BATTERY, DATA AND HARDWARE SECURITY ISSUES RELEVANT TO CABLELESS OPERATIONS.

INTRODUCTION

There is no doubt that cableless/cablefree* instruments (*these words used synonymously here) have brought significant benefits to land exploration. Additionally, with a few types of cableless systems even shallow water seismic recording has been made quicker, faster and lower in cost. But cableless technology can bring new problems to face. The greatest of these are (a) the number of batteries to deal with, (b) that many such systems force use of lithium ion based batteries, and (c) hardware and data security, which is the main subject of this paper - although all three issues are intimately related.

Some cableless systems can force the use of up to one hundred times as many batteries for the same amount of channels as a cabled system, though some cableless system are far better. Cabled systems can also make use of simple car or small truck batteries. With most digital cable telemetry systems, if any ground unit, battery or sensor is stolen or damaged it is likely that the observer is alerted instantaneously and he can do something about it. Further, data is not stored inside remote units as it is sent along cables in real time to the central system. Thus, battery, hardware and data security are all easily controlled with cabled systems. [1]

However, in cablefree systems things are not so simple. These types of instrument fall into different groupings as far as communication between the spread and the observer are concerned, and thus the level of security risk.

SHOOTBLIND SECURITY RISK

Shootblind recorders are by far the most troublesome when it comes to security. Some manufacturers claim that there has never been any instance of theft or data loss from crews using their shootblind system, whereas a little investigation reveals this usually not to be the case. Even for those shootblind crews lucky enough not have suffered badly, as with other problems in exploration, it is beginning to seem that “it is only a matter of time”.

Some manufacturers do admit to the problem and suggest it is best addressed by burying the equipment so that it is not longer visible to thieves. Putting aside the issue of the manpower, tools and HSE exposure in having to do this, it is simply not always practical.

If channel counts are high, if the terrain does not support digging of holes, or if wet conditions mean that putting equipment underground prevents reception of GPS timing signals by the ground unit, then burying is not a viable way to solve security risk. Further, as such equipment has no means to communicate with the operator, then loss of GPS signals may go unnoticed before it is too late. In such cases it is no longer a case of losing data from a few random traces but large numbers of adjacent channels - perhaps rendering the entire survey unusable. There are also more and more cases of thieves catching on to the practice of burying equipment and digging it up, especially if they know it to contain valuable batteries, and reports of significant equipment theft are increasing.

An article in New Technology Magazine (Oct 2011) is just one example of the theft problem with shootblind nodes. It refers positively to using cableless equipment, that failure rate of equipment is very low but that vandalism and theft meant the loss of over $100,000 in batteries and ground units on a single survey. Other instances of damage and loss in shootblind operations are less well publicised.

Whatever the true scale of the problem, nowadays taking the risk of using shootblind recorders is simply technically unnecessary and not even financially advantageous. The cost of purchase difference between

[1] The situation for cable crews which leave equipment out for 24 hours/day but only operate during daylight hours is a different matter and can sometimes be a greater security risk than the more sophisticated cableless systems.

everything needed in a shootblind system and a non-shootblind recorder may be insignificant or even negative. This is because shootblind systems usually require purchase of many more channels which can be used while some are in the data harvesting rack, which itself tends to be very expensive. Shootblind channels tend to have to use lithium batteries and chargers which are far more expensive than alternatives. Such recorders can also be more expensive to operate than instruments with communication capability due to the extra personnel needed, while risk of hardware and data loss is much greater.

PREVENTION BETTER THAN CURE

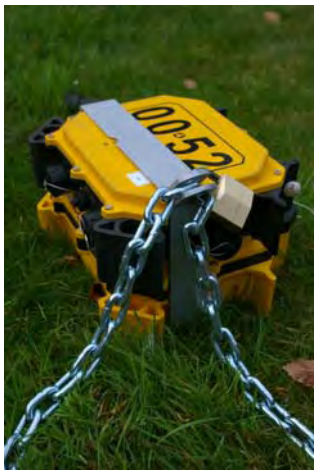
The issues surrounding hardware theft on seismic operations are similar to those in any situation. It is always better to try to prevent theft than to try to deal with it after it has happened. It also the case that such prevention is better undertaken with low cost and simple measures than with complex ones. If theft ever does take place, it is then better to know about it quickly rather than hours or days later. This is what we have been used to with cabled systems, so why accept anything worse with cableless?

Finally, it is better to have a variety of measures to suit each security situation rather than be limited to a few approaches which may not be suited to all circumstances. Sigma scores significantly higher in all these areas than any other system.

SIMPLE SECURITY

Some equipment theft is simply opportunistic. The equipment looks valuable and so passers by may try to steal it. Other theft is planned, for example to get hold of internal batteries or even memory chips.

To prevent such theft of Sigma system-specific equipment, and depending on the area, grounds units and batteries can be very securely chained in place. A simple locking and clamping device can be supplied or manufactured locally if required, as well as good quality padlock and chain. This mechanically locks the Sigma battery box to the Sigma ground unit.



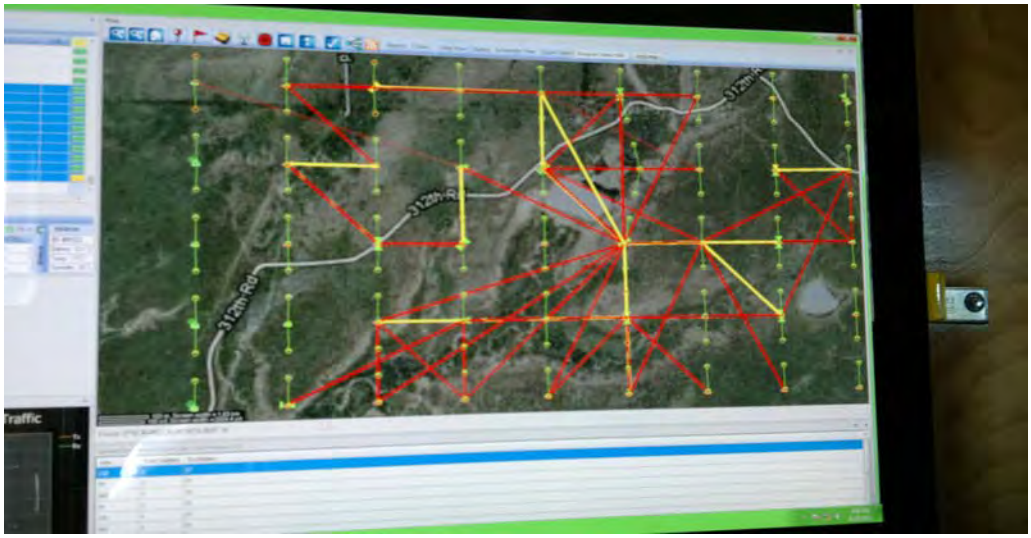
Being able to steal a package in this configuration would require heavy duty cutting equipment. As Sigma does not come as standard with an internal battery (see later for advantages to this) this simple device also makes it harder to detach the external battery. This means that the Sigma box could remain powered up for extended periods even if the chain is cut. This enables the first line of more sophisticated Sigma defence to be enabled - use of the mesh radio network.

OTHER LEVELS OF SECURITY

Most non-shootblind cableless systems rely on the 2.4 GHz ISM band for communications. The problem with this band is that it is very quickly absorbed by water molecules. See iSeis on-line technical paper on 2.4 GHz absorption.

However, the reliability of successful communication using 2.4 GHz also depends on other issues. The most important of these are the communication topology and attempted data rate. Sigma comes as standard with a way of using 2.4 GHz which provides the most reliable method of remote security, called Mesh Radio Networking - MRN.

GPS track of Sigma ground unit.



Mesh routing. Long range is not attempted meaning comms is more reliable, easy to deploy at ground level and useful as a security measure. Range can be extended at survey periphery by simple use of elevated antenna.

MRN-based communication is where each active ground unit only attempts to talk to its nearby boxes, and with a relatively low data rate. This short-range/low data rate approach is by far the most reliable method of communication and makes ground equipment simple to deploy. In areas of no vegetation, transmission range is a few kilometres but as foliage density increases range drops to due the nature of 2.4 GHz signal absorption, so Sigma always assumes range will be much shorter. To increase range in areas of thick foliage, repealers can easily be used if required.

Trying to transmit long range or with high data rate leads quickly to communication problems. Because Sigma's MRN is so reliable it is possible to transmit security-related information, for example: a box's GPS position, box internal humidity (indicating deliberate damage), if a sensor or battery is disturbed and so on. Some other non-shootblind systems also have methods of communicating dependent on different protocols or topologies. Such methods of communications have proven not be at all as reliable as Sigma's MRN in difficult environments - which after all is where theft is more likely to take place.

As a more sophisticated option, perhaps not suited to all territories, Sigma also offers satellite tracking of boxes. This requires payment to a third party of a subscription but it may be an appropriate measure in some locations.

Sigma ground unit showing mesh radio network repeater.

SECURITY AND DATA RETRIEVAL

In most seismic surveys, the value of the data inside the ground unit once shooting has begun is greater than the replacement cost of the hardware. Of course, the ideal with a cableless system is to have all data transmitted with the minimal delay to the central system, thus securing the data. However, whereas Sigma has multiple real time transmission options, each configurable for different operational environments, as with all cableless hardware real time transmission requires additional equipment compared to the basic Sigma-MRN system. If the operator chooses to run Sigma without a real time option, data must be harvested by some method which necessitates an operator to connect to the line unit or get close to it.

Most methods which allow the user to download data by being in proximity to the ground unit also rely on 2.4 GHz transmissions. We have already seen that this band can be seriously absorbed my water molecules, so reliance on this single method of data harvesting can lead to difficulties and delays in retrieving data. And, the longer it takes/more time consuming it is to retrieve data, the longer it stays on the line at risk of being lost.

Thus, Sigma also has various remote harvesting options, some of which rely on 2.4 GHz, but importantly-some do not. Such methods include direct ethernet cable connection to the ground unit; another use of an external USB-type memory into which data from the internal memory will flow upon connection. This is a very rapid method of data harvesting and can be a very efficient way to reduce data loss risk.

EXTERNAL OR INTERNAL BATTERIES FOR CABLELESS HARDWARE?

Most cableless equipment does not offer an internal battery as standard. There are very good reasons for this. Generally batteries need to be changed within one or two years. An internal battery requires that the ground unit is opened but ideally ground units should not be opened up, especially in field conditions, as this can affect the sensitive electronics. If internal batteries are usually based on some lithium chemistries, there is risk to the box electronics and its data from such batteries erupting or even catching fire. It is not difficult to find examples of this on line.

The next reason to avoid internal batteries is that they can only be charged within a much narrower temperature range than the operating range of the unit, and to achieve maximum number of charge cycles, some battery chemistries (i.e most of those based on lithium) can be very fussy about the precise changing temperature. This means, that once nodes are brought in from the field, they must firstly be allowed to reach a rather narrow temperature range before they can be charged. If temperature forcing (air condition in hot climates, heaters in cold climates) is not available for large numbers of channels, then ground units can take a significant time to reach charging temperature meaning they are kept off the line for even longer periods, so reducing productivity.

Further, internal batteries are quoted with a certain energy capacity, often equating this to operating time. However, as the batteries age/undergo many charge discharge cycles, this capacity decreases, meaning that it is unlikely that the node will operate without external power for any typically minimum duration, so now the extra weight of an almost useless internal battery is also being carried around.

SUMMARY

Cableless systems have brought many advantages to exploration but the issues of security must also be considered, and how this is affected by use of the 2.4 GHz band. iSeis' Sigma system offers the largest range of approaches to deal with these interconnected issues.

It is thanks to the various security measures available with Sigma that users suffer demonstrably much low levels of theft and damage compared not just to shootblind hardware, but also compared to other systems which are claimed to be able to communicate in real time.