7.png" alt="Image" /></td>
<td><img src="image8.png" alt="Image" /></td>
<td><img src="image9.png" alt="Image" /></td>
<td>180°</td>
<td>2</td>
</tr>
<tr>
<td>Dd6</td>
<td><img src="image10.png" alt="Image" /></td>
<td><img src="image11.png" alt="Image" /></td>
<td><img src="image12.png" alt="Image" /></td>
<td>180°</td>
<td>2</td>
</tr>
<tr>
<td>Dy1</td>
<td><img src="image13.png" alt="Image" /></td>
<td><img src="image14.png" alt="Image" /></td>
<td><img src="image15.png" alt="Image" /></td>
<td>-30°</td>
<td>3</td>
</tr>
<tr>
<td>Yd1</td>
<td><img src="image16.png" alt="Image" /></td>
<td><img src="image17.png" alt="Image" /></td>
<td><img src="image18.png" alt="Image" /></td>
<td>-30°</td>
<td>3</td>
</tr>
<tr>
<td>Dy11</td>
<td><img src="image19.png" alt="Image" /></td>
<td><img src="image20.png" alt="Image" /></td>
<td><img src="image21.png" alt="Image" /></td>
<td>+30°</td>
<td>4</td>
</tr>
<tr>
<td>Yd11</td>
<td><img src="image22.png" alt="Image" /></td>
<td><img src="image23.png" alt="Image" /></td>
<td><img src="image24.png" alt="Image" /></td>
<td>+30°</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 2: Transformer winding connections
10 DIFFERENTIAL PROTECTION FOR THREE-PHASE TRANSFORMERS

For 3-phase transformer differential correction to work properly, the outputs of the current transformers on both sides of the system transformer must be nominally equal not just in magnitude, but also in phase. Depending on the type of connection used, there will be a phase displacement of the quantities between the voltages HV and LV sides of the system transformer. If left uncorrected, this would result in a spill current and consequent maloperation.

It is possible to compensate for this phase shift by connecting the current transformers on the LV side in the same arrangement as the HV windings of the system transformer, and the current transformers on the HV side to match that of the LV windings of the system transformer. This method is used for electromechanical relays and other simple types of protection device without numeric computational abilities. Figure 1 demonstrates this type of connection. You can see that the system transformer is of a delta-star arrangement (Dy1). Therefore the current transformers on the HV side are connected in a star arrangement and the current transformers on the LV side are connected in a delta arrangement.

Further, the magnitude differences between the HV and LV sides due to the chosen turns ratio can also be compensated for by having the same ratio for the current transformers but in reverse. So if the system transformer has a turns ratio of n:1 where n refers to the HV side, the current transformers on the LV side will have n more turns than that of their counterparts on the HV side.

Modern IEDs can handle these phase and magnitude differences quite conveniently in software, so there is no need to overcomplicate the current transformer connectivity. The current transformers are usually connected in a Y configuration on both sides of the system transformer irrespective of its winding type. The measured currents are fed into the IED, where they are sampled and digitized. Phase compensation is then carried out by the IED's software, as is the differential calculation.
11 TRANSFORMER INRUSH CURRENT

When a transformer is initially connected to a source of AC voltage, there may be a substantial surge of current through the primary winding called inrush current. This is analogous to the inrush current exhibited by an electric motor that is started up by sudden connection to a power source, although transformer inrush is caused by a different phenomenon.

We know that the rate of change of instantaneous flux in a transformer core is proportional to the instantaneous voltage drop across the primary winding, i.e. the voltage waveform is the derivative of the flux waveform, and the flux waveform is the integral of the voltage waveform. In a continuously-operating transformer, these two waveforms are phase-shifted by 90°. Since flux ($\Phi$) is proportional to the magnetomotive force (MMF) in the core, and the MMF is proportional to winding current, the current waveform will be in-phase with the flux waveform, and both will be lagging the voltage waveform by 90°. This is shown in Figure 1.

![Figure 1: Phase relationships of v, i, and $\Phi$](image)

Let us suppose that the primary winding of a transformer is suddenly connected to an AC voltage source at the exact moment in time when the instantaneous voltage is at its positive peak value. This is shown in Figure 2. In order for the transformer to create an opposing voltage drop to balance against this applied source voltage, a magnetic flux of rapidly increasing value must be generated. The result is that winding current increases rapidly, but actually no more rapidly than under normal operating conditions. Both core flux and coil current start from zero and build up to the same peak values experienced during continuous operation. Thus, there is no "surge" or "inrush" or current in this scenario.
Alternatively, let us consider what happens if the transformer's connection to the AC voltage source occurs at the exact moment in time when the instantaneous voltage is at zero. During continuous operation (when the transformer has been powered for quite some time), this is the point in time where both flux and winding current are at their negative peaks, experiencing zero rate-of-change ($\frac{d\Phi}{dt} = 0$ and $\frac{di}{dt} = 0$). As the voltage builds to its positive peak, the flux and current waveforms build to their maximum positive rates-of-change, and on upward to their positive peaks as the voltage descends to a level of zero.

A significant difference exists, however, between continuous-mode operation and the sudden starting condition assumed in this scenario. During continuous operation, the flux and current levels were at their negative peaks when voltage was at its zero point. In a transformer that has been sitting idle, however, both magnetic flux and winding current would start at zero. When the magnetic flux increases in response to a rising voltage, it will increase from zero upwards, not from a previously negative (magnetized) condition as would be the case for a transformer that is already powered up. Thus, in a transformer that is just starting up, the flux will reach approximately twice its normal peak magnitude as it integrates the area under the voltage waveform's first half-cycle. This is demonstrated in Figure 3.

In an ideal transformer, the magnetizing current would rise to approximately twice its normal peak value as well, generating the necessary MMF to create this higher-than-normal flux. However, most transformers are not designed with enough of a margin between normal flux peaks and the saturation
limits to avoid saturating in a condition like this, and so the core will almost certainly saturate during this first half-cycle of voltage. During saturation, disproportionate amounts of MMF are needed to generate magnetic flux. This means that winding current, which creates the MMF to cause flux in the core, could rise to a value way in excess of its steady state peak value. Furthermore, if the transformer happens to have some residual magnetism in its core at the moment of connection to the source, the problem could be further exacerbated.

Impact of inrush current on protection scheme

We can see that inrush current is a regularly occurring phenomenon and should not be considered a fault, as we do not wish the protection device to issue a trip command whenever a transformer is switched on at an inconvenient time point during the input voltage cycle. This presents a problem to the protection device, because it should always trip on an internal fault. The problem is that typical internal transformer faults may produce overcurrents which are not necessarily greater than the inrush current. Furthermore faults tend to manifest themselves on switch on, due to the high inrush currents. For this reason, we need to find a mechanism that can distinguish between fault current and inrush current. Fortunately this is possible due to the different natures of the respective currents. An inrush current waveform is rich in harmonics, whereas an internal fault current consists only of the fundamental. We can thus develop a restraining method based on the harmonic content of the inrush current. The mechanism by which this is achieved is beyond the scope of this discussion.
12 RESTRICTED EARTH FAULT (REF) PROTECTION

Winding-to-core faults in a transformer are quite common due to insulation breakdown. Such faults can have very low fault currents, but they are faults nevertheless and have to be picked up. Often the fault currents are lower than the nominal load current. Clearly, neither overcurrent nor percentage differential protection is sufficiently sensitive in this case. We therefore require a different type of protection arrangement. Not only should the protection arrangement be sensitive, but it must create a protection zone, which is limited to the transformer windings. Restricted Earth Fault protection satisfies these conditions.

Figure 1 shows an REF protection arrangement for the delta side of a delta-star transformer. The current transformers measuring the currents in each phase are connected in parallel. A fault outside the protection zone (i.e. outside the delta winding) will not result in a spill current, as the fault current would simply circulate in the delta windings. However, if any of the three delta windings were to develop a fault, the impedance of the faulty winding would change and that would result in a mismatch between the phase currents, resulting in a spill current, sufficient to trigger a trip command.

Figure 1: REF protection for delta side

Figure 2 shows an REF protection arrangement for the star side of a delta-star transformer. Here we have a similar arrangement of current transformers connected in parallel. The only difference is that we need to measure the zero sequence current in the neutral line as well. We know that an external unbalanced fault causes zero sequence current to flow through the neutral line, resulting in uneven currents in the phases, which would cause the IED to maloperate. By measuring this zero sequence current and placing the current transformer in parallel with the other three, the currents are balanced up resulting in stable operation. Now only a fault inside the star winding can create an imbalance sufficient to cause the IED to issue a trip command.

Figure 2: REF protection for star side
13 GROUNDING TRANSFORMERS

Star-delta transformers are usually used when stepping down from a high voltage to a low voltage. We know that delta connected transformers have no neutral point. This inherent characteristic is usually undesirable for various reasons, one of which is the effect of zero sequence current. On the star side, a fault current causes zero sequence current to flow from the star point to neutral. The zero sequence current obviously induces a zero sequence component on the delta side, but the delta winding cannot deliver this current to ground. For this reason it is necessary to have an earthing transformer (neutral grounding transformer).

Figure 1 shows a star-delta transformer with connected earthing transformer.

![Earthing Transformer Diagram]

Figure 1: Earthing transformer
14 ZERO SEQUENCE CURRENT

On a Y-connected three phase winding, the star point, also known as Neutral, is generally grounded, (either solidly or through an impedance). Under balanced conditions, no current flows through the neutral wire to ground. A fault where all three phases are grounded is known as a balanced fault, because although there is a fault current flowing from each phase to ground, there is still no current flowing in the neutral line.

If there is a fault from one phase to another, or from one phase to ground, the system becomes unbalanced. This is known as an unbalanced fault. Under these circumstances the imbalance causes a current to flow between the neutral point and ground. This neutral current is called Zero Sequence Current.

In star-delta transformer arrangements, the delta side has no star point and therefore no neutral line. An unbalanced fault on the star-side results in a flow of zero sequence current. This zero sequence current is reflected on the delta-side in the form of an additional current component flowing through the transformer windings. Assuming the transformer has differential protection, this could cause the protection to maloperate, because the fault is likely to be outside the protection zone. We therefore need to filter out this zero sequence current component. Today this filtering is achieved with software algorithms within the IED.

Needs further explanation?

Kind of covered this in symmetrical components bit – combine?
Busbars are the nerve centers of the power system. This is where power lines are connected together in a substation. Essentially a bus bar is a robust and highly conductive metal framework, onto which power lines are connected. Figure 1 depicts a busbar protection zone. The main principle behind busbar protection is that under non-fault conditions, the sum of all currents coming into the busbar must equal the sum of all currents going out of the busbar, as shown in the equation:

$$\sum_{k=1}^{N_{in}} I_{in_k} = \sum_{m=1}^{N_{out}} I_{out_m}$$

Where $N_{in}$ is the number of incoming lines and $N_{out}$ is the number of outgoing lines.

Busbars can pass current from a large number of lines, so a fault on the busbar could result in an extremely large fault current resulting in enormous damage. Faults on busbars are generally rare, but because of the extreme consequence in the event of failure, it is generally wise to provide dedicated protection for them.

Because the connections to busbars are close together, differential protection offers the best solution for busbar protection. We need only to compare the sum of the incoming currents with the sum of the outgoing current and see if there is a difference.

Fault currents external to the protection zone will not cause a spill current, providing the current transformers are operating within their linear operating range. However, if an external fault current is large enough to cause a current transformer to go into saturation, a spill current will be caused by the imbalance, resulting in maloperation.

To prevent this occurring, a stabilizing resistance is necessary. This stabilizing resistor limits the current in the current transformers to a level such that it stays within its operating range. This is called High impedance Figure 2 shows the principle of a high impedance scheme.
Figure 2: High impedance scheme
16 DISTANCE PROTECTION

Simple forms of overcurrent protection have the advantage of being simple and cost effective, but they have one major disadvantage; they are prone to maloperation. This is acceptable for low voltage distribution (LV systems), because the only thing at risk is continuity of supply to consumers. Although inconvenient to the consumer, this risk is considered acceptable. EHV systems on the other hand, are part of a large and complex interconnected grid, where maloperation of protection devices can severely jeopardize grid stability. Major cascading blackouts, as recently seen in Europe and the USA, are examples of what can happen when electrical power grids become unstable. It is therefore essential that a more reliable form of protection is implemented on EHV systems.

The “reach” of an IED is defined as the maximum electrical distance at which the IED should operate. This may vary from a few meters to a few kilometers, depending on the type of protection that the designated IED is assigned to.

The reach of an overcurrent IED is dependent on several factors, but the one we need to consider here is the line impedance. Because the line impedance increases the further the fault is away from the source, the fault current decreases correspondingly. Now, a three-phase fault will give rise to a larger fault current than a Line-Line-Ground (L-L-G) fault in the same location, due to its higher voltage. Likewise, an L-L-G fault will give rise to a larger fault current than an L-G fault.

The fault current versus distance characteristic of all three fault types is shown in Figure 1.

![Figure 1: Fault type reach](image)

Figure 1: Fault type reach

Now it becomes clear that the reach of an IED is dependant on fault type, in addition to other factors such as source impedance. So if we wish to set the reach such that the IED protects fault in the region of the busbar B, depending on the fault type, it may well underreach, in which case the required circuit breaker will not trip, or overreach, in which case we may cause a circuit breaker outside the protection zone to trip.

We therefore need a protection principle where the reach does not depend on the absolute magnitude of the fault current, but on the magnitude of the fault current in relation to the voltage at the IED location. This is possible under the following circumstances

1. We know the nominal line impedance per unit length of line
2. We can measure both the voltage and the current at the IED location

Fortunately, both these criteria can be satisfied. The nominal line impedance per unit length is a known quantity, and it is possible to measure the voltage at the IED location using a voltage transformer. So from this, we can accurately define the reach point by defining an impedance $Z_{set}$ at the point where you wish to place your reach point, where $Z_{set} = |V_{IED}| / |I_{IED}|$. 
From this, we can define a Trip Law that can be written in several different ways:

\[
\text{If } |V_{\text{IED}}| < |V_{\text{set}}| \text{ then trip else restrain}
\]

\[
\text{If } \frac{|V_{\text{IED}}|}{|I_{\text{IED}}|} < |Z_{\text{set}}| \text{ then trip else restrain}
\]

\[
\text{If } |Z_{\text{IED}}| < |Z_{\text{set}}| \text{ then trip else restrain}
\]

where \( Z_{\text{IED}} \) is the magnitude of the impedance seen by the IED.

The IED will compute the impedance as seen from its location and compare it with the set value in order to take a trip decision. The resistance and inductance (i.e. the impedance) of a transmission line is directly proportional to the length of the line, therefore the impedance of a faulted line as seen from the IED is directly proportional to the distance of the fault from the IED. This is why this type of protection is called distance protection and the element of the IED responsible for this function is called a Distance Protection element.

Figure 2 demonstrates the above ideas. It depicts a length of line with faults at various places, being controlled by an impedance IED.

![Figure 2: Faults at various points in the line](image)

Three fault points have been drawn; F1 (within the reach zone), F2 (the extent of the reach zone and F3 (beyond the reach zone). For convenience, the line impedance is split up into its component parts and into 3 separate regions as shown. This nicely demonstrates the linearly increasing line impedance with line length. The line impedances to the three faults are summarized as follows:

\[
Z_{F1} = R_1 + jX_1 = R_1 + j\omega L_1
\]

\[
Z_{F2} = (R_1 + R_2) + j(X_1 + X_2) = (R_1 + R_2) + j\omega (L_1 + L_2)
\]

\[
Z_{F3} = (R_1 + R_2 + R_3) + j(X_1 + X_2 + X_3) = (R_1 + R_2 + R_3) + j\omega (L_1 + L_2 + L_3)
\]

In this example, we have set the impedance element to \( Z_{\text{set}} \) such that the IED’s protection zone is between the two Busbars A and B.

It is convenient to plot the IED characteristic on the Real/Imaginary plane, as shown in Figure 3. Here we can see that the IED should trip if the fault lies within the circle and restrain if it is outside.
16.1 **Effect of arcing on distance protection**

Many faults involve arcing of some kind, where electricity jumps from a high voltage point to a lower voltage point through air. This is not a zero impedance short-circuit path. It actually offers a significant resistance. The arc path resistance is described by the well-known Warrington formula shown below:

\[
R_{arc} = \frac{8750(S + 3ut)}{I^{1.4}}
\]

Where S is the spark-over distance (in feet), u is the wind velocity in mph, t is the time of the arc in seconds and I is the fault current.

This arc resistance alters the impedance of the line by adding a resistive component to it.

It becomes apparent by inspecting the modified characteristic, arc resistance would cause a simple impedance relay to underreach, as depicted by the triangular section just outside the trip zone.
17 GENERATOR PROTECTION

Generators in the context of power transmission are very large and expensive bits of equipment, and their protection presents a special challenge. A lot of things can go wrong with a generator, both electrical and mechanical and, if not properly protected, can result in expensive damage.

A generator is subject to several different types of fault, initiated either electrically, mechanically or by abnormal operating conditions. The main types of fault are as follows:

- Stator phase fault
- Stator ground fault
- Stator inter-turn fault
- Rotor ground fault
- Unbalanced loading
- Loss of excitation in rotor field winding
- Loss of prime mover
- Overspeeding

17.1 Stator phase and ground faults

Stator phase and ground faults can be easily detected using differential protection. In the context of Generator protection, this type of protection is referred to as longitudinal differential protection. This is shown in Figure 1.

![Figure 1: Longitudinal differential protection](image)

Although longitudinal differential protection is suitable for detecting stator ground and phase faults, it cannot be used for stator inter-turn faults. For that you need transverse differential protection.
17.2 Stator inter-turn faults

In order to adequately detect stator inter-turn faults, the stator winding must consist of two parallel windings as shown in

![Stator Winding Diagram](image)

Figure 1: Transverse differential protection

The stator winding is split into two identical parallel windings. Under normal operation, the differential current induced in the current transformers will be identical, thus there is no spill current to initiate a trip signal. If, however, there is an inter-turn fault, this will result in a current differential, resulting in a spill current, which in turn will initiate a trip signal.

Questions for Graeme.

Why can't longitudinal be used to detect inter-turn faults?

Are all generator stator windings split?

Do we have 18 CTs protecting generator stators? (12 for ground and phase and 6 for inter-turn?)

17.3 Rotor faults

The rotor's field winding is electrically isolated from the ground. A ground fault on the field winding will therefore not affect the functioning of the generator. A further ground fault, on the other hand would cause a section of the field winding to be shorted. This would result in an uneven flux distribution, causing instability in the rotary speed. The resulting asymmetry can cause severe vibrations of the rotor resulting in catastrophic damage.

For this reason, it is necessary to detect the first instance of rotor ground fault and trip the breaker before any damage can take place. We can achieve this by superimposing a DC voltage onto the rotor circuit as shown in

As this DC voltage is referenced to ground, a ground fault in the field winding causes a DC current to flow, which can easily be detected by a simple overcurrent IED. This is demonstrated in
17.4 Unbalanced loading

If the generator loads are unbalanced, this results in a negative sequence current component in the stator windings. This negative sequence component produces a magnetic field component that rotates in the opposite direction of the steady state rotating magnetic field, which is in phase with the field of the rotor. The velocity of the field caused by the negative sequence component relative to the rotating field in the rotor is thus double that of the regular field. This causes double frequency currents to be induced in the rotor conductors causing overheating.

Now we know that the power generated in a resistor is equal to $I^2R$. Therefore the heat generated in the rotor is proportional to $I_2^2 R t$ where $I_2$ is the offending negative sequence current, $R$ is the resistance of the rotor/stator and $t$ is the time for which the negative sequence current is present.

Assuming the value of $R$ to be constant, the thermal characteristic of the machine follows the equation:

$$I_2^2 t = K$$

We can also express this in the time flow which the offending current can flow is equal to:

$$t = \frac{K}{I_2^2}$$

This characteristic is similar to that of an extremely inverse time overcurrent relay. To protect against unbalanced loading then, we need to extract the negative sequence current with a negative sequence filter, and feed this into an IDMT protection IED with suitable inverse characteristic.

Look in book of effect of unbalanced loads

17.5 Overspeeding

17.6 Loss of excitation

17.7 Loss of prime mover
18 GPS TIME SYNCHRONIZATION

When dealing with real-time systems, an accurate and reliable time reference is required. Luckily, modern society is blessed with a Global Positioning System (GPS) that offers this functionality. There are several geostationary satellites in orbit around the earth, providing all the measurement information necessary for identifying a position anywhere on the earth. These satellites also contain ultra-accurate atomic clocks all synchronized with one another. A clock signal from any one of these satellites is sufficient to provide an accurate time reference for any real time system.

Figure 1 illustrates a typical GPS time-synchronized substation application. The satellite RF signal is picked up by a satellite dish and passed on to receiver. The receiver receives the signal and converts it into time signal suitable for the substation network. IEDs in the substation use this signal to govern their internal clocks and event recorders.

![Figure 1: IRIG-B architecture](image)

In 1956 the American Inter Range Instrumentation Group standardized the different time code formats. These were published in the IRIG Document 104-60. This was revised in 1970 to IRIG Document 104-70, and published later as IRIG Standard 200-70. The latest publication is 200-98.

The name of an IRIG code format consists of a single letter plus 3 subsequent digits. Each letter or digit reflects an attribute of the corresponding IRIG code. The following tables contain the meanings of the suffixes and descriptions of the abbreviations used.

<table>
<thead>
<tr>
<th>Suffix position</th>
<th>Suffix description</th>
<th>Suffix</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>First letter</td>
<td>Format</td>
<td>A</td>
<td>1000 PPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B</td>
<td>100 PPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>D</td>
<td>1 PPM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>E</td>
<td>10 PPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>G</td>
<td>10000 PPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>H</td>
<td>1 PPS</td>
</tr>
<tr>
<td>First digit</td>
<td>Modulation Frequency</td>
<td>0</td>
<td>DC Level Shift, width coded, no carrier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>Sine wave carrier, amplitude modulated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>Manchester Modulated Code</td>
</tr>
<tr>
<td>Second digit</td>
<td>Frequency/Resolution</td>
<td>0</td>
<td>No carrier/index count interval</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>100 Hz / 10 milliseconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>1 kHz / 1 milliseconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>10 kHz / 100 microseconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>100 kHz / 10 microseconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>1 MHz / 1 microsecond</td>
</tr>
</tbody>
</table>

© Alstom Grid

Author: Michael Bergstrom
### Table 3: Serial time code formats

<table>
<thead>
<tr>
<th>Suffix position</th>
<th>Suffix description</th>
<th>Suffix</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third digit</td>
<td>Coded expressions</td>
<td>0</td>
<td>( BCD_{TOY}, CF, SBS )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>( BCD_{TOY}, CF )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>( BCD_{TOY} )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>( BCD_{TOY}, SBS )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>( BCD_{TOY}, BCD_{YEAR}, CF, SBS )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>( BCD_{TOY}, BCD_{YEAR}, CF )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>( BCD_{TOY}, BCD_{YEAR} )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
<td>( BCD_{TOY}, BCD_{YEAR}, SBS )</td>
</tr>
</tbody>
</table>

### Table 4: Suffix descriptions

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPS</td>
<td>Pulses Per Second</td>
</tr>
<tr>
<td>PPM</td>
<td>Pulses Per Minute</td>
</tr>
<tr>
<td>DCLS</td>
<td>DC Level Shift</td>
</tr>
<tr>
<td>BCD</td>
<td>Binary Coded Decimal, coding of time (HH,MM,SS,DDD)</td>
</tr>
<tr>
<td>CF</td>
<td>Control Functions depending on the user application</td>
</tr>
<tr>
<td>SBS</td>
<td>Straight Binary Second of day (0...86400)</td>
</tr>
<tr>
<td>TOY</td>
<td>Time Of Year</td>
</tr>
</tbody>
</table>

There are many subsets of the IRIG-B format. These were developed to provide functionality primarily for military applications dealing with missile and spacecraft tracking, telemetry systems, and data handling systems. IRIG-B is the standard for time synchronization using 100 PPS. It was this flavour that was embraced by the utility industry to provide real-time information exchange between substations. Areva uses IRIG-B12x for modulated signals and IRIG-B00x for its demodulated signals.

The IRIG-B time code signal is a sequence of one second time frames. Each frame is split up into ten 100 mS slots as follows:

- Time-slot 1: Seconds
- Time-slot 2: Minutes
- Time-slot 3: Hours
- Time-slot 4: Days
- Time-slot 5 and 6: Control functions
- Time-slots 7 to 10: Straight binary time of day

The first four time-slots define the time in BCD. Time-slots 5 and 6 are used for control functions, which control deletion commands and allow different data groupings within the synchronization strings. Time-slots 7-10 define the time in SBS (Straight Binary Second of day).

Each frame starts with a position reference and a position identifier. Each Time-slot is further separated by an 8mS position identifier.

A typical 1 second time frame is illustrated in Figure 2. If the CF or SBS time-slots are not used, the bits defined within those fields are set as a string of zeroes.
The 74-bit time code contains 30 bits of BCD time-of-year information in days, hours, minutes and seconds, 17 bits of SB seconds-of-day, 9 bits for year information and 18 bits for control functions.

The BCD code (seconds sub-word) begins at index count 1 (LSB first) with binary coded bits occurring between position identifier bits P0 and P6: 7 for seconds, 7 for minutes, 6 for hours, 10 for days and 9 for year information between position identifiers P5 and P6 to complete the BCD word. An index marker occurs between the decimal digits in each sub-word to provide separation for visual resolution.

The SBS word begins at index count 80 and is between position identifiers P8 and P0 with a position identifier bit, P9 between the 9th and 10th SBS coded bits. The SBS time code recycles each 24-hour period.

The eighteen control bits occur between position identifiers P6 and P8 with a position identifier every 10 bits.

The frame rate is 1.0 seconds with resolutions of 10 mS (dc level shift) and 1 mS (modulated 1 kHz carrier).
19 THE OSI MODEL

In the early days of data communications, solutions were typically developed by companies in proprietary formats, without thoughts of interoperability. This had the disadvantage that if you wished to install a data communications network, you would be obligated to by software and hardware limited to the proprietary solution you were installing.

To provide some level of uniformity among network vendors, the International Standards Organisation (ISO) developed the Open Systems Interconnection (OSI) standard. This is not really a standard. It does not provide any detail about the hardware or software protocols necessary for data exchange. It is a conceptual model, which provides a framework for describing and modelling open network communications systems.

The OSI model divides the data communication process into seven distinct layers. Each of the seven layers defines how the data is handled during the different stages of transmission. Each layer provides a service for the layer immediately above it.

A model representing the seven layers is shown in Figure 1.

<table>
<thead>
<tr>
<th>Layer Type</th>
<th>Data Unit</th>
<th>Layer</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Layers</td>
<td>Data</td>
<td>7 Application</td>
<td>Communication application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 Presentation</td>
<td>Encryption and data representation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 Session</td>
<td>Inter-host communication</td>
</tr>
<tr>
<td>Media Layers</td>
<td>Segment</td>
<td>4 Transport</td>
<td>End-to-end connections and reliability</td>
</tr>
<tr>
<td></td>
<td>Packet</td>
<td>3 Network</td>
<td>Logical addressing</td>
</tr>
<tr>
<td></td>
<td>Frame</td>
<td>2 Link</td>
<td>Physical addressing</td>
</tr>
<tr>
<td></td>
<td>Bit</td>
<td>1 Physical</td>
<td>Media, signal and binary transmission</td>
</tr>
</tbody>
</table>

Figure 1: OSI model

Layer 1 – The Physical Layer

Every data message is transmitted on some medium. This medium usually takes the form of cables, wires, or fibers, but it could just as well be wireless, the data being carried on electromagnetic waves. The physical layer specifies the type of medium to be used between one end of the data exchange and the other. A very common medium is the CAT 5 UTP cable. This is a cable consisting of four twisted pairs of wires terminated with RJ45 connectors.

The physical layer also concerns itself with the electrical implementation of the data stream to be transmitted. This includes the voltage levels of the signals that define the value of the bit (0 or 1), the data transmission timing, the rules governing the handshake between the two ends, and whether the bits are to be sent half duplex or full duplex.

Layer 2 – The Data Link Layer

The physical layer provides the Data Link layer with bits. The Data Link layer now provides some intelligence this sequence of bits by defining Data Frames. These Data Frames are packets of data containing the data to be transmitted and some control information governing the transmission. The control information comprises flags to indicate the start and finish of the message. The standards used at this layer must ensure that the control flags are not mistaken for data and that the data frames are checked for errors.
The most commonly used Data Link protocol used today is Ethernet. Examples of equipment that works at this layer are: Bridges and Switches

**Layer 3 – The Network Layer**

The network layer concerns itself with packet delivery. It establishes logical paths between the sending and receiving equipment, by adding information onto the data frame, which defines where the packet has come from and where the packet is going to. This takes the form of a logical source and destination address for each packet of information. The most commonly used Network protocol used today is IP (Internet Protocol).

The best example of equipment that operates at the network layer is the router.

**Layer 4 – The Transport Layer**

The transport layer is the first layer that is not concerned with the mechanics of the data transfer. It concerns itself with sorting out the packets once they have arrived. There is an array of transport layer protocols ranging from the very simple, which simply accepts the data as it comes in, not caring about whether the packets have errors even if they are in the right order, to quite complex protocols, which check the data for errors, send out an acknowledgement to the sending equipment, order the packets into the correct sequence and present the data to the next layer guaranteed error-free and correctly sequenced.

An example of a simple protocol is UDP (User Datagram protocol). The most commonly used transport layer protocol used is TCP (Transmission Control Protocol), which is among one of the cleverer ones.

Layer 4 functionality is achieved at the IED level – most commonly the computer.

**Layer 5 – The Session Layer**

The first four layers have established a means of reliable communication between two IEDs (Intelligent Electronic Device) such as computers, but hey have not yet dealt with intelligent management of the communication. This is where the session layer comes in. It is the first layer that has user interaction. Each communication session is governed by criteria pertinent to the session. One communication session may be downloading a file from a web site, whilst another may be working on a file situated on a remote server. Session layer software can implement password control, monitor system usage, and allow a user interaction with the communication.

**Layer 6 – The Presentation Layer**

As the name implies, the presentation layer concerns itself with how the data is presented. A good example of this is ASCII (American Standard Code for Information Interchange). An ASCII code is an 8-bit binary code, which defines the character set that we are all so familiar with. For example the character ‘A’ is defined by the binary code 01000001, which is 41 hexadecimal or 65 decimal. The presentation layer, if compliant with the ASCII format, knows this.

**Layer 7 – The Application Layer**

The application layer is the layer, which interacts with the user. This is in the main, software that allows the user to define the communication. Examples of application level protocols would be FTP, HTTP, POP3, SMTP.
20.1 The need to standardize communications within substations

Communication has always played a critical role in the real-time operation of power systems. In the beginning, the telephone was used to communicate line loadings back to the control center, and to dispatch operators to substations to perform switching operations.

As digital communications became more viable, data acquisition systems were installed to automatically collect measurement data from the substations. Since bandwidth was severely limited in those days, communication protocols were optimized to operate over low-bandwidth communication channels. Due to this optimization, it took time to configure, map, and document the location of the various data bits received by the protocol.

Today, communication bandwidth is no longer a limiting factor. Ethernet LANs are slowly replacing the legacy systems that operated in the kilobit region, offering bandwidths of 10 Mbps, 100 Mbps and 1 Gbps, depending on LAN bandwidth requirements. Even 10 Gbps Ethernet LANs are now available.

With the migration towards high bandwidth communications, the problem area has shifted away from bandwidth limitation and towards configuration and documentation. Consequently, a key component of a communication system is the ability to describe itself from both a data and services perspective.

Key requirements include:

- High-speed communication
- Networkable throughout the substation and to the outside world
- High-availability
- Guaranteed delivery times
- Multi-vendor interoperability
- Support for Voltage and Current samples data
- Support for File Transfer
- Auto-configurable / configuration support
- Support for security

Given these requirements, it became clear that an open standard was necessary. It began with the development of the Utility Communication Architecture (UCA) in 1988. The result of this work was a profile of recommended protocols for the various layers of the Open System Interconnect (OSI) model. This architecture resulted in the definition of a profile of protocols, data models, and abstract service definitions that became known as UCA. The concepts and fundamental work done in UCA became the foundation for the work done in the IEC Technical Committee Number 57 (TC57) Working Group 10 (WG10) which culminated in the International Standard, IEC 61850 - Communication Networks and Systems in Substations.

IEC 61850 is a very comprehensive and detailed standard, comprising ten parts and around 1000 pages. A detailed description is therefore not within the scope of this document, which can only provide information at a level sufficient for the requirements of the product user. Should the descriptions contained herein not suffice, please refer to the standard for further information.

20.2 Benefits of IEC61850

IEC 61850 is now the international standard for Ethernet-based communication in substations. It enables integration of all protection, control, measurement and monitoring functions within a substation, and additionally provides the means for interlocking and inter-tripping.
IEC 61850 is much more than a protocol, or even a collection protocols. It is a comprehensive standard, which was designed from the ground up to operate over modern networking technologies. It delivers functionality that is simply not available from legacy communications protocols. These unique characteristics of IEC 61850 can significantly reduce costs associated with designing, installing, commissioning and operating power systems.

Although it is possible to recast old serial link protocols onto a TCP/IP over Ethernet platform, this simply enables the substation engineer to do exactly the same thing that was done years ago, only on a different medium and maybe faster. IEC 61850 does more than this. It enables fundamental improvements in the substation automation process that is simply not possible with a legacy approach, with or without TCP/IP-Ethernet.

To better understand the specific benefits we will first examine some of the key features and capabilities of IEC 61850 and then explain how these result in significant benefits that cannot be achieved with the legacy approach.

The standard provides the following:

- **Use of a virtualized model**: In addition to the protocols that define how the data is transmitted over the network, the virtualized model also allows definition of data, services, and device behavior.

- **Use of names for data**: Every element of IEC 61850 data is named using descriptive strings.

- **Object names are standardized**: Names are not dictated by the device vendor or configured by the user. They are defined in the standard and provided in a power system context, which allows the engineer to immediately identify the meaning of data.

- **Devices are self-describing**: Client applications can download the description of all the data, without any manual configuration of data objects or names.

- **High-Level Services**: IEC61850’s ACSI supports a wide variety of services, such as GOOSE, SMV, and logs.

- **Standardized configuration language**: SCL enables the configuration of a device and its role in the power system to be precisely defined using XML files.

The major benefits of the standard are as follows:

- **Eliminates procurement ambiguity**: As well as for configuration purposes, SCL can be used to precisely define user requirement for substations and devices.

- **Lower installation cost**: IEC 61850 enables devices to exchange data using GOOSE over the station LAN without having to wire separate links for each relay. By using the station LAN to exchange these signals, this reduces infrastructure costs associated with wiring, trenching and ducting.

- **Lower transducer costs**: A single merging unit can deliver measurement signals to many devices using a single transducer. This reduces transducer, wiring, calibration, and maintenance costs.

- **Lower commissioning costs**: IEC 61850-compatible devices do not require much manual configuration. Also, client applications do not need to be manually configured for each point they need to access, because they can retrieve this information directly from the device or import it via an SCL file. Many applications require nothing more than the setting up a network address. Most manual configuration is therefore eliminated drastically reducing errors, rework and therefore costs.

- **Lower equipment migration Costs**: The cost associated with equipment migrations is reduced due to the standardized naming conventions and device behavior.

- **Lower extension costs**: Adding devices and applications into an existing IEC 61850 system, can be done with little impact on existing equipment.

- **Lower integration costs**: IEC 61850 networks are capable of delivering data without separate communications front-ends or reconfiguring devices. This means the cost associated with integrating substation data is substantially reduced.
Implement new capabilities: IEC61850 enables new and innovative applications that would be too costly to produce otherwise. This is because all data associated with a substation is available on its LAN in a standard format and accessible using standard protocols.

20.3 Structure of the IEC 61850 standard

The IEC 61850 standard consists of ten parts, as summarized in Table 1.

<table>
<thead>
<tr>
<th>Part</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction and overview</td>
</tr>
<tr>
<td>2</td>
<td>Glossary</td>
</tr>
<tr>
<td>3</td>
<td>General requirements</td>
</tr>
<tr>
<td>4</td>
<td>System and project management</td>
</tr>
<tr>
<td>5</td>
<td>Communication requirements for functions and device models</td>
</tr>
<tr>
<td>6</td>
<td>Configuration description language for communication in electrical substations related to IEDs</td>
</tr>
<tr>
<td>7</td>
<td>Basic communication structure for substation and feeder equipment</td>
</tr>
<tr>
<td>7.1</td>
<td>- Principles and models</td>
</tr>
<tr>
<td>7.2</td>
<td>- Abstract communication service interface (ACSI)</td>
</tr>
<tr>
<td>7.3</td>
<td>- Common data classes</td>
</tr>
<tr>
<td>7.4</td>
<td>- Compatible logical node classes and data classes</td>
</tr>
<tr>
<td>8</td>
<td>Specific Communication Service Mapping (SCSM)</td>
</tr>
<tr>
<td>8.1</td>
<td>- Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3</td>
</tr>
<tr>
<td>9</td>
<td>Specific Communication Service Mapping (SCSM)</td>
</tr>
<tr>
<td>9.1</td>
<td>- Sampled values over serial unidirectional multidrop point to point link</td>
</tr>
<tr>
<td>9.2</td>
<td>- Sampled values over ISO/IEC 8802-3</td>
</tr>
<tr>
<td>10</td>
<td>Part 10: Conformance testing</td>
</tr>
</tbody>
</table>

Table 1: Structure of IEC 61850 standard

Parts 1 and 2 introduce the standard, provide an overview and a glossary of all terms used throughout the standard. Parts 3, 4, and 5 of the standard start by identifying the general and specific functional requirements for communications in a substation (key requirements stated above). These requirements are then used as forcing functions to aid in the identification of the services and data models needed, application protocol required, and the underlying transport, network, data link, and physical layers that will meet the overall requirements.

Part 6 of the standard defines an XML-based Substation Configuration Language (SCL). SCL allows formal description of the relations between the substation automation system and the substation switchyard. Each device must provide an SCL file that describes its own configuration.

Part 7 is the crux of the standard. It specifies the communication structure for substations. Part 7 consists of 4 sub-sections. IEC 61850 abstracts the definition of the data items and the services from the underlying protocols. These abstract definitions allow data objects and services to be mapped to any protocol that can meet the data and service requirements. The definition of the abstract services is found in part 7.2 of the standard and the abstraction of the data objects (referred to as Logical Nodes) is found in part 7.4. Many of the data objects belong to common categories such as Status, Control, Measurement, and Substitution. These are known as Common Data Classes (CDCs). These CDCs, which define common building blocks for creating the larger data objects, are defined in part 7.3.

The abstract definitions of data and services can be mapped onto various suitable protocols. Section 8.1 of the standard defines the mapping of these onto the Manufacturing Messaging Specification (MMS). Section 9.2 defines the mapping of Sample Measured Values onto an Ethernet data frame. The 9.2 document defines what has become known as the Process Bus.
20.4 The IEC 61850 data model

A typical communications protocol defines how data is transmitted over a medium, but does not specify how the data should be organized in terms of the application. This approach requires power system engineers to manually configure objects and map them to power system variables at a low level (register numbers, index numbers, I/O modules, etc.)

IEC 61850 is different in this respect. In addition to the protocol elements, it specifies a comprehensive model for how power system devices should organize data in a manner that is consistent across all types and brands of devices. This eliminates much of the tedious non-power system configuration effort because the devices can configure themselves. For instance, if you put a CT/VT input into an IEC 61850 IED, it can detect this module and automatically assign it to a measurement unit without user interaction.

Some devices use an SCL file to configure the objects. If this is the case, the engineer needs only to import this SCL file into the device. The client application will then extract the object definitions from the device over the network. This significantly reduces the effort needed to configure the device.

The data model of any IEC 61850 IED can be viewed as a hierarchy of information, whose nomenclature and categorization is defined and standardized in the IEC 61850 specification. The IEC61850 data model is represented conveniently by Figure 1.

![IEC 61850 device model](image)

Figure 1: IEC 61850 device model

The device model starts with a physical device that connects to the network – typically, the IED. The physical device is defined by its network IP address. Within each physical device, there may be one or more logical devices. The IEC 61850 logical device model allows a single physical device to act as a proxy or gateway for multiple logical devices.

Each logical device contains one or more logical nodes. A logical node is a named grouping of data and associated services that is logically related to some power system function. These logical nodes are categorized into 13 different groups and 86 different classes. Table 2 lists these groups and specifies the number of classes within each group.

<table>
<thead>
<tr>
<th>Logical node groups</th>
<th>Group designator</th>
</tr>
</thead>
<tbody>
<tr>
<td>System logical nodes</td>
<td>L</td>
</tr>
</tbody>
</table>
### Logical node groups

<table>
<thead>
<tr>
<th>Logical node groups</th>
<th>Group designator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection functions</td>
<td>P</td>
</tr>
<tr>
<td>Protection related functions</td>
<td>R</td>
</tr>
<tr>
<td>Supervisory control</td>
<td>C</td>
</tr>
<tr>
<td>Generic function references</td>
<td>G</td>
</tr>
<tr>
<td>Interfacing and archiving</td>
<td>I</td>
</tr>
<tr>
<td>Automatic control</td>
<td>A</td>
</tr>
<tr>
<td>Metering and measurement</td>
<td>M</td>
</tr>
<tr>
<td>Switchgear</td>
<td>X</td>
</tr>
<tr>
<td>Instrument transformer</td>
<td>T</td>
</tr>
<tr>
<td>Power transformer and related functions</td>
<td>Y</td>
</tr>
<tr>
<td>Further power system equipment</td>
<td>Z</td>
</tr>
<tr>
<td>Sensors</td>
<td>S</td>
</tr>
</tbody>
</table>

#### Table 2: Logical node categorization

The names of these logical nodes have been standardized in IEC61850 and cannot be changed. The naming convention is as follows:

\(<\text{Single letter group designator}>\text{three-letter mnemonic abbreviation of function}>\text{<instance ID>}\>

For example: PDIR1 belongs to the group “Protection functions” and is the “Directional element” for the first feeder. A complete list of logical node names is provided in the standard.

Each logical node contains one or more elements of Data. There are several hundred data elements, which can be broadly categorized into seven groups:

- System information
- Physical device information
- Measurands
- Metered values
- Controllable data
- Status information
- Settings

Each data element has a unique purposeful name determined by the standard, along with a set of attributes. These data names provide a mnemonic description of its. For example, a circuit breaker is modeled as an **XCBR** logical node. This contains a variety of data including:

- **Loc** for determining if operation is remote or local
- **OpCnt** for an operations count
- **Pos** for the position
- **BlkOpn** block breaker open commands
- **BlkCls** block breaker close commands
- **CBOpCap** for the circuit breaker operating capability

Each element of data conforms to the specification of a common data class (CDC), which describes the type and structure of the data within the logical node. There are CDCs for:

- Status information
- Measured information
• Controllable status information
• Controllable analog set point information
• Status settings
• Analog settings

Each CDC has a set of attributes each with a defined name, defined type, and specific purpose. A set of functional constraints (FC) groups these attributes into categories. For example, there is a CDC called SPS (Single Point Status).

In the Single Point Status (SPS) CDC there are functional constraints for status (ST) attributes, substituted value (SV) attributes, description (DC) attributes, and extended definition (EX) attributes. In this example the status attributes of the SPS class consists of a status value (stVal), a quality flag (q), and a time stamp (t).

Example:
Suppose that you have a logical device called Relay1 consisting of a single circuit breaker logical node XCBR1, and you want to determine if the breaker is in the remote or local mode of operation. To determine this you would use the expression:

Relay1/XCBR1$ST$Loc$stVal

20.5 Mapping IEC 61850 to a protocol stack
The IEC 61850 abstract model needs to work over a real set of protocols, which are convenient and practical to implement, and which can operate within the computing environments commonly found in the power industry. The IEC61850 standard leverages existing protocols to achieve each necessary layer of communication.

We assume in this section that you are familiar with the OSI model, which describes the communication process in terms of seven abstract layers. Figure 2 shows a simplified version of the IEC61850 protocol stack, and how it fits in with the OSI model.

![Figure 2: IEC 61850 protocol stack](image)

IEC 61850 part 8.1 maps the abstract objects and services to the Manufacturing Message Specification (MMS) protocols specified in ISO9506. MMS is the only public ISO-compliant protocol that can easily support the complex naming and service models specified by IEC 61850. MMS is a good choice because it supports complex named objects and a rich set of flexible services that supports the mapping to IEC 61850 in a straightforward manner.

Part 8.1 also defines profiles for the lower layers of the communication stack, as shown in Figure 2. MMS operates over connection-oriented ISO, or TCP/IP. SNTP operates over TCP/IP or UDP/IP. Sampled Values and GOOSE data map directly into the Ethernet data frame thereby eliminating processing of any middle layers and providing very fast response.
### 20.6 Substation Configuration Language

IEC 61850-6-1 specifies an XML-based Substation Configuration Language (SCL) to describe the configuration of IEC 61850 based systems. SCL specifies a hierarchy of configuration files, which enable the various levels of the system to be described. These are:

- System specification description (SSD)
- IED capability description (ICD)
- Substation configuration description (SCD)
- Configured IED description (CID) files

These files are constructed in the same method and format, but have different scopes depending on the need. Even though an IEC 61850 client can extract the configuration from an IED when it is connected over a network, there are several benefits of having a formal off-line description language for reasons other than configuring IEC 61850 client applications. These benefits are as follows:

- SCL enables off-line system development tools to generate the files needed for IED configuration automatically from the power system design. This significantly reduces the cost and effort associated with IED configuration by eliminating most of the manual configuration tasks.
- SCL enables the sharing of IED configuration details among users and suppliers. This helps to reduce inconsistencies and misunderstandings in system configuration requirements. Users can specify and provide their own SCL files to ensure that IEDs are configured according to their requirements.
- SCL allows IEC 61850 applications to be configured off-line without requiring a network connection to the IED.
21 REDUNDANCY IN INDUSTRIAL ETHERNET NETWORKS

21.1 Network topology types

The two most commonly used network topology types are:

- **Star topology**: this is where a physical connection runs from each device on the network to a central location, which is usually a hub or a switch. It is called a star topology because it can be represented in the form of a star as shown in Figure 1.

- **Ring topology**: this is where a physical connection is daisy-chained around the devices in the form of a ring. It is called a ring topology because it can be represented in the form of a ring as shown in Figure 1.

A network usually comprises one type or the other, or a mixture of both. Due to the lack of standardization in the early days, power system companies had no choice but to develop their own proprietary protocols for their substation networks. Eventually, Ethernet became the dominant type of network and was standardized. Ethernet is by far the most widely used network type today. IEEE802.1 Ethernet, the most common Ethernet form today, is by nature a star-based network topology. It did not used to allow a ring topology due to the risk of data storms and consequent paralysis of the network. However, a technology called IEEE 802.1D Spanning Tree Protocol (STP) was developed to get over this problem, allowing Ethernet to be used in rings. It does this by identifying one of the switches in the network as the “root switch” of the network, which is then configured to block packets from going in the wrong direction. It does this by controlling the status of the Ethernet ports, such as blocking, listening, learning and forwarding. This is demonstrated in Figure 1.
STP has some performance related limitations. For this reason, IEEE 802.1W Rapid Spanning Tree Protocol (RSTP) was developed. This newer protocol has all the advantages of IEEE 802.1D, but provides higher performance. Despite the enhanced performance offered by RSTP, it is still not ideal for the demanding requirements of substation automation, for which a more appropriate solution has been devised (see section 21.3).

21.2 Principle of redundancy in communications

The term redundancy can be a little misleading, as it implies that something may not be needed. If the term is qualified such that it reads “Redundancy is any resource that would not be needed if there were no failures”, it becomes clear what redundancy means in the context of IT systems, or indeed any other industrial system. Redundancy is transparent backup. It is required where failure cannot be tolerated, and is thus required in critical applications such as substation automation. Redundancy acts as an insurance policy, providing an alternative system in the event that one system fails. When designing a redundant system, it is necessary to consider the following:

- Degree of redundancy (full, partial duplication): The number of components that must fail to stop service
- Switchover delay: duration of loss of service in case of failure
- Integration delay: duration of disruption to restore redundancy after repair
- Consequences of failure: partial / total system loss, graceful degradation, fault isolation

It is up to the system designer to design in a level of redundancy suitable for the application. The more redundancy you have in a system, the higher the cost.

Redundancy can be introduced at various levels of the OSI model. A certain amount of physical layer redundancy is necessary before you can achieve adequate protection. This may include duplicate cables, devices and other hardware (layer 1 of the OSI model). In order to exploit the alternative path offered by duplicate hardware, however, the communication protocols also need the intelligence to select between the paths in the event of failure of one of them. Protocols providing redundancy, may operate at the data link layer (layer 2 of the OSI model), or at the network layer (layer 3 of the OSI model).

IP is a layer 3 protocol, which is used for routing packets of information around the internet and between devices on LANs. Network redundancy can be built in quite simply at a logical level, but this is not normally sufficient for industrial Ethernet networks, as real-time recovery is not possible. To achieve real-time recovery, redundancy needs to be implemented at layer 2, i.e. the data link layer.
Figure 3 shows how redundancy can be incorporated into a star network. A connection from each node goes to a different switch, providing an alternative path. This topology is called Dual Homing Star Topology.

![Dual Homing Star Topology Diagram]

**Figure 3: Redundant connections in star topology**

With a ring topology, the cable is daisy-chained from device to device in a ring, the idea being if the link from one direction fails, the link in the other direction can be used. This is depicted in Figure 4.

![Redundancy in Ring Topology Diagram]

**Figure 4: Redundancy in ring topology**

In the event that there is a break in one point of the ring, appropriate redundancy protocols can automatically readjust the ring such that the data is sent back in the opposite direction, ensuring it will get to its destination. This is also useful during installation, commissioning or troubleshooting when, for example, the connection to a device's Ethernet port is purposely unplugged for one reason or another.

### 21.3 Redundancy requirements for automation networks

In terms of performance, we can broadly categorize redundancy into two types:

**Dynamic redundancy**

This is where an alternative path is provided in a *standby* arrangement. When the primary path fails, this is detected and the alternative path is switched into action. This type of redundancy needs a certain amount of time to operate. A popular analogy is that of a single tire failing.
have to stop, get the spare one out of the trunk, jack up the car and replace it before you can carry on with your journey. This takes time.

**Static redundancy:**

This is where an alternative path is provided in a *workby* arrangement. When one path fails, the alternative path is already up and running. This type of redundancy does not need any time to operate, because it is already operating. The analogy in this case is that of dual tires on a truck. If one tire blows, you do not have to stop immediately, you can carry on to your destination and fix it later when it is convenient.

Dynamic redundancy is cost-effective, but requires switchover time. Static redundancy provides bumpless switchover but generally costs more. In substations we are dealing with critical real-time information, therefore static redundancy is more appropriate.

### 21.3.1 Switchover time and grace time

The switchover delay is the most constraining factor in fault-tolerant systems. The switchover delay is dictated by the grace time, i.e. the time that the plant allows for recovery before taking emergency actions.

IEC62439 is a standard, which specifies requirements for High Availability Automation Networks. This standard specifies some grace time examples, as shown in Table 1.

<table>
<thead>
<tr>
<th>Applications</th>
<th>Typical grace time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncritical automation applications, e.g. enterprise systems</td>
<td>20s</td>
</tr>
<tr>
<td>Automation management, e.g. manufacturing</td>
<td>2s</td>
</tr>
<tr>
<td>General automation, e.g. process automation, power plants</td>
<td>0.2s</td>
</tr>
<tr>
<td>Time-critical automation, e.g. synchronized drives</td>
<td>0.02s</td>
</tr>
</tbody>
</table>

Table 1: Examples of grace time

Table 2 provides examples of recovery times for various protocols used for implementing redundancy.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
<th>Frame Loss</th>
<th>Typical recovery time</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>IP routing</td>
<td>Yes</td>
<td>30 seconds</td>
</tr>
<tr>
<td>STP</td>
<td>Spanning Tree Protocol</td>
<td>Yes</td>
<td>20 seconds</td>
</tr>
<tr>
<td>RSTP</td>
<td>Rapid Spanning Tree Protocol</td>
<td>Yes</td>
<td>2 seconds</td>
</tr>
<tr>
<td>CRP</td>
<td>Cross-network Redundancy Protocol</td>
<td>Yes</td>
<td>1 second</td>
</tr>
<tr>
<td>MRP</td>
<td>Media Redundancy Protocol</td>
<td>Yes</td>
<td>200 milliseconds</td>
</tr>
<tr>
<td>BRP</td>
<td>Beacon Redundancy Protocol</td>
<td>Yes</td>
<td>8 milliseconds</td>
</tr>
<tr>
<td>PRP</td>
<td>Parallel Redundancy Protocol</td>
<td>No</td>
<td>0 seconds</td>
</tr>
<tr>
<td>HSR</td>
<td>High-availability Seamless Ring</td>
<td>No</td>
<td>0 seconds</td>
</tr>
</tbody>
</table>

Table 2: Typical recovery times for common redundancy protocols

From table 1 and 2 it is plain to see that the only appropriate protocol for substations is PRP for Dual Homing Star Topologies and HSR for ring topologies, because they are the only ones that provide true static redundancy. This is also called *bumpless* redundancy.

**21.4 PRP**

Until recently, power system companies have been using proprietary protocols for providing redundant communications, because the standardized protocols could not satisfy the requirements for real-time systems. PRP, however, has recently been standardized in IEC62439 for use in Dual Homing Star Topology networks. PRP is capable of providing bumpless redundancy for real-time systems, and hence is the new standard for Star-topology networks in the substation environment.
A PRP compatible device has two ports operating in parallel, each port being connected to a separate LAN segment. IEC62439 assigns the term DANP (Doubly Attached Node running PRP) to such devices.

Figure 5 shows an example of a PRP network. The doubly attached nodes DANP 1 and DANP 2 have full node redundancy, while the singly attached nodes SAN 1 and SAN 4 do not have any redundancy. Singly attached nodes can be connected to both LANs, however via a RedBox (a device that converts a singly attached node into a doubly attached node). Devices such as PCs with one network card, printers, IEDs with one network card are singly attached nodes. These may be connected into the network via a RedBox.

Both ports share the same MAC address, so there is no impact on the functioning of ARP (the way devices talk to each other at layer 2 in an Ethernet network). Every data frame is seen by both ports.

When a node sends a frame of data, the frame is duplicated on both ports and thus on both LAN segments, providing a redundant path for the data frame in the event of failure of one of the segments. When both LAN segments are operational, as is the normal case, each port receives identical frames. There are two ways of handling this: Duplicate Accept and Duplicate Discard.

**Duplicate Accept**
Both frames are received and sent to the next layer (TCP, UDP) for processing. There are two disadvantages of this method:

- It cannot be applied to IEC61850 GOOSE messages as these are encapsulated directly within the Ethernet frame.
- The duplicate frame requires processing by the CPU.

**Duplicate discard**
The first frame received is sent to the next layer (TCP, UDP) for processing and the duplicate is discarded at layer 2. There are two consequences of this method, one an advantage, the other a disadvantage:

- Disadvantage: Four extra bytes are needed in the frame sequence to identify the sequence number, the LAN ID and the LPDU size.
- Advantage: No CPU involvement is necessary. A FPGA is capable of discarding the unwanted frame.
21.5 HSR

Until recently, power system companies have been using proprietary protocols for providing redundant communications, because the standardized protocols could not satisfy the requirements for real-time systems. HSR, however, has recently been standardized in IEC62439 for use in Ring Topology networks. HSR is capable of providing bumpless redundancy for real-time systems, and hence is the new standard for ring-topology networks in the substation environment.

HSR works on the premise that each device connected in the ring is a doubly attached node running the HSR protocol. IEC62439 assigns the term DANH (Doubly Attached Node running HSR) to such devices. Singly attached nodes have to be connected via a Redbox (a device that converts a singly attached node into a doubly attached node). Devices such as PCs with one network card, printers, IEDs with one network card are singly attached nodes. These may be connected into the network via a switch (which is itself a singly attached node) and a RedBox.

Figure 6 shows a simple HSR network, where a doubly attached node is sending a multicast frame. The frame (C frame) is duplicated, then each duplicate frame is tagged with the destination MAC address and the sequence number. The frames differ only in their sequence number, which is used to identify one copy from another. For convenience, the duplicate frames are labelled the A frame and B frame. Each frame is sent to the network via a separate port. The destination DANH receives two identical frames from each port, removes the HSR tag of the first frame received and passes this to its upper layers. This now becomes the D frame. The duplicate frame is discarded.

The nodes forward frames from one port to another unless it was the node that injected it into the ring.

Figure 6: HSR for multicast traffic

With unicast frames, there is just one destination and the frames are sent to that destination alone. All non-recipient devices simply pass the frames on. They do not process them in any way. In other words, D frames are produced only for the receiving DANH. This is illustrated in Figure 7.
21.5.1 Peer coupling of two rings

It is possible to connect two HSR rings together using QuadBoxes. These are 4-port devices with forwarding capabilities. A single QuadBox would represent a single point of failure, therefore two QuadBoxes can be used to provide redundant coupling. Figure 8 shows the architecture for this solution with a unicast frame example.

Like any HSR node, a Quadbox forwards frames over each ring and passes the frames unchanged to the adjacent ring, unless it is identified as a frame not to be passed to the other ring. To this effect, a QuadBox is expected to filter traffic based on multicast filtering or VLAN filtering. The QuadBox does not learn MAC addresses, since this could lead to a short break in communication.
With QuadBoxes realized as single physical entities, the two interconnected rings share the same redundancy domain concerning fault tolerance. If one QuadBox breaks down, both interconnected rings are in a degraded state and cannot tolerate a further fault.

Therefore, constructing QuadBoxes in the same way as a RedBox can help keep the redundancy independent. The QuadBox then consists of two devices connected by an interlink. For this reason, the RedBox specifications include the HSR connection.

The presence of two QuadBoxes on the same ring causes two copies of the same frame to be transferred from the first ring to the second, each generating another two copies. This does not cause four frames to circulate on the second ring, however, because when a copy from the first QuadBox reaches the second QuadBox on the same ring, the second QuadBox will not forward it, if it has already sent a copy that came from its interlink. Conversely, if the second QuadBox has not yet received a copy from its interlink, it will forward the frame, but not the copy that comes later from the interlink.

When a QuadBox receives a frame, which was injected into the ring by itself, or a frame that the other QuadBox has inserted into the ring, it forwards this to the interlink and to its other port, if it has not already sent a copy. This duplicate will be discarded at the other end of the interlink. This scheme may cause some additional traffic on the interlink, but it allows simplification of the logic design.

21.5.2 Hierarchical ring topology

An HSR network may consist of rings connected by QuadBoxes, as show in Figure 9.

![Figure 9: Example of hierarchically connected rings](image)

Although a single Quadbox is sufficient to sustain traffic, two independent quadBoxes are needed to avoid a single point of failure.

21.5.3 Connecting an HSR ring to a PRP network

An HSR may also be coupled to a PRP network through two RedBoxes, one for each LAN. In this case, the RedBoxes are configured to support PRP traffic on the interlink, and HSR traffic on the ring ports.
The sequence number from the PRP Redundancy Check Tag (RCT) is reused for the HSR tag and vice versa, to allow communication from one network to the other. This also allows identification of pairs and duplicates on the HSR ring, which have been introduced by a twofold injection into the ring through the two HSR RedBoxes.

**Diagram still required**

### 21.5.4 Meshed topology

HSR allows meshed network topologies and provides redundancy as long as the structure is free from single point of failure. In this case, nodes have more than two ports operating in parallel, which operate like QuadBoxes. A frame received from one port is forwarded to all other ports except the one that received it. Each port forwards the frame unless it has already sent a duplicate.

**Diagram still required**

Mixed HSR PRP architectures Bay level HSR interconnected to local control using PRP 1588 time synchronization.
In the past, substation networks were traditionally a) very isolated and b) the protocols and data formats used to transfer information between devices were more often than not proprietary. For these two reasons, the substation environment was very secure against cyber attacks. The terms used for this inherent type of security are:

- Security by isolation (if the substation network is not connected to the outside world, it can’t be accessed from the outside world).
- Security by obscurity (if the formats and protocols are proprietary, it is very difficult, to interpret them).

The increasing sophistication of protection schemes coupled with the advancement of technology and the desire for vendor interoperability has resulted in standardization of networks and data interchange within substations. Today, devices within substations use standardized protocols for communication. Furthermore, substations can be interconnected with open networks, such as the internet or corporate-wide networks, which use standardized protocols for communication. This introduces a major security risk making the grid vulnerable to cyber-attacks, which could in turn lead to major electrical outages.

Clearly, there is a need to secure message exchanges in the substation environment. The information that needs to be securely exchanged is as follows:

- Security Context: This defines information that allows users to have Role Based Access Control (RBAC). It includes passwords, permissions and user credentials.
- Log and Event Management: This includes security logs, which are stored in different IEDs.
- Settings: This includes information about the IED, such as the number of used and unused ports and performance statistics. It does not include IEC61850 settings.
- IEC61850 messages: Some qualifier here

Before addressing the communications security issue, a reminder of the basic principles of communication is necessary. The Open Systems Interconnection model (OSI) is an abstract description for layered communications and computer network protocol design. The OSI model divides the communication process into seven layers as follows:

- Layer 1: Physical
- Layer 2: Data Link
- Layer 3: Network
- Layer 4: Transport
- Layer 5: Session
- Layer 6: Presentation
- Layer 7: Application

There are two methods for attaining substation security, based on the OSI model:

- Session layer security: This method controls the dialog between two devices. It establishes, manages and terminates the connections between the two devices in question. The most popular protocol for this approach is the Transport Layer Security protocol (TLS). This is also known as Secure Socket Layer (SSL).
- Application layer security: This method secures the messages directly, and is not dependent on other security layers.
This section describes how the security challenges can be met by using the two security approaches described above. It goes on to explain why the Service Oriented Architecture (SOA) philosophy is the most appropriate approach for substation networks.

IEC62351 proposes TLS as the solution to secure IEC61850 communications. Although this SSL-based security solution guarantees confidentiality, integrity and authenticity, it is difficult to implement because it relies on security provided by the transport layer. This type of secure data exchange is limited to point-to-point communication, which clearly is not very flexible.

Unlike layer 4 security solutions, the SOA approach supports security at the application level (layer 7). To achieve this, SOA is based on web services that are message oriented. This means that secure messages can be sent between any of the devices in the network and is not limited to point-to-point communication. This allows a more flexible architecture and improved use of resources.

Our SOA approach is based on the Device Profile for Web Services (DPWS) protocol.

One SOA solution uses the Universal Plug and Play protocol (UPnP). This protocol, however, does not adequately address security-related issues. For this reason the Device Profile for Web Services (DPWS) protocol has been developed.

DPWS enables secure web services on devices with limited resources. This means that DPWS is very applicable to embedded systems and intelligent electronic devices (IEDs). To illustrate the extent of DPWS acceptance and deployment, it is embedded in the Windows Vista and Windows 7 operating systems, as well as the DotNet framework.

DPWS integrates web services based on the core web services standards WSDL, XML and SOAP. Figure 2 shows how these web services fit in with the OSI model.

Figure 1: TLS vs DPWS (Update diagram with all IEDs talking to each other)
Many web services are added on top of the core services. These include the WS-Policy, WS-Addressing, WS-Security and WS-Eventing services. (ensure this ties up with diagram)

The WS-security standard specifies how to sign and encrypt the message, ensuring confidentiality, integrity and authenticity. The message may be encrypted in part or in its entirety. Encrypting only part of the message allows intermediary nodes to be able to view parts of the message intended for them (if required), while the rest of the message stays encrypted. Intermediary nodes can add additional information to the messages headers and sign them.

In order to have a complete security solution, other criteria must be taken into consideration, such as Authentication, Authorization and Accounting (AAA). An AAA server stores security-related data such as user credentials and permissions.

The figure below shows how the messages are exchanged

Figure 2: OSI representation of web services (update this diagram)

Figure 3: Flow of message exchanges (change diagram. I want slopes on the lines)
Once a device is attached to the network, an automatic device discovery process may be performed. Following that, the user selects the device he would like to interact with. The chosen device requests a token from the user to prove he has been authenticated by the security server. The user transfers this token to the end device (in this case, the IED). This can be done automatically using One Time Password (OTP). The IED then requests the user roles and credentials from the authorization server. If successful, a secure exchange of data can occur between the devices applications. This secure exchange covers any data interchange including log events and messages stored at the IED level.