CyberDet I™ Wireless Detonator System
User Training Manual
UTM-00353 | Rev 12

Page Left Intentionally Blank

TABLE OF CONTENTS

TABLE OF FIGURES

Page Left Intentionally Blank

1 USERS OF THIS MANUAL

DetNet endeavours to upgrade the CyberDet I software regularly to comply with new challenges and needs faced by users in the market. As new software becomes available, the DetNet version control policy requires that all control equipment be upgraded to ensure support is provided on the latest software version as deployed on customer sites.

1.1. Purpose of this manual

The purpose of this manual is to provide a step-by-step guideline explaining how to successfully deploy, verify and perform a blast using the DetNet CyberDet I.

This manual is only to be used for the CyberDet I and the applicable software version as displayed.

1.2. End User

1.2.1. Requirements

- Only trained and competent personnel are allowed to operate the system.
- Users of the system shall be aware of the recommended procedures for using the CyberDet I as per the manufacturer's recommendations.
- These recommendations do not supersede the method as required by local mine, explosives, or statutory regulations / procedures / codes of practise regarding the use of detonators. In such cases, the MOST STRINGENT set of rules between the mine, explosives or local regulations/procedures/codes of practise and the manufacturer must be followed.

1.3. Training

Training and software upgrades shall only be performed by a subject matter expert of DetNet SA or its channel partners.
Contact the DetNet head office for additional information.

ALL USERS OPERATING THE CYBERDET I SHALL HAVE SUCCESSFULLY COMPLETED THE SPECIFIC TRAINING BEFORE PERFORMING ANY WORK WITH THE DEVICE(S).

1.4. Information

Refer to http://www.detnet.com/ for additional detail and documentation.

2 CYBERDET I PRODUCT SAFETY

ELECTRONIC WIRELESS DETONATORS ARE TOTALLY DIFFERENT TO CONVENTIONAL WIRED ELECTRIC DETONATORS AND ABSOLUTELY NO CONNECTION WITH CONVENTIONAL ELECTRIC DETONATORS OR ANY OTHER ELECTRONIC DETONATORS SHOULD BE ATTEMPTED AS IT CAN LEAD TO UNINTENDED INITIATION. ALL USERS OPERATING THE ELECTRONIC WIRELESS INITIATION SYSTEM SHALL HAVE SUCCESSFULLY COMPLETED THE SPECIFIC TRAINING BEFORE PERFORMING ANY WORK WITH THE DEVICE(S). DO NOT USE ANY DEVICES OTHER THAN THOSE SPECIALLY DESIGNED FOR THIS TYPE OF ELECTRONIC DETONATOR.

2.1. DetNet Safety Philosophy

DetNet safety philosophy is to design, manufacture and provide control equipment, detonators and accessories to the highest safety standards.

- BlastCards remain in possession of the accountable person and should only be used to authorize the blast process at such a time as stipulated by the Mine after completion of the required Risk Assessment.
- All products must conform to local and international standards before they are sold for use.
- DetNet complies to ISO 9001, SANS 551:2009, CEN/TS 13763-27 which is acceptable to countries we operate in; in countries not subscribing to the above marks, we advise users to engage with DetNet to ensure that all equipment complies to local regulations.

2.2. User Safety

Safety is ensured when the user supplements the product's in-built safety systems through adequate training in the safe use of the product:

- Induction training
- Refresher training

DetNet continuously upgrades software to make our products more user friendly and to ensure that users stay abreast of latest developments, it is important that users get trained on the relevant changes before their equipment is updated.

USERS WITH A CARDIAC PACEMAKER MAY NOT OPERATE THE EQUIPMENT OR BE IN THE VICINITY OF A DEPLOYMENT.

2.2.1. Battery Safety and Emergency Situations

- Leaking Batteries If the battery pack leaks electrolyte, avoid contact with the leaking liquid or gas. If one is exposed to the leaked substance, immediately perform the actions described below.
- Inhalation: Evacuate the contaminated area and seek medical attention.
- Contact with eyes: Rinse eyes with flowing water for 15 minutes and seek medical attention.
- Contact with skin: Wash the affected area thoroughly with soap and water and seek medical attention.
- Ingestion: Induce vomiting and seek medical attention.
- Fire - NO WATER! Only dry powder fire or carbon dioxide extinguisher can be used; if possible, move the battery pack to a safe area before it catches fire.
- Wet Batteries - if the battery pack is wet or submerged in water, this could cause a short circuit. Do not attempt to recharge or use the battery. Isolate immediately and contact Pylontech or an authorized dealer for technical support.

- Damaged Batteries - damaged batteries are dangerous and must be handled with the utmost care. They are not fit for use and may pose a danger to people or property. If the battery pack seems to be damaged, pack it in its original container, and then return it to the supplier.

2.3. Transportation, Storage and Handling

The CyberDet I equipment must be transported, stored, handled, and used in conformity with all federal, state, provincial and local laws and regulations. Control equipment and accessories should be handled with due care and not dropped, mishandled, subjected to excessive vibration, or exposed to any chemical agents. Connectors should be kept clean, and the equipment must be kept in a safe environment to avoid misappropriation or misuse.
Verify that in the Storage State the Tx shall be switched off.
Verify that in the Storage State Rx units shall be kept in their storage containers.
Verify that receivers, detonators and boosters are shipped separately.

2.4. Maintenance Schedule

All equipment in the field will need to be returned to DetNet, or its repair centres, for service at the following intervals:

- Handheld Equipment (Tagger, etc.) – 18 Months.
- Other equipment (Excluding accessories) – 24 Months.

Other Care and Maintenance

- Inspect the transmitter enclosures to ensure no moisture or dust ingress - 3 monthly.
- Visual inspection of antenna cable and connectors to ensure no damage - Every time it is used.
- Battery - As per manufacturer specification.
- Transmitter – 1000 running hours (Tx has built in timer that counts the hours in operation, warning at 900 hours).

2.4.1. Battery Care and Maintenance

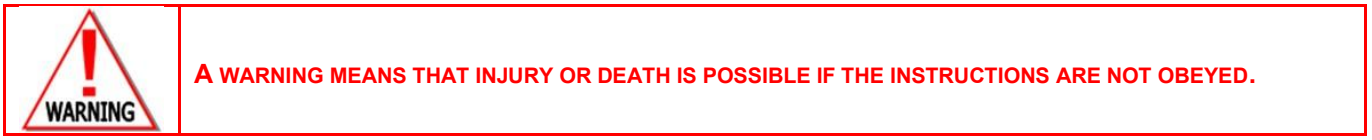
- If the battery is stored for a long time (Long Storage 4-6 Months), the battery must be charged once every six months, and the SOC should be no less than 90%.
- Battery needs to be recharged within 12 hours, after fully discharged.
- Every 12 months since the procurement of the CyberDet I System, the condition of power connectors, grounding points, power cable and screws are to be checked. Make sure there is no loose, no broken, no corrosion at connection points.

2.5. Information in case of emergency

Refer to http://www.detnet.com/ for additional detail and documentation.

2.6. Warning, Caution, and Note Statements

WARNING, CAUTION, and ***NOTE*** statements are used throughout this manual to emphasise important and critical information. Observe these statements to ensure safety and to prevent product damage. The statements are defined as follows:



Warnings draw special attention to anything that could injure or kill the reader/ user. *Warnings* are generally placed before the step in the procedure they relate to. Warning messages are repeated wherever they apply.

A CAUTION MEANS THAT DAMAGE TO EQUIPMENT IS POSSIBLE.

Cautions draw special attention to anything that could damage equipment or cause the loss of data and will normally describe what could happen if the caution is ignored. *Cautions* are generally placed before the step in the procedure they relate to.

Notes are added to provide additional information.

Notes are used to emphasise important information by visually distinguishing this from the rest of the text. Notes can contain any type of information except safety information, which is always placed in cautions or warnings.

Refer to http://www.detnet.com/ for additional detail and documentation.

2.7. Disclaimer

This document forms part of the User Manual for the CyberDet I and is confidential. This document contains restricted information for company and channel partners' application only.
Should any of the restricted information contained in this document be disclosed to any third party either intentionally or unintentionally, DetNet South Africa will not be held responsible, accountable or liable for any resulting event and or issue.
DetNet accepts no liability in respect of any claim relating to any safety related incident, damage, loss or injury arising from the use of any software and/or control equipment supplied by DetNet. Any liability which may be lawfully attributed to DetNet shall not exceed the purchase price paid to DetNet for the software and/or control equipment which gave rise to the claim. DetNet shall not be liable for lost profits, goodwill, data or business nor any special, indirect, incidental or consequential damages under any theory of liability.

2.8. RF compliance - FCC (USA) and ICES (Canada)

2.8.1. Unauthorised Changes

DetNet South Africa has not approved any changes or modifications to this device by the user. Any changes or modifications could void the user's authority to operate the equipment.

2.8.2. Declaration of conformity

The equipment complies with the requirements of the:
Australian Communications and Media Authority (ACMA) Standards made under the *Radiocommunications Act 1992 and the Telecommunications Act 1997*.
South African Act and Regulations in terms of the Mine Health and Safety act No.29 of 1996
IEC61010-1: Safety Requirements for Electrical Equipment for Measurement, Control, And Laboratory Use - Part 1: General Requirements
IEC62368-1: Audio/video, information and communication technology equipment – Part 1: Safety requirements

IEC61508: Functional Safety of electrical/electronic/programmable electronic safety-related systems
EU Low Voltage Directive 2014/35/EU
EU EMC Directive 2014/30/EU
EU Explosive Directive 2014/28/EU
EU Radio Equipment Directive 2014/53/EU Electronic Communications Act (ICASA) exemption due to the very low operating frequency.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

2.8.3. Radio Interference and Exposure

This equipment has been tested in accordance with the required standards as listed above.
The transmitter equipment may cause interference with other equipment in close proximity due to Radio Frequency Emissions in the frequency range from 150 KHz to 6 GHz. A minimum distance of 0.5 m must be observed from the transmitter to all other equipment, cabling and infrastructure.
The equipment output energy at the antenna emits a high level of low frequency energy. The minimum safe distance of 20 m from the antenna must be observed and demarcated in accordance with the mine procedures for exclusion zone demarcation.

AN EXCLUSION DISTANCE OF 10 METERS FROM THE ANTENNA FOR ANY TYPE OF ELECTRIC DETONATORS MUST BE ADHERED TO.

3 CYBERDET I INTRODUCTION

3.1. CyberDet I Basic Description

The CyberDet I system communicates through the rock strata without the use of any downline (in the hole) or external connecting wires. The CyberDet I system makes use of a very low frequency magnetic spread spectrum communication mechanism, which enables Through-The-Earth (TTE) communication.

The CyberDet I consists of a Blast Control Unit (BCU II), a Transmitter (Tx), Tx Battery, Capacitor box, high voltage cable, an Antenna, a Receiver (Rx) assembly that contains the receiver electronic unit, detonator, booster , Field Strength Meter (FSM) and NFC-enabled Tagger. The surface blast controller (SBC) will communicate from surface to the BCU II underground.

The BCU II will communicate with the Tx using RS-485 and/or proprietary DetNet bi-phase protocol over twisted pair cable. Communication between the Tx and the Rx will be via a spread spectrum magnetic signal. The Rx is equipped with an LED interface to aid in indicating its status before and after tagging. The primary method of interrogating and programming the Rx during assembly and deployment will be via the Tagger using Near Field Communication (NFC).

The BCU II can be controlled locally or from a Surface Blast Controller (SBC) to authorise and initiate a wireless detonator blast.

Magnetic Field Strength meter(s) are used to determine the strength of the magnetic field measured at the blast site and will also indicate the optimum Tx Antenna placement.

The illustration below depicts the CyberDet I system lay-out and individual components.

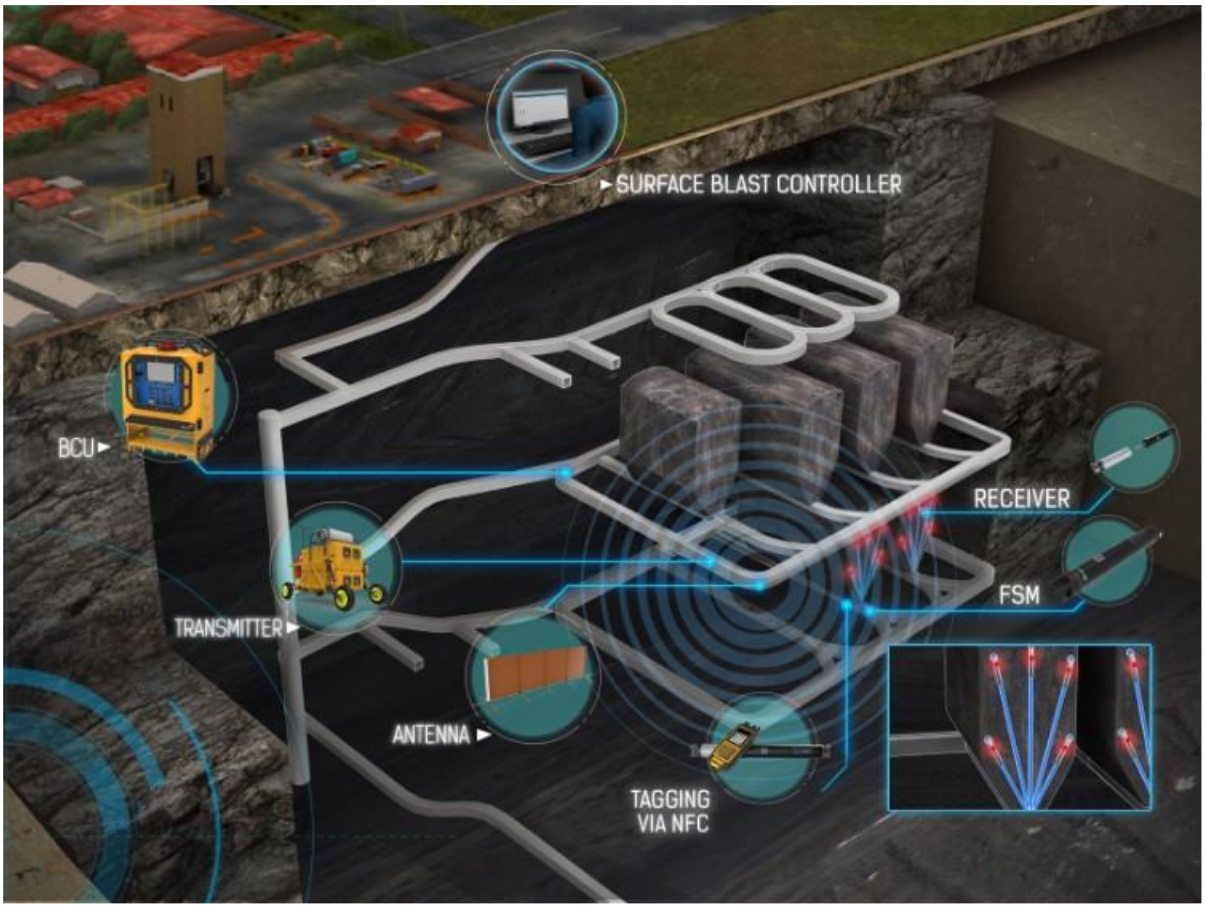


Figure 1: CyberDet I

3.2. Blast Control Unit II (BCU II)

Figure 2: Blast Control Unit II

Figure 3: Portable BCU II

The Blast Control Unit II (BCU II) is designed to meet EU standards and control the blast through commands to the Tx. All CyberDet I Blast commands originate from either the SBC or BCU II while the Tx simply relays the messages via Through-The-Earth (TTE) communications.
The cable from the BCU II to the Tx allows for the low voltage communication to be successful over large distances and is immune to magnetic interference.
The BCU II can override the Tx in an emergency.

3.3. Magnetic Field Strength Meter (FSM)

Figure 4: Magnetic Field Strength Meter

The magnetic field strength meter(s) are used to determine the strength of the magnetic field generated in the blast domain. It will also indicate to the user whether the current Antenna placement position covers the intended blast area or not. (The user may have to adjust the antenna position to a more suitable location where required). The magnetic field strength meters log test data that is used to evaluate signal strength and, apart from visually indicating the signal strength, the data can also be downloaded for analysis. The meter is equipped with LED indicators that will flash when the internal antenna detects signals and is able to lock onto the signal. The LEDs function as a secondary interface, while the tagger functions as the primary method of determining link quality and must be used to download metering data.

NOTE	**It is recommended that a Magnetic Field Strength Meter is active during Rx deployment as it will immediately indicate magnetic signal issues.** **The Magnetic Field Strength Meter can only register test messages and as such transmission of blast commands will be registered as broken or invalid messages by the FSM and will affect the interpretation of field strength survey results. It is therefore recommended to not transmit blast commands while conducting a survey.** **It is recommended that the FSMs and Rx's should not be placed next to large metallic materials as it may weaken the signal. Ideally, they should maintain a 1 m distance.**

CAUTION	**CHECK FIELD STRENGTH METER BATTERIES BEFORE USE TO ENSURE IT IS IN A GOOD USABLE CONDITION. BATTERY REPLACEMENT UNDERGROUD SHOULD NOT BE PERFORMED. STANDARD ALKALINE AA BATTERIES SHOULD LAST AT LEAST 80 HOURS. THE BATTERY VOLTAGE SHOULD BE AT LEAST 1.3V PER CELL OR 2.6V FOR BOTH. BATTERY LEVELS CAN BE CHECKED USING THE TAGGER.**

3.4. Transmitter Antenna

3.4.1. Standard Antenna

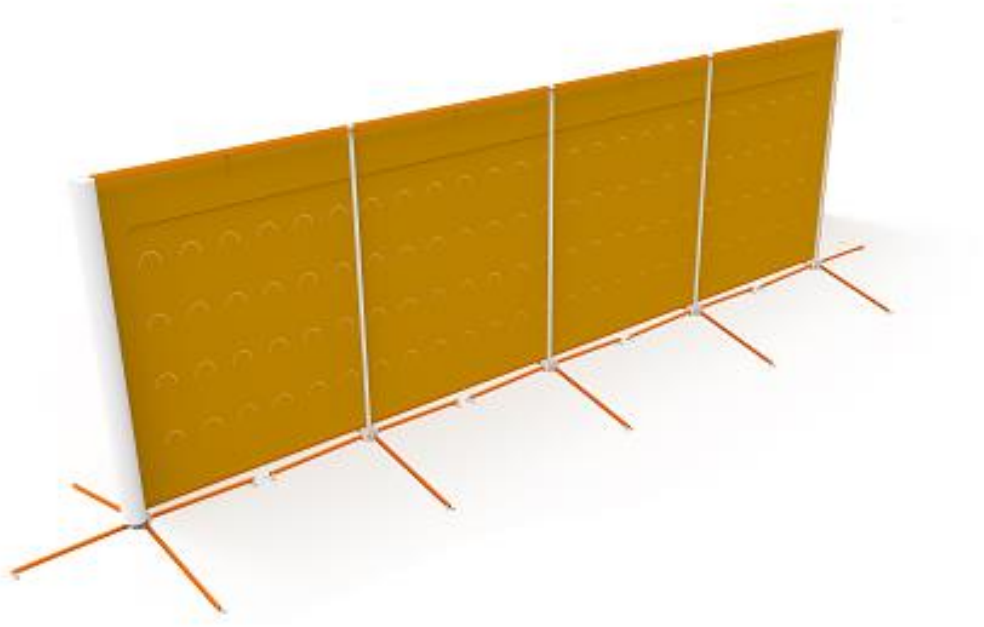


Figure 5: Antenna (2 m X 8 m)

- The Antenna is omni-directional measuring 2 m x 8 m and is easily deployable and man-portable.
- The Antenna is a flexible loop that emits a magnetic field to communicate.
- The maximum connecting cable length between the Transmitter and Antenna is 100 m.
- The maximum antenna range is 300 m.
- When deployed, the antenna must be fully extended and not coiled or folded.
- As the transmitter antenna is omnidirectional it may be deployed in any position such as laid flat or mounted on floor or wall.

IT IS RECOMMENDED THAT USERS KEEP AT LEAST 5M AWAY FROM THE TRANSMITTER ANTENNA WHILE TRANSMITTING TO ENSURE THAT THE USER WILL NOT BE EXPOSED TO ELECTRICAL FIELD STRENGHTS OF HIGHER THAN 5 V/M.

3.4.2. Optional Transmitter Antenna

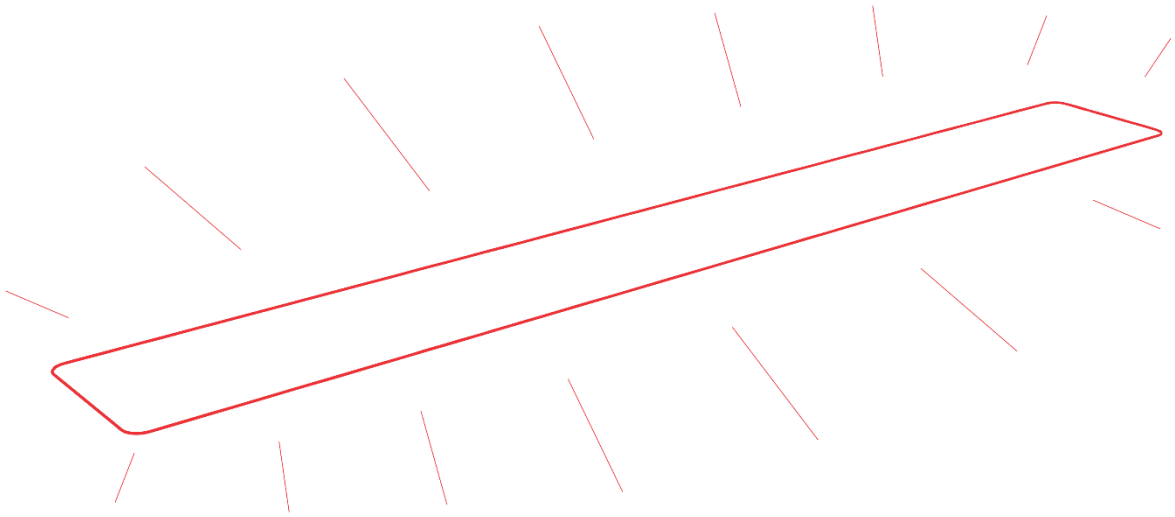


Figure 6: Antenna - Long Range (50 m X 300 m)

- The option Tx Long Range Antenna is omni-directional measuring 50 m x 300 m.
- The Antenna is a flexible loop that emits a magnetic field to communicate.
- The maximum connecting cable length between the Tx and Antenna is 100 m.
- The maximum antenna range is up to 1500 m depending on the terrain it is deployed in.
- When deployed, the antenna must be fully extended and not coiled or folded.
- As the transmitter antenna is omnidirectional it may be deployed in any position such as laid flat or mounted on floor or wall.

3.5. Transmitter

The Tx is controlled from the BCU II via a twisted pair cable connection. This cable may be up to 500 m in length and will allow connection to a fixed installation BCU II and will also ensure that the BCU II, Tx and Antenna are removed away from damage at the blast site.

The Tx is of a modular design and equipped with wheels to facilitate easier transport. Tx components are installed in a shock proof IP68 rated case.

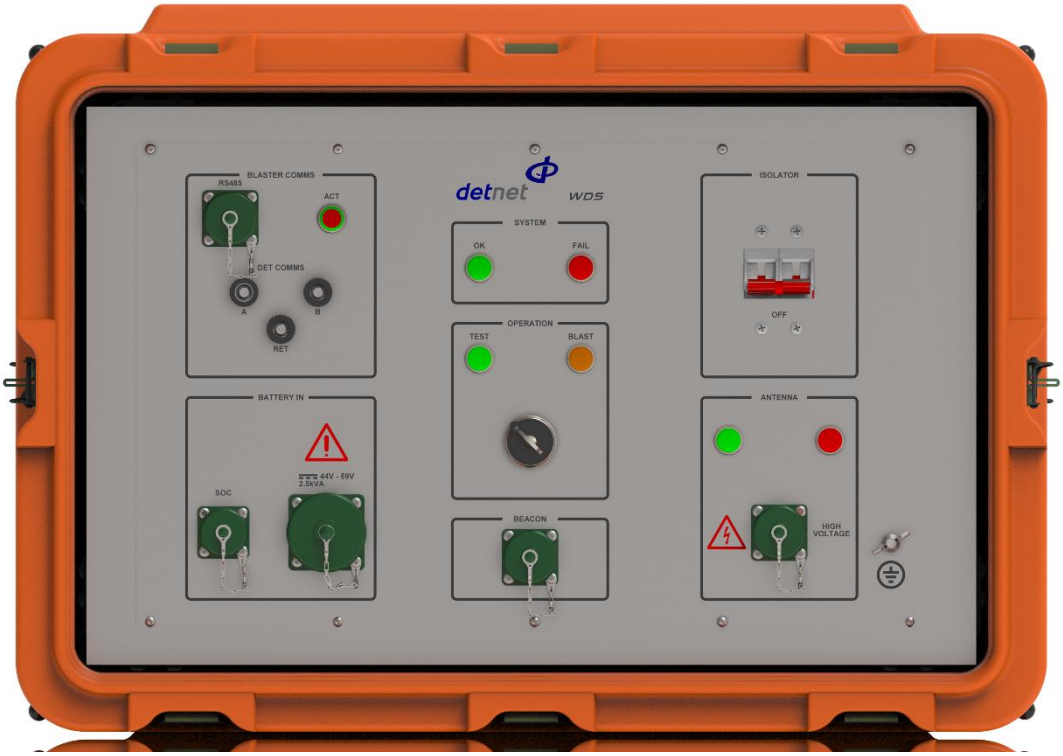


Figure 7: Transmitter

Parameter	Value
Tx – Rx range (max)	300 m
Transmission frequency	3900 to 4100 Hz
Transmission power (max)	2000 W
Operating Voltage	200 VDC. Note: The operating voltage of the cable may increase up to 2000V during operation
Encryption	Centrally generated and used for a single blast
Magnetic field	Dissipates quickly and will be limited to below 5 V/m at 5 m from Antenna
Removable key switch modes	Test – test signal at operating frequency Blast – send encrypted commands
Dimensions	0.95 m x 0.66 m x 0.4 m
Weight	42 kg

Figure 8: Transmitter Battery Pack

Parameter	Value
Lithium battery pack	48 V
	3.5 kWh
Dimensions	0.44 m x 0.42 m x 0.13 m
Weight	65 kg

3.5.1. Transmitter safety

TO AVOID EXPOSURE TO ELECTRICAL SHOCK, AN EARTH STRAP CAN BE ATTACHED TO THE METAL BODY OF THE TRANSMITTER AND CONNECTED TO THE MAINS DISTRIBUTION GRID OR ALTERNATIVELY, CONNECT THE EARTH STRAP TO A CONDUCTIVE EARTH SPIKE SECURED IN THE GROUND.

The cable from the Tx to the Antenna is checked continuously during operation to ensure integrity.

- The cable from the BCU II to the Tx is resistant to magnetic interference.
- The antenna cable is multicore to ensure integrity and connectivity checked.
- All proprietary connections make use of specialized high voltage DC connectors.
- The battery and battery management system are CE certified.
- The transmitter antenna will only emit magnetic fields during the blasting process when in Blast mode and commands are being transmitted.
- The transmitter antenna will emit magnetic fields for 35 seconds every minute while in Test mode.
- In Blast mode the Tx acts as a relaying device to send Wake, Arm and Fire commands originating from the BCU II. After the Wake command, the other commands have time-out periods. The Tx acts as a relaying device and cannot generate its own commands.
- The Tx is equipped with an Emergency Isolation switch to disconnect power from the antenna.
- It is important that the isolator is in the off position during antenna set up and connection.
- The Battery level should be at least 30% to cater for a full test and blast. This should provide at least 2 hours of transmission time. Battery level is indicated on the battery LED array. Each LED represents

approximately 17% battery level therefore at least two LEDs need to have a solid display before transmissions.

- A fully charged battery will allow for at least 8 hours of continuous transmission.
- It is recommended that the battery be fully charged once it drops below 30%.
- Keep the lid on the transmitter closed while transporting to eliminate dust and grit from entering.

3.5.2. Battery charging

Figure 9: Transmitter Battery Pack front panel

- Remove the case lid to expose the battery and battery charger front panel.
- Verify that the orange BATT POS and black BATT NEG cables are connected, with the correct orientation, on the front panel, Figure 9.

Figure 10: Transmitter Battery power socket

- Insert the socket of a 110 - 220 VAC mains power cord into the 220 VAC input socket on the battery charger front panel, Figure 10.

Figure 11: Power outlet 220 VAC.

- Insert the 110 - 220 VAC mains power cord into a 220 VAC power outlet socket. Do not switch the 110 - 220 VAC power outlet on yet, Refer to Figure 11.

Figure 12: Battery power switch

- Switch the POWER switch on the battery front panel to the ON position, (Figure 12) the green ON LED will illuminate.

Figure 13: LEDs on Battery front panel indicating charging

- Press and hold the Red SW Switch on the front panel of the battery for three seconds.
- The green RUN LED and the SOC LED's will be illuminated and switch off.
- Switch on the 110 - 220 VAC power outlet (As per Figure 11 above).
- The green RUN LED with continue to flash every four seconds.
- The battery is now charging.

Figure 14: Charging LEDs.

- Each illuminated state of charge (SOC) LED on the battery front panel represents approximately 17% of the battery capacity and the flashing SOC LED indicates charging progress.

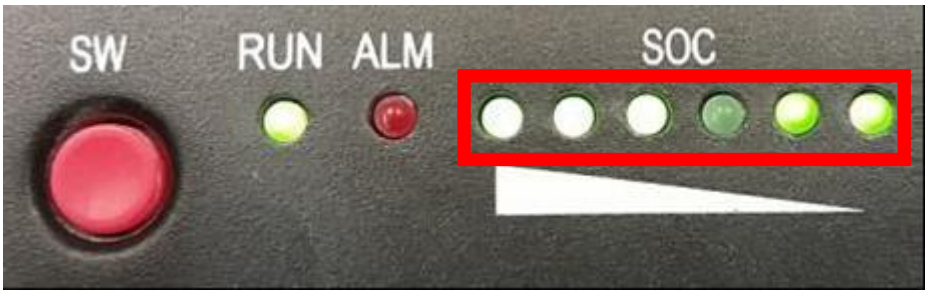


Figure 15: LEDs indicating battery status.

- Once the battery is fully charged, the final SOC LED will stop flashing, and all the SOC LEDs will remain illuminated.
- Switch off the 110 - 220 VAC power outlet (Figure 10) and the POWER switch (Figure 11) on the battery front panel.
- Disconnect the charging cable.

3.6. Receiver

The electronic Rx module consisting of a 3D antenna, electronic module and batteries will be shipped pre-assembled from manufacturing.

Figure 16: Receiver

Parameter	Value
Rx enclosure diameter	50 mm
Rx weight	490 g
Rx length	500 mm
Battery operating power	3 V (24 V high voltage only at firing).
Battery Quantity and Type	2 X AA Alkaline Batteries
In-hole sleep time	30 days after activation.
Rx	Omnidirectional. Not orientation specific
Detonator	4G
IP rating	67
Rx to Tagger communication	Bi-directionally via NFC
Rx state	• Default – sleep • Test/Blast – powered up, awaiting commands
Endcaps	Custom endcaps to connect a tether for removal of units if required, or deployment in down-holes.
Spider assembly	Optional – clip on to endcaps to lock the receiver in position during up-hole applications

3.6.1. Receiver safety

- The Rx is battery powered (low voltage, only high voltage in the device at firing) and will remain switched off (not powered) until deployment.
- The batteries are verified during self-diagnostic and when Tagging and Rx interrogation via NFC is performed.
- The commands received are encrypted, the encryption keys are centrally generated per site and never

overlap and are unique for every blast on the specific mining site. Previous keys are archived in a central database to ensure that subsequent keys do not overlap. Keys are transferred via the Tagger's NFC interface.

- After the Wake command, other commands will have time-out periods causing the receiver to revert to a sleep cycle.
- A Power/ blast key is required to initiate a blast (32bit hardwired, only stored on receiver).
- The Rx diagnostic data downloaded before programming is allowed using the Tagger.
- Rx's that have had functional communications with the Tx, detonator and sufficient battery level will be allowed to be tagged.
- The NFC tagging procedure transfers the desired detonator delay as well as the decryption key to the Rx.
- The Rx has an auto-terminate function which is activated immediately after the FIRE command is sent to the attached detonator– the receiver is then physically disabled.
- It is not recommended that Users change the batteries due to electronics and dust ingression. Batteries will only start discharging once a detonator is connected to the Rx and via NFC for the FSM.
- It is recommended that the FSMs and Rx's should not be placed next to large metallic materials as it may weaken the signal. Ideally, they should maintain a 1 m distance.

3.6.2. Setup Blast Receiver

For Use with Explosives	
1. Clip detonator into receiver	
	

2. Attach booster onto receiver and twist to lock into position	
	

3. Blast Rx: When switched “ON” the green LED will flash 3 times at 1 Hz. Once the receiver has received test messages from the transmitter the green LED will switch on for 10 seconds. Due to the Tx test signal duty cycle, this process can take up to 90 seconds to complete. **Note** that the Blast Rx is required to have received at least one test message before Tagging will be allowed. The Rx is therefore required to be within range of a Tx sending test messages after the Rx has been assembled (detonator plugged into the Rx). A No Sig Error indicates that the above process was not successfully executed.	
4. The Tagger is used to check the Rx diagnostics and tag the Rx det assembly. Any Rx diagnostic failures detected while interrogated by the Tagger will result in the red LED flashing continuously at 1 Hz. The tagger will not allow tagging of Rx units when diagnostic errors are detected. The Tagger will indicate what failed during NFC interrogation. The error message will indicate whether the Rx unit needs to be replaced or the detonator before re-attempting tagging.	

3.6.3. Setup Field Strength Meter

1. The FSM logs are first cleared, and the unit activated using the Tagger through NFC. Once activated the FSM is in a fully powered state ready to log incoming test messages.	
2. The Field Strength Meter (FSM), when activated, will flash its green LED 3 times at 2 Hz. Subsequently it will flash its RED LED every 5 seconds indicating that the FSM is still searching for a signal and has not locked onto any transmission. A spider may be attached to enable in hole deployment of the FSM. A rapidly flashing RED LED indicates that the batteries must be replaced.	

4 CYBERDET I TAGGER

The function of the CyberDet I Tagger is to:

- Tag and test CyberDet I Rx's.
- Connect to Field Strength Meters to determine the strength of the magnetic field measured at the blast site
- Connect wirelessly to the Control Equipment e.g. connecting to BCU II to transfer the CEK when conducting local blast.

4.1. CE4 Tagger System Information

This function enables the user to view battery charge information, current consumption, state-of-health of the battery, temperature information, hardware and software serial numbers, GPS detail and User ID.

System Info

From the Main Menu, press SoftKey to view the CE4 Tagger System Information

Regulatory Info

Regulatory information will be displayed.

System Info - Battery

93%: Battery charge information Charging will be indicated by **(USB)** when a USB charger is used or **(AUX)** when a wireless charger is used. Should the charger not be able to supply enough power to charge the CE4 Tagger, 'Weak Charger' will be indicated as the charging status, instead of 'Charging (USB)'.

Current Consumption: By convention, a negative value indicates that current is being drawn from the battery.

Cell Status: (Good) indicates the state of health of the battery. Should the status indicate 'Low' the unit should be serviced to have the battery replaced.

NOTE	**The CE4 Tagger will switch OFF automatically when the battery capacity drops below 3%. (The CE4 Tagger will display a warning at 9% and switch OFF at 3%).**

System Info - Temperature and the Relative Humidity
The Temperature and the Relative Humidity as measured inside the CE4 Tagger are displayed as follows:

Temperature: The Temperature is displayed in degrees Celsius or Fahrenheit (Dependant on Units Setting under Device Setup).

Humidity: The Relative Humidity is displayed as a percentage.
Press ➡ to select next page.

System Info - Hardware Serial Number and SW Release Number
Hardware Serial Number will be displayed, and
Software Release Number will be displayed.
Service will display the required date for servicing. Should the date be exceeded, an Error message will be displayed stating “Device service due”.
Press ➡ to select next page.

Hardware Serial number is required when Challenge Response tickets are required from the DetNet Portal.

System Info - GPS Detail
The GPS location will be displayed.
Altitude and the number of satellites found will also be displayed.
Press ➡ to select next page.

System Info –User ID
Press SoftKey to enter or edit User ID.
Use alphanumeric characters to enter a User ID.
Press ➡ to select next page.

System Info – QI Charging
The QI charging status will be displayed.

The User ID may be used to identify ownership of the CE4 Tagger such as the User name or Site name/code where used. Clearing the USER ID will result in NO USER to be displayed after saving/enter is pressed.

4.2. CE4 Tagger Configuration Settings

Configuration Settings consist of the following menus:
1. Device Setup
2. Advanced Setup
3. Factory Setup

4.2.1. Device Setup

This menu will allow the user to adjust device specific settings. The following options are available:
1. Contrast
2. Brightness
3. Time Zone
4. Time Outs
5. Language
6. Units

4.2.1.1. Contrast

This function enables the user to adjust the LCD screen contrast.

NOTE	**The contrast adjusts as the value changes but the setting will only be saved permanently when the SoftKey is pressed.**

1. Main Menu

Press SoftKey to select Configuration Settings.

2. Configuration Settings Menu

Press 1 to select **Device Setup**.

3. Device Setup

Press 1 to select **Contrast**.

4. Contrast

Use the arrow key 4 6 to adjust contrast.

Adjust to ensure the displayed contrast 'blocks' are distinguishable to allow viewing 'greyed out' versus 'bold' items. If the contrast is either too high or too low, these font differences will not be notable.

Press SoftKey to save.

Press SoftKey to return to Main Menu.

4.2.1.2. Brightness

The Brightness menu allows the LCD screen display brightness to be adjusted using the 4 6 arrow keys.

The Brightness adjusts as the value changes but the setting will only be saved permanently when the SoftKey is pressed.

1. Main Menu

Press SoftKey to select Configuration Settings.

2. Configuration Settings Menu

Press 1 to select **Device Setup**.

3. Device Setup

Press 2 to select **Brightness**.

4. Adjusting the Brightness

Use the arrow 4 6 keys to adjust brightness.

Press SoftKey to save.

Press SoftKey to return to Main Menu.

4.2.1.3. Time Zone

This function enables the user to define the time zone. Date/time settings are controlled by GPS GMT data but, since the time **zone** is not configured automatically, it should always be set by the user to ensure the correct time display. The time zones may be adjusted in 0.5-hour increments.

1. Main Menu

Press SoftKey to select Configuration Settings.

2. Configuration Settings Menu

Press 1 to select **Device Setup**.

3. Device Setup

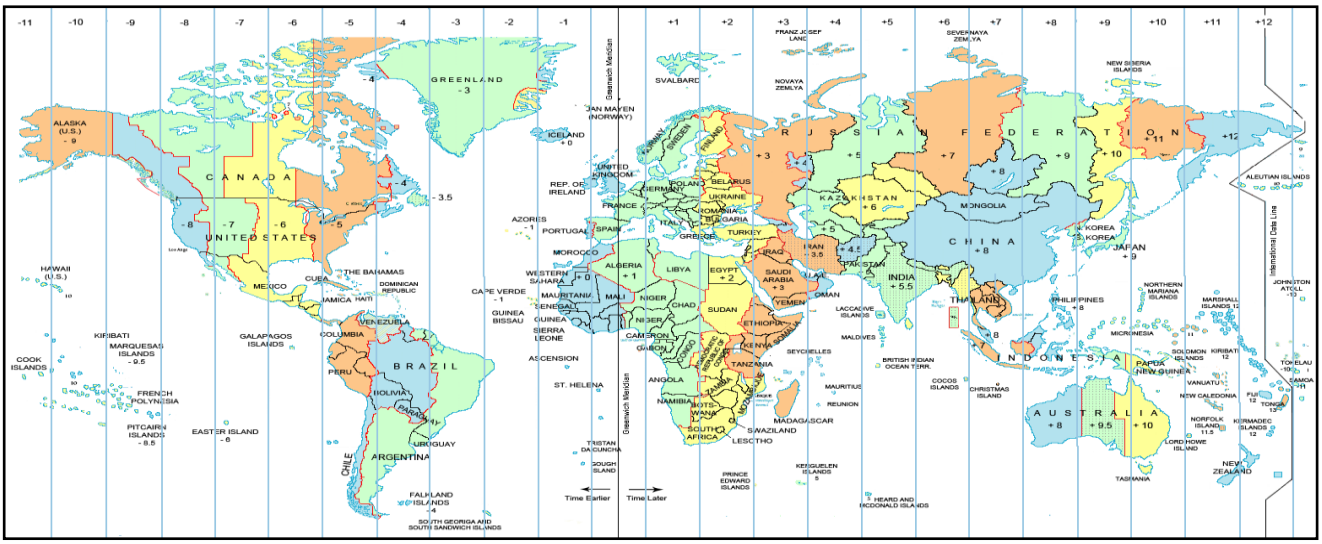
Press 3 to select **Time Zone**.

4. Set Time Zone

Use the arrow key 2 8 to navigate the Time Zone options (Time zone can be adjusted in 0.5-hour increments).

Press SoftKey to save.

Press SoftKey to return to Main Menu.



4.2.1.4. Timeouts

This function enables the user to set the auto power off function of the Tagger if inactivity for a set period of time. The function is available to conserve battery power. The user can set the idle time between 2 to 360 minutes.

1. Main Menu

Press SoftKey to select Configuration Settings.

2. Configuration Settings Menu

Press 1 to select **Device Setup**.

3. Device Setup

Press 4 to select **Timeouts.**

4. Auto Shutdown

Use 2 8 navigational keys to navigate selection.

- Minimum of 2 minutes.
- Maximum of 360 minutes.

Press SoftKey to save.

Press SoftKey to return to Main Menu.

4.2.1.5. Language

This function enables the user to select a language preference for the CE4 Tagger menus.

1. Main Menu

Press SoftKey to select Configuration Settings.

2. Configuration Settings Menu

Press 1 to select **Device Setup**.

3. Device Setup

Press 5 to select **Language.**

4. Language

Press 1 on the keypad to select English.
Press 2 on the keypad to select Español.
Press 3 on the keypad to select Français.
Press SoftKey to return to Main Menu.

4.2.1.6. Units

This function enables the user to select either the Imperial or Metric Units of Measure as preferred.

1. Main Menu

Press SoftKey to select Configuration Settings.

2. Configuration Settings Menu

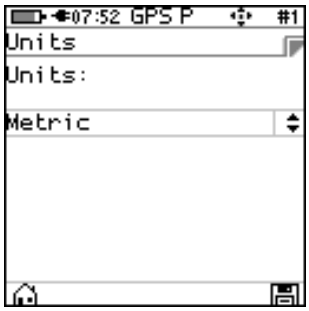
Press 1 to select **Device Setup**.

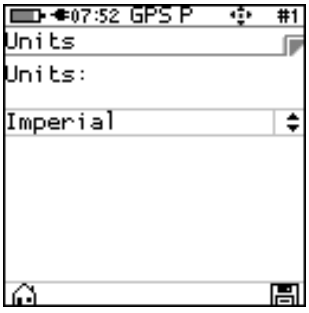
3. Device Setup

Press 6 to select **Units.**

4. Units

Use 2 8 navigational keys to toggle selection.
Press to select either Imperial or Metric.
Press SoftKey to save.





4.2.2. CE4 Tagger Advanced Setup

The Advanced Setup Menu displays the following options:

1. Tagger ID
2. Connections
3. Remote View
4. Device Password

4.2.2.1. Tagger ID

This function enables the user to set a unique Tagger ID that is used for device identification. The Tagger ID should be unique amongst all Taggers at a site. Tagger IDs range from 1 to 10 are supported.

NOTE	**The current CE4 Tagger ID is displayed on the right side of the top bar on the screen (#1 in the screen depicted below).**

CAUTION	**WHEN USING MULTIPLE TAGGERS ON THE SAME BLAST, ENSURE THAT TAGGER IDS ARE UNIQUE AS TAGGERS USING THE SAME ID WILL CAUSE ERRORS ON THE BLAST.**

1. Main Menu

Press SoftKey to select Configuration Settings.

2. Configuration Settings Menu

Press 2 to select Advanced Setup.

3. Advanced Setup

Press 1 to select **Tagger ID**.

4. Tagger ID

Use numerical keypad to enter Unique Tagger ID between 1 and 10.

Press SoftKey to **save**.

Press SoftKey to return to Main Menu.

4.2.2.2. Connections

This function enables the user to activate the Wi-Fi and/or USB module allowing the Tagger to communicate with other equipment.

NOTE	**Additional software for a PC may be required from the manufacturer to support this feature. USB cable or Wi-Fi must be connected, and the PC software must be configured and activated before this function can be used.**

1. Main Menu

Press SoftKey to select **Configuration Settings.**

2. Configuration Settings Menu

Press 2 to select **Advanced Setup**.

3. Advanced Setup Menu

Press 2 to select **Connections**.

4. Connections

Press 1 on the keypad to connect Tagger to **PC via Wi-Fi**.

Press 2 on the keypad to connect Tagger to **Ranger/Commander via Wi-Fi**

Press 3 on the keypad to connect Tagger to **PC via USB**

NOTE

During initial connection with a PC, the device will be displayed on the PC Wi-Fi List and will require a Password to connect. Use Generic Password: 145634235. Subsequent connections will connect automatically.

Connect Tagger to PC via Wi-Fi

NOTE

To establish Wi-Fi connectivity between the CE4 Tagger and a PC, the PC must be equipped with the required Wi-Fi functionality and corresponding software.

5. PC via Wi-Fi

CE4 Tagger will search for access point on PC.

CE4 Tagger will connect to the PC.

Follow on-screen prompts to connect to CE4 Tagger Access point Wi-Fi.

Connect CE4 Tagger to Commander via Wi-Fi

6. Ranger via Wi-Fi

Enter the Ranger's ID using the keypad to connect.

Press ↵ to continue.

Enter Commander's ID will also be displayed if Ranger is not found while attempting to connect.

NOTE	**Only one Commander with selected ID must be active when connected.** **When connectivity is established between the CE4 Tagger and the Commander an audible "Bling" and subsequent "Tock" sound should be heard for every button press.**

CE4 Tagger will connect to the selected Commander.

NOTE	**Shortcut key combination is available from the Tagger main menu to connect the CE4 Tagger to Commander via Wi-Fi menu as follows:** **Press and hold FN key and then press the ↵ key to connect.** **Press and hold FN key and then press the ESC key to disconnect.**

7. USB Link with PC

The CE4 Tagger will wait for the connection to be established, and the following messages will appear:

- Ready for PC – Connect USB cable between PC and CE4 Tagger
- Connected to PC

4.2.2.3. Remote View

This function enables the user to demonstrate the CE4 Tagger in action by replicating the screen on a PC. It may be used by trainers, product presenters and document writers.

NOTE	**Additional PC software may be required from the manufacturer to support this feature. USB cable or Wi-Fi must be connected, and the PC software must be configured and activated before the Remote View function can be used.**

Select Remote View on CE4 Tagger

1. Main Menu

Press ⚙ SoftKey to select **Configuration Settings.**

2. Configuration Settings Menu

Press 2 to select **Advanced Setup**.

3. Advanced Setup Menu

Press 3 to select **Remote View**.

4. Screen Capture

Press 1 to Enable on USB when prompted.

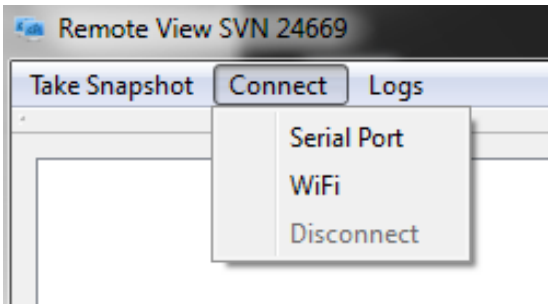
CE4 Tagger actions will be replicated on the PC screen.

5. Press 1 to disable remote view.

Initiate Remote View on PC

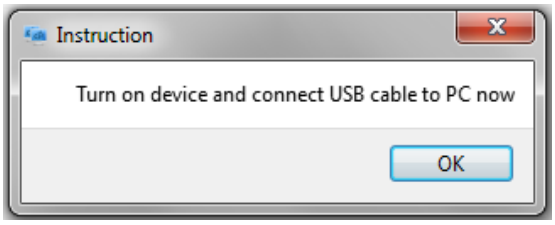
1. Open the Remote View software application on the PC.

2. Click on **Connect** tab.
3. Select either **Serial Port** or **Wi-Fi** as required from option – note that when Wi-Fi is used then the PC should be connected to the Tagger via Wi-Fi.

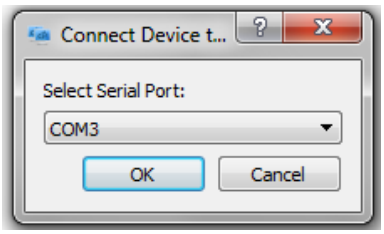


4. Ensure CE4 Tagger is switched ON.

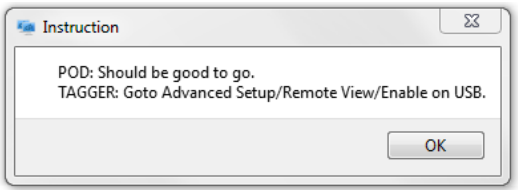
Connect USB cable between CE4 Tagger and PC
Click OK to continue



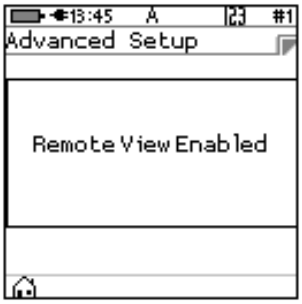
Connect Device when connecting via USB.
Select Serial (COM) Port from dropdown list.
Click OK to continue.



5. Navigate to Advanced Setup/ Remote View on CE4 Tagger
6. Press 3 DEF to select **Remote View.**



7. Press 1 to enable Remote View on **PC via USB**
8. Remote View will be displayed on PC.



4.2.2.4. Device Password

The CE4 Tagger is protected from unauthorised use by assigning a password.
This function enables the user to change the default password by assigning a new unique password that is known only to the user.

1. Main Menu

Press SoftKey to select **Configuration Settings.**

2. Configuration Settings Menu

Press 2 to select **Advanced Setup**.

3. Advanced Setup Menu

Press 4 to select **Device Password.**

4. Passwords

Use the numerical keypad to enter **Current Password.**

Press ↵ to confirm.

Use the numerical keypad to enter **New Password.**

Leave blank and press ↵ for NO password requirement during start-up of the Tagger.

Press ↵ to confirm.

Information message confirming password changed will be displayed briefly.

Press ESC to return to Advanced Menu.

Press SoftKey to return to Main Menu.

The Password should be changed regularly to maintain security.

Unlike conventional password entry, the chosen password is visible to the user (rather than **) to enable the user to see if any typing errors are being made.**

4.3. Tagger Main Menu

The Tagger main menu comprises of the following:

1. Tag Rx
2. Test Rx
3. Surveys
4. Change Design
5. View Design
6. Connectivity

4.3.1. Tag Receiver

This function allows the user to tag the receivers from the downloaded plan detonator list.

1. Main Menu

Press 1 SoftKey to select **Tag Receiver.**

Enter pin code, 0, and press ENTER.

Press to filter the list and display the receiver label entered.

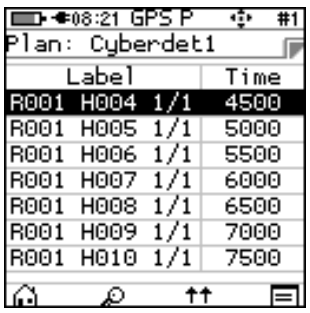
Press to sort the list according to TagPath forward, TagPath reversed, Ascending order or descending order.

Press to display the advanced WDS menu.

Select 1 to add a receiver.

Select 2 to untag the receiver.

Select 3 to receive alternate info on the receiver.



Select receiver to tag from the plan list and press enter. Place Tagger on receiver NFC and Enter to tag. Tagger should display Tagging Passed.

4.3.2. Test Receiver

This function allows the user to test receivers.

1. Main Menu

Press 2 SoftKey to select **Test Receiver.**
Place Tagger on Rx NFC and press Enter to test.
Tagger should display test results.

4.3.3. Surveys

Field strength meters are used to determine the establishment good signal for data transfer. The field strength meters are interacted with using these menus. The menu allows the user to:

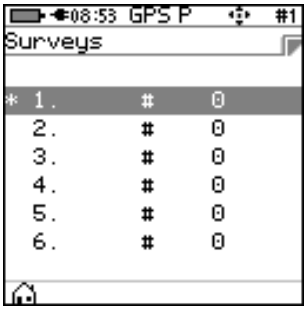
- View FSM data.
- Activate FSM.
- Download results.
- Rename survey.
- Clear survey name.
- Clear survey.

1. Main Menu

Press 3 SoftKey to select **Surveys.**
Select Survey from the list and press Enter.

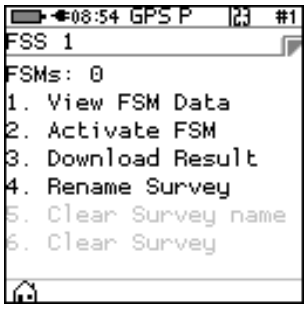
2. Surveys

Select 1 to View FSM Data.



3. FSS 1

Select 2 to Activate FSM.
Place Tagger on FSM NFC and press Enter prior to selecting.



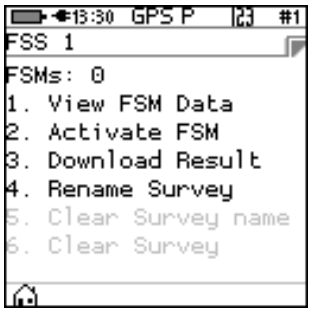
4. Download Results

Select 3 to Download Result.
Select next soft key

5. FSS1

Select 4 GHI to Rename Survey.

Enter new plan name and press Enter to save.



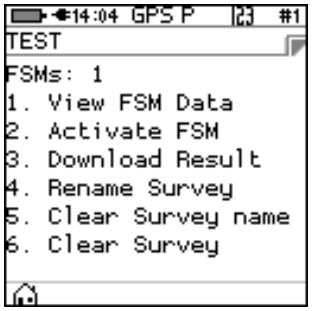
6. Rename Plan

Rename the plan.

7. Test

Select 6 MNO to Clear Survey.

Select Yes to clear survey.

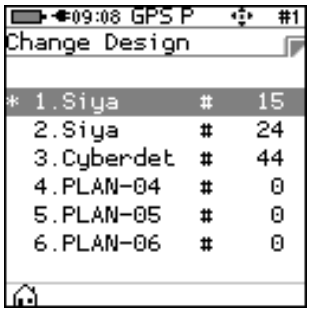


4.3.4. Change Design

This menu allows the user to select a plan for uploading of the design plan from the planning tool. Ten plans are available for selection. The selected plan with be displayed with an Asterix.

1. Main Menu
Press 4 SoftKey to select **Change Design.**
Move up or down to highlight the plan to be selected and press ENTER.

2. Change Design
Press 1 to select the plan.



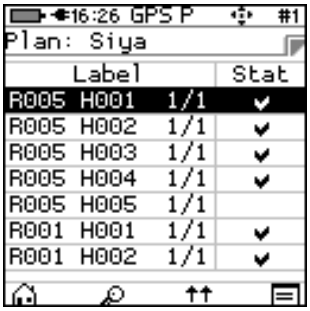
4.3.5. View Design

This menu enables the user to view the list of detonators uploaded to the Tagger from the Planning Tool. The user may also view the list of detonators tagged and the design summary. Select the following menus:

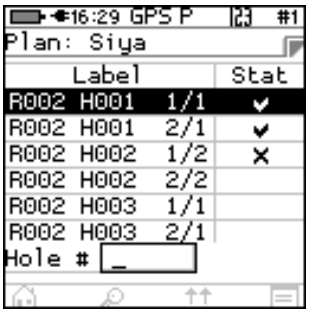
1. Main Menu
Press 5 SoftKey to select **View Design.**

2. View Design Menu
Press 1 to select **View Plan.**

A ✔ symbol displays tagged receivers.
A ✖ symbol displays a deleted receiver.
A symbol displays an untagged receiver.



Press to filter the list and display the receiver label entered.



Press to sort the list according to TagPath forward, TagPath reversed, Ascending order or descending order.

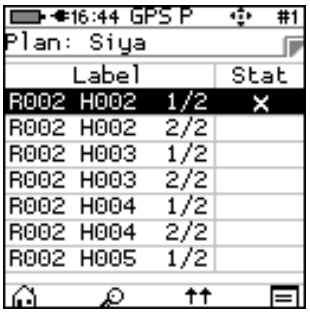
Press to display the advanced WDS menu.
Select to add a receiver.
Select to untag the receiver.
Select to receive alternate info on the receiver.

Press ENTER to display the detonator details.
Press to change the detonator delay.

Press to delete or restore the detonator.

3. View Design Menu

Press 2 to select **List Tagged**.
Screen will display receiver labels that have been tagged.
A symbol displays tagged receivers.
Press ENTER on the highlighted receiver and an advanced screen will be displayed.



4. View Design Menu

Press 3 to select **Design Summary.**
Design Summary screen will display.
Total number of receivers in plan.
Total number of receivers tagged.
The remaining receivers that must be tagged.
Number of new receivers added to the plan.
Number of receivers deleted from plan.

4.3.6. Connectivity

This function enables the user to transfer the survey, plan or key to the BCU II. Connection to the BCU II via Wi-Fi or USB must be setup prior to the transfer. Select the following to establish Wi-Fi or USB connectivity:

1. Main Menu
Press 6 SoftKey to select **Connectivity.**

2. Connectivity Menu
Press 1 to select **Activate Wi-Fi.**
Press 2 to select **Activate USB**.

Once connection is established, the user may send survey, plan or key to BCU II. Follow the steps:

3. Connectivity Menu
Press 3 SoftKey to select **Send Survey to BCU II.**
Tagger will connect to BCU II and send survey.
Tagger will confirm that BCU II transfer completed.

4. Connectivity Menu

Press 4 SoftKey to select **Send Plan to BCU II.**
Tagger will connect to BCU II and send plan.
Tagger will confirm that BCU II transfer completed.

5. Connectivity Menu

Press 5 SoftKey to select **Send Key to BCU II.**
Tagger will connect to BCU II and send survey.
Tagger will confirm that BCU II transfer completed.

5 DEPLOYMENT

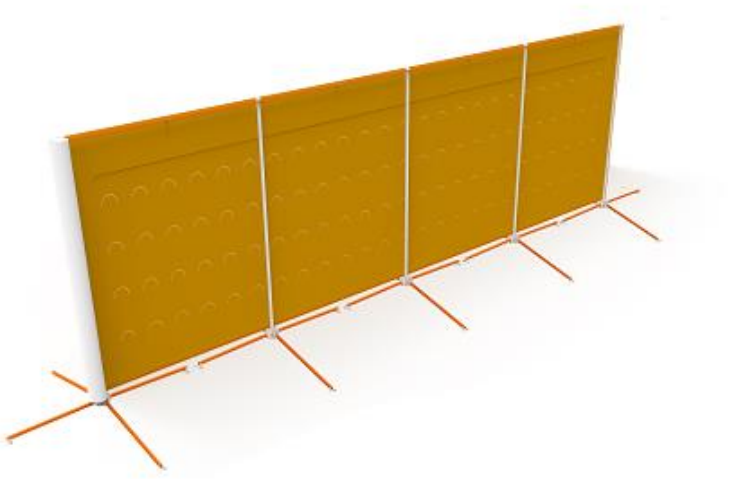
5.1. Pre-deployment – Site survey and Magnetic field testing

CAUTION	THE CYBERDET I USES MAGNETIC COMMUNICATION AT A FREQUENCY OF APPROXIMATELY 4000 HZ. THE HIGH POWER EQUIPMENT AS USED UNDERGROUND BY THE MINE COULD CAUSE ELECTRICAL INTERFERENCE THAT COULD AFFECT THE MAGNETIC SIGNAL. IT IS ALSO POSSIBLE FOR SOME ORE BODIES CONTAINING HIGH LEVELS OF IRON AND CHROMIUM TO REDUCE THE SIGNAL. IT IS THEREFORE A PREREQUISITE TO PERFORM A SITE SURVEY BEFORE THE SYSTEM IS DEPLOYED. IT IS IMPORTANT THAT THE FSMS ARE ABLE TO RECEIVE AT LEAST 30 MINUTES OF TRANSMISSION TIME WITH LESS THAN 2% OF MESSAGES BEING MISSED - VERIFIED BY DOWNLOADING TEST DATA WITH THE TAGGER. THIS WILL ALSO ASSIST IN OPTIMUM DEPLOYMENT OF THE ANTENNA TO ENSURE THE BEST SIGNAL POSSIBLE UNDER THE CONDITIONS UNDERGROUND

The Tx has a **TEST** mode which transmits a carrier signal that can be utilized for site surveying. The Magnetic Field Strength Meter can also be used to test for signal strength. The device is contained in a similar shell as the actual Wireless Rx units. It is transportable and can be deployed in and out of holes. The meter has on-board signal strength logging capability and can be interrogated via NFC by the CE4 Tagger.

CAUTION	THE PLACEMENT OF THE ANTENNA IS CRITICAL AS IT SHOULD BE DEPLOYED IN THE EXACT POSITION FOR BLASTING AS WAS USED FOR THE SURVEY.

The Tx Antenna emits a magnetic field. Current legislation recommends a safe operating exclusion zone for electrical field radiation greater than 5 V/m. The Tx antenna radiation (converted to electrical field strength) is less than 5 V/m at a distance of 5 meters from the antenna.
The Tx is switched to TEST mode using the key switch and the key removed.



When the magnetic field strength meter is deployed, field strength data is logged. Should the downloaded data indicate that the signal strength was not reliable the procedure, such as moving the transmitting antenna closer to the blast site, will need to be repeated until satisfactory results are obtained. The signal strength is deemed unreliable if less than 70 messages were received or more than 1 in 3000 bits were in error during 30 minutes of transmission.
The meter is equipped with LED indication that will flash when the internal antenna detects signals and is able to lock onto the signal. The green LED will flash immediately indicating the test pattern was received without errors.
This LED signal will be a crude initial indication of good Tx-antenna placement. Final verification must be performed using a Tagger.
Upon retrieval of the testers deployed in-hole, the testers are interrogated by the Tagger to indicate the level of signal when deployed and will also indicate if changing the position of the Tx antenna is required.
The Tx TEST mode can then be de-activated by switching the Tx off.

5.2. Deploy Transmitter and Antenna

1. Perform the following steps to ensure the CyberDet I operates within the system limits:
   - The location of the blast area must be identified on the mine plan (level, section, tunnel etc.)
   - A 300 m radius from the blast area is to be marked on the plan.
   - An area to be identified within the 300 m radius for the location of the antenna unit.

NOTE	**The 300 m radius for the location of the Antenna unit can include levels above and below the blast area.**

   - The Antenna should be set up in an area away from personnel and equipment and must conform to a 5m exclusion zone when in operation.
   - The Antenna needs to be fully extended and laid out flat or hung from the stands. It is important that the antenna is as flat as possible (i.e., in one plane) and care should be taken to keep the antenna out of standing water.

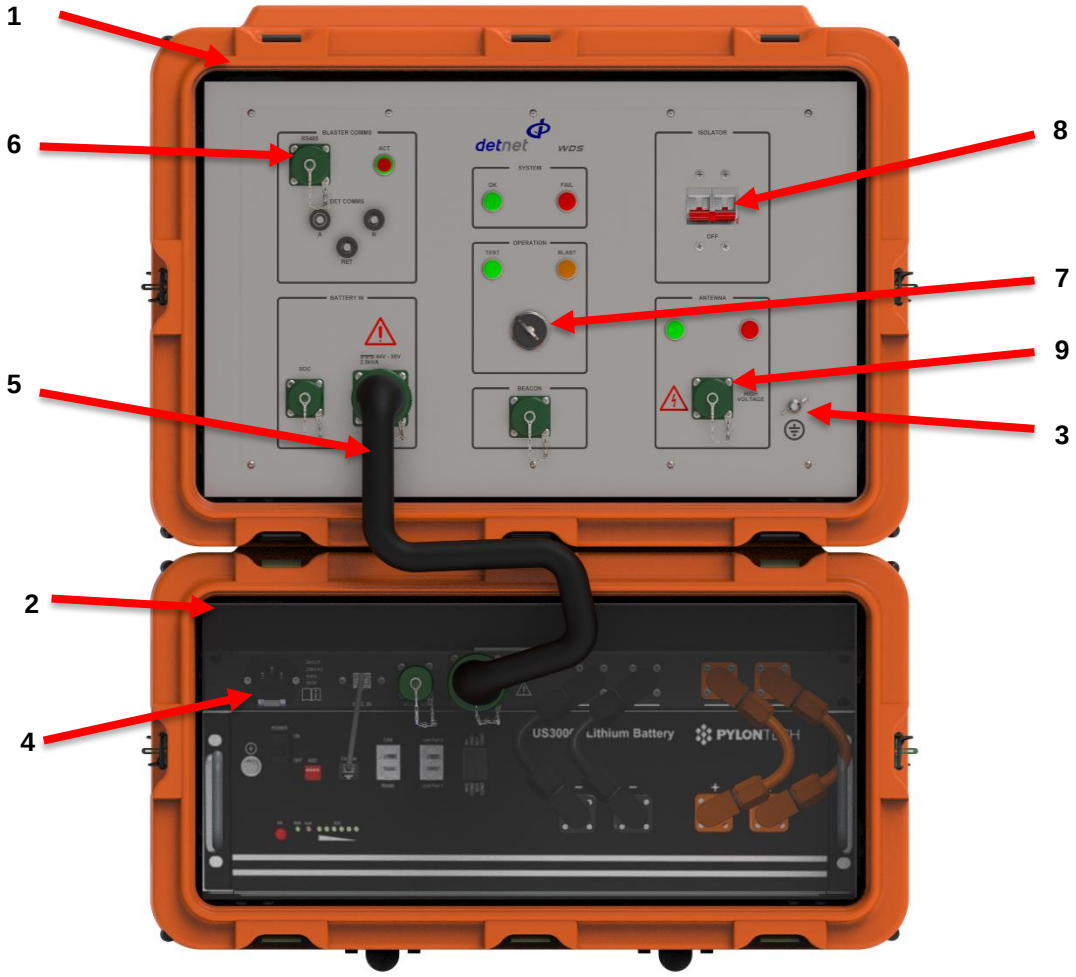


Figure 17 : Transmitter Assembly

   - The Tx (1) must be placed directly above the battery (2) as depicted in .
   - Figure 17 above.
   - Ensure that the Tx and Battery are in a visible location to all personnel and heavy equipment vehicles working in the same area.

- Where possible barricades and warning beacons can be used to safeguard equipment that is to be set up where there is high traffic of personnel or vehicles (or as per mine operational requirement, safety and risk analysis).
- Plug the antenna extension lead into the connector (3) on the transmitter marked “Tx Antenna” as detailed in .
- Figure 17 above.

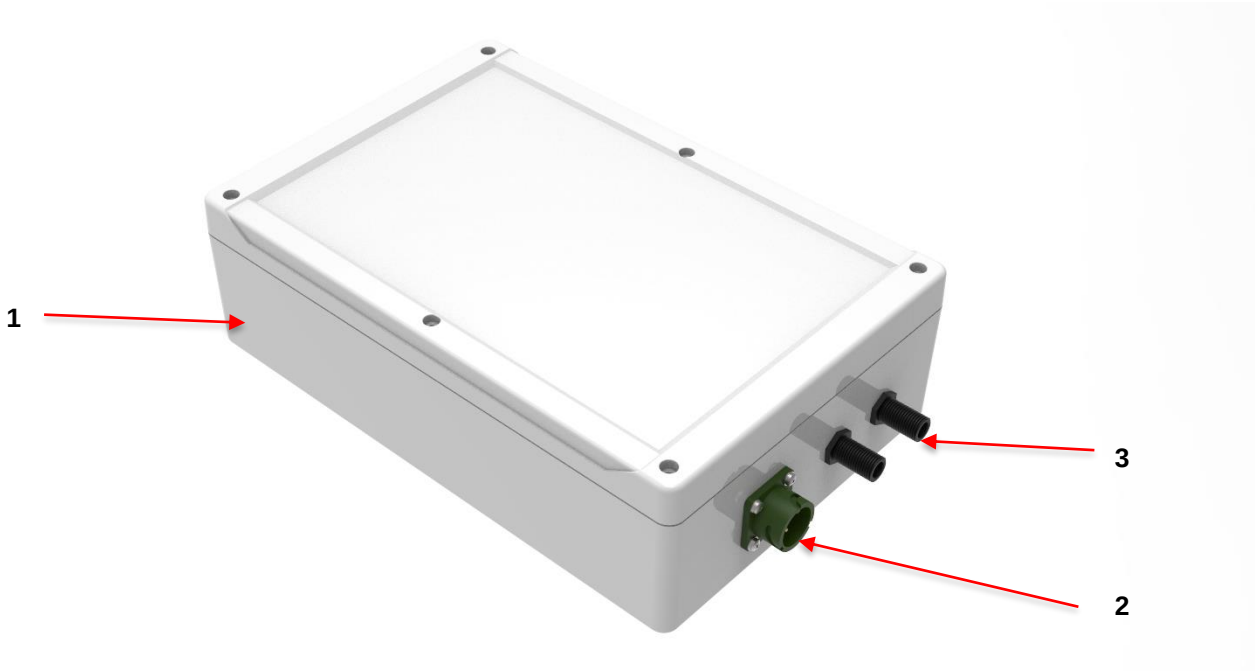


Figure 18: Capacitor Box

- Connect the other end of the antenna extension lead into the capacitor box (1) detailed in Figure 18 using the bayonet coupling (2). A positive ‘click’ on the bayonet coupling confirms connection.
- Connect the high voltage connections on the antenna to the capacitor box (1) by screwing the threaded shells onto the connectors (3) to secure the antenna connections as per Figure 18 above.

NOTE	**The high voltage connections on the antenna are not polarity specific. (The two connections are identical).**

- Ensure the battery switch (4) is in the “OFF” position then connect the Tx to the Battery using the interconnect cable (5) detailed in .
- Figure 17 above. The interconnect cable is fitted with dust caps that will need to be removed. The cable will only fit one way due to the gender of the connectors and connector keying used. The bayonet coupling on the power cable requires positive torque to be mated. A ‘click’ confirms successful coupling.
- Connect the BCU II cable to the plug marked ‘Blaster Comms’ (6) on the transmitter detailed in .
- Figure 17 above.

WARNING	**THE GROUNDING OF THE TX IS CRITICAL TO PROTECT THE USERS AND EQUIPMENT FROM THE DANGERS OF HIGH VOLTAGE. IF THE CONDUCTIVE SURFACE IS NOT GROUNDED AND BECOMES ELECTRICALLY ENERGIZED, IT CAN CARRY A VOLTAGE SUFFICIENT TO ADMINISTER A FATAL SHOCK.**

2. A copper conductor connects the rod to the GND terminal (9) on the Tx. Ground the Tx by connecting the ground/ earth wire to the ground terminal (9) using a wing nut to fasten detailed in .
3. Figure 17 above.

4. At the time of blasting:
   - Deploy antenna in the exact position and orientation (or as near as possible) as determined during the site survey.
   - Tx placement is not critical. The Tx to antenna cable allows for 100 m maximum and 20 m minimum.
   - Connect Tx to BCU II via RS485, 300 – 500 m (6) detailed in .
   - Figure 17 above.
5. Before the actual blasting procedure commences and to confirm placement of the antenna:
   - Ensure that the battery level is adequate (above 30%) for the planned blast.
   - Turn the operation key (7) to TEST mode on the Tx detailed in .
   - Figure 17 above.
   - Ensure that the Tx isolation switch (8) is in the ON position and battery is switched on (4) detailed in .
   - Figure 17 above.
   - Redeploy the Magnetic Field Strength meter out-hole to visually indicate the strength of the magnetic signal. The testers should remain deployed during Receiver activation and deployment.

5.3. Blast code generation and transferral.

- Blast codes need to be generated prior to tagging the Rx's with the required blast code.
- The Planning tool is used to generate and store all blast codes. Refer to UTM-00368.

5.4. Transmitter signal testing for Blasting

FSM will test receipt of the TTE signal.

1. First and foremost, it is important to clear the FSM logs before a round of testing is to be conducted. This ensures that previous test results are not used to assess the current deployment. Refer to 4.3.3.
2. Next step is to switch the FSM on (activate the FSM) through NFC using the Tagger.
3. The FSM needs to be placed in its final location (most likely to have a weak TTE signal) before switching the transmitter to test mode. If the FSM's are placed in holes, one FSM should be placed somewhere visible as a monitor.
   NB: The serial number/UID must be recorded for reference.
4. The transmitter is then activated for test messages by switching the Tx isolator to the up position and switching on the battery while the key switch is in the Test position.

TRANSMISSION OF BLAST COMMANDS WHILE FSMS ARE DEPLOYED WILL REGISTER AS BROKEN MESSAGES AND WILL AFFECT SURVEY RESULTS NEGATIVELY.

5. The FSMs communicate their status through the LED lights on the light ring. A slow, one second red flash every 5 seconds indicates a search pattern while a quick red flash followed by a green flash indicates receipt of a successful message. A red flash without a preceding green flash indicates receipt of an unsuccessful message.
6. If the messages received are unsuccessful, the transmitter and antenna must be moved to the next test location. At each location, the transmitter is ON and in the Test mode for at least 30 minutes. Receipt of successful message is verified by the flashing green light on the FSM. Final verification must be done by downloading the FSM logs to the tagger to verify test results.
7. Verify that in the Site Survey State, if any change in position of the Tx and/or its antenna takes place after Rx units have been placed, the quality of the signal shall be verified using FSMs in parts of the blast area most likely to have a weak TTE signal.
8. Verify that if any change of position for the Tx and/or antenna occurs after the signal quality test has been completed, the site survey shall be repeated.
9. Before moving the antenna, the transmitter must be switched OFF including the Battery for safety reasons. The FSM's logs must be cleared and activated before the Tx is switched on again for a new round of testing.
10. Upon completion, the FSMs can be retrieved, and their logs can be analysed using the Tagger or NFC Reader (Described in Section 4.3.3)
11. Verify that if the signal quality test is successful, loading of the holes shall be authorised.

5.5. FSM Log Interrogation using Tagger

The Tagger must be placed against the NFC antenna of the FSM. Refer to Section 4.3.3 for log interrogations.

It is important to note that the FSM requires at least 70 data packets to have been received for the test to have been deemed successful and the percentage packets received is at of 98%. This equates to less than 1/100000 chance of misfire.

- Date Time Activated – time stamp to indicate use.
- Packets Rxd – should be equal to or greater than 70.
- Packets missed - as low as possible (<2).
- 5 Rxd - equal to or greater than 98%.
- BER – less than 1/100 000.

5.6. Receiver activation

The detonators are equipped with a 4-pin connector crimped onto the detonator shell.

1. Activate the Rx unit (switch on) by inserting the 4-pin connector. Note that the Test Mode on the Tx should be selected during this procedure.

Figure 19: Receiver Activation

2. The Rx will flash the green LEDs 3 times at 1 Hz and perform a self-diagnostic test.
   - When a successful TEST signal is received the green LED will turn “ON” for 10 seconds.
   - If the red LED flashes continuously remove the detonator and replace it with a new detonator. The failed detonator should be marked and isolated for further analysis.
3. The results of the self-diagnostic test are stored on the Rx and will be downloaded to the Tagger when polled, “Test Rx” menu item 3, as depicted in **Error! Reference source not found.**.
4. Attach the booster by inserting the detonator end and then turn the booster clockwise to fasten.
5. The power of the Rx will be deactivated when the detonator connector is disconnected. The detonator can be reconnected to check functionality.

NOTE	**The non-functional detonator should be treated according to the mine’s procedure for handling out-of-box detonator failures.**

6. As the underground mining situation is dynamic, the Magnetic Field strength meters could be deployed out-of-hole to visually indicate any change in magnetic signal strength during Rx activation and deployment.
7. Deactivate the TEST mode on the Tx.

5.7. Tagging

Figure 20: Tagging

The NFC mode is activated on the Tagger for Rx communication and detonator programming.
The Blast plan and encryption code are downloaded to a specific Tagger from the BCU II and/or the Surface Blast controller. The Tagger will first request a self-diagnostic test by the Rx and the results from the test downloaded to the Tagger.
This Tagger will be used to program all the detonators in the specific group. A Tagger can only have one encryption code loaded at a time to prevent incorrect tagging of receiver groups.
If the Tagger fails during the tagging of a group of detonators, a second Tagger can be used to complete the process.
Refer to section 4.3.1 to tag receivers and section 4.3.2 to test receivers.

NOTE	**Multiple Taggers may be used to tag/program detonators in the same group. Users must ensure that the correct key has been loaded onto the tagger prior to tagging the Rx's.**

NOTE	**It is recommended that the Rx's with Detonators connected be tested after tagging process. This should be included in the mines blast preparation processes and procedures.**

5.8. Deploy Receiver into Borehole

To ensure the correct receiver unit is deployed in the correct blast hole, the blast hole number as defined in the blast plan should be written on the Rx unit.
Attach a tether with a tag indicating the relevant hole information to the receiver. This will assist recovery of units if receivers are non-functional and will also assist in identification of holes that have been primed.

Figure 21: Spider Attachment on Receiver

Screw the spider attachment onto the assembled Rx. The spider can be attached to the top end, or both ends as depicted above, depending on user preference.
Attach the Rx unit to a lance or charging pipe for up-hole deployment.

5.9. Switch Transmitter to BLAST mode

The encrypted commands for firing Tx will be generated either by the BCU II or the Surface Blast Controller.

Ensure that the blast area is evacuated before switching to BLAST mode.

- Switch Tx to BLAST mode using the key switch.

The key cannot be removed when in BLAST mode to ensure that anyone can abort a blast by switching it back to TEST. When in test mode the key can be removed to ensure that it cannot accidentally be switched back to BLAST while people are busy performing MSF or deploying Rx's.

- After the Fire sequence is complete, an auto TERMINATE is immediately (within 500 microseconds) executed to ensure no unfired Rx (detonator/s) are still deployed. This will disable the Rx units.

5.10. Sending the Blast Commands via the BCU II

The Blast commands may be sent via the BCU II in standalone mode using a red key or via remote blasting using a yellow key.

The BCU II will provide 2 FIRE buttons for user to press to initiate the blasts. For the underground system, the Fire buttons must be pressed within 30 seconds of count down and if not pressed the Rx's will go back to sleep mode or power saving.

5.11. Sending the Blast commands from BCU II to CyberDet I

The BlastWeb II BCU II is able to send the CyberDet I Blast command via the Tx through Antenna and to the CyberDet I detonators.

1. The BCU II connects to the Tx on channel 6. The Wireless capability must be activated from the BCU II on channel 6. The DetNet bi-phase communication protocol is used with twisted pairs of wire to connect BCU II to the Tx.
2. The Maximum distance between BCU II and Tx is 2000 m.
3. The first step to blast CyberDet I from the Surface Blast Controller is to create a communication encrypted key (CEK) from the Planning Tool (see UTM-00368) and download it to the Tagger that will be used for tagging Rx. This step will be preceded by the site survey in which the position of the Antenna will decided.
4. The BCU II will be enabled to communicate with the Tx as follows:

6 FAULT FINDING

6.1. BCU II to Tx Communications

The BCU II will continuously communicate with the Tx. The BCU II will report if any communications failure exists whereby, it detects a break in the communications link between the BCU II and Tx.
The BCU II will enter a safe mode state whereby it will not attempt to communicate further with the Tx.
The Tx-BCU II cable assembly must then be inspected for possible damage.
The communications link health will be indicated on both the Tx and BCU II.

6.2. Tx Error Codes

Should any hardware faults occur on the Tx that prevent blasting an Error message will be displayed indicating the cause of such a fault and possible remedies and advisories.
Possible faults are but not limited to:

- Disconnected or damaged cable to Tx (open circuit).
- Damaged power electronics on the Tx.
- Overcurrent detected on the Tx resulting from cable, connector or antenna damage causing a short circuit.
- Battery level too low for blast.
- Mode switch not set to blast.
- Overheating of the equipment.

Table 1: Rx LED Descriptions

#	Action	Green LED Behaviour	Red LED Behaviour	Comment
Rx Behaviour				
a	Power Up + Internal Diagnostic Excluding TTE	Flash 3 times at 1Hz 50% duty cycle	Off	Disable Tagging, Units can be placed somewhere waiting for TTE signal
b	Not been tagged + TTE signal	Keep Green LED on for 10 seconds		Tagging enabled, TTE signal Rx disabled while LED on,
c	Tagging Unit	Off	Red LED flashed 1 Hz 50% duty cycle	TTE signal reception disabled unit needs reprogramming or/new det
FSM Behaviour				
a	Power Up	Flash 3 times at 1 Hz 50% duty cycle	Off	
b	FSM Activate	Flash 3 times at 2 Hz 50% duty cycle	Off	
c	FSM Deactivate	Flash 3 times at 1 Hz 50% duty cycle	Off	
d	Scanning	Off	LED flashes once every 5 seconds while scanning	
e	TTE signal reception	Flash once (LED on for 100 ms) when TTE signal has no errors	Off	
f	Battery Low	Off	Red LED flashed continuously 1Hz 50% duty cycle	TTE Disabled
g	NFC full (80% full)	Off	Red LED flashed continuously 1Hz 50% duty cycle	TTE Disabled

6.3. CyberDet I Error messages and actions

Table 2: CyberDet I Error Description

Item	Activity	Error message	Description	Suggested Action
Rx's	Power on	RED LED on	Rx diagnostics error during startup.	Unplug detonator, wait 5 seconds for unit to power down and plug it back in. If it happens again replace the Rx unit.
		RED LED flashing	Rx diagnostics error during startup.	Unplug detonator, wait 5 seconds for unit to power down and plug it back in. If it happens again replace the Rx unit.
		GREEN LED flashing 3 times	Rx startup diagnostics successful.	Unit it ready to receive test signal and be tagged.
		GREEN LED on for 10 seconds	Rx has received a test signal and can be tagged.	
Rx's	Testing with Tagger	LOW BAT	Rx battery below 3000 mV	Replace the Rx unit.
		BAD DETCOMMS	Rx failed to a get reply from detonator	Unplug detonator, wait 5 seconds for unit to power down and plug the Detonator back in. If it happens again replace the Rx unit.
		BAD FUSE	Detonator fuse detected as faulty	Replace the attached detonator
		ID NOT SET	Detonator ID not set	
		BAD STATUS	Detonator self-calibration bit not set	This error is shown when Rx has not been tagged. Tagging the Rx will set the self-calibration bit on the detonator.
		CAL PER ERR	Detonator calibration period not set to 1000 ms	This error is shown when Rx has not been tagged. Tagging the Rx will set the calibration period to 1000 ms on the detonator.
		CAL TIME ERR	Invalid det delay detected	This error is shown when Rx has not been tagged. Tagging the Rx will set the calibration time to the desired delay (0 to 20 000 ms) on the detonator.

Item	Activity	Error message	Description	Suggested Action
		NO SIG ERR	Rx has not received a test signal since powerup	The Rx has not received a test signal. Expose the Rx to a test signal. This is a requirement before being able to tag the Rx.
		DET PROG ERROR	Det ID or delay does not match Rx ID and delay. This means that the attached detonator has not been programmed correctly or a new detonator has been attached after tagging.	Retag the Rx to reprogram the attached detonator so that the Rx ID and delay matches that of the detonator.
		DISARM ERR	Rx has been disarmed/self-terminated	Replace the Rx.
		BLAST LINE ERR	The Rx has detected HV on the detonator lines during BIT.	Repeat the Tagging or Testing process. Should the problem persist replace the Rx this is a hardware fault
		NFC TIMEOUT	No Rx NFC was detected, and tagging has been aborted after timeout.	Could be due to poor positioning of the Tagger over the NFC tag. Retry communication if it fails after repeating 3 times then replace the Rx as this could be due to NFC hardware faults such as damaged/disconnected NFC antennas.
		NO RESPONSE	The Rx was not able to respond to the test request. This is most often due to the Rx not being powered and therefore not responding to the Tagger.	Unplug detonator await 5 seconds for unit to power down and plug the detonator back in. Ensure that the GREEN LED flashes, indicating that the Rx was able to power up. If it happens again replace the Rx unit.
		NFC PROG ERROR	Tagger was unable to write programming data to the Rx. This could be due to faulty NFC EEPROM in the Rx.	Replace the Rx unit.

Item	Activity	Error message	Description	Suggested Action
		PROG DATA INVALID	Programming data CRC read from the Rx is invalid/corrupt. This is detected during testing of an Rx. This can happen if a tagging operation on a Rx was interrupted, and the unit tested.	Retag the Rx unit and ensure that the Tagging operation is completed successfully.
		Rx NOT TAGGED	The error is shown when an Rx is tested. It means an Rx has never been tagged and still has the factory default data in its EEPROM. This just means the unit can be tagged.	No action required simply Tag the Rx unit with valid data.
	Tagging / Programming	NO SIG ERR	Rx has not received a test signal since powerup	The Rx has not received a test signal. Expose the Rx to a test signal. This is a requirement before being able to tag the Rx.
		BAD FUSE	Detonator fuse detected as faulty	Replace the attached detonator
		TAG ABORT	The tagging operation was aborted from the Tagger.	User aborted the Tagging operation. Simply retry tagging.
		DISARM ERR	Rx has been disarmed/self-terminated	Replace the Rx.
		BLAST LINE ERR	The Rx has detected HV on the detonator lines during BIT.	Replace the Rx this is a hardware fault.
		NFC TIMEOUT	No Rx NFC was detected, and tagging has been aborted after timeout.	Could be due to poor positioning of the Tagger over the NFC tag. Retry communication if it fails after repeating 3 times then replace the Rx as this could be due to NFC hardware faults such as damaged/disconnected NFC antennas.

Item	Activity	Error message	Description	Suggested Action
		NO RESPONSE	The Rx was not able to respond to the tagging/test request. This is most often due to the Rx not being powered and therefore not responding to the Tagger.	Unplug the detonator and wait 5 seconds for the Rx to power down and plug the detonator back in. Ensure that the GREEN LED flashes, indicating that the Rx was able to power up. If it happens again replace the Rx unit.
		DISARM ERR	Rx has been disarmed/self-terminated	Replace the Rx.
		BLAST LINE ERR	The Rx has detected HV on the detonator lines during BIT.	Repeat the Tagging or Testing process. Should the problem persist replace the Rx this is a hardware fault.
		NFC TIMEOUT	No Rx NFC was detected, and tagging has been aborted after timeout.	Could be due to poor positioning of the Tagger over the NFC tag. Retry communication if it fails after repeating 3 times then replace the Rx as this could be due to NFC hardware faults such as damaged/disconnected NFC antennas.
		NO RESPONSE	The Rx was not able to respond to the tagging request. This is most often due to the Rx not being powered and therefore not responding to the Tagger.	Unplug the detonator and wait 5 seconds for the Rx to power down and plug the detonator back in. Ensure that the GREEN LED flashes, indicating that the Rx was able to power up. The Rx unit must receive a test message before tagging can proceed. If it happens again replace the Rx unit.
FSMs	Activation	RED LED flashing	FSM scanning for signal. No signal has been detected.	If the Tx is in test mode wait for a minute before the FSM can lock onto the signal. If it fails to lock it means that the Tx antenna needs to be moved closer to the FSM.
		Green LED flashing	FSM detected a valid test signal.	FSM is receiving test messages, no action required.
		LOW BATTERY ERR	FSM battery below 2600 mV	

Item	Activity	Error message	Description	Suggested Action
		NFC TIMEOUT	FSM did not respond to activation, or no FSM was detected.	Ensure that the FSM NFC area is properly aligned. If it still fails, it means the FSM's battery is too low to switch on the device and will require replacement.
FSMs	Download Logs	LOW BATTERY ERR	FSM battery below 2600 mV	The FSM battery is dangerously low and requires replacement. There is a strong chance of the FSM switching off while a survey is being conducted.
		LOGS ERR	Invalid last log index detected. This can happen if the FSM was unable to write the last log index in EEPROM memory due to HW failure or the FSM has not overwritten the factory default value.	First ensure that the FSM was activated prior to the logs being downloaded. If the FSM was activated and the logs are unable to be read the FSM needs to be replaced.
		LOGS EMPTY	No FSM logs detected meaning the FSM has not logged any test messages.	The FSM has not been exposed to any test signal or has not detected any test signal since activation. You need to expose the FSM to the test signal by switching on the Tx in test mode and having the FSM within range of the Tx signal.
		TOO FEW MSGS RxD	Less than 70 test messages have been received. This can mean that the test pattern hasn't been running long enough or that communications link to the Tx is poor and less than 70 messages have been received.	Ensure that you run a survey for at least 30 minutes to receive at least 70 test messages. If it can be confirmed that the test was run for at least 30 minutes, it means that the FSM is not within range of the Tx signal. The Tx antenna will have to be moved closer to the FSM.

Item	Activity	Error message	Description	Suggested Action
		LOW % RxD	The FSM received less than 98% of the messages transmitted.	This is an indication of a poor Tx communications link, and the Tx antenna will have to be moved closer to the FSM. The survey needs to be conducted again to ensure good signal coverage.
		NFC TIMEOUT	No FSM NFC detected when trying to communicate.	The Tagger did not detect the FSM NFC. Ensure that the NFC area is positioned underneath the Tagger and retry. Should this fail repeatedly it means that the NFC on the FSM has been damaged, and the FSM needs to be replaced.
Tx's	Power on	SYSTEM FAIL LED RED ON	An internal Tx HW fault has been detected preventing operation.	Power cycle the Tx again. If the problem persists the Tx needs to be returned and inspected.
	System idle	SYSTEM FAIL LED RED FLASHES	An intermitted fault occurred but the system recovered.	No action is required if the LED turns off by itself. Power cycle the Tx if the LED remains on.
Tx's	Tx Transmitting	Tx ANTENNA RED light on	The Tx is attempting to transmit but the current running through the antenna is below the required level.	Check deployment and connections to the antenna. Inspect the antenna wire or capacitor bank for any damage. The antenna needs to be deployed completely flat with no/little metallic or material with high magnetic permeability close to it.
		Tx ANTENNA RED light flashing	The Tx antenna light transitions from RED to GREEN when the transmission starts as the current in the antenna builds up. Should the light transition from GREEN to RED during transmission it means that there is an antenna fault.	Check deployment and connections to the antenna. Inspect the antenna wire or capacitor bank for any damage. Replace the antenna or capacitor bank should any damage be found. The antenna needs to be deployed completely flat with no/little metallic or material with high magnetic permeability close to it.

Item	Activity	Error message	Description	Suggested Action
		COMMS GREEN light on	The communications light goes on when a command has been received from the control equipment. The light will stay lit for the duration of the Tx executing the command before responding to the control equipment. During TTE transmissions the light will stay on for the duration of the transmission indicating that the command is still being executed.	The communications light should flash during diagnostics interrogation from the control equipment. Check the communications cables and connectors for damage should the light not flash during initial connection.
		COMMS GREEN light off	The communications light switches off after the Tx has executed the desired request from the control equipment.	The communications light should flash during diagnostics interrogation from the control equipment. Check the communications cables and connectors for damage should the light not flash during initial connection.

7 MISFIRE HANDLING PROCEDURE

Only a competent person as appointed by the mine may handle and remove misfires in accordance with this procedure, the mine's procedures, and regulations. Do not continue unless you are thoroughly familiar with the system components and the operation of the Wireless detonator. Failure to observe the contents of this section may lead to personal injury or damage to equipment.

7.1. Misfire Recovery

- Ensure that the CyberDet I transmitter is switched off prior to handling and recovering of misfires.
- Treat misfires carefully, as damaged detonators and boosters can be unstable, and sensitive to detonation.
- Wear the recommended PPE (safety goggles and gloves) when treating misfires.
- Never attempt to pull a Wireless detonator assembly out of a misfired shot-hole when it is stuck: In the case where the detonator is damaged to the extent that the explosives charge in the detonator is exposed, friction, especially with grit in the hole, could cause accidental initiation.
- Detonators and explosives are to be put in separate approved explosive containers – never together.
- Always remember that a Wireless detonator assembly in a misfired hole has been exposed to extreme external forces during the blast. This means that a detonator retrieved from a misfired shot-hole is not in the state of original manufacturing and could be in a potentially more sensitive state.
- When retrieving a Wireless detonator assembly from a misfired hole, transfer directly into the approved explosives container – never place it on the floor.
- Always handle/carry the Wireless detonator assembly on the receiver side with the booster/detonator away from your body.
- Avoid handling detonators by picking it up on the detonator or carrying it in your hand. Always handle it by means of the connector part and ensure that the detonator is pointing away from you.
- A damaged detonator tube could have the explosive compounds exposed. This will make the detonator more sensitive for initiation through impact and friction especially if grit is present.
- Do not handle any damaged units where possible and destroy in-situ.
- Always follow mine procedures and regulations when destroying misfires in terms of designated areas for destruction, maximum quantities allowed, blasting times and procedures.

KEY POINTS	ADDITIONAL INFORMATION
Safety Notes: • ***Inspect the unit for deformation or other mechanical damage prior to disassembly of the unit.*** • ***Do not remove the booster end cap from the booster assembly.*** • ***Misfires that cannot be removed from the mine shall be destroyed in accordance with the Mine's Destruction of Explosives procedure at the end of each shift.*** **7.1.1. Removal of the Booster** • The booster will require 3 Newton of rotational torque force to unlock from the Rx. No special tools are required for this operation. • To unlock, turn the Booster in an anticlockwise direction for 45° • Pull the booster free from the detonator and receiver. • Place the booster in a suitable container such as an elephant foot bag as per mine procedures for removal off- site for misfire storage, investigation, or destruction. Each mine will have their own mine specific safety procedures that needs to be adhered to.	

KEY POINTS	ADDITIONAL INFORMATION
7.1.2. Removal of the Detonator. • The Detonator is clip-locked in place connected to the Rx. • To unlock, turn the Detonator, press the two clips on the side of the connector main body and pull the connector free from the receiver. Ensure that the detonator always faces away from you at all times during handling. • Place the Detonator in a suitable container such as an elephant foot bag as per mine procedures for removal off- site for misfire storage, investigation, or destruction.	
7.1.3. Receiver disposal • The Rx should be decontaminated by removal of all explosive residue and removed from the blasting area. • The Rx should be secured, packaged, and immediately returned to DetNet for further analysis. • Decontamination certificate as per mine procedures to be issued for the device being removed.	

8 PRE-BLAST CHECKLIST

Prior to starting the TTE blast command transmissions the following checklist must be completed:

CHECK TO PERFORM	ANSWER
1. Field strength survey done to ensure signal coverage?	
2. Tx antenna and capacitor bank connected to Tx?	
3. Tx antenna location and deployment identical to when FSM survey was performed. If not, the field strength survey must be done prior to blasting.	
4. All relevant Rx units tagged with the correct blast-key and inserted into holes? It is critical that a site inspection be done as well as register be kept of any Rx units used in the blast to ensure all units are accounted for. Any units not used in a blast must be disassembled and their blast keys encryption keys deleted using the tagger.	
5. Tx battery state of charge above 30%?	
6. Tx key/mode switch position in blast mode?	
7. Tx isolator switch in the ON position?	
8. Tx system OK light on and FAIL light off?	
9. BCU II or BCU II SIM has a stable connection with Tx?	

.

Only once all the system checks mentioned above have been performed and are all confirmed to be true may the authorised user select the appropriate blast key and commence TTE blast command transmissions.