WHITE PAPER

MAKING SAFE WAVES IN HAZARDOUS AREAS!

March 2009

By John Hartley, Managing Director

Extronics Ltd, Meridian House, Roe Street, Congleton, Cheshire, CW12 1PG, Tel +44 (0)1260 292651, Fax +44 (0)1260 297280 | www.extronics.com

Making Safe Waves in Hazardous Areas!

As wireless devices such as mobile phones and laptop computers become more reliable and cost effective, there is growing interest amongst the process industry as to the benefits to be found from enabling such devices to be used in hazardous areas. However, unlike most industries this is not a simple task. Installing wireless networks in hazardous areas requires careful, expert planning and execution. John Hartley, Managing Director of Extronics, explains the hazards posed by radio frequency sources and the issues involved when installing wireless networks in hazardous areas, and how to minimise the potential risk.

We've been using radio waves in both the business and consumer worlds for a long time, but it is only in the last decade or so that radio devices have become more prevalent in the process industries. Portable radios and pager devices were the first devices to gain certification for use in hazardous areas, after they had been tried and tested in the wider business world.

The radio frequency spectrum covers a wide range from radio waves to gamma rays but the agreed area of RF under the explosion protection standards only covers the range from 10KHz to 300GHz and that is where this article will focus.

It has always been understood that radio frequency (RF) can cause ignition in the right set of circumstances, but when the early radios and pagers were first introduced to the process plants, there was little information or guidance in the Explosion Protected (Ex)- type approval standards to clarify what was a safe amount of RF power to be allowed in the different types of hazardous area. The earliest research into this matter came about more than 30 years ago when the UK Government was proposing to build new petrochemical facilities near to existing TV and radio transmitter networks and those in opposition to the schemes objected on the basis that these installations would be dangerous due to the risk of inadvertent ignition by the radio frequency transmissions. Because of the strategic nature of these facilities and their importance to the UK economy a large amount of research and testing was undertaken and the resultant findings proved what the acceptable safe limits of RF were. It is only in more recent times, as interest is gathering in RF devices and networks, that this information has been more widely circulated and published and acceptable explosion protection techniques sanctioned. There are now a number of approval standards that must be adhered to, including the BS 6656:2002, EN60079 series and IEC60079-0 which we will refer to in this article.

The standard 'BS 6656:2002' explains the methods that can be used to assess if an RF installation is safe to operate in a hazardous area. It details methods and principles to assess installations that are above the safe RF power limits and if they present a hazard due them acting as an antenna and possible source of spark ignition. The final draft of 'IEC60079-0 Ed 5.0' provides radio frequency power or energy threshold tables (table 4 and 5), which can be used to determine if equipment will be safe for use within hazardous areas. Many people don't even realise that RF is a hazard. We have had customers ask "why do we need a certified antenna when it is only fed with RF?" This common misconception is understandable, as there are still very few certified wireless devices on the market and they are only just starting to appear under relevant standards.

The threshold power of radio frequency (10 kHz to 300 GHz) for continuous transmissions and for pulsed transmissions whose pulse durations exceed the thermal initiation time shall not exceed the values shown in Table 4. Programmable or software control intended for setting by the user shall not be permitted.

Table 4 – Radio frequency power thresholds

Equipment For	Threshold power (W)	Thermal initiation time (Averaging period) (µs)
Group I	6	200
Group IIA	6	100
Group IIB	3,5	80
Group IIC	2	20
Group III	6	200

NOTE – The same values are applied for Ma, Mb, Ga, Gb, Gc, Da, Db, or Dc equipment due to the large safety factors involved.

Figure 1. Radio frequency Ex power levels table 4

For pulsed radar and other transmissions where the pulses are short compared with the thermal initiation time, the threshold energy values Z_{th} shall not exceed those given in Table 5

Table 5 - Radio-frequency energy thresholds

Equipment for	Threshold energy Z_{th} (µJ)
Group I	1 500
Group IIA	950
Group IIB	250
Group IIC	50
Group III	1 500

Figure 2. Radio frequency Ex power levels table 5

There are a number of ways radio frequency can be a potential hazard in explosive atmospheres. We know that radio waves and microwaves induce currents in metallic structures such as cranes, pipes and vessels, which can cause sparking if there is a gap in the structure. The power dissipated in the spark may be sufficient to ignite a flammable atmosphere if the radio wave is strong enough. For some applications, such as pulsed radio transmissions in radar, the amount of power may be higher than these levels, but only for a relatively short amount of time. It is possible in these circumstances to use another limit, based on threshold energy. Where the pulse time is less than half the thermal initiation time, and the interval between pulses is longer than the thermal initiation time, the above mentioned EN60097-0 table can be referred to establish the safety of the device.

Fortunately, much of the wireless technology we deal with has RF power levels lower than the 2W limit, which means it can be used in a hazardous area without restrictions. However, when the amount of power is above the safe levels then the BN 6656 can be used to assess the installation for safe use in hazardous areas.

The most obvious, but not necessarily the most practical solution for a safe installation is to ensure the antenna is placed a safe distance outside of the hazardous area so that the level of RF power is below the safe limit before it enters the hazardous area. It is also possible to certify specific devices for use only within a safe distance from metallic structures and structures or equipment such as cranes, columns, pipes and tanker loading stations, which can act as antenna and thus pose as a sparking hazard. The issue with this approach though is ensuring that the conditions subsequently remain the same as when the assessment was carried out.

Gas detectors can be employed to monitor the unsafe perimeters around an antenna and certify the system for use to reduce the level of hazardous area the equipment is installed in. Should a hazardous area be detected the power is isolated from the equipment, thus rendering it safe. We would only recommend this approach for lower risk areas such as Zone 2.

The main hazard to be found with wireless networks is associated with the electrical hazard from the RF output stage. The hazard posed by electrical equipment has been catered for over many decades with the earliest standards and protection concepts now over 50 years old. The two key hazards are the risk of a spark when a device short circuits due to inadequate creepage and clearances or from a foreign body entering a piece of equipment. Ignition can also be caused by the heating effect of components conducting electrical current which are not adequately power rated.

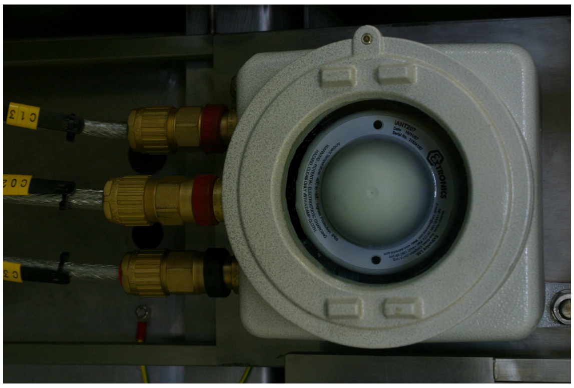

Figure 3. Antenna in Ex'd enclosure with window

Also a non battery powered radio transceiver is ultimately connected to mains voltage and thus under fault conditions this voltage could be transferred through to an antenna and if that antenna does not have suitable creepage and clearance or be of a suitably robust construction it could cause an incendive spark or become dangerously hot. This means that either the RF stage has to have an intrinsically safe output or antennas must meet a range of stringent mechanical, constructional and thermal requirements to ensure that the installation is safe should any of the above events occur.

Many of the earlier deployments of 802.11 WLAN access points used antennas pointing through 'Ex d enclosure windows' (flameproof, sealed enclosures with a toughened glass window for reading dials or, in this case, transmitting data). Some still do today. This is quite suitable for applications at lower frequencies but not ideal for higher frequencies such as 2.4 and 5GHz WLAN as the glass attenuates a high proportion of the signal and with only 100mW max power permitted from the transceiver in the case of an 802.11b/g WLAN it is not the best solution.

Another issue with this method is that the access point only directs RF power from the front of the enclosure (not in the case of glass dome Ex d enclosures), which will limit the flexibility of the device and also cause RF shadows in the close proximity of the unit. RF multi-path interference can also be created at higher frequencies which is an effect one seeks to avoid in deployments. However, although this method has its failings, it is cost effective and the Ex certification is very simple, so it does have its place!

Figure 4. iANT100 Antenna

If the antenna complies with the EN60079-0 general requirements and specific sub-categories, such as Ex d flame proofing EN60079-1, Ex e increased safety EN60079-7 or Ex m device encapsulation EN60079-18, the only other area requiring assessment by the installer is the maximum power output of the RF stage. This is because the antenna will have been designed and certified to be safe under fault conditions in a hazardous area, for instance a 250VAC mains fault being transferred into the antenna by the RF stage of the transceiver. The only issue regarding these specially designed and Ex approved antennas is that currently there are only omni directional types available and they are very expensive compared with standard industrial antennas due to the fact they are made in low volumes and constructed from special materials. The best solution to minimise costs and extend the diversity of antenna's in hazardous areas is to find a way of using standard industrial antennas. This is possible if the output of the RF transceiver is intrinsically safe, Ex i in accordance with EN60079-11.

The classic 'zener barrier' (a safety barrier consisting of a current limiter circuit, a voltage limiter circuit and a fuse for voltage limiter circuit protection) is the simplest solution to making the transceiver RF stage intrinsically safe, as it will prevent any possible faults in the transceiver being propagated or transferred to the hazardous area. Any fault current up to a value of 250 VAC will be absorbed by the zener diodes and very quickly the fuse will blow, turning off the power to the hazardous area.

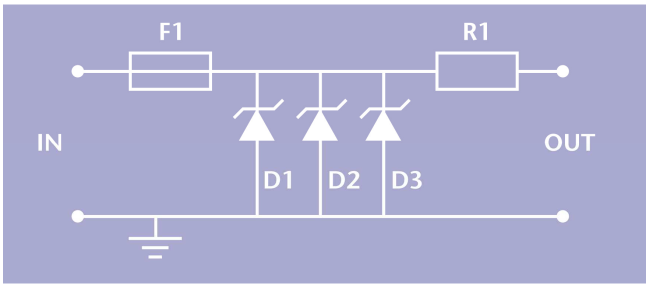

Figure 5. Zener barrier

However nothing is ever that simple. Although the RF output stage may have been made intrinsically safe, the constraints of the zener barrier's capabilities (various reasons but the key components in currently available devices are not of an RF grade design) means that this principle can only be used on lower frequency signals, typically less than 500KHz, as the signal attenuation and distortion effectively renders the signal useless. The easiest way to block low frequency mains faults is to use series coupled capacitors as these block all low frequency signals but not all faults so they also require a current limiting resistor to protect against transient faults (EN60079-11 clause 8.5 Blocking Capacitors - stipulates that when used between intrinsically safe circuits and non intrinsically safe circuits - All possible transients shall be taken into account, and the effect of the highest nominal operating frequency (as that supplied by the manufacturer) in that part of the circuit shall be considered.)

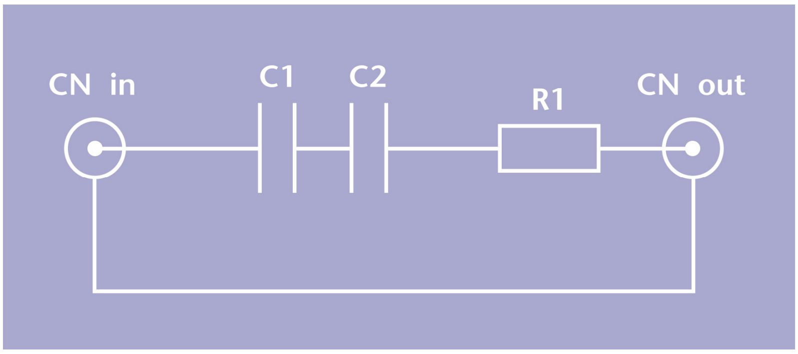

Figure 6. High frequency RF barrier

However although this type of circuit is a bone fide technique it must be assessed along with the transceiver electronics to make sure other faults such as the MHz range cannot pass through the circuit incendively. Currently the only practical way to make an RF stage intrinsically safe is to design the modifications into the equipment in the initial development phase and take it through notified body certification. For zone 2 applications the protection of the transceiver RF stage is much easier due to the fact that fault conditions are not considered. The point being made here is that for Zone 0 and Zone 1applications there is currently no off the shelf RF intrinsically safe barrier that can just be inserted into a circuit and applied to an RF output stage like it were a 4.20mA or 24 VDC signal without it being further considered by a notified body and a type approval issued.

Also, the antenna gain must not be forgotten when assessing if the RF transceiver is suitable for use in a hazardous area. A calculation of the maximum EIRP (Effective Isotropic Radiated Power) must be made to ensure the power radiating from the antenna is below the limits for the relevant hazardous area. In this example of a long distance link it is easy to see how the RF output stage is intrinsically safe and way below the 2W limit. But once a high gain antenna is connected, it is massively over the limit and would become an incendiary in any hazardous area.

Figure 7. RF Link Calculator

It is not just a matter of making the network and devices safe and compliant with regulations. It also has to work! Any wireless point-to-point or MESH link more than a few hundred metres should be calculated to see if it will function reliably, taking into account power from the transceiver, receive sensitivity, antenna gain and losses in cables, connectors and free space loss. This is often referred to as a link budget calculator. It is good practice to have at least 6dBm of fade margin between the link working and not to allow for changing RF conditions. Our calculator enables the user to determine if their planned installation is safe to use in a hazardous area with a simple 'green-go' and 'red-no-go' legend.

Every decade or so, there is a major new technology that offers huge gains in productivity in the work place. Roughly 20 years ago came the microprocessor, replacing analogue electronics. Then, 10 years ago, the PC and commercial grade operating systems were accepted as suitable for use for plant control and supervision as a DCS. We firmly believe that the next decade will see wireless networking technology make the next step change in working practices, safety and in productivity improvements in the process industry.

There is a huge amount of complex information for communications engineers to consider when planning a wireless network in any of the process industries, before they even start to consider what devices to support. We are focused on the development of 802.11 products that are suitable for use in extreme environments, including WiFi and MESH Ethernet infrastructure, Real Time Location Systems for people safety and asset tracking, Telemetry devices and RFID. We are looking forward to creating the opportunities to lead the process industry into a new era based upon sound, researched and developed technology.