Chambers C., Hookham S., Clay M. (2017). *EU type certification of non-standard Electronic Initiations Systems used in blasting at mines and quarries.* Paper presented at the 43rd Annual Conference on Explosives and Blasting Technique, ISEE 2017, Jan. 29 – Feb. 1 Orlando, Florida

Open access paper available at www.hsl.gov.uk

EU type certification of non-standard Electronic Initiations Systems used in blasting at mines and quarries

Colin Chambers, Susan Hookham, Matthew Clay

GB Explosives Notified Body (ENB), Health and Safety Executive, UK.

Abstract

Opencast (quarries) and underground mines around the world use blasting methods to mine valuable ore. Traditional blasting systems use technologies such as electric delay detonator systems (developed in the 1950s) and non-electric detonator systems (developed in the 1970s) to initiate a detonation train to blast rock more effectively, and so retrieve valuable product more efficiently. However, the lack of precise control over blast timings with these approaches can result in undesirable outcomes such as significant flyrock, excessive ground vibration, uneven grade of rock and misfires (in which sections of the blast can remain unfired). The development of Electronic Initiation Systems (EIS), first used in the 1990s, introduced a higher level of control over the blast. These systems greatly reduce the negative issues associated with blasting. However, this precision introduces complexity, and with this complexity comes difficulty in demonstrating the predictability, safety and reliability of such systems.

The European Commission require that all commercially available explosives placed on the market in the European Union are safe and reliable to use and that risks to people and property are identified and controlled. To this end, the European Commission produced the Civil Uses Directive 93/15/EEC (now recast as Directive 2014/28/EU) which details the Essential Safety Requirements (ESR) for explosives including detonators. Harmonised standards have been produced to evaluate conformity with the ESR requirements. In the case of detonators the harmonised standard is BS EN 13763:2004 parts 1 to 25. In addition, there is also a Technical Specification, DD CEN/TS 13763-27:2003, (TS), which is not harmonised and applies to the EIS, including both electronic hardware and programmable electronic aspects. Other Directives also apply to EIS, for example: Low Voltage (LVD), Electro Magnetic Compatibility (EMC) and Radio Equipment (RED). Relevant parts of harmonised standards associated with these directives are also adhered to by the manufacturers of EIS. To show that all of these requirements have been applied, these systems are required to be assessed and CE marked by an European Union (EU) Explosives Notified Body (ENB). The Great Britain (GB) ENB is based at the Buxton site of Health and Safety Executive's (HSE) Science Division.

This paper presents the benefits of electronic blasting systems. An outline of a generic EIS is presented, highlighting some of the technical complexities involved.

This paper also discusses the TS, which was published in 2003, its application to rapidly evolving EIS that constantly strive to take advantage of new technical developments, (BSI 2003) and how these new technological developments can be appropriately assessed to meet EU legislative requirements. This paper describes an approach developed by the GB ENB to assess such systems, using a generic EIS to highlight key issues covered in the assessment process.

Chambers C., Hookham S., Clay M. (2017). *EU type certification of non-standard Electronic Initiations Systems used in blasting at mines and quarries.* Paper presented at the 43rd Annual Conference on Explosives and Blasting Technique, ISEE 2017, Jan. 29 – Feb. 1 Orlando, Florida

Open access paper available at www.hsl.gov.uk

Introduction

Opencast (quarries) and underground mines around the world use blasting methods to mine valuable product. Traditional blasting systems use technologies such as electric delay detonator systems (developed in the 1950s) and non-electric detonator systems (developed in the 1970s) to initiate a detonation train to blast rock effectively, and so retrieve valuable product efficiently. However, the lack of precise control over blast timings with these approaches can result in undesirable outcomes such as significant flyrock, excessive ground vibration, uneven grade of rock and misfires (in which sections of the blast can remain unfired). The development of Electronic Initiation Systems (EIS), first used in the late 1990s, introduced a higher level of control over the blast. This greatly reduced many of the negative issues associated with blasting as described later in this paper. However, this precision introduces complexity, and with this complexity come difficulties in achieving and demonstrating the predictability, safety and reliability of such systems. The European Union (EU) requires that an EIS is shown to comply with relevant legislation before it can be placed on the market and used in the EU to show that the risks associated with blasting are minimised.

Civil Uses Explosive Application in the EU

The free movement of goods in the EU requires safety standards for goods to be harmonised. The CE mark demonstrates that a product complies with the harmonised safety standards in the EU. Electronic detonators, which form part of an EIS, are classed as Civil Uses Explosives covered by EU Directive 2014/28/EU, (EC 2014a).

The Explosive Regulations that implement the Directive (EC 2014a) state that no person shall place any explosives on the market unless:

- The explosive satisfies the Essential Safety Requirements (ESR) as laid down by the Directive.
- Conformity of the explosive with the ESR has been assessed by a Notified Body.
- The CE mark has been affixed to the explosive.

Harmonised test standards have been produced to evaluate conformity with these ESR. In the case of detonators the harmonised standards are BS EN13763 part 1 (requirements) and parts 2-25 published in 2004, (EC 2004). In addition, there is also a Technical Specification DD CEN/TS 13763-27: 2003, (TS), which is not harmonised and apply to the EIS, including both electronic hardware and programmable electronic aspects, (EC 2003). Other Directives that apply to EIS are, for example: Electro Magnetic Compatibility (EMC), Low Voltage (LVD) and Radio Equipment (RED) (EC 2014b, 2014c, 2014d). Relevant parts of harmonised standards associated with these directives are also adhered to by the manufactures of EIS. To show that all of these requirements have been applied, these systems are required to be assessed and then CE marked by an EU Explosives Notified Body (ENB). In the UK this is the GB ENB run by the Health and Safety Executive's (HSE) Science Division.

Problems Associated with Quarry and Mine Blasting

There are a number of factors associated with blasting that need to be minimised for a blast to satisfy local, national and international regulations and commercial requirements, namely:

- Fragmentation used in this sense refers to the general size of the individual pieces of rock after blasting has occurred. It is generally desirable that the resultant rock fragments are approximately uniform in size and are sufficiently small as to minimise the amount of post processing required.
- 'Flyrock' refers to individual pieces of rock that are projected by the blast in an undesired direction potentially leading to risk of injury to people and damage to property.

- Ground vibration is caused by detonation of explosives on or in the ground. The effects of ground vibration increase significantly in quarry blasting because of the multiple detonations usually combined in a single blast.
- Misfire refers to the complete or partial failure of a blasting charge to detonate as planned. Hence the explosive materiel could explode at some time during product removal.
- Unintended firing refers to the firing of a blasting charge when it was not intended.

Manufacturers of EIS have shown through experience that initiating detonators in sequence with predicable and reliable millisecond control of the time delay between each detonation can greatly reduce these undesirable attributes. This level of control allows consideration of varying quarry bench conditions to be accounted for in the blast design.

Electronic detonators (first developed in the 1990s) use programmable microelectronics to initiate up to hundreds of detonators in a single blast, each one uniquely identified and with a precise delay programmed on site at the quarry or mine. The blast pattern can be designed on a computer and then downloaded to the electronic detonators. All the detonators receive the fire signal instantly removing the potential for any 'cut off' in the blast pattern.

Electronic Initiation Systems and their Operation

Electronic detonators (Figure 1) rely upon passing an electric current through an Initiation Element (IE) to cause a small quantity of high explosive material to detonate. This in turn initiates the secondary explosives which have been placed around the detonator. The IE is typically a resistive heating element surrounded by an ignition mixture and a primary explosive, all contained within the body of the detonator.

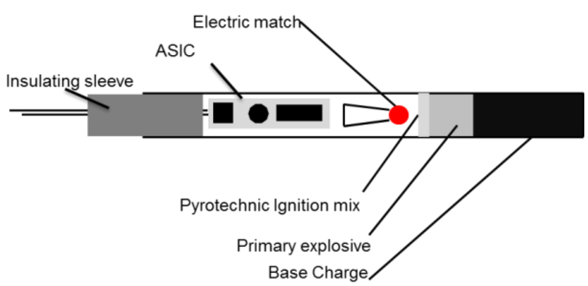

Figure 1. Electronic delay detonator

Detonators in an EIS are typically based on the simplified architecture shown in Figure 2. The exact architecture will vary between manufacturers.

The detonator is connected to a communications line, which also supplies current to power the microcontroller and charge the firing capacitor as well as facilitating communication between the detonator and other devices within the EIS. This communication is typically two-way, such that the detonator can receive commands from, and report its status back to, the firing unit. The detonator often contains a power supply capacitor which enables the microprocessor to function correctly if power is removed from the communications line. This can facilitate a safe shutdown, for example discharging the firing capacitor upon loss of communications. Additional hardware measures also ensure safe discharge of the firing capacitor to prevent a misfire.

Chambers C., Hookham S., Clay M. (2017). *EU type certification of non-standard Electronic Initiations Systems used in blasting at mines and quarries.* Paper presented at the 43rd Annual Conference on Explosives and Blasting Technique, ISEE 2017, Jan. 29 – Feb. 1 Orlando, Florida

Open access paper available at www.hsl.gov.uk

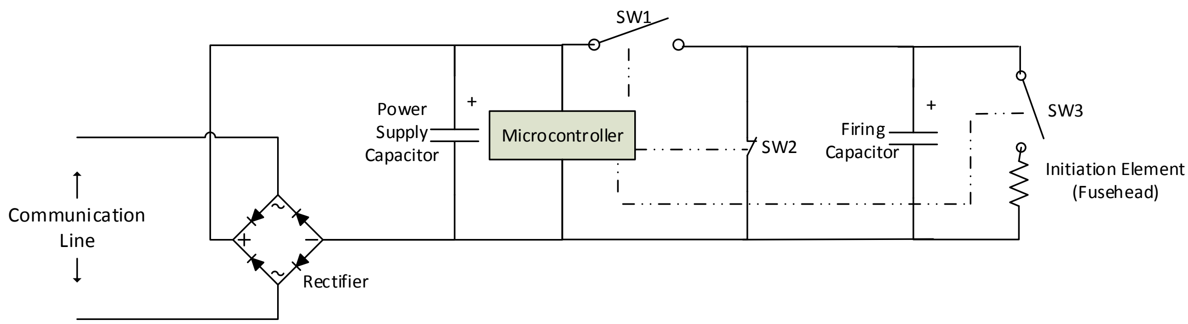

Figure 2. Simplified electronic detonator circuit diagram

The most complex device within the detonator is the microcontroller. This can be a generic microcontroller or an Application Specific Integrated Circuit (ASIC), see Figure 1. The microcontroller processes commands received from the communications line and fires the detonator element by closing a switch. This allows energy stored within the firing capacitor to be rapidly delivered across the initiation element. The firmware running on the microcontroller enforces a protocol designed by the manufacturer to avoid unintended initiations and to prevent misfires. The protocol used is manufacturer specific and typically involves a number of unique commands that execute the firing sequence, with various 'health checks' being reported back from the detonator at each stage.

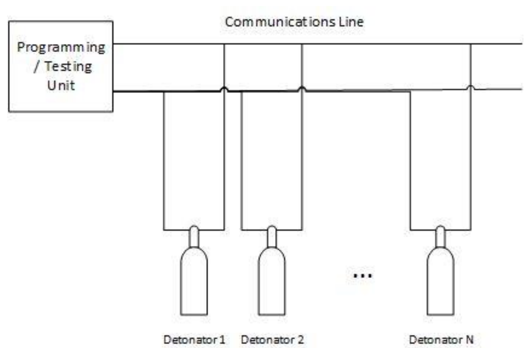

Figure 3. Detonators connected to integrated programming/testing unit via a communications line

EIS typically include a firing unit, programming and/or testing unit and electronic detonators, often programming and testing functions are integrated into the same device. The programming/testing device is connected to either a single detonator or a group of detonators via the communications line as shown in Figure 3. The device is used primarily to program the detonators with a specific delay time and also register the detonator's unique identifier. The device is often able to perform diagnostics on the detonators confirming continued communications and that any self-testing (for example by the microcontroller) has been successfully executed.

The EIS programming and testing units incorporate inherently safe principles. For example, they are incapable of generating sufficient voltage to initiate a detonator, even in fault conditions. Similarly they do not contain the 'Arm' and 'Fire' sequence commands. Programming and testing can be performed manually or via blast design software, which facilitates more complex blast designs. After programming/testing and the evacuation of the blast area, the firing unit can be connected to the detonators. The connection of the firing unit to the communications line is shown in Figure 4.

Chambers C., Hookham S., Clay M. (2017). *EU type certification of non-standard Electronic Initiations Systems used in blasting at mines and quarries.* Paper presented at the 43rd Annual Conference on Explosives and Blasting Technique, ISEE 2017, Jan. 29 – Feb. 1 Orlando, Florida

Open access paper available at www.hsl.gov.uk

The firing unit provides sufficient voltage and current to charge the detonators' firing capacitors up to a level which can reliably initiate the blast. The firing unit typically enforces additional checks, over and above those already performed by the programming unit. Once the required final tests are concluded successfully, the firing unit can be put into an 'Armed' state from which the blast can be initiated. The blast can be aborted by the operator or by the EIS itself, at any time before the fire command has been issued. The 'Abort' command results in the detonators being placed into a safe state with their firing capacitors discharged and incapable of firing.

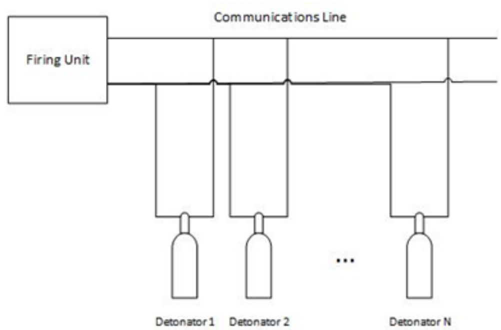

Figure 4. Firing unit connected to detonators

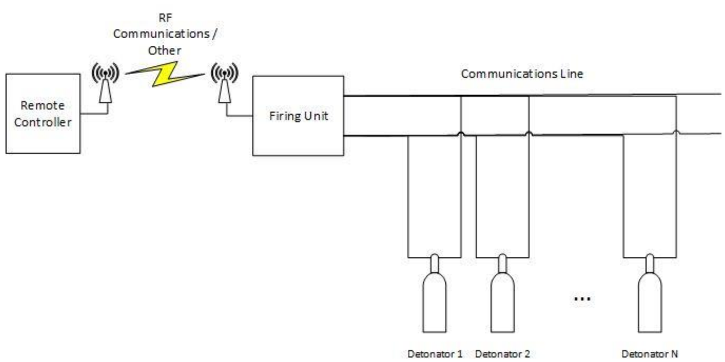

Figure 5. Firing unit operated remotely via RF communications

The firing unit can be connected to the detonators by a lead wire used for communication and for charging the firing capacitors. In some cases this is not practicable and therefore the firing unit is connected to a remote device over a Radio Frequency (RF) link as shown in Figure 5. This configuration requires an operator (albeit for a short exposure time) to connect a device which is capable of generating blast voltages to the communications line whilst the operator is closer than would be considered safe. Therefore, these systems incorporate additional measures to prevent the firing sequence being sent prematurely. Some EIS incorporate limited data logging, such that a record of the blast can be kept. For example, some systems allow a blast to proceed with a limited number of detonators unable to initiate if this is deemed safe and acceptable by the operator. The system can keep a record of which detonators were not functional.

Issues Associated with EIS and their Assessment

EIS have a good track record for reliability and safety since their deployment into the marketplace. However, as with any engineered system, zero risk is unattainable and there are a number of failure modes, which manufacturers and Explosives Notified Body's need to understand and assess. The main undesirable outcomes of EIS failure are: unintended initiation, misfires and timing errors. These outcomes can lead to safety hazards as well as being costly to the mine in lost production. Misfires can result in damaged but live detonators in a blast hole surrounded by secondary explosive in close proximity to people. Any failure which affects the ability of EIS to initiate an explosion reliably (e.g. a harness continuity problem) can lead to safety hazards.

All EIS need to be designed and assessed to take into account the possibility for hardware and software mal-operation. Hardware problems can be defined as one of two types. Random hardware faults (referred to in the TS as 'hardware stochastic' faults) are faults in individual components, which are probabilistic in nature and would be expected to occur even in well-designed systems. For example, if a 'bleed' resistor used to safely discharge a detonator firing capacitor after a given period fails 'open circuit', this could result in an increased risk of misfire leading to harm to people or damage to property. The second type is systematic design errors (referred to in the standard as 'hardware design faults') and these are effectively weaknesses in the design, which might be undetected during normal operation. An example of this would be a designer specifying the wrong component parameters (e.g. the wrong working voltage for a firing capacitor). The increasing use of firmware (e.g. software running on a firing unit's microprocessor) and software (e.g. blast design PC software) means that what the TS defines as 'software faults' must also be considered (BSI 2003). Software faults are systematic in nature, i.e. the result of a specification/design flaw. Software faults can either defeat functionality entirely or make functions behave unpredictably. For example, the blast sequence implemented in a firing unit sends a sequence of commands typically interspersed with various checks in between each one (e.g. to verify communication.) If these checks are omitted, or the sequence is issued without the operator requesting it, then a misfire or unintended initiation could occur. The challenge with software is that often faults only manifest themselves in particular combinations of circumstances, making testing challenging. Therefore, software faults must be given careful consideration and techniques such as defensive programming adopted to avoid failure.

It is also important that as well as each device within an EIS working correctly and within its specification that the system as a whole works correctly as intended. For example some functions (such as blast abort) rely upon several devices and communications media to operate correctly in conjunction with each other to achieve the end result. Similarly, influences outside of the system itself need to be carefully considered, for example Electromagnetic Interference, stray/induced currents, operator errors, mechanical shock and thermal influences. Importantly the TS prescribes fault tolerance requirements that guard against the numerous faults and failures that can and do occur, (BSI 2003). For example, the standard states that an unintended initiation should not occur even in the presence of two independent faults anywhere in the system. This includes diverse types of fault, for example the combination of a random hardware fault in the detonator together with a software fault in the firing unit.

Assessment to CEN/TS 13763-27

The stated aim of the TS is to enable EIS to reach the same levels of safety and reliability as corresponding standards do for none-electronic delay detonators, (BSI 2003). Given the levels of complexity associated with EIS a detailed set of assessment criterion need to be satisfied and these are given in the Technical Specification (TS), (BSI 2003). The TS specifies a risk analysis, evaluation and testing procedure to investigate the safety and reliability of EIS by identifying hazards and estimating the risks associated with these hazards. Where the risks are not considered to be acceptable, further risk reduction is required to be implemented. The thrust of the TS is to demonstrate robustness of design, implementation and operation by subjecting EIS to testing of required functionality, key physical and environmental factors and tolerance of faults (BSI 2003).

Areas Not Well Covered in CEN/TS 13763-27

Because of the generic assumed functionality of an EIS the TS can state how the EIS and its devices should be tested and what success looks like in terms of demonstrating functional safety and meeting the ESR of the Directive, (EC 2014a). The TS uses a mixture of goal orientated requirements and prescriptive requirements, thus allowing a degree of flexibility in demonstrating how the requirements of the TS are met (BSI 2003). However, this approach has limitations in that the prescriptive requirements are in danger of becoming obsolete as soon as any significant EIS design paradigm changes are introduced. The TS assumes that the traditional mechanisms of performing a blast sequence will remain constant even if new technology is used, (BSI 2003). This mixture of goal setting targets and prescriptive requirements generally works well providing that technology does not make the prescriptive requirements obsolete.

Only the relevant sub clauses in the TS need be evaluated for each EIS to be assessed. This might seem to solve the problem of accounting for new technology or approaches to the blasting process, but this is not necessarily the case (BSI 2003). An example of a goal oriented requirement from the TS is sub-clause 4.5.1.2.2 "Evaluate that the detonator cannot reach unsafe states in ways other than intended" (BSI 2003). This is likely to remain valid regardless of the technology employed or how that might change in the foreseeable future. An example of a prescriptive requirement from the TS is sub-clause 4.5.1.2.3 "evaluate that five minutes after interruption of the firing sequence, or if the detonator is disconnected from the wire system, the shot firing capacitors shall not offer sufficient energy to allow a blast" (BSI 2003). EIS design changes could make the shot firing capacitor obsolete, by replacing the firing capacitor with an alternative means of energy on the detonator. The detonator design could still provide sufficient safeguards, which could be demonstrated to be sufficiently reliable and safe, to ensure that a blast cannot continue in the event of an interruption in the firing sequence from any means, but this might not comply with sub clause 4.5.1.2.3 of the TS (BSI 2003). We can see from this hypothetical example, how limitations in potentially 'out of date' standards and Codes of Practice (CoP) such as the TS could raise difficulties in evaluating a novel EIS design.

An existing technology that is not directly covered in the TS is the application of an RF link used to replace a section of lead wire that connects, in full or in part, the firing unit to the detonators, see Figure 5, (BSI 2003). When assessing an EIS with an RF link, the assessment was approached on two fronts. Firstly, all the relevant issues assessed on EIS using only wired links between EIS devices were also considered with respect to an EIS that utilised an RF link. This covered issues such as communication integrity, interference from external sources, and EIS behaviour in the presence of faulty communication links. Secondly, conformity of the RF subsystems to relevant directives such as the Radio Equipment Directive (RED), Low Voltage Directive (LVD) and Electromagnetic Compatibility Directive (EMC) was determined (EC 2014b, 2014c, 2014d). The LVD and EMC directives were already applied to EIS with conformity documentation supplied as part of the ENB assessment process. RF subsystems were not assessed by the GB ENB to these directives, but instead checks were made to see that relevant harmonised standards and CoPs were cited and that reputable certified test houses had performed the testing to the relevant standards and that relevant reports and certificates of conformity were supplied, (BSI, 1999, 1990, 2002, 1996, 1997, 1984). This is not a direct requirement of the TS but was considered necessary by GB ENB to the assessment and to demonstrate that the ESR' of the Directive were met, (BSI 2003, EC 2014a). This approach helped GB ENB develop its ability to assess EIS containing new technologies that are not directly covered by the TS (BSI 2003).

New Developments on the Horizon

The TS aims to be both generic and goal setting to a degree but it still does not adequately cover new and emerging technologies used in other industries that could find application in the civil blasting industry (BSI

2003). These technologies are not yet deployed in EIS probably because of the hazardous nature of the mining and tunnelling industries with respect to their use of explosives. However, companies that develop EIS will be aware of new technologies and will be considering how they could take full advantage of the improved performance, flexibility and development costs from utilising new technologies in the development of new EIS.

A group of technological advances extensively discussed on the internet and widely expected to be developed further in industry is the 'Internet of Things' (IoT) (ITU 2012). This is often discussed in reference to ‘smart home’ and ‘smart office’ and can also refer to the use of distributed computing power, software tools and smart control systems over a network structure not unlike the internet. An example of the IoT could be the connection of devices used in industrial applications, to a communications network accessed by a company and their clients so that ‘smart devices’ can communicate with each other and with engineers remote from the point of use. For the mining industry, the point of use of specific EIS would be the mine, quarry or tunnel. Such systems could be used to perform activities such as field trial control and the collecting and analysis of blast data in real time, optimising EIS performance parameters such as detonator delay times and performing advanced real-time diagnostics that can be analysed by EIS developer engineers regardless of where they are based.

Approaches like those associated with the IoT must give priority to safety, reliability and security. Technologies like IoT should not be used on safety critical tasks until they are mature and proven in use through many years of use in non-critical applications and have been subjected to rigorous testing. Explosive Notified Bodies might not be equipped to assess all such systems and it is likely that such systems would not be awarded a CE mark at the current time because of the uncertainties associated with their safety, reliability and security and their demonstrable compliance with relevant legislation. Other examples of new technologies that could possibly be used in EIS designs might be a ‘system on a chip’ device preprogramed for a specific (entire) blast and initiated over a 4G mobile network. The blast could be designed and simulated remotely using geological and geographical information for the mine/quarry in question. This would facilitate remote blasting on a different scale to that performed at present.

With any network based or remotely operated EIS, cyber security is a key issue. At present, existing mines security and electronic validation including password protection within EIS will cover most requirements. However, this could potentially be an area of rapid expansion in blasting systems if/when the IoT approach starts to be considered for remote access of blasting preparation and control (ITU 2012). Another technology that could be employed in the near future is a permanent energy source replacing the firing capacitor on an electronic detonator. Such a system would require a rigorous demonstration to show that the relevant Directive’s ESR’ have been met.

Approach Adopted by GB ENB to Include New Technologies for CE Mark

How can technologies not directly covered by the TS be appropriately assessed to meet EU legislative requirements (BSI 2003)? This paper describes the approach applied by the GB ENB to assess such systems:

1. Identify new technologies associated with the EIS i.e. those that are not clearly directly covered by the TS (BSI 2003).
2. Identify hazards associated with the new technology.
3. Identify relevant directives and standards.
4. Determine the status of the new technology sub systems with respect to relevant directives, e.g. are relevant subsystems already CE marked or have relevant certificate(s) of conformity.

5. Determine what relevant demonstrations are required for the new technologies based on meeting the Directive ESR.
6. Incorporate this information into the assessment performed to the TS, (BSI 2003).
7. Where relevant, require demonstrations to be reviewed by external competent persons/organisations.

This approach has been applied to the assessment of EIS that included an RF subsystem used to replace a section of lead wire connecting the blasting unit to the detonators.

Conclusions

The aim of the paper has been to paint a picture of EIS used in quarries and mines in the EU, how such systems are regulated, and what impact new technology can have with regard to meeting some of the requirements of regulation. To fulfil this aim, this paper has looked at the EIS, which is typically based on programmable electronics, which are complex in their design and operation. EIS have been shown to give benefits with regard to safety and reliability. The benefits are mostly derived from millisecond delay timing of individual detonators thus facilitating precise control of blasting scenarios. The main outcomes of this precise control are: better fragmentation leading to reduced post blast processing of the mined material and reduced ground vibration and flyrock, partially due to a reduced quantity of explosives required, leading to reduced collateral damage to property and increased safety to people. The EU decided that EIS should be at least as safe and reliable as existing blasting systems, which require CE marking if they are to be sold in the EU. The EU concluded that EIS are complex when compared to conventional electric blasting systems and shock tube systems. Therefore, to apply existing legislation to EIS and to account for the programmable electronic aspects of the EIS, a TS was produced in 2003, to help ensure that the EIS met the ESR of Directive 2014/28/EU (BSI 2003, EC 2014a). However, since 2003 technology has moved on and the TS might not now cover all of the new technologies in the same way that it did when first published, (BSI 2003). The approach described in this paper has been used by the GB ENB to allow some new technologies to be assessed and part of the CE type certification process. This approach uses existing related EU legislation to fill in for gaps in the relevant TS [CEN 2003]. It is suggested that this approach can be taken further than it has at present, but this would be considered on a case by case basis. There are however, limitations to this approach in that the new technology must satisfy the Directive ESR and this must be demonstrable to the relevant ENB, (EC 2014a). Without a successor to the TS divergence between ENBs is possible with regard to what constitutes demonstration of the Directive ESR for new technologies in the future (BSI 2003).

Disclaimer

This report and the work it describes was funded by the Health and Safety Executive (HSE). Its contents, including any opinions and/or conclusions expressed, are those of the authors alone and do not necessarily reflect HSE policy.

References

EC, (2014a), Directive 2014/28/EU, Explosives for civil uses, European Commission.

EC, (2014b), Directive: 2014/30/EU, The Electromagnetic compatibility (EMC), European Commission

EU, (2014c), Directive 2014/35/EU, The Low Voltage Directive (LVD), European Commission

EU, (2014d), Directive 2014/53/EU, Radio Equipment Directive (RED), European Commission

BSI, (2004), BS EN 13763-1 to 26:2004, Explosives for civil uses – Detonators and relays, Parts 1 to 26: Definitions, methods and requirements for electronic initiation systems, BSI

BSI, (2003), DD CEN/TS 13763-27:2003, Explosives for civil uses – Detonators and relays -, Part 27: Definitions, methods and requirements for electronic initiation systems, BSI

BSI, (1999), BS EN ISO/IEC 17025; General requirements for the competence of testing and calibration laboratories (ISO/IEC 17025:1999), BSI

BSI, (1990), BS EN 60870-5-1; Telecontrol equipment and systems — Part 5: Transmission protocols — Section 1: Transmission frame formats (IEC 60870-5-1:1990), BSI

BSI, (2002), BS EN 61000-4-3; Electromagnetic compatibility (EMC) — Part 4-3: Testing and measurement techniques. Radiated, radio-frequency, electromagnetic field immunity test (IEC 61000-4-3:2002), BSI

ITU, (2012), Series Y: Global information infrastructure, Internet protocol aspects and next-generation networks, next generation Networks – Framework and functional architecture models, Overview of the Internet of things, ITU-T Y.2060, International Telecommunication Union