NOT
MEASUREMENT
SENSITIVE

MIL-STD-187-721
18 FEBRUARY 1993

MILITARY STANDARD

PLANNING AND GUIDANCE STANDARD FOR AUTOMATED CONTROL APPLIQUE FOR HF RADIO

AMSC N/A

AREA TCSS

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

FOREWORD

1. This military standard is approved for use by all Departments and Agencies of the Department of Defense.

2. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document should be addressed to: HQ U.S. Army Information Systems Engineering Command: ATTN: ASQB-OSE-TT, Fort Huachuca, Arizona 85613-5300, by using the self-addressed Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

3. Interoperability of DoD telecommunications systems, and of DoD with non-DoD telecommunications systems, has been and will continue to be a major consideration in the development and adoption of standards for military use.

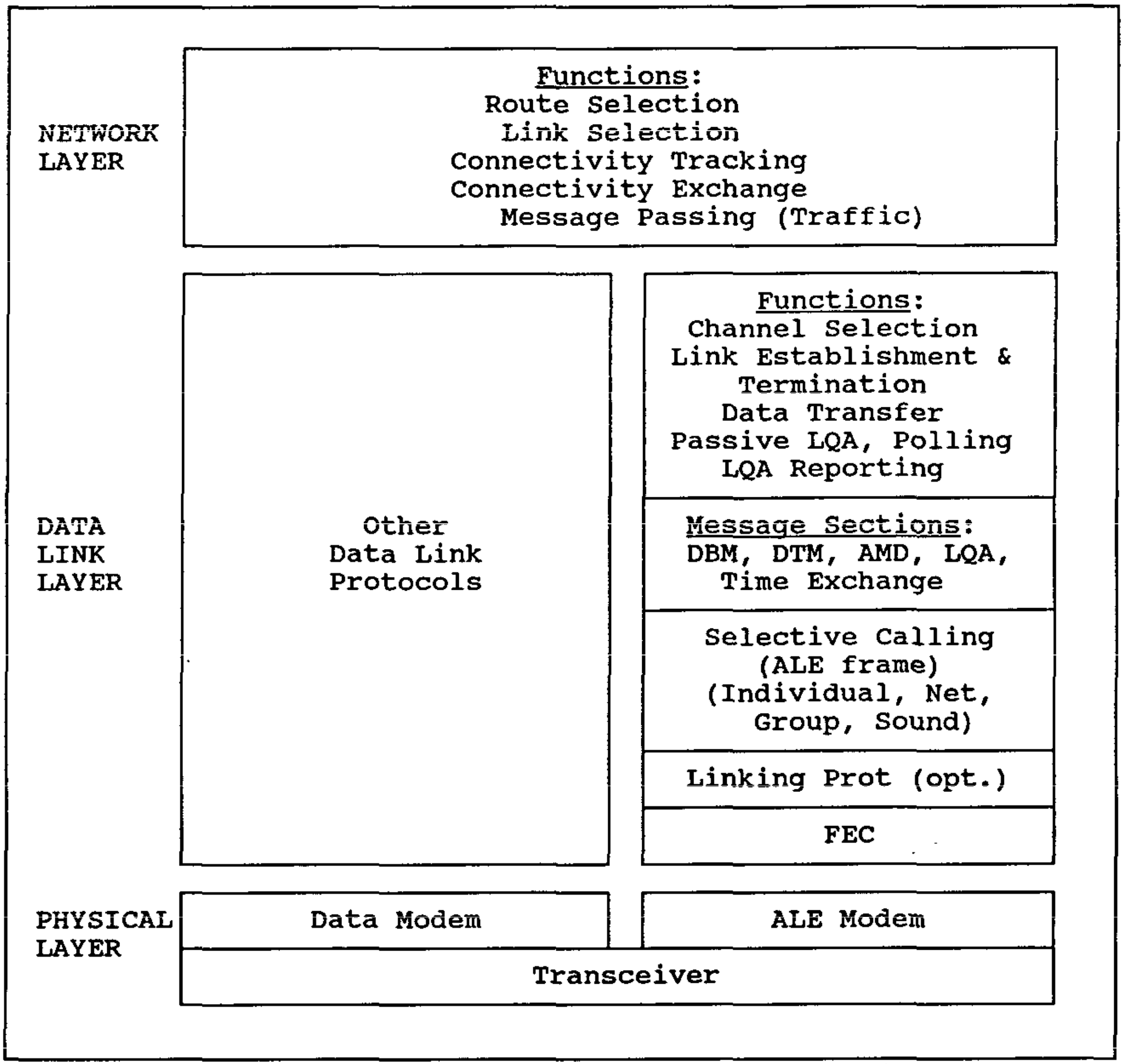
a. Military standards in the 188 series (MIL-STD-188-XXX) document telecommunications design parameters that are based on empirical data, and must be used in all new or major upgrades of inter- and intra-DoD systems and equipment to ensure interoperability.

b. Military standards in the 187 series (MIL-STD-187-XXX) document evolving telecommunications design parameters and concepts that are subject to change and that have not been adequately proven through the use of empirical test data. MIL-STD-187-XXX standards should be used as planning standards and guides until parameters are proven and included in approved federal, allied, MIL-STD-188-XXX, or DoD adopted commercial standards.

4. MIL-STD-187-XXX standards provide uniform guidance for the design of the evolving and future Defense Information System. Providing this guidance at the concept engineering stage will help to minimize ineffective designs and costly interoperability problems at later stages of implementation, as well as to assure utilization of appropriate advances in technology. Planning standards are developed considering present and future plans for the Defense Information System, commercial systems (both national and international), and NATO and other allied military systems.

5. The treatment of automatic link establishment (ALE) in MIL-STD-188-141 provides the technical foundation upon which this document rests. The second generation ALE system was one of the adaptive high frequency (HF) radio features developed through a MITRE effort in 1986. The remainder of the original concept is being documented in MIL-STD-187-721. Therefore, a brief summary of the basic principles of this ALE system is provided.

6. The principal functions included in an automated HF station are shown schematically in the figure on page iii. This diagram is structured along the lines of the ISO Open Systems Interconnection Reference Model, with functions at each layer supporting higher layers and using lower layers.



Functional hierarchy of automated HF station.

7. MIL-STD-188-141 specifies a basic HF radio, along with a set of robust physical and data link layer functions for ALE. The ALE modem employs 8-ary frequency shift keying (FSK) with 8 millisecond (ms) tones; the 3-bit symbols are sent at a rate of

125 per second, giving a raw data rate of 375 bits per second (bps). Forward error correction (FEC) coding is applied to the 24-bit ALE words used at the data link layer; a (24,12) Golay code is applied to each (12-bit) half of the 24-bit ALE word, producing two 24-bit results. These two 24-bit Golay words are then interleaved bit by bit, and a stuff bit is appended to produce a 49-bit word to be transmitted. Finally, each 49-bit word is sent three times, which allows the receiver to correct some errors using 2 of 3 majority voting.

8. At the receiver, received bits from the modem are (conceptually) shifted into a 99-bit register. Majority voting among the outputs of this shift register yields a 48-bit "majority word" (stuff bits are discarded), which is de-interleaved to produce two 24-bit Golay words. These are delivered to the Golay decoder, which attempts to recover a 24-bit ALE word.

9. Because no bits in the ALE word are spent on synchronization, the acquisition of word sync in this system employs a series of tests on the prospective word after each received symbol (tri-bit) is shifted in. First, the number of unanimous votes in the majority vote decoder must exceed a threshold. Next, the Golay decoder must successfully decode both halves of the 48-bit word. Finally, the resulting 24-bit ALE word must be acceptable to the ALE protocol module. Once word sync has been achieved, it is automatically tracked for the remainder of the transmission using these same tests.

10. The MIL-STD-188-141 data link layer comprises several sublayers. The lowest sublayer is concerned with error detection and correction (FEC sublayer). Above this is an optional protection sublayer (linking protection), which protects layers above it from unwanted interference. The ALE protocol is divided into three sublayers in the figure on page iii: the lowest manages the exchange of ALE frames among stations that are specified using a standardized addressing structure; the next deals with orderwire and other message sections embedded within ALE frames; the highest contains the data link layer functions apparent to users, such as channel selection, link establishment, and orderwire communications.

11. The contents of this document provide the technical parameters for the functions and features of advanced adaptive HF radio, and provide logical and cohesive guidelines for both industry and the Government.

CONTENTS

CONTENTS

PARAGRAPH PAGE

CONTENTS

FIGURE PAGE

TABLE

THIS PAGE INTENTIONALLY LEFT BLANK

1. SCOPE

1.1 Scope. The purpose of this document is to describe the technical parameters for adaptive high frequency (HF) radio that are more advanced than that described in MIL-STD-188-141, Interoperability and Performance Standards for Medium and High Frequency Radio Equipment. This document is structured segmentally, with each segment being added as it is developed. Together, these segments will guide the planning of military adaptive HF radio network technology into the 21st century. The outline of MIL-STD-187-721 used in this document includes areas anticipated to be covered in other segments. These areas are referenced in this document as "not yet standardized."

1.2 Applicability. This standard is approved for use within the Department of Defense (DoD) in the design and development of new (adaptive) HF radio equipment. MIL-STD-187-721 contains theoretical designs and solutions that may have been supported by desk top analysis and modeling, but contains technology that has not been imbedded into hardware/software or undergone proof of concept testing.

1.3 Application guidance. MIL-STD-187-721 is a planning standard, organized in segments to allow the various functions and features of adaptive radio to be documented separately to encourage technical development. This document contains information on adaptive HF radio beyond that which is contained in MIL-STD-188-141. MIL-STD-188-141 contains only technical documentation that is supported by empirical data; whereas this standard documents the advanced techniques, providing a greater level of technology, but not yet supported by test data. Either a DoD user or an industry manufacturer may develop hardware or software implementations of technical parameters described in a MIL-STD-187-721 document. A manufacturer may wish to implement the technical parameters described in this document in order to be first in a market offering, thereby, gaining market and advertising advantage. Also, a DoD user organization may have a requirement for technical features described in this document and include MIL-STD-187-721 in an acquisition contract, thereby, causing the development of the equipment or software as a part of the contractor's effort. Whether a manufacturer implements a MIL-STD-187-721 function using "venture capital" or a Government agency "sponsors" the development through inclusion in a contract, the result is the same; testable hardware/software and empirical data. This empirical data allows the MIL-STD-187-721 segment (wholly or in part) to migrate into a MIL-STD-188 series document. This process provides a logical and orderly progression while assuring a level playing field for Government and industry alike.

2. APPLICABLE DOCUMENTS

2.1 Government documents.

2.1.1 Specifications, standards, and handbooks. The following specifications, standards, and handbooks form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the issue of the Department of Defense Index of Specifications and Standards (DODISS) and supplement thereto, cited in the solicitation.

STANDARDS

FEDERAL

FED-STD-1037	- Glossary of Telecommunications Terms

MILITARY

MIL-STD-188-141	- Interoperability and Performance Standards for Medium and High Frequency Radio Equipment.

(Unless otherwise indicated, copies of federal and military specifications, standards, and handbooks are available from the Naval Publications and Forms Center, ATTN: NPODS, 5801 Tabor Avenue, Philadelphia, PA 19120-5099.)

2.1.2 Other Government documents, drawings, and publications. The following other Government documents, drawings, and publications form a part of this document to the extent specified herein. Unless otherwise specified, the issues are those cited in the solicitation.

USAISEC Technical Report No. ASBQ-OSI-S-TR-92-04	- A 24-Bit Encryption Algorithm for Linking Protection (Johnson Algorithm)

2.2 Non-Government publications. None.

2.3 Order of precedence. In the event of a conflict between the text of this document and the references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

3. DEFINITIONS

3.1 Terms. Definitions of terms used in this document are in accordance with (IAW) the current edition of FED-STD-1037. In addition, the following definitions are applicable for the purposes of this standard.

a. Application level 0 (AL-0) - In adaptive radio, the unprotected application level of linking protection.

b. Application level 1 (AL-1) - In adaptive radio, the unclassified, least protected application level of linking protection.

c. Application level 2 (AL-2) - In adaptive radio, the unclassified, enhanced application level of linking protection.

d. Application level 3 (AL-3) - In adaptive radio, the unclassified but sensitive application level of linking protection.

e. Application level 4 (AL-4) - In adaptive radio, the classified application level of linking protection.

f. Linking protection (LP) - In adaptive radio, a technique that protects the linking functions from unintentional or malicious interference by scrambling the ALE signaling exchanged among protected stations for cryptographic authentication of HF ALE signaling.

g. Protection interval (PI) - In linking protection, transmissions are encrypted using time-varying randomization data. The period between changes in the time of day portion of this randomization data is termed a protection interval.

3.2 Abbreviations and acronyms. The abbreviations and acronyms used in this document are provided below. Those listed in the current edition of FED-STD-1037 have been included for the convenience of the reader.

a. AL-O - unprotected application level.

b. AL-1 - unclassified application level.

c. AL-2 - unclassified enhanced application level.

d. AL-3 - unclassified but sensitive application level.

e.	AL-4	-	classified application level.
f.	ALE	-	automatic link establishment.
g.	ASCII	-	American Standard Code for Information Interchange.
h.	bps	-	bits per second.
i.	CMD	-	ALE preamble word COMMAND.
j.	CRC	-	cyclic redundancy check.
l.	DBM	-	data block message.
m.	DO	-	design objective.
n.	DoD	-	Department of Defense.
o.	DODISS	-	Department of Defense Index of Specifications and Standards.
p.	DTM	-	data text message.
q.	FEC	-	forward error correction.
r.	FSK	-	frequency shift keying.
s.	GPS	-	Global Positioning System.
t.	HF	-	high frequency.
u.	IAW	-	in accordance with.
v.	ICD	-	interface control document.
w.	ISO	-	International Organization for Standardization.
x.	LP	-	linking protection.
y.	LPCM	-	linking protection control module.
z.	LQA	-	link quality analysis.
aa.	ms	-	millisecond.
ab.	NPODS	-	Naval Print on Demand System.
ac.	NSA	-	National Security Agency.

ad. OSI - open systems interconnection.

ae. PI - protection interval.

af. ppm - parts per million.

ag. REP - ALE preamble word REPEAT.

ah. TOD - time of day

ai. UTC - coordinated universal time.

aj. USAISEC - U.S. Army Information Systems Engineering Command.

3.3 Timing symbols.

a. T_{lc} - leading call phase.

b. T_{rs} - redundant sound phase.

c. T_{sc} - scanning call phase.

4. GENERAL REQUIREMENTS

4.1 Data link sublayers. The MIL-STD-188-141 data link layer contains three sublayers: a lower sublayer concerned with error correction and detection (forward error correction [FEC] sublayer), an upper sublayer containing the automatic link establishment (ALE) protocol (ALE sublayer), and an optional protection sublayer in between, as shown in figure 1. Within the FEC sublayer are redundancy and majority voting, interleaving, and Golay coding applied to the 24-bit ALE words which constitute the (FEC sublayer) service-data-unit, in terms of the International Organization for Standardization (ISO) model. The ALE sublayer specifies protocols for link establishment, data communication, and rudimentary link quality analysis (LQA) based on the capability of exchanging ALE words. Linking protection (LP) is placed in the intermediate "protection" sublayer so that it may make full use of the error correcting power of the FEC sublayer while intercepting unauthorized attempts to communicate with the local ALE protocol entity to establish links or otherwise disrupt operations.

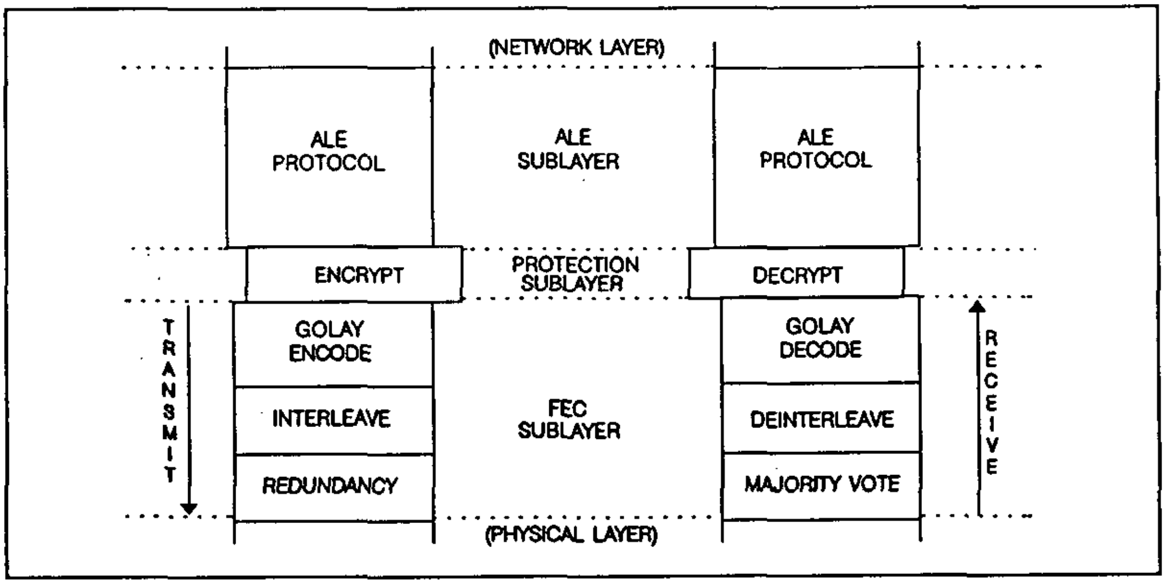


FIGURE 1. Conceptual model of data link layer protocols in MIL-STD-188-141.

4.2 Linking protection.

a. LP is intended to prevent the establishment of unauthorized links, and does this through an authentication process. (Some cryptographic protection is provided to the ALE words by the LP mechanism, but this is not the primary purpose of LP.)

b. Block diagrams of the data flow through unprotected and protected radios are shown in figures 2a and 2b. The blocks in the figures represent logical operations only, and do not necessarily represent distinct hardware modules.

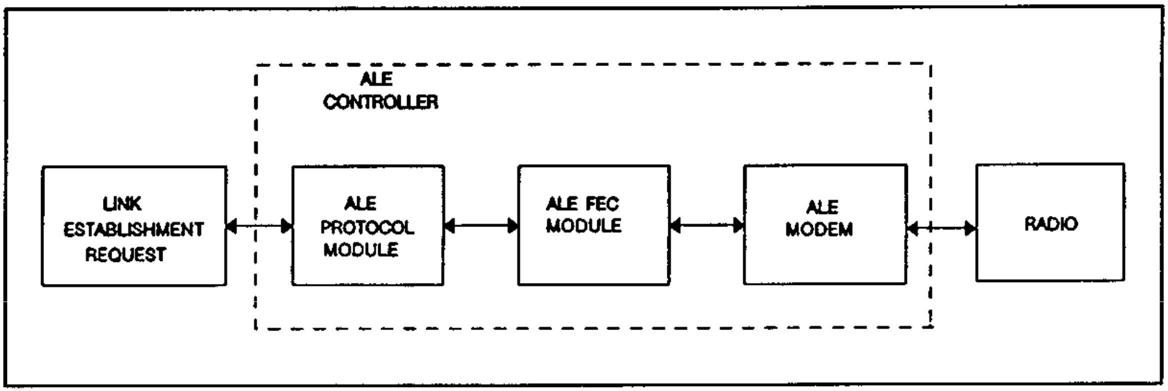


FIGURE 2a. Data flow in a system without LP.

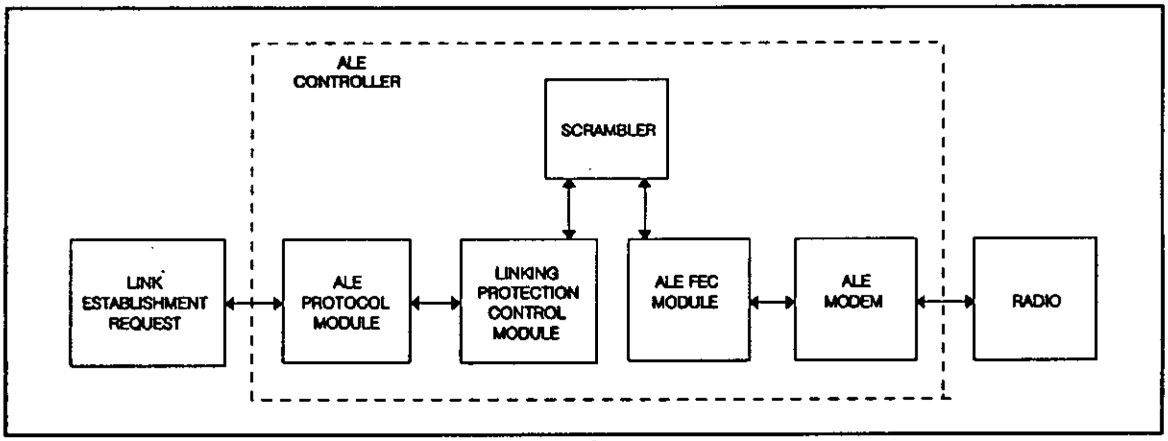


FIGURE 2b. Data flow in a protected system.

c. LP is achieved by encrypting ALE words under a private key that is changed periodically using known "randomization" information (frequency, time, date, etc.) to vary the results of this encryption on a shorter basis (a "protection interval [PI]"). The private key is entered directly into the scrambler via an appropriately protected circuit, and is protected during use by the design of the scrambler.

d. The addition of LP to a radio involves adding the functions of a linking protection control module (LPCM), that implements the LP protocol, and a scrambler, that scrambles ALE words under the control of the LPCM. The security of the system is based upon the inability of an adversary to "spoof" the LPCM, and relies on the difficulty of discovering the key used to scramble the ALE words. Because of the wide range of applications for LP, several different scramblers are specified; however, the LPCM function is common to all LP applications, as is a common denominator scrambler for assured interoperability of all protected radios.

e. Note that the existing LPCM handles unclassified ALE words only. Any classified traffic must be encrypted by a National Security Agency (NSA) approved cryptographic device; the resulting BLACK data may then be sent through the ALE controller or via a separate data modem.

4.2.1 Linking protection application levels. The following application levels of LP are defined in this section, with the classified application (AL-4) providing the highest degree of protection. The classified and unclassified but sensitive application levels (AL-4 and AL-3 respectively) require distinct hardware scramblers, while the unclassified enhanced application level and the unclassified application level (AL-2 and AL-1 respectively) scramblers may be implemented in software or firmware. All protected radios shall be capable of operation at AL-1. A means shall be provided to disable automatic linking at linking protection application levels less secure than the application level in use by the station being called. For example, a station which is operating at AL-3 shall be able to disable the receiver from listening for linking attempts at AL-0 through AL-2. (Design objective [DO]: Alert the operator but do not link automatically when a valid call is received from a transmitter with a lower linking protection application level.) This mechanism shall not preclude the operator from manually initiating ALE using a disabled application level. This manual override is required for interoperability.

4.2.1.1 AL-0 (unprotected application level). AL-0 indicates that no linking protection is being employed. No protection is provided against interfering, unintentional, or malicious linking attempts.

4.2.1.2 AL-1 (unclassified application level). The AL-1 scrambler shall employ the lattice encryption algorithm as specified in U.S. Army Information Systems Engineering Command (USAISEC), Fort Huachuca, Arizona, Technical Report, ASQB-OSI-S-TR-92-04, A 24-bit Encryption Algorithm for Linking Protection, March 1992, and may be implemented in hardware or software with manufacturer specified interfaces. This scrambler is for general U.S. Government and commercial use. This application level is mandatory for all protected radio systems, and therefore provides protected interoperability within the U.S. Government. The AL-1 protection interval is 60 seconds, which provides slightly lower protection than that available using the unclassified enhanced application level, but which permits relaxed synchronization requirements.

4.2.1.3 AL-2 (unclassified enhanced application level). The AL-2 scrambler shall employ the same algorithm as specified for the AL-1, and may be implemented in hardware or software, with manufacturer specified interfaces. This scrambler is for general U.S. Government and commercial use. The AL-2 protection interval is 2 seconds.

4.2.1.4 AL-3 (unclassified but sensitive application level). The AL-3 scrambler (for U.S. Government use only) shall employ the algorithm and the interface control document (ICD) developed by NSA. Systems employing AL-3 LP must meet NSA security requirements. The protection interval is a maximum of 2 seconds.

4.2.1.5 AL-4 (classified application level). The AL-4 scrambler (for U.S. Government use only) shall employ the algorithm and the ICD developed by NSA. An AL-4 scrambler may be used to protect classified orderwire traffic. Systems employing classified application level LP must meet NSA security requirements. The AL-4 protection interval is a maximum of 1 second.

4.2.2 Protocol transparency. A principal consideration in implementing LP is that the presence of an LP module in a radio (or its controller) shall have no impact on any protocols outside of the protection sublayer in the data link layer. This means that achieving and maintaining crypto-sync must occur transparently to the ALE waveform and protocols. Furthermore, scanning radios must be able to acquire crypto-sync at any point in the scanning call portion of a protected transmission if this transmission was encrypted under the key in use by the receiving station. Thus, LP modules shall not insert sync bits into the data stream, and must acquire crypto-sync without the use of synchronization preambles or message indicator bits.

4.2.3 Transmit processing. The LP module in a sending station encrypts each 24-bit ALE word to be sent using the seed data then in use (frequency, PI number, word number, etc.; see 5.1.1.3) and delivers the encrypted word to the FEC module. (Data block message [DBM] mode is a special situation; see 5.1.2.3.)

4.2.4 Receive processing.

a. The receive side of an LP module is responsible for achieving crypto-sync with transmitting stations, and for decrypting protected ALE words produced by the Golay decoder. In operation, when a scanning receiver arrives at a channel carrying valid tones and timing, the FEC sublayer (majority voter, de-interleaver, and Golay decoder) shall process the output of the ALE modem and alert the LP receive module when an acceptable candidate word has been received. (This occurs roughly once every 8 milliseconds [ms] when the Golay decoders are correcting 3 errors, or once every 78 ms when correcting 1 error per Golay word.)

b. The receive LP module must then decipher the candidate words, and pass them to the receive ALE module which determines whether word sync has been achieved by checking for acceptable preamble and ASCII subset. This task is complicated by the possibility that the received word (even if properly aligned) may have been encrypted using a different PI than that currently at the receiver, requiring the receiving LP module to decrypt each candidate word under several seeds. (Seeds are discussed in 5.1.1.3.)

c. A further complication is the possibility that a word may satisfy the preamble and character set checks under multiple seeds. When this occurs, the valid successors to all seeds which produced valid words shall be used to decrypt the next word, and each result shall be evaluated in the context of the corresponding first word. The probability is increasingly minute that multiple PI possibilities will exist after this second word is checked. For example, if during a scanning call (or sound) a received word decrypts to "TO SAM" using seed A, and to "DATA SNV" using seed B, the next word is decrypted using the successors to those seeds, denoted A′ and B′. If the result of decrypting this next word under A′ is not "TO SAM", the first decrypt under seed A was invalid, because the word following a "TO" word in a scanning call must be the same "TO" word. To be valid in a scanning call or sound, the word following "DATA SNV" must have three ASCII-38 characters and either "THRU", "REPEAT", "THIS IS", or "THIS WAS" preamble. A diagram showing all valid preamble sequences can be found in the figure titled Valid Word Sequence in MIL-STD-188-141.

4.3 Time of day (TOD) synchronization.

a. Because LP employs protection intervals (which are time-based), all stations must maintain accurate TOD clocks. Practical considerations suggest that station local times may differ by significant fractions of a minute unless some means is employed to maintain tighter synchronization. Because the effectiveness of LP increases as the length of the PI decreases, there is a trade-off between protection and the cost of implementing and using a time synchronization protocol.

b. Operators must synchronize station time to a common time source to within one minute, ±30 seconds, and then to employ a protocol to synchronize stations to within one or two seconds (fine sync) for enhanced linking protection. While operating networks with only coarse (one minute) time synchronization, the protection offered by this system against playback (tape recorder) attacks is reduced.

c. Synchronization of local times for LP requires some cooperation between the protocol entity and the LP time-base. One concept of how the coordination across the ALE-LP sublayer boundary may be effected in this case is as follows:

(1) TOD is maintained by the ALE entity, and is provided to the LP entity as required.

(2) The transmit LP entity uses the TOD provided by the transmit ALE entity to form seeds during the scanning call phase (T_{sc}) and for the initial time setting for the leading call phase (T_{lc}). Thereafter, the TOD from ALE is ignored and the transmit LP entity sequences seeds IAW 5.1.2.1.

(3) On the receive side, seed sequencing is performed by the functions responsible for achieving and maintaining word sync. These functions may be implemented within either the LP or the ALE module, but must know the current phase of the ALE protocol (e.g., T_{sc}, T_{lc}, etc.).

(4) For authentication of unprotected time exchanges, the ALE module must be able to call upon the LP module to encrypt and decrypt individual ALE words "off line."

4.4 Link quality functions. Not yet standardized.

4.5 Advanced link quality functions. Not yet standardized.

4.6 Networking functions. Not yet standardized.

4.7 Interface to link controllers. Not yet standardized.

4.8 Network management. Not yet standardized.

4.9 Multi-media networking. Not yet standardized.

4.10 Special requirements. Not yet standardized.

5. DETAILED REQUIREMENTS

5.1 Linking protection.

a. The LP procedures specified herein shall be implemented as distinct functional entities for the control functions and cryptographic functions. (Unless otherwise indicated, however, distinct *hardware* for each function is not required.) The LPCM shall perform all control functions specified herein and interface to the ALE controller as shown in figure 2b. Scrambler(s) shall perform all cryptographic operations on ALE words under the control of the LPCM.

b. Use of LP shall neither increase the time to establish a link compared to a non-protected radio, nor degrade the probability of linking below the requirements for non-protected linking (see MIL-STD-188-141 table titled Probability of Linking).

c. A means shall be provided to disable the LP functions and operate the radio in clear (unprotected) mode. Hardware scramblers shall be removable without impairment of the unprotected functionality of a radio.

5.1.1 Linking protection control module. The LPCM shall execute the LP procedure specified in 5.1.2 and control the attached scrambler(s) as specified below.

5.1.1.1 Scrambler interfaces. The LPCM shall interact with hardware scrambler(s) IAW the circuits and protocols specified in the ICD for each scrambler (see 4.2.1). Interaction with *software* implementations of scramblers shall comply with the applicable function call ICD, when specified.

5.1.1.2 Time and date. The LPCM requires accurate time and date for use in the LP procedure. The local time base shall not drift more than ±1 second per day when the station is in operation.

5.1.1.2.1 Time of day entry. A means shall be provided for entry of time of day (date and time) via either an operator interface or an electronic fill port such as an interface to a Global Positioning System (GPS) receiver. (DO: Provide both operator interface and electronic port.) This interface may also provide for the entry of a measure of uncertainty of the time entered. If time uncertainty is not provided, a default time uncertainty shall be used. Defaults for the various time fill ports may be separately programmable; unless otherwise programmed, the default uncertainty shall be within ±15 seconds.

5.1.1.2.2 Time exchange protocols. After initialization of TOD, the LPCM shall execute the time protocols of 5.2 as required to maintain total time uncertainty less than the protection interval length of the most secure LP application level it is using. The LPCM shall respond to time requests IAW 5.2.3.2 unless this function is disabled by the operator.

5.1.1.3 Seed format.

a. The LPCM shall maintain randomization information for use by scrambler(s), and shall provide this information, or "seed," to each scrambler IAW the applicable ICD.

b. The 64-bit seed shall contain the frequency carrying the protected transmission, the current PI number, the date, and a word number, in the format shown in figure 3a, where the most significant bits of the seed and of each field are on the left. The TOD portion of the seed shall be monotonically non-decreasing; the remaining bits are not so constrained.

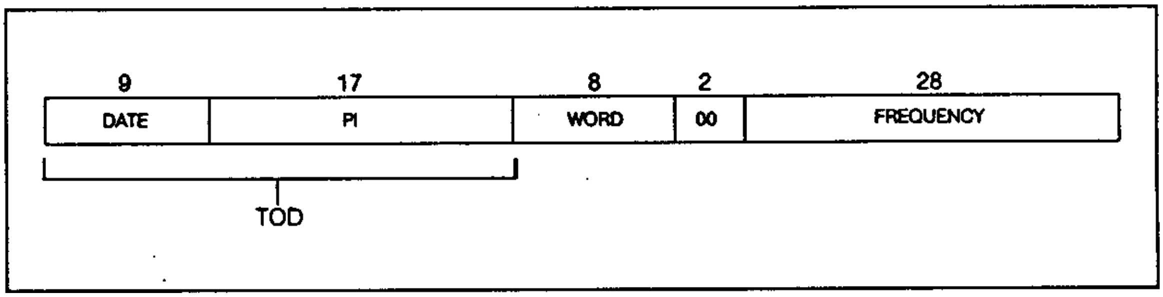


FIGURE 3a. Seed format.

c. The Date field shall be formatted IAW figure 3b. The Month field shall contain a 4-bit integer for the current month (1 for January through 12 for December); the Day field shall contain a 5-bit integer for the current day of the month (1 through 31). A mechanism shall be provided to accommodate leap years.

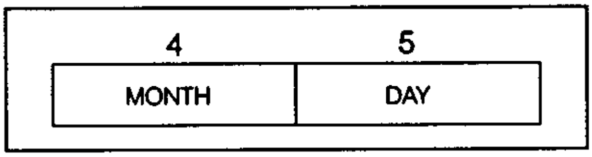


FIGURE 3b. Date format.

d. The PI field shall be formatted IAW figure 3c. The Coarse Time field shall contain an 11-bit integer that counts minutes since midnight. (Temporary discrepancies may occur as discussed in 5.1.2.) The 6-bit Fine Time field shall be set to all 1's when using AL-1 LP. When a time synchronization protocol (see 5.2) is employed to obtain more accurate time, the Fine Time field shall be set to the time obtained using this protocol and incremented as described in 5.1.2.

11	6
COARSE TIME	FINE TIME

FIGURE 3c. PI number format.

e. The Fine Time field shall always (except when all 1's) be a multiple of the PI length, and shall be aligned to PI boundaries (e.g., with a 2 second PI, Fine Time shall always be even).

f. The Word field shall be used to count words within a PI, as specified in 5.1.2.

g. The Frequency field shall be formatted IAW figure 3d. Each 4-bit field shall contain one binary-coded decimal digit of the frequency of the current protected transmission.

4	4	4	4	4	4	4
100 MHz	10 MHz	1 MHz	100 KHz	10 KHz	1 KHz	100 Hz

FIGURE 3d. Frequency format.

5.1.2 Procedure.

a. The procedure to be employed in protecting transmissions consisting entirely of 24-bit ALE words is presented in 5.1.2.1 and 5.1.2.2, followed by the procedure for the data block portion of data block mode transmissions.

b. When a radio is neither transmitting nor receiving, the PI number shall be incremented as follows:

(1) When using AL-2, AL-3, or AL-4 LP, the Fine Time field shall be incremented at the end of each PI by the length of the PI, modulo 60.

(2) When the Fine Time field rolls over to 0, the Coarse Time field shall be incremented, modulo 1440.

At midnight, the Coarse Time and Fine Time fields shall be set to 0, and the Date fields shall be updated.

c. When using AL-1 LP, the Fine Time field shall contain all 1's, and the Coarse Time field shall be incremented at the end of each minute, modulo 1440. At midnight, the Coarse Time field shall be set to 0, and the Date fields shall be updated.

5.1.2.1 <u>Transmitting station</u>.

a. Each word to be transmitted shall be encrypted by the scrambler using the current seed information. In the course of a transmission, the protocol described below may cause a discrepancy between the TOD fields in the seed and the real time. Such a discrepancy is a normal consequence of the LP procedure, and shall persist until the conclusion of each transmission, whereupon the TOD fields of the seed shall be corrected.

b. The word number field **w** shall be used as follows:

(1) During the scan calling phase (T_{sc}) of a call, the calling station shall alternate transmission of words encrypted using **w** = 0 and **w** = 1. The first word of T_{sc} shall use the value of **w** that results in **w** = 1 for the last word in T_{sc}. The TOD used during T_{sc} shall change as required to keep pace with real time, except that TOD shall only change when **w** = 0; words encrypted with **w** = 1 shall use the same TOD as the preceding word.

(2) At the beginning of the leading call phase (T_{lc}) of a call (which is the beginning of a single-channel call), the first word shall be encrypted using **w** = 0 and the correct TOD for the time of transmission of that word.

(3) All succeeding words of the call shall use succeeding word numbers up to and including **w** = $\mathbf{w}_{max}$; for the word following a word encrypted with **w** = $\mathbf{w}_{max}$, the TOD shall be incremented and **w** shall be reset to 0. $\mathbf{w}_{max}$ = 2 for a 1 second PI, $\mathbf{w}_{max}$ = 5 for a 2 second PI, and $\mathbf{w}_{max}$ = 153 for a 60 second PI.

(4) Responses and all succeeding transmissions shall start with **w** = 0 and the current (corrected) TOD, with these

fields incremented as described in step (3) above for each succeeding word.

c. Figure 4a illustrates the permissible TOD¦**w** combinations for a transmitting station using a 2 second PI ($\mathbf{w}_{max}$ = 5), and the permissible sequences of these combinations. In the figure, T represents the stored TOD.

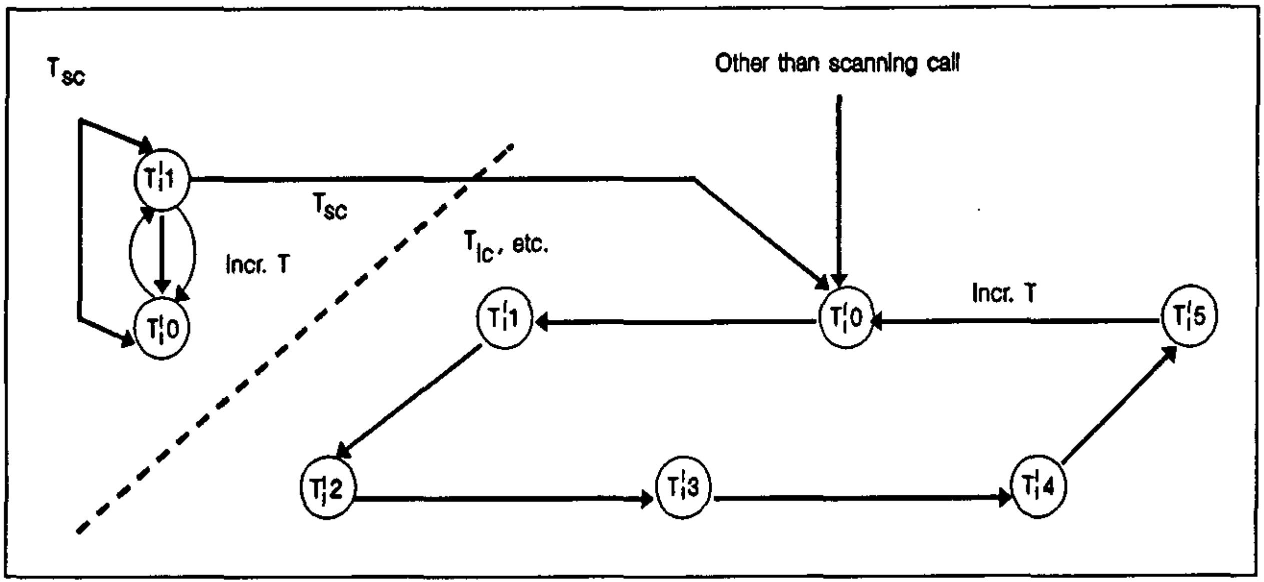


FIGURE 4a. Transmitting station state diagram (2 second PI).

d. Sounds are protected in the same fashion, with T_{rs} (redundant sound phase) in the place of T_{lc}. A single-channel sound is analogous to a single-channel call, and begins the above procedure at step (2) above. A multi-channel sound is analogous to a scanning call, and begins at step (1) above.

5.1.2.2 Receiving station.

a. Because of the possibility of acceptable decodes under multiple TOD/word number combinations, receivers shall attempt to decode received words under all allowed combinations (the current and adjacent PIs [future and past], and both **w** = 0 and **w** = 1) when attempting to achieve word synchronization with a calling station (six combinations). Stations prepared to accept time requests (see 5.2.3.2) shall also attempt to decode received words using coarse TOD (Fine Time = all 1's, correct Coarse Time only) with both **w** = 0 and **w** = 1 (eight combinations total). All VALID COMBINATIONS SHALL BE CHECKED while seeking word sync; after achieving word sync, the number of valid combinations is greatly reduced by the LP protocol.

b. Figure 4b illustrates the permissible TOD¦W sequences for a receiving station using a 2 second PI after word sync is achieved. Note that, unlike the transmitter, the receiving station state machine may be non-deterministic. For example, when in T_{sc} and in state T¦1, a received word may yield valid preambles and ASCII when decrypted using all of the valid combinations: T¦0, (T+1)¦0, and T¦2 (the latter implying that T_{lc} started two words previously), and will therefore be in three states at once until the ambiguity is resolved by evaluating the decrypted words for compliance with the LP and ALE protocols.

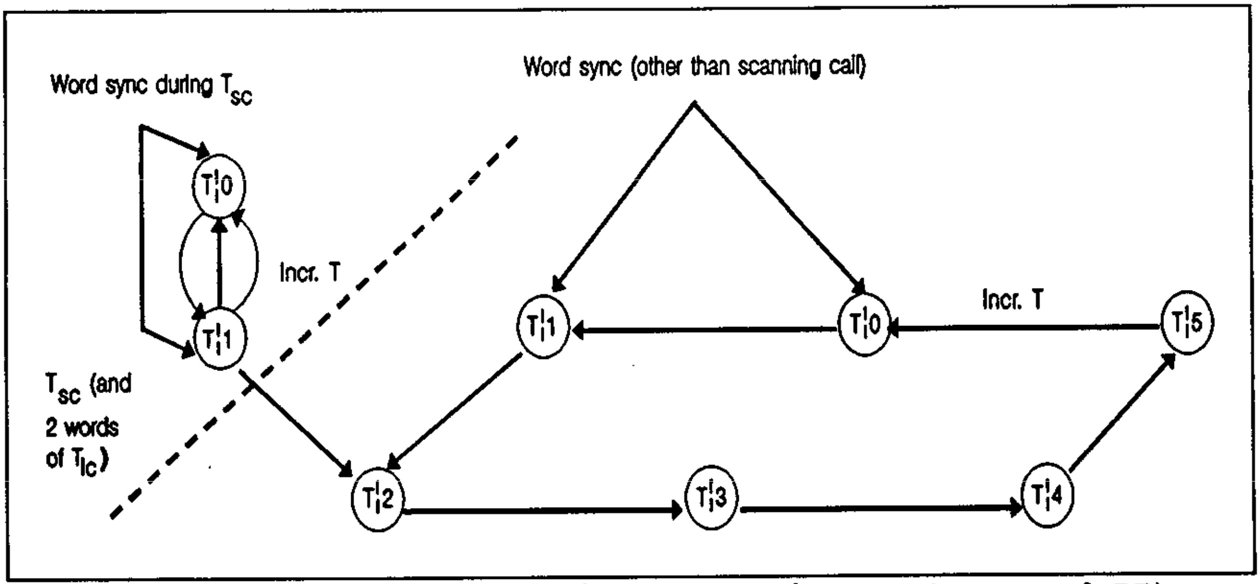

Word sync during T_{SC}
Word sync (other than scanning call)
T¦0
T¦1
Incr. T
T_{SC} (and 2 words of T_{lc})
T¦1
T¦0
Incr. T
T¦5
T¦2
T¦3
T¦4

FIGURE 4b. Receiving station state diagram (2 second PI).

c. Stations using a protection interval of two seconds or less shall not accept more than one transmission encrypted using a given TOD, and need not check combinations using that TOD. For example, if a call is decrypted using TOD = X, no TOD before X + 1 is valid for the acknowledgment.

5.1.2.3 Data block message mode.

a. A DBM data block contains an integral number of 12-bit words, the last of which comprises the least significant 12 bits of a cyclic redundancy check (CRC). These 12-bit words shall be encrypted in pairs, with the first 12-bit word presented to the LPCM by the ALE protocol module as the more significant of the two. When a data block contains an odd number of 12-bit words (i.e., Basic DBM data block and Extended DBM data blocks with odd N), the final 12-bit word shall not be encrypted, but shall be passed directly to the FEC sublayer.

b. The word number field **w** of the seed shall be incremented only after three pairs of 12-bit words have been encrypted (rather than after every 24-bit word as in normal operation), except that the word number **w** shall be incremented exactly once after the last pair of 12-bit words in a DBM data block is encrypted, whether or not it was the third pair to use that word number.

5.2 Time exchange protocols. The following protocols shall be employed to synchronize LP time bases. The time service protocols for active time acquisition, both protected (see 5.2.3) and non-protected (see 5.2.4), are mandatory for all implementations of LP.

5.2.1 Word formats. The mandatory time protocols employ the following three types of ALE words: command words, coarse time words, and authentication words in the formats listed below.

5.2.1.1 Command words. Time exchange command words, including the *Time Is* command and the *Time Request* command used to request and to provide TOD data, shall be formatted as shown in figure 5. The three most significant bits (W_{1-3}) shall contain the standard CMD preamble 110. The next seven bits (W_{4-10}) shall contain the ASCII character '~' (1111110), indicating a time exchange command word. The three time quality bits shall indicate the magnitude of time uncertainty at the sending station IAW 5.2.2. Seconds and 40 ms Ticks fields are described below.

3	7	3	6	5
CMD	TIME EXCHANGE	TIME QUALITY	SECONDS	40 MS TICKS

FIGURE 5. Time exchange command words.

5.2.1.1.1 *Time Is* command.

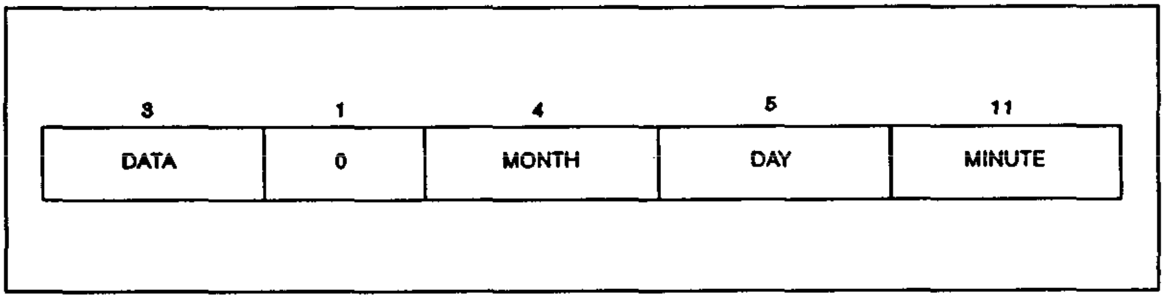
a. The *Time Is* command word carries the fine time current at the sending station as of the start of transmission of the word following the *Time Is* command word, and is used in protected time requests and all time service responses. In a *Time Is* command word, the Seconds field shall be set to the current number of seconds elapsed in the current minute (0-59), and the Ticks field shall be set (or rounded) to the number of 40 ms intervals that have elapsed in the current second (0-24). The *Time Quality* shall reflect the sum of the uncertainty of the local time and the uncertainty of the time of transmission of the *Time Is* command IAW table I.

b. When a protocol requires transmission of a *Time Is* command word, but no time value is available, a NULL *Time Is* command word shall be sent containing a time quality of 7, and the Seconds and Ticks fields both set to all 1's.

5.2.1.1.2 Time Request command. The *Time Request* command word shall be used to request time when no local time value is available, and is used only in non-protected transmissions. In a *Time Request* command word, time quality shall be set to 7, the Seconds field to all 1's, and the Ticks field to 30 (11110).

5.2.1.1.3 Other encodings. All encodings of the Seconds and Ticks fields not specified here are reserved, and shall not be used until standardized.

5.2.1.2 Coarse time words. Coarse time words shall be formatted as shown in figure 6, and shall contain the coarse time current as of the transmission of the beginning of that word.



3	1	4	5	11
DATA	0	MONTH	DAY	MINUTE

FIGURE 6. Coarse time words.

5.2.1.3 Authentication words. Authentication words, formatted as shown in figure 7, shall be used to authenticate the times exchanged using the time protocols. The 21-bit authenticator shall be generated by the sender as follows:

a. All 24-bit words in the time command message preceding the authentication word (starting with the *Time Is* or *Time*

Request command word that begins the message) shall be bit by bit "exclusive-ored."

NOTE: "Exclusive-or" is the condition that exists when each resulting bit is a 1 if the two input bits do not match, or the resulting bit is a 0 when the two input bits match.

b. If the message to be authenticated is in response to a preceding time command message, the authenticator from that message shall be exclusive-ored with the result of paragraph a above.

c. The 21 least significant bits of the final result shall be used as the authenticator.

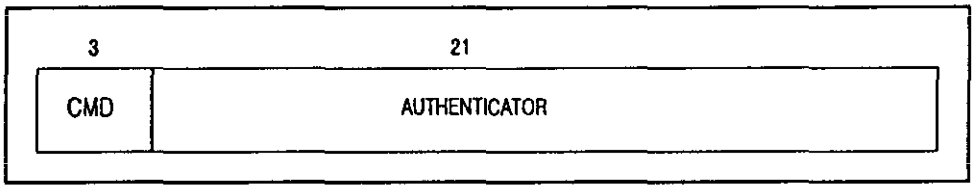


FIGURE 7. Authentication words.

5.2.2 Time quality.

a. Every time exchange command word transmitted shall report the current uncertainty in TOD at the sending station, whether or not time is transmitted in the command word. The codes listed in table I shall be employed for this purpose. The time uncertainty windows in the table are upper bounds on total uncertainty (with respect to coordinated universal time). For example, uncertainty of ±6 seconds is 12 seconds total, and requires a transmitted time quality value of 6.

TABLE I. Time Quality.

TIME QUALITY CODE	TIME UNCERTAINTY WINDOW
0	none*
1	20 ms
2	100 ms
3	500 ms
4	2 s
5	10 s
6	60 s
7	unbounded

*Reserved for use by UTC time standard stations.

b. Stations shall power up from a cold start with a time quality of 7. Time uncertainty is initialized when time is entered (see 5.1.1.2.1), and shall be maintained thereafter as follows: the uncertainty increases at a rate set by oscillator stability (e.g., 72 ms per hour with a ±10 parts-per-million [ppm] time base), until the uncertainty is reduced upon the acceptance of time with less uncertainty from an external source, after which the uncertainty resumes increasing at the above rate.

c. A station accepting time from another station shall add its own uncertainty due to processing and propagation delays to determine its own internal time uncertainty. For example, if a station receives time of quality 2, it adds to the received uncertainty of 100 ms (±50 ms) its own processing delay uncertainty of, perhaps, ±100 ms, and a propagation delay bound of ±35 ms, to obtain a new time uncertainty of ±185 ms, or 370 ms total. With a ±10 ppm time source, this uncertainty window would grow by 72 ms per hour, so after two hours the uncertainty becomes 514 ms, and the time quality has dropped to 4. In another 20 hours, the uncertainty grows to approach 2 seconds, and the station (if using a 2 second PI) shall request the correct time before it drops to time quality 5 and is presumed to have lost fine time synchronization.

d. If a low-power clock is used to maintain time while the rest of the unit is powered off, the quality of this clock shall be used to assign time quality upon resumption of normal operation. For example, if the backup clock maintains an accuracy of ±100 ppm under the conditions expected while the station is powered off, the time uncertainty window shall be increased by 17 seconds per day. Such a radio that has been powered off for much over three days may not be presumed to retain even coarse sync, despite its backup clock, and may require manual entry of time.

5.2.3 Active time acquisition (protected). A station that knows the correct date and time to within one minute may attempt to actively acquire time from any station with which it can communicate by employing the protocol in the following paragraphs. The quality of time so acquired is necessarily at least one grade more uncertain than that of the selected time server. A station that does not know the correct date and time to within one minute may nevertheless employ this protected protocol by repeatedly guessing the time until it successfully communicates with a time server.

5.2.3.1 Time request call.

a. A station requiring fine time shall request the current value of the network time by transmitting a time request call, formatted as follows:

TO <time server> **CMD** *Time Is* <time> **DATA** <coarse time> **REP** <authenticator> **THIS IS** <requester>.

(In principle, any station may be asked for the time, but some stations may not be programmed to respond, and others may have poor time quality; thus, multiple servers may need to be tried before sufficient time quality is achieved.)

b. The *Time Is* command shall be immediately followed by a coarse time word and an authentication word. The authenticator shall be generated by the exclusive-or of the command word and the coarse time word, as specified in 5.2.1.3.

c. The time request call transmission shall be protected using the procedure specified in 5.1.2. When acquiring time synchronization, the coarse seed (Fine Time field in the seed set to all 1's) current at the requesting station shall be used; when used to reduce the time uncertainty of a station already in time sync, the current fine seed shall be used.

5.2.3.2 Time service response.

a. A station that receives and accepts (see below) a time request call shall respond with a time service response formatted as follows:

TO <requester> **CMD** *Time Is* <time> **DATA** <coarse time> **REP** <authenticator> **THIS IS/WAS** <requester>.

b. The *Time Is* command shall be immediately followed by a coarse time word and an authentication word. The authenticator shall be generated by the 3-way exclusive-or of the command word and the coarse time word from this transmission and the authentication word (including the **REP** preamble) from the requestor, as specified in 5.2.1.3. The entire time service response shall be protected as specified above, using the time server's current *coarse* seed if the request used a coarse seed, or the current fine seed if otherwise. Note that the seed used in protecting a time service response may differ from that used in the request that caused that response.

c. A time server shall only respond to the first time request call using each fine or coarse seed; i.e., one coarse request per minute, and one fine request per fine PI. Acceptance of each class of time requests (coarse and fine) may be disabled by the operator. Stations that are prepared to accept coarse *Time Request* commands shall decrypt the initial words of incoming calls under eight (versus six) possible seeds: **w** = 0 and **w** = 1 with the current coarse TOD, and with the current fine TOD ±1 PI. Note that only one coarse TOD is checked versus three fine TODs.

5.2.3.3 Time server request. Normally, the time server concludes the time service protocol by terminating its response with *This Was*. A time server may instead request authenticated time from the original requester by returning a Time Server Request, which is identical to the time service response as discussed above except that the *This Was* termination is replaced by *This Is*. The original requester shall then respond with a time service response, as above, with an authenticator generated by the 3-way exclusive-or of the command word and the coarse time word from its time service response and the authentication word (including the **REP** preamble) from the Time Server Request, as specified in 5.2.1.3.

5.2.3.4 Authentication and adjustment.

a. A station awaiting a time service response shall attempt to decrypt received words under the appropriate seeds: if the request used a coarse seed, the waiting station shall try the coarse seeds used to encrypt its request with

w = 0 and **w** = 1, and those corresponding to one minute later. If the request used a fine seed, the waiting station shall try the usual six seeds:

w = 0 and **w** = 1 with the current *fine* TOD ±1 PI.

b. Upon successful decryption of a time service response, the requesting station shall exclusive-or the received command and coarse time words with the authentication word it sent in its request. If the 21 least significant bits of the result match the corresponding 21 bits of the received authentication word, the internal time shall be adjusted using the time received in the *Time Is* command and coarse time word, and the time uncertainty shall be set IAW 5.2.2c.

5.2.4 Active time acquisition (non-protected). A station that does not know the correct date and time to within one minute may attempt to actively acquire time from any station with which it can communicate in non-protected mode by employing the protocol in the following paragraphs. Because time is not known in this case with sufficient accuracy to employ LP, the entire exchange takes place in the clear with the authentication procedure as the only barrier against deception.

5.2.4.1 Time request call (non-protected).

a. A station requiring time shall request the current value of the network time by transmitting a non-protected time request call, formatted as follows:

TO <time server> **CMD** *Time Request* **DATA** <coarse time>
REP <"random"#> **THIS IS** <requester>.

b. The *Time Request* command shall be immediately followed by a coarse time word, followed by an authentication word containing a 21-bit number, generated in such a fashion that future numbers are not predictable from recently used numbers from any net member. Encrypting a function of a radio-unique quantity and a sequence number that is incremented with each use (and which is retained while the radio is powered off) may meet this requirement.

5.2.4.2 Time service response (non-protected).

a. A station that receives and accepts (see paragraph c below) a non-protected time request call shall respond with a non-protected time service response formatted as follows:

TO <requester> **CMD** *Time Is* <time> **DATA** <coarse time> **REP** <authenticator> **THIS WAS** <time server>.

b. The *Time Is* command shall be immediately followed by a coarse time word and an authentication word. The 21-bit authenticator shall be generated by encrypting the 24-bit result of the 3-way exclusive-or of the command word and the coarse time word from this transmission and the entire random number word (including the **REP** preamble) from the requester, as specified in 5.2.1.3. The encryption shall use the AL-1 algorithm, and a seed containing the time sent with **w** = all 1's. The least significant 21 bits of this encryption shall be used as the authenticator.

c. A time server shall respond to only the first error-free non-protected time request call received each minute (according to its internal time). Acceptance of non-protected time requests may be disabled by the operator.

5.2.4.3 Authentication and adjustment (non-protected). Upon receipt of a non-protected time service response, the requesting station shall exclusive-or the received coarse time word with the received *Time Is* command word, exclusive-or the result with the entire random number word it sent in its time request call, and encrypt this result using **w** = all 1's and the coarse time contained in the time service response. If the 21 least significant bits of the result match the corresponding 21 bits of the received authentication word, the internal time shall be adjusted using the received coarse and fine time, and the time uncertainty shall be set IAW 5.2.2c.

5.2.5 Passive time acquisition.

a. As an alternative to the active time acquisition protocols specified above, stations may attempt to determine the correct network time passively by monitoring protected transmissions. Regardless of the technique used to otherwise accept or reject time so acquired, passive time acquisition shall include the following constraints:

(1) Local time may only be adjusted to times within the local window of uncertainty. Received transmissions using times outside of the local uncertainty window shall be ignored.

(2) Local time uncertainty shall be adjusted only after receipt of transmissions from at least two stations, both of which include time quality values, and whose times are consistent with each other within the windows implied by those time qualities.

b. A passive time acquisition mechanism may also be used to maintain network synchronization, once achieved.

c. Passive time acquisition is optional; if provided, the operator shall be able to disable it.

5.2.6 Time broadcast.

a. To maintain network synchronization, stations shall be capable of broadcasting unsolicited *Time Is* commands to the network, periodically or upon request by the operator:

> **TO** <NET> **CMD** *Time Is* <time> **DATA** <coarse time>
> **REP** <authenticator> **THIS WAS** <time server>.

b. The *Time Is* command shall be immediately followed by a coarse time word and an authentication word. The authenticator shall be generated by the exclusive-or of the command word and the coarse time word from this transmission, as specified in 5.2.1.3. If the broadcast is made without LP (i.e., in the clear), the authenticator shall be encrypted as described in 5.2.4.2.

c. Note that the use of an authenticator that does not depend upon a challenge from a requesting station provides no protection against playback of such broadcasts. A station receiving such broadcasts must verify that the time and the time uncertainty that they contain are consistent with the local time and uncertainty before such received time is at all useful.

5.3 Channel and frequency designators. Not yet standardized.

5.4 Link quality functions. Not yet standardized.

5.5 Advanced link quality analysis. Not yet standardized.

5.6 Additional orderwire functions. Not yet standardized.

5.7 ALE support for relaying. Not yet standardized.

5.8 Networking functions. Not yet standardized.

5.9 Network management. Not yet standardized.

5.10 Multi-media operation. Not yet standardized.

5.11 Special requirements. Not yet standardized.

6. NOTES

(This section contains information of a general or explanatory nature that may be helpful, but is not mandatory.)

6.1 Intended use.

a. The purpose of this document is to provide the technical parameters for the functions and features of advanced adaptive HF radio, and provide logical and cohesive guidelines for both industry and the Government.

b. There is no requirement for linking protection to be a part of a user's acquisition unless the user has an identified need. Optional levels of linking protection are identified and detailed. These options, AL-1 and AL-2, provide an inexpensive, least protected mode and a more sophisticated protection mode. The user should establish his or her application level based on minimum essential requirements.

c. This document is structured segmentally, with each segment being added as it is developed. The outline of MIL-STD-187-721 used in this document includes areas anticipated to be covered in other segments. These areas are referenced in this document as "not yet standardized."

6.2 Issue of DODISS. When this standard is used in acquisition, the applicable issue of the DODISS must be cited in the solicitation (see 2.1.1 and 2.2).

6.3 Tailoring. This document cannot be tailored further than the proper selection made from the intended use paragraph above.

6.4 Subject term (key word) listing.

Adaptive HF radio
ALE
Automatic link establishment
Application level
Forward error correction
Linking protection
Protection interval
Time protocols

CONCLUDING MATERIAL

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

Review activities:
Army - CR
Navy - MC
DoD - DC, NS, DI

User activities:
Army - AC, PT
Navy - NC, TD, OM, CG
Air Force - 02,13,21
DoD - DH, ECAC, MP
DOT - FAA, OST

Civil agency coordinating activities:
NCS

Preparing activity:
Army - SC

(Project TCSS-7210)

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

INSTRUCTIONS

1. The preparing activity must complete blocks 1, 2, 3, and 8. In block 1, both the document number and revision letter should be given.
2. The submitter of this form must complete blocks 4, 5, 6, and 7.
3. The preparing activity must provide a reply within 30 days from receipt of the form.

NOTE: This form may not be used to request copies of documents, nor to request waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

I RECOMMEND A CHANGE:	**1. DOCUMENT NUMBER** MIL-STD-187-721	**2. DOCUMENT DATE** *(YYMMDD)* 930218

3. DOCUMENT TITLE
Planning and Guidance Standard for Automated Control Applique for HF Radio

4. NATURE OF CHANGE *(Identify paragraph number and include proposed rewrite, if possible. Attach extra sheets as needed.)*

5. REASON FOR RECOMMENDATION

6. SUBMITTER

a. NAME *(Last, First, Middle Initial)*	**b. ORGANIZATION**	
c. ADDRESS *(Include Zip Code)*	**d. TELEPHONE** *(Include Area Code)* (1) Commercial (2) AUTOVON *(If applicable)*	**7. DATE SUBMITTED** *(YYMMDD)*

8. PREPARING ACTIVITY

a. NAME Department of the Army USAISEC	b. TELEPHONE *(Include Area Code)* (1) Commercial (602) 538-3354	(2) AUTOVON 879-3354
c. ADDRESS *(Include Zip Code)* ATTN: ASQB-OSE-TT Fort Huachuca, Arizona 85613-5300	**IF YOU DO NOT RECEIVE A REPLY WITHIN 45 DAYS, CONTACT:** Defense Quality and Standardization Office 5203 Leesburg Pike, Suite 1403, Falls Church, VA 22041-3466 Telephone (703) 756-2340 AUTOVON 289-2340	

Previous editions are obsolete.

198/290