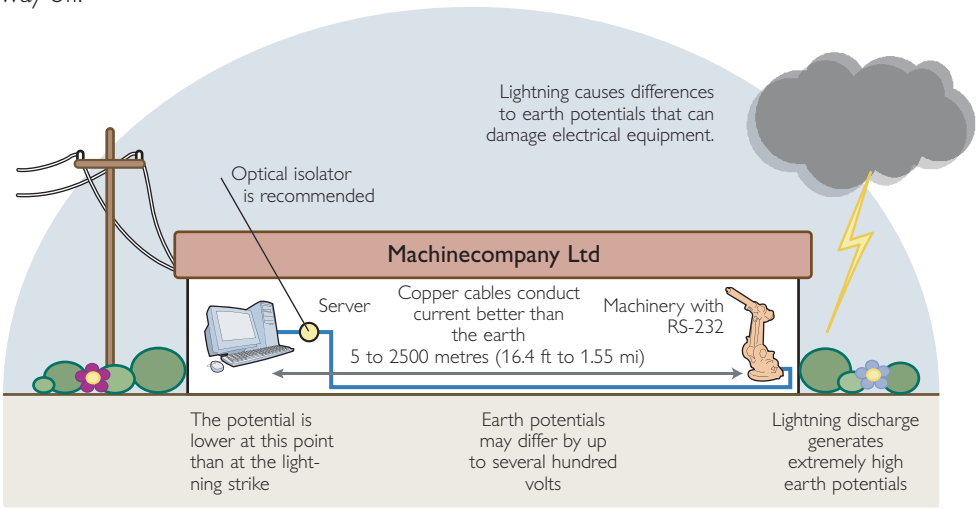
The Problem of Interference

Unfortunately not everything is resolved just because we have succeeded in finding the right transmission methods and the right interface. The largest irritant to data communications still remains-Interference. Outside disturbances that result in data loss, transmission errors and in the worst possible scenario knock out equipment. Computer development has resulted in smaller circuits and components being driven by less power. This is ideal from an energy standpoint, but regrettably they have also become more sensitive and more vulnerable to overvoltages. Investigations have shown that up to 70% of all data disturbances are due to deficiencies in the installations or disturbances from the local environment, from neighbouring equipment, machines and cabling. Only 20% are due to either hardware or software faults. Accordingly, most culprits can be found within our own walls or in the vicinity. The others come from outside. Like a bolt from the blue. The largest group is transients. Short yet high voltage pulses on the network. Computer equipment exposed to transients, 1,000 V and upwards to 10 kV lasting a few milliseconds, lives dangerously.

Lightning, machinery and fluorescent lamps

We know that a direct stroke of lightning discharges very high voltage and that these propagate and damage electrical and telecommunication lines, and in worse cases result in fire. Though you may escape a direct hit, you can be affected by pulses that propagate over large distances in the cable network or by earth potential differences between two points. That is why a light can flicker even when a storm seems a long way off.



It is not just storms that create external transients. Your lamps may also flash when a neighbouring industry starts or shuts down its machinery, this also causes transients and voltage peaks on the network.

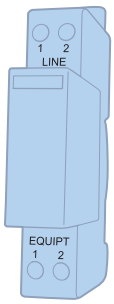
As a rule most transients are created within your own premises. Machines, equipment and fluorescent lamps cause voltage pulses on the network. A fluorescent lamp that is switched off can, for example, emit stored energy in the form of a transient of up to 3000 V. A stroke of lightning close to an electric cable can cause a transient of between 6–10 kV. A standard communication circuit card in a computer is designed for ±12 V. Transients are usually the reason why computer equipment is unexplainably knocked out or communications are temporarily disturbed. Transients are the most common cause of disturbances. Only in about 10% of cases are the disturbances due to a mains fault, i.e. long term undervoltage or overvoltage or a power failure.

Overvoltage protection and lightning protection

As overvoltages or lightning discharges can damage communications equipment we are often asked what the most effective protection is.

To fully control the effects of lightning is extremely difficult; however, many problems can be avoided by installing suitable protective equipment. When discussing lightning protection it is for two categories, direct hits and induced overvoltages.

Protection against direct hits requires the ability to divert several hundred thousand amperes. It is easier to protect yourself against induced voltages; these do not have such a rapid transient time and the current that occurs when diverting is no where near as severe. Induced overvoltages as the name implies are transferred through induction, thus no contact with the lighting is necessary. These overvoltages are the most frequent as they occur in connection with each stroke of lightning.



Examples of overvoltage protection

Interface	Rated voltage
RS-232	12 V
RS-422/RS-485	12 V
W1	24 V
4-20 mA	24 V
Telecom modem leased line	24 V
Telecom modem dialled-up	170 V

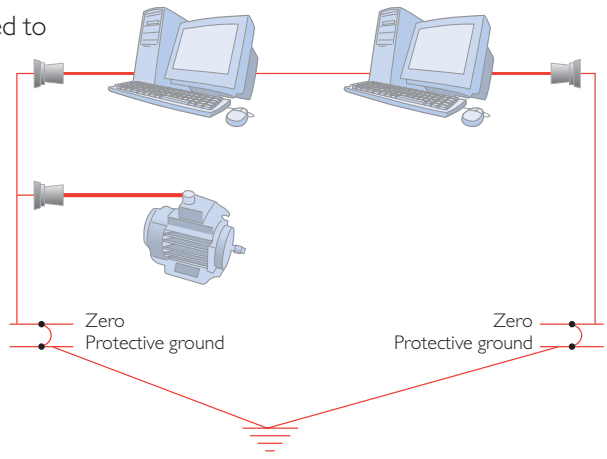
There is a large selection of overvoltage protection for signal/telecommunication lines available on the market as well as for telecom modems, RS-232, 4–20 mA, RS-485 and other typical signals. The protection consists of primary protection and secondary protection, where the secondary protection is adapted to the communication method. The protection is usually maintenance free, when a transient is taken care of the protection returns to its original state. If not, the protection has gone down due to one of the following:

- The transient energy was greater than what the protection could handle (as the stroke of lightning was very close to the installation).
- Damage due to long term overvoltage, for example because of a direct connection to 230 V.

Earth Loops

Another common causes of data communication errors are differential ground potentials or *earth loops*. Especially when network equipment is powered from different distribution panels with different ground potentials when referenced to earth. Any stray current could take two different routes to ground, either the correct path via the earth in the distribution panel, or via the signal ground of the serial port to the earth on the another distribution panel. Ground currents that travel in the network can cause both disturbances and damage the circuits that power the line. A communication network consists of many metres of physical cable. Frequently routed with other cables for electricity and telecommunications. All cables that carry a current create an electromagnetic field that effects adjacent or crossing cables. Together these form large *antennae* that can catch different types of interference. There are recommendations concerning how different types of cabling should be routed to minimise electromagnetic interference. The easiest way to counteract problems with both transients and differential ground potentials is to use a modem with *galvanic isolation* that electrically isolates the cables and the equipment from each other yet does not affect the signals. This prevents transients, lightning and ground currents from reaching the equipment.

In the below example, the earth currents can take the wrong route, via the computer network's signal ground to a fuse panel, and thereby causing interference.

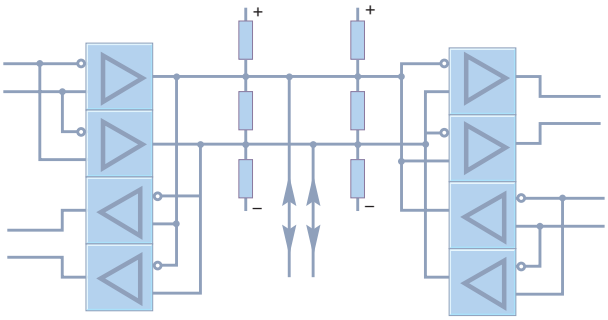


Reducing Interference

In any system, electronic signals are always prone to interference. Analogue signals tend to be more prone due to the fact that all points on the signal carry information- i.e. amplitude and frequency. Small disturbance to the signal will cause the receiving system to interpret the signal differently to that of the original transmitted signal and give an incorrect output. Digital signals are less prone to interference as there are only two basic states; high or low. However due to the interaction of the capacitance, resistance and inductance of the cables used to carry the digital signals and the effects of external noise, the information contained in the signals can be distorted until the signal is unrecognisable.

Balanced Signals

Balanced signals are used to transfer pulse signals over long distances with differential interfaces like RS-422/485 or W1.



Fast balanced communication

When balanced protocols are used on twisted pair cable the cross talk between the pairs is effectively cancelled out by the oppositely induced fields caused by the current flow.
This effect does not occur in unbalanced systems.

Isolation

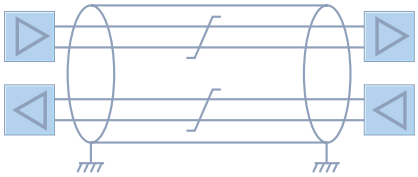
In all data communications it is essential to galvanically isolate equipment and networks from each other to prevent the propagation of transients and other forms of interference that can cause transmission errors or damage equipment.

There are several methods ensuring isolation for example relays, transformers, isolation amplifiers and optocouplers. Incoming transients can also be removed using protective components such as varistors, capacitors, RC filters and zener diodes.

Westermo use optocouplers for isolation in their receivers. Optocouplers provide better performance than for example differential amplifiers. Transformers provide isolation on the power source and varistors and zener diodes are used to suppress transients.

Ground networks

The very best overall method to minimise disturbances is for the system to have an equipotential design. This means that buildings, electronics, fieldbuses and field devices all have the same ground potential. This is very difficult to achieve in practice, you can obtain a uniform potential with the help of special ground conductors and ground wire networks. It is important that the ground wire network and protective ground are interconnected and that they lie as close to each other as possible.

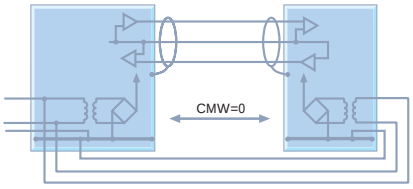


Data communications to RS-422 for 10 Mbit.

Shielding

Shielded or double shielded cables can be used to increase the resistance to external interference. Under normal circumstances the cable shield should only be connected to ground at one end.

In some extreme circumstance where high frequency noise is a problem, the cable can be connected to ground at both ends. However this method introduces a potentially larger problem if there is a potential difference between the points. If this is the case current will start to flow through the shield of the cable and carry with it any noise on the ground plain.



Data communications to RS-232/V.24.

As an alternative it is sometimes possible to connect one end of the shield to ground and the other to ground via a small value, high voltage capacitor

Short Connections without a modem

Direct data communication using RS232/V.24 without a modem will only work over very short distances. The cables must be routed separately from other cables, yet be as close to the ground cable as possible. The device chassis should also be interconnected using copper wire to reduce CMV (**C**ommon **M**ode **V**oltages) noise problems. RS-232/V.24 provides slow communications over ranges up to a maximum of 15 m (50 ft). A line driver or modem should be used for distances above 15 m (50 ft).

RS-422 provides better protection as both the transmitter and receiver are balanced. Screened twisted pair cable can be used and devices must, if they are separate, have their chassis interconnected and preferably fed from the same power source.

Telecom modems and interference

When telecom modems are used within industry you must remember that these are extra sensitive to interference, despite isolation and signal codes. Communication can be disturbed and component faults can result when the cable is not protected carefully. Cabling for telecommunications must be separated from process cabling. Combination protection can provide increased protection in harsh industrial environments.

Fibre cable

Data transfer using fibre cable in this context is completely insensitive to electrical interference. However, communications over fibre cable can be affected by the cable type and splice attenuation.