

GBPPR 'Zine



Issue #42 / The Monthly Journal of the American Hacker / October 2007

"When you give help to these Albanians,' Dimé said, 'is like sending money directly to Usama bin Laden."

--- Quote from *Blowing My Cover* by Lindsay Moran about the Balkans conflict during the 1990s. More proof those fucking Eurosavages (and Clinton) are behind the support for terrorists.

Table of Contents

- ◆ **Page 2 / Office Alarm System Description / #1A ESS**
 - ◆ Overview of audio and visual alarms under a #1A ESS central office.
- ◆ **Page 20 / Improvised Ceramic Weapons**
 - ◆ Simple cutting instruments which will pass through metal detectors.
- ◆ **Page 25 / Anti-TASER Clothing Experiments**
 - ◆ Don't tase me, Bro!
- ◆ **Page 34 / Nortel DMS-100 Receiver Table (RECEIVER)**
 - ◆ Controls the different types of audio and signalling tone receivers in a DMS switch.
- ◆ **Page 38 / Bugging**
 - ◆ Scan of an August 1987 article in *Popular Science* on espionage and spy tradecraft.
- ◆ **Page 45 / Bonus**
 - ◆ I Can Has Password?
- ◆ **Page 46 / The End**
 - ◆ Editorial and rants.

Office Alarm System Description / #1A ESS

BELL SYSTEM PRACTICES
AT & TCo Standard

SECTION 231-035-000
Issue 1, July 1976

OFFICE ALARM SYSTEM DESCRIPTION/THEORY 2-WIRE NO. 1 AND NO. 1A ELECTRONIC SWITCHING SYSTEM

CONTENTS	PAGE	CONTENTS	PAGE
1. GENERAL	2	POWER ALARM CONTROL UNIT	11
INTRODUCTION	2	ALARM BATTERY SUPPLY CONTROL UNIT	12
PURPOSE OF OFFICE ALARM SYSTEM	2	ALARM GROUPING CONTROL UNIT	12
OFFICE ALARM SYSTEM CHARACTERISTICS	2	CRITICAL ALARM UNIT	12
ALARM CATEGORIES	3	4. ALARM REPORTING	12
AUDIBLE AND VISUAL ALARM INDICATORS	3	GENERAL	12
2. PHYSICAL DESCRIPTION	5	ALARM REPORTING - MULTIFLOOR OFFICE	12
OFFICE ALARM SYSTEM	5	ALARM REPORTING - MULTIFLOOR OFFICE (SAME MCC OR MAINTENANCE CENTER)	18
AISLE PILOT CONTROL UNIT	5	5. POWER	18
FLOOR ALARM CONTROL UNIT	5	6. MAINTENANCE	19
POWER ALARM CONTROL UNIT	5	7. REFERENCES	19
ALARM BATTERY SUPPLY CONTROL UNIT	5		
ALARM GROUPING CONTROL UNIT	5		
CRITICAL ALARM UNIT	6		
MISCELLANEOUS ALARM UNITS	6		
3. FUNCTIONAL DESCRIPTION	7		
OFFICE ALARM SYSTEM	7		
AISLE PILOT CONTROL UNIT	11		
FLOOR ALARM CONTROL UNIT	11		

FIGURES

1. Miscellaneous Power Frame with Office Alarm Units	7
2. Aisle Pilot Control Unit	8
3. Floor Alarm Control Unit	8
4. Power Alarm Control Unit	8
5. Alarm Battery Supply Control Unit	8

NOTICE

Not for use or disclosure outside the
Bell System except under written agreement

Printed in U.S.A.

Page 1

Office Alarm System Description / #1A ESS

SECTION 231-035-000

CONTENTS	PAGE
6. Alarm Grouping Control Unit	8
7. Critical Alarm Unit	9
8. Main Aisle Pilot Lamp Assembly	9
9. Aisle Pilot Lamp Assembly	10
10. Exit Pilot Lamp Unit (For Single Floor Office)	11
11. Exit Pilot Lamp Unit (For Multifloor Offices)	11
12. Audible Alarm Panel	12
13. No. 1 or No. 1A ESS Office Alarm System Block Diagram	13
14. No. 1 or No. 1A ESS Office Alarm System Functional Block Diagram	15

TABLES

A. No. 1 and No. 1A ESS Audible and Visual Alarms	4
B. Typical Office Arrangement Options for No. 1 or No. 1A ESS - One Building Floor	5
C. Typical Office Arrangement Options for Three No. 1 or No. 1A ESS Floors and Power Room in Building	6

1. GENERAL

INTRODUCTION

1.01 This section describes the office alarm system for the No. 1 or No. 1A Electronic Switching Systems (ESS) as follows:

- Purpose of office alarm system
- Office alarm system characteristics
- Alarm categories
- Audible and visual alarm indicators

Page 2

- Physical description of alarm equipment
- Functional description of alarm system
- Theory of operation
- Power restrictions
- Maintenance features.

1.02 Whenever this section is reissued, the reason for reissue will be given in this paragraph.

PURPOSE OF OFFICE ALARM SYSTEM

1.03 The purpose of this alarm system is to:

- Detect a trouble condition
- Sound an audible alarm
- Light lamps for visual guidance
- Provide a teletypewriter (TTY) output message to the responsible maintenance center.

An alarm may be generated from hardware- or software-detected troubles. The alarm system will sound an audible alarm, light lamps, and initiate the printing of an output message with each alarm.

OFFICE ALARM SYSTEM CHARACTERISTICS

1.04 The No. 1 (Centrex 7 or later) and No. 1A ESS have a trilevel (critical, major, minor) alarm system. In addition to this trilevel system that is activated by either software or hardware (equipment) alarms, the office alarm system includes existing power major, power minor, and alarm battery supply alarms. Alarm responsibilities for the No. 1 or No. 1A ESS may be assigned to the switching control center system (SCCS) in the event that the central office is unattended. During unattended operation, all alarm information is transmitted to a remote TTY at a distant maintenance center. When transferred, audible and visual alarms are simultaneously activated in both the attended and unattended areas unless silenced in the unattended area. Associated output messages are sent to both areas.

Office Alarm System Description / #1A ESS

ISS 1, SECTION 231-035-000

ALARM CATEGORIES

1.05 The trilevel alarm system activated by the system software and hardware is categorized and described as follows.

- Critical (CR)—Activated when trouble condition affects call processing. Software or hardware activated.
- Major (MJ)—Activated when a trouble condition exists that, if not already affecting call processing, could do so. Software or hardware activated.
- Minor (MN) Spurt—Activated when an output message has been generated concerning a trouble condition that is not affecting call processing. This alarm is activated by software only and is self-retiring after approximately five seconds.
- Power Major (PMJ)—Activated when a trouble condition exists in the power supply equipment which affects or could affect call processing. Activated by hardware only.
- Power Minor (PMN)—Activated when a trouble condition exists in the power supply equipment and does not affect call processing. Activated by hardware only.
- Alarm Battery Supply (ABS)—Activated when a trouble condition occurs in the office alarm battery supply circuit. Activated by hardware only.

1.06 Alarm grouping options to alarm circuits on the same or adjacent floor are as follows:

- Preceding audible and visual alarm circuit
- No. 5 Crossbar system alarm circuit
- Preceding or adjacent to other system alarm circuit.

Grouping with a foreign alarm system other than No. 1 or No. 1A ESS office alarm system is activated manually by the AG (alarm grouping) key provided with the main exit pilot lamp unit. This unit is located at the main exit door. This grouping is limited by the system hardware. Grouping

between work centers is activated by a TTY message and is controlled by the system software.

1.07 Another feature of the office alarm system is the ability to accept alarms from common system frames (frames other than No. 1 or No. 1A ESS).

AUDIBLE AND VISUAL ALARM INDICATORS

1.08 Six distinct audible signals are provided in the office alarm circuit (Table A):

- (a) Critical alarm—tone bar (two tones per cycle)
- (b) Major alarm—tone bar (one tone per cycle)
- (c) Minor alarm and minor power alarm—loud ringing subset
- (d) Major power alarm—loud bell
- (e) Alarm battery alarm—loud ringing subset
- (f) Single stroke bell for code signaling (optional).

1.09 These signaling devices are arranged on a wall-mounted panel with provisions for four such panels per floor of ESS equipment, including the power and/or engine room.

1.10 Visual signals are provided by four distinct sets of lamps as follows:

- (a) Two red and one yellow lamp at the MCC to indicate that a system (program) detected and initiated critical, major, or minor alarm has occurred. A key is associated with each lamp to extinguish it and retire the corresponding system initiated audible alarm.
- (b) A red pilot lamp in the end guard at one or both ends of each equipment lineup. This indicates a critical/major locally detected trouble in that equipment aisle.
- (c) A red, a yellow, and a green pilot lamp in the end guard at one or both ends of each main cross aisle. The red pilot lamp (main aisle pilot) indicates a critical/major locally detected trouble in this cross aisle. The yellow and the green pilot lamps indicate critical/major or minor alarms, respectively, in some adjacent area (other

Page 3

Office Alarm System Description / #1A ESS

SECTION 231-035-000

TABLE A
NO. 1 AND NO. 1A ESS AUDIBLE
AND VISUAL ALARMS

ALARM DESIGNATION	HOW DETECTED	HOW REPORTED	AUDIBLE SIGNAL
Critical System Detected	System Diagnosis	Audible Only	Tone Bar (2 tones per cycle)
Major System Detected	System Diagnosis or Scan Points	Audible Only	Tone Bar (1 tone per cycle)
MCC System Detected	System Diagnosis or Scan Points	Audible and Visual	Tone Bar (1 tone per cycle)
Minor Switchroom	Dedicated Scan Points, Program, or Frame Location Scan Points	Audible Only	Loud Ringing Subset
Major Locally Detected (Fuse Alarm)	Contact Closure to Office Alarm circuit plus Frame Location Scan Points	Audible and Visual	Tone Bar (1 tone per cycle)
Major Power	Contact Closure to Office Alarm Circuit	Audible Plus Exit Pilots Indicating Power Room	PF Bell
Minor Power	Contact Closure to Office Alarm Circuit	Audible Plus Exit Pilots Indicating Power Room	Loud Ringing Subset

floor) of a multifloored office when the alarms are grouped together (interconnected).

(d) Yellow exit pilot lamps over each main exit door of a multifloored office. These lamps are arranged vertically, one lamp representing each floor in order, including the basement if the power equipment is located there. On each floor, the lamp cap representing that floor is stenciled THIS FLOOR. A critical alarm, major alarm, minor alarm, major power alarm, or minor power alarm will light the exit pilot lamp representing this floor on all other floors. In addition, an alarm battery alarm on the floor containing the alarm circuit will light the exit pilot lamp representing that floor on all other floors if the fuse that failed is not the one powering the exit pilot lamps.

(e) For partially attended operation (maintenance personnel is same multioffice building but not necessary in area of ESS), an alarm grouping key and associated pilot lamp are located at the main exit door. If the ESS power area is not part of the switchroom a MULT key and associated pilot lamp provide the alarm grouping to the power area.

(f) For unattended operation (maintenance personnel at some remote location), an alarm transfer pilot is located at the main exit.

1.11 Typical office arrangement options for No. 1 or No. 1A ESS are given in Table B and C.

1.12 Listed below are the abbreviations used in this section.

Office Alarm System Description / #1A ESS

ISS 1, SECTION 231-035-000

ESS—electronic switching system

MCC—maintenance control center

SCCS—switching control center system

TTY—teletypewriter

2. PHYSICAL DESCRIPTION

OFFICE ALARM SYSTEM

2.01 An office alarm system consists of various J units located on the miscellaneous power frame as indicated in Fig. 1. The frame is 2 feet 2 inches wide by 7 feet high.

AISLE PILOT CONTROL UNIT

2.02 The aisle pilot control unit (Fig. 2) contains four terminal strips and one relay for each equipment aisle to a maximum of 16. These components are mounted on a 2- by 25-inch mounting plate. Space is provided in the miscellaneous power frame for a second aisle pilot control unit.

FLOOR ALARM CONTROL UNIT

2.03 The floor alarm control unit (Fig. 3) contains seven relays and three terminal strips mounted on a 2- by 25-inch mounting plate. One unit is required for each floor of ESS equipment.

POWER ALARM CONTROL UNIT

2.04 The power alarm control unit (Fig. 4) contains seven relays and four terminal strips mounted on a 2- by 25-inch mounting plate. One unit is required for each power area.

ALARM BATTERY SUPPLY CONTROL UNIT

2.05 The alarm battery supply control unit (Fig. 5) contains eight relays, two terminal strips, and an ABS AUD ALM lamp/key. One unit is supplied for each building alarm group (set consisting of all ESS floors between which alarms may be grouped).

ALARM GROUPING CONTROL UNIT

2.06 The alarm grouping control unit (Fig. 6) contains 11 relays and 4 terminal strips

TABLE B

TYPICAL OFFICE ARRANGEMENT OPTIONS
FOR NO. 1 OR NO. 1A ESS
(ONE BUILDING FLOOR)

EQUIPMENT ARRANGEMENT	OPTION			
	Y	Z	W-Z	X
Switching Equipment on floor is ESS exclusively - - -	X	X	X	X
Power room is on same floor	X			
Power room is not on same floor		X	X	X
Power alarms are supervised in area of ESS - - - -	X	X	X	
Power alarms are not supervised in area of ESS - - - -				X
Adjacent floors have non-ESS office alarm circuits - - -	X	X	X	X
ABS fuses are located on this floor	X	X	X	X
Major audible alarm circuit provided			X	

Office Alarm System Description / #1A ESS

SECTION 231-035-000

TABLE C
TYPICAL OFFICE ARRANGEMENT OPTIONS
FOR
THREE NO. 1 OR NO. 1A ESS FLOORS AND
POWER ROOM IN BUILDING

EQUIPMENT ARRANGEMENT	OPTION	
	Z MCC ON FLOOR A ONLY	Z ONE MCC OR MTCE/FLOOR
Power alarms are supervised from floor A ----	X	X
ABS fuses are located on floor A	X	X
Floor C is top floor	X	X
One MCC or MTC located on each floor ---		X
MCC on floor A only	X	
One power plant powers all three floors ----		X

mounted on two 2- by 25-inch mounting plates. These units are supplied on the basis of one unit per two adjacent non-ESS areas to which alarm grouping is required.

CRITICAL ALARM UNIT

2.07 The critical alarm unit (Fig. 7) contains five relays and two terminal strips mounted on 2- by 25-inch mounting plate.

MISCELLANEOUS ALARM UNITS

2.08 Miscellaneous alarm units are used for audible and visual indications of alarms. These units will vary slightly with each office installation to provide the flexibility needed for single or multifloor offices and different floor layouts. The following are part of the miscellaneous alarm unit installation.

- Main aisle pilot lamp assembly
- Aisle pilot lamp assembly
- Exit pilot lamp unit (for single floor office)
- Exit pilot lamp unit (for multifloor office)

- Audible alarm panel.

Main Aisle Pilot Lamp Assembly

2.09 The main aisle pilot lamp assembly (Fig. 8) is generally mounted on the side edge of the door of the end guard to face the maintenance aisle. Three lamps are furnished for main aisle alarm indications. The lamps have red, yellow, and green lenses for indicating, respectively, a critical/major alarm in the main aisle, major, and minor alarms in other areas on the same floor or on other floors.

Aisle Pilot Lamp Assembly

2.10 The aisle pilot lamp assembly (Fig. 9) contains a light assembly with a red lens. The unit is mounted on the face side of the door for indicating a critical/major locally detected alarm in that equipment aisle.

Exit Pilot Lamp Unit (For Single Floor Office)

2.11 The exit pilot lamp unit (Fig. 10) is a dual lamp arrangement for a single floor ESS installation. This unit contains an exit pilot lamp

Office Alarm System Description / #1A ESS

ISS 1, SECTION 231-035-000

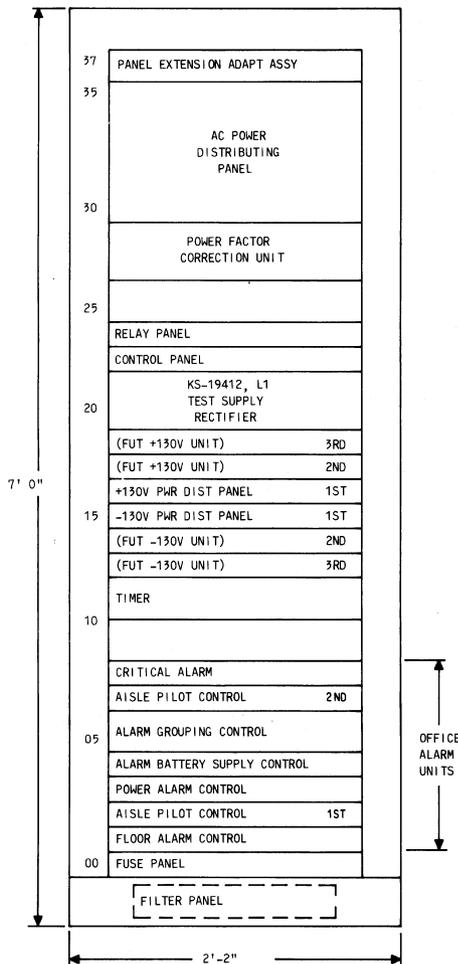


Fig. 1—Miscellaneous Power Frame with Office Alarm Units

and an alarm transfer lamp. The exit pilot lamp is mounted at the main exit door of the office.

Exit Pilot Lamp Unit (For Multifloor Office)

2.12 The exit pilot lamp unit (Fig. 11) is a five-lamp unit for a multifloored office. This unit contains an alarm transfer lamp (white), three exit pilot lamps (yellow), an alarm grouping lamp (white) for partially attended operation, and an alarm grouping key. If the ESS power area is not part of the switchroom, a MULT key and associated MULT pilot lamp provide the alarm grouping to the power area. The exit pilot lamp unit is mounted at the main exit door of the ESS office and the unit with the MULT key and associated MULT pilot lamp is located at the exit of the power room.

Audible Alarm Panel

2.13 The audible alarm panel (Fig. 12) is a wall-mounted unit that contains a tone bar (chime signal) for critical/major alarms, two ringing subsets (one for alarm battery and one for minor alarms), a signal bell for power failures, and an optional signal bell for code signaling.

3. FUNCTIONAL DESCRIPTION

OFFICE ALARM SYSTEM

3.01 Functions of the office alarm system are to provide the audible and visual indications used in an ESS office to report critical, major and minor office alarms, major and minor power alarms, and alarm battery alarms in both switchroom and power areas. Figure 13 is a block diagram of the office alarm system.

3.02 The No. 1 or No. 1A ESS recognizes alarm conditions and initiates alarms. The system is capable of recognizing certain internal trouble conditions and reporting the existence of such conditions via audible and/or visual indicators of the office alarm circuit, and providing trouble location information via the TTY. Negative 48 volts is the main power in the office alarm system and is supplied through frame fuses.

Office Alarm System Description / #1A ESS

SECTION 231-035-000

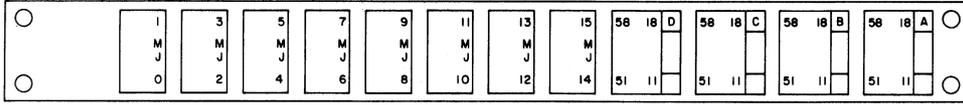


Fig. 2—Aisle Pilot Control Unit

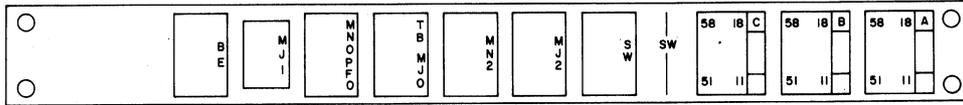


Fig. 3—Floor Alarm Control Unit

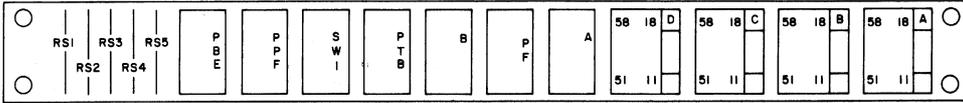


Fig. 4—Power Alarm Control Unit

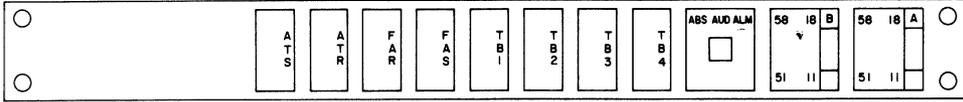


Fig. 5—Alarm Battery Supply Control Unit

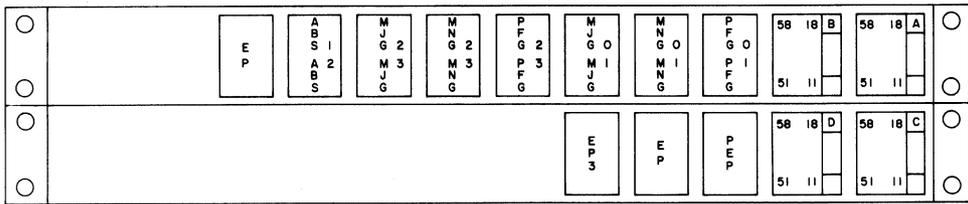


Fig. 6—Alarm Grouping Control Unit

Office Alarm System Description / #1A ESS

ISS 1, SECTION 231-035-000

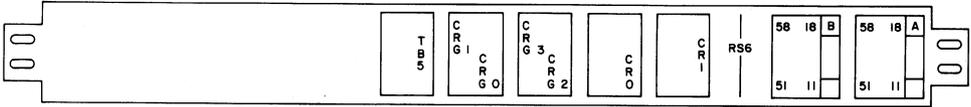


Fig. 7—Critical Alarm Unit

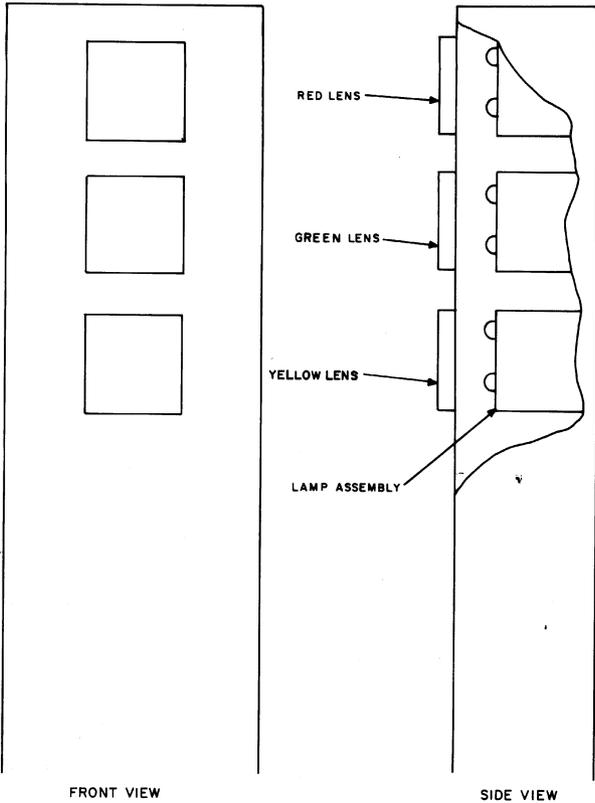


Fig. 8—Main Aisle Pilot Lamp Assembly

Office Alarm System Description / #1A ESS

SECTION 231-035-000

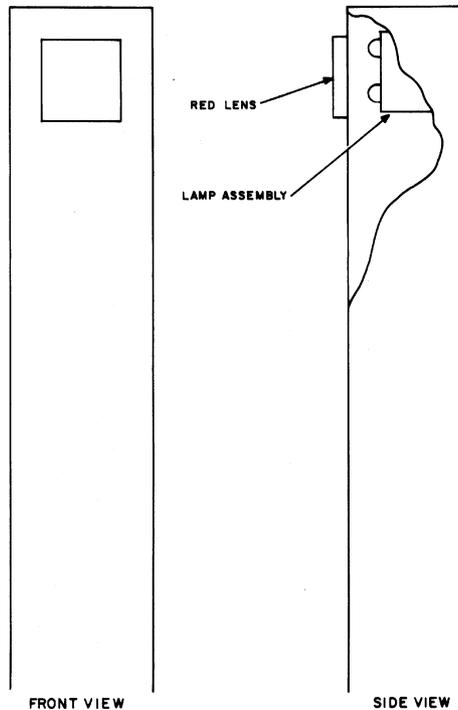


Fig. 9—Aisle Pilot Lamp Assembly

3.03 Other types of trouble, such as fuse alarms, which the system is unable to detect by self-diagnosis, are reported directly to the office alarm circuit by a relay contact closure or by a power control switch on the frame housing the equipment in which the trouble originates.

3.04 Trouble conditions are indicated by a distinctive audible signal and the frame in question is identified by a system of pilot lights. In addition, the location of the trouble frame or the type of the trouble is also reported directly to the system via MCC or master scanner scan points associated with the frame. The scan points initiate messages on the TTY providing a record of the trouble and identifying the frame or type of frame at a remote location if the office is unattended.

Output messages indicate blown fuses. Refer to the output message manual for the TTY message description.

3.05 The existence of a trouble condition in Non-ESS equipment is reported by the "AR01 MISC ALM IDLD SPL....." TTY message (SPL = special). The same message is used to report: (1) building alarms (BLDG), (2) carrier group alarms (CGA), (3) service alarms (SERV), and (4) toll alarms (TOLL). The building alarm message reports trouble with certain miscellaneous equipment within the building housing the No. 1 or 1A ESS.

(a) Monitoring the equipment high temperature indicators is an example of this type of trouble reporting.

Office Alarm System Description / #1A ESS

ISS 1, SECTION 231-035-000

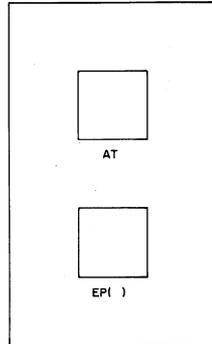


Fig. 10—Exit Pilot Lamp Unit (For Single Floor Office)

- (b) Trouble with the equipment that produces carrier signals, which are used for interoffice communication, is reported by printing the AR01 message with the CGA subfield.
- (c) The SERV subfield of the message is used to alert office personnel that a service alarm has been reported at an order wire and alarm panel.
- (d) The TOLL subfield indicates trouble with the equipment in the toll transmission facilities area of the switchroom.

AISLE PILOT CONTROL UNIT (FS 2, SD-1A158-01)

3.06 The function of the aisle pilot control unit is to light the aisle pilot lamps and main aisle pilot lamps associated with a specific equipment lineup. When a major alarm condition occurs in a frame, the relays on the panel that are associated with that particular equipment lineup operate by a contact closure on the frame associated with that aisle.

FLOOR ALARM CONTROL UNIT (FS 1)

3.07 The floor alarm control circuitry functions as an interface for the various office alarm

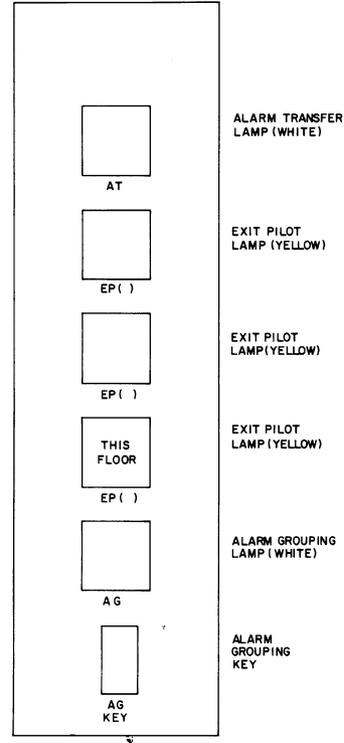


Fig. 11—Exit Pilot Lamp Unit (For Multifloor Office)

units and provides the control and logic functions of the office alarm circuit.

POWER ALARM CONTROL UNIT (FS 4)

3.08 The power alarm control unit monitors the power plants. It provides detection

Office Alarm System Description / #1A ESS

SECTION 231-035-000

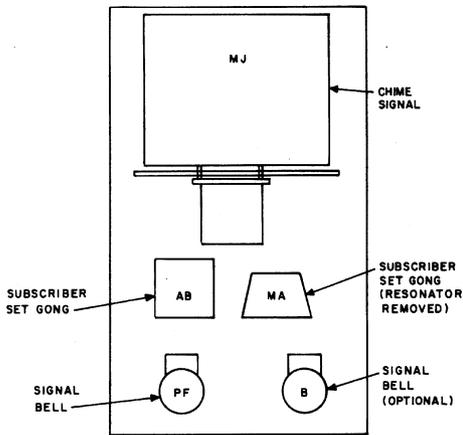


Fig. 12—Audible Alarm Panel

arrangements for power area alarms and relay control for audible signals in the power room not in the area of ESS switching equipment.

ALARM BATTERY SUPPLY CONTROL UNIT (FS 3)

3.09 The alarm battery supply control, interrupter, and alarm silencer circuitry provides the logic for reporting alarm battery failures and, in addition, provides interrupted -48 volts to operate the critical/major tone bar. This circuit also contains relays which operate when the office is unattended, silencing the audible signals and providing contact closures (or opens) as required to other circuits in the office.

ALARM GROUPING CONTROL UNIT (FS 11)

3.10 The alarm grouping control unit circuitry provides the transfer of alarm information between ESS and other switching systems on the same or adjacent floors via repeater relays.

CRITICAL ALARM UNIT (FS 1)

3.11 The critical alarm unit provides the relays for bringing up the critical alarm syncopated tone and alarm grouping. This panel houses components for the alarm battery supply control

unit, the alarm grouping control unit, and the power alarm control unit.

4. ALARM REPORTING

GENERAL

4.01 The office alarm system may be activated by software or hardware. Processor frames are equipped with power control switches; keys on the switches control the state of the frame. Two scan points in the MCC scan point matrix are assigned to each switch to monitor its state. A blown fuse is detected by the switch, and is reported to the system by a change in state of the scan points. The switch also activates directly the major alarm in the office alarm circuit. Peripheral frames are equipped with keys to control the status of the frame. Each frame is assigned master scan points so that the system can monitor the frames status. A blown fuse will be reported by a change in state of the scan points, which activates directly the major alarm in the office alarm circuit. Transmission type frames also activate the alarm system directly via relay contacts. Refer to Figure 14 for the functional block diagram of the office alarm system.

4.02 In addition to the visual indicators included in the office alarm circuit, supplementary visual indicators are contained in other ESS circuits as follows:

- (a) In each frame, there is a red POWER OFF pilot lamp which lights whenever power is removed from any circuit in the frame by operation of a POWER OFF key, or operation of a fuse in that frame.
- (b) On the MCC control and display panel, there are three red lamps which indicate the presence of a system-detected minor, critical, or major alarm condition in the office.

ALARM REPORTING—MULTIFLOOR OFFICE

4.03 To simplify the explanation in the following description of alarm reporting in a multifloor office, it is assumed that the floor under discussion is some intermediate floor in a multifloored office, with power equipment in the basement and with alarm grouping arrangements between adjacent floors. It is also assumed that the floor under

Office Alarm System Description / #1A ESS

ISS 1, SECTION 231-035-000

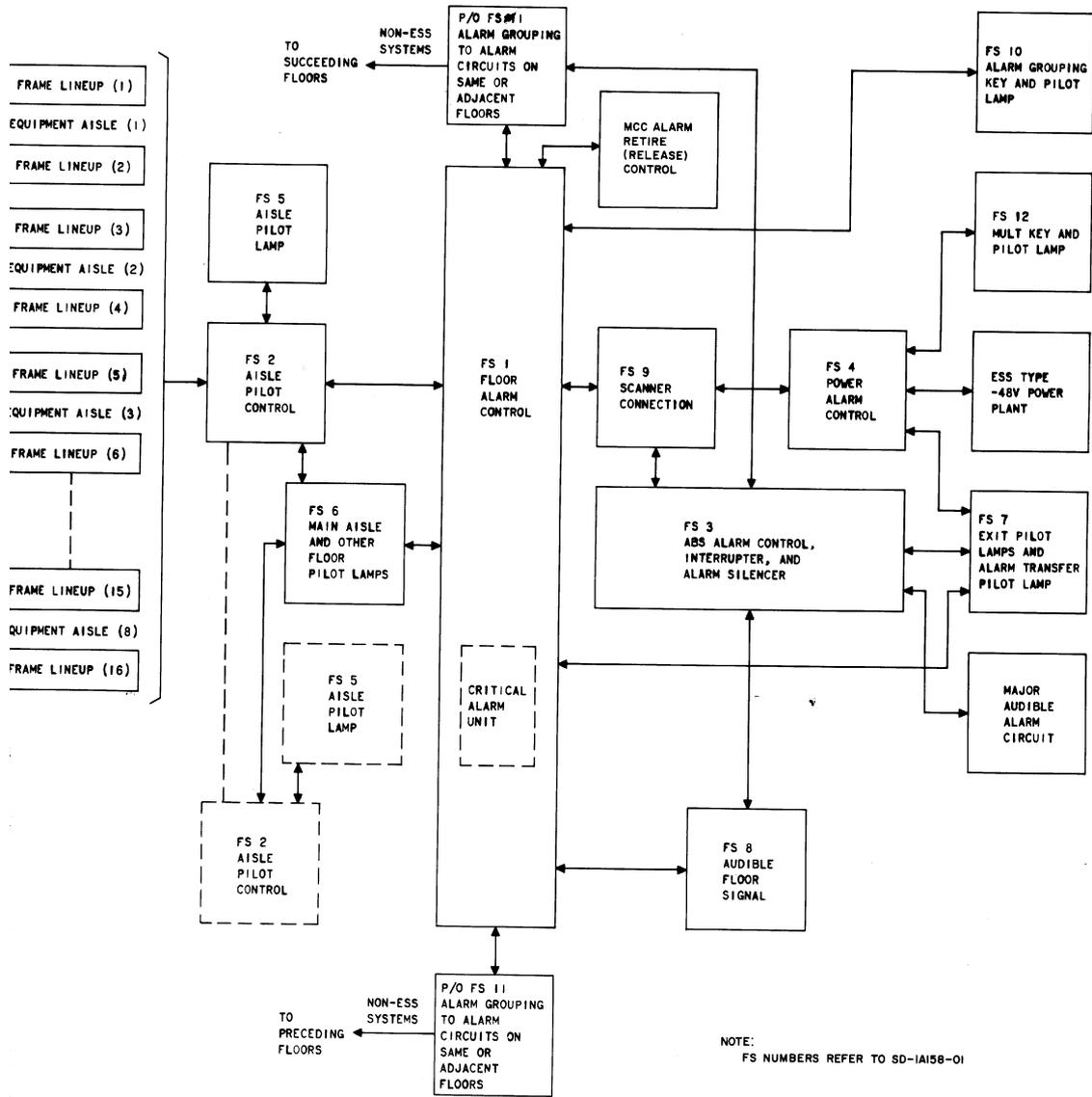


Fig. 13—No. 1 or No. 1A ESS Office Alarm System Block Diagram

Office Alarm System Description / #1A ESS

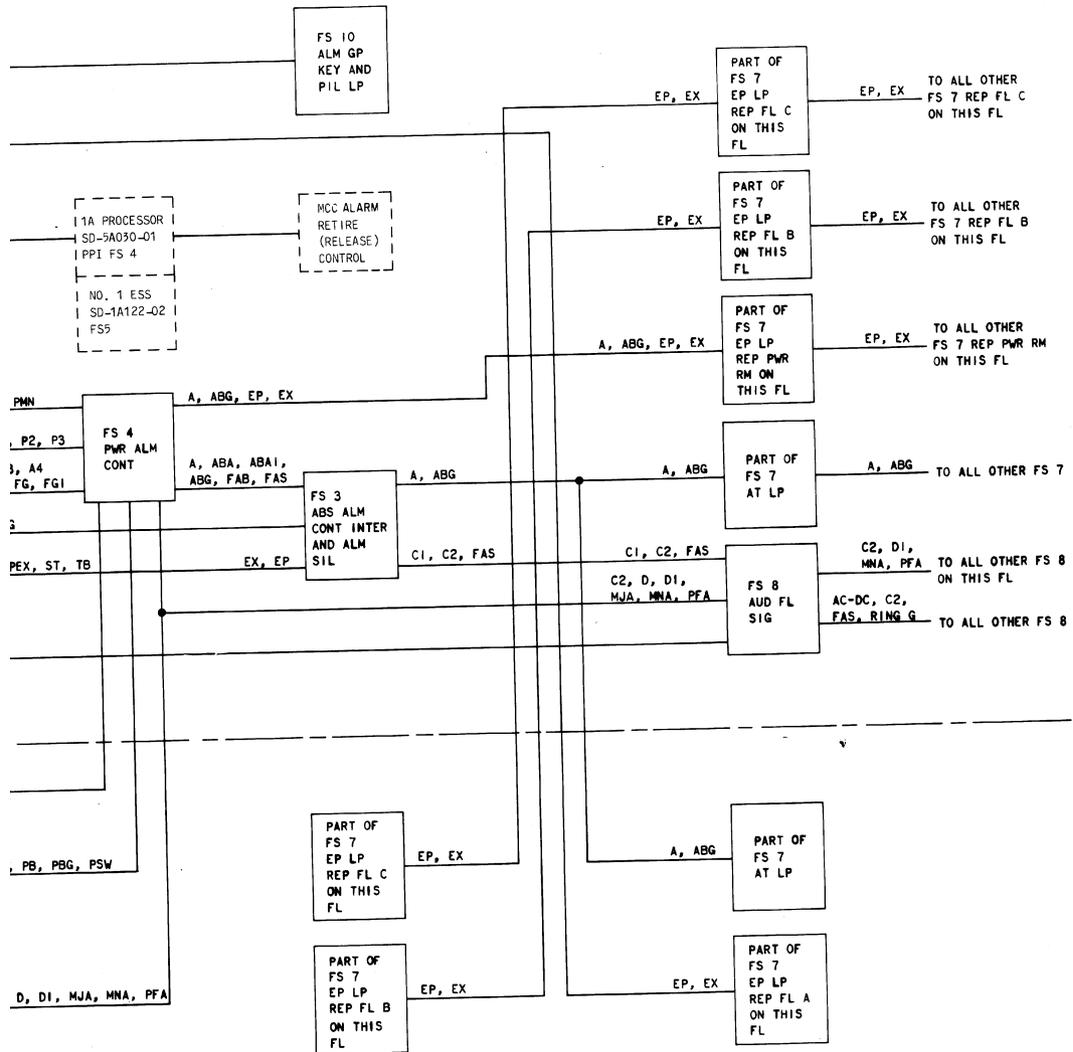


Fig. 14—No. 1 or No. 1A ESS Office Alarm System
Functional Block Diagram

Office Alarm System Description / #1A ESS

ISS 1, SECTION 231-035-000

discussion is the only floor containing ESS equipment associated with the MCC on that floor.

4.04 When a blown fuse occurs at a frame, the red POWER OFF lamp at the frame lights and a signal is placed in the office alarm circuit. This will cause the aisle pilot lamp for this aisle to light, the main aisle pilot lamp for this cross aisle to light, an audible signal to be given on this floor, and the exit pilot lamps for this floor to light on all other floors. Lighting the other floor lamps and giving audible signals on other floors is optional and depends on whether or not the alarm grouping key on each floor has been operated. When this key has been operated on any one floor, a trouble on that floor will light the other floor lamps on the succeeding floor and will sound the audible alarm on the succeeding floor. Conversely, a trouble on the succeeding floor will light the other floor lamps and sound the audible alarm on the first mentioned floor. With all the alarm grouping keys operated, the maintenance personnel on any floor other than the one from which the alarm originates, will be alerted by the audible signal, note the other floor lamp lighted, and find the floor with the alarm by noting which exit pilot lamp is lighted. The exit pilot lamps are arranged in a column with one lamp for each floor, top lamp for top floor, etc. On each floor, the lamp cap representing that floor is stenciled "THIS FLOOR." The correct floor is indicated by the relative position of the lighted lamp to THIS FLOOR lamp. Once on the floor on which the trouble is located, the main aisle pilot lamps and aisle pilot lamps will indicate the proper aisle, and the lighted POWER OFF lamp on the frame will indicate the equipment causing the alarm. The aisle pilot lamps and the audible alarm signal may be retired on most frames by operating a pushbutton on the frame originating the alarm. The individual frame POWER OFF lamp will remain lighted however, to indicate the alarm condition still exists. Operating the MCC ALARM RETIRE key will not retire this alarm. Replacing the blown fuse will retire the alarm.

4.05 A critical alarm is detected by the system through maintenance or diagnostic routines. The repeated PC (Processor Configuration Circuit) state also triggers a critical alarm. The system then lights the MCC critical alarm lamp and places a critical alarm signal in the office alarm circuit, which sounds the tone bar in a syncopated manner, lights the exit pilot lamp representing this floor

on all other floors, and, under the control of the alarm grouping key, lights the major other floor lamps, and sounds the critical/major tone bar on the other floor. The alarm may be retired with the ALARM RETIRE key at the MCC.

4.06 When a system-detected major alarm occurs at a frame, it is detected by the system through diagnostic routine. The system then lights the MCC major alarm lamp and places a major alarm signal in the office alarm circuit, which sounds the major alarm tone bar (indicating that the TTY will provide further trouble location information), lights the exit pilot lamp representing this floor on all other floors, and, under control of the alarm grouping key, lights the major other floor lamps and sounds the major alarm tone bar on the other floors. The system-detected major alarm may be retired by operating the ALARM RETIRE key at the MCC.

4.07 When a minor alarm (all minor alarms are system-detected) occurs at a frame, it is detected by the system through change of state of the frame alarm scan points or through dedicated scan points. The system then lights the MCC minor alarm lamp and places a minor alarm in the office alarm circuit, which sounds the minor alarm audible signal (indicating that the TTY will provide trouble locating information), lights the exit pilot lamp representing this floor on all other floors, and, under control of the alarm grouping key, lights the minor other floor lamps and sounds the minor audible alarm signal on the other floors. The minor alarm may be retired by operating the ALARM RETIRE key in the MCC. (ALM RLS for No. 1 ESS MCC)

4.08 The power equipment in the power room is tied into the office alarm circuit such that major power alarms light the yellow other floor lamps, light the exit pilot lamps on all floors indicating the power room, and sound a distinctive power failure audible alarm on all floors under control of the alarm grouping keys. Minor power alarms will light the green other floor lamps on all floors and sound the regular minor audible alarm on the floor where power alarms are normally supervised. The exit pilot lamps representing the power room are lighted on all floors as for the major power alarm. When the grouping keys are operated, the minor power alarm audible signal will be transmitted to all floors.

Page 17

Office Alarm System Description / #1A ESS

SECTION 231-035-000

4.09 The MULT key and pilot lamp in the power area serve the same functions as the ALARM GROUPING key and pilot lamp associated with switching floors, except that operation of this key accomplishes grouping between the power room and the ESS floor from which power alarms are normally supervised. In the case where power equipment is not in a separate power room but is sharing a floor with switchroom equipment, connection to the office alarm circuit is such that major power alarms sound the distinctive power failure audible alarm on all floors and light the yellow other floor lamps on all other floors, whether or not the grouping keys are operated. A regular major office alarm is also signaled which lights the appropriate aisle pilot lamps on the floor with the power equipment and lights the exit pilot lamps for this floor on all other floors. The regular major audible alarm is also operated on this floor. Minor power alarms are signaled as regular minor office alarms and sound the regular minor audible alarm. The regular major and minor audible alarm signals can be transmitted to all floors by operation of the grouping keys.

4.10 The office alarm circuit also contains alarms to indicate a failure in the battery supply that powers the alarm circuits themselves. A failure in any one of the fuses that supply the alarm circuit will cause the exit pilot lamps for the floor on which the alarm circuit fuses are located to light on all other floors (if the fuse that powers these lamps was not the one that failed). The yellow other floor lamps will light on all other floors, and a distinctive audible signal will sound on all floors whether or not the grouping keys are operated. A failure of the power room fuse, which powers the power alarm circuit, lights the exit pilot lamps for the power room, lights the yellow other floor pilot lamps on all floors, and sounds the same distinctive audible signal on all floors whether or not the grouping keys are operated. A failure in the fuse which powers the power alarm circuit for power equipment on a floor with switchroom equipment is signaled to adjacent areas as an alarm battery for that floor. A loss of the -48 volt battery to the alarm circuit for any reason (failure of the charge-discharge fuse, open or shorted cable) will cause the same distinctive audible signal to sound on all floors. No lamps can be lighted in this case, however, since no power is available. (The distinctive audible signal for failures in the alarm circuit is powered by the 20-cycle ac-dc continuous ringing supply.)

4.11 When fully unattended operation is desired, a contact closure from the signal distributor applique circuit or contact closures from the peripheral decoder applique circuit operate relays in the office alarm circuit, silencing the audible signals, lighting the alarm transfer pilot lamp, and providing contact closures and opens required by other circuits in the office when the office is unattended. During the unattended operation, the local maintenance TTY continues to provide a record of alarms and trouble location information and, in addition, all alarm information is transmitted to a remote TTY at a distant maintenance center.

ALARM REPORTING—MULTIFLOOR OFFICE (SAME MCC OR MAINTENANCE CENTER)

4.12 When adjacent floors contain ESS equipment under control of the same MCC, major locally detected alarms and MCC system-detected alarms are reported as described in 4.04. However, under these circumstances, each floor is provided with maintenance TTY. Consequently, a system-detected critical or major alarm or a minor alarm is reported by simply multiplying the respective audible signals on each floor. This indicates that the nearest TTY will provide further identification and location information.

5. POWER

5.01 The feeders supplying the miscellaneous units on the miscellaneous frames and on the miscellaneous power frames may be any of the following combinations:

- Two -48 volts feeders with two filters
- One -48 volts feeder with two filters
- One -48 volts feeder with one filter
- One -48 volts and one +24 volts feeder with two filters.

5.02 Feeders supplying the office alarm circuits bypass the power distribution frame and come directly from the charge and discharge at the power plant. The feeders should be fused at 20 amperes.

Office Alarm System Description / #1A ESS

ISS 1, SECTION 231-035-000

6. MAINTENANCE

6.01 Testing and troubleshooting procedures for office alarm circuitry are provided by task oriented practices.

SECTION

231-301-000

TITLE

Processor Peripheral Interface Frame and Control and Display Frame Description—2-wire No. 1A Electronic Switching System

7. REFERENCES

7.01 The following list provides the number and title of related documents.

231-301-001

Processor Peripheral Interface Frame and Control and Display Frame Theory—2-wire No. 1A Electronic Switching System

SECTION

TITLE

231-125-301

966-120-100

2-wire No. 1A Electronic Switching System—General Description

Master Control Center Alarm, Display, and Control Panel Method of Operation—2-Wire No. 1 Electronic Switching System

966-100-100

2-Wire No. 1 Electronic Switching System—General Description

201-400-100

Switching Control Center System—Overall Description

Improvised Ceramic Weapons

Overview

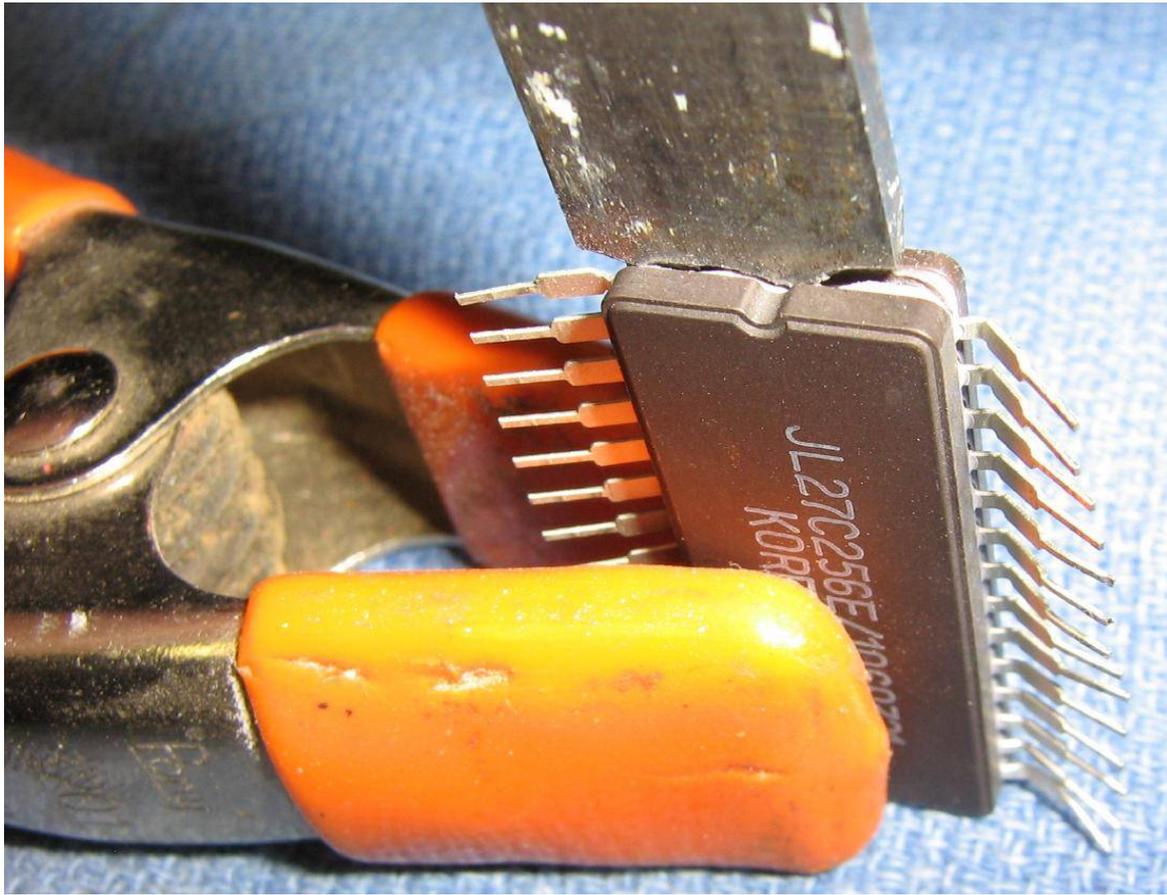
It appears that every place you travel today has banned most forms of self-defense weapons. Instead of just banning shit-skins and Muslims from the country, these "security" personal spend all their time harassing little old ladies and hard-working white farmers from the midwest. This makes *no sense* to anyone with even half a brain. But that's what you'd expect when you place "diversity & multiculturalism" ahead of basic logic.

You can fight back though! It's possible to create simple, improvised ceramic weapons from the high-grade ceramic packages used in manufacturing "military grade" integrated circuits. Ceramic ICs (CerDIP), such as old EPROMs, are very easy to find at ham radio and used electronics swap fests. Look for old circuit boards from telecom giants, like AT&T, and use a hot air gun to remove them. You'll then use Dremel "diamond" cut-off wheels and grinding stones to shape the ceramic pieces into small improvised weapons which will have the ability to pass through a metal detector. Other possibilities for using the ceramics are for making high-voltage insulators, or even for making certain "parts" which you don't want setting off a metal detector.

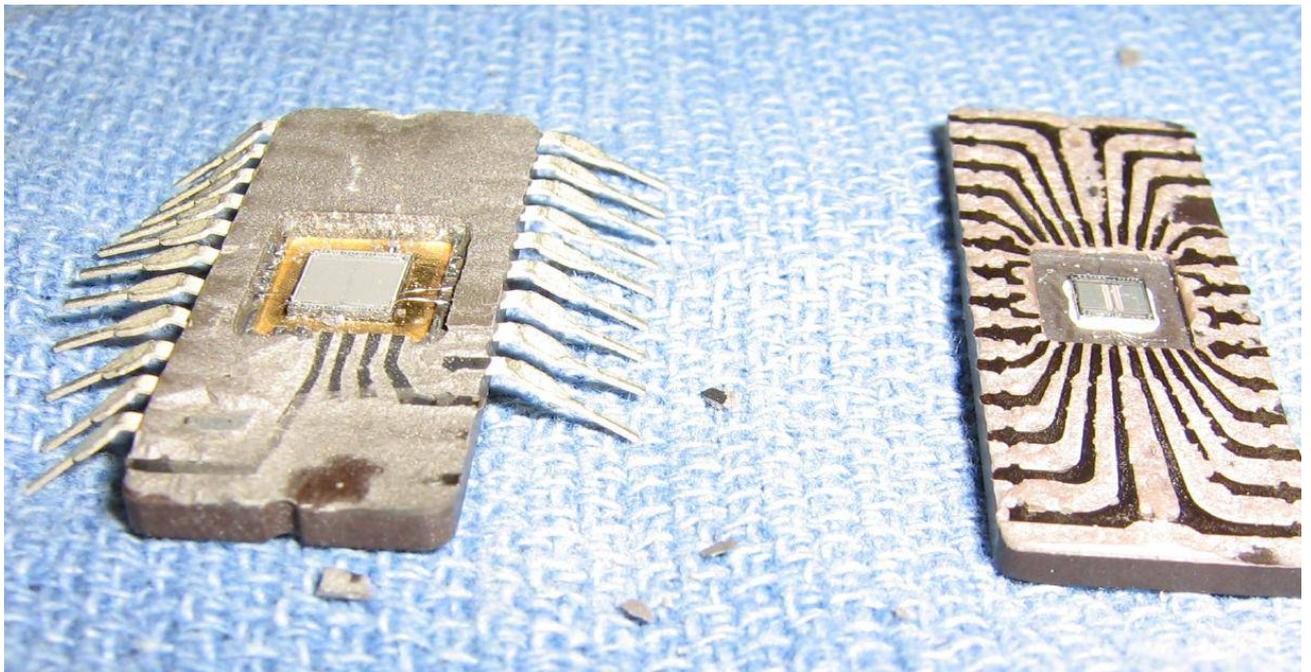
Construction Notes & Pictures



What you'll need. Several ceramic packaged DIP integrated circuits and a Dremel tool with some diamond cut-off wheels and grinding bits. The cut-off wheels shown above are from Harbor Freight Tools, part #31501. The other diamond grinding bits are part #40547.



Use a padded spring clamp and a chisel to separate the two halves of the ceramic IC package. The spring clamp "gives" a little bit, and helps to prevent cracking the ceramic halves.



Clean up the ceramic halves by pulling off the metal leads. You may wish to use an angle grinder to further clean up the ceramic pieces.



Take one of the ceramic halves and begin to grind a pattern that resembles something like a knife edge or some other type of stabbing weapon.



Clean it up a bit so the final result is something like what is shown above. This ceramic edge is actually fairly sharp.

These will make great concealed cutting edges for weakening plastic hand cuffs.



Experimental ceramic arrowhead.

Anti-TASER Clothing Experiments

Overview

The following story takes place in a few years...

Your attending a political rally for some open borders, liberal traitor nutjob. Half way through the politician's rhetoric, you charge the podium with your improvised ceramic knife in hand – it passed through the metal detector security check with no problem. You get halfway to the traitor before one of their "security guards" fires his TASER X26C electronic control device at you. You smirk slightly as you see the bright yellow blast doors fly off the X26C. The two shock probes impact your body and you immediately wince in pain. A split-second later, you regain your thoughts, and quickly pull out each of the probes, individually, by their connecting wire. The security guards stand in awe as their shiny new barbecue grill lighter appears to have had no effect on you. Scared of getting shocked, the guards left you with just enough room to continue your mission towards the traitor's neck. You only have another split-second to react. You attack the traitor's neck and slash it wide open as you scream "open borders gets open head wounds!" at the top of your lungs. The open borders traitor is now laying on the floor in a pool of their own AIDs ridden blood. Eventually, you are wrestled to the ground and arrested. As you leave the building, a "news" reporter sticks their microphone in your face and asks "Do you have anything to say for yourself?" Your reply is quick, smug, and broadcast worldwide; "Eric Corley is a pedophile!"

It appears to be possible to defeat TASER electronic control devices (those stun guns shooter things) with a simple modification to your undergarments. Lining the inside of a T-shirt with an electrically conductive fabric allows you to "short out" the electrical shock from the two metal contact probes, or it will at least load down the high-voltage generator in the TASER device, resulting in an electrical shock that is not as intense as the standard 50,000 volts or so.

The good news is that this electrically conductive fabric is readily available. For this experiment, we'll be using the "High Performance Silver Mesh Fabric" from [Less EMF, Inc.](#), Catalog #A1222. This fabric is perfect for experimenting and is very easy to work with. The bad news is that this fabric is fairly expensive. Around \$15 a linear foot (54" wide). You'll probably need several layers of this material for this method to work "in real life." Also, the silver coating on the nylon fabric will wear off over a period of time and continuous use.

Construction is quite simple. Get an old, tight-fitting T-shirt (you'll want it to be snug against your body) and some 3M Super77, or similar, spary adhesive. Lay out the T-shirt and roughly fit the conductive fabric to match the contour of the shirt. Remove the conductive fabric and apply a good coat of the spray adhesive. Let the adhesive sit for a minute, or until it gets "tacky." Gently place the conductive fabric back onto the T-shirt, cautiously avoiding any tears or creases. Press the fabric down into the adhesive using an old rolling pin. You may wish to apply another coat of the spray adhesive or add additional layers of the conductive fabric. The finished shirt will have a "stiff" feel to it, though.

If using multiple pieces of conductive fabric, *they must all have a continous electrical connection!* This is a major requirement for this method to work. For example, if lining a pair of pants to protect your legs, there should be a wire (or another piece of fabric) connecting to the fabric on the torso area. The copper/metallic tape used for making stained glass windows can be useful for these applications.

Conductive Fabric Specifications

Less EMF, Inc. - High Performance Silver Mesh Fabric

Base Fabric : Knit Nylon
Substrate : Nylon
Weight : 40 g/m²
Temp. Range : -30° to 90° C
Metal Coating : Silver
Metal Purity : > 99%
Electrical Resistance : < 0.5 ohms/cm²

Wash in warm water, mild soap. No bleach. Air dry. Do not apply heat. Do not iron.

Helpful TASER Information

Here are some helpful little tidbits directly from a TASER manual:

- The bottom probe impacts at an 8° angle from the top probe. This results in a spread of approximately **one foot** for every **seven feet** of distance from the target. Greater probe spread increases the effectiveness. If possible, a minimum 4-inch spread between the probes is recommended.
- The current must pass between both probes. If one or both probes miss the subject, deploy a second cartridge if available. If one probe has made contact with the subject, using the drive-stun on any area of the body will complete the circuit and cause Neuromuscular Incapacitation (NMI). However, the charge effects will stop as soon as the TASER is moved away from the subject.
- If the probes impact in an area where there is very little muscle mass (e.g., the side of the rib cage), the effectiveness can be significantly diminished.
- Probe spreads of less than four inches (including drive-stun) result in little or no effect from NMI and become primarily a pain compliance option. If a close range deployment resulting in limited probe spread does not incapacitate the subject, apply a drive-stun, as described below, to a point away from the probes. This will effectively widen the contact area and can achieve NMI.
- Normally, aim the laser of the device at one of the large muscle groups (center of mass) such as the torso or thigh areas.

Construction Notes & Pictures



Overview of what's needed. An old T-shirt, some electrically conductive fabric, a good pair of scissors, some masking tape, and some spray adhesive.



Lay out the T-shirt on a surface which will not get ruined by the overspray from the spray adhesive. Stretch it out so there are no creases and secure it with some masking tape.



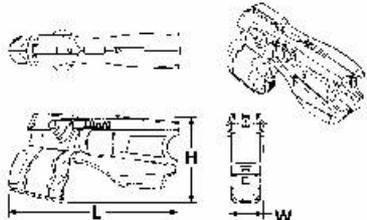
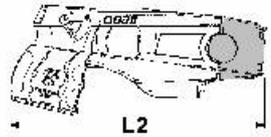
Before applying the spray adhesive, cut the conductive fabric so it fits the contours of the shirt. Remove the fabric and apply a good coating of the adhesive. Carefully reapply the conductive fabric, avoiding any creases. Press it down using a rolling pin.

(The upper corner was cut wrong on this example.)

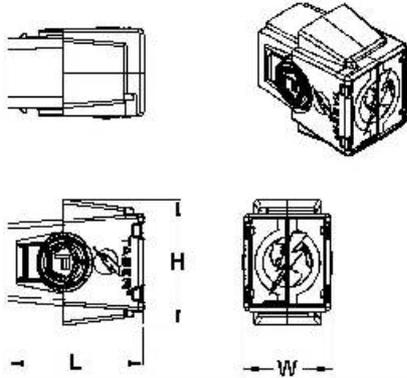
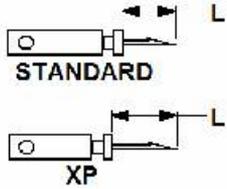


Conductivity test. With the probes about one foot apart, the meter is reading "2.1 Ohms."

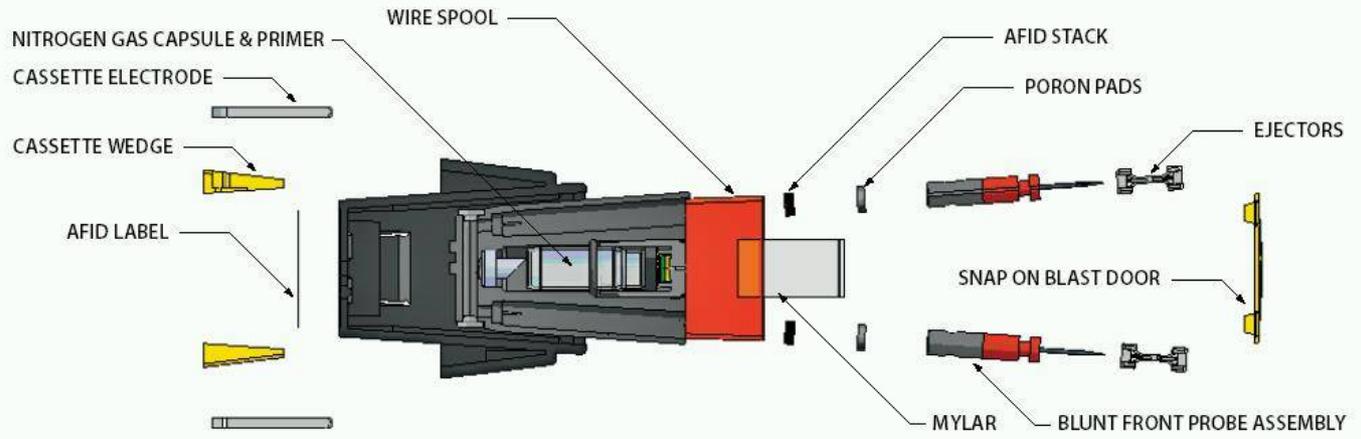
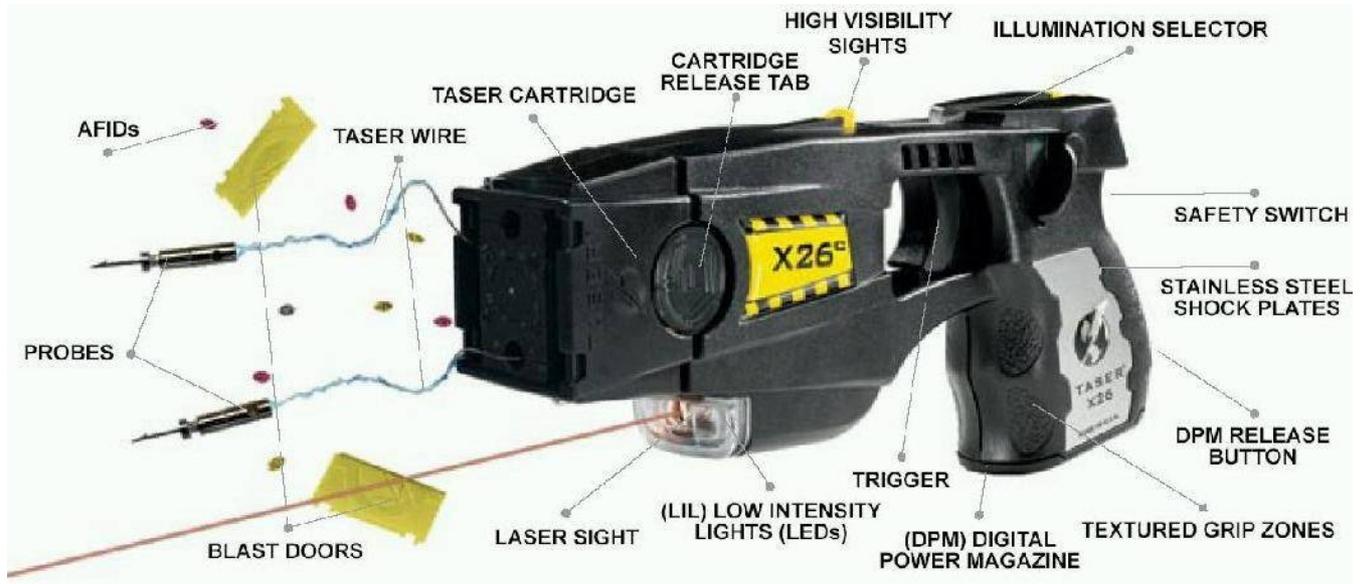
TASER X26C Series Electronic Control Device Specification

 X26C SERIES ELECTRONIC CONTROL DEVICE SPECIFICATION		 WARNING <small>Electronic Control Device Do not touch the electrical contacts or the battery pack. Do not use in rain or wet conditions.</small>			
Consumer Models					
Model	Model No.	Color	Magazine Type	Grip color/style	Holster
TASER® X26C	26010	Yellow	DPM	Metal	Soft Carry
TASER® X26C	26009	Black	DPM	Black	Soft Carry
TASER® X26C	26008	Clear	DPM	Black	Soft Carry
Specifications		Features			
<ol style="list-style-type: none"> Output characteristics¹: Wave form: Complex shaped pulse Pulse rate: 17 PPS for 2 seconds, 10 PPS thereafter for up to 30 seconds total Pulse duration: 100 microseconds The trigger activates a 10-second cycle. Second and third pull increments the cycle 10 seconds each up to 30 seconds total. Peak open circuit arcing voltage: 50,000 V Peak loaded voltage: 1,200 V Current: 1.9 mA average @ 17 PPS Energy per pulse: Nominal at main capacitors: 0.36 joules Delivered into load: 0.07 joules Power rating @ 17 PPS: Nominal at main capacitors: 6 watts Delivered into load: 1.2 watts Power Source: Digital Power Magazine (DPM)^{6,7} Temperature Range: -4 °F [-20°C] to 122 °F [50 °C] Relative humidity: 15% to 80% Housing: High impact polymer Patent: U.S. D508,277 D504,489 and other patents pending 		<ol style="list-style-type: none"> Integrated ultra-bright LED's (low intensity illumination). Integrated 650 nm laser (used for target acquisition). Capable of drive stun with or without TASER Cartridge installed. Electrical charge can penetrate up to 2" [5 cm] of clothing. Central Information Display (CID) 2 digit LED displays remaining DPM energy percentage, burst time, warranty expiration, unit temperature, illumination status and current time and date. Ambidextrous safety levers with Safe "S" and Fire "F" denotation. Warranty: 1-year standard, with extended warranties available.⁵ Video/Audio Recorder capable with optional TASER Cam™. 			
Physical Dimensions¹					
Dimensions (Without Cartridge)				Dimensions (With Cartridge) ²	
Length (L)	Height (H)	Width (W)	Weight	Length (L2)	
6.00" [15.24 cm]	3.20" [8.13 cm]	1.300 [3.30 cm]	7.20 oz [204.12 g]	7.250" [18.52 cm]	
					
<ol style="list-style-type: none"> Dimensions are in English [metric]. For additional cartridges contact TASER International sales representative. TASER Cartridges available only in 15' [4.57 m] range. Use of cartridges not authorized by TASER International will void the product warranty. Product specification may change without notice; actual product may vary from picture. Additional terms and conditions may apply (for additional information contact a TASER International sales representative or visit online at: www.TASER.com for additional details.) Material Safety Data Sheets (MSDS) concerning lithium batteries available upon request. Output specifications may vary dependant upon temperature, battery charge and load characteristics. Additional models available. Please contact a TASER International sales representative for more information. TASER is a registered trademark of TASER International, Inc. All rights reserved. 					

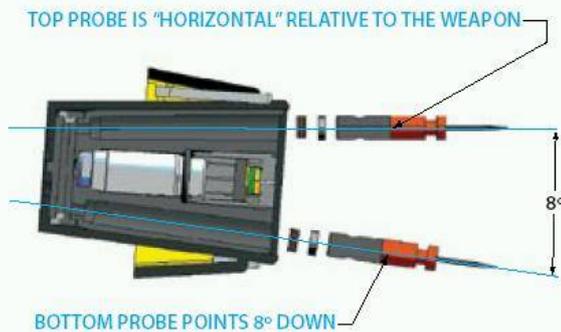
TASER Cartridge Specification

		<h2>TASER® Cartridge Specification</h2>					WARNING <small>Electronic Control Device "TASER" is a registered trademark of TASER International, Inc. © 2006 TASER International, Inc. All rights reserved. For more information, visit www.taser.com</small>	
Models								
Model	Model No.	Propellant	Range ²	Door/Wedge Color				
TASER® Cartridge 15'	34200	Compressed Nitrogen ⁴	15' [4.57 m]	Yellow				
TASER® Cartridge 21'	44200	Compressed Nitrogen ⁴	21' [6.40 m]	Silver				
TASER® Cartridge 25' XP	44203	Compressed Nitrogen ⁴	25' [7.62 m]	Green				
Specifications⁶				Features				
1. Shelf life: 5 years 2. Housing: High impact black polymer 3. Patent: U.S. 5,078,117				1. Reversible cartridge installation. 2. Anti-Felon Identification (AFID) tracking system with serialized microdots. 3. Drive stun capability (when attached to TASER electronic control device).				
Dart Grouping^{1,5}								
Model	Dart	3.3' [1 m]	9.8' [3 m]	13.8' [4.2 m]	20' [6.1 m]	24' [7.3 m]	29.9' [9.1 m]	34.8' [10.6 m]
34200 15'	Top	2.15" [5.5 cm]	2.48" [6.3 cm]					
	Spread	2.18" [5.5 cm]	18.10" [46 cm]					
44200 21'	Top	2.15" [5.5 cm]	2.48" [6.3 cm]	1.18" [3 cm]	-1.74" [-4.4 cm]			
	Spread	2.18" [5.5 cm]	18.10" [46 cm]	24.02" [61 cm]	34.02" [86.4 cm]			
44203 25'	Top	1.85" [4.7 cm]	0.68" [16.6 cm]	-0.13" [-0.33 cm]	-3.63" [-9.2 cm]	-7.80" [-19.8 cm]		
	Spread	6.53" [16.6 cm]	15.88" [40.3 cm]	23.10" [58.7 cm]	29.14" [74 cm]	36.79" [93.4 cm]		
Physical Dimensions¹								
Cartridge				Probe				
Length (L)	Height (H)	Width (W)	Weight	Length of probe point (L)				
2.125" [5.40 cm]	1.890" [4.80 cm]	1.400" [3.57 cm]	2.4 oz [68.04 g]	Standard	0.375" [9.53 mm]			
				XP	0.525" [13.33 mm]			
								
1. Dimensions are in English [metric]. 2. Actual wire length may be up to 6" longer. 3. For training cartridges see TASER specification RD-SPEC-CRTG-002. 4. Material Safety Data Sheet (MSDS) related to nitrogen gas charged cartridges available upon request. 5. Dart grouping distances are averages measured in correlation to the laser dot projection at specified distance, test performed at ambient temperature [70 °F (25 °C)], results listed are averaged +/-0.50" [1.27 cm]. "Spread" is average measurement from top dart to bottom dart. 6. Product specification may change without notice; actual product may vary from picture. 7. Additional models available. Please contact a TASER International sales representative for more information. 8. TASER is a registered trademark of TASER International, Inc. All rights reserved.								

TASER X26C Overview



CARTRIDGE CUTAWAY



15' CARTRIDGE

Nortel DMS-100 Receiver Table (RECEIVER)

Table Name

Receiver Table

Functional Description of Table RECEIVER

Table RECEIVER contains the following information for each audio tone detector, DIGITONE, multifrequency receiver, and mechanized calling card service:

- The code assigned to the equipment in table CLLI.
- Analog equipment for COMMON or GATEWAY switching.
- Digital switching equipment.
- The equipment location of the circuit.
- The Product Engineering Code (PEC) of the receiver.

The pseudo-fixed codes in table CLLI for these circuits appear in the following table:

Pseudo-Fixed Codes

Title	Code	Code Applicability
DIGITONE Receiver	RCVRDGT	COMMON Switches
Multifrequency Receiver	RCVRMF	COMMON Switches
Mechanized Calling Card Receiver	RCVRMCCS	COMMON Switches
Audio Tone Detector	RCVRATD	COMMON Switches
DMS-300 DIGITONE Receiver	DGT300	GATEWAY Switches Only
DMS-300 Multifrequency Receiver	MF300	GATEWAY Switches Only
R2 Signaling	KSR2OCVR	For Licensee Use Only
R2 Signaling	KSR2ICVR	For Licensee Use Only
Automatic Toll Coin Service	RCVRCOIN	TOPS Switches Only
A-Law Automatic Tone Detector	RCVATDUK	U.K. Operating Companies Only
A-Law DIGITONE Receiver	RCVRDTUK	U.K. Operating Companies Only
Receiver Coin Detection Circuit	RCVRCDC	Restrictions Do Not Apply

-End-

The audio tone detector contains a trunk card with PEC NT5X29AC. The detector is an option for Integrated Business Network (IBN) switching units. Other types of switches do not require the detector.

Implementation of RCVRCOIN occurs on the NT3X08 card. Each NT3X08 card supports a maximum of eight RCVRCOIN circuits. For every NT3X08 card in the system, this table can contain a maximum of eight entries. Use card code 3X08AA for feature package NTX208AA (Automatic Coin Toll Service). Use card code 3X08AB for feature package NTX208AB.

Field CARDCODE indicates the PEC of the receiver. The different groups of CARDCODE, CLLI, and RCVRTYPE appear in the following table.

The RCVRKEY field accepts a receiver coin detection circuit in the range of values. The field accepts the circuit to determine the number of five-cent deposits collected on each call. Enter data in this field in table CLLI.

CARDCODE, CLLI, and RCVRTYPE Correlation

CARDCODE	CLLI	RCVRTYPE
2X48AA	MF300	Digital
2X48AA	RCVRMF	Digital
2X48AB	RCVRMCCS	Digital
2X48AB	RCVRDGT	Digital
2X48AB	DGT300	Digital
2X48CA	RCVRMF	Digital
2X48CB	RCVRDGT	Digital
2X48CC	RCVRDTUK	Digital
3X08AA	RCVRCOIN	Digital
3X08AB	RCVRCOIN	Digital
3X80AA	RCVRCDC	Digital
5X29AB	RCVRATD	Analog
5X29AC	RCVRATD	Digital
5X29BA	RCVATDUK	Digital

-End-

The maximum number of circuits of each type is 1,024.

The system allocates memory for the total number of circuits for the following fixed pseudo-codes. Field TRKGRSIZ in table CLLI indicates the total number of circuits.

- Code DGT300
- Code KSR2ICVR
- Code KSR2OCVR
- Code MF300
- Code RCVRATD
- Code RCVRDGT
- Code RCVRMCCS
- Code RCVRMF

Datafill Sequence & Table Size

You do not need to enter data in other tables before you enter data in table RECEIVER.

You can use data to increase table size. To increase table size, change field TRKGRSIZ in table CLLI for the following fixed pseudo-codes:

- Code DGT300
- Code KSR2ICVR
- Code KSR2OCVR
- Code MF300
- Code RCVRATD
- Code RCVRDGT
- Code RCVRMCCS
- Code RCVRMF

Activation

To allow datafill changes in table RECEIVER to activate:

- You can increase table size without a restart after you change the receiver data of fixed pseudo-codes. A load that depends on CSP02 software (post BCS36) contains the fixed pseudo-codes.
- A warm restart is a requirement in BCS36 and earlier versions. Perform the restart to allow the ACTS feature to function. If you do not perform the restart, TRAPs occur for each attempt to attach to a RCVRCOIN.

Datafill

The following table describes datafill for table RECEIVER:

Table RECEIVER Field Descriptions

Field	Subfield	Entry	Explanation and Action
RCVRKEY		See Subfields	<i>Receiver Key</i> This field contains subfields CLLI and NUM. This field is the key to the tables.
	CLLI	RCVRATD RCVRDGT RCVRMF RCVRMCCS DGT300 MF300 KSR2OCVR KSR2ICVR RCVRCOIN RCVATDUK RCVRDTUK or RCVRCDC	<i>Common Language Location Identifier</i> This field indicates the Common Language Location Identifier (CLLI) for the circuit type. * Enter "RCVRATD" for an audio tone detector circuit. * Enter "RCVRDGT" for a DIGITONE digital receiver circuit. * Enter "RCVRMF" for a multifrequency receiver circuit. * Enter "RCVRMCCS" for a mechanized calling card receiver circuit. * Enter "DGT300" for a DIGITONE circuit for GATEWAY. * Enter "MF300" for a multifrequency receiver circuit for GATEWAY. * Enter "KSR2OCVR" or "KSR2ICVR" for a R2 signaling circuit for licensee use only. * Enter "RCVRCOIN" for an automatic coin toll service receiver. * Enter "RCVADTUK" for an A-Law audio tone detector circuit acceptable for use in the UK. * Enter "RCVRDTUK" or an A-Law digitone receiver circuit acceptable for use in the U.K. * Enter "RCVRCDC" for a receiver coin detection circuit.
	NUM	0 to 1,023	<i>Circuit Number</i> Enter the number assigned to the circuit. Entries out of the 0 to 1,023 range are not correct.
RCVRTYPE		A or D	<i>Receiver Type</i> Enter the type of circuit, "A" (analog) for COMMON and GATEWAY, or "D" (digital) for switching units.
TMTYPE		MTM, T8A, TM2, TM4, or TM8	<i>Trunk Module Type</i> Enter the type of trunk module where the circuit mounts. Only the entries that appear are correct.
TMNO		0 to 2,047	<i>Trunk Module Number</i> Enter the number of the trunk module where the circuit mounts. If the trunk module type is TM2, TM4, TM8, or T8A, the range is 0 to 2,047. If the trunk module type is MTM, the range is 0 to 255.

TMCKTNO	0 to 29	<i>Trunk Module Circuit Number</i> Enter the trunk module circuit number assigned to the circuit. For an analog receiver, the range is even numbers 0 to 28 only. For a digital receiver mounted on trunk module type TM2, TM4, TM8 or T8A, the range is 0 to 29. For a digital receiver or audio tone detector mounted on a MTM, the range is 0 to 24.
---------	---------	--

CARDCODE	2X48AA 2X48AB 2X48CA 2X48CB 2X48CC 3X08AA 3X08AB 5X29AB 5X29AC 5X29BA	<i>Card Code</i> Enter the PEC of the receiver card. Only these entries are correct.
----------	--	--

-End-

Datafill Example

Sample datafill for table RECEIVER appears in the following example:

RCVRKEY	RCVRTYPE	TMTYPE	TMNO	TMCKTNO	CARDCODE
RCVRMF 0	D	MTM	11	16	2X88AA
RCVRMF 1	D	MTM	11	17	2X88AA
RCVRMF 2	D	MTM	11	18	2X88AA
RCVRDGT 0	D	MTM	4	14	2X88AA
RCVRDGT 1	D	MTM	4	15	2X88AA
RCVRDGT 2	D	MTM	4	16	2X88AA

What's News

When Naomi Freundlich, John Free, and I began looking into the subject of bugging, we ran into problems. Government agencies, who know all about bugging and countermeasures and counter-countermeasures and tricky things governments do to try to out-wit each other, wouldn't talk. They refused even to see us. That was no surprise.

So we looked elsewhere. There is, we reasoned, an active and healthy private bugging industry—companies that sell bugging equipment. We figured that if we could learn about their equipment, that would give us clues about the state of the art in this field. Then perhaps we could tie that information to the sketchy reports that have come out about the bugging war between the United States and the Soviet Union. It didn't work. It turns out that bugging—except under highly controlled conditions—is illegal. So nobody selling bugs would talk; in fact, nobody would admit to such dealings. The one situation where bugs can be used legally occurs when law-enforcement officers get a court order allowing them to place a suspect under surveillance. But, we learned, companies that legally sell equipment to the police refuse to talk or show their wares to anyone except those authorized to buy them; that is, law-enforcement officials.

Nevertheless, we were able to dig up an amazing amount of information. And we learned an astonishing thing: Despite the high-tech image of the field, most of it is based on the application of relatively simple, well-known technology. Let me explain.

One of our best sources was the industry that protects private companies and individuals *against* bugging, the companies that come in with highly sophisticated gear and sweep an office or meeting room to make sure it contains no bugs. Such companies—completely legal—are often happy to talk about what they do. And in the process of talking about how they *spot* bugs, they give considerable details about the bugs themselves. After all, to find them, you must know what you're looking for.

We also got information from some textbooks. The books are used in schools that train anti-bugging experts, the people who do the sweeping. Those texts contain much information about the state of the art when it comes to modern bugs.

Homemade bugs

From these sources we learned that highly effective bugs can be made from small wireless mikes available on the market for legitimate purposes. Smaller, easier-to-conceal devices—though illegal—can be bought in many places. We were also surprised to find that it does not take an advanced electronics laboratory to make extremely small, advanced bugs. In fact, any handy person with some electronics background could build one in a well-equipped home workshop. We uncovered plans for building a bug hardly bigger than a pencil eraser. They were in a manual used to train security professionals. The object was not to help people build such bugs, which are undoubtedly available to law-enforcement officials through legal channels (and no doubt to others from illegal ones). They serve, instead, to show anti-bugging technicians what they're up against.

We had also seen news stories about perhaps the most high-tech device around, one that bounces a laser beam off a window pane to listen in on conversations going on inside a closed room. We learned that it, too, is not as sophisticated as we thought. It is, in fact, fairly simple to build using an easy-to-obtain off-the-shelf laser made by General Electric and an amateur telescope from the Edmund Scientific catalog.

Computer bugging is another art that has been whispered about, but about which little has been forthcoming. It has been assumed that highly advanced electronic listening posts would be needed. At first, our attempts at getting information from those charged with making computers secure—both national security officials and computer manufacturers who develop the techniques for them—were to no avail. Then we found that a

Dutch computer expert had published a paper in an obscure journal telling how easy it is to tune in on a computer from blocks away, using about \$500 worth of equipment that anyone familiar with what goes on inside a television set could build. We also found out that an enterprising reporter for the British Broadcasting Corporation had got such a rig together and given an amazing demonstration of unauthorized tapping of confidential computer information.

What about micro-mikes?

At first, we had trouble learning about the tiny microphones like the one on the cover. We got that one from a source who gave it to us on the condition that he not be identified. But how does such a miniature device work? No one would discuss it as long as we called it a bug. We took it apart and examined it under a low-powered microscope. We could see what was there, but what was it?

Then, inspiration. Where does such a microphone appear routinely in an innocent, legal function? Who makes them by the millions? The answers: 1) In tiny slip-in-the-ear hearing aids. 2) The hearing-aid industry. Representatives of this industry were happy to supply us with technical details of their products.

So little by little, the picture began to emerge. With the accretion of clues, we were able to put together an account of the basic technology behind the widely publicized bugging war. There certainly are details that are and will be kept secret by those charged with the responsibility for national security. But an amazing amount can be learned when information from multiple legitimate sources is assembled into a coordinated picture. The report starts on the cover and continues on the next page.


Editor-in-Chief

[Continued from cover]

which they are based. Almost nothing has been written about how some of the most interesting equipment works.

What kinds of bugs are available? How are they put in place? Detected? Designed to avoid detection? What about tuning in on the computer down the block to learn the secrets it contains? Bugging typewriters? Bouncing laser beams against window panes?

In the larger picture, what is happening in the bugging war between the superpowers? What did security officials find in the Moscow embassy?

Most of this information is classified. Yet much can be learned. Today, snooping is big business with widespread industrial and commercial applications. Companies make and sell a remarkable variety of devices.

In addition, bits and pieces of information have leaked from Congressional hearings and from other unclassified sources. Those with inside knowledge make occasional statements that, combined with what we know about commercial equipment, can be revealing. From these sources emerges a hazy but informative picture of the shadowy world of spying.

The veil of secrecy

Nobody wants to talk about bugs. The Central Intelligence Agency and National Security Agency refused to be interviewed. Private companies were also wary; several prospective sources hung up when they learned why we were calling.

Most manufacturers of bugs make it clear that they will not talk for publication. For example, Intelligence Devices Corp. of Fairfield, N.J., advertises 100 different pieces of security equipment. The ad begins: "We supply the most sophisticated electronic intelligence devices available to law enforcement, but law prohibits us from discussing our products in detail without the proper written requests. . . . Complete and detailed product information is available only to authorized agencies upon written request on departmental letterhead."

Despite such problems, we were able to dig out some surprising facts. Among them:

- Bugs can be made almost any size. The smallest we actually saw was the one pictured on the cover. It is a tiny electret microphone just $\frac{1}{16}$ inch across at its largest dimension. The security expert who gave it to us wouldn't say where he got it.

- Bugs are widely available. Tiny ones undoubtedly used in industrial espionage can be bought openly in some European and Asian cities, though they're illegal there as here. Easily available even here, however, are wireless microphones smaller than a cigarette pack. They have legitimate uses, but also can be used for bugging.

- Bugging experts use dozens of methods to keep their devices from being detected, from planting them in electronic equipment to wiring them with the latest in fiber-optic technology. The Soviets planted thousands of false bugs in the now infamous U.S. embassy in Moscow to confuse sweeping attempts.

- While the CIA and FBI undoubtedly bring the latest in electronics technology to bear in acquiring supersmall, difficult-to-detect devices, surprisingly sophisticated bugs are relatively easy to build. We obtained plans for the

so-called "martini olive" bug that received considerable publicity several years ago. It can be built in any reasonably equipped electronics workshop by anybody with even a moderate amount of electronics knowledge.

- Sensitive information in computers is easy to steal; a \$500 device can tune in on any unprotected computer at ranges of perhaps a mile and reproduce anything appearing on the computer's screen. A British expert recently gave a demonstration that left computer users in a state of shock.

- The highly publicized laser beam that can be bounced off a window pane to eavesdrop on voices inside sounds flashy, but is apparently of limited usefulness in real life.

- People who don't want their conversations bugged rely on frequent sweeping of sensitive areas. We saw a demonstration of several kinds of advanced equipment used in

BUG

this effort.

Because of the sensitive nature of the subject, *no one* was willing to come right out and talk in detail about bugs and bugging, or even to admit to having detailed knowledge. Nevertheless, we uncovered bits and pieces, and a picture began to form. Bugs—devices designed to eavesdrop surreptitiously on conversations—we learned, come in three basic forms. First are units that contain both a microphone and a small transmitter. They are hidden in a room and transmit a signal to a nearby receiver. If such a unit is tied into a power source—room electrical wiring or a telephone line, for example—it can transmit indefinitely. And the wiring may also be used to route signals from the bug to distant points.

Second are microphones. Because they can be extremely small, they can be hidden almost anywhere. But they require wires—which can be smaller than a human hair—to conduct the signal to a listening post outside the room. Finally, there are passive devices, which sit silent and unobserved but which can transmit room sounds when stimulated by a radio signal from outside. More about this later.

Although all bugs fall into one of these categories, they come in a variety of shapes, forms, and sizes. Private investigators who talked on the condition they not be identified told us that bugs they find are sometimes built on small circuit boards, at other times they're simply strung together in little balls of wires and components that look like a tangle of spaghetti. They can be put in small cases or encapsulated in epoxy. Epoxy encapsulation is attractive, says a textbook we saw, because such bugs look like little blobs of unidentifiable substances and may not even be recognized as bugs. Incidentally, the book, *Measure by Countermeasure, a Textbook on Anti-Eavesdropping*, was

By JOHN FREE, NAOMI FREUNDLICH,
and C. P. GILMORE

RESEARCH BY EDUARDO R. C. CAPULONG

44 | POPULAR SCIENCE

Bugging

written to train security professionals who attend the school conducted by a security company called Microlab/FXR located in Livingston, N.J. It talks about bugs, how they work, their sizes and types, and how to find and recognize them.

While some bugs are homemade, others are available commercially; you can buy them from radio supply stores where they are sold as wireless microphones or baby-sitting devices. Several such devices are pictured in this article. They cost just a few dollars and transmit a signal that can be picked up by an ordinary FM radio. "Lots of people are taking Radio Shack wireless microphones and converting them," says Charles Miller, a technician with Law Enforcement Associates, Inc., of Medford, N.J. "Take the shell off, and if you're good with your hands you can make them pretty small." "You can find them advertised in the backs of magazines," says Rob Muessel, a technical serv-

was probably a transmitter planted inside his phone."

Similar bugs can be designed to send out signals all the time—even when the telephone is thought to be inoperative. "Wires are often put in telephones for nonexistent intercoms or speaker phones," says Mason. "So there is a spare pair of wires." If someone intent on bugging can get to a terminal board in that building, he can wire the spare pair so that the microphone in the telephone sends a voice signal to the terminal even when it is on the hook. "In government agencies where the phones must be replaced quite often," he says, "they test phones before new ones are put in and find that eight out of ten phones are 'hot on the hook.'"

Another astonishing fact is how easy it is to build very small—and very effective—bugs. For example, a San Francisco security expert named Hal Lipset won momentary fame some years ago as the man who had bugged a martini olive. During our research we obtained plans and directions on how to build the infamous martini-olive bug.

The plans call for hollowing out opposite ends of a small copper cylinder with a lathe, then carefully mounting in the two cavities about a dozen tiny parts—transistors, resistors, capacitors—available from any electronics supply house. The instructions describe how to cut apart a standard alkaline battery and use parts of it to construct a very small battery.

Finally, a disc made of foil serves as a microphone. The instructions say the unit can be made in several sizes, including one in which the finished device is approximately ½ inch in length and slightly less than that in diameter. It will transmit at a frequency of 600 megahertz.

How do you make it look like an olive? "A case may be formed around the unit with fiberglass putty and molded to any desired shape," the instructions conclude. The antenna is disguised as a toothpick in the olive!

The most interesting bug we saw was the one pictured on the cover, which falls into the second category: microphones. The bug, a miniature electret microphone, would need thin wires leading to a receiving station. That would be no problem for someone with access to the target room; we were told that the "wires" can actually be two lines of metallic paint on a wall, which are then covered by regular paint. Such an installation is almost impossible to find.

Although the term electret, representing an electrostatic analogy with permanent magnets, first appeared in 1885, a practical device wasn't devised until 1925 (the drawing shows its operating principle). An electret is made by polarizing certain waxes or plastics with high voltage: one side has a strong positive charge; the opposite side of the electret material has an equally strong negative charge. An electrical potential is permanently "frozen" into the material. Practical applications of electrets for microphones became possible with the development of low-noise transistors and suitable dielectric—nonconducting—materials.

Just how small bugs can be is unknown. Frequently news reports speak of "pinhead-sized" bugs. Yet there is no evidence that bugs that small really exist. It seems at least possible that they do not, and that the pinhead estimate is the result of logical confusion. The electret mike

Continued



GING

ices coordinator for Information Security Associates of Stamford, Conn.

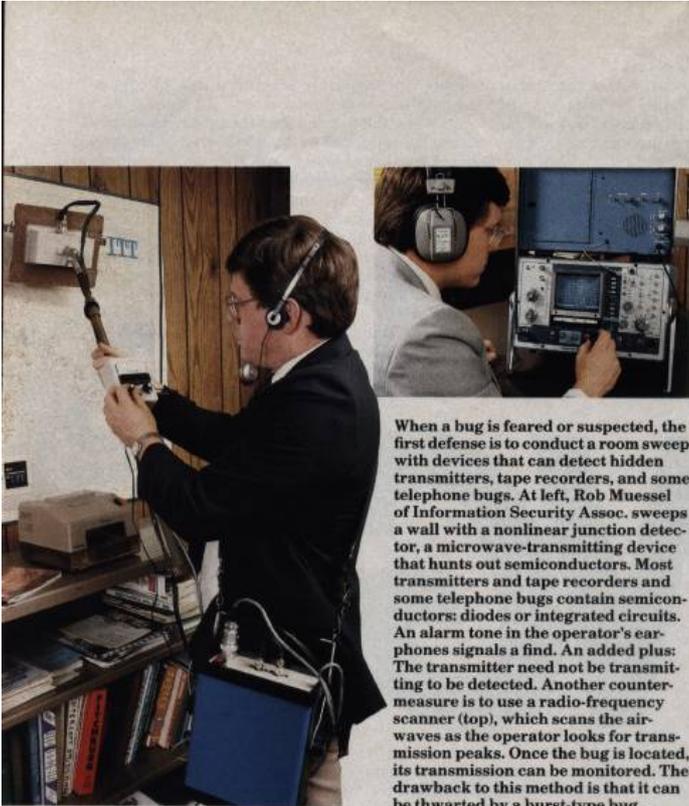
More-sophisticated devices—legally available in this country only to law-enforcement officers—are available off the shelf in Tokyo, Hong Kong, and at the Frankfurt airport in West Germany. "In Japan they make one transmitter that's a quarter inch square and about one and one-half inches long," says Muessel.

Bugs can be very small—small enough to be built into a fountain pen or stuck into a small hole in the wall, the binding of a book, or elsewhere. Harry A. Augenblick, president of Microlab/FXR, tells of one clever design. "This is a picture-hook bug," says Augenblick, pointing to a one-inch-long, ¼-inch-diameter spike with a picture hook on its flat end. "First you use a tool that punches a hole in a wall, then you slip the bug in. After you hang the picture back on the wall, you wouldn't know for years that somebody had changed your picture hook."

Another investigator who insisted on anonymity showed us a transmitter about the size of a book of matches. "With its battery pack this one will transmit for nine days," he said. "You can throw one of these guys in a trash can and retrieve it later." How far can such bugs transmit? "A matchbook-sized device can have a range of a quarter of a mile," says Frank G. Mason, president of a Fairfield, Conn., security firm that bears his name.

The variety is endless. Pictures accompanying this article show a bug that slips into a telephone handset. Picking up the handset supplies telephone line voltage to the bug, which then transmits anything said into the mouthpiece to a nearby receiver. "We once got a call from a guy who said every time he picked up his telephone his television picture went blurry," said Muessel. "We never found out what that meant because he didn't hire us. But there

Bugging



When a bug is feared or suspected, the first defense is to conduct a room sweep with devices that can detect hidden transmitters, tape recorders, and some telephone bugs. At left, Rob Muessel of Information Security Assoc. sweeps a wall with a nonlinear junction detector, a microwave-transmitting device that hunts out semiconductors. Most transmitters and tape recorders and some telephone bugs contain semiconductors: diodes or integrated circuits. An alarm tone in the operator's earphones signals a find. An added plus: The transmitter need not be transmitting to be detected. Another countermeasure is to use a radio-frequency scanner (top), which scans the airwaves as the operator looks for transmission peaks. Once the bug is located, its transmission can be monitored. The drawback to this method is that it can be thwarted by a burst-type bug.



contains a tube on one side through which the sound enters. The hole is approximately the size of a pinhead. Thus it is possible that the smallest bugs are not themselves pinhead sized, but require a pinhead-sized hole in the wall through which they pick up sound. Says Mike Russell of Sherwood Communications in Southampton, Pa., "Microphones are usually found in ceilings or mid-level in the wall. They're usually behind the wall, with a tiny hole the size of a pencil point drilled through."

Perhaps the most sneaky of all bugs is the passive device. It first came to light some years ago when American security experts revealed that they were worried about low-level microwaves beamed by the Soviets at the American embassy in Moscow. Now they're reasonably sure that these were aimed at mysterious cavities built into the structure of the building.

Steel reinforcing rods or small cone-shaped metal cavities can be hidden in the walls during construction. Sound waves within the room cause the walls to vibrate slightly, distorting these metal structures. If a microwave beam at a critical frequency is aimed at such a device, the reflected signal is slightly modulated by the sound vibrations. Careful analysis of the returning reflections can re-create the original voice signals that caused the vibration.

Perhaps the most advanced—and talked about—technique of all is bouncing a laser beam off a window. The window pane vibrates slightly from the sound pressure generated by the conversation inside. The returning laser beam is modulated by these vibrations, and the original voice signals are recovered.

One of the textbooks designed to train security personnel contains a section on such devices. It says one can be built using a General Electric H1A1 laser, which radiates about 35 watts of power in the infrared band. It is pulsed with a simple transistor circuit at 10 kilohertz. The receiver is an astronomical reflecting telescope bought from Edmund Scientific Company. A photomultiplier tube, which turns the pulsed infrared signal into a series of electrical pulses, is mounted in place of the eyepiece. The output of the photomultiplier is then fed to an amplifier to recover the voice signal from within the room.

It is questionable just how effective this technique is. Richard Heffernan, vice president of Information Security Associates says the technique probably doesn't work too well. He points out that the window pane also vibrates from passing traffic and random noise, and picking out the relatively low-level voice signals would be difficult. Other experts point out that filtering techniques have been developed to get clear pictures out of TV signals returning from space—signals that when they are received are buried in and obscured by noise. Such processing might dig voices out of the background noise.

Cleaning up the premises

While companies are reluctant to talk about bugging, they're often happy to talk about their *anti-bugging* activities, which are legal, and which, indirectly, reveal a good bit about bugs, too. For example, Microlab/FXR's Augenblick gave Associate Editor Naomi Freundlich a demonstration of the company's SuperScout—a \$25,000

Specialist in repairs of parts and instruments
Only \$10.00 per hour
Call or write: M.C. Tech. Inc. for complete details
1000 E. 12th St., Dept. 1000, Springfield, MA 01102
U.S. Mail: C.O.D. with \$1.00. Payment please
within 10 days

DEAN'S Bands, Cables, Coils, Springs, etc. Dept. 1000
Law Office, 1000 E. 12th St., Springfield, MA 01102
Hobbies, Dept. 1000, Springfield, MA 01102

HOME REPAIRS, ALUMINUM
Dept. 1000, Springfield, MA 01102

SAVE THOUSANDS Dept. 1000
Dept. 1000, Springfield, MA 01102

PATCHES, DECALS Dept. 1000
Dept. 1000, Springfield, MA 01102

GUARANTEED Dept. 1000
Dept. 1000, Springfield, MA 01102

WARRANTY Dept. 1000
Dept. 1000, Springfield, MA 01102

PHOTON MICROSCOPE Dept. 1000
Dept. 1000, Springfield, MA 01102

ASTRONAUTICAL Dept. 1000
Dept. 1000, Springfield, MA 01102

FOREIGN PERIODICALS Dept. 1000
Dept. 1000, Springfield, MA 01102

WORLDWIDE Dept. 1000
Dept. 1000, Springfield, MA 01102

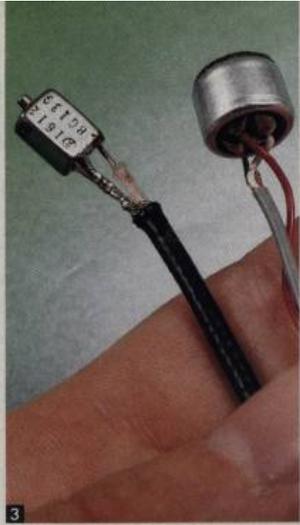
REPRODUCTION Dept. 1000
Dept. 1000, Springfield, MA 01102

PERIODICALS Dept. 1000
Dept. 1000, Springfield, MA 01102

ASTRONAUTICAL Dept. 1000
Dept. 1000, Springfield, MA 01102

ASTRONAUTICAL Dept. 1000
Dept. 1000, Springfield, MA 01102

Bugging



Except for secret high-tech devices used by government spies, the common bug is ingenious but not terribly sophisticated. **1** A drop-in transmitter replaces the microphone in a telephone receiver. It transmits a radio signal when the phone is in use and gets its power from the telephone line. **2** Another small bug, wired into a light switch may use AC lines for both power and transmission. **3** Tiny microphones, one from a hearing aid (left) and the other an electret-type (right), can be wired into walls or slung into the space above a dropped ceiling. **4** Although the manufacture, use, and sale of bugging equipment is illegal, the back of a magazine offers ways around the law. Most equipment needed for bugs is available in hobbyist shops. **5** FM transmitters were all obtained by mail or in shops; battery life: one day. **6** and **7** Ordinary items, an intercom, cigarette pack, and outlet, are disguised transmitting devices.



bug detector the company says is used daily by 53 lesser world governments and hundreds of Fortune 500 companies.

"It looks like a cross between a vacuum cleaner and a beach-variety metal detector," she reports (see photo). "The body of the device is a briefcase-sized receiver, and attached by long electrical cords is an adjustable boom with a flat vacuum cleaner-like head on its end that functions as an antenna. Augenblick slung it over his shoulder.

"We will find your little tape recorder whether it's on or off or even if you take the batteries out of it," he promised. Moments before, out of his presence, I had hidden it on the lower shelf of the office coffee table under a stack of magazines.

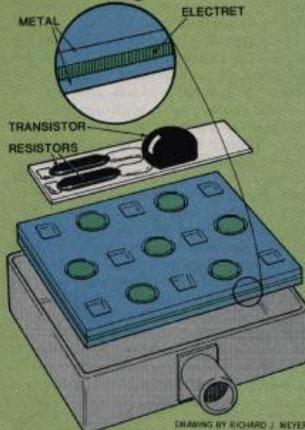
"He switched on the detection device, a nonlinear junction detector. Augenblick had explained the operating principle earlier. 'Normally if I sent a signal out around this room, it would bounce off everything and the signals coming back would all have the same frequency as the one that went out,' he said. 'But semiconductors such as transistors and diodes are nonlinear devices in which current flows more readily in one direction than in the other. That means that when SuperScout transmits at exactly one gigahertz, any semiconductor nearby will generate harmonics

Continued

The Soviets allege that bugs, including a transmitter wired into a brick from the Soviet embassy in Washington, D.C. (above right), and a microphone and transmitter fitted into a socket for the master TV antenna from the residence of their U.N. representative (right), were planted by U.S. spies.



Cover bug



Tiny components inside a 0.2-by-0.2-by-0.09-in. electret microphone ensure small size but high sensitivity. The electret diaphragm (see text) is sandwiched between conducting metal electrodes, connected to a transistor. As the electret flexes, it generates a current that is amplified by the transistor. External leads supply transistor power and a path to other circuits.

High-tech bugging techniques—and a costly fix

1 MICROWAVE INTERCEPTS. Microwave dishes used by telecommunication firms relay voice and computer signals from point to point or back and forth to communication satellites. Although the dishes concentrate the beams into narrow paths, signals that spill over can easily be intercepted at many points along the beam path.

2 PASSIVE BUGS. In 1952, an unusual type of bug, a small metal cylinder, was found in a decoration at the U.S. embassy in Moscow. The cylinder contained no electronics and had no source of power, but it apparently relayed voices in the room to a Soviet listening post outside the embassy. By beaming 330-MHz radio waves at the cylinder from outside the embassy, the Russians picked up return signals modulated by voices in the room, which vibrated part of the tiny metallic can.

3 LASER AUDIO SURVEILLANCE. Because laser beams don't scatter and spread like ordinary light, a laser can be focused on a window some distance away. Voices in a room vibrating the window glass shift the wavelengths of the reflected beam. A receiver in the path of the reflection can amplify the beam, and a demodulator can separate audio from light. A laser surveillance technique that avoids most extraneous window vibrations, and avoids the difficult positioning of a laser transmitter and receiver at different locations, bounces the beam from objects within a room. Tiny flexible reflectors, planted ahead of time, can pick up voices and modulate a beam reflected to a receiver next to the transmitter.

4 BURST TRANSMISSIONS. Advanced mi-

crocircuits now enable devices smaller than a calculator to electronically encode, compress, and record information. The recording—voices or computer data, for example—can then be transmitted in a burst lasting only a split second. Such transmissions are very hard to detect on radio frequencies.

5 COMPUTER INTERCEPTS. Computers emit radio frequencies that may be intercepted some distance away. Decoding gear (see text) can then show what appears on the computer screen.

6 FALSE BUGS. Nonlinear junction detectors look much like ordinary metal detectors, except they beam radio waves into walls and pick up return signals produced when the junctions of dissimilar materials such as semiconductors radiate harmonic frequencies back to the detector. Well-designed bugs have shielding that minimizes penetration of the detector beam and greatly reduces the harmonic frequencies reaching the detector. In Moscow, the Russians have reportedly sown the new embassy walls with "junk" junctions, complicating sweeps for true bugs.

7 SHIELDED ROOM. A cure for high-tech bugging is a specially designed room isolated from outside prying. In addition to shielding that stops radio-frequency leaks, acoustic baffles can absorb voices; ventilation and plumbing must also be protected. An elaborate suspension system may "float" the entire structure. Such an add-on room has been proposed as a partial fix for the heavily bugged new embassy building in Moscow.

—that is, it will send back signals in exact multiples of the original frequency—one, two, and three gigahertz, for example.

"He methodically swept the head of the antenna up and down the office walls, across book shelves, over furniture, and finally across the floor—all the while keeping an eye on the needle at the top of the shoulder-slung portion of the device.

"Then he began sweeping over the coffee table. The monitor needle swung to the right and he grinned. 'There it is!' he exclaimed triumphantly.

"Nonlinear junction detectors can be misled—especially if electronic equipment containing semiconductors is anywhere nearby. 'In the beginning we did some very crude things,' said Augenblick. 'An operator conducting a sweep of former Israeli Prime Minister Golda Meir's office literally tore down her office wall and found nothing. There was just a simple radio in the next room.' "

Although a nonlinear junction detector such as the one Augenblick demonstrated can find just about any bug containing semiconductors if used with sufficient care, it is expensive and tedious to use. Thus many persons debugging a site use a device called a scanner, which detects RF signals from bugs instead of the circuits inside the bug. Naomi Freundlich saw one in action at Information Security Associates in Connecticut. She reports:

"Rob Muessel turned a knob on the VCR-sized receiver; at each click he homed in on radio-frequency signals. 'This instrument can scan signals from twenty kilohertz to a thousand megahertz—one gigahertz—and up into the seven-to-eight-gigahertz microwave range,' he said. At one point the scanner screen danced with a whole mountain range of blue peaks, stronger than any we had seen yet. 'What are you picking up now?' I asked excitedly, imagining us picking up secret transmitted conversations.

Muessel turned some dials and a particularly large peak appeared on the screen. But instead of satisfying my voyeuristic tendencies, strains of Simon and Garfunkel's song 'The Boxer' came through. We had stumbled across the FM mountain range.

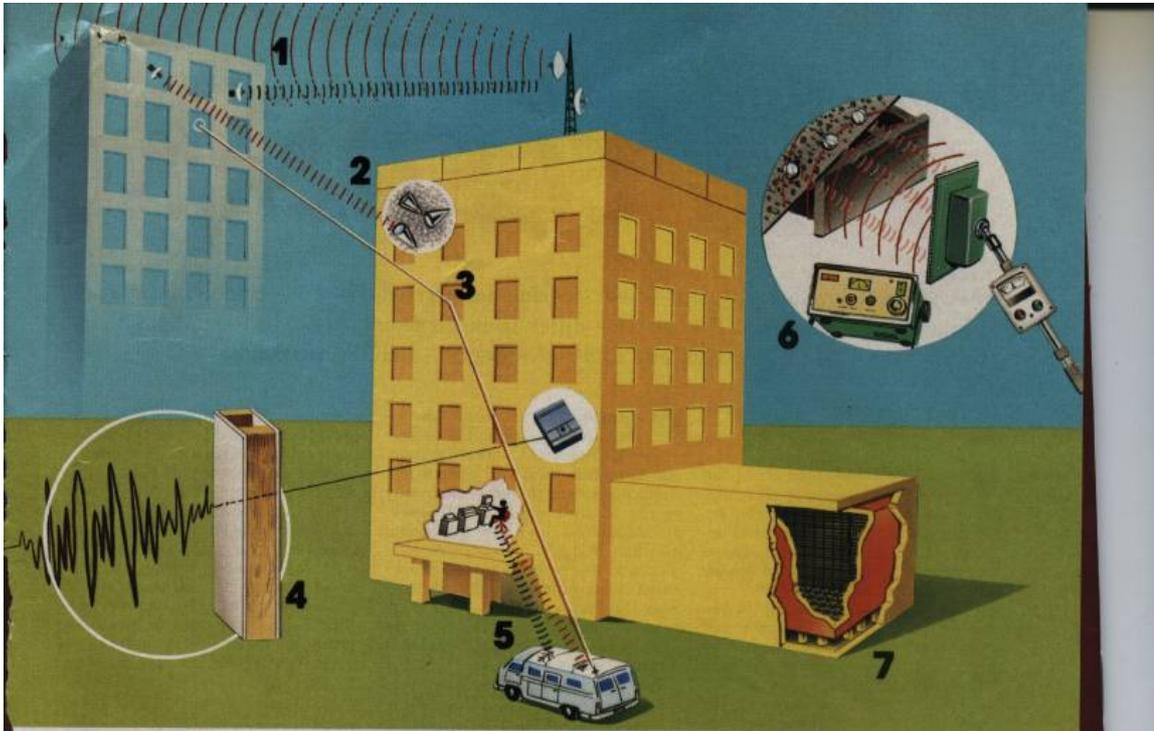
"That's all that's really involved in using this device,' said Muessel. 'You just tune through and listen.' Tuning through and zeroing in on some of the larger peaks, we picked up ham radio, cellular telephones, and even the repetitive staccato sound of transmitted data from pocket pagers.

"Then Muessel set up a transmitter in the room. Even when there was no sound in the room there was a peak on the scanner screen. 'We sometimes use a steady sound source,' said Muessel as he turned on a high-pitched beeper. As the transmitter signal pulsed like a heart beat in time with the beeper I heard the regular sound in my earphones. I also listened as we picked up the same pulsating peak at exactly two and four times the frequency of the original signal.

"The RF scanner can also be used to detect hidden video cameras. 'If we had a closed-circuit TV monitor, we could hook up a television receiver and display video signals,' said Muessel as we passed a large peak from a nearby TV station."

As this demonstration illustrates, bugs that transmit continuously have a serious weakness: They're relatively easy to detect. Several ingenious schemes have been developed to minimize that possibility. For example, bugs can be built to collect information and transmit it in practically undetectable short bursts. One source speculates that such a bug could collect information in digital form for perhaps 15 seconds, then send out the whole package in one microsecond. Such a device would be practically impossible to find with a scanner.

Bugging



DRAWING BY DAN OSYCHKA

Others come with voice-actuated circuits that turn them on when there are sounds of voices in the room, off when not. Some have remote switches by which they can be turned on and off. "I can put a bug someplace and turn it on and off remotely," Miller says. "I hear you come into the room, and if I have any idea that you're going to start checking for bugs, click, it's off." All these methods help prevent detection by scanners that look for signals being radiated.

Yet other bugs use a technique known as "snuggling" to avoid detection. The designer has it transmit at a frequency just barely different from a local TV station's, for example. Because its signal tends to be lost in the much more powerful TV signal, it may go undetected. Other bugs are frequency switchers: They transmit at one frequency for a few thousandths of a second, then change to another, and then another.

Active bugs can often be detected by nonlinear junction detectors or scanners. These methods, however, will not detect microphones, which neither contain semiconductors nor put out an RF signal. "You can find them," says Frank Mason, "by X-raying the walls inch by inch, but that's time-consuming, expensive, and hazardous to your health. The only other defense is physical inspection such as looking for pinholes in walls."

An even more difficult-to-detect setup can be created by using a hairlike optical fiber to transmit the signal out of the room and perhaps out of the building. Because the signal is in the form of light, it creates no electromagnetic signal that can be detected, nor is it detectable by normal sweeping methods.

Bugs of many types—both transmitters and microphones—are widely used, and, according to the Microlab textbook, easily placed. The book says that Microlab never identifies its clients, what it did for them, or what it found.

However, it says, the company knows of actual cases of bugging detected by others. In one case, it says, one company wanted to find out what progress a competitor was making in research. So while a member of the bugging company visited the office of the director of research at the rival company, he noted the title of a book in the office. He then bought an identical book and had it fitted with a 520-kilohertz bug. The bug, made into a thin strip and sealed in epoxy, was glued into the binding of the book. Then a maintenance worker was persuaded to substitute the bugged book for the original one. The sneaky competitors parked in a car nearby and tuned in on conversations in the research director's office.

In another case a financial operator widely known for sending flowers to his friends and acquaintances sent a bouquet to a legal firm reviewing a company's financial disclosure statement. In the flowers he planted a small commercially available wireless transmitter, tuned in to the conversations, and was able to make a profitable investment prior to the release of the financial statement.

Sometimes planting a bug turns out to be a *really* inside job. In February 1982 the manager of the Soviet airline in Indonesia was arrested for running a spy ring. While he was in custody, authorities became suspicious about a scar on his chest, which he said was from an operation. But a closer look showed that a bug had been planted in the man's chest so KGB agents nearby could hear all conversation around him.

Computer bugging

Bugs have got most of the headlines in recent months, but sleuths use a lot of other high-tech tricks. One active area: eavesdropping on the sensitive information in somebody else's computer. Computer users were recently shocked

[Continued on page 86]

AUGUST 1987 | 49

Bonus

~~Δ PASSWORD (DMS 100 SWITCH)~~

~~PASSWORD (ENTER)~~

~~TO BUSY LINE:~~

~~AFT. POST S #~~

~~DO: 5 (ENTER)~~

~~TO GET BACK DO: 6 (ENTER)~~

End of Issue #42



Any Questions?

Editorial and Rants

1. Iran's major trade partner is Euro savage Land.
2. U.N. places sanctions against Iran.
3. Euro savages need the money for their failing socialist policies.
4. Hey! Let's sue Microsoft!

Do you think they'll ever pay back all that Marshall Plan money? Death to Europe!

Attack on U.S. Innovation in the Global Market

September 27, 2007 – From: www.sbecouncil.org

By Raymond J. Keating

The news out of Brussels last week was not good for innovation and U.S. market leading companies. On Monday, September 17, the European Court of First Instance rejected an antitrust appeal brought by Microsoft Corp., and thereby handed regulators at the European Commission an enormous amount of discretionary power to harass U.S. businesses.

In March 2004, the European Commission ruled against Microsoft, saying that the firm abused its market share by bundling its Media Player to Windows and supposedly refusing to provide interoperability information for Windows to competitors. **With the European Court's decision, Microsoft could face fines reaching as high as \$2.77 billion, according to news reports.** And there could be more trouble for the software maker, as reports indicate that the European Commission is looking at interoperability regarding Microsoft Office products and the new operating system Vista.

What are some of the potential consequences of this ruling?

Innovation Suffers

Innovation could suffer in the high tech arena as companies will have to focus on what European regulators might think about various product designs, rather than focusing on customers/consumers, as should be the case. Indeed, leading U.S. companies even have to be

concerned about their level of success. The Wall Street Journal reported that European Competition Commissioner Neelie Kroes declared that consumers are "suffering at the hands of Microsoft," and that "she would like to see a 'significant drop' in Microsoft's nearly 95% market share in operating-system software." Apparently, Kroes fails to understand how markets work. That's a problem for a "competition commissioner." Microsoft gained market share by serving consumers well. And in the dynamic high-tech marketplace, the company will be toppled if it fails consumers.

I.P. Rights Undermined

Intellectual property rights will suffer a mighty blow as European regulators are forcing Microsoft to hand over its intellectual property to competitors, and apparently, the company will have to do so for free.

Protects Competitors Not Consumers

As bad as antitrust regulation is in this country, the European model is even worse. While antitrust policy in the U.S. is at least supposed to be about protecting consumers, the European Commission blatantly shows that antitrust regulation in Europe is about protecting competitors. That not only is dangerous for leading U.S. firms operating in Europe, but those doing business around the world as regulators in other nations could take their cue from Europe.

European regulators not only still have Microsoft in their sites, but also are pursuing chipmakers Intel Corp. and Rambus Inc. There also are concerns that Apple and Google could be next.

In the end, this is a form of protectionism through antitrust regulation. It is anti-free trade, and U.S. policymakers have to be aware of this and clearly communicate to our trading partners that this is not acceptable in a global economy. U.S. Rep. Robert Wexler (D-FL), chairman of the House Foreign Affairs subcommittee, correctly called the European court ruling a "dangerous precedent," and said he would soon hold hearings on this "new form of protectionism," according to a Wall Street Journal report.

One of the key competitive advantages that the U.S. holds in world markets is our ability to innovate. The European Court of First Instance's decision last week is directly targeted at undermining that U.S. edge.

The BBC gets caught helping terrorists... again!

"The British are responsible for destroying the Caliphate system. They are the ones who created the Palestinian problem. They are the ones who created the Kashmiri problem. They are the ones who put the arms embargo on the Muslims of Bosnia so that two million Muslims were killed. They are the ones starving Iraqi children."

--- Quote from Usama bin Laden in a June 2000 speech.

BBC's Newsround Fed Youngsters Al Qaeda Propaganda, Claims Ex-Spy Chief

September 29, 2007 – From: www.dailymail.co.uk

By James Chapman

Britain's former spy chief accused the BBC of "parroting" Al Qaeda propaganda to children as young as six.

Dame Pauline Neville Jones, who is also a former BBC governor, is infuriated at the stance the corporation's Newsround programme took on the September 11 attacks.

She accused the flagship children's news bulletin of feeding an "ugly undercurrent" which suggests the terrorist outrage was somehow justifiable.

Newsround is aimed at viewers aged between six and 12.

On its website it answered the question concerning 9/11, "Why did they do it" by saying: "The way America has got involved in conflicts in regions like the Middle East has made some people very angry, including a group called al Qaeda – who are widely thought to have been behind the attacks."

After the public complained, the text was amended.

It now reads: "Al Qaeda is unhappy with America and other countries getting involved in places like the Middle East.

"People linked to al Qaeda have used violence to make this point in the U.S.A, and in other countries."

Dame Pauline, who headed the Government's Joint Intelligence Committee and is described as the most formidable female diplomat Britain has produced, said the new version was even worse.

"It still says it's all America's fault, and now for daring to be involved in the Middle East at all," she said.

"It wasn't 'people linked to' al Qaeda who killed 3,000 people that day, it was al Qaeda itself.

"Osama bin Laden even boasted of the attacks. Is the BBC really saying that if you're 'unhappy' it's quite normal behaviour to murder people?

"Is the BBC so naive as to take al Qaeda's propaganda at face value? Or is there something more sinister at work here?"

Dame Pauline, who is now a shadow security spokesman, added: "Al Qaeda make the manifestly false claim that America is part of an enormous Jewish–Christian conspiracy to dominate the world and kill Muslims.

"This is no secret – Osama bin Laden has said as much himself.

"We know that in the long run the struggle against terrorists is a battle for hearts and minds.

"How can we expect to win when our national broadcaster is parroting their line to our own children?

"There is only one set of people who are ever to blame for terrorist attacks and that's the perpetrators themselves."

Dame Pauline said the BBC was a "national treasure" and she had been proud to serve as a governor.

"But from time to time I have found myself asking questions about BBC's attitude to terrorism. It even orders its journalists not to use the word terrorist," she added.

"Although almost everyone in Britain quite rightly reacted with horror to the attacks of September 11, there was an ugly undercurrent that blamed America for being attacked.

"Just two days after the attacks the BBC screened an edition of the Question Time programme where they invited an anti–American audience that laid into the American ambassador, leaving him close to tears. In fairness, the BBC apologised for that outrage.

"Even though this was an appalling example of knee–jerk prejudice, at least it was meant for adults.

"I never imagined the rot would spread to the BBC's children's programmes. I was wrong."

Dame Pauline has complained to the BBC's head of journalism Mark Byford, who is understood to have defended the text as "clear and concise".

Sinead Rocks, editor of the Newsround programme, said the first version of the text was several years old and should no longer have been available.

But she defended the new version, insisting it was not an attempt to "justify" the events of September 11.

"We feel it is entirely legitimate to question the motives of the people who carried out the attacks," she said.

"Our contact with our audience has shown that their understanding is helped by events being put into some kind of context.

"We often have to translate complex and emotive issues into language appropriate for children. It's a responsibility we take very seriously."

San Francisco values invade the midwest.

First Jell-O, Now Santa

September 28, 2007 – From: www.suntimes.com

By Angela Caputo

So long, Halloween parade. Farewell, Santa's gift shop.

The holiday traditions are facing elimination in some Oak Lawn schools this year after complaints that the activities are offensive, particularly to Muslim students.

Final decisions on which of the festivities will be axed will fall to the principals at each of Ridgeland School District 122's five schools, Supt. Tom Smyth said.

Parents expect that the announcement is going to add to the tension that has been building since officials agreed earlier this month to change the lunch menu to exclude items containing pork to accommodate Muslim students. News that Jell-O was struck from the menu caused such a stir that officials have agreed to bring it back. Gelatin is often made with tissue or bones of pigs or other animals.

That controversy now appears to have been dwarfed by the holiday debate, which became so acrimonious Wednesday that police were called to Columbus Manor School to intervene in a shouting match among parents.

"It's difficult when you change the school's culture," said Columbus Manor Principal Sandy Robertson.

Elizabeth Zahdan, a mother of three District 122 students, says she took her concerns to the school board this month, not because she wanted to do away with the traditions, but rather to make them more inclusive. "I only wanted them modified to represent everyone," she said.

Nixing them isn't the response she was looking for. "Now the kids are not being educated about other people," she said.

There's just not time in the six-hour school day to celebrate every holiday, said Smyth, who sent the message to principals that they need to "tone down" the activities that he sees as eating too much into instructional time. "We have to think about our purpose," Smyth said. "Are we about teaching reading, writing and math or for parties or fund-raising during the day?"

Robertson is hoping to strike compromises that will keep traditions alive and be culturally acceptable to all students --- nearly half of whom are of Arab descent at Columbus Manor, she says. Fewer than a third of students districtwide are of Arab descent, according to Smyth.

Following the example of Lieb Elementary School, Columbus Manor School will exchange the annual Halloween parade for a fall festival next month. The holiday gift bazaars at both schools also will remain, but they'll likely be moved to the PTA-sponsored after-school winter festival. And Santa's annual visit probably will be on a Saturday.

More money taken from our schools to cover for those assholes in Europe. We should have killed every one of those bastards during WWII.

Funny how German "pacifism" has no problems selling weapons to the Arabs and Iran.

NATO Staggers in Afghanistan as Some Can't Fight On

October 8, 2007 – From: www.bloomberg.com

By James G. Neuger

Oct. 8 (Bloomberg) — NATO's campaign in Afghanistan is under threat from member countries on the front lines clamoring to get out and others on the sidelines refusing to go in.

With military casualties on the increase this year, the Netherlands and Canada are weighing full or partial pullouts within the next 18 months. Meanwhile, leaders in Germany, France, Spain and Italy, mindful of polls showing a majority of Europeans oppose the conflict, are resisting calls to send troops to relieve them.

The European reluctance to fight is making it harder for the 41,000-strong force to consolidate gains against the Taliban, which is battling on in the rugged terrain of southern Afghanistan six years after the U.S. drove it from power in response to the Sept. 11 attacks. It is also endangering the unity of the North Atlantic Treaty Organization, raising the stakes for a meeting of defense ministers later this month.

“If NATO can't succeed with the task that it's been given, it's had it, it's lost all credibility,” says Frank Cook, 71, a U.K. Labour member of Parliament who toured the war zone with allied lawmakers last month. “Certain NATO members haven't fulfilled their NATO commitment.”

As the U.S. military hunkers down in Iraq, President George W. Bush is trying to shift more of the Afghan burden to Europe. The U.S. remains the dominant force in Afghanistan, with 15,000 soldiers under NATO command and another 11,000 in a separate counterinsurgency mission. Britain, which is shifting forces from Iraq to Afghanistan, now fields 6,700, the second-largest contingent.

Trainers and Helicopters

U.S. Defense Secretary Robert Gates will use the Oct. 24–25 NATO meeting in Noordwijk, Netherlands, to prod the allies to provide another 3,200 trainers — to build up Afghan military and police forces that are understaffed, underequipped and underpaid — and 20 helicopters to relieve an American unit in Kandahar.

“We have been very direct with a number of the NATO allies about the need to meet the commitments that they made,” Gates told a Sept. 27 press conference.

“It's important that the full coalition show as much solidarity as possible,” NATO Secretary-General Jaap de Hoop Scheffer told a news conference in Copenhagen today. “Winning and keeping the hearts and minds of the NATO nations is as important as winning and keeping the hearts and minds of the Afghan people.”

Under Strength

Afghanistan's army now numbers 50,000 soldiers, according to NATO. It won't reach the desired strength of 70,000 combat-ready troops until 2009 at the earliest, the NATO commander in the country, U.S. General Dan K. McNeill, said last month.

As a result, NATO is conducting a two-tiered war, with the U.S., Britain, Canada and the Netherlands doing most of the fighting and dying while troops from countries such as Germany are confined to safer areas. In the first nine months of this year, 110 NATO soldiers were killed in action, almost double the 58 for all of 2006. The U.S. tops the casualty list, having lost more than 440 men and women since 2001.

The government of the Netherlands, with 10 of its soldiers killed and its reserves depleted, is weighing a cut in its force to around 1,200 soldiers from 1,700 next August and is negotiating with Norway, Slovakia and Ukraine to fill the gaps.

'They Can Do It'

For Hans van Baalen, a Dutch opposition lawmaker, there's one European country that can make a difference: France.

France's military is "well-equipped, well trained to go down south -- they can do it," says van Baalen, 47, who chairs the Dutch Parliament's defense committee. "The French should reconsider, the same with the Germans."

So far, France has confined its 1,000 soldiers to the relatively safe Kabul region, and new President Nicolas Sarkozy's offer of six Mirage fighters to patrol the southern skies won't alter the balance of power on the ground.

Canada's 3,000-strong contingent has suffered more than 70 dead, on a par with Britain. With resentment brewing over the performance of other allies, the war may now claim a political casualty: Prime Minister Stephen Harper.

The three opposition parties that hold a majority in the House of Commons are pressing Harper to pull the troops out by February 2009. Confidence votes in late October may bring down the government and force new elections.

Hostage-Takings

War fatigue has gripped Europe, with the public troubled by the guerrilla fighting with no fixed front lines or exit strategy and by constant hostage-takings and casualties.

In the latest kidnapping involving westerners, four Red Cross workers were abducted southwest of Kabul on Sept. 27. At least 900 Afghan civilians were killed in 2006, Human Rights Watch estimates; for the first eight months of 2007 alone, the United Nations puts the figure at over 1,000.

"This was sold as an easier mission than it turned out to be, and once things got difficult, the governments have done a miserable job of explaining why we've got to be there," says Tomas Valasek, a former Slovak Defense Ministry official now at the London-based Centre for European Reform.

Opposition on the European continent to a shooting war — 60 percent are against in France, 70 percent in Italy, according to a poll last month co-sponsored by the German Marshall Fund of the United States — raises questions whether Europe has the muscle to back up its foreign-policy ambitions.

German Attitudes

In Germany, the culture of pacifism that took root after the two world wars is clashing with 21st-century realities. Opposition to the Afghan war is highest there, with 75 percent of people against active combat, the poll found.

Germany's parliament has to approve the dispatch of troops overseas, and some Social Democrats in the ruling coalition plan to vote against reauthorizing the 3,000-strong mission on Oct. 12, firing a warning shot at Chancellor Angela Merkel. More resistance is likely next month when the Bundestag considers whether to yank 100 elite German troops from the U.S.-led counterinsurgency force.

“It may in the end just be a purely symbolic gesture, but it won't help Germany down the road if the image that's given by the government is that Germany's commitment to Afghanistan will be costless, non-violent and purely humanitarian,” says John K. Glenn, director of foreign policy at the German Marshall Fund in Washington.

Economy Neglected

One Social Democrat who plans to vote no, Klaus Barthel, blames the U.S. for overemphasizing military solutions and neglecting the buildup of Afghanistan's economy, which is still riddled with corruption and heavily dependent on poppy production.

“I don't detect readiness among the allies, rather a reliance on the military card in an increasingly fragile environment,” says Barthel, 51. “The policy doesn't seem to have any answers to the growing influence of the Taliban.”

One index of the Taliban's resurgence is the opium harvest, which rose 38 percent to a record 8,200 tons this year. Afghanistan produces 93 percent of the world's opium, the UN says, warning that the Taliban-infested southwest is taking on the traits of a narco-state.

Under pressure from Europe, the U.S. this year backed a “comprehensive approach” — code for putting more resources behind civilian reconstruction.

“Insurgency, weak governance and the narco-economy” may stall progress or throw Afghanistan back to where it was five years ago, UN Secretary-General Ban Ki-Moon wrote in a Sept. 21 report. One warning sign: Economic growth slipped to 8 percent in 2006–7 from 14 percent in 2005–6, according to the UN.

What remains, for visitors like Cook, the U.K. lawmaker, is a country reminiscent of 12th-century Europe: a “positively feudal, pre-Magna Carta system.”



Photo : Ebrahim Noroozi

FARS NEWS AGENCY

"They're always after me Lucky Charms!"



"Ummm..... No!"

