International ALE (automatic link establishment) standard for HF Transceiver XK2000

Because of the dynamic propagation conditions in the shortwave range, setting up a reliable link for this type of communication is anything but a simple task, which in the past could only be performed successfully and within relatively short time by experienced operators. Today this job has been taken over and perfected by automatic-link-establishment techniques. Besides company-specific procedures such as ALIS (automatic link setup) from Rohde & Schwarz [1; 2], which were specially developed and optimized for fast

FIG 1 Modern HF transceiver of XK2000 family with integrated communication processor
Photo 41 251

data transmission via critical HF paths (adaptive response), international standards like FED-STD-1045 and MIL-STD-188-141 have been worked out and widely accepted.

For reasons of interoperability these standardized ALE (automatic link establishment) techniques along with R&S-specific ALIS are supported by the XK2000 HF transceiver family [3] from Rohde & Schwarz and their integrated Data Link Processor GS2200 (FIG 1).

ALE specifies solely the shortwave link setup; subsequent communication (speech, data) is not defined by the standard and may take place in accordance with any other protocol desired. However, brief messages may be conveyed by the setup protocol. Besides the actual link setup protocol, the ALE standard provides several addressing modes for operation in a network as well as means of protection of the link setup against eavesdropping and deception through encrypting the protocol.

link setup are also specified. Standard 1045 is supplemented by standards 1046 to 1052. An 8FSK signal with discrete frequencies from 750 Hz to 2500 Hz is used for link setup. This signal type is suitable for transmission via HF transceivers as an SSB (single-sideband) signal with bandwidth of 3 kHz. The tones are transmitted at a symbol rate of 125 per second. An ALE word consists of 24 data bits (3 bits for the preamble and 3 x 7 data bits). To enhance the transmission reliability of ALE words on the HF channel, each one is extended by a 24-bit Golay FEC code (forward error correction), then interleaved and emitted with threefold redundancy. The entire ALE word including error correction consists of 49 tones and is 392 ms long (FIG 2).

Each ALE network is assigned a number of frequencies for establishing links. A station switched to receive mode scans all assigned frequencies at a rate of two or five channels per second, waiting for calls to come in on any

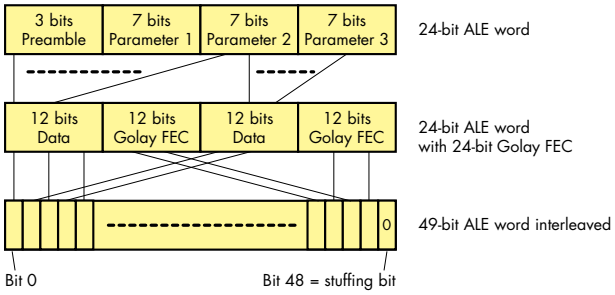

FIG 2
ALE word coding and interleaving

Technical features of ALE standard

FED-STD-1045 specifies the parameters involved in automatic link setup with HF transceivers. Besides basic parameters like modulation type and transceiver bandwidth, signal type, coding methods and protocol sequence for automatic

of those frequencies. A calling station emits a call whose length is matched to the number of channels available, so the call can be captured by the scanning receive station. If a call is not successful, another call will be performed on the next channel. Several such frequency lists (scan groups) may be stored in an ALE station.

When a link is being set up, ALE words are combined to form an ALE frame. This frame is divided into individual sections, the transitions between which are indicated by preambles contained in the ALE words. A complete ALE link setup is made up of three such frames. First the calling station emits a call frame, which is answered by the called station (response frame). The calling station acknowledges receipt of the response frame by transmitting an appropriate frame to the called station. At this juncture the link setup is completed.

An ALE station is identified by an address with a maximum length of 15 characters consisting of upper-case letters A to Z and numbers 0 to 9. Besides this unequivocal addressing of an individual station (individual call, point-to-point link), further addressing methods for contacting all stations or groups of stations in a network are also possible. All Call serves for addressing all stations of a network (broadcast) and is not acknowledged by the called stations (FIG 3). Selective All Call is used to call stations with the same final character. With Group Call, several stations of a network respond to a call according to a predefined response protocol. Net Call addresses all stations of a network assigned to a network address. Again the called stations respond according to a predefined protocol. Further types of addresses are Any Call for emergencies, which is responded to by all stations receiving this call, and Wild Card addressing, in which case only certain characters of the address are to conform.

ALE allows the link quality of the transmission path to be checked in order to minimize link establishment times. The sequence in which frequencies are called will then be made dependent on actual link quality. This is possible by storing and administering the link quality to each subscriber. The information on link quality is provided by a sounding process that involves calls being emitted at programmable inter-

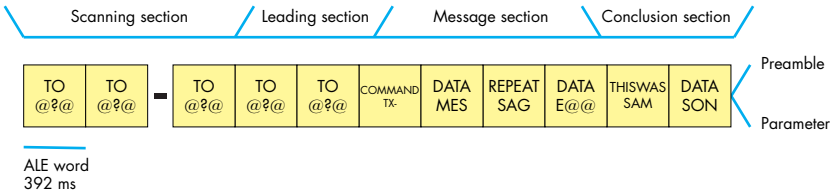

FIG 3 Example of frame for All Call from SAMSON station in automatic message display function with Tx message

vals and determination of their receive quality (link quality analysis, LQA).

Brief messages may already be transmitted during link setup. AMD (automatic message display) enables the calling station to transmit, while calling, a predefined message up to 90 characters long, which is displayed at the called receive station. This feature of the standard is utilized by Transceiver XK2000, among other things for transmitting a phone number to the receive station to allow a telephone network link to be set up via an APP (automatic phone patch). UUF (user-unique function) enables transmission of a manufacturer-specific 14-bit value during link setup, which may for example be used for controlling the subsequent data transmission protocol (in Data Link Processor GS2200). With the aid of DTM (data text message) mode, brief messages can be transmitted without requiring an additional data modem and protocol.

Encryption of link setup

Linking protection (FED-STD-1049) is one of the ALE functions. It serves to protect the information contained in the protocol such as address and network relation against eavesdropping. This method is also resistant to deception (spoofing) by the enemy through recording and retransmitting the emitted information. This function protects the link setup only. For the protection of subsequent speech and data messages, additional cryptographic measures have to be taken at the transmit and receive ends.

The Rohde & Schwarz implementation supports three of five protection levels defined in FED-STD-1049 (AL-0, AL-1 and AL-2). Level AL-2 offers the greatest security (protection interval 2 s), but also means more stringent requirements for network synchronization, while Level AL-1 offers somewhat less security (protection interval 60 s), but network synchronization requirements are not as high either. The protection interval is the time interval within which the input variables of the encryption algorithm are constant.

The 24-bit ALE words for link setup are encrypted with the aid of the Johnson algorithm [4]. Input variables for this algorithm are the crypto key defined by the user, frequency, date and time. The key may be a word up to 63 bits long, which results in a maximum number of keys of 2^{63}. Because this technique is time-referenced, a time-synchronized network is required. Different procedures are provided to first establish and then maintain synchronization. One station in the network serves as the time master station, supplying the other stations with the exact time via protocols. Time may also be manually entered at each station. For maintaining synchronization, a time-acquisition protocol polling the exact time from the time reference station is started whenever a certain degree of inaccuracy is detected in the system. This protocol is also protected as long as the time deviations are found to be within tolerance by the linking protection process. For stations without any information on date and time or with insufficient time accuracy, an acquisition protocol has been implemented, which however is not protected because of the absence of time information. This option is primarily intended for stations entering the network at a later date.

Günter Wicker; Erich Schippan

REFERENCES

[1] Greiner, G.: Reliable shortwave with ALIS. News from Rohde & Schwarz (1987) No. 116, pp 47–50

[2] Greiner, G.: Fast and secure data transmission on shortwave – result of intensive research. In this issue, pp 41–43

[3] Helmke, B.; Wachter, G.: HF Transceiver XK2100 – Digital shortwave for future-proof, long-haul communication. News from Rohde & Schwarz (1994) No. 144, pp 47

[4] Johnson, E.: A 24 bit Encryption Algorithm for Linking Protection. Technical Report ASQB-OSI-S-TR-92-04, March 1992

Reader service card 155/08