Operational considerations for 9003B Digital Scramblers

The use of the 9003B Digital Scrambler on the HF communication medium requires specific operating practices to ensure reliable performance. To improve reliability of your system when using the 9003B, please take note of the following:

- When more than two 9003B units are actively used in a network e.g. 3 or 4-party conversations, then either

    - wait for lock to drop out before pressing PTT and talking (indicated by **LOCK** LED on 9003B extinguishing), or

    - wait for 2.5 seconds after pressing PTT before talking

- Use Codan transceivers with linear audio stages. This requires 'talk power' enhancements in current production transceivers to be disabled.

The remainder of this note explains how the 9003B scrambler operates and hence the importance of the prerequisites mentioned above.

Operation of the 9003B Digital Scrambler

The 9003B is a time domain scrambler in which the voice frequency signal is digitised and divided into 512 ms time frames. These are divided into a number of time segments. The time segments are sampled in a complex sequence determined by the encrypting algorithm. Each frame, having the time segments of the input digital signal now rearranged in coded order, is reconverted to analog form for transmission. This process necessarily introduces a time delay in the speech path.

APPLICATION

The scrambler uses a disjointed frame sliding window technique. This reduces the transit time of the signal through the system and hence the time between conversations.

In order for restitution of the original signal at the receiving point, the decrypting algorithm must be a replica of that used for encryption. This requires the decryption algorithm to be generated from the same key as that used for transmission and also entails time synchronisation with the encryption process.

Time delay

In a 2–party network comprising of stations A and B, when PTT is pressed at station A, transmission of synchronising pulses commences, however there is no coded message output from station A for about 450 ms. This delay is due to the signal being clocked sufficiently far through the 512 ms shift register so that a segment is selected by the sliding window for output. On initiating transmission at station A, station B is not aware that station A has started to speak until the voice is heard, although the **LOCK** LED at station B would illuminate, indicating that communication is underway.

By the time that station B hears the last of the message from station A, station A has already been waiting for 600–700 ms after release of the PTT button. Station B now responds in the same manner as described for station A, with the same time delays. Consequently, station A waits in the order of 1 second after releasing the PTT button before the reply from station B is heard.

Synchronisation

Synchronisation is required to maintain the decryption process in step with encryption. There are three ways in which this might be accomplished:

- There may be a synchronising handshake (continuing until each station has confirmed synchronisation) prior to each message session. After this, the clocks at both stations keep time well enough to allow a number of messages to be passed.

- A single synchronisation signal sent at the beginning of each transmission may be used.

- Synchronising signals may be sent during each message either as a continuous transmission, or, as is done in the 9003B, at sufficiently frequent intervals.

If synchronisation occurs only at the beginning of the message, late entry of a third party is denied as this station will not receive a synchronising signal until commencement of the next complete transmission. Further, if synchronisation is not achieved, station B too will miss the whole of that transmission.

To avoid the above, the 9003B repeats the synchronisation during the course of each transmission. This signal consists of a burst of a 1 kHz tone transmitted about every 0.5 s. Of course, there is a trade–off between the length of the tone burst necessary for signalling over a noisy path and the degradation of audio quality due to the time. Audio is suppressed whilst sending and recognising the synchronisation signal. As the synchronisation signal is repetitive, third parties are allowed late entry to the transmission.

Initially, the time at which a synchronisation pulse is received is unknown. After synchronisation, the time position of the synchronisation signal is known and recognition of synchronisation can be limited to a short time window such that it will not be disturbed by 1 kHz components in the encrypted speech. However, this narrow recognition window will not allow for fast synchronisation acquisition, if at all, since the incoming signal may never coincide with the window. It is necessary, therefore, that whenever the PTT button is released (or after five successive synchronisation pulses are missed) the search window in the receiver is opened to facilitate synchronisation recognition. This ensures that after each transmission from station A to station B or from station B to station A, the window is open ready for reception of the other station. The timing of the synchronisation pulse will bear no relationship to that of the previous transmission.

When a third party, station C, is listening to station A at the same time as station B, the clock in each receiving station is synchronised to station A and the synchronisation recognition windows close to the narrow state. When station B responds to station A, station C is still expecting synchronisation at the instants in time established by station A and the clock continues to idle for a further five periods (about 2.5 s). If, within this period, station B commences to transmit, station C will not decrypt the message as the synchronisation signals from station B will not be recognised at station C. After the time set aside for lost synchronisation pulses has elapsed, station C will resynchronise on the next synchronisation pulse (or later if the path is noisy) but with the effect that the beginning of station B's transmission is lost.

If both sides of the conversation between station A and station B are to be heard by station C, then each of the stations A and B must wait for 2.5 s after operating their PTT buttons before starting to speak or alternatively, wait until the **LOCK** LED has extinguished before pressing the PTT to commence transmission. This ensures that sufficient time has elapsed for the synchronisation detector sampling window to open to the wide state.

Talk power

The talk power facility within Codan transceivers must be disabled when being operated with a 9003B scrambler.