# Safety of Blasting with Electronic Detonators

C.M. Lownds [1] and U. Steiner [2]

## Abstract

Electronic detonators have been in commercial use for a decade, with an excellent safety record. This paper lists known incidents involving electronic detonators. Typical standards required by regulatory bodies for static electricity and electromagnetic fields are reviewed. The performance of some detonators is compared to these standards; in general the minimum standards are easily exceeded. The general resistance of electronic detonators to extraneous electrical energy that can be derived from the body of test results is compared to danger levels for exposure of humans to these energies; it is shown that electronic detonators can safely tolerate higher electrical energies than people can. This comparison includes comparable data for electric detonators, which are shown to be more vulnerable to extraneous electrical energy than people are. Electronic detonators also bring significant safety benefits in blasting due to their testability, two-way communications, reliability, programmability and precision. The links between these attributes and enhanced safety are discussed with examples from actual blasting. Although electronic detonators are usually more vulnerable to extraneous electricity than non-electric initiation systems, the paper shows that the net safety benefit in handling and blasting is in favor of electronic detonators, which are the safest initiation system that has ever been offered to the mining industry.

1. Orica USA, Inc
2. Orica Germany GmbH

## Introduction

Electronic detonators have been in commercial use globally for a little over a decade. These systems are available in all major mining countries from one or more of the several manufacturers. Global sales from inception to mid-2009 are estimated to have been about 50 million electronic detonators, with annual sales in 2010 estimated at about 8 million.

Most electronic detonators have the following features in common:

- A variety of wire lengths to suit mining applications
- Fully programmable delay time (which significantly reduces inventory)
- Much more precise firing than pyrotechnic systems (leading to more predictable blasting)
- Programmable in increments of 1ms (giving great scope to blast design options)
- Safely testable in situ to ensure reliable firing of the whole blast

The benefits of blasting with electronic detonators are becoming ever more widely recognized. Cost savings from reducing powder factor and/or from reduced cost of operations downstream of blasting are commonplace. Novel mining methods, some impossible without electronic detonators, are being tried and introduced.

All electronic detonators have significant safety features built into the design of the electronics inside the detonator and in the control equipment. These will be discussed in more detail below.

In the time since the introduction of these products, regulatory authorities in some countries have introduced comprehensive new rules specific to electronic detonators. In other countries, slower to react, electronic detonators still fall by default under the rules for electric detonators. In this paper the most progressive regulatory requirements will be discussed.

Data for 2 brands of Orica's electronic detonators will be presented: the brands will be called Type i for i-kon™ electronic detonators and Type u for Uni tronic™ electronic detonators.

## Known Incidents

To the authors' knowledge there have been no injuries caused by the use of approximately 20 million electronic detonators (from all suppliers) to date. Several suppliers have had uncommanded firings of electronic detonators. In such cases of Type i and Type u detonators, each incident occurred only after the blast pattern had been cleared and guarded and the detonators had been deliberately powered up to firing voltage. Lownds and Lindenau reported four cases of blastholes initiating due to a direct or very close lightning strike. In 2 later cases known to the authors, detonator wires were struck by lightning; the insulation melted and showed scorch marks, but the holes did not initiate.

## Typical Safety Features in the Design of Electronic Detonators

Typically three protection elements are used in the circuitry inside the detonator to guard against extraneous electrical energy: spark gaps, input resistors and the ASIC itself. (ASIC means application

specific integrated circuit, also called the chip). An arrangement of these elements is shown in Figure 1 and their functions are explained below.

Spark gaps

A spark gap is a passive component inside the detonator designed to protect against high voltages, which are especially prevalent in static electricity. In principle spark gaps are two conducting electrodes separated by a gap filled with gas - in this case the air inside the detonator. Spark gaps are arranged between the two legwires as well as between the wires and the shell of the detonator. The gaps in spark gap structures are typically of the order of $1/10^{th}$ of a millimeter; the smaller the spark gap, the lower is the flash-over voltage. At high enough voltage, the air between the two electrodes ionizes, significantly reducing the electrical resistance between them. The resulting spark can carry significant current from one electrode to the other, neutralizing the wire-wire or wire-shell voltage while safely bypassing the input resistors and the ASIC.

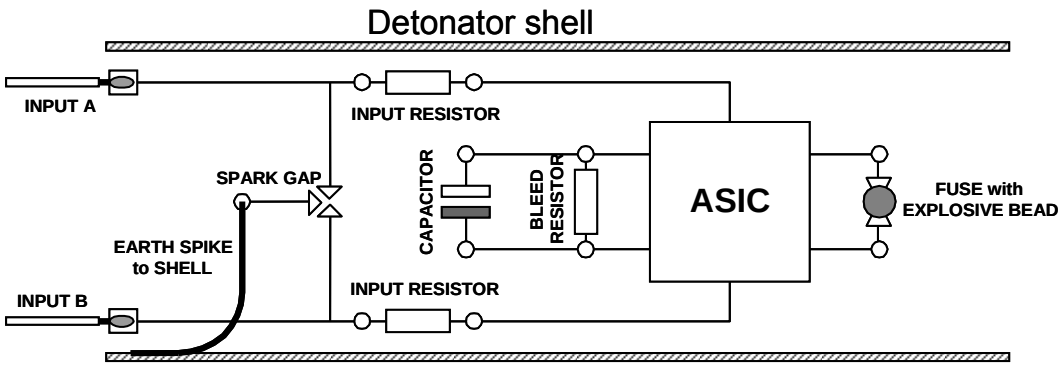


Figure 1: Schematic arrangement inside a particular electronic detonator.

Input resistors

The aim of the input resistors is to protect the ASIC from high current. The following example illustrates how the input resistors limit the current in an electronic detonator compared to an electric detonator:

Consider input resistors of 500 ohms each and a voltage of 12V applied across the inputs A and B (Figure 1). Then the maximum current that can flow in the circuit is 12/1000 = 12 milliamps. This is not enough to fire the fuse. By contrast, the current in an electric detonator with a fuse of (typical) resistance = 6 ohms will be 2 amps; more than enough to fire the fuses used in commercial electric detonators. In fact the ASIC also presents a high resistance to current flow, so the actual current drawn by an electronic detonator is tens or hundreds of microamps.

Input resistors can have different power ratings, but all will fail if the power they carry (voltage x current) is too high. When an input resistor fails open circuit it is effectively an electrical fuse. Thus high current can no longer be supplied to the ASIC or to the fusehead, and the detonator will be well protected against uncommanded firing. Such a detonator will however no longer be functional.

The above example illustrates an essential safety feature of electronic detonators; they operate with a "trickle" current and an on-board energy storage device in the form of the capacitor. The current that can flow through an electronic detonator is not enough to fire the fuse; energy must be stored in the capacitor for later release in a burst of energy to fire the fuse.

Protection on the ASIC

The ASIC is the last electronic element on the printed circuit board (PCB) protecting the fusehead against extraneous electrical energy. There are two mechanisms inside the ASIC that ensure protection. Firstly the firing signal is digitally encoded, meaning that a simple energy impulse as used for electric detonators will not allow the detonator to fire. Only if the correct digital code is received will the ASIC allow the capacitor to discharge its energy to the fusehead. Second there are electronic components inside the ASIC ensuring current and voltage protection.

Some ASICs operate at 2 different voltages: the low voltage allows the ASIC to communicate but does not charge the capacitor with sufficient voltage to fire the fuse, while the high voltage provides ample energy for both the electronic countdown of delay time and for firing the fuse. The low voltage is used on the blast pattern during deployment while the high voltage may only be applied to the detonators after the pattern has been cleared and guarded.

## Extraneous Electrical Energy

Electronic and other detonators are exposed to extraneous electrical energy. The main sources of electrical energy that could affect detonators during handling and use include

- electrostatic discharge (ESD), most likely from static electricity on the human body and also machine bodies.
- stray currents causing voltage gradients in the ground
- radio-frequency electric fields (RF) from cell phones, hand-held 2-way radios, etc.
- lightning striking on or near the blast pattern and causing high voltage gradients in the ground

ESD, lightning and some stray current effects are short duration. For such stimuli it is commonly found that the target responds according to the electrical *impulse* delivered by the source. Impulse is

$M = \int_{t1}^{t2} i^2 dt$, where i is the current. For the total discharge of a capacitor through a resistive load,

$M = i_0^2 \tau/2$, where $i_0$ is the initial peak current, and $\tau$ is the time constant,

$\tau = RC$, R = resistance and C = capacitance.

Current impulse is often called the "i squared t criterion". With i in Amps, t in seconds, R in Ohms and C in Farads the units of M are $A^2s$. Descriptions of the impulse for detonators is usually expressed in the equivalent units of Ws/Ω or mWs/Ω.

In many cases the electrical stimulus is measured as voltage rather than current. Helfrich and Reynolds suggest converting between these using Ohm's Law (V=iR), with R being a typical value for the hand to foot resistance of the human body of 1500Ω. Thus current impulse ($A^2s$) can be converted to voltage impulse ($V^2s$) for comparison between different extraneous electrical phenomena.

The parameter for RF fields is the field strength in Volts per meter. Detonators respond to RF when their wires become an antenna. The best performance of an antenna occurs when its length is half the wave-length of the radio wave. Since any part of the wiring of a blast can form an antenna, the extremes of antenna lengths in typical blasting are about 1m to 100m (3 to 330 ft). Using the relationship between dipole antenna length and frequency of L=143/f (L in m and f in MHz) gives a frequency range of interest of about 1MHz to 1GHz. RF in this range will result in the highest pickup of energy by blast wiring.

## Regulatory Requirements for Detonators

European regulations set standards for all the important attributes of electronic detonators (see ref "CEN"). Products that pass this comprehensive set of requirements are awarded the CE mark. (Both Types i and u and several other brands of electronic detonators have the CE mark). In summary, the properties of detonators (including electronic detonators) that are examined include:

Wires: abrasion resistance, cut resistance, low temperature cracking, tensile strength
Detonator: thermal stability, resistance to impact, bending, vibration, dropping, hydrostatic pressure
Detonators + System: electrostatic discharge, radio-frequency radiation.

The electrostatic discharge test is called the "Human Body Model" and requires the detonators to survive a capacitor discharge with an electrical impulse =.0006$A^2$s.

The European regulatory requirements in terms of radio-frequency electromagnetic fields (RF) are no-fire levels for electric detonators of 0.6V/m and for electronic detonators of 10V/m.

The US guideline for RF field strengths (see ref "IME") varies with frequency, with a maximum field strength for safe exposure of electric detonators of 100V/m and a minimum field strength of about 0.5V/m at a frequencies of 0.8 and 10MHz respectively.

## Vulnerability of Humans

Human vulnerability to electric shock (mostly 60Hz AC) is summarized by El-Sharkawi. Human responses to electricity progress from discomfort to pain to the inability to let go the wires to heart fibrillation to death caused by heart seizure.

The critical electrical impulse for humans (where there is a 5% chance of heart fibrillation) is 0.0135$A^2$s. Using the proposal of Helfrich and Reynolds this is equivalent to 30375$V^2$s. This is the short-duration human vulnerability limit. For longer durations: male humans are unable to let go energized electric wires when the current flowing through their bodies is 9mA, 60Hz. Using a body resistance of 1500Ω, a critical long-duration voltage for humans is 13.5V AC. The DC value is significantly higher than this.

The safe exposure limits for humans to RF are given by IEEE (see ref). They vary with frequency, as will be shown below.

## Behavior of Detonators

Lownds and Steiner described simulated lightning testing of Types i and u electronic detonators. The two series were called high current and high voltage tests. The results are summarized below for the more realistic wire to shell tests:

| Voltage | Capacitance | Peak current | Impulse | Type i results | Type u results |
|---|---|---|---|---|---|
| 6 kV | 55 µF | 18 kA | 3300 $A^2s$ | 0/10 fired | 0/10 fired |
| 800 kV | 60 nF | 10 kA | 240 $A^2s$ | 0/10 fired | 1/10 fired |
| 600 kV | 60 nF | 7.5 kA | 135 $A^2s$ | 0/10 fired | 0/10 fired |

Both detonator types were also subjected to very high field strength RF tests. Type i detonators were tested more recently, when higher field strengths were available. The maximum field strength available of 500V/m did not cause any detonators to fire, although the wire insulation was melted in some tests.

Published data (Atlas) is available for electric detonators' critical impulse and no-fire DC current. Figures 2 and 3 compare the electronic detonators described here with electric detonators and with human vulnerability to electric shock and RF fields.

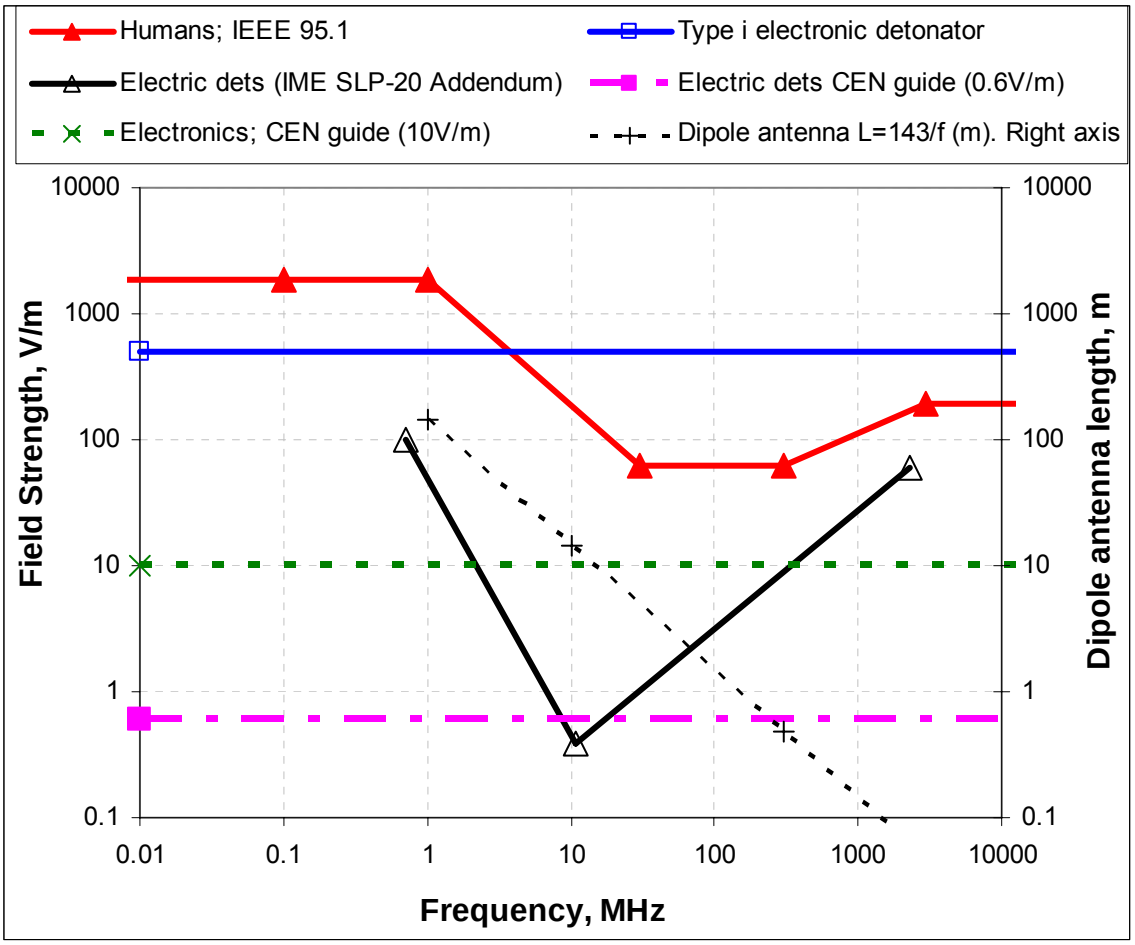


Figure 2: Vulnerability of detonators and humans to radio-frequency fields

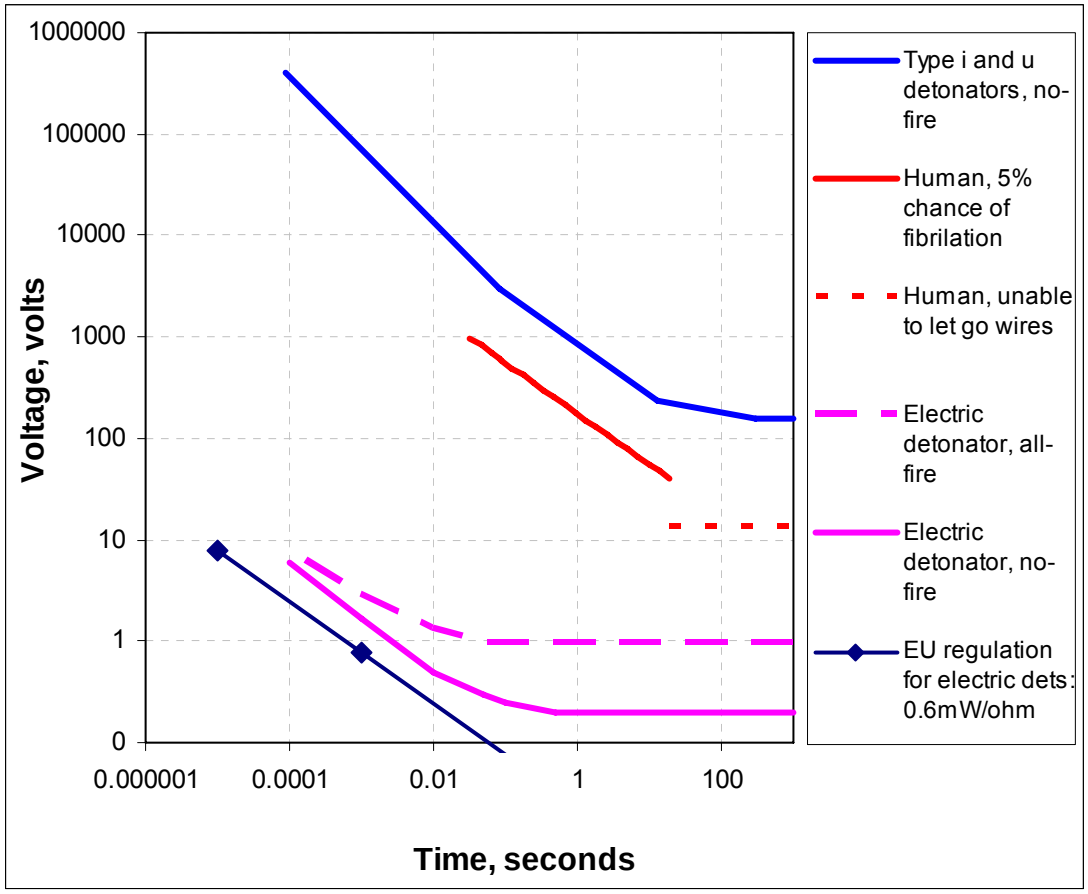


Figure 3: Vulnerability of detonators and humans to extraneous electricity

It is immediately clear that Types i and u electronic detonators can safely tolerate electrical stimuli that are orders of magnitude greater than the corresponding critical levels for electric detonators. Compared to human vulnerability, these electronic detonators can tolerate stimuli that are, in most cases, significantly higher than the safe levels for humans. The only exception is human tolerance of RF at very long wave lengths. Due to test limitations, Type i detonators were not tested beyond 500V/m, so the upper limit of their tolerance is not known.

In general it appears that if humans are safe, electronic detonators are safe. However, each manufacturer's specific safety recommendations should be followed.

## Safety Benefits in Blasting

Safety benefits can be separated into safety and security issues. Security in blasting is generally improved by the following factors:

- Programmable detonators greatly reduce inventory and make accurate record keeping in magazines easier.
- With some electronic detonator systems it is possible to keep a record of destruction of individual detonators due to their unique identity numbers.
- Electronic detonators that get into the wrong hands (due to theft) cannot be initiated except with their own programming and firing equipment.

Safety benefits of electronic blasting systems arise from 3 sources: safe designs for operation on the blast pattern, management of misfire risk, and predictability of blast results. The following applies to most electronic detonators and certainly to Type i and Type u detonators.

Safe operations on the blast pattern

All manufacturers that allow personnel to engage in electrical or electronic interaction with detonators on the blast pattern have safety designs to prevent the detonator from firing. This aspect of the design of electronic detonators is critical to their safe operation. Manufacturers have been successful in these endeavours because electronic detonators have an injury-free record (as far as these authors are aware). Type i and Type u detonators are based on the principle of inherent safety: the electrical energy supplied to the detonators while personnel are on the blast pattern is insufficient to initiate the detonator, regardless of the fault condition in the detonator. This means that these detonators cannot fire when used with their own on-bench equipment even in the extreme cases of:

- a fusehead being directly connected to the input leads in the detonator (see Figure 1), or
- the firing switch in the ASIC being permanently closed or closing during at any time during logging

Misfires

Electronic detonators have 2-way communication between control equipment and the detonator, both during production and in the field during deployment and blasting. The full electronic functionality of the detonator can therefore be thoroughly tested in the factory. These include the communications, timing precision, the safety of the fusehead (to ensure it is not too sensitive), etc. Since the fusehead is also tested electrically and measured optically for size, the only possible failure of an as-shipped detonator is in the explosives train between the fusehead and the base charge of the detonator. This is very mature and extremely reliable technology.

Two-way communication with detonators is especially useful in the field. Detonators can be logged before deployment in the hole to ensure they are working (although with the reliability of modern products this is seldom done). More importantly they can be logged at any stage during or after deployment, and preferably shortly before the blast pattern is vacated. If a detonator fails to report back during such checks it is almost certainly due to damage to the legwires during loading and stemming. The operator then has the choice to follow one of these options:

- Check that the second electronic detonator in a double-primed explosives deck is working, to ensure that the deck will fire
- Tie in the backup pyrotechnic initiator if one is used
- Suck out the stemming and reprime the hole
- Note the exact location of the potential misfire so that it can be monitored during digging

The same checks of functionality are performed by the blasting equipment during the first stage of the firing sequence. If potential misfires are detected at this stage (which is unusual because of the earlier checks), then the blast should be aborted and the operators return to the blast pattern for remedial actions.

Two-way communication in electronic detonators reduces the chance of an unexpected misfire to an extremely low level. Expected misfires are usually caused by damage to legwires during deployment and are therefore controllable by the operators.

Predictable blast results

Unsafe results of blasting include mainly flyrock and overbreak causing unsafe highwall or hanging-wall conditions. Oversize fragments can be a safety issue (see Figure 4), but this is rare. Excessive ground vibration which is very effectively reduced by electronic timing, is not usually a safety issue.

Figure 4: Extreme examples of the hazards of flyrock and of oversized fragments

All unsafe blast results can have one or more of several causes, not least of which is the geology of the rock being blasted. However, timing also plays an important part. Every process in blasting, like dissipation of the shock wave, propagation of fractures, beginning of burden motion and full relief of burden requires a length of time that is characteristic of the geology, the borehole diameter, explosive type, burden and spacing, etc. For example it is often found that vibration signatures from adjacent holes will not be additive if the delay between them is longer than about 8ms. For large diameter surface blasting relief of burden can require 10 or more milliseconds per m of burden. Inadequately relieved

burden can cause flyrock and backbreak. These hazards are also more likely if holes in a row fire with too short an inter-hole delay, resulting in effectively simultaneous firing.

Blast designers are usually aware of the critical time delays that need to be obeyed for good and safe blast results. However, with pyrotechnic detonators it is difficult to avoid all chance of violating these critical delays.

Consider for example adjacent hole in a surface blast with in-hole pyrotechnic delays of 250ms each and an interhole surface delay = D ms (commonly in the range 10-100ms). The interhole delay of firing is typically normally distributed with a mean of D and a standard deviation of the root sum of squares of the standard deviations of all the delays in the train, in this case 250ms + D ms + 250ms. The precision of delays is best expressed as the coefficient of variation (CoV = standard deviation divided by mean). In this example the likely range of CoVs for pyrotechnic delays of 2, 3 and 5% will be considered. In Figure 5 below the time difference means the difference in time (in ms) between the designed time interval and the critical time interval for a particular blast result. Violation of this time difference can lead to an unacceptable and sometimes a hazardous blast result. Say for example a critical time delay to avoid adjacent holes cooperating to generate flyrock is 7ms and the blast is designed with an interhole delay of 17ms. Then the required time difference for safe blasting is 10ms, but because of timing scatter, there is a probability of violating 10ms. Now consider pyrotechnic delays with a very good CoV of 2%. The circle in Figure 5 shows that the probability of violation of the required 10ms time difference is 8%.

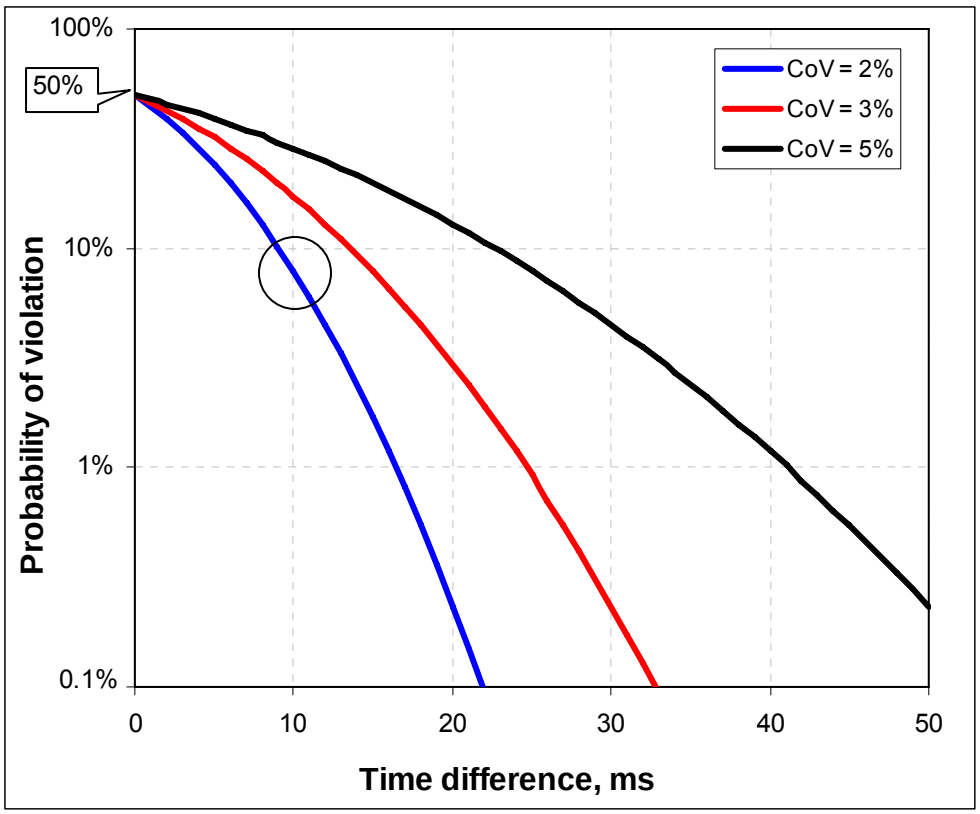


Figure 5: Probability of violating a required time difference with pyrotechnic detonators

The practical problem for safe blasting is that this probability applies to every adjacent hole pair in a blast. A blast with 5 rows of 41 holes each will have 200 pairs of adjacent holes. The statistics discussed above mean that there will be 8% or 16 pairs of holes firing close enough in time to generate flyrock in *every* such blast. This is why pyrotechnic blasting is far less predictable than electronic blasting, and why electronic systems give better and safer blast results with a much smaller probability of surprises.

## Conclusion

Electronic detonators are safe to handle because of sophisticated safety features inherent in their design. Test data for RF hazards and stray electricity show that electronic detonators are orders of magnitude less vulnerable than electric detonators and much less vulnerable than humans to most electrical stimuli. These data show that in general electronic detonators are likely to be safe if humans are safe, but manufacturers'' recommendations should still be followed at all times. The testability and 2-way communication ability greatly reduces the probability of unexpected misfires. Timing precision makes blasting more predictable and in particular avoids the often high probability of violating a time interval that is critical to safe blasting.

## References


CEN TS 13763-27 July 2003: Explosives for civil uses – Detonators and Relays – Part 27: Definitions, methods and requirements for electronic initiation systems.

El-Sharkawi, M.A., 2005, "Electric Energy an introduction", CRC press.

IEEE C95.1 - 2005 Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz.

IME Safety Library Publication #20: July 2001, "Safety Guide For The Prevention Of Radio Frequency Radiation Hazards In The Use Of Commercial Electric Detonators (Blasting Caps)". August 2008, "Addendum to SLP-20: Acceptable Field Strength for Wireless Devices in Close Proximity to Electric Detonators".

Helfrich, W.J. and Reynolds, R.L., 1985, "Safety Grounding – A performance Approach" IEEE 1985 Mining Industry Technical Conference, Golden CO.

Lownds, C.M., Lindenau, J., 2008, "Electronic Detonators and Lightning", 34th Annual Conference on Explosives and Blasting Technique, International Society of Explosives Engineers.

Lownds, C.M., Steiner, U., 2009, "Electronic Detonators and Lightning – part 2", 35th Annual Conference on Explosives and Blasting Technique, International Society of Explosives Engineers.