

RF Radiated Energy in Close Proximity to Explosives

The process of well perforation requires the use and handling of explosive materials. Strict safety processes and procedures are required to prevent accidental detonation of the perforating guns. As wireless technologies and systems became more widely used, the industry was initially concerned that radio frequency (RF) emissions from wireless systems could potentially result in accidental triggering of the perforating guns. However, as the industry moved from analog to digital triggering systems, the probability for accidental detonation was significantly reduced. Smart Wireless Field Network Devices from Emerson comply with IEC62591 (WirelessHART) and have very low RF emission potential, making them appropriate for use in the vicinity of well perforating systems.

Introduction

This paper discusses the use of Wireless Field Network Devices complying with IEC62591 (WirelessHART). These devices comply with the same safety processes and procedures required for well perforating equipment and explosive triggering systems due to their very low RF emission potential.

Types of Operating Environments

There are several types of technologies utilized for triggering explosives. Originally, analog triggering techniques were used. These early systems were triggered by applying an electrical charge of a predefined magnitude to cause the explosive to detonate. It was possible for these first generation systems to be triggered accidentally by external RF energy. Examples of RF emitters included high powered wireless voice communication systems. These concerns about accidental triggering due to RF energy led to a common practice of using radio silence during perforation operations (removing all RF energy from the environment).

Note: For more information on radio silence support in Emerson Smart Wireless Networks please read “Radio Silence for Wireless Field

Networks” available from Emerson Process Management at www.emersonprocess.com.

Over the past 20 years the industry’s well perforating and explosive triggering technologies have moved from analog to digital devices and systems. Digital system detonators still receive incoming signals, however, the digital security code must now match exactly for the triggers to activate. The use of this technology helps ensure that other RF sources will not cause inadvertent detonation of the explosive triggers. This has led to much safer well perforation operations and explosives handling.

Use of Analog Triggering Techniques

Due to the inherent risk posed by the older analog technology and the broad availability of newer and safer digital technology options; use of the older analog triggering techniques has almost been completely phased out globally.

However, the concern regarding the potential effect of RF interference on the safety of well perforation and explosive triggering systems remains. There are several sources and standards that limit the maximum RF power levels allowed. The following examples are two of the more conservative documented references that include published guidelines which can be utilized as references if RF interference requires mitigation.

- 1.) Alberta Occupational Health and Safety Code – 2009, Schedule 10, Table 2: Minimum separation distances between explosives and fixed radio frequency transmitters.

Notes & Comments:

- a. This table is intended for transmitters with significantly more power output than many IEC62591 (WirelessHART) compliant very low power RF transmitters. The lowest power output level in Table 2 requires transmitters with output power of 25 W or less (compared to the 10mW output of Emerson’s WirelessHART transmitters with an integrated or internal antenna) to be at least 30 meters away from the explosives, drill hole, or borehole.
- b. Table 3 in this document addresses mobile transmitters (such as a handheld walkie-talkie) but only extends down to 5W or less where equipment transmitting at 450 MHz or above must be at least 5 meters away.
- c. The table below contains the data from Alberta Occupational Health and Safety Code – 2009, Schedule 10, Table 2.

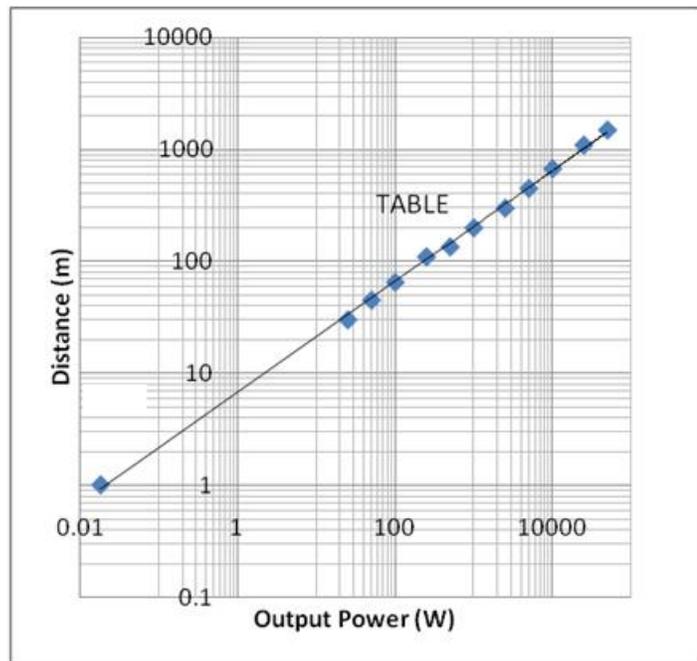
Table		Calculated	
Power (Watts)	Distance (meters)	Tx Power (dBm)	Rx Power (dBm)
25	30	44	-25.6
50	45	47	-26.1
100	65	50	-26.3
250	110	54	-26.8
500	135	57	-25.7
1000	200	60	-26.1
2500	300	64	-25.6
5000	450	67	-26.1
10000	675	70	-26.6
25000	1100	74	-26.9
50000	1500	77	-26.6

Note 1: Data from Alberta Occupational Health and Safety Code 2009 - Table 2

- i. To compare how this relates to an IEC62591 (WirelessHART) transmitter, the table below shows how the significantly lower power levels would compare. The separation distances are based on a received power limit of -27.5 dBm and assume free space path loss without reflected energy. This equivalent calculation shows that given the much lower power RF output would require a minimum separation distance of 0.8 to 1.5m to generate the same accepted Rx power levels.

Table		Calculated	
Power (Watts)	Distance (meters)	Tx Power (dBm)	Rx Power (dBm)
0.010	0.8	10	-27.5
0.018	1.0	12.5	-27.5
0.040	1.5	16	-27.4

Note 2: Three examples of radiated output levels of IEC62591 (WirelessHART) devices.



Note 3: This depicts graphically the data from Alberta Occupational Health and Safety Code 2009 - Table 2 and the example of the WirelessHART transmitters.

- 2.) Institute of Makers of Explosives Safety Library Publication No. 20: Safety Guide for the Prevention of Radio Frequency Radiation Hazards in the Use of Commercial Electric Detonators
 - a. The lowest power value in the table for “Mobile Transmitters” (Table 3) is 1 W. At 1 W, this standard requires 8 ft of separation for devices operating above 450 MHz. Note: This document does not have a guideline for fixed transmitters that cover low power 2.4 GHz RF transmitters such as IEC62591 (WirelessHART) devices.

Many WirelessHART Field Devices would clearly fall into the lowest power category addressed by each of two referenced published guidelines. It is not clear from either of these published guidelines whether extrapolation for much lower power devices is allowed, however, we have provided the extrapolated information to illustrate the order of magnitude difference between the very low power devices and those cited in the published materials.

Use of Modern Digital Triggering Techniques

Digital triggering techniques ensure that regardless of the signal level, an exact protocol must be followed before an explosive trigger can be executed. Using such digital protocols enables the use of digital encryption, digital security measures, bi-directional orderly communication, validation and other strategies that ensure the integrity of the ignition signal. All of this leads to significantly reduced risk of a false trigger.

When utilizing a digital triggering device, an undetected bit error could theoretically create an erroneous communication. By utilizing common techniques such as checksum or CRC's in the communication messages, bit errors can be easily detected and rejected in the communication protocol. If a transmitter is within close proximity to the digital trigger, the signal to noise & interference ratio is affected if the transmitter and the digital trigger are receiving and transmitting on the same RF band with similar carrier frequencies. An increase in the noise and/or

interference can cause increased bit error rates which can be detected by a checksum or CRC.

Although the possibility that some bit errors may not be detected, the probability that an undetected bit error that would cause a valid byte, word, or key to be exactly identical to the trigger protocol causing a false trigger is extremely small. That is why digital triggering systems have been successfully used for many years.

WirelessHART compliant devices further decrease this probability of a trigger by using encryption techniques, spread spectrum modulation, message validation and other modern protocol features.

When multiple digital protocols are operating in close proximity of each other, many mechanisms come into play to ensure no miscommunication can occur which could lead to communication errors and/or increased RF interference.

Conclusion

Extra safety precautions are needed during well perforation operations and when handling or working in close proximity to explosives. Moving from analog to digital well perforation and triggering devices and systems has significantly improved safety by dramatically reducing the potential for accidental triggering by RF interference. Low power IEC62591 (WirelessHART) compatible Wireless Field Devices can be successfully used in proximity to modern digital triggering techniques due to their extremely low RF emission potential and digital protocols. Since they utilize the IEC62591 (WirelessHART) protocol and incorporate multiple techniques of encryption and spread spectrum modulation, they further limit the risk of unintended RF interference with other digital protocols like the ones used in digital triggers. Even in an analog triggering environment, the extremely low power RF emission potential of IEC62591 (WirelessHART) Field Devices also places them at the very bottom of the lowest power level category of the published industry guidelines addressing minimum separations for use with the older analog triggering systems.