FEDERAL STANDARD

TELECOMMUNICATIONS: INTEROPERABILITY REQUIREMENTS FOR ENCRYPTED, DIGITIZED VOICE UTILIZED WITH 25 KHZ CHANNEL FM RADIOS OPERATING ABOVE 30 MHZ

This standard is issued by the General Services Administra tion pursuant to the Federal Property and Administrative Services Act of 1949, as amended.

1. SCOPE

1.1 Description. This standard establishes interoperability requirements regarding the analog to digital conversion, encryption (with related synchroniza tion), and modulation of encrypted voice associated with Frequency Modulation (FM) radio systems employing 25 kHz channels and operating above 30 MHz. In this standard, voice is digitized using 12 kbit/s Continuously Variable Slope Delta -modulation (CVSD) and then encrypted using a National Security Agency (NSA) Commercial COMSEC Endorsement Program (CCEP) Type I encryption algorithm.

1.2 Purpose. This standard is to facilitate interoperability between telecommunication facilities and systems of the Federa l Government.

1.3 Application. This standard shall be used by all Federal Departments and agencies in the design and procurement of digitized voice Type I encryption equipment for use with nominal 25 kHz channel FM radio systems that operate above 30 MHz and digitize voice at greater than 4.a kbits/s and less than 16 kbits/s. All such equipment must be capable of digitizing voice using 12 kbit/s Continuously Variable Slope Delta -modulation (CVSD).

Note: This standard applies only to Type I (i.e., protection of classified information) systems and does not restrict the use of other systems, such as Data Encryption Standard (DES) encryption or analog and quasi -analog scrambling systems.

2. REFERENCED DOCUMENTS

a. NSA Specification 86-33, INDICTOR Interface Control Document (FOUO)

b. NSA Specification 86-32, WINDSTER Interface Control Document (FOUO)

c. Communications Security Equipment System Document 14, TSEC/KY -57/58 (CQNFIDENTIAL)

Note: All references to the above document assume the KY -57/58 has been modified to operate at 12 kbits/s (i.e., 75 percent normal clock rate).

The above three documents are published by the National Security Agency (NSA), Fort Meade MD 20755, and can be made available to Government departments and agencies and to manufacturers participating in the NSA Commercial COMSEC Endorsement Program (CCEP).

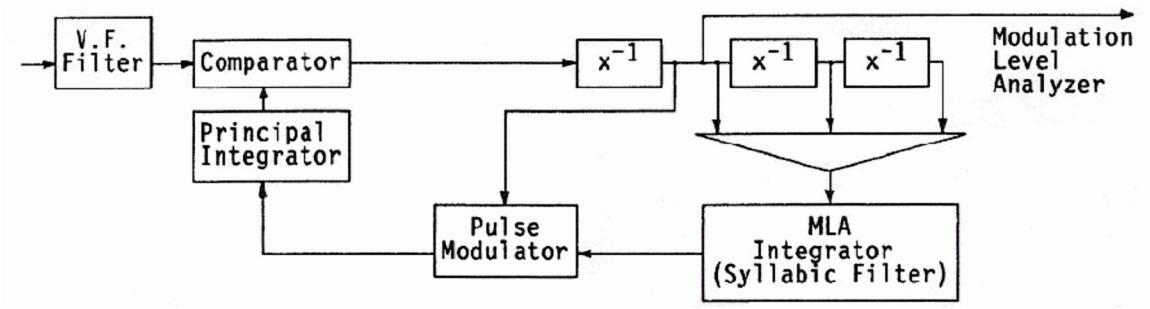
3. REQUIREMENTS

3.1 Overview. This standard describes interoperability-related requirements for the conversion of analog voice to digital form (section 3.2), its encryption and related synchronization (section 3.3), and subsequent *frequency* modulation (section 3.4).

3.2 Analog to Digital Conversion

3.2.1 Digital Rate: Voice shall be converted, using Continuously Variable Slope Delta -modulation (CVSD), to a 12,000 bit s/s ±.018 percent digital stream.

3.2.2 Block Diagram and General Description. The following diagram is a typical representation of the CVSD analog -to-digital conversion process.



In the typical CVSD representation above, the incoming analog voice signal is passed through a Voice Frequency (V.F.) Filter and then compared, by a Comparator, with the output of the Principal Integrator. The previous bit output of this Comparator is used: (1) as the digital output of the CVSD encoder, (2) to determine the po larity of the pulse generated by the Pulse Modulator, and (3) as input of the Modulation Level Analyzer. The Modulation Level Analyzer (MLA) provides indication to the MLA Integrator whenever the last and previous two bits from the Comparator are either al l ONEs or all ZEROs. (This is referred to as run-of-three coincidence coding). The MLA Integrator determines the step size, which is variable and based upon the MLA output, and provides this pulse FED - amplitude information to the Pulse Modulator. The Pulse Modulator provides pulses to the Principal Integrator as the Principal Integrator attempts to follow the shape of the input voice waveform.

3.2.3 V.F. Filter. The V.F. Filter should have an attenuation at 6 kHz and higher frequencies relati ve to frequencies between 300 and 3,000 Hz of at least 20 dB. It is recommended that the filter be essentially flat (i.e., ~3 dB) between 300 and 3,000 Hz.

3.2.4 Comparator. The binary digital output of the Comparator shall be either ONE or ZERO, depending upon whether the amplitude of the input voice signal is greater than or less than the output of the Principal Integrator.

3.2.5 Modulation Level Analyzer. The Modulation Level Analyzer (MLA) shall charge the MLA Integrator whenever the last and two immediately preceding bits from the Comparator are either all ONEs or all ZEROs (i.e., there is run -of-three coincidence).

3.2.6 MLA Integrator. The MLA Integrator (often called Syllabic Filter) provides pulse amplitude information to the Pulse Modulator. The change in pulse amplitude from one bit time to the next (i.e., quantizing step size) should vary, in a linear manner, from a run -of-three coincidence rate of 0 percent to a rate of 50 percent by a voltage ratio of approximately 10 to 1 (i.e., 20 dB). The time constant of the MLA Integrator shall be 6~2 ms.

3.2.7 Pulse Modulator. The pulse modulator shall create pulses using amplitude information from the MLA Integrator and polarity information from the Comparator.

3.2.8 Principal Integrator. The Principa l Integrator shall have a time constant of 1+.25 ms.

3.3 Encryption

3.3.1 Encryption Algorithm. Encryption of the digitized voice shall be accomplished with the encryption algorithm used in the INDICTOR and WINDSTER COMSEC Modules (see references a and b) using the cryptographic mode that has cryptographic compatibility with the KY-57/58. (Other compatible implementations may be substituted.)

3.3.2 Encryption Operating Mode. The encryption process shall use the cryptographic operating mode of the INDfCTOR and WINDSTER COMSEC Modules designated for compatibility with the KY -57/58. (Other compatible implementations may be substituted.)

3.3.3 Cryptographic Synchronization

3.3.3.1 Synchronization Check Bits. Transmitting radios shall predictably force synch ronization check bits in the unencrypted digitized voice, prior to encryption, as is done by the KY-57/58 (see reference a (section 5.3, paragraph 2) and reference c). Receiving radios shall utilize these predictable synchronization check bits to determine whether cryptographic synchronization has been lost (see reference a, section 5.3.3, paragraph 3).

3.3.3.2 Alternating ONE/ZERO Pattern. Continuously Variable Slope Delta-modulation (CVSD) should inherently produce an alternating binary ONE/ZERO pattern during the idle condition (i.e., pauses in speech). In order to promote rapid initial synchronization and resynchronization, transmitting radios shall ensure that a segment of alternating ONE/ZERO pattern at least 95 percent the length of the segment produ ced by the KY -57/58 (see reference c) is produced in the unencrypted bit stream, prior to encryption, at least once every two seconds. All receiving radios shall be capable of initial synchronization and subsequent resynchronization (after detecting absenc e of synchronization check bits) utilizing segments of alternating ONE/ZERO pattern in the decrypted bit stream.

3.3.4 End-of-Message Sequence. Radios shall transmit the same encrypted End -of-Message sequence used by the KY -57/58, with a duration between 60 and 120 percent of that transmitted by the KY-57/58, at the end of each half-duplex transmission, followed by 160+10 ms of unencrypted alternating ONE/ZERO pattern, to mark the end of a transmission. (Note: this -is to assist encryption equipment and re peaters in distinguishing between a fade condition and an actual end of transmission.)

3.3.5 Additional Non-voice Sequences. Radios may employ additional, unspecified, non-voice sequences at the start of transmissions (e.g. KY-57/58 initial synchronization). However, use of these additional sequences shall not impair interoperation with radios not utilizing such additional sequences.

3.4 Modulation Deviation and Coding. Transmitter deviation shall be ~4 kHz (~10 percent) from the carrier frequency. Receiving radios shall operate satisfactorily regardless of whether transmitted binary ONEs (or ZEROs) were coded as positive or negative 4 kHz shifts in carrier frequency.

3.5 Spectrum Standards. Applicable spectrum standards for Federal Government radio communication systems are given in Chapter 5 of the National Telecommunications and Information Administration's (NTIA) "Manual of Regulations and Procedures for Radio Frequency Management", 47 Code of Federal Regulations Part 300.

4. EFFECTIVE DATE. The use of this standard by U.S. Government departments and agencies is mandatory effective 270 days following the date of this standard.

5. CHANGES. When a Government department or agency considers that this standard does not provide for its essential needs, a statement citing specific requirements shall be sent in duplicate to the General Services Administration (K), Washington, DC 20405, in accordance with the provisions of Federal Information Resources Management Regulation 41 CFR 201 -13.103. The General Servi ces Administration will determine the appropriate action to be taken and will notify the agency.

PREPARING ACTIVITY:
National Communications System
Office of Technology and Standards
Washington, DC 20305-2010

MILITARY INTEREST:
Military Coordinating Act ivity
DCA C

Custodians
Army -- SC
Navy -- EC
Navy -- EC
Air Force 90

Review Activities
Army -- SC, CR
Navy -- EC, MC
Air Force -- 02, 17
NSA n NS
JTC3A -- JT

U.S. GOVERNMENT PRINTING OFFICE: *1990-0-704.QOO/00023*