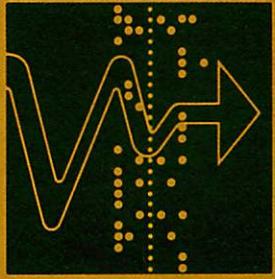


GRETAGCODER® 812

**AUTOMATIC
ON-LINE/OFF-LINE
CIPHER SYSTEM**



AUTOMATIC ON-LINE/OFF-LINE CIPHER SYSTEM TC-812

The TC-812 is a compact solid state cipher system, intended for tactical teletypewriter communication over short wave radio links and wire circuits.

The TC-812 is primarily an on-line system, but off-line operation is also possible. In the on-line mode a message typed in is enciphered, transmitted, deciphered and printed out at the receiving station in a single operation, without any noticeable delay. Special synchronization circuits keep the transmitting and receiving cipher system synchronized at all times.

The TC-812 is a self-contained computer based system offering excellent reliability and the highest possible security under all operating conditions. An extremely large number of internally generated cipher programs is available for automatic enciphering and deciphering of messages. A particular program is selected by the combination of a secret wiring patch board, a secret elementary key and a non-secret auxiliary key. The secret wiring patch board is removable from the machine and the wiring configuration is easily modified by the user. The secret elementary key consists of ten letters to be typed in on the teletypewriter keyboard prior to operation. This key is stored in an electronic memory. The auxiliary key is a random key inserted automatically with every clear/cipher transition. This feature allows multiple use of a single elementary key without impairing the system's security.

Cryptologically speaking the machine is of no value to an enemy without the secret wiring patch board. If a secret wiring patch board should fall into enemy hands, knowledge of the secret elementary key is still necessary to decipher the message. In practice, the TC-812 cipher is unbreakable, provided that the necessary precautions are taken in handling and selecting the secret elements.

The system is easy to use as most operations are controlled by simple instructions typed in on the teletypewriter keyboard.

CONFIDENTIAL
for official use only

TC-812, CONDENSED TECHNICAL SPECIFICATIONS

The cipher system is shock-mounted in a watertight transport container with the interconnecting cables and accessories located in the container cover during transport.

The machine is entirely solid state and uses primarily integrated circuits.

Dimensions: (including transport container)

535 x 280 x 355 mm / 21 x 11 x 14 inches

(width x height x depth)

Weight:

25 kgs / 53 lbs.

Temperature range:

- Operating 0° to 50° C (32° to 122° F)
- Storage -20° to 70° C (-4° to 158° F)

Power connection:

- Power line voltage: 110/220 V AC $\begin{smallmatrix} +15\% \\ -20\% \end{smallmatrix}$
- Power line frequency: 50/60 Hz $\pm 10\%$
- Power consumption: 100 VA
(without teletypewriter)

Buffer battery:

A built-in nickel-cadmium battery is permanently charged as long as the unit is switched ON. In case of power failure, the battery delivers the necessary power for some important circuits up to 1 hour. During the power failure period no communication is possible since the teletypewriter and the radio station have no power either. However, the synchronism of the network remains due to the buffer battery feature and after the power failure the TC-812 is automatically switched into the same mode as it was before.

Teletypewriter connections: (see appendix)

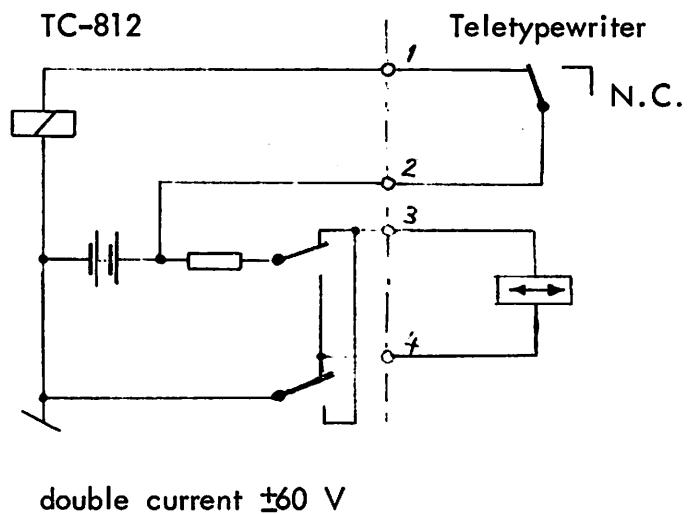
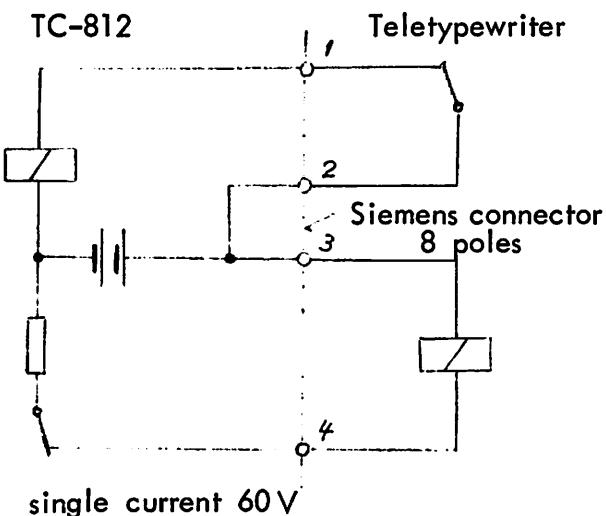
- Code: CCITT Code No. 2
- Operating speed: 45.45 / 50 / 75 / 100 baud
(internal speed selector)

- Line current, line voltage:

Single or double current, depending on built-in PC-board; current selectable with switch:

PC-board FSA/A : single current 60 V 20 / 40 / 60 mA

PC-board FSA/C : double current \pm 60 V 20 / 40 / 60 mA



Transmission channel:

- Code: CCITT Code No. 2

- Operating speed: 45.45 / 50 / 75 / 100 baud
(internal speed selector)

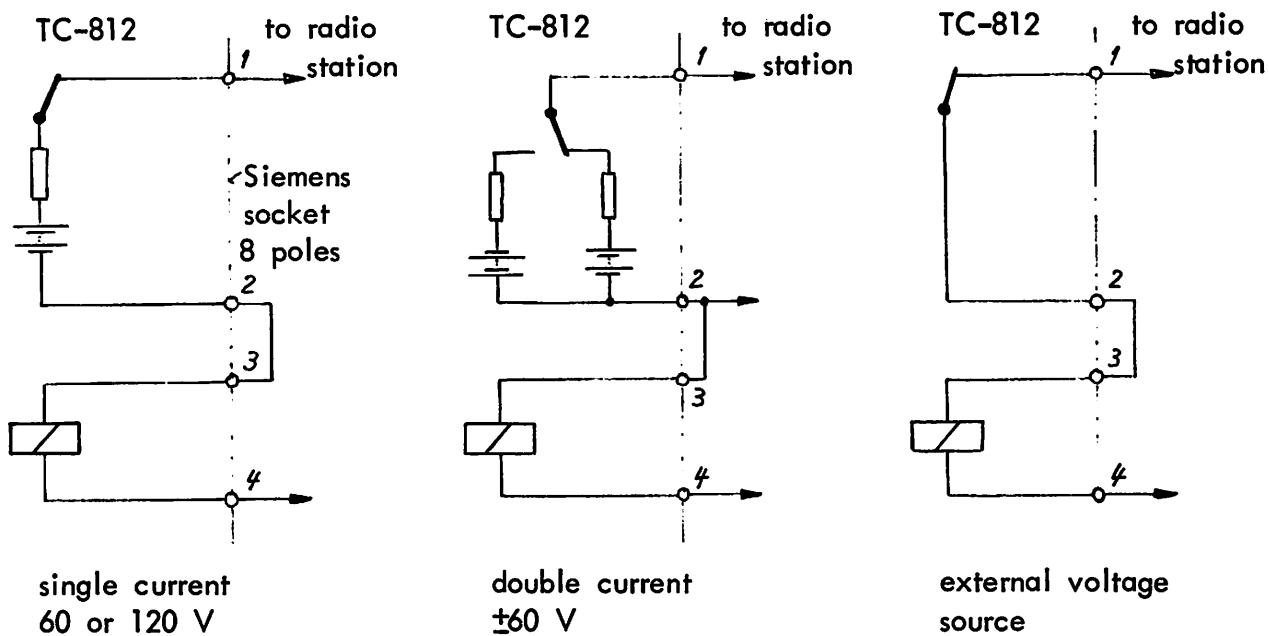
- Line current, line voltage:

Single or double current depending on build-in PC-board, current selectable with switch:

PC-board LTA/A : single current 60 V 20 / 40 / 60 mA

PC-board LTA/B : single current 120 V 20 / 40 / 60 mA

PC-board LTA/C : double current \pm 60 V 20 / 40 / 60 mA



The send-receive status of a radio station connected to the TC-812 is automatically controlled by the unit with a relay contact (see appendix).

Synchronization

Initial synchronization is achieved by special binary sequences in order to minimize the effects of atmospheric noise, fading and/or selective enemy jamming on the transmission channel. At the receiving station, special correlators process this information automatically. A synchronization sequence is automatically released by typing in very simple commands on the teletypewriter keyboard.

Automatic propagation delay correction: When changing the transmission direction in multistation networks the difference in propagation delay between stations is automatically corrected for in order to maintain synchronism. To achieve this in an optimum way, two modes of operation are possible:

- adaptive delay correction with automatic resynchronization during every transmit/receive transition. This mode is primarily used in multiple networks with changing or unknown propagation delays between the stations.

- fixed delay correction without resynchronization. Whenever the propagation delay remains constant, it can be measured with the unit itself and it is individually set for every station with the delay correction selector switch. This mode is primarily used in simple wire networks (fixed point to point and star networks) or multiple radio networks (star or mesh) whenever the propagation delays between the stations depend primarily on the fixed (i.e. measurable) delays in the radio transmitter and receiver circuits.

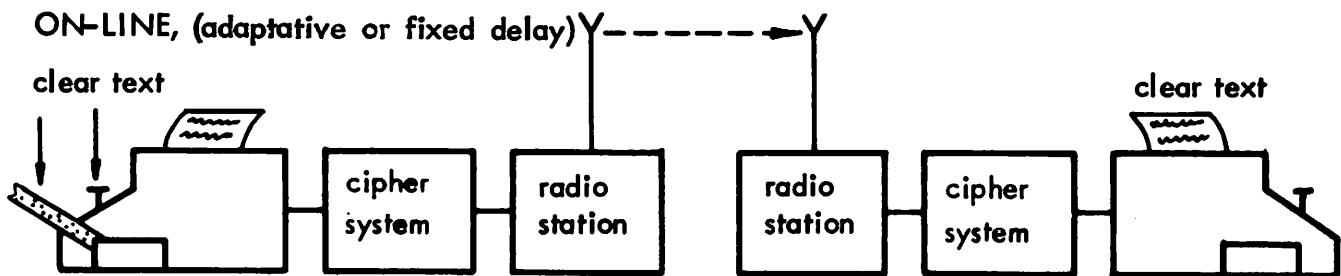
Automatic resynchronization in both crypto modes (avoiding a clear-crypto transition) after a commanded transmission pause (radio silence) is guaranteed after an idle time of up to 60 hours at 50 baud. During an undesired (incidental) transmission interruption (deep fade, burst noise, power failure) synchronous operation is always automatically maintained due to the inherent clock stability for periods of up to 1 hour at 50 baud, i.e. without any resynchronization.

Operating modes

On-line operation

Synchronous crypto operation (normal mode of operation)

In this mode the network is always controlled by that station that is transmitting at the moment. The receiving stations follow the encrypted commands of the transmitting station momentarily providing the correct secret wiring configuration and secret elementary key are used. All commands are typed in on the teletypewriter keyboard. The status actuated by those commands is indicated by two of four indicator lights (CLEAR, CRYPTO, TRANSMIT, RECEIVE) in the whole network. Due to the automatic call and answering feature to change transmission directions, anyone of the stations in the network may take command and control the network, should the designated leading station fall out. The commanding transmitting station is able to remotely switch anyone of the receiving stations to become the transmitting station, thereby switching itself back to the receiving status and initiating all necessary delay corrections in order to maintain synchronism in the network. If the newly called transmitting station is unattended, the unit (after a short time) automatically sends out a command for a transmission pause to the network, switching itself back to the receiving status. By this means an undesired blocking of the transmission frequency is avoided, and any station that has a need to transmit information may do so anytime by typing in the command to resynchronize the network (without a clear-crypto transition).



Synchronous clear operation

This mode is used for test purposes only. The transmitted signal is synchronous and not enciphered. An acoustical signal warns the operator each time the keyboard of the teletypewriter is actuated.

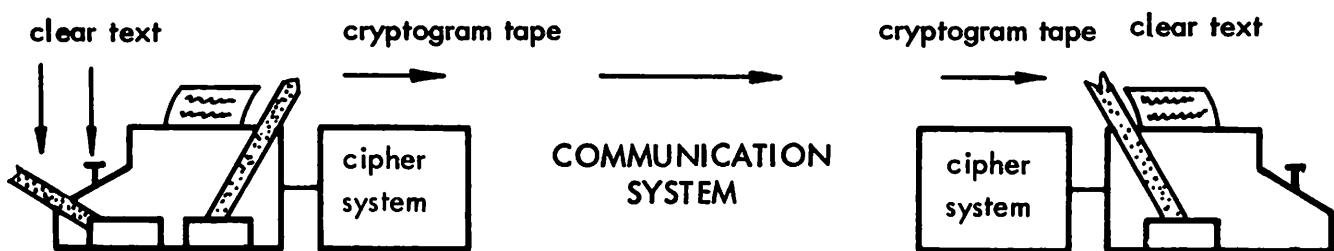
Asynchronous clear operation

This asynchronous mode works on the start-stop principle in clear. It is used to establish communication in regular telex networks (exchange of "Who Are You?" / Answer back) or when establishing a radio communication in order to tune the receiver to the transmitter frequency.

Off-line operation

This mode is used to work independently of the communication system. An enciphered punched tape which is produced by the unit can be sent by regular mail, or forwarded by a messenger and can be deciphered at the receiving station. In the off-line mode any communication equipment is automatically disconnected from the TC-812 unit.

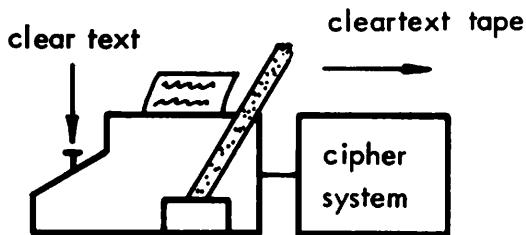
OFF-LINE



Local operation

This mode is used to prepare punched tapes. The information is not transmitted, but an incoming signal has priority and the unit is always ready to receive it.

LOCAL



Automatic friend-foe identification in multistation networks

In all synchronous operation and delay correction modes the following identification systems are possible for networks with up to 5 stations:

- Automatically controlled answering with selective station identification

A message is transmitted by one station and is received by all other stations in the network. The actual transmitting station can selectively switch any receiving station into the transmission mode. This station now takes control of the network.

- Automatically controlled selective receiving

After establishing communication, at first a message is transmitted by one station and is received by all others in the network. After a change of direction with any station in the network, messages can only be exchanged between those two stations. All other stations remain in synchronism but the print-out on their teletypewriters is automatically suppressed.

Operating commands

Special command sequences (similar to the synchronization sequences) are released by typing the appropriate command on the teletypewriter. These sequences are transmitted in enciphered form and can therefore not be detected by an enemy. On the receiver the individual command sequences are recognized by correlation thereby guaranteeing correct reception even under worst conditions.

S S S S S Preparation of the unit to accept secret ten letter elementary key prior to transmission.

Q Q Q Q Q Establishing of synchronous communication by any station in the network with automatic clear/crypto transition. The connected communication equipment (e.g. radio station) is automatically switched into the transmit position (calling station) or into the receive position (all other stations).

P P P P P End of transmission with automatic crypto/clear transition. All units go into receiving position (clear-idle position). Re-establishing of synchronous crypto communication can be actuated by any station in the network by typing Q Q Q Q Q.

N N N N N End of transmission without automatic crypto/clear transition (desired transmission interruption, e.g. radio silence). All units go into receiving position (crypto-idle position). Re-establishing of synchronous crypto communication can be actuated by any station in the network by typing its own identification (e.g. A A A A A), thereby initiating automatic re-synchronization.

A A A A A) The actual transmitting station (e.g. B) can control the selective
B B B B B) answering of any station in the network by typing the appropriate
D D D D D) identification (e.g. F F F F F) of the station, which will be the new
F F F F F) transmitting station (e.g. F). An acoustical signal draws the operator's
G G G G G) attention to the new mode of operation.

The stations are identified by setting the appropriate selector switch mounted on the frontpanel.

In networks with more than 5 stations semi-automatic operation is possible.

Break-in

In half-duplex operation the receiving station can signal back to the transmitting station (e.g. bad reception).

Reset

The reset push button can be pressed to clear the TC-812 unit in case of transmission difficulties. The elementary key remains stored. It may be erased in emergency cases by turning off the power switch.

Dummy text

When not typing any text, the ciphering program computer is automatically disconnected from the line and a signal derived from a truly random generator is transmitted. The transition between the two modes is actuated by GRETAG proprietary techniques. Since there are no "gaps" or other significant signal elements (bits) between the random signal and the normal enciphered text the transitions between the two random signal trains cannot be detected by an enemy. During dummy text transmission the print-out of the teletypewriter is automatically switched off.

Monitor system to prevent unwanted transmission of clear text

A digital monitor system continuously checks the ciphering computer, the clear text and the enciphered text for insufficient encryption at the mixer. In case of any malfunctioning of the ciphering computer or the mixer (unwanted clear text transmission) the line is automatically disconnected and an acoustical signal immediately warns the operator of the circuit breakdown.

Solid state ciphering program computer

A special computerized cipher principle, proprietary to GRETAG, is used. The ciphering programs are determined by:

- Secret wiring patch board:

24 plugable wires with a diversity of $\approx 10^{23}$. Secured by a mechanical safety lock the secret wiring patch board can easily be removed by an authorized person and stored in a secure location, thereby permitting unattended storage of the TC-812 in a non-secret area.

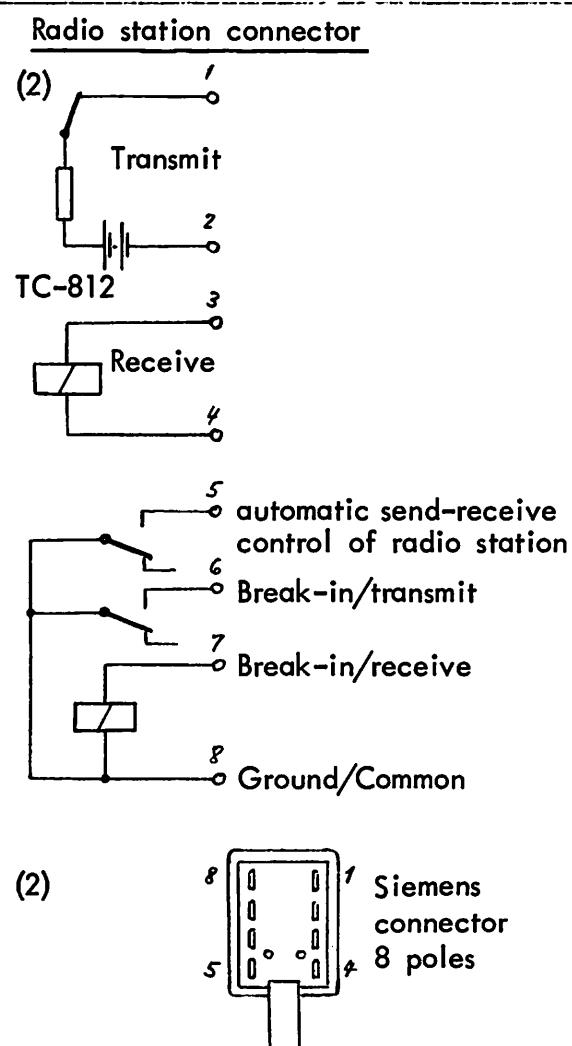
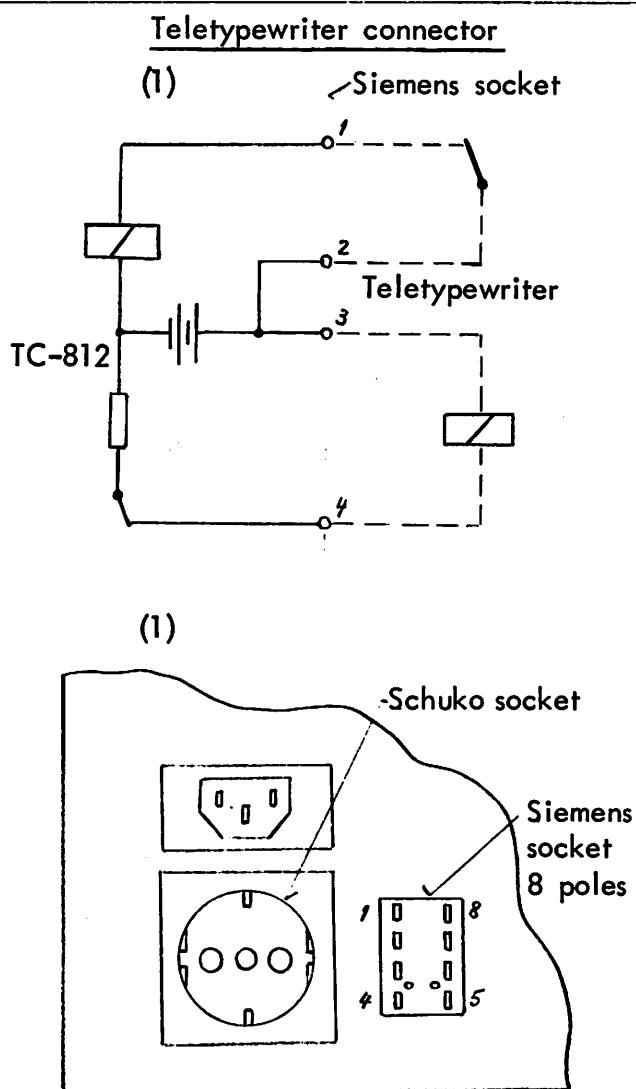
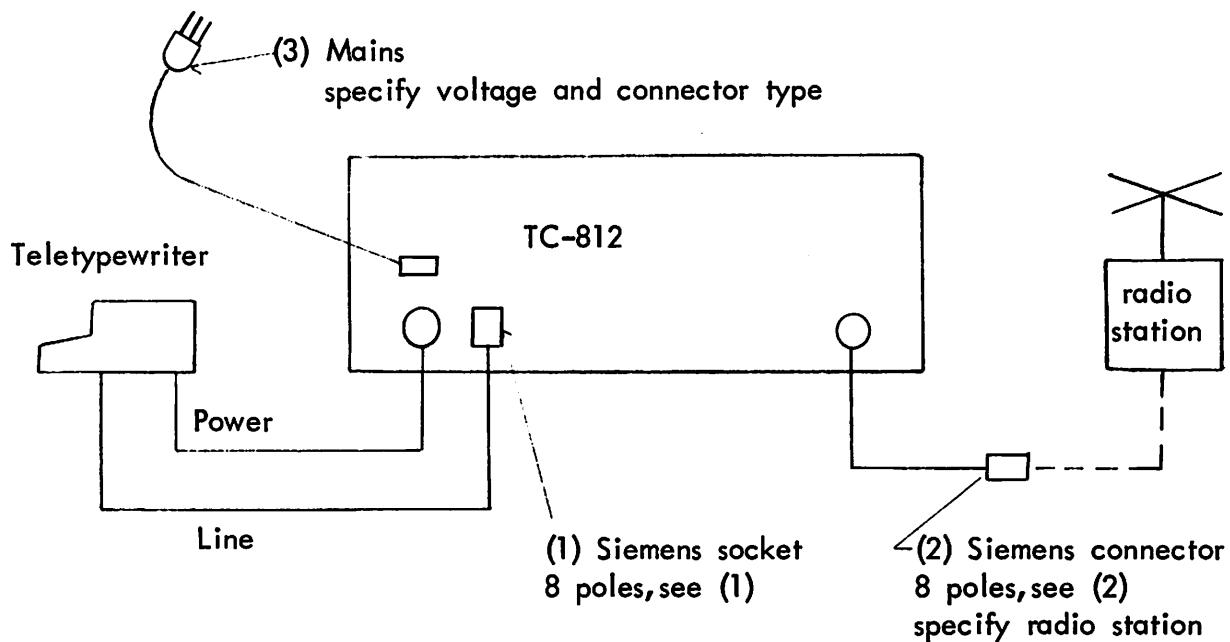
- Secret elementary key:

10 letters, typed in on the keyboard with a diversity of $\approx 10^{14}$.

- Non-secret auxiliary key:

8 letters, automatically derived from a built-in random generator for each clear/crypto transition. Due to this automatic feature a particular elementary key (daily key) can be used several hundred times without impairing the system's security (absolutely resistant to Kerckhoff superimposition and "Index of Coincidence"-methods by Friedmann).

Appendix



Please detach this form when requesting further information. Mark the appropriate space

(1) Teletypewriter

Manufacturer: _____

Type: _____

single current 60 V from TC-812 20 / 40 / 60 mA selectable

single current 120 V from TC-812 20 / 40 / 60 mA selectable

double current \pm 60 V from TC-812 20 / 40 / 60 mA selectable

(2) Transmission channel

Radio station or teletype converter:

Manufacturer: _____

Type: _____

		line current		
		20 mA	40 mA	60 mA
single current	60 V from TC-812 to radio station	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
single current	120 V from TC-812 to radio station	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
double current	\pm 60 V from TC-812 to radio station	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
single current	60 V from radio station to TC-812	<input type="checkbox"/>	<input type="checkbox"/>)
single current	120 V from radio station to TC-812	<input type="checkbox"/>)	20 / 40 / 60 mA
double current	\pm 60 V from radio station to TC-812	<input type="checkbox"/>))

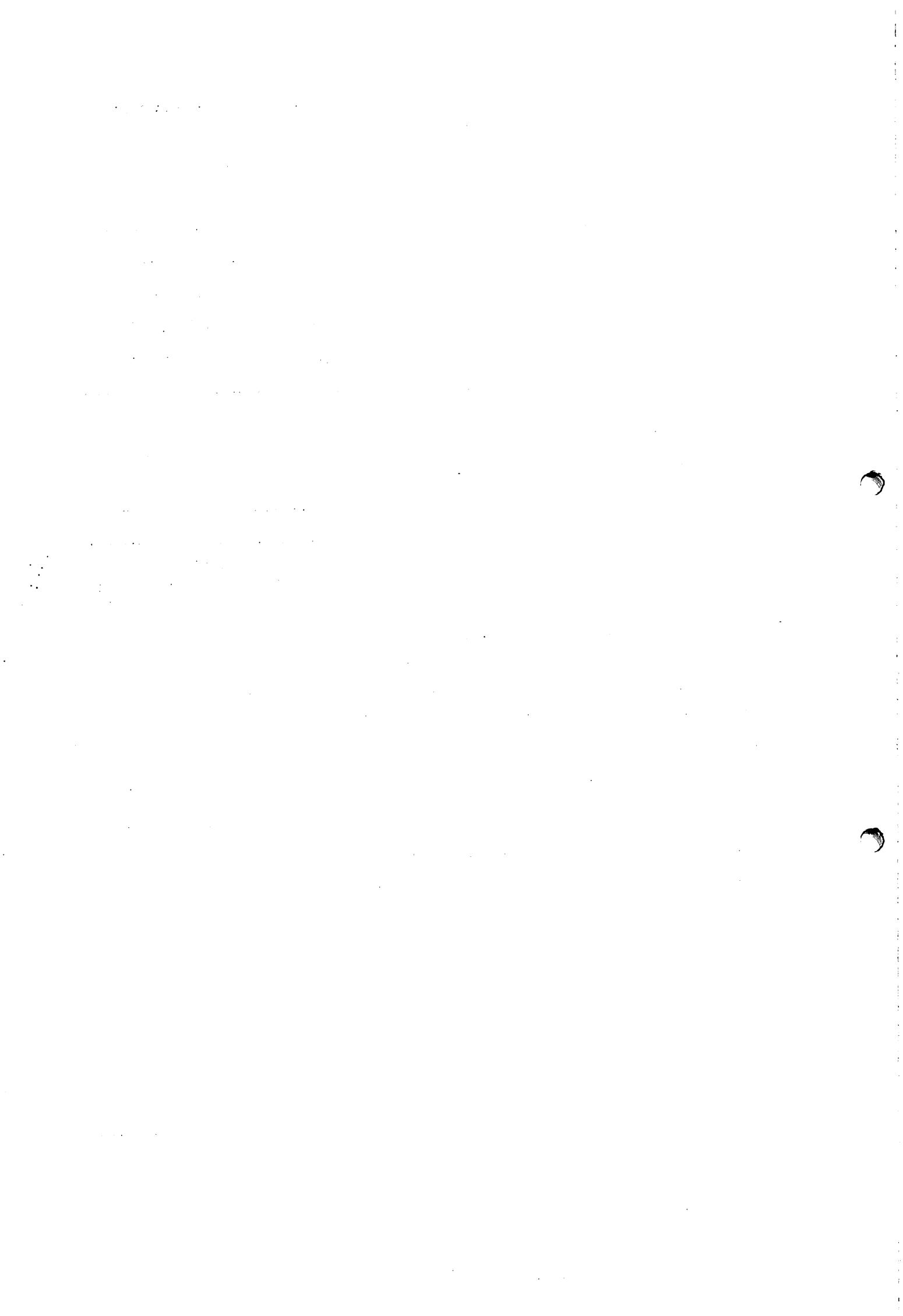
Specify send-receive and break-in relay contacts and connecting wiring in radio station (schematic) DC or AC voltage / current / earth ground / signal ground / impedance

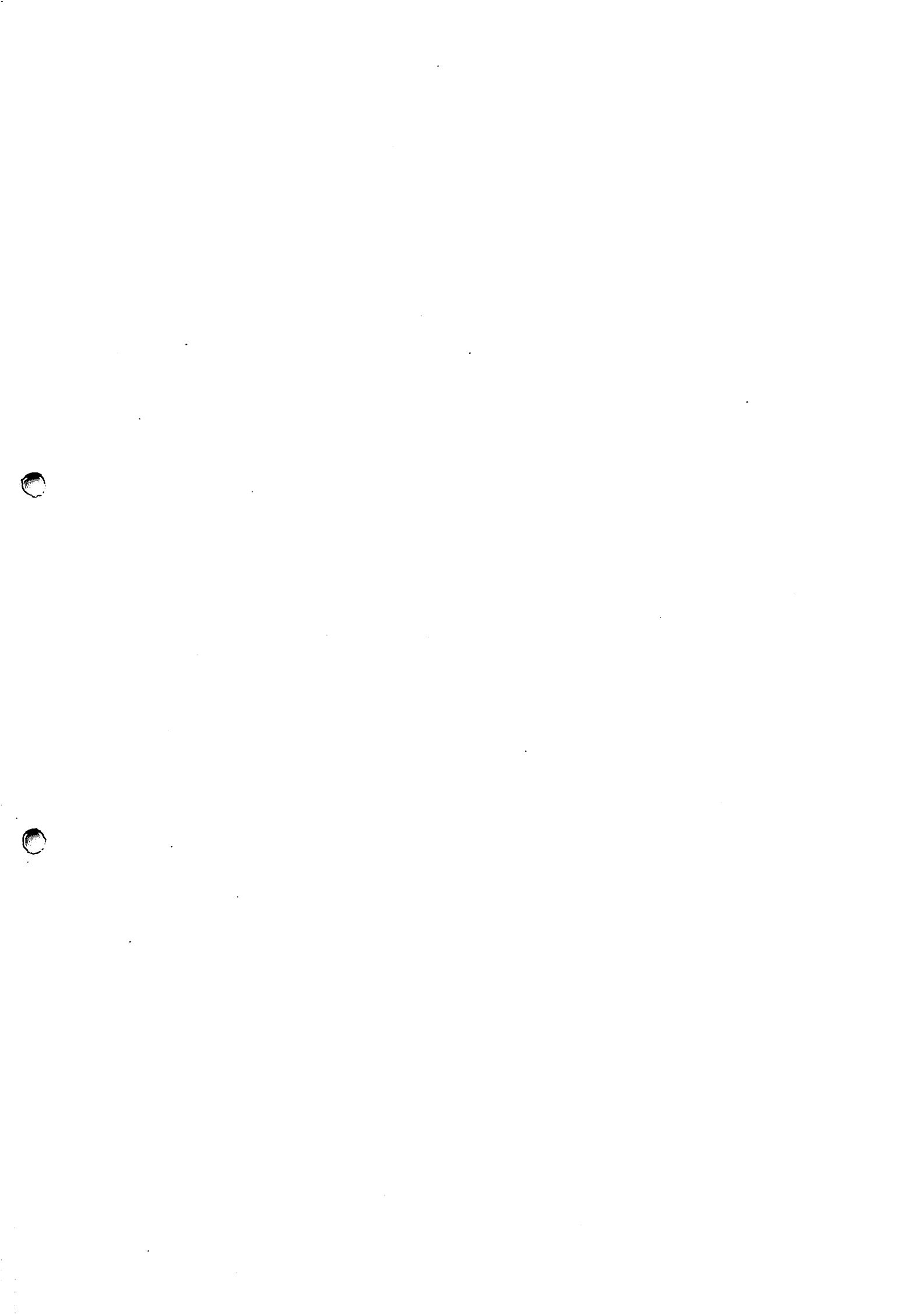
(3) Mains

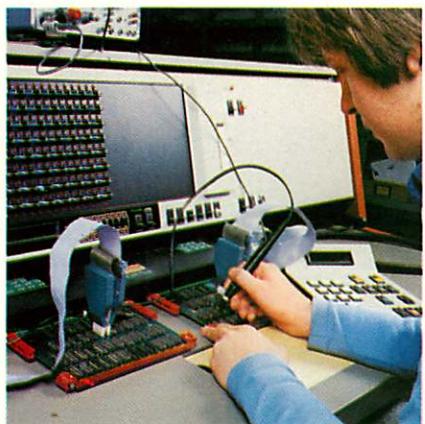
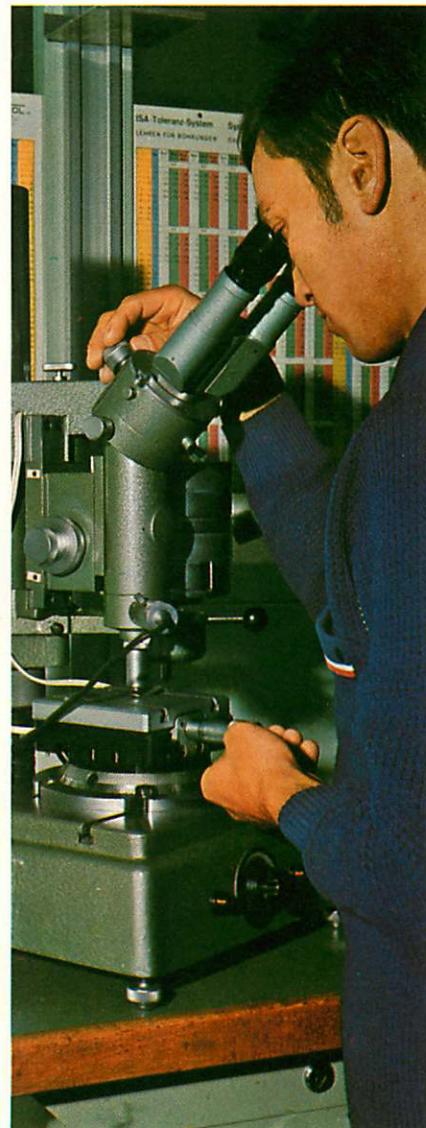
Voltage: V

Frequency: Hz

Type of connector: approx. drawing







GRETAG SECURITY SYSTEMS

GRETAG Limited

Althardstrasse 70, CH-8105 Regensdorf/Zurich, Switzerland Phone: 01 842 11 11, Telex: 53950