Reverse Engineering an Army Larkspur-era Secure Voice Encryption BID150 ‘DM Box’

Brian Blackwell G3YVW

The author, since serving an apprenticeship in the REME - 36 Command Workshop Colchester, in Telecommunications, 1969-1973, has maintained a strong interest (and collection, since retirement) of the Larkspur range of army radios/communications equipment, and to make operational.

The latest acquisition was a DM box. This was the interface box used with the army’s first combat net secure encrypted voice communication in conjunction with the Larkspur VHF radio sets C42/C45 and the ***BID150 (DELPHI) encryption unit, in service from the mid/late 1960’s to around 1980 and used from Aden to BAOR to Northern Ireland. The BID150 used daily-changeable punched cards for the key settings for the unit’s three card readers.

***BID stands for BRITISH INTER DEPARTMENTAL, ‘BID’ being the prefix normally used for secure/encrypted communication equipment type numbers, and the authority for the equipment was the Communications-Electronics Security Group (CESG) – now called the National Cyber Security Centre, part of the Government Communications Headquarters (GCHQ).

No documentation exists apparently for the DM box and the author assumes this formed part of the BID150 classified documentation and hence is not available/destroyed.

The aim of the author was to reverse engineer the DM box so as to be able to provide the main (original) ‘J1’ harness facilities **[6]**, *i.e.* in CLEAR mode (as against SECURE mode when using encryption with the BID150) for use with a C42 (or C45), but also – once circuits were produced, to investigate the operation of the DM box’s ‘reported’ A/D converter and delta modulation operation and so to observe the type of signal the BID150 would have used.

Background of Project and Reverse-Engineering Preliminary Work

The project was to proceed without access to BID150 (or associated documentation) - the only known example of one in existence is within the Royal Signals museum. **Figure 1** shows a photo of the BID150 together with 'sample' punched key cards.

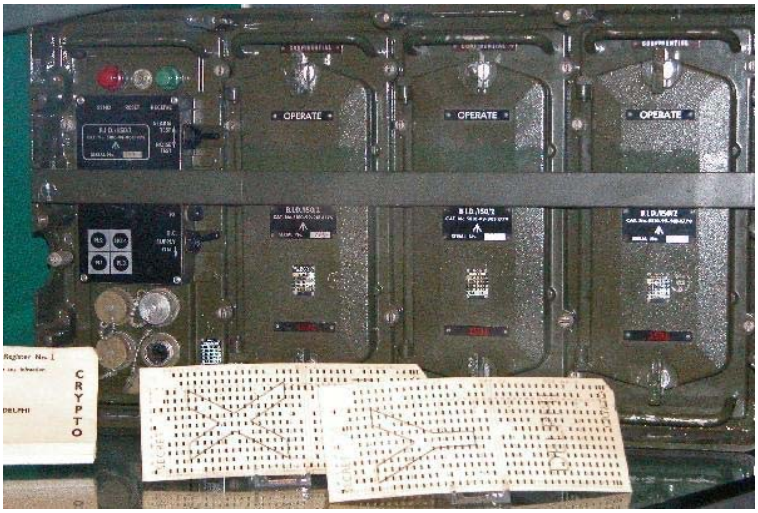

Figure 1. Photo of a BID150 with typical punched key cards

The DM box has been reported as providing many functions – some of the basic army 'J1 harness box' operations (set-intercom-call switching, headset/microphone connections/gain control, remote and rebroadcast operation); and analogue/digital (A/D) conversion/delta modulation (ΔM), connection to a remote box ('RCDM'); rebroadcast; enabling of SECURE/CLEAR operation; ensuring correctly received secure signal levels.

Delta modulation (ΔM) appeared (from comments and users' experience) to be the type of modulation used rather than pulse code modulation, due to possibly bandwidth and complexity limitations with PCM.

In fact there are many references to the DM box in various publications and sites but using different names - e.g. Deviation Monitor, Digital Modulator, Delta Modulator, etc. No name has been found for the DM box in official army documentation available or on equipment used with the DM box that the author has seen**.

** One other piece of radio equipment the author is in possession of is the combat net 'Net Radio Access Unit' **[17]** from the BRUIN trunk communication system for the BAOR **[16]**. Although this unit was possibly not put into general use, it was, as the name suggests able to connect into the Larkspur VHF radio net (and hence into the BRUIN trunk system) by means of the 'J1' 6-pin harness audio connection or via a 'DM (REM)' socket internally connected with the 'J1' plug, which would have connected into the DM box remote connection when one was in use.

A typical army communications setup with the C42 (and PSU), BID150 and DM box, taken from an army user handbook of the time is shown in **Figure 2**, with the DM box at the top right, above the C42/C45 radio set.

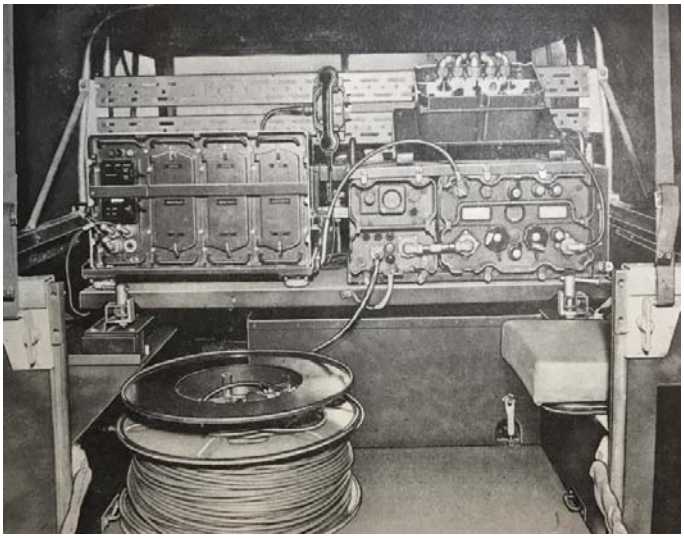

Figure 2. BID150 installation in an army ¼ ton truck

Now that a DM box(s) had been obtained by the author – see **Figure 3**, it was opened up for inspection to see what the likely issues would be in making the unit operational, at least in part. It was hoped that the unit could be made to function in the CLEAR mode and so would operate as a near basic 'J1' box together with the author's C42 No. 3 **[8]** and Goodman*** box, and also simulate the A/D aspect of the unit with appropriate input and output signals that occurred between the BID150/C42 with the DM box. Note the No. 3 version of the C42 (or C45) was required as this unit was adapted to additionally handle digital pulse code modulation (as well as voice FM) - required for the BID150. The frequency range was 36-60 MHz (the C45 set was identical except for a frequency range of 23-38 MHz), power output was 15 W with ±15 kHz deviation. Channel spacing was 100 kHz.

*** The 'Goodman box' ('VHF Applique Unit') **[3]**, **[4]** was an aid to checking the system antenna integrity, transmitter power output, the received signal strength - required for satisfactory/reliable ('secure') communication, and to help protect against unwanted interfering ('clear') signals. See **Figure 21** for the author's final system setup including the Goodman box. This box was designed by Royal Signals S/Sgt (at the time) Rodney 'Benny' Goodman, and it would appear after the introduction of the BID150/C42(C45) system. It was noted that the original U/Hs dated in the 1960s do not show or make reference to this box. It is assumed (by the author) that 'Benny' Goodman did also previously design the DM box. The Royal Signals 'Roger So Far…' **[15]** publication cites – *He was awarded the BEM for his work designing a sophisticated control system to enable the BID150 to work with the C42 and C45 radios.*

Figure 3. One of the author's DM boxes prior to reverse engineering

However, making the unit operational was not to be as simple as first thought. The inside was quite complex regarding the build - electrically and mechanically, and the unit was well made although very compacted. **Figure 4** shows the case removed and the two main PCBs hinged open for access.

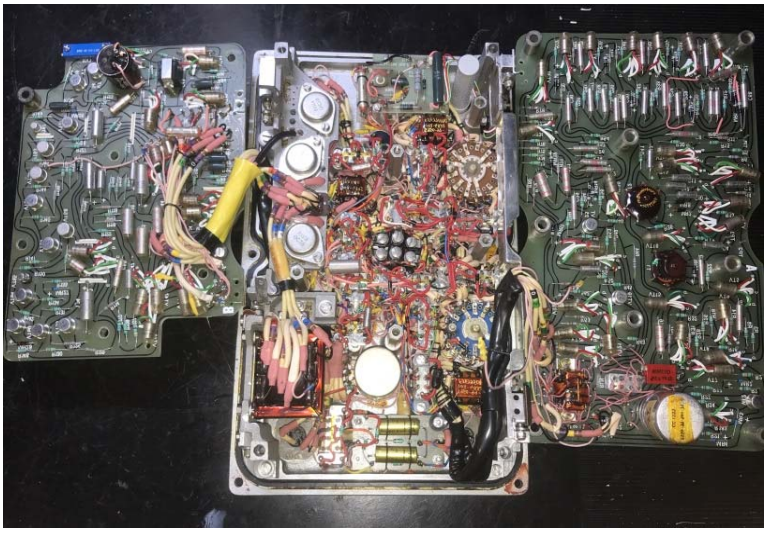

Figure 4. The DM box opened with the two main boards (‘A’ and ‘B’) opened out, the ‘A’ card on the right

A further greater complication arose though; the DM box was not the standard/original Larkspur unit for the BID150, but a modified Larkspur unit used with the later Clansman UK/VRC 353 VHF set - when used in conjunction with a Clansman DMU (Digital Master Unit) and the newer BID250 (LAMBERTON) encryption system, to enable remote working. In other words to (only) use the remote operation aspects of the DM box (together with the Larkspur remote box and handset – the RCDM box, coloured red).The DM box had then been re-named ‘Control Radio Set DM box (Clansman), NATO no. 580-99-643-8433. No other Larkspur original unmodified DM boxes appeared to be in current circulation, thus only ‘Clansman’ modified ones assumed to exist (interestingly, one of the author’s DM boxes undergoing testing showed date codes on some components as late as the 1978/1979, inferring the original Larkspur boxes were still manufactured into the late 1970’s).

To achieve this end (adaption for Clansman use) multiple modifications had been made to the original Larkspur box electronics and wiring, to both enable the RCDM box operation for Clansman use (SECURE and CLEAR plus CALL operation) **[5]**. But, more importantly – and concerning to the author - the disabling of many functions within the box, especially in the SECURE mode, including switching circuits (relays and wafer switches). **Figure 5** shows a close-up of the central area of the box – multiple yellow (heat shrink) pieces of sleeving can be seen - these are some of the obvious ‘Clansman’ modifications – where wires have been de-soldered, folded back and sleeved, then tucked under adjacent components or cable forms.

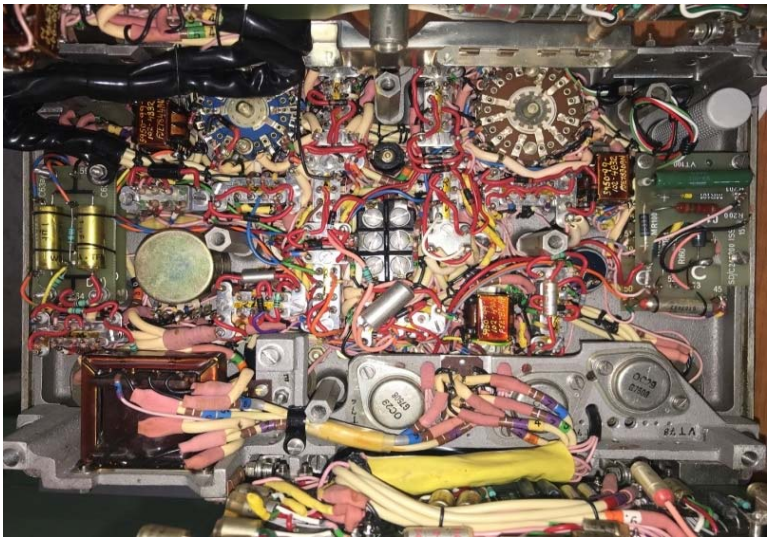

Figure 5. Close up view of the central chassis area

The main 12-way connector on the DM box that connected to the C42 (via the Goodman box) had been rewired as part of the modifications to enable the connection to the Clansman DMU instead. As the box was then essentially only the connection/electronic interfacing to the remote RCDM box, the rest of the front panel controls were not required and had, in the main been disabled internally as part of the modification process

and a special plastic cover had been fitted over the controls, only allowing access to the DMU connection and the remote RCDM connection. At this point the author decided to test the DM (Clansman) boxes with simulated DMU inputs and outputs, and connect to an RCDM/handset to check for correct operation (as the unit was designed later, to do with Clansman). **Figure 6** shows the author's unit connected as intended for Clansman operation. Function tests were carried out satisfactorily.

It was at this point that the author decided to go ahead and attempt a full reverse engineering on the unit, so as to produce circuit diagrams of the PCBs and the interconnections – relays, wafer switches, etc., such that if all went well then perhaps a ΔM audio signal could be obtained from the box (which would have fed to the BID150 connection) once an audio signal had been applied from the microphone input, and then the reverse – the de-modulation of the digital (ΔM) signal from the BID150, thus checking both the A/D and the de-modulation circuits of the DM box.

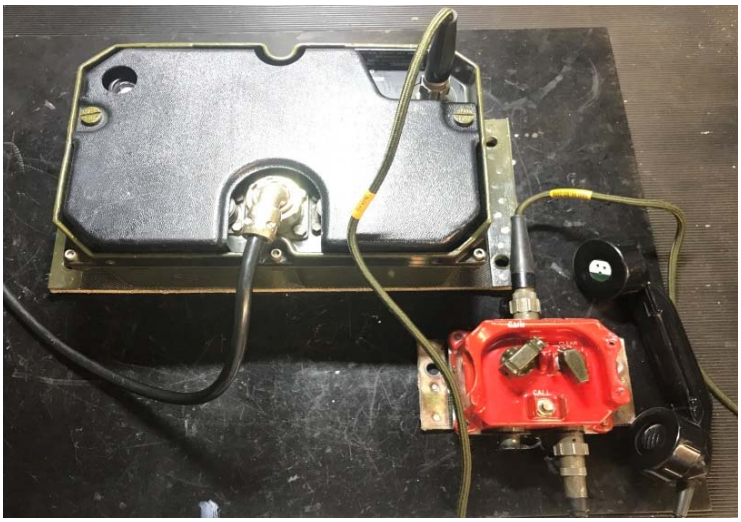

Figure 6. The working DM box (Clansman) together with the Larkspur red RCDM remote box and handset

As an initial help to reverse engineering, a part-circuit diagram of the smaller of the two main PCBs – the 'B' card was found in the Clansman Secure Speech Harness EMER (ELECTRICAL AND MECHANICAL ENGINEERING REGULATIONS) **[5]**. But certain components had been disconnected and functions of parts of the circuit changed. The EMER also gave technical details of the RCDM box as well as details of post-modification connections to the DM box relays and the 'B' PCB (but not how they were connected previously!), but none-the-less, it was a good starting point. The question was never answered as to why the DM box was extensively modified/altered, rather than a new unit produced – a smaller, simpler remote 'adapter' unit, especially as the modifications carried out would have been quite labour intensive the author believed, as well as the initial time/resources required to re-design the existing box to produce the Clansman version.

To start the reverse engineering, two DM boxes had been obtained. One unit was to remain complete, to eventually undergo 'de-modification', followed by powering up for testing/evaluation and then fitting to the author's current operational C42 system. The second unit was to be 'surgically' taken apart to enable tracing of the 'A' card circuit, and then tracing all of the interconnections to the rest of the equipment. The individual appropriate items of this DM box could be bench tested separately, especially the 'A' card - the card of main interest, which was 'reported' to house the A/D converter/de-modulator, etc.

Then, if full circuits and interconnections could be obtained, the task would be to decide what the modifications were, and how the unit should have previously worked in its Larkspur and BID150 days. Bearing in mind of course there was no information at all on them, other than very basic details in various user handbooks (U/Hs) of the C42 and C45 'Secure Terminal and Secure Rebroadcast Station' setting up drills, and Goodman equipment installations **[1]**, **[2]**, **[4]**, plus other installation details, e.g. the FV432 tracked armoured personnel carrier **[9]**. The actual descriptions of the operation and testing the BID150 and associated equipment in the radio set U/Hs were vague and it was no doubt intentional to help maintain confidentiality/security.

Reverse-Engineering/Circuit Tracing

A quick count up of the individual main components gave:

Transistors:	63 off NPN/PNP, power and signal, Ge and Si.
Transformers:	8 off ('signal frequency/PCM' type)
Relays:	11 off 2-pole c/o
Wafer Switches:	1 off 'SA' (4 way 9-pole dual wafer), 1 off 'SB' (4 way 10-pole dual wafer)
Multipole Connectors:	8 off

Miscellaneous switches, potentiometers, fuses, etc.
Multiple cable forms
Total number of (wire) joint/connections: approx. 500

A spare 'A' card from an unserviceable DM box was utilised for the circuit trace of this board. A first draft was produced within a day or so, and took up five sheets of A4 taped together. This trace involved literally putting down onto paper exactly what was traced from the board without any particular need or attempt for arranging in logical format at this time (except for the obvious areas of identifying 0V lines/tracks, etc.). From the author's previous circuit tracing experience, this was found to be nearly always the quickest way to start the tracing. See **Figure 7** for the first 'A' card draft circuit trace underway.

Then a cross-check was carried out to ensure all components had been accounted for on the circuit – resistors, capacitors, transistors, etc., including all windings and connections of the transformers and relays.

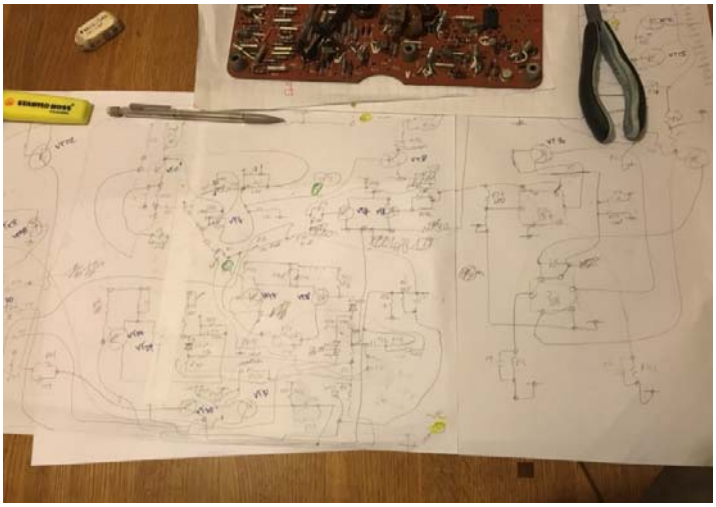

Figure 7. First draft circuit trace of the 'A' card underway

The next stage was to produce a second draft, which involved laying out the circuit in a more logical way, and looking for patterns and circuit areas which made sense such that at the end of the second draft a reasonably 'sensible' circuit was produced. This took up eight sheets of A4 joined together. Although 'patterns' and aspects of the circuit could now be followed logically, including an oscillator - which it was presumed at this point was the clock oscillator, albeit a rather complicated one it seemed for its function. Patterns could also be seen with the transistor circuits, e.g. feeding back on each other as suspected bistables, but the circuit still required another 'iteration'. So a third circuit (hopefully final) was drawn, issue 3, and taking up four sheets of A3. This provided the first working circuit later with the powered-up DM box.

Finally the author was ready to start the trace of the main DM box/chassis, including relays and switches, etc., and the multipole connectors on the front panel.

This part of the process took the longest time, and was spread over about a month. **Figure 8** shows part of the main chassis circuit trace underway.

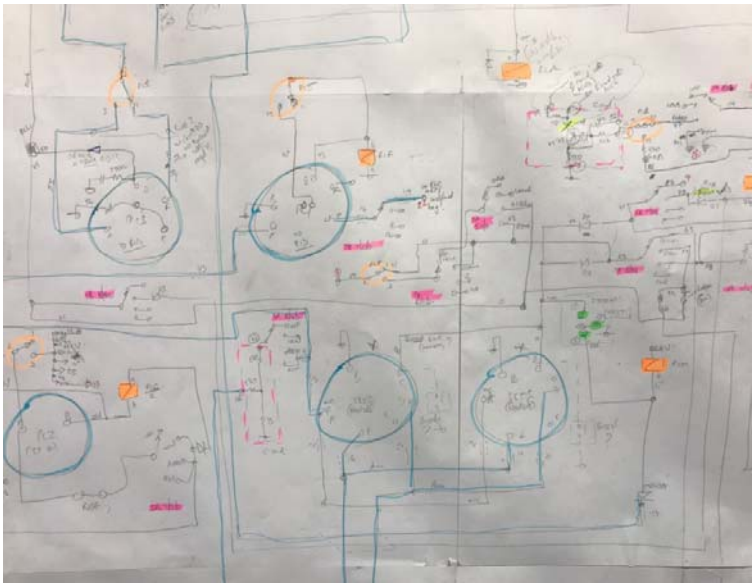

Figure 8. Part of the second draft of the chassis wiring (six sheets of A3 joined together)

Difficulty was found in tracing through connections to the various components. Although each internal original connecting wire had a unique number, which undoubtedly helped with the trace, sometimes these were found unterminated at ‘the other end’, and sleeved with one of the yellow Clansman modification sleeves, and usually hidden from view. **Figure 9** shows the DM box opened out, but also with the power transistor and transformer arrangement on the left of the chassis hinged out, for access. The chassis area components and wiring can be seen ‘disassembled’ – cable forms ‘opened up, front panel components removed, and the wafer switches with their shafts removed ready for inspection/access.

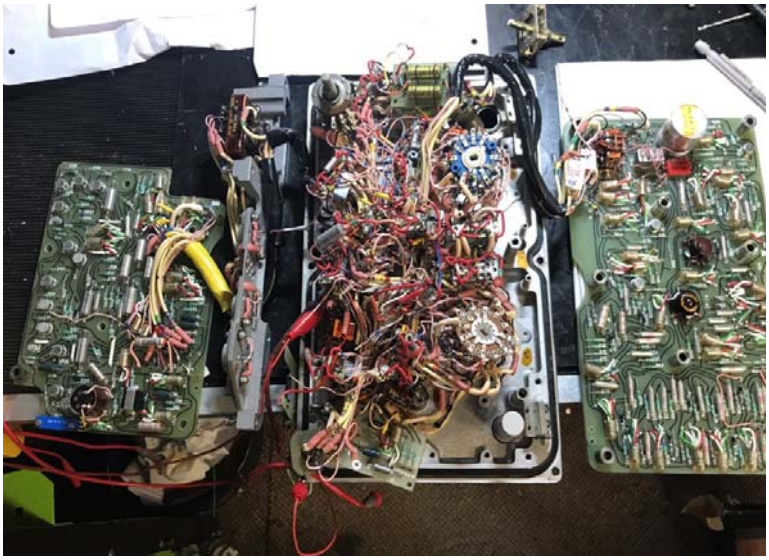

Figure 9. The DM box opened out together with the power transistor and transformer assembly hinged open, and the main chassis area in a state of ‘disassembly’

Gradually more and more chassis components were (carefully) removed – and de-soldered where necessary, to gain access to the cable forms underneath, e.g. cable forms running under relays, and of course the components were so tightly packed in that eventually all of the front panel components had to be removed, including the wafer switches disassembled to gain access to the switch contacts above and below each wafer section. **Figure 10** shows a close up of part of the components on the chassis. The lacing cord then had to be cut on the cable forms to enable wires to be traced through to their destination.

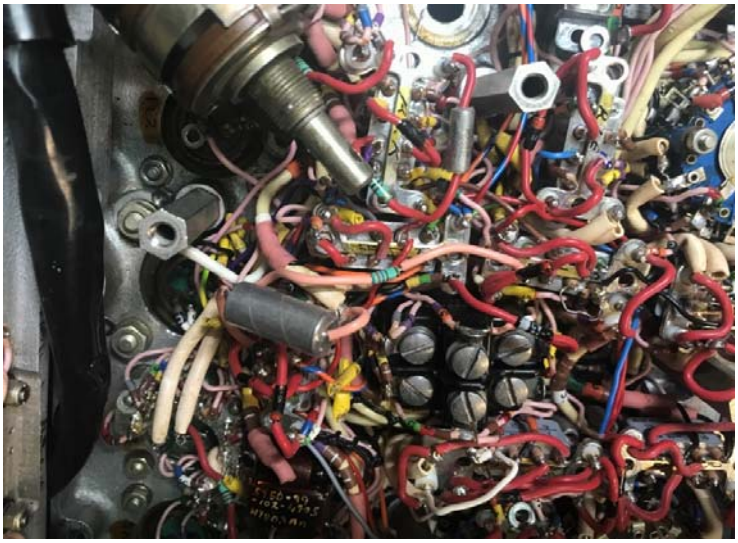

Figure 10. Part of the chassis wiring components once relays and other components were removed for access to cable forms below

During this phase, many wires would break off their soldered connections and so the second DM box was invaluable for comparison purposes to ascertain where the broken wires should then go back to.

All of this time of course, a system was required to record all 'obvious' modifications found (yellow sleeving), along with their positions, as ultimately the time would come when the author would need to 'step back' and view the whole system and attempt to decide how the unit should have worked before the modifications were made and various internal circuits and connections disconnected. For example, the main 12-pin Plessey connector to the set (C42) was virtually completed rewired for the Clansman modifications, including a new power supply feed (33 VDC) from the Clansman DMU and hence an extra internal regulator board fitted in the DM box.

Understanding the Design and De-Modifying

As well as the 'yellow sleeve' modifications (wires disconnected), many components had been added, including modifications made to the 'B' card circuitry. So at this stage, all the obvious additional components added for the Clansman modifications were carefully removed – they had already been identified on the author's latest issue chassis connection diagram.

A general layout to indicate where the chassis components were (supplied as part of the Clansman CSSM EMER) was used by the author to mark up and indicate where obvious modifications appeared, suitably numbered and identified such that notes could be made against them when some idea of their function was later discovered.

This was an ongoing process, as the author's thinking and reasoning changed over the weeks, that is, in trying to interpret the modifications and what the previous function would have been. Indeed, there are many pages of the author's notes – e.g. especially with the physical positioning of the relays and the 'yellow sleeve' modifications adjacent to them, and hence attempting to determine if the previously removed wires should actually connect to the relays in question. There were many variations and combinations that the (disconnected and removed) wires could have been used for because of the many (switched) functions of the box – e.g. SECURE/CLEAR operation (hence encrypted digital or analogue clear speech), LOCAL, REBROADCAST, REMOTE, INTERCOM and CALL functions, receive and transmit (*i.e.* pressel-operated) and hence the 'direction' change of the signal flows within the unit.

Likewise, with the relays themselves, although some of the relay functions were reasonably obvious from the overall chassis connection diagram traced/produced, several were not, as there had been so many changes - in fact there still remains within the final 'operational' DM box several original modifications, *i.e.* wires disconnected (and all those wires surround two specific relays) but unfortunately too many variations/permutations of how the relays should be connected to these wires and what their functions were, so this condition remains! In all, greater than around forty modifications were found, with virtually each one presenting the author with a problem – *i.e*. what was the reason for the modification, what did it do and why, what should it have done in the Larkspur (required) version and hence where to connect (or reconnect) to.

Eventually the overall DM box operation was better understood, together with the operation of the 'A' and 'B' boards, which allowed an 'A' card block diagram to be drawn (**Figure 11**) as different parts of the overall

circuit began to slot into place. The process of de-modifying continued, *i.e*. in the main connecting up the ‘yellow sleeve’ modifications, re-wiring the main 12-pin plug, re-wiring transformers and re-connecting components (transistors) removed on the ‘B’ card, all once the relevant modifications had been understood and hence where the re-connections should be made.

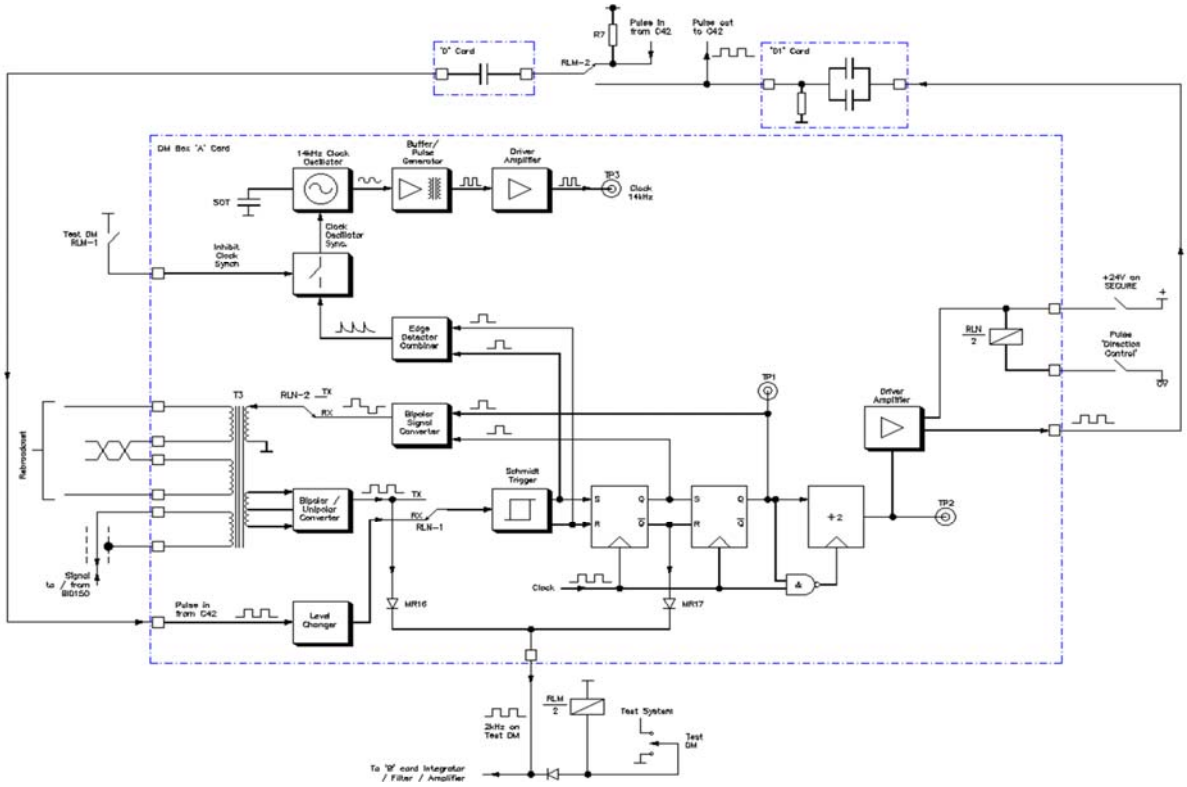

Figure 11. The ‘A’ card block diagram produced by the author

One of the (apparently simple) problems the author thought, for example was tracing out the microphone input from the (C42) set to the ‘reported’ A/D converter on the ‘A’ card. After much head scratching, it was decided/found that there is no A/D converter in the DM box – ‘A’ card or otherwise! The components on the ‘A’ card were found to be essentially digital ‘signal processing’ – from/to the set, and hence to/from the BID150 for the ‘pulse code’ signal.

The microphone signal on SECURE, *i.e*. for encryption (digital) as against non-encrypted (analogue) CLEAR is passed via the SECURE switch direct to one of the two BID150 connectors. Likewise there is a (disconnected) wire from the BID150 from this connector, which infers this is the audio (?) out. And so it would seem that as well as the analogue to digital conversion being within the BID150 unit, audio amplification/processing was also present in that unit.

Thus analysing further the ‘A’ card and the signal flows from the C42 and the BID150 – both digital and the phones/mic, a good understanding was then made of the DM box operation in relation to these signals. At this stage a final iteration of the ‘A’ card circuit was made - now issue 4, and a ‘respectable’/workable and understandable version (A2 size) was produced.

The digital/pulse inputs from the C42 on receive and then out to the C42 on transmit were located, *i.e.* traced through from where they should connect on the 12-pin connector from the C42 and reconnected to the appropriate ‘A’ card terminals. They are both capacitor-coupled signals and both the screened connecting cables had both been previously removed and the yellow sleeves fitted.

The ‘A’ card houses a tuned-collector (metal-cased toroidal transformer) 14 kHz sine-wave oscillator/pulse generator (**see Figure 12**) followed by two transformer/driver stages which produce the internal clock, 3 µS pulses at 14 kHz. An external select on test (SOT) capacitor is fitted adjacent to the transformer can (33 pF in the author’s operational unit) to set 14 kHz.

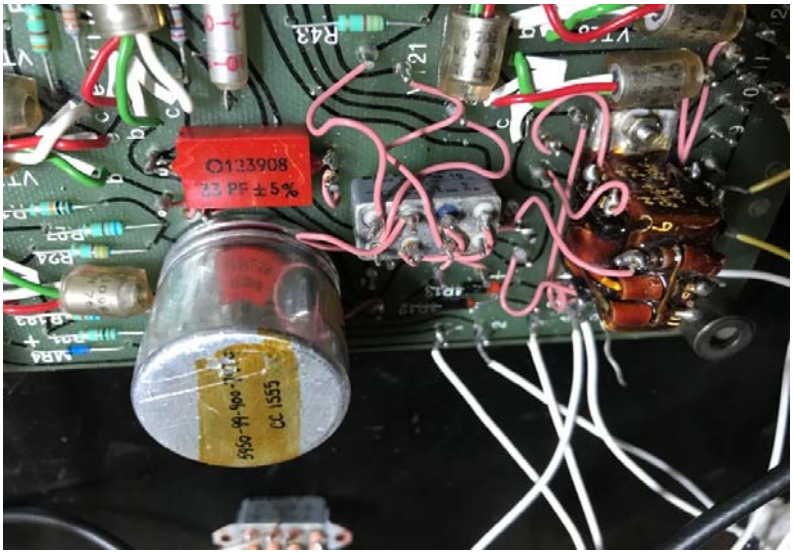

Figure 12. Close up view of the clock oscillator transformer can - together with SOT capacitor, and the main signal/data transformer T3

Input/output (that is, receive/transmit) digital processing is located on the 'A' card. This consists of input signal processing/Schmitt trigger (from the C42 on receive) - which provides pulses (one every half cycle) to synchronise with the clock oscillator via the combining circuit.

The C42 signal from the Schmitt trigger also feeds two clocked bistables configured as a 2-stage shift register, driving a bipolar signal converter which provides a type of 'bipolar RZ' (return to zero) digital signal for passing to the BID150 via the 'A' card transformer T3 on receive. Two out of phase signals are fed to the converter from the shift register such that, when both are a logic '1' there will be a +Ve output pulse, when both are '0' there will be a –Ve output pulse and when both signals are different there will be 'zero' out. See **Figure 18** for waveforms of this operation

Referring to **Figure 16** waveforms, The shift register output at TP1 will 'mirror' the input signal, and is applied to the final flip flop where, on transmit it will form a gating input with the clock pulse thus producing a 7 kHz output but gated by the action of TP1. The 7 kHz square wave on TP2 (and hence the pulse output connection) is also present on SECURE with no input signal present (TP1), thus the final flip flop acts as a divide by two circuit in these circumstances, clocked by the 14 kHz.

Thus the maximum frequency out from the DM box to the pulse modulation input of the C42 is 7 kHz. It is assumed by the author that the maximum pulse frequency into the DM box from the BID150 is somewhat less than 14 kHz corresponding with it is believed with a 14 kHz clock signal/sampling rate within the BID150 using ΔM. This is the clock frequency the author used in his ΔM test generator.

Anecdotal comments would indeed suggest this is the BID150 clock frequency, and also that the 'sound quality is poor', which would perhaps confirm that the BID150 used a relatively low clock/sampling rate for the ΔM modulator. Checking the C42 modulating frequencies on receive, the EMER specification calls for an audio response (+1.0 dB to -1.5 dB) – following the limiter and discriminator at the cathode follower - from 50 Hz to 10 kHz with an external square wave modulating input. This would then appear to align with the DM box circuit's maximum 7 kHz frequency out to the C42 for transmission.

Note the Signal Engineering Instruction, dated 1984 **[7]** states; *The delta modulation for military use has a bit rate of 16 kbits/sec although for improved quality this can be increased to 32 kbits/sec; whereas for a PCM channel the present standard calls for a bit rate of 64 kbits/sec. It can be seen therefore that the bit rate, and consequently bandwidth for a delta modulated channel makes it more acceptable for military use.*

Note on transmit (the digital/encrypted signal coming from the BID150) the signal will be coupled via transformer T3 to the bipolar to unipolar converter (the bipolar converter will be isolated on transmit by relay contact RLN-2) before taking the same route as the signal above on receive – via the Schmitt trigger and shift register, but on transmit out to the C42 pulse input connection via the output driver amplifier on the 'A' card. This provides a pulse signal of 20 V pk-pk referenced to 0V from the common-emitter output stage. The frequency deviation from the C42 is limited to ±15 kHz by clipping diodes within the C42 modulator unit.

It has to be assumed that the 'bipolar RZ' signal is the type of signal the BID150 was designed for, in other words the modulation (ΔM) and de-modulation are all carried out within the BID150, including any audio amplification and audio processing ('companding'?) required. The signal is clearly of a bipolar RZ nature from

the BID150 when it is on transmit into the DM box, as the first circuit the signal encounters upon entering the box is the bipolar/unipolar converter, as can be seen from the block diagram. Likewise the signal into the BID150 is clearly a bipolar RZ type - from the bipolar converter and out via the transformer T3.

It was reasoned by the author that the development of the BID150 possibly proceeded in isolation, *i.e*. without at the time a particular radio set selected in which to interface with and so presumably once the C42/C45 (these sets were in service from 1955) was selected, an interface box (DM) became a requirement, along with a modified version on the 'standard' C42 producing the C42 No.3 which had provision for pulse code type modulation, and likewise for the C45 No. 3

A confusing part initially (for the author) of the DM box operation was the use of an 'integrator/filter' on the 'B' card (re-used for the 'IB Call' function from the Clansman DMU). This function was initially reasoned that perhaps it could have been a ∆M de-modulator – *i.e.* a 'conventional' basic ∆M type. However, it was since established by the author that this was the 'filter' for the TEST DM function on the DM box.

When the TEST DM front panel switch is operated, the 7 kHz on the driver amplifier output (when switched to SECURE and the pressel not operated) is fed back into the 'A' card pulse input. A digital pulse signal will then appear on the on-card transformer T3 driving the bipolar/unipolar converter (which is normally used on transmit) but an output is taken in this test position from this circuit via MR16 and combined with an output from the shift register and fed to the output pin via MR17.

This output was disconnected as part of the Clansman modifications but the author concluded this resulting (2 kHz) signal almost certainly should be fed to the audio amplifier on the 'B' card via the 'integrator/filter' circuit such that the operator can hear the 2 kHz test tone as per the user handbooks. Note the '-3db' points of the filter are 1.3 kHz lower and 2.5 kHz upper, therefore a bandpass filter – see **Figure 20** - so clearly not meant for normal audio/speech (or ∆M de-modulation). Measuring the series L and C components, the resonance was then calculated as 1.9 kHz.

As can be seen from the block diagram **Figure 11**, appropriate signals are taken both from the shift register (common to both transmit and receive signal paths) as well as the bipolar to unipolar signal converter stage. For the signal to arrive at the output of this stage it would have first been converted by the bipolar converter stage, and fed back to the unipolar converter input via the transformer T3. The clock would naturally have to have been functional and so it can be seen that virtually the whole of the 'A' card (plus other parts of the DM box) would have been tested by this one operation - by the operator with a front panel switch.

Note the TEST SYSTEM function switch though is not particularly a function that can be tested/useful without the BID150. When operating the switch the 'pressel' circuits are operated putting the set into transmit, but also the BID150, and as the U/H **[2]** states for the operators to listen on the phones; *this sounds like 'mush' but a good operator should, with practice, be able to readily distinguish pulse noise from random 'mush'* – the 'mush' presumably being the pulse modulation out from the BID150.

Additional windings on the 'A' card transformer ('rebroadcast') connect into relay RLA c/o contacts on the main chassis, and when the DM box is switched to REBRO (rebroadcast) the (digital encrypted) signal is sent (or received) via the REM socket - via the ubiquitous (4-core) 'tinsel tail' connection. Note when an audio signal is present (when the RCDM box is used locally through a handset – using the same connections) then the audio is routed to a separate audio transformer within the DM box for processing/transmission.

Other 'B' card modifications previously made were the i) disconnection of the transistor oscillator that provided the SECURE 'pips' – 1 kHz 'pips' every 2 seconds, and ii) the change of the SIGNAL SENSITIVITY/SIGNAL lamp circuits to provide the secure/clear relay drive, for the CLANSMAN DMU 'SEC A' signal. Both circuits were de-modified back to their original function.

‘A’ Card Testing

When finally powering up, it was very useful (essential?) to use a 4-channel digital storage scope for checking. The author, thinking initially before the reverse engineering was completed that there was indeed a ΔM /de-modulator on the ‘A’ card/within the box, a simple ΔM circuit was constructed. This would then feed an appropriate signal into the DM box (receive) terminal, and hence the waveforms could be followed through from this input signal, and on an appropriate point on the PCB take the ΔM signal and demodulate it externally to end up with the ‘original’ audio signal.

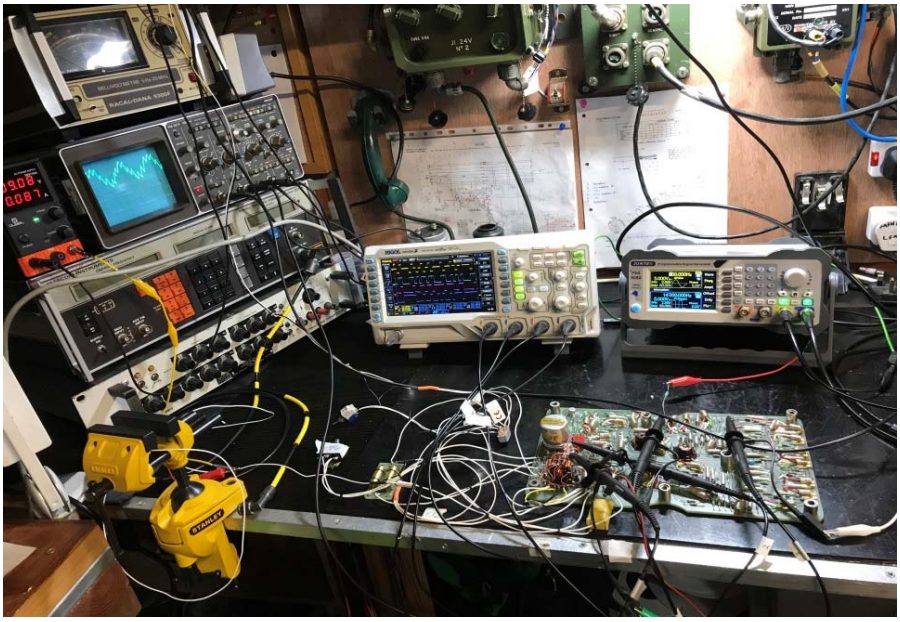

Figure 13 ‘A’ card testing underway

However it was found that there was indeed no A/D converter or delta modulator on the ‘A’ card nor within the DM box, so instead the ΔM test generator constructed was used as a very convenient pulse generator to simulate the output from the C42 and into the DM box ‘A’ card – varying the audio frequency (and digital switching clock) input into the author’s ΔM generator would then produce an output pulse signal of varying widths and position, hence frequency, for various integrator CR time constants of the ΔM generator, which was to prove useful in the testing and understanding of the ‘A’ card circuit.

14 kHz was used as the clock frequency on this external test ΔM (with 500 Hz audio sine wave input) and it was clearly seen that the DM box clock oscillator becomes locked/synchronised to the external ΔM signal, maintaining lock for around +/- 250 Hz on the ΔM clock frequency. **Figure 14** shows the waveforms from the ΔM test circuit with the output applied to the ‘A’ card input (*i.e.* simulating a pulse output from the C42).

Note that the 14 kHz ‘A’ card clock oscillator would also become locked on to the ΔM generator clock if 7 kHz was used as the ΔM generator clock frequency - although the locking frequency range was around half, and then with some difficulty the oscillator would lock onto a 3.5 kHz ΔM generator clock frequency. It should be noted that the ‘A’ card clock oscillator is free running, and it is therefore assumed that 14 kHz is the required ΔM clock frequency required (*i.e*. used/required within the BID150), both from a frequency locking range point of view and being a suitably high enough frequency for the encoding of the audio speech frequency range required, plus of course it was the same frequency as the ‘A’ card clock oscillator.

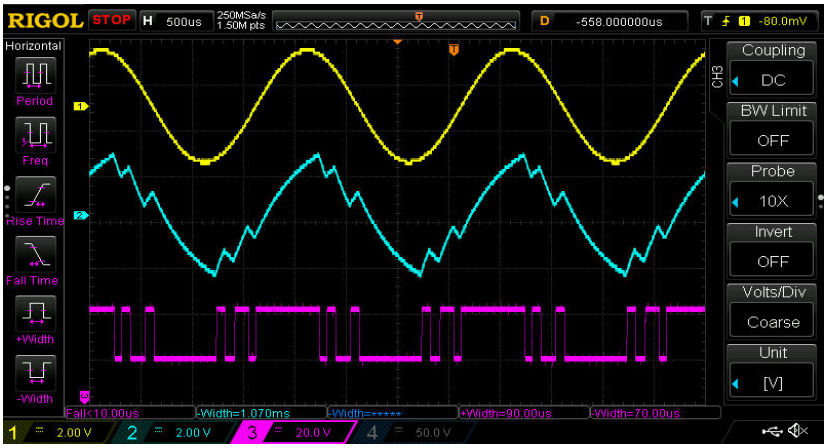

Figure 14. Delta modulation test generator waveforms

CH1: Audio in 500 Hz

CH2: ΔM 'CR' integrator

CH3: 'A' card pulse I/P (ΔM output)

Referring to **Figure 14**, the integrator waveform (channel 2, blue) is showing signs of 'slope overload' caused by the integrator (CR type) time constant being too long for the given audio frequency signal and clock rate, but this is deliberate (and academic) here purely to allow for a more 'bunched' set of pulses (in the non-overload portion) in the ΔM output signal to the DM box 'A' card input, for testing purposes.

Referring again to the block diagram **Figure 11**, with the ΔM test signal applied to the 'A' card input, and the signal to the BID150 (and 'A' card) set to receive, the bipolar RZ output signal can be seen at the on-card transformer T3 which feeds the BID150. The transformer accepts both inputs and outputs from/to the 'A' card to/from the BID150 as the signal path is set to transmit or receive depending upon the transmit/receive relay c/o contacts. Thus the (common) signal to/from the 'A' card is from the same winding on the transformer to the BID150. Depending upon whether the unit is set to transmit or receive, the 'A' card relay will direct signals to/from its transformer via either the drive circuit outputs (bipolar converter) on receive, or inputs to the separate processing circuits (bipolar/unipolar converter) on transmit.

Figure 15. The 'bipolar RZ' waveform from transformer T3 that feeds the BID150 - channel 4, with the 'A' card switched to receive

CH1: ΔM 'CR' integrator

CH2: 'A' card pulse input (ΔM output)

CH3: 'A' card clock pulse TP3

CH4: 'A' card output to BID150 appearing on RLN-2/RX

It should be noted that the width of the bipolar RZ pulses (**Figure 15**) are the width of the clock pulse repetition, hence the full cycle will be half the clock frequency – therefore the pulses will be at a frequency of 7 kHz.

The received input signal at transformer T3 is fed via the level changer and the Schmitt trigger to the shift register, the input signal then appearing on TP1. This is applied to the bipolar converter together with a second input from the shift register - as shown in **Figure 18** below for the bipolar converter waveforms.

With no input signal and hence no signal on TP1, a 7 kHz square wave will be present on TP2, (see **Figure 16**) also used as part of the TEST DM function.

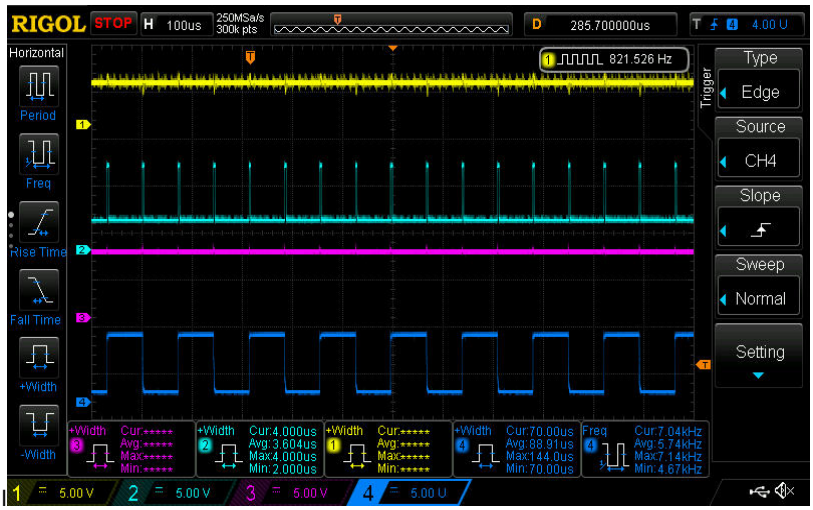

Figure 16. 'A' card switched to receive, with no signal input. TP2 (channel 4) showing the 'standing' 7 kHz square wave output with no signal in hence no signal on TP1

CH1: 'A' card input signal

CH2: Clock pulse TP3

CH3: TP1 signal

CH4: TP2 7 kHz square wave

When the TEST DM front panel switch is operated and the DM switched to SECURE, the square wave on the driver amplifier output is fed back into the 'A' card pulse input, via relay RLM-2. The output is taken from the junction of MR16/MR17 - channel 4, as **Figure 17**.

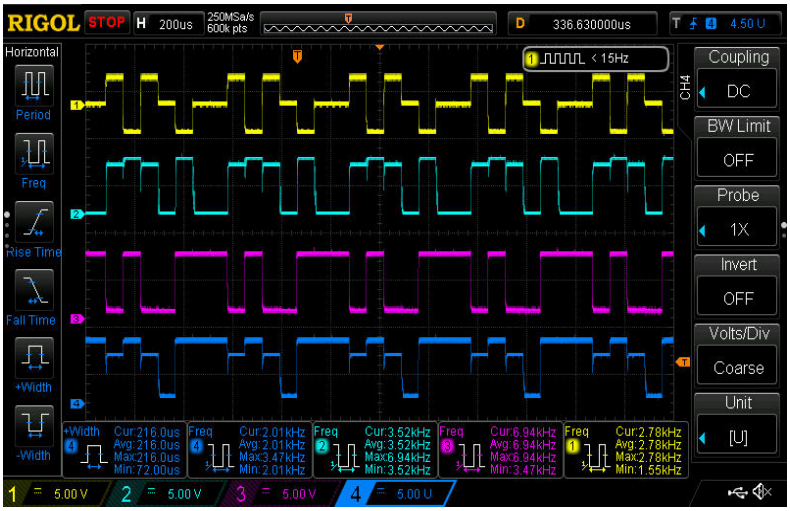

Figure 17. The TEST DM circuit waveforms (on SECURE receive)

CH1: ‘A’ card output to BID150 via T3

CH2: ‘A’ card output from MR16 anode - simulating the BID150 signal coming into T3 on transmit

CH3: MR17 anode

CH4: ‘A’ card TEST DM output (2 kHz out to ‘B’ card/audio amp.)

Regarding the waveforms in **Figure 17,** channel 1 shows the signal at the output of the bipolar signal converter, which is fed to the BID150 via T3. But it is also induced into the winding feeding the bipolar/unipolar converter, and it is this circuit that would be used on transmit. This is shown on channel 2. This is a convenient way of checking for the correct operation of the unipolar converter. When on receive, the relay contact RLN-1 blocks this path – the signal can only pass through to the Schmitt trigger and beyond when the receive/transmit relay RLN is set to transmit, so an output is therefore taken to the TEST DM output before the relay, hence from MR16.

Channel 3 shows a shift register output signal, which is combined with channel 2 to produce the TEST DM output at channel 4. Note though with channel 2 that parts of the signal – when at a logic ‘1’ are ‘joined’ and some are ‘discreet’ pulses (although the clock pulses are not shown on this picture, the pulses in channel 1 change at the clock repetition rate). This is caused by the action of the bipolar/unipolar converter circuit – when there is a single pulse deviation from ‘zero’ on channel one in either direction, there will be a single pulse on channel 2. However, when channel 1 pulse changes one polarity to the other at the next clock pulse, then the pulses on channel 2 will be shown ‘as one’ (the formation of the bipolar RZ pulses can be seen in **Figure 18** – the bipolar signal converter).

Looking again at channel 4, **Figure 17**, the unipolar signal derived from channel 1 is combined with channel 3 (an output from the shift register first stage) via the diodes MR16 and MR17, such that there is only a (-Ve going) pulse when channels 2 and 3 are both 0V. Each of the ‘smaller’ pulse widths is 71.4 µS (corresponding to a frequency of 14 kHz). The resultant output that appears on channel 4 is thus an output that occurs every 7^{th} pulse, equating to 2 kHz.

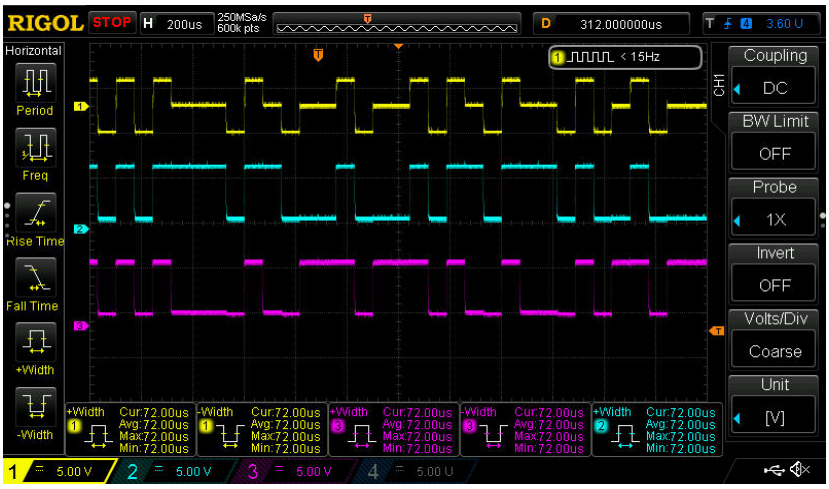

Figure 18. Waveforms of the bipolar converter

CH1: ‘A’ card output to BID150 via T3/bipolar converter output

CH2: Bipolar signal converter input 1

CH3: Bipolar signal converter input 2

It will be seen in **Figure 18,** the two input signals to the bipolar converter are combined, such that when both are a logic ‘1’ there will be a +Ve output pulse on channel 1, when both are ‘0’ there will be a –Ve output pulse and when both signals are different there will be ’zero’ out on channel 1.

Figure 19 shows the relationship between the input signal to the ‘A’ card (TP1) on channel 3, the bipolar RZ signal fed out to the BID150 on channel 1, the bipolar/unipolar converter signal simulated BID150 output on channel 2, and the output TP2 with the ‘gated’ 7 kHz on channel 4. The time base of the waveforms is such (500µs) so as to show more clearly ‘at a glance’ the relative signal relationships. Now that the time base is set to 500 µS, it can be seen that TP2 consists of the gated 7 kHz pulses, derived from the 14 kHz clock. Thus when TP1 is a logic ‘1’ there will be 7 kHz output pulses, but inhibited when TP1 is a logic ‘0’.

It will also be noted, although with some difficulty on this waveform due to the time base, that TP2 will change at the negative-going transition of TP1 when corresponding with the clock pulse, other than when TP1 is already at a logic '1' when 7 kHz pulses will be 'allowed through'. Note the signal at TP2 will/can only pass to the C42 on transmit when the +24 VDC is applied to the driver/amplifier on SECURE, and the pulse 'direction control' is set to 0V from the BID150, *i.e.* enabling relay RLN, to set the receive/transmit paths on the 'A' card.

As stated earlier, also of note here is that the output frequency of the DM box can never be higher than 7 kHz due to the clock frequency and subsequent action of the shift register, and the final output flip-flop. As can be seen from the channel 4 data on **Figure 19**, the average output frequency with this particular input signal case – and hence audio frequency and sampling rate - is '5.71 kHz'.

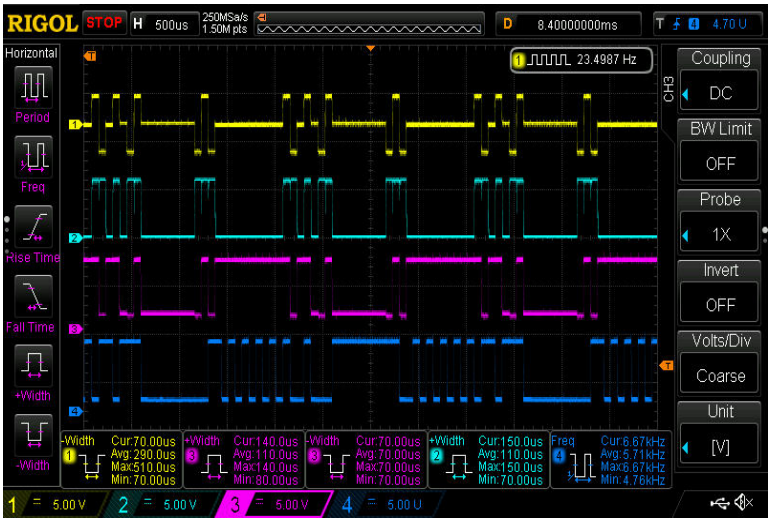

Figure 19. The input/output signal flow within the 'A' card on receive

CH1: 'A' card output to BID150 via T3/bipolar converter output on relay RLN-2

CH2: 'A' card input (on bipolar/unipolar converter output on RLN-1/TX) - simulating the BID150 signal coming into T3 on transmit.

CH3: TP1 ('mirrors' the input signal from the C42)

CH4: TP2 – 'A' card output to C42, prior to the final driver/amplifier.

Other DM Box Tests

‘B’ Card ‘BID Pips’ Generator

Once the 1 kHz oscillator was reconnected (the transistor collectors had been de-soldered as part of the Clansman modifications) the ‘pips’ were tested satisfactorily, *i.e*. 1 kHz ‘pips’ every 2 seconds, and fed to the headphones via the on-card amplifier.

‘Integrator/Filter’

Figure 20. The bandpass filter, centred on 1.9 kHz (passband ± 600 Hz) as used on the TEST DM function

‘B’ Card SIGNAL SENSITIVITY/SIGNAL Lamp Driver Circuit

The Clansman modification was removed from the input to the card (from the DMU) and re-connected to the 12-pin connector for the C42 limiter grid current signal, which operated the SIGNAL lamp (and internal relays), with sensitivity/operating point set by the front panel SIGNAL SENSITIVITY control.

This signal is fed from the C42 via the external Goodman box. When this box is switched to SECURE the limiter grid current is supplied to the DM box, until/if an ‘interfering signal’ is received by the C42. The C42 will then apply a 0V signal to the Goodman box (via the C42 RRB line from the squelch circuit when an interfering signal is detected) which operates a relay/open-circuits the limiter grid current to the DM box and switches the DM box SIGNAL lamp circuits off.

This method is used to detect an incoming ‘interfering’ signal (actually for this purpose a ‘conventional FM voice analogue transmission) – which could re-trigger a rebroadcast net (*i.e.* cause the ‘other’ set to go to transmit) – required because the C42 squelch circuit will not properly operate with a digital (‘normal’ on SECURE) received signal.

The circuit was tested satisfactorily, in conjunction with the Goodman box and C42. The adjustment appeared not to be of a ‘precise’ type - the U/H states (for rebroadcast, therefore two sets) in the setting up procedure: *Both squelch controls must be correctly adjusted to allow the clear signal cut out on the Goodman boxes to operate. Final adjustments must be made on receipt of a SECURE incoming signal on both sets. If the squelch light is permanently lit when a secure signal is being received, the squelch control is to be turned slightly further anti-clockwise.*

It would appear that in practice when the units were in service that this function required care in setting up, *i.e.* reaching a ‘POB’ (point of balance) with the light just off, and as the user handbook states: *Fine adjustment of the SENSITIVITY control is vital in attaining the greatest working range of the equipment.*

‘B’ Card Power Supply

The 24 VDC DM box external input is fed via PL2 (LT IN) via a fuse and series reverse polarity protection diode to a 2-pole power relay. When the relay operates, 24 VDC will be applied to the rest of the DM box as well as to the BID150 (via SKTH).

The 24 VDC is also fed directly to various parts of the ‘B’ PCB – namely the audio amplifier and relay circuits, and also provides a regulated +9 VDC for the ‘BID pips’ oscillators, and the ‘A’ card , plus there is regulated

+18 VDC supplied to the ‘B’ card signal sensitivity switching circuits. All were tested as satisfactory. Note as mentioned previously, the Clansman 33 VDC input circuit board was removed, and discarded.

‘B’ Card Audio Amplifier

This amplifier was tested in use for the ‘BID pips’ and TEST DM on SECURE, but also, previously along with the input and output transformers T6 and T7 and associated power transistors - prior to the DM box de-modification when tested with the RCDM box in its ‘Clansman’ role (see **Figure 6**).

Headphone Operation

The headphone operation, that is, operation in both earpieces when on CLEAR, and separate earpieces depending upon mode – SECURE/LOCAL and SIGNAL SENSITIVITY setting – tested generally in accordance with the U/H ‘Confidence Testing and Fault Finding’ section.

Interestingly – according to the U/H, the headset was used in practice checking the REM socket (remote or rebroadcast) when initially setting up/testing the system. The 6-way headset plug would be plugged into the REM socket – only 4 terminals used where the SECURE ‘BID pips’ would be received in one earpiece (checking the audio out in SECURE mode) but ‘pulse noise’ would be heard in the microphone insert when the system was set to SECURE/rebroadcast and transmitting (pressel operated), *i.e.* the pulse signal from the BID150 via the ‘A’ card transformer T3 and out to the ‘next DM’ box REM connection. Note the signal sensitivity light would need to be set to ‘on’ first for this test.

Conclusions

The extensive modifications that were required (and indeed possible) to ‘modify’ back from the DM (Clansman) box to the DM (Larkspur) box were carried out and the DM box tested as far as possible within a complete (radio) system and using the appropriate circuits and drawings produced.

These included circuit and connection diagrams, ‘A’ card block diagram and circuit, modification listings and multiple waveforms showing the detailed ‘A’ card operation. The unit was then ‘boxed up’ and connected into the author’s C42 No. 3 (with Power Supply Unit Transistorised No. 1), Goodman box and ATU No.6 (with dummy load) setup – see **Figure 21** below. ‘Normal’ operation was then achieved in conjunction with the DM box set to CLEAR, *i.e.* operation from the mic/headphone assembly on the DM box – on both set and intercom, with gain control. Operation of the SIGNAL SENSITIVITY/SIGNAL function was observed in SECURE mode, in conjunction with an external RF signal generator feeding into the C42 providing an ‘interfering’ signal via the Goodman box.

‘BID pips’ were also tested on SECURE mode once the Clansman modification was removed. The TEST DM function on SECURE was a useful tool in checking for correct operation/faulty finding when necessary.

The author achieved his first aim of making the DM box operational in the CLEAR mode, effectively simulating the ‘speech’ actions of the Larkspur ‘J1’ harness box. The second aim was also achieved, of analysing the digital signal section (the ‘A’ card) of the DM box with respect to the signals that the BID150 required, therefore being reasonably confident of the signals necessary to/from the BID150, although of course it was found during the reverse engineering process that the ΔM section was to actually be within the BID150 itself.

The results and tests/observations obtained during this project are those of the author’s with a view to giving some insight into the signals required during secure speech encryption using the DM box/C42 No. 3 VHF set, together with the BID150. No BID150 technical documentation has ever been seen (nor is it likely to be) but it is hoped that the information contained here has at least proved of interest to anyone interested in the army’s first combat net radio secure speech system.

Figure 21. The final completed ‘operational’ system setup including the Goodman box on the top left

Acknowledgements

1 Alan Belton, G8LIT, for supplying a DM box.
2 Alan Knell, G0BNE, for supplying a DM box.
3 Nick Blackwell, for converting the author's 'scribblings' of the 'A card to a CAD drawing.
4 The REME Museum, Lyneham (Archivists) for their huge help in searching for possible DM box information.
5 Royal Signal Museum, Blandford for kind permission for the use of their BID150 photo.
6 https://groups.io/g/wireless-set-no19
7 www.royalsignals.org.uk

References

1 User Handbook for Station Radio C42/C45 No. 3. Secure Rebroadcast Station. Army Code; 60936.
(https://groups.io/g/wireless-set-no19, www.royalsignals.org.uk file reference: 1633).
2 User Handbook for Station Radio C42/C45 No. 3. Secure Terminal Station. Army Code 60938
(https://groups.io/g/wireless-set-no19, www.royalsignals.org.uk file reference: 1634).
3 User Handbook for VHF Applique Unit. Army code 60884
(https://groups.io/g/wireless-set-no19, www.royalsignals.org.uk file reference: 1631).
4 VHF Applique Unit (Larkspur) EMER TELECOMMUNICATIONS L690/L692
(https://groups.io/g/wireless-set-no19, www.royalsignals.org.uk file reference: 1367).
5 Clansman Secure Speech Harness EMER TELECOMMUNICATIONS L820/L822.
6 User Handbook for Wireless Control Harness Type 'B', W.O. Code 11195
(https://groups.io/g/wireless-set-no19, www.royalsignals.org.uk file reference: 691).
7 Signal Engineering Instruction, General DG03, Army code 14400.
8 Station Radio C42 No. 3 EMER TELECOMMUNICATIONS H432 Part 1, Technical Handbook – Technical Description
(https://groups.io/g/wireless-set-no19, www.royalsignals.org.uk file reference: 1316).
9 User Handbook for BID/150 Installations in Armoured Personnel Carrier FV432. Army code 13745.
10 User Handbook for BID150 Basic Installations in FFR 'B' Vehicles. Army code 13963.
11 Technical Folder TF/TELS/5/78. Installation of UK/VRC 353, UK/VRC 321 and C42D with BID/150 in FV432 (Larkspur Harness).
12 Intersil Delta Modulation Application Note AN607.1, January 1997.
13 Report of the Bloody Sunday Inquiry, 2010, Volume IX, Army and Police Communications.
14 Signal Processing, Modulation and Noise, UNIBOOKS, J.A. Betts, ISBN 0 340 09895 3
15 Royal Corps of Signals. 'Roger So Far…' 2020. The History Press Ltd, ISBN 0750990503.
16 'The Bruin Communications System', Alister J Mitchell, 2012, ISBN/EAN: 978-90-819271-7-8
17 User Handbook for Radio Access Unit, Army code 61045.