

# GBPPR 'Zine



Issue #90 / The Monthly Journal of the American Hacker / October 2011

*"We are getting exactly what the school system was designed to produce – a uniformly dumbed-down product of a compliant, lackluster people who have had their individuality crushed out of them by a system that rewards mediocrity."*

---- Quote from aerospace engineer John Ross on the talkback forum for *EDN* magazine. ([bit.ly/nHMMlm](http://bit.ly/nHMMlm))

## Table of Contents

- ◆ **Page 2 / Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)**
  - ◆ Procedures for the provisioning, maintenance, and troubleshooting of the 5ESS switch for CALEA applications.
- ◆ **Page 48 / Brown County, Wisconsin Bomb Squad Robot**
  - ◆ Various pictures of the Remotec robot used by the Brown County Bomb Squad.
- ◆ **Page 68 / Intercepting Older Digital Cordless Phones**
  - ◆ Experiment to decode digital audio from some older Sony & VTech 900 MHz cordless phones.
- ◆ **Page 85 / Sony SPP-ID910 Schematics**
  - ◆ Schematics for the Sony/VTech SPP-ID910 digital cordless phone.
- ◆ **Page 95 / Bonus**
  - ◆ So Much for Freedom of Speech
- ◆ **Page 96 / The End**
  - ◆ Editorial and rants.

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

The following error types are sent to CALEA ROP via the CALEA SAS error report when 5ESS experiences any abnormal condition related to CALEA functionality

<b>Error type:</b>	Attempt to send a CALEA message to a CALEA process failed.
<b>Condition:</b>	OSDS cannot send CALEA related message to a target CALEA process.
<b>Sensitive CALEA Data:</b>	Some scenarios will dump Party Identifier (calling or called party number).
<b>Potential Impact:</b>	Missing a CDC message, or an interception.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	Attempted to add monitoring station when 5 already exist.
<b>Condition:</b>	More than 5 LEAs are assigned to this packet subject.
<b>Sensitive CALEA Data:</b>	Party identifier (party member number): Either B1, B2, or D channel, and channel number.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	Bridge Resource Failure
<b>Condition:</b>	None
<b>Sensitive CALEA Data:</b>	None
<b>Priority :</b>	N/A
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	Bridge Loop Channel Unavailable
<b>Condition:</b>	Cannot bridge into the call, as loop channel is not available.
<b>Sensitive CALEA Data:</b>	Subject's port information
<b>Potential Impact:</b>	No call content is available.
<b>Priority :</b>	High
<b>Action to be considered:</b>	It may be required to relocate lines from this SM other SMs.
<b>Error type:</b>	CCC Dial Out Answer Timeout
<b>Condition:</b>	Law enforcement collection facility for CCC Dial Out did not answer call in specified time.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CCC data for surveillance.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	CCC Dial Out connection dropped
<b>Condition:</b>	Call to CCC destination LEA DN was either cleared or could not be established.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Call content is no longer provided to law enforcement.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	CCC Dial Out fanout not supported
<b>Condition:</b>	Subject to subject redirection resulted in an attempt to merge or fanout call content.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Call content is not provided or no longer provided to law enforcement for specified subject/surveillance.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	CCC Dial Out RCV path failed
<b>Condition:</b>	Attempt to establish CCC dial out subject receive connection failed.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Subject receive portion of call content is not provided to law enforcement for affected surveillance.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	CCC Dial Out retry failed
<b>Condition:</b>	Third attempt to establish CCC dial out connection failed.
<b>Sensitive CALEA Data:</b>	None

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

<b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	Call content is not provided to law enforcement for affected surveillance. High Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	CCC Dial Out three port conference circuit dropped Conference circuit used to combine subject transmit and receive is no longer available. None Call content is no longer provided to law enforcement for specified subject/surveillance. High Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	CCC Dial Out three port conference circuit unavailable A Conference circuit to combine subject transmit and receive is not available. None Call content is provided in separated mode. Low Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	CCC Dial Out unsupported supplementary service encountered A supplementary service (e.g., MLHG queuing, queued call pickup) at the intra-switch CCC destination LEA DN was encountered. None Call content is not provided to law enforcement. High Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	CCC Dial Out XMIT path failed Attempt to establish CCC dial out subject transmit connection failed. None Subject transmit portion of call content is not provided to law enforcement for affected surveillance. High Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	CCCTP cannot activate port, can not add. Cannot activate an outgoing CALEA CCC digital trunk port. In other words, CALEA cannot gain ownership of the trunk circuit and links the peripheral side data structures to the terminal process. Subject's port information. No call content is available. High Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	CCCTP cannot close network path The call content channel network path cannot be closed Subject's port information No call content is available High Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	CCCTP cannot idle all ports. Cannot successfully release the source and restore C-tone on the trunk. None No C-tone is restored. Low Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b>	CCCTP can not merge ports on different SMs. Two CCC bridges from different SMs are to be merged and is rejected. Bridge merging is required to merge the bridge and CCC resources associated with multiple subjects when one subject disconnects from a call but the call is not released (e.g. call transfer). None

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

<b>Potential Impact:</b>	One of the CCCs will not have call content.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	CCCTP can not release all ports
<b>Condition:</b>	Cannot de-couple the ports when more than one port is associated with the PCBLA.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Trunk ports are not properly released.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	CCCTP could not remove CTONE.
<b>Condition:</b>	It occurs when the hardware (e.g., DSU/DSU2) supplying the tone is OOS (high runner case) or Glctone (a global parameter) was overwritten with an invalid value.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Call content cannot be successfully delivered.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	CCCTP couple port failed, can not add.
<b>Condition:</b>	Cannot associate a CCC trunk port with the CALEA process.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Call content cannot be successfully delivered.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	CCCTP port access failed, can not add.
<b>Condition:</b>	Cannot find the port information from relation RLGROU_POR.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Call content cannot be successfully delivered.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel. It is unlikely unless database is corrupted.
<b>Error type:</b>	CCCTP port limit exceeded, can not add.
<b>Condition:</b>	There are more than 50 CCC trunks to be linked to one PCBLA for adding new CCC scenarios.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Call content cannot be successfully delivered.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	CCCTP port limit exceeded, cannot merge.
<b>Condition:</b>	There are more than 50 CCC trunks to be linked to one PCBLA for merging scenarios.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Call content cannot be successfully delivered.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	CCCTP port move failed, can not merge.
<b>Condition:</b>	Cannot move the PORTLA or CCB to the other CALEA process for merging scenarios. When ports are moved/merged, only the data structures are affected. All hardware related connections are unaffected.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Call content cannot be successfully delivered.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	CCCTP received MGINTERRUPT on port.
<b>Condition:</b>	CALEA receives unexpected message MGINTERRUPT for the CCC trunk.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	The call content channel will be released.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

<b>Error type:</b>	CCCTP rcv cannot be accessed.
<b>Condition:</b>	The receiving CCC trunk PCBLA structure and the CALEA process are not properly linked.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	The call content cannot be properly delivered.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.

<b>Error type:</b>	CCCTP trunk hunt failed, can not add.
<b>Condition:</b>	Cannot allocate CCC trunk successfully.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	The call content cannot be properly delivered.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Increase number of CCC trunks.

<b>Error type:</b>	CDC Dial Out connection dropped.
<b>Condition:</b>	SVC for CALEA IP Interface was disconnected due to PH hardware problems or X.25 packet network outage.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	CALEA CDC data will not be delivered for affected CDC SVC Dial Out surveillance case(s) until hardware/network outage is corrected.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Verify PH and X.25 packet network connections.

<b>Error type:</b>	CDC Dial Out message queue corrupt
<b>Condition:</b>	Software problem.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Impact: CDC message(s) in CDC Dial Out (SVC) message queue on specified SM are no longer available to law enforcement.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.

<b>Error type:</b>	CDC Dial Out message queue full
<b>Condition:</b>	CDC Dial Out message queue overflowed as a result of no active SVC(s) to establish TCP/IP socket.
<b>Sensitive CALEA Data:</b>	CALEA ASN.1 CDC message dumped to CALEA ROP may have subject's DN and other call identifying information.
<b>Potential Impact:</b>	CDC message(s) dumped on CALEA ROP will no longer be available to send to law enforcement.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.

<b>Error type:</b>	CDC Dial Out set failed due to invalid data.
<b>Condition:</b>	SVC-related CALEA surveillance provisioning is incorrect. RC view C.4's SVC LOC LEA CDC TN, SVC DEST LEA CDC TN or RC view 33.2 (IP INTERFACE ASSIGNMENT)/23.40 (X.25 (XAT) PACKET SWITCHING CHANNEL ASSIGNMENT) provisioning for SVC LOC LEA CDC TN is incorrect.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	CALEA CDC data will not be delivered until provisioned data is corrected. If condition is not corrected, CALEA CDC data will not be delivered to law enforcement collection facilities.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Verify data provisioned on above RC views to CALEA customer documentation.

<b>Error type:</b>	CDC Dial Out setup failed, will attempt retry
<b>Condition:</b>	SVC for CALEA IP Interface could not be established due to OOS XAT logical channel, the X.25 SVC could not be established due to network problems or temporary PH resource contention.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	CALEA CDC data will not be delivered until XAT logical channel is restored to in-service or temporary network problems are corrected.
<b>Priority :</b>	High

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

<b>Action to be considered:</b>	Restore OOS XAT logical channel, check X.25 packet network.
<b>Error type:</b>	CDC message dropped, GR30 interface send failed
<b>Condition:</b>	Third attempt to send a CDC message over a GR30 connection failed.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CDC data for surveillance(s) using specific GR30.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	CDC or PDC Message length invalid
<b>Condition:</b>	The message to be sent to LEA is more than 500 bytes.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	The call data cannot be properly delivered.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel. It should not happen.
<b>Error type:</b>	Can not create surveillance bridge
<b>Condition:</b>	CALEA bridge process cannot be successfully created to perform interception.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	The subject call cannot be properly intercepted.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	It should not happen unless the SM is overloaded.
<b>Error type:</b>	Could not apply CTONE
<b>Condition:</b>	CALEA cannot provide CTONE to CCC trunks.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	No CCC trunks are available if call is intercepted.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	Destination GR30 LEA CDC DN not recognized by digit analysis
<b>Condition:</b>	GR30 destination LEA DN doesn't pass digit analysis or has an invalid destination type.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CDC data for surveillance(s) using specific GR30.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Verify the GR30 destination LEA DN.
<b>Error type:</b>	Digit Surge Tone Decoder Dropped
<b>Condition:</b>	A burst of digits greater than 100 digits in 20 seconds occurred.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CDC dialed digit extraction message.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Nothing we can do about it.
<b>Error type:</b>	Discarding buffered CDC messages due to inactivity
<b>Condition:</b>	Failed to establish the GR30 CDC Dial out connection in specified time.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Queued CDC messages will be dumped to the CALEA ROP.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	Error return from close application program interface.
<b>Condition:</b>	Socket cannot be successfully deleted.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	None. The CALEA socket was closed due no surveillance case using the socket (destination IP address and port). Another CALEA TCP/IP socket will be established if another CDC message needs to be sent.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	None
<b>Error type:</b>	Error return from connect application program interface.
<b>Condition:</b>	Cannot initiate socket connection.
<b>Sensitive CALEA Data:</b>	None

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

<b>Potential Impact:</b>	CDC cannot be properly delivered.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	Error return from getsockdesc application program interface.
<b>Condition:</b>	Cannot retrieve a socket descriptor associated with the local IP address.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	CDC cannot be properly delivered.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	Error return from getsockname application program interface.
<b>Condition:</b>	None
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	None
<b>Priority :</b>	N/A
<b>Error type:</b>	Error return from select application program interface.
<b>Condition:</b>	None
<b>Sensitive CALEA Data:</b>	None
<b>Priority :</b>	N/A
<b>Error type:</b>	Error return from send application program interface.
<b>Condition:</b>	The TCP packet cannot be successfully sent.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	CDC message cannot be properly delivered.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	Error return from setsockopt application program interface.
<b>Condition:</b>	Cannot set socket option.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	CDC message cannot be properly delivered.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	Error return from shutdown application program interface.
<b>Condition:</b>	Cannot shut down the receiving direction for the socket.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	None
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	Error return from socket application program interface.
<b>Condition:</b>	Cannot create a new socket to the destination socket address.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	CDC message cannot be properly delivered.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	Failed to route to GR30 LEA CDC DN
<b>Condition:</b>	Attempt to establish GR30 CDC dial out connection failed.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CDC data for surveillance(s) using specific GR30.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Verify the routing for GR30 destination LEA DN.
<b>Error type:</b>	Failed to send GR30 CDC message to link SM
<b>Condition:</b>	Attempt to send a CDC message to the SM with the GR30 connection failed.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CDC data for surveillance(s) using specific GR30.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	Found socket data inconsistency. Internal socket data structure is corrupted. None CDC message cannot be properly delivered. Low Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	GR30 CAGS TP received MGINTERRUPT GR30 process received an unexpected MGINTERRUPT. None Missing CDC data for surveillance(s) using specific GR30. Low Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	GR30 CAGS/CAGR TP cannot be created GR30 process cannot be created. None Missing CDC data for surveillance(s) using specific GR30. Low Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	GR30 CDC connection dropped Call to GR30 CDC destination LEA.DN was either cleared or could not be established. None Missing CDC data for surveillance(s) using specific GR30. High Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	GR30 CDC message discarded. Link occupancy above threshold Attempt to send a CDC message to another SM and the SM to SM link occupancy above threshold. None The CDC message will be dumped to the CALEA ROP. Low Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	GR30 Internal Failure Internal failure encountered while processing a CDC message. None Missing CDC data for surveillance(s) using specific GR30. Low Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	GR30 Length of CDC message too large for OSDS Received a CDC message too large to process. None CDC message will be dumped to the CALEA ROP. Low Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	GR30 msg queue full, oldest message discarded The GR30 CDC message buffer is already full when another CDC message is received. None The CDC message will be dumped to the CALEA ROP. Low Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	HEARTBEAT message dropped, GR30 interface send failed Third attempt to send a HEARTBEAT CDC message over a GR30 connection failed. None Missing CDC data for surveillance(s) using specific GR30. Low Contact Lucent TSS personnel.

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

<b>Error type:</b>	IAP times out waiting for login digits
<b>Condition:</b>	Law enforcement collection facility for GR30 CDC Dial Out didn't respond with GR30 login digits in the specified time.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CDC data for surveillance(s) using specific GR30.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact LEA personnel.

<b>Error type:</b>	Invalid IP route
<b>Condition:</b>	The IP route destination for an incoming IP datagram is not associated with a CALEA IP interface. The CALEA TCP/IP Security Enhancement feature discarded the incoming IP datagram.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Unauthorized access to a switch processor (SMP or PH) via CALEA IP interface was detected. If the unauthorized activity continues, the CALEA IP interface will be removed from service. Valid CALEA CDC/PDC data delivery will be impacted if no other IP interface is available for the destination IP address.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Verify IP network for security breach or misconfiguration.

<b>Error type:</b>	Invalid LOGIN digits received
<b>Condition:</b>	Law enforcement collection facility for GR30 CDC Dial Out responded with invalid GR30 login digits.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CDC data for surveillance(s) using specific GR30.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact LEA personnel.

<b>Error type:</b>	Invalid Protocol Handler CAL_INFO attribute value.
<b>Condition:</b>	Could not find a case ID from CAL_INFO for a packet subject.
<b>Sensitive CALEA Data:</b>	Call Content in X.25 Packet format.
<b>Potential Impact:</b>	Missing call content of the packet subject.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.

<b>Error type:</b>	IP datagram fragment received
<b>Condition:</b>	An IP datagram fragment received on a CALEA IP interface was detected. The CALEA TCP/IP Security Enhancement feature discarded the incoming IP datagram fragment.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	A potential security breach was detected on a CALEA IP interface. If the unauthorized activity continues, the CALEA IP interface will be removed from service. Valid CALEA CDC/PDC data delivery will be impacted if no other IP interface is available for the destination IP address.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Verify IP network for security breach or misconfiguration.

<b>Error type:</b>	LOGIN message dropped, GR30 interface send failed
<b>Condition:</b>	Third attempt to send a LOGIN CDC message over a GR30 connection failed.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CDC data for surveillance(s) using specific GR30.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.

<b>Error type:</b>	LOGIN Successful
<b>Condition:</b>	Law enforcement collection facility for GR30 CDC Dial Out responded with valid GR30 login digits.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	None
<b>Priority :</b>	N/A
<b>Action to be considered:</b>	None

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

<b>Error type:</b>	No FSK or UTD resources available for GR30 interface
<b>Condition:</b>	Attempt to establish GR30 CDC dial out connection failed because no FSK resources were available.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CDC data for surveillance(s) using specific GR30.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.

<b>Error type:</b>	No IP route.
<b>Condition:</b>	There is no IP routing information available for the incoming IP packet. The CALEA TCP/IP Security Enhancement feature detected and discarded an incoming IP packet datagram that is not a response to switch-generated IP data.
<b>Sensitive CALEA Data:</b>	None.
<b>Potential Impact:</b>	Unauthorized access to a switch processor (SMP or PH) via CALEA IP interface was detected. If the unauthorized activity continues, the CALEA IP interface will be removed from service. Valid CALEA CDC/PDC data delivery will be impacted if no other IP interface is available for the destination IP address.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Verify IP network for security breach or misconfiguration.

<b>Error type:</b>	No Tone Decoder Available
<b>Condition:</b>	Cannot allocate a tone decoder.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	No Dialed Digit Extraction CDC message can be sent.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Notify switch maintenance personnel. Additional tone decoders may need to be provisioned in the office.

<b>Error type:</b>	PDC collection facility IP address not obtained.
<b>Condition:</b>	Cannot determine which IP address and port to be sued for a packet level II subject.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	No call content is sent and the intercepted call is handled as a level I subject.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.

<b>Error type:</b>	PSLAESCASE tuple missing when adding new monitoring station.
<b>Condition:</b>	PSLAESCASE tuple is not available for a packet subject.
<b>Sensitive CALEA Data:</b>	Party identifier (party member number): Either B1, B2, or D channel, and channel number.
<b>Potential Impact:</b>	Call content for the packet subject may not be available.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.

<b>Error type:</b>	Protocol Handler Resource CAL_INFO Exhaustion
<b>Condition:</b>	None
<b>Sensitive CALEA Data:</b>	Party identifier: Either B1, B2, or D member.
<b>Potential Impact:</b>	Party identifier: Either B1, B2, or D member
<b>Priority :</b>	High
<b>Action to be considered:</b>	The SRE RC view can be used to insert more RLCAL_INFO tuples in the affected SMs.

<b>Error type:</b>	RLCASE_IDX data inconsistency
<b>Condition:</b>	Could not find a matching LAES case ID in relation RLcase_idx for a packet subject.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing packet data channel as IP address cannot be obtained
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.

<b>Error type:</b>	RLCASE_IDX tuple missing.
<b>Condition:</b>	Could not find the expected tuple in relation RLCASE_IDX.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CCC and/or CDC.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

<b>Error type:</b>	RLEQUIPDSL tuple missing
<b>Condition:</b>	Could not find the expected tuple in relation RLEQUIPDSL.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CDC data for surveillance(s) using specified tuple.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	RLFC_LINE tuple missing
<b>Condition:</b>	Could not find the expected tuple in relation RLFC_LINE.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CDC data for surveillance(s) using specified tuple.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	RLGR30INTF tuple missing
<b>Condition:</b>	Could not find the expected tuple in relation RLGR30INTF.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CDC data for surveillance(s) using specified tuple.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	RLLAESCASE tuple missing.
<b>Condition:</b>	Could not find the expected tuple in relation RLLAESCASE.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CCC and/or CDC.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	RLLAESPROF tuple missing.
<b>Condition:</b>	Could not find the expected tuple in relation RLLAESPROF.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CDC messages.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	RLOFFICECODE tuple missing
<b>Condition:</b>	Could not find the expected tuple in relation RLOFFICECODE.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Subject's DN is not outputted at end of call content when using CCC Dial Out.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	RLPORTLA tuple missing
<b>Condition:</b>	Could not find the expected tuple in relation RLPORTLA.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CDC data for surveillance(s) using specified tuple.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	RLPR_DNTRAN tuple missing
<b>Condition:</b>	Could not find the expected tuple in relation RLPR_DNTRAN.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CDC data for surveillance(s) using Local LEA CDC DN.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	RLRTDNMOD tuple missing
<b>Condition:</b>	Could not find the expected tuple in relation RLRTDNMOD.
<b>Sensitive CALEA Data:</b>	None
<b>Potential Impact:</b>	Missing CCC or CDC data.
<b>Priority :</b>	High
<b>Action to be considered:</b>	Contact Lucent TSS personnel.
<b>Error type:</b>	RLRT_DNTRAN tuple missing

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

<b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	Could not find the expected tuple in relation RLRT_DNTRAN. None Call content is not provided to law enforcement for surveillance(s) requiring DN in RLRT_DNTRAN tuple. High Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	Resource Unavailable. The port for a CCC trunk is not in a valid state. None Missing CTONE. High Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	Socket not found. Could not find the last connected socket or a connected socket. It occurs when a/the TCP/IP socket used to send CDC data or X.25 packets for a subject's X.25 packet call could not be located. None For CDC, another socket will be established. For PDC, subject call content is lost. Low Contact Lucent TSS personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	Surveillance not started due to SM RLCAL_INFO Exhaustion. Could not allocate RLCAL_INFO for an intercepted subject. None CDC and CCC cannot be properly delivered. High The SRE RC view can be used to insert more RLCAL_INFO tuples in the affected SMS.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	Tone Decoder Dropped. Tone decoder dropped due to other failure/maintenance. None Missing DDE CDC message. Low Notify maintenance personnel.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	Tone Decoder Dropped Due to Load. Tone decoder is dropped, as there is no digit is received after one minute and the tone decoder usage is over the threshold. None Missing DDE CDC message. Low No action is required unless LEA wants the DTMF status become essential.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b> <b>Potential Impact:</b> <b>Priority :</b> <b>Action to be considered:</b>	Too many IP datagrams received Too many (more than 5 in 10 seconds) TCP/IP datagrams received on a CALEA IP interface had inappropriate data in TCP segment. A TCP/IP segment can only have SYN+ACK, ACK, FIN, FIN+ACK, or RST and no attached data. None A potential security breach was detected on a CALEA IP interface. If the unauthorized activity continues, the CALEA IP interface will be removed from service. Valid CALEA CDC/PDC data delivery will be impacted if no other IP interface is available for the destination IP address. High Verify IP network for security breach or misconfiguration.
<b>Error type:</b> <b>Condition:</b> <b>Sensitive CALEA Data:</b>	WARNING: GR30 buffered messages will be discarded in 15 minutes Failed to establish the GR30 CDC Dial out connection. 15 minutes before start dumping CDC messages to the CALEA ROP. None

# **Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)**

## **Provisioning, Troubleshooting, and Maintenance**

235-200-400

June 2003

<b>Potential Impact:</b>	The CDC messages will be dumped to the CALEA ROP.
<b>Priority :</b>	Low
<b>Action to be considered:</b>	Contact Lucent TSS personnel.

235-200-400

June 2003

### 7. RECENT CHANGE VIEWS - CLASS 33

For your convenience, this chapter contains a detailed description of each Class 33 recent change view used by network administrators or others involved in the provisioning tasks for the CALEA feature set.

These views, along with all other recent change views referenced in this information product are also documented in 235-118-25x, *5ESS<sup>®</sup> Switch Recent Change Reference*. Also, detailed procedures for the general use of the switch's Recent Change interface are documented in 235-118-251, *Recent Change Procedures*.

**NOTE:** The views contained in this Chapter apply to the 5E15 software release. The 33 class of views were **not** modified for the CALEA application between the 5E14 and 5E15 software releases. View 33.2 was modified in the 5E15 software release due to a non-CALEA feature and is documented appropriately. Please refer to

- 235-118-255, *5ESS<sup>®</sup> Switch Recent Change Reference — 5E14 Software Release*, for 5E14-specific documentation.
- 235-118-256, *5ESS<sup>®</sup> Switch Recent Change Reference — 5E15 Software Release*, for 5E15-specific documentation.
- 235-118-257, *5ESS<sup>®</sup> Switch Recent Change Reference — 5E16.1 Software Release*, for 5E16.1-specific documentation.
- 235-118-258, *5ESS<sup>®</sup> Switch Recent Change Reference — 5E16.2 Software Release*, for 5E16.2-specific documentation.
- 235-118-259, *5ESS<sup>®</sup> Switch Recent Change Reference — 5E17.1 Software Release*, for 5E17.1-specific documentation.

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

### 33V1 INTERNET PROTOCOL (RC\_IPPROC)

Form ID: 33V1

Form Name: RC\_IPPROC

View ID: RVIPPROC

Title: INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

#### 1. VIEW DESCRIPTION:

The INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT view (33.1) provides the capability to provision up to five IP addresses and subnet masks, and associated IP, TCP and UDP parameters to a processor (SM or PH).

#### 1.1 VIEW INFORMATION:

SOFTWARE RELEASE = 5E15

OFFICE RECORD(S) = (5987)

ODA FORM NAME = ipproc

ODA FORM TITLE = INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

ODA OFFICE RECORD(S) = 5987

VIEW PERMISSIONS = RUDI

MAXIMUM TIME OUT = 330

FUNCTION NAME = vipproc

ERROR ID = 660

---

SCREEN 1 OF 2  
(5987)

5ESS SWITCH  
RECENT CHANGE 33.1  
INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

\*1. PROCESSOR ID \_\_\_\_  
\*2. PROCESSOR TYPE \_\_\_\_  
(\* ) 3. QUALIFIER 2 \_\_\_\_  
(\* ) 4. QUALIFIER 3 \_\_\_\_

5. IP ADDRESS

ROW	LOCAL IP ADDR	IP SUBNET MASK
1	____.____.____.____	____.____.____.____
2	____.____.____.____	____.____.____.____
3	____.____.____.____	____.____.____.____
4	____.____.____.____	____.____.____.____
5	____.____.____.____	____.____.____.____

---

5ESS SWITCH

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

```
SCREEN 2 OF 2                                RECENT CHANGE 33.1
(5987)                                       INTERNET PROTOCOL (IP) PROCESSOR ASSIGNMENT

IP PARAMETER ASSIGNMENT                     UDP PARAMETER ASSIGNMENT
16. REASSEM TIMER _____                23. UDP CHKSUM EN _____
17. ICMP ERR CNT _____                 24. UDP START PORT _____
18. MTU ENABLE _____                   25. UDP DEF TTL _____
19. MTU DISC _____

TCP PARAMETER ASSIGNMENT
20. TCP MSS _____
21. TCP START PORT _____
22. TCP DEF TTL _____
```

---

## 2. FIELD DEFINITIONS

- \* **1. PROCESSOR ID - (PROCESSORID) - (domain IM)** - The ID of the processor. For SM, the SM number. For PH, the number of the SM on which the PH resides.

**Domain:**

Enter a number from 1 to 192.

**Default:** no default

- \* **2. PROCESSOR TYPE - (PROCESSORTYPE) - (domain PRCTP)** - The type of processor.

**Domain:**

Enter SM or PH.

**Default:** no default

**Form Checks:**

If PROCESSORTYPE equals "SM", then do the following:

QUALIFIER2 is set to unspecified.

QUALIFIER3 is set to unspecified.

If PROCESSORTYPE equals "PH", then QUALIFIER2 must be specified.

If PROCESSORTYPE equals "PH", then QUALIFIER3 must be specified.

- (\* **3. QUALIFIER 2 - (QUALIFIER2) - (domain I0\_254)** - Second qualifier of the processor address. For a PH, this field is the PSU community address (COM ADDR) found on RC view 22.2, Packet Switch Unit.

**Domain:**

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

For an SM, leave blank. For a PH enter a number from 1 - 254.

**Default:** no default

**Form Checks:**

See form check(s) for PROCESSORTYPE.

(\* **4. QUALIFIER 3 - (QUALIFIER3) - (domain QUAL3)** - Third qualifier of the processors address.

**Domain:**

For an SM, leave blank. For a PH, enter PSU SHELF [0-4] (RC view 22.16) and channel group [00-15] (GRP from RC view 22.16).

**Default:** no default

**Form Checks:**

See form check(s) for PROCESSORTYPE.

**5. IP ADDRESS - (IPADDRESS) - (domain positional list with 5 rows)** - IP addresses consisting of a Local IP address and subnet mask. At least one IP address must be specified.

**Form Checks:**

For every element in the list IPADDRESS do the following:

If IPSUBNETMASK.IPADDR0 is specified, then IPSUBNETMASK.IPADDR0 must equal "255".

If LOCALIPADDR.IPADDR0 is specified, then LOCALIPADDR.IPADDR0 must be in {"001" thru "126", "128" thru "223"}.

On IPADDRESS element, do the following:

If LOCALIPADDR is specified, then IPSUBNETMASK must be specified.

If IPSUBNETMASK is specified, then LOCALIPADDR must be specified.

If LOCALIPADDR is specified, then LOCALIPADDR.IPADDR0 concatenated with LOCALIPADDR.IPADDR1 concatenated with LOCALIPADDR.IPADDR2 concatenated with LOCALIPADDR.IPADDR3 must be in {"001000000001" thru "126255255254", "128001000001" thru "191254255254", "19200001001" thru "223255254254"}.

If LOCALIPADDR.IPADDR0 is in {"001" thru "126"}, then do the following:

IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255000000000", "255192000000" thru "255255255000"}.

LOCALIPADDR.IPADDR1 concatenated with LOCALIPADDR.IPADDR2 concatenated with LOCALIPADDR.IPADDR3 must not be in {"000000000", "255255255"}.

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

If LOCALIPADDR.IPADDR0 is in {"128" thru "191"}, then do the following:

IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255255000000", "255255192000" thru "255255255000"}.

LOCALIPADDR.IPADDR2 concatenated with LOCALIPADDR.IPADDR3 must not be in {"000000", "255255"}.

If LOCALIPADDR.IPADDR0 is in {"192" thru "223"}, then do the following:

IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255255255000", "255255255192" thru "255255255240"}.

LOCALIPADDR.IPADDR3 must not be in {"000", "255"}.

See form check(s) for IPADDRESS.LOCALIPADDR.

**LOCAL IP ADDR - (IPADDRESS.LOCALIPADDR) - (structure domain CIPADDR)** - Local IP address which is to be assigned to the processor.

**Domain:**

For Local IP address set 1, enter 0 - 126 for Class A, 128 - 191 for Class B, or 192 - 223 for Class C. For Local IP address set 2, 3, and 4, enter 0 - 255.

**Form Checks:**

The count of elements of {select LOCALIPADDR from IPADDRESS} must be greater than 0.

{Select LOCALIPADDR from IPADDRESS} must be a unique set.

- (IPADDRESS.LOCALIPADDR.IPADDR0) - (domain C0\_255RZ) - .

**Default:** no default

- (IPADDRESS.LOCALIPADDR.IPADDR1) - (domain C0\_255RZ) - .

**Default:** no default

- (IPADDRESS.LOCALIPADDR.IPADDR2) - (domain C0\_255RZ) - .

**Default:** no default

- (IPADDRESS.LOCALIPADDR.IPADDR3) - (domain C0\_255RZ) - .

**Default:** no default

**IP SUBNET MASK - (IPADDRESS.IPSUBNETMASK) - (structure domain CIPADDR)** - IP subnet mask to be assigned to the processor.

**Domain:**

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

Blank, or enter 255 for IP subnet mask set 1. Blank, or enter 0 - 255 for IP subnet mask set 2, 3, and 4.

- (IPADDRESS.IPSUBNETMASK.IPADDR0) - (domain C0\_255RZ) - .

**Default:** no default

- (IPADDRESS.IPSUBNETMASK.IPADDR1) - (domain C0\_255RZ) - .

**Default:** no default

- (IPADDRESS.IPSUBNETMASK.IPADDR2) - (domain C0\_255RZ) - .

**Default:** no default

- (IPADDRESS.IPSUBNETMASK.IPADDR3) - (domain C0\_255RZ) - .

**Default:** no default

**16. REASSEM TIMER - (REASSEM\_TIMER) - (domain I1\_255)** - Time in seconds that the processor waits to process a packet.

**Domain:**

Enter 1 to 255 seconds

**Default:** default = 60

**17. ICMP ERR CNT - (ICMPERRCNT) - (domain I20\_255)** - Number of bytes returned in internet control message protocol (ICMP) error reporting message for this processor.

**Domain:**

Enter 20 to 255 bytes.

**Default:** default = 64

**18. MTU ENABLE - (MTUENABLE) - (domain BOOL)** - Flag to indicate whether the maximum transmission unit discovery algorithm is enabled.

**Domain:**

Enter Y for yes or N for no.

**Default:** default = N

**19. MTU DISC - (MTUDISC) - (domain I10\_10000)** - Interval in seconds at which the path maximum transmission unit (MTU) discovery algorithm tries to increase the MTU.

**Domain:**

Enter 10 to 10000 seconds.

**Default:** default = 30

**20. TCP MSS - (TCPMSS) - (domain I108\_8000)** - The maximum segment size for the transmission control protocol in bytes.

**Domain:**

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

Enter 108 to 8000 bytes.

**Default:** default = 536

**21. TCP START PORT - (TCPSTARTPORT) - (domain I32768\_65535)** - Lowest automatically allocated (ephemeral) port number for a transmission control protocol connection. Modifying the TCP Start Port field may result in the tear down of any/all currently existing sockets.

**Domain:**

Enter a number from 32768 to 65535.

**Default:** default = 49152

**Form Checks:**

If the database operation equals "U", then TCPSTARTPORT must equal OLDTCPSTARTPORT, otherwise the following warning will be issued: "Updating the TCP starting ephemeral port may reset existing TCP connections using this processor."

See form check(s) for IPADDRESS.LOCALIPADDR.

**22. TCP DEF TTL - (TCPDEFTTL) - (domain I1\_255)** - The number of intermediate hops a packet can make before being discarded (one hop is assumed to take one second).

**Domain:**

Enter 1 to 255.

**Default:** default = 255

**23. UDP CHKSUM EN - (UDPCHKSUMEN) - (domain BOOL)** - Flag to indicate if the datagram protocol checksum option is enabled.

**Domain:**

Enter Y for yes or N for no.

**Default:** default = Y

**24. UDP START PORT - (UDPSTARTPORT) - (domain I32768\_65535)** - Lowest automatically allocated (ephemeral) port number for a datagram protocol connection. Modifying the UDP Start Port field may result in the tear down of any/all currently existing sockets.

**Domain:**

Enter a number from 32768 to 65535.

**Default:** default = 49152

**Form Checks:**

If the database operation equals "U", then UDPSTARTPORT must equal OLDUDPSTARTPORT, otherwise the following warning will be issued: "Updating the UDP starting ephemeral port may reset existing UDP connections using this processor."

See form check(s) for IPADDRESS.LOCALIPADDR.

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

**25. UDP DEF TTL - (UDPDEFTTL) - (domain l1\_255)** - The number of intermediate hops a packet can make before being discarded (one hop is assumed to take one second).

**Domain:**

Enter 1 to 255.

**Default:** default = 255

### 3. TRIGGER FUNCTIONS

BASE RELATION = TRIGGER FUNCTION (PERMISSIONS)

RLIPTOPCR = PSiptopcr (iud)  
RLPCRTOIP = PSpcrtiop (ud)  
RLPROTPARM = PSprotparm (iud)

### 4. BASE RELATIONS

(PERMISSIONS) BASE RELATION — DISTRIBUTION

(r) RLDSLGDATA — FP  
(r) RLMODATT — LR  
(r) RLPSUSM — LRF  
(u) RLIPADRLOC — FR  
(u) RLIPADRLOC — FR  
(u) RLLOCIPADR — LP  
(u) RLPCRTOIP — FR  
(u) RLPROTPARM — FP  
(u) RLRC\_HOLE — LP  
(u) RLRC\_QIDX — LP

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

### 33V2 INTERNET PROTOCOL (RC\_IPINTF)

Form ID: 33V2

Form Name: RC\_IPINTF

View ID: RVIPINTF

Title: INTERNET PROTOCOL (IP) INTERFACE ASSIGNMENT

#### 1. VIEW DESCRIPTION:

The INTERNET PROTOCOL (IP) INTERFACE ASSIGNMENT view (33.2) provides the capability to provision up to five IP addresses and subnet masks, and associated IP parameters to an internet interface. View may be keyed by:

- PKT TN and LCN
- PKT MLHG, PKT MEMB and LCN
- TGN, TGN MEMB and LCN
- OE, ISCN and LCN

#### 1.1 CHANGES THIS RELEASE:

- The allowed range of multiline hunt group was increased from 1 - 2000 to 1 - 8191 for the Multiline Hunt Group Capacity Expansion feature. This feature was first made available in the 5E15 software release.

#### 1.2 VIEW INFORMATION:

SOFTWARE RELEASE = 5E15

OFFICE RECORD(S) = (5988)

ODA FORM NAME = ipintf

ODA FORM TITLE = INTERNET PROTOCOL (IP) INTERFACE ASSIGNMENT

ODA OFFICE RECORD(S) = 5988

VIEW PERMISSIONS = RUDI

MAXIMUM TIME OUT = 330

FUNCTION NAME = vipintf

ERROR ID = 831

---

5ESS SWITCH  
RECENT CHANGE 33.2  
(5988) INTERNET PROTOCOL (IP) INTERFACE ASSIGNMENT

(*) 1. PKT TN	_____	12. IP ADDRESS
(*) 2. PKT MLHG	_____	ROW GATEWAY IP ADDR IP SUBNET MASK



# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

**Form Checks:**

See form check(s) for PKTTN.

- (\*) **3. PKT MEMB - (PKTMEMB) - (domain MEMBR1)** - This field specifies the number of a particular member within the specified packet switching multiline hunt group. The PKT MLHG and PKT MEMB combination can either be an individual packet service on a DSL (PPB1 or PPB2) or an XAT.

**Domain:**

Enter a number from 1 to 2015.

*Interactions:* This PKT MEMB and group must be provisioned with a destination facility type (FCL TYPE) of INET on View 23.11.

**Default:** no default

**Form Checks:**

See form check(s) for PKTTN.

- (\*) **4. TGN - (TGN) - (domain TRKGRP1)** - This field specifies the group number for the trunk associated with the IP interface.

**Domain:**

Enter a number from 1 to 4000.

*Interactions:* This field can only be greater than 2000 when the Increased Number of Trunk Groups (SFID 172) feature has been purchased using the Secured Feature Upgrade view (8.22). This TGN and member must be provisioned with a destination facility type (FCL TYPE) of INET on view 5.5.

**Default:** no default

**Form Checks:**

See form check(s) for PKTTN.

- (\*) **5. TGN MEMB - (TGNMEMB) - (domain X75PMEMB)** - This field specifies the number of a particular trunk member within the specified trunk group.

**Domain:**

Enter a number from 0 to 23.

*Interactions:* This TGN MEMB and TGN must be provisioned with a destination facility type (FCL TYPE) of INET on View 5.5

**Default:** no default

**Form Checks:**

See form check(s) for PKTTN.

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

(\*) **6. OE - (OE) - (structure domain DSLXATOE)** - Enter one alphabetic character followed by an equipment number of the following format:

**Form Checks:**

See form check(s) for PKTTN.

**- (OE.LCENTYPE) - (domain DSLXATOETY)** - Office equipment line card equipment type.

**Domain:**

Enter A, D, E, G, I, K, N, or O where:

**Where:**

A = INEN [Integrated Digital Loop Carrier (IDLC) Network Equipment Number].  
D = DEN [Digital Line Trunk Unit Equipment Number].  
E = AIUEN [Digital (U Circuit) Access Interface Unit (AIU) Equipment Number].  
G = GEN [GAMA-Integrated Digital Carrier Unit (IDCU) Equipment Number].  
I = ISDN [Digital (U & T Card) Integrated Services Line Unit (ISLU) Equipment Number].  
K = LCKEN [Digital (T & U Circuit) Integrated Services Line Unit 2 (ISLU2) Equipment Number].  
N = NEN [Digital Networking Unit - SONET (DNU-S) Equipment Number].  
O = OIUEN [Optical Interface Unit Equipment Number]

**Default:** no default

**- (OE.LCEN) - (domain LEN)** - Office equipment line card equipment number.

**Domain:**

For INEN [Integrated Digital Loop Carrier (IDLC) Network Equipment Number], enter (1-192) (0-7) (01-99) (0001-2048) where:

**Where:**

(1-192) = SM (Switching Module)  
(0-7) = DNUS (Digital Networking Unit - SONET)  
(01-99) = RT (Remote Terminal)  
(0001-2048) = LINE (Remote Line)

For DEN [Digital Trunk Equipment Number], enter (1-192) (0-5) (01-10) (01-48) where:

**Where:**

(1-192) = SM (Switching Module)  
(0-5) = DLTU (Digital Line Trunk Unit)  
(01-10) = DFI (Digital Facility Interface)  
(01-48) = DCHAN (Digital Channel)

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

For AIUEN [Digital (U Circuit) Access Interface Unit Equipment Number], enter (1-192) (000-104) (00-19) (00-15) where:

**Where:**

(1-192) = SM (Switching Module)  
(000-104) = AIU (Access Interface Unit)  
(00-19) = PACK (Pack number)  
(00-15) = CKT (Circuit number)

For RT GEN [GAMA-Integrated Digital Carrier Unit (IDCU) Equipment Number], enter (1-192) (00-42) (01-31) (0001-2048) where:

**Where:**

(1-192) = SM (Switching Module)  
(00-42) = IDCU (Integrated Digital Carrier Unit)  
(01-31) = RT (Remote Terminal)  
(0001-2048) = LINE (Remote Line)

For ISDN [Digital (U & T Card) Integrated Services Line Unit (ISLU) Equipment Number], enter (1-192) (0-7) (00-15) (00-31) where:

**Where:**

(001-192) = SM (Switching Module)  
(0-7) = ISLU (Integrated Services Line Unit)  
(00-15) = LGC (Line Group Card)  
(00-31) = LC (Line Card)

For LCKEN [Digital (T & U Circuit) Integrated Services Line Unit 2 (ISLU2) Equipment Number], enter (1-192) (00-42) (00-15) (0-7) (00-07) where:

**Where:**

(1-192) = SM (Switching Module)  
(00-42) = ISLU2 (Integrated Services Line Unit Two)  
(00-15) = LGC (Line Group Card)  
(0-7) = L Board (Line Board).  
(00-07) = L Circuit (Line Circuit)

For NEN [Digital Networking Unit - SONET (DNU-S) Equipment Number], enter (1-192) (0-7) (0-1) (0-5) (01-28) (01-24) where:

**Where:**

(1-192) = SM (Switching Module)  
(0-7) = DNUS (Digital Networking Unit - SONET)

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

(0-1) = DG (Data Group)  
(0-5) = STS (Synchronous Transport Signal number)  
(01-28) = VT (Virtual Tributary)  
(01-24) = DS0 (Digital Signal Level 0 channel)

For OUIEN [Optical Interface Unit Equipment Number], enter (000-192) (0-7) (0-9) (1) (1-3) (1-7) (1-4) where:

**Where:**

(000-192) = SM (Switching Module)  
(0-7) = OIU (Optical Interface Unit Number)  
(0-1) = PG (Protection Group Number)  
(1) = OC-3 (Optical Carrier Level-3 Number)  
(1-3) = STS (Synchronous Transport Signal Number)  
(1-7) = VTG (Virtual Tributary Group)  
(1-4) = VTM (Virtual Tributary Member)  
(1-28) = CH (Channel Number)

**Default:** no default

(\* **9. ISCN - (ISCN) - (domain ISCN)** - This field specifies the ISCN to which the address is to be assigned.

**Domain:**

Enter SU shelf[0-4] CHL group [00-15] PH chan [000-127]

**Default:** no default

**Form Checks:**

See form check(s) for PKTTN.

\* **10. LCN - (LCN) - (domain LCN1)** - This field defines the Logical Channel Number for the packet switching interface.

**Domain:**

Enter a number from 1 to 127.

**Default:** no default

# **11. INTERFACE NAME - (INTERFACENAME) - (domain INTFNM)** - This field specifies the name of the interface.

**Domain:**

Enter name starting with an alphanumeric character followed by 4 to 18 characters including '.', '\_', or '-'.  
The name must be unique within the interface.

**Default:** no default

**12. IP ADDRESS - (IPADDRESS) - (domain positional list with 5 rows)** - Gateway or interface addresses consisting of an IP address and subnet mask. At least one IP address must be specified.

**Form Checks:**

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

For every element in the list IPADDRESS do the following:

If IPSUBNETMASK.IPADDR0 is specified, then IPSUBNETMASK.IPADDR0 must equal 255.

If GATEWAYIPADDR.IPADDR0 is specified, then GATEWAYIPADDR.IPADDR0 must be in {"001" thru "126", "128" thru "223"}.

On IPADDRESS element, do the following:

If GATEWAYIPADDR is specified, then IPSUBNETMASK must be specified.

If IPSUBNETMASK is specified, then GATEWAYIPADDR must be specified.

If GATEWAYIPADDR is specified, then GATEWAYIPADDR.IPADDR0 concatenated with GATEWAYIPADDR.IPADDR1 concatenated with GATEWAYIPADDR.IPADDR2 concatenated with GATEWAYIPADDR.IPADDR3 must be in {"001000000001" thru "126255255254", "128001000001" thru "191254255254", "192000001001" thru "223255254254"}.

If GATEWAYIPADDR.IPADDR0 is in {"001" thru "126"}, then do the following:

IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255000000000", "255192000000" thru "255255255000"}.

GATEWAYIPADDR.IPADDR1 concatenated with GATEWAYIPADDR.IPADDR2 concatenated with GATEWAYIPADDR.IPADDR3 must not be in {"000000000", "255255255"}.

If GATEWAYIPADDR.IPADDR0 is in {"128" thru "191"}, then do the following:

IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255255000000", "255255192000" thru "255255255000"}.

GATEWAYIPADDR.IPADDR2 concatenated with GATEWAYIPADDR.IPADDR3 must not be in {"000000", "255255"}.

If GATEWAYIPADDR.IPADDR0 is in {"192" thru "223"}, then do the following:

IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255255255000", "255255255192" thru "255255255240"}.

GATEWAYIPADDR.IPADDR3 must not be in {"000", "255"}.

See form check(s) for IPADDRESS.GATEWAYIPADDR.

**GATEWAY IP ADDR - (IPADDRESS.GATEWAYIPADDR) - (structure domain CIPADDR)** - IP address to be assigned to the interface.

**Domain:**

For Gateway IP address set 1, enter 001 - 126 for Class A, 128 - 191 for Class B, or 192 - 223 for Class

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

C. For Gateway IP address set 2, 3, and 4, enter 0 - 255.

### Form Checks:

The count of elements of {select GATEWAYIPADDR from IPADDRESS} must be greater than 0.

{Select GATEWAYIPADDR from IPADDRESS} must be a unique set.

- (IPADDRESS.GATEWAYIPADDR.IPADDR0) - (domain C0\_255RZ) - .

**Default:** no default

- (IPADDRESS.GATEWAYIPADDR.IPADDR1) - (domain C0\_255RZ) - .

**Default:** no default

- (IPADDRESS.GATEWAYIPADDR.IPADDR2) - (domain C0\_255RZ) - .

**Default:** no default

- (IPADDRESS.GATEWAYIPADDR.IPADDR3) - (domain C0\_255RZ) - .

**Default:** no default

**IP SUBNET MASK - (IPADDRESS.IPSUBNETMASK) - (structure domain CIPADDR)** - IP subnet mask to be assigned to the interface.

### Domain:

Enter 255 for IP subnet mask set 1. Enter 0 - 255 for IP subnet mask set 2, 3, and 4.

- (IPADDRESS.IPSUBNETMASK.IPADDR0) - (domain C0\_255RZ) - .

**Default:** no default

- (IPADDRESS.IPSUBNETMASK.IPADDR1) - (domain C0\_255RZ) - .

**Default:** no default

- (IPADDRESS.IPSUBNETMASK.IPADDR2) - (domain C0\_255RZ) - .

**Default:** no default

- (IPADDRESS.IPSUBNETMASK.IPADDR3) - (domain C0\_255RZ) - .

**Default:** no default

**23. MCAST ADDR - (MCASTADDR) - (structure domain CIPADDR)** - This field defines the multicast address for the interface.

### Domain:

Blank, or enter 224 - 239 for Multicast IP address set 1. Blank, or enter 0 - 255 for Multicast IP address set 2, 3, and 4.

- (MCASTADDR.IPADDR0) - (domain C0\_255RZ) - .

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

**Default:** no default

**Form Checks:**

If MCASTADDR.IPADDR0 is specified, then MCASTADDR.IPADDR0 must be in {224 thru 239}.

- (MCASTADDR.IPADDR1) - (domain C0\_255RZ) - .

**Default:** no default

- (MCASTADDR.IPADDR2) - (domain C0\_255RZ) - .

**Default:** no default

- (MCASTADDR.IPADDR3) - (domain C0\_255RZ) - .

**Default:** no default

**28. MTU SIZE - (MTUSIZE) - (domain I128\_1600)** - This field defines the maximum number of bytes per transfer from this interface.

**Domain:**

Enter 128 to 1600 bytes.

**Default:** default = 256

**29. CALEA IN USE - (CALEAINUSE) - (domain BOOL)** - This field indicates if this interface is in use by the CALEA Application.

**Domain:**

Enter Y for yes or N for no.

**Default:** default = N

### 3. TRIGGER FUNCTIONS

BASE RELATION = TRIGGER FUNCTION (PERMISSIONS)

RLIPINTCNF = PSipintcnf (iud)

RLIPRTTAB = PSiprttab (iud)

### 4. BASE RELATIONS

(PERMISSIONS) BASE RELATION — DISTRIBUTION

(r) RLDSLEQUIP — FP

(r) RLEQUIPDSL — FP

(r) RLPR\_DNTRAN — FG

# ***Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)***

## ***Provisioning, Troubleshooting, and Maintenance***

235-200-400

June 2003

(r) RLPSGP\_PRT — LPFFFG  
(r) RLSPVCINF — FP  
(r) RLRT\_MHG — LPFR  
(u) RLINTFNAM — LP  
(u) RLIPADRLOC — FR  
(u) RLIPINTCNF — FP  
(u) RLIPRTTAB — FP  
(u) RLLOCIPADR — LP  
(u) RLNAMINTF — LP  
(u) RLRC\_HOLE — LP  
(u) RLRC\_QIDX — LP

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

### 33V3 INTERNET PROTOCOL (RC\_IPROUT)

Form ID: 33V3

Form Name: RC\_IPROUT

View ID: RVIPROUT

Title: INTERNET PROTOCOL (IP) ROUTING TO INTERFACE

#### 1. VIEW DESCRIPTION:

The INTERNET PROTOCOL (IP) ROUTING TO INTERFACE view (33.3) provides the capability to provision an IP gateway between an external IP destination and a local IP interface.

#### 1.1 VIEW INFORMATION:

SOFTWARE RELEASE = 5E15

OFFICE RECORD(S) = (5989)

ODA FORM NAME = iprout

ODA FORM TITLE = INTERNET PROTOCOL (IP) ROUTING TO INTERFACE

ODA OFFICE RECORD(S) = 5989

VIEW PERMISSIONS = RUDI

MAXIMUM TIME OUT = 330

FUNCTION NAME = viprout

ERROR ID = 832

---

```
                    5ESS SWITCH
                    RECENT CHANGE 33.3
(5989)              INTERNET PROTOCOL (IP) ROUTING TO INTERFACE

*1. DEST IP ADDR   ____ . ____ . ____ . ____
*6. INTERFACE NAME _____
 7. NET OR HOST    _____
 8. IP SUBNET MASK ____ . ____ . ____ . ____
#13. GATEWAY IP ADDR ____ . ____ . ____ . ____
18. ROUTE METRIC   ____
```

---

#### 2. FIELD DEFINITIONS

\* 1. DEST IP ADDR - (DESTIPADDR) - (structure domain CIPADDR) - This field specifies one of the

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

network or host IP addresses that can be reached via this route.

**Domain:**

For Destination IP address set 1, enter 001 - 126 for Class A, 128 - 191 for Class B, or 192 - 223 for Class C. For Destination IP address set 2, 3, and 4, enter 0 - 255.

- (DESTIPADDR.IPADDR0) - (domain C0\_255RZ) - .

**Default:** no default

**Form Checks:**

DESTIPADDR.IPADDR0 must be in {"001" thru "126", "128" thru "223"}.

DESTIPADDR.IPADDR0 concatenated with DESTIPADDR.IPADDR1 concatenated with DESTIPADDR.IPADDR2 concatenated with DESTIPADDR.IPADDR3 must be in {"001000000001" thru "126255255254", "128001000001" thru "191254255254", "192000001001" thru "223255254254"}.

See form check(s) for NETORHOST.

- (DESTIPADDR.IPADDR1) - (domain C0\_255RZ) - .

**Default:** no default

**Form Checks:**

See form check(s) for DESTIPADDR.IPADDR0.

- (DESTIPADDR.IPADDR2) - (domain C0\_255RZ) - .

**Default:** no default

**Form Checks:**

See form check(s) for DESTIPADDR.IPADDR0.

- (DESTIPADDR.IPADDR3) - (domain C0\_255RZ) - .

**Default:** no default

**Form Checks:**

See form check(s) for DESTIPADDR.IPADDR0.

- \* **6. INTERFACE NAME - (INTERFACENAME) - (domain INTFNM)** - This field assigned on view 33.2 specifies the name of and interface.

**Domain:**

Enter name starting with an alphanumeric character followed by 4 to 18 characters including '.', '\_' or '-'.

235-200-400

June 2003

**Default:** no default

**7. NET OR HOST - (NETORHOST) - (domain NETHOST)** - This field indicates if the destination IP address given is a network or host IP address.

**Domain:**

Enter NET or HOST.

**Default:** default = NET

**Form Checks:**

If NETORHOST equals "NET", then do the following:

If DESTIPADDR.IPADDR0 is in {"001" thru "126"}, then IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255000000000", "255192000000" thru "255255255000"}.

If DESTIPADDR.IPADDR0 is in {"128" thru "191"}, then IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255255000000", "255255192000" thru "255255255000"}.

If DESTIPADDR.IPADDR0 is in {"192" thru "223"}, then IPSUBNETMASK.IPADDR0 concatenated with IPSUBNETMASK.IPADDR1 concatenated with IPSUBNETMASK.IPADDR2 concatenated with IPSUBNETMASK.IPADDR3 must be in {"255255255000", "255255255192" thru "255255255240"}.

IPSUBNETMASK must be specified.

If NETORHOST equals "HOST", then IPSUBNETMASK must be unspecified.

**8. IP SUBNET MASK - (IPSUBNETMASK) - (structure domain CIPADDR)** - This field specifies the subnetwork mask associated with the destination IP address.

**Domain:**

Blank, or enter 255 for IP subnet mask set 1. Blank, or enter 0 - 255 for IP subnet mask set 2, 3, and 4.

**Form Checks:**

See form check(s) for NETORHOST.

**- (IPSUBNETMASK.IPADDR0) - (domain C0\_255RZ) - .**

**Default:** no default

**Form Checks:**

See form check(s) for NETORHOST.

**- (IPSUBNETMASK.IPADDR1) - (domain C0\_255RZ) - .**

**Default:** no default

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

### Form Checks:

See form check(s) for NETORHOST.

- (IPSUBNETMASK.IPADDR2) - (domain C0\_255RZ) - .

**Default:** no default

### Form Checks:

See form check(s) for NETORHOST.

- (IPSUBNETMASK.IPADDR3) - (domain C0\_255RZ) - .

**Default:** no default

### Form Checks:

See form check(s) for NETORHOST.

- # 13. **GATEWAY IP ADDR - (GATEWAYIPADDR) - (structure domain CIPADDR)** - This field specifies the IP address of the gateway through which data is sent to the destination.

### Domain:

For Gateway IP address set 1, enter 001 - 126 for Class A, 128 - 191 for Class B, or 192 - 223 for Class C. For Gateway IP address set 2, 3, and 4, enter 0 - 255.

*Interactions:* The GATEWAY IP ADDR must be assigned to the INTERFACE NAME with View 33.2.

- (GATEWAYIPADDR.IPADDR0) - (domain C0\_255RZ) - .

**Default:** no default

### Form Checks:

GATEWAYIPADDR.IPADDR0 concatenated with GATEWAYIPADDR.IPADDR1 concatenated with GATEWAYIPADDR.IPADDR2 concatenated with GATEWAYIPADDR.IPADDR3 must be in {"001000000001" thru "126255255254", "128001000001" thru "191254255254", "192000001001" thru "223255254254"}.

- (GATEWAYIPADDR.IPADDR1) - (domain C0\_255RZ) - .

**Default:** no default

### Form Checks:

See form check(s) for GATEWAYIPADDR.IPADDR0.

- (GATEWAYIPADDR.IPADDR2) - (domain C0\_255RZ) - .

# Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)

## Provisioning, Troubleshooting, and Maintenance

235-200-400

June 2003

**Default:** no default

**Form Checks:**

See form check(s) for GATEWAYIPADDR.IPADDR0.

- (GATEWAYIPADDR.IPADDR3) - (domain C0\_255RZ) - .

**Default:** no default

**Form Checks:**

See form check(s) for GATEWAYIPADDR.IPADDR0.

**18. ROUTE METRIC - (ROUTEMETRIC) - (domain I1\_255)** - This field specifies the route metric associated with the routing path. This is use for load balancing in multi-routing.

**Domain:**

Enter 1 - 255.

**Default:** default = 1

### 3. TRIGGER FUNCTIONS

BASE RELATION = TRIGGER FUNCTION (PERMISSIONS)

RLIPRTTAB = PSiprttab (iud)

### 4. BASE RELATIONS

(PERMISSIONS) BASE RELATION — DISTRIBUTION

(r) RLINTFNAM — LP  
(r) RLIPADRLOC — FR  
(r) RLLOCIPADR — LP  
(r) RLNAMINTF — LP  
(u) RLIPRTTAB — FP

### GLOSSARY

This section provides acronyms and abbreviations used in this document.

-- --

**ACK**

Acknowledge

# ***Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)***

## ***Provisioning, Troubleshooting, and Maintenance***

235-200-400

June 2003

**AM**  
Administrative Module

**AP**  
Attached Processor

**ARS**  
Automatic Route Selection

**ASM**  
Administrative Services Module

**BAUTO**  
BRCS Autoform

**BFG**  
BRCS Feature Group

**BMI**  
Batch Mode Immediate (RC)

**BMI**  
Beginning Of Managed Introduction

**BMR**  
Batch Mode Release

**BRCS**  
Business And Residential Custom Services

**BRI**  
Basic Rate Interface

**BRI**  
Batch-Review Inhibited Relation

**BST**  
Bitmap Salvage Technique

**CALEA**  
Communications Assistance for Law Enforcement Act

**CAR**  
Customer Assistance Request

**CCC**  
Call Content Channel

**CDC**  
Call Data Channel

**CM1**  
Communications Module 1

# ***Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)***

## ***Provisioning, Troubleshooting, and Maintenance***

235-200-400

June 2003

**CM2**  
Communications Module 2

**CMD**  
Command

**CPE**  
Customer Premises Equipment

**CST**  
Central Standard Time

**DB**  
Database

**DB**  
Database Subsystem

**DBM**  
Database Manager

**DBM**  
Database Mode

**DEN**  
Digital Equipment Number

**DISP**  
Display

**DN**  
Directory Number

**DSL**  
Digital Subscriber Line

**DTMF**  
Dual Tone Multifrequency

**ECD**  
Equipment Configuration Data

**ECD**  
Equipment Configuration Database

**FIOP**  
Flexible Input/Output Processor

**FOA**  
First Office Application

**FAC**  
Facilities

# ***Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)***

## ***Provisioning, Troubleshooting, and Maintenance***

235-200-400

June 2003

**FAC**  
Facility Administration And Control

**FAC**  
Feature Assignment And Construction

**FM**  
Facilities Management

**FM**  
File Manager

**HSM**  
Host Switching Module

**IAP**  
Intercept Access Point

**IGN**  
Ignore

**IM**  
Immediate Mode (RC)

**IM**  
Input Manual

**IM**  
Input Message

**IM**  
Interface Module (now SM)

**IOP**  
Input/Output Processor

**IP**  
Internet Protocol

**ISDN**  
Integrated Services Digital Network

**LASS**  
Local Area Signaling Services

**LAES**  
Lawfully Authorized Electronic Surveillance

**LATA**  
Local Access And Transport Area

**LCC**  
Line Class Code

# **Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)**

## **Provisioning, Troubleshooting, and Maintenance**

235-200-400

June 2003

**LEA**  
Law Enforcement Agency

**LEC**  
Local Exchange Carrier

**LEN**  
Line Equipment Number

**MC**  
Master Control

**MCC**  
Maintenance (Master) Control Center

**MCC**  
Master Control Console

**MLHG**  
Multi-Line Hunt Group

**MML**  
Man Machine Language

**MMRSM**  
MultiModule Remote Switching Module

**MSG**  
Message

**MSG**  
Message Switch

**MTU**  
Maximum Transmission Unit

**NIC**  
Network Information Center

**NOC**  
Normalized Office Code

**NPA**  
Numbering Plan Area

**NSC**  
Network Service Center

**NSC**  
Network Services Complex

**NSC**  
Network Software Center

# **Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)**

## **Provisioning, Troubleshooting, and Maintenance**

235-200-400

June 2003

**NSC**  
Network Systems Corporation

**NXX**  
Office Code (Part Of Dialed Number)

**OA&M**  
Operations, Administration, And Maintenance

**OC**  
Overload Control

**ODA**  
Office Data (Assembler)

**ODA**  
Office Data Administration System

**ODA**  
Office Database Administrator

**ODB**  
Office Database

**ODBE**  
Office Database Editor

**ODD**  
Office Dependent Data

**OE**  
Office Equipment (OEN)

**OFR**  
Office Records

**OKP**  
Operational Kernel Process

**OOS**  
Out Of Service

**OP**  
Operation

**ORIG**  
Originating

**ORM**  
Optical Remote Module

**OS**  
OSDS Subsystem

# ***Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)***

## ***Provisioning, Troubleshooting, and Maintenance***

235-200-400

June 2003

**OS**  
Operating System

**OS**  
Operations Support

**OS**  
Operations System

**OSPS**  
Operator Services Position System

**OTC**  
Operating Telephone Company

**OTR**  
Operational Trouble Report

**OTR**  
Operator Trouble Report

**PARAM**  
Parameters

**PC**  
Peripheral Controller

**PDC**  
Packet Data Channel

**PF**  
Printout Follows

**PF**  
Private Facility

**PH**  
Packet Handler

**PING**  
Packet Internet Groper

**PSU**  
Packet Switching Unit

**PVC**  
Permanent Virtual Circuit

**RAO**  
Revenue Accounting Office

**RBOC**  
Regional Bell Operating Company

# **Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)**

## **Provisioning, Troubleshooting, and Maintenance**

235-200-400

June 2003

**RC**

Recent Change Subsystem

**RCV**

Recent Change And Verify

**RCOS**

Recent Change Operations System

**RCV**

Recent Change And Verify

**REPT**

Report

**RMAC**

Remote Memory Administration Center

**RMAS**

Recent Change Memory Administration System

**RMAS**

Remote Memory Access System

**RMAS**

Remote Memory Administration System

**ROP**

Read (Receive) Only Printer

**ROP**

Receive Only Printer

**RSM**

Remote Switching Module

**RTAC**

Regional Technical Assistance Center

**RTR**

Real Time Reliable

**SAI**

Surveillance Administration Interface

**SAS**

Surveillance Administration System

**SAUTO**

Shared Autoform

**SCCS**

Switching Control Center System

# **Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)**

## **Provisioning, Troubleshooting, and Maintenance**

235-200-400

June 2003

**SM**

Switching Module

**STLWS**

Supplementary Trunk And Line Work Station

**SU**

Software Update

**TASC**

Telephone Company Administrative Support Capability

**TCP/IP**

Transmission Control Protocol/Internet Protocol

**TG**

Translation Guide

**TG**

Trunk Group

**TG-5**

5ESS<sup>®</sup> Switch Translation Guide

**TGN**

Trunk Group Number

**TLWS**

Trunk And Line Work Station

**TMS**

Time Multiplexed Switch

**TMS**

Transmission Measuring Set

**TPKT**

Transport Control Protocol Packet

**TSP**

Telephone Service Provider

**TTY**

Teletypewriter

**UTD**

Universal Tone Decoder

**V**

Verify

**VDT**

Video Display Terminal

# ***Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)***

## ***Provisioning, Troubleshooting, and Maintenance***

235-200-400

June 2003

**VER**

Verify

**VFY**

Verify

**XAT**

X.25 Access on a T1

# ***Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)***

## ***Provisioning, Troubleshooting, and Maintenance***

235-200-400

June 2003

### **List of Figures**

Figure 2-1 : CALEA Network Overview

Figure 2-2 : CALEA Network Diagram

Figure 2-3 : CCC Quick Reference

Figure 3-1 : Switch Administration Task Overview

Figure 3-2 : Surveillance Administration Terminal Installation (SPARC5)

Figure 3-3 : Surveillance Administration Terminal Installation (Ultra)

Figure 3-4 : Surveillance Administration Printer Installation (SPARC5)

Figure 3-5 : Surveillance Administration Printer Installation (ULTRA)

Figure 3-6 : CDC/PDC Network Block Diagram

Figure 3-7 : IP Address Assignment Example

Figure 3-8 : Example of Adding a New Trunk Group and Members (Display 1 of 2)

Figure 3-9 : Example of Adding a New Trunk Group and Members (Display 2 of 2)

Figure 3-10 : Example of Deleting a Member From a Trunk Group

Figure 3-11 : Recent Change View Interactions

# ***Lawfully Authorized Electronic Surveillance / 5ESS (Part 6)***

## ***Provisioning, Troubleshooting, and Maintenance***

235-200-400

June 2003

### **List of Tables**

Table 3-1 : SPARC5 Terminal Locations

Table 3-2 : Ultra Terminal Locations

Table 3-3 : SPARC5 Terminal Locations

Table 3-4 : Ultra Terminal Locations

# ***Brown County, Wisconsin Bomb Squad Robot***

## **Overview**

Pictorial overview of the Remotec ANDROS F6 series robot used by the Outagamie/Brown County, Wisconsin Sheriff Department's bomb squad. This line of robots is marketed toward law enforcement agencies specifically for bomb disposal and EOD applications. Remotech is a division of Northrop Grumman.

There are multiple (fixed) color video cameras and a single full 360° pan, tilt, and zoom low-light camera. A halogen lamp provides local area illumination and there's even a microphone/speaker for two-way audio. A water disruptor can be used to neutralize any timing or triggering devices.

It weighs around 500 pounds and the angled track allows the robot to navigate stairs. The unit's power supply is several standard gel-cell batteries providing a total of +24 VDC.

The controlling data link is RF, with an optional wired cable connection. The operator has a tabletop controller and LCD display for the video cameras. I noticed three antennas, two UHF Larsen antennas labeled "DATA" and "AUDIO," and a higher-mounted rubber duck, which is probably for video in the 2.4 GHz range.

There are several FCC licenses assigned for robot use by the Brown County Sheriff's Department:

## **FCC License: WQKC738**

VIDEO LINK FOR REMOTE BOMB ROBOT USED BY SHERIFF'S DEPT FOR PUBLIC SAFETY AND TO DIFFUSE TERRORIST THREATS FOR HOMELAND SECURITY.

Control Point 1: 300 EAST WALNUT STREET, GREEN BAY, BROWN COUNTY, WI, Phone: 920-448-4218

2462.50000 Mobile, 5 watt(s), 1 unit(s), Mobile, Transmit Location  
32km radius around GREEN BAY, BROWN COUNTY, WI

## **FCC License: WQKC752**

AUDIO & DATA LINK FOR REMOTE BOMB ROBOT USED BY SHERIFFS DEPT FOR PUBLIC SAFETY & TO DIFFUSE TERRORIST THREATS FOR HOMELAND SECURITY.

Control Point 1: 300 EAST WALNUT STREET, GREEN BAY, BROWN COUNTY, WI, Phone: 920-448-4218

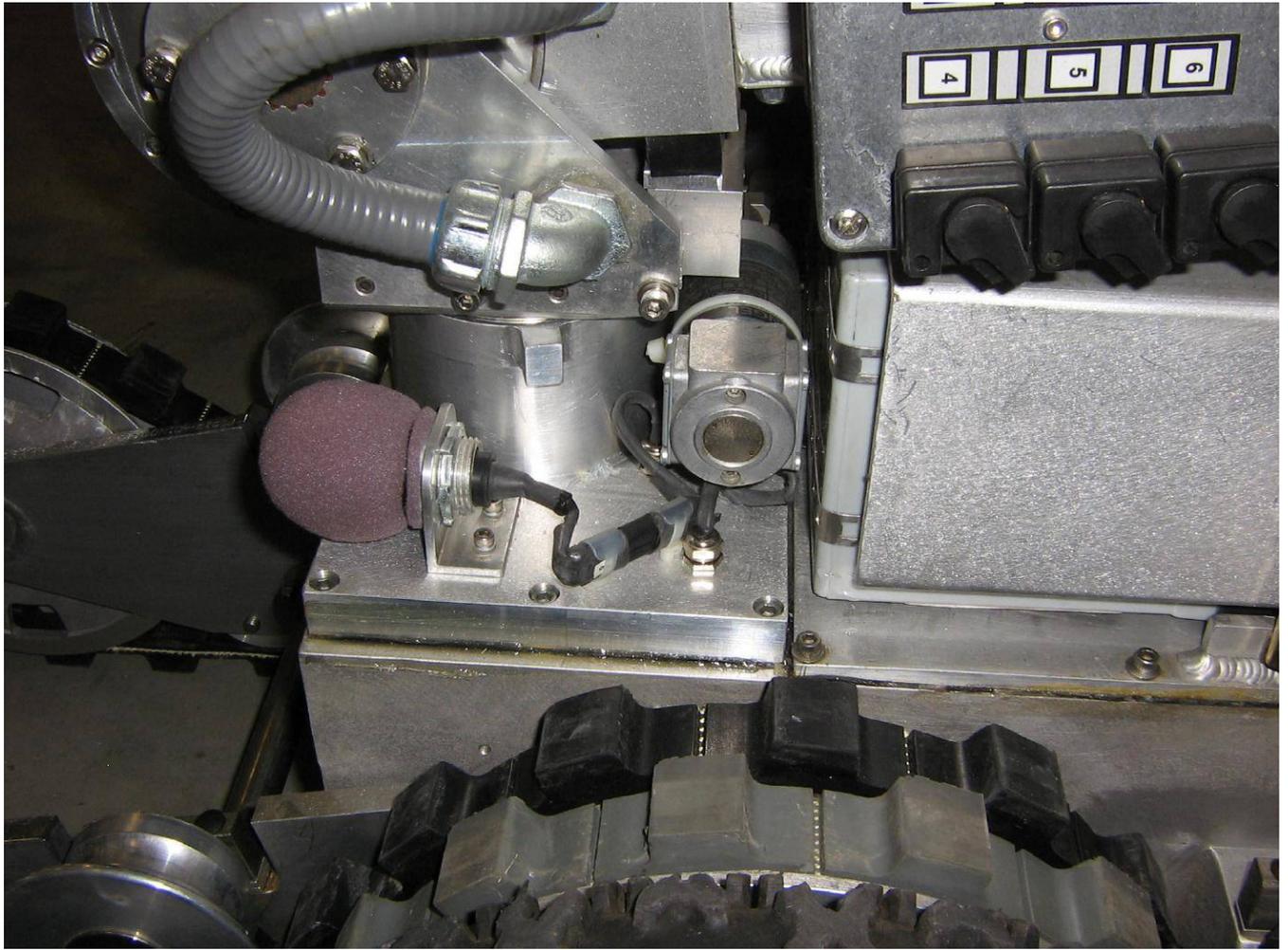
460.30000 Mobile, 5 watt(s), 3 unit(s), Mobile, Transmit Location  
32km radius around GREEN BAY, BROWN COUNTY, WI

465.30000 Mobile, 15 watt(s), 1 unit(s), Mobile, Transmit Location  
32km radius around GREEN BAY, BROWN COUNTY, WI

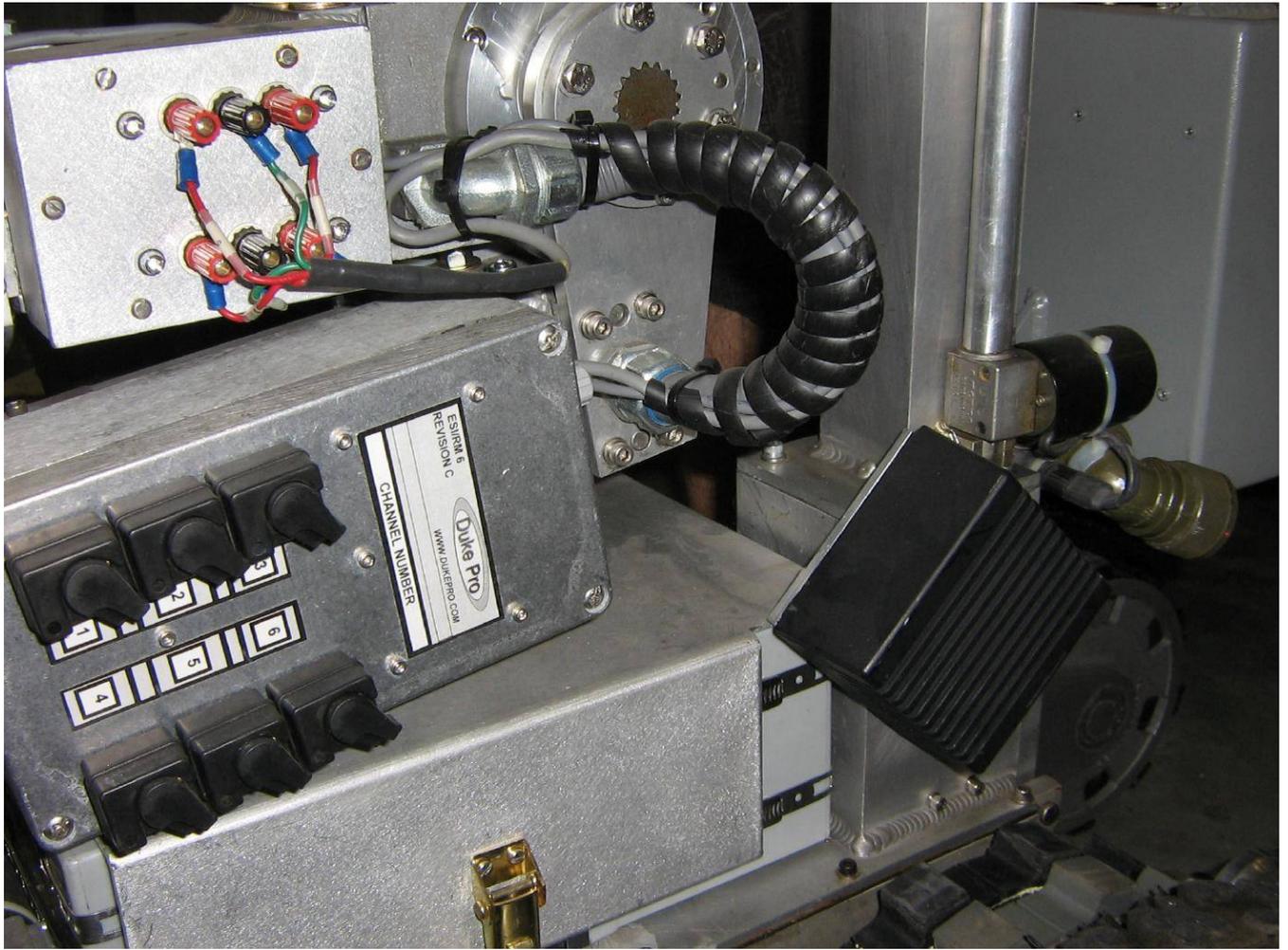
The Milwaukee County bomb squad robot is at 2470 MHz (video) and 453.2625 MHz / 458.2625 MHz for audio and data.



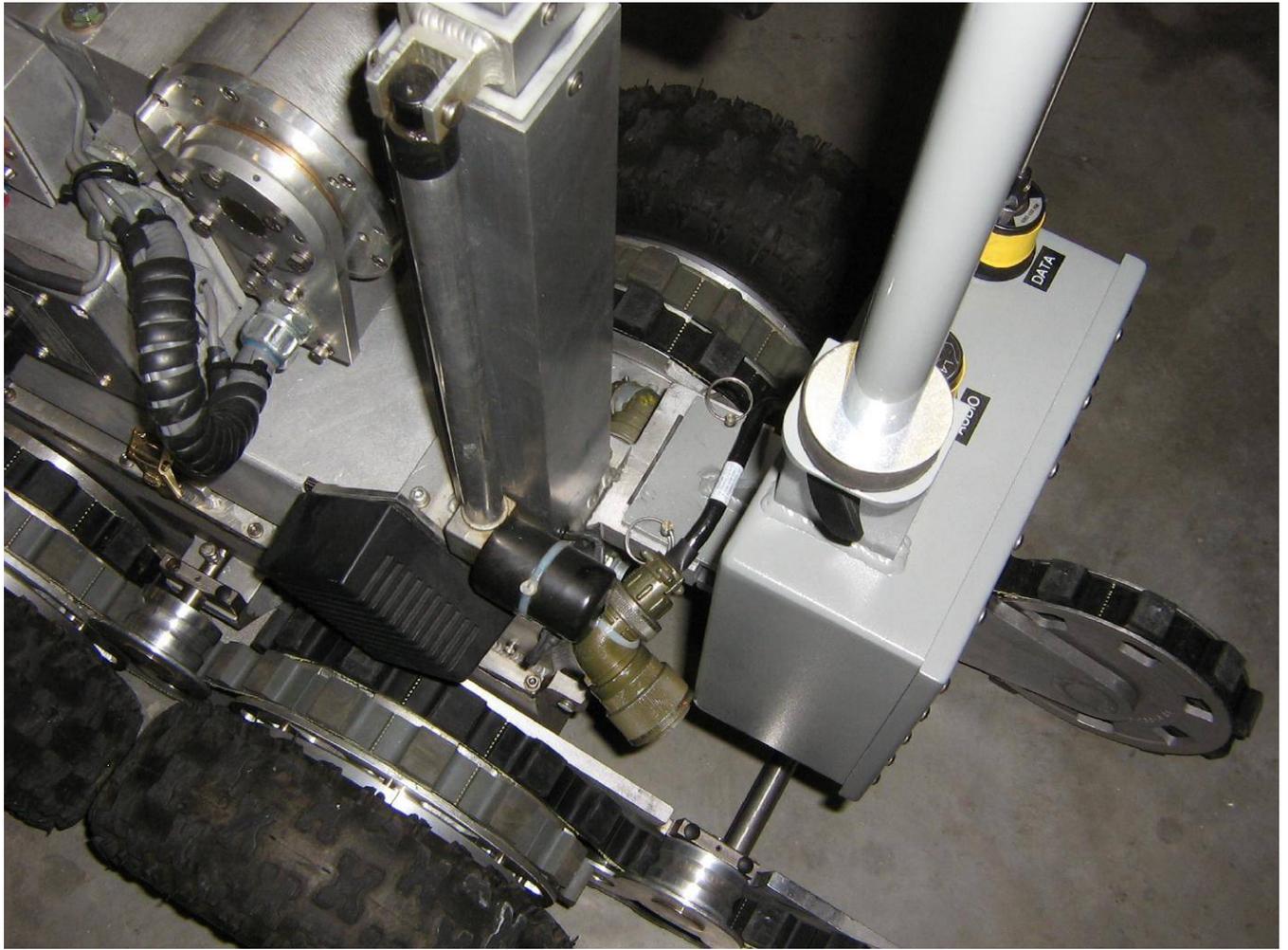
General overview.



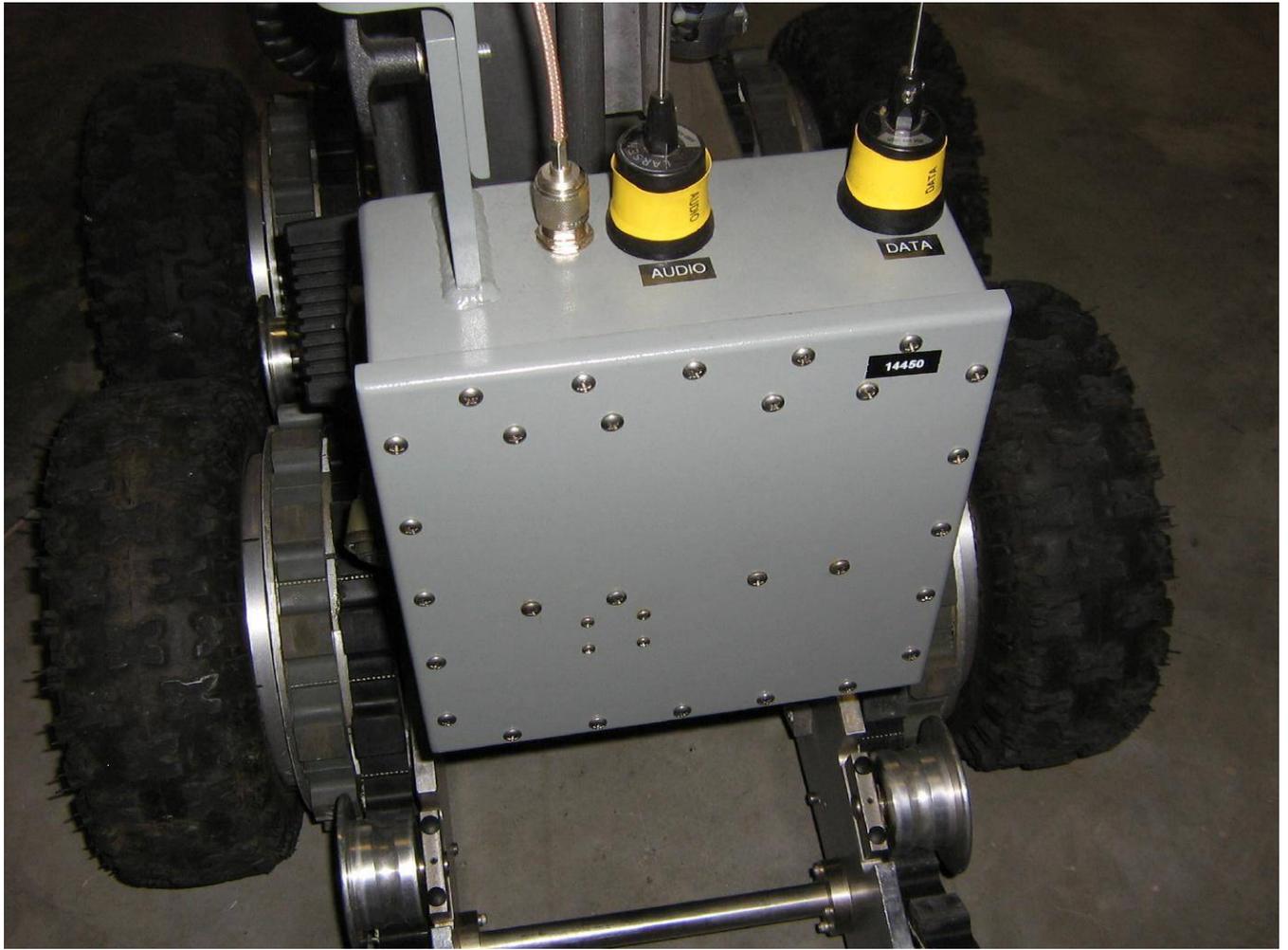
Microphone with wind screen.



Duke Pro ESI/RM6 6-channel shock tube initiator.

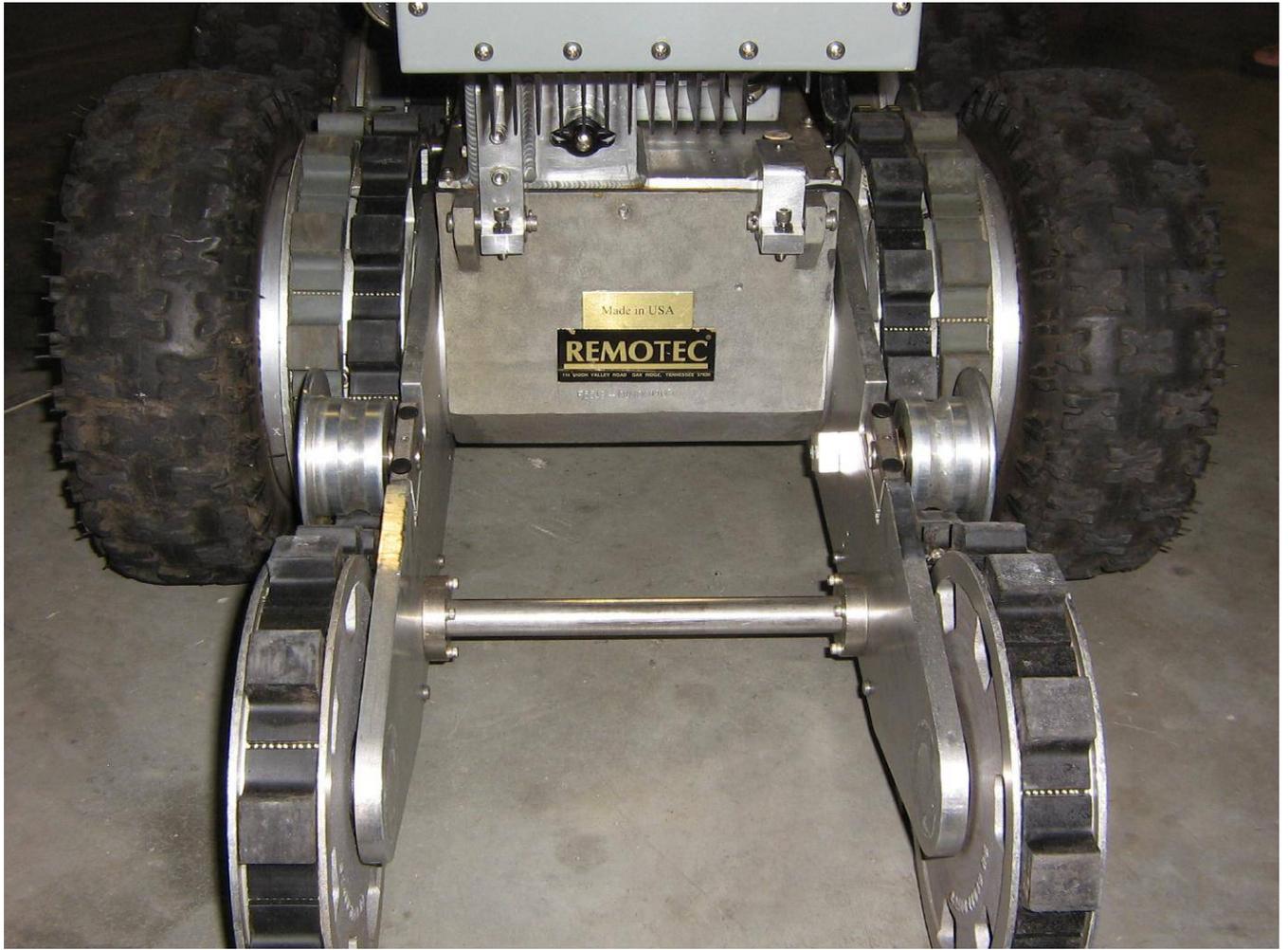


Rear view.

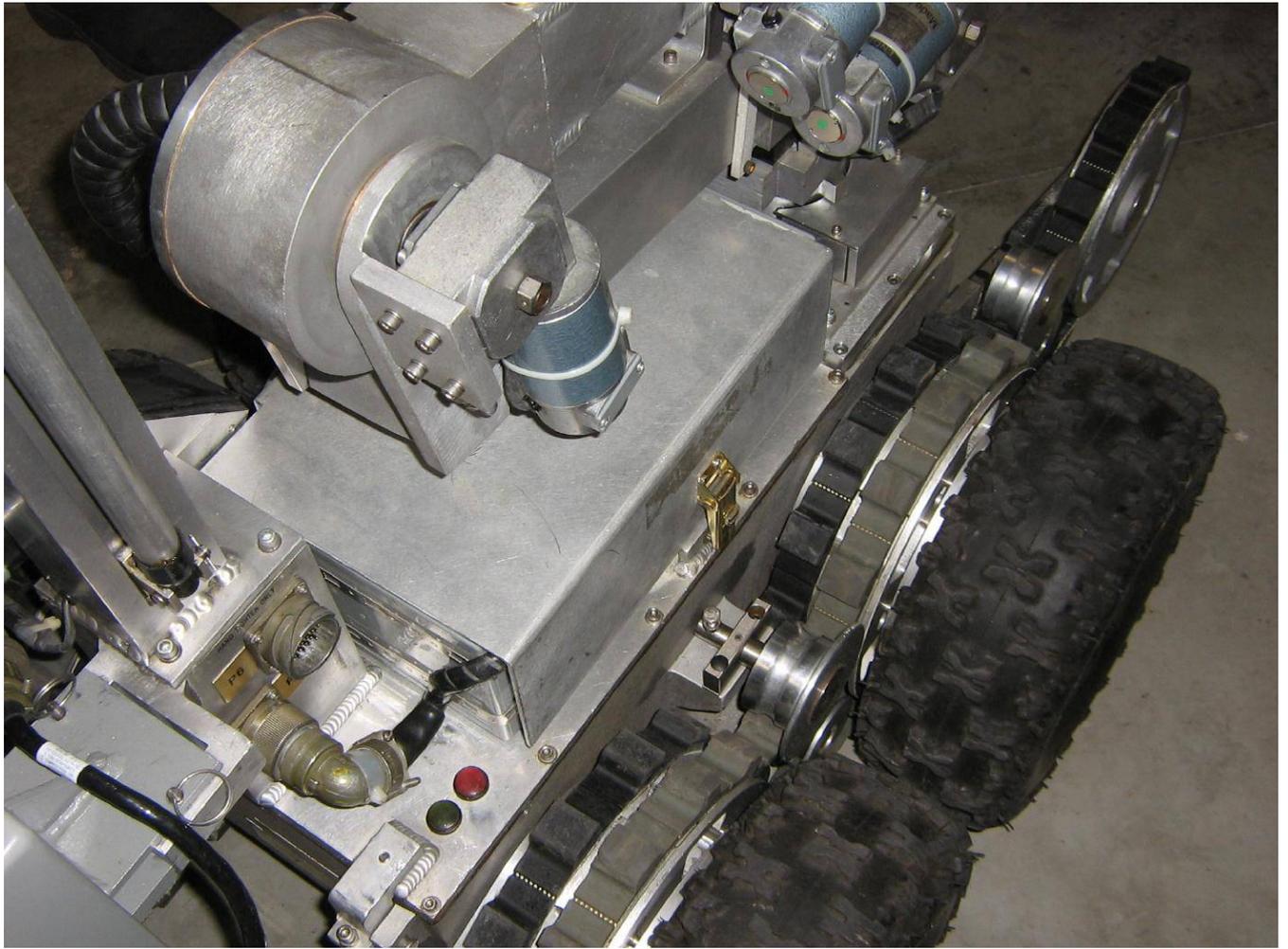


Antenna mounts.

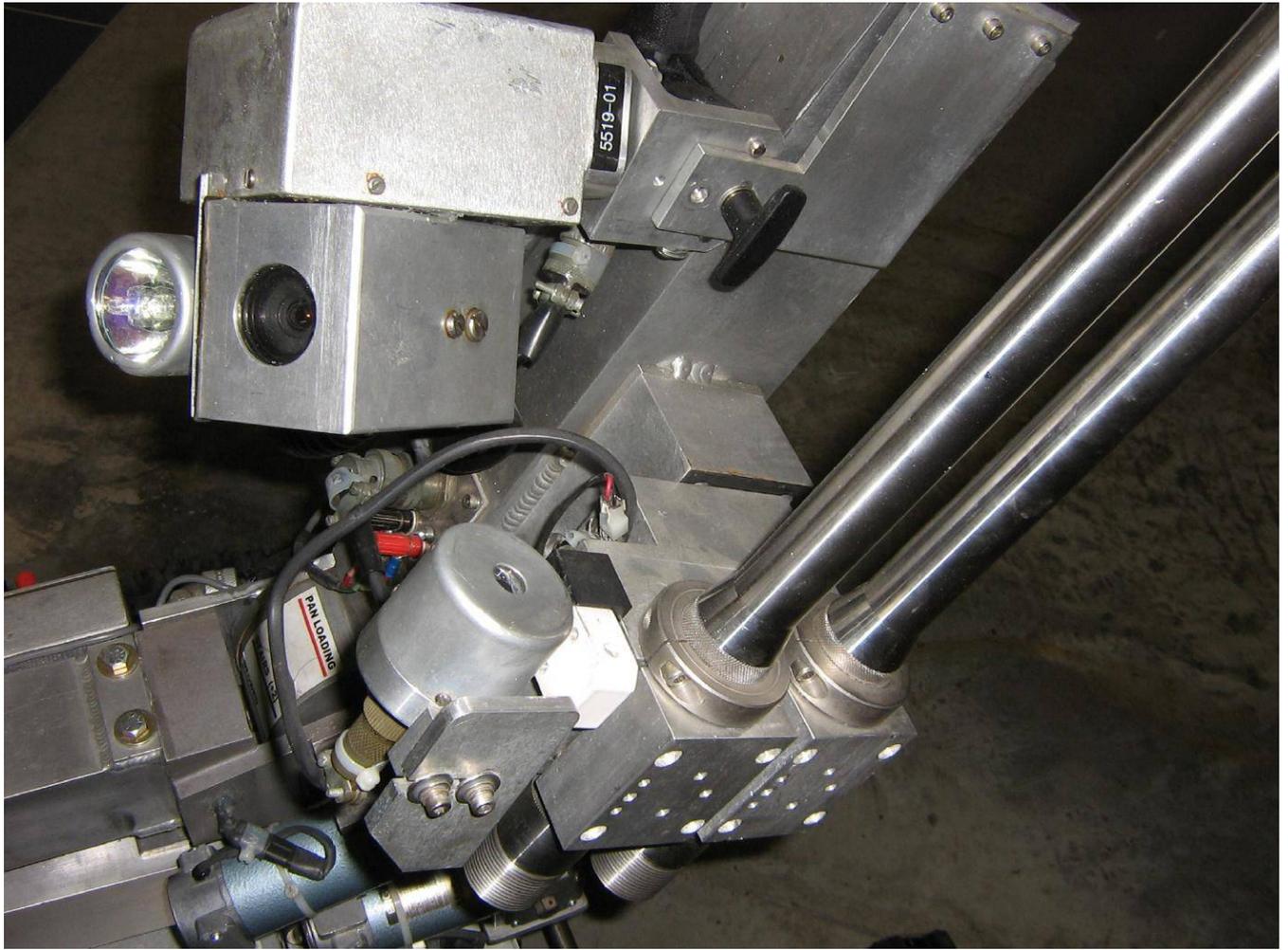
Two Larsen UHF (450 MHz) models and the N connector goes to a rubber duck which is probably used for 2.4 GHz video.



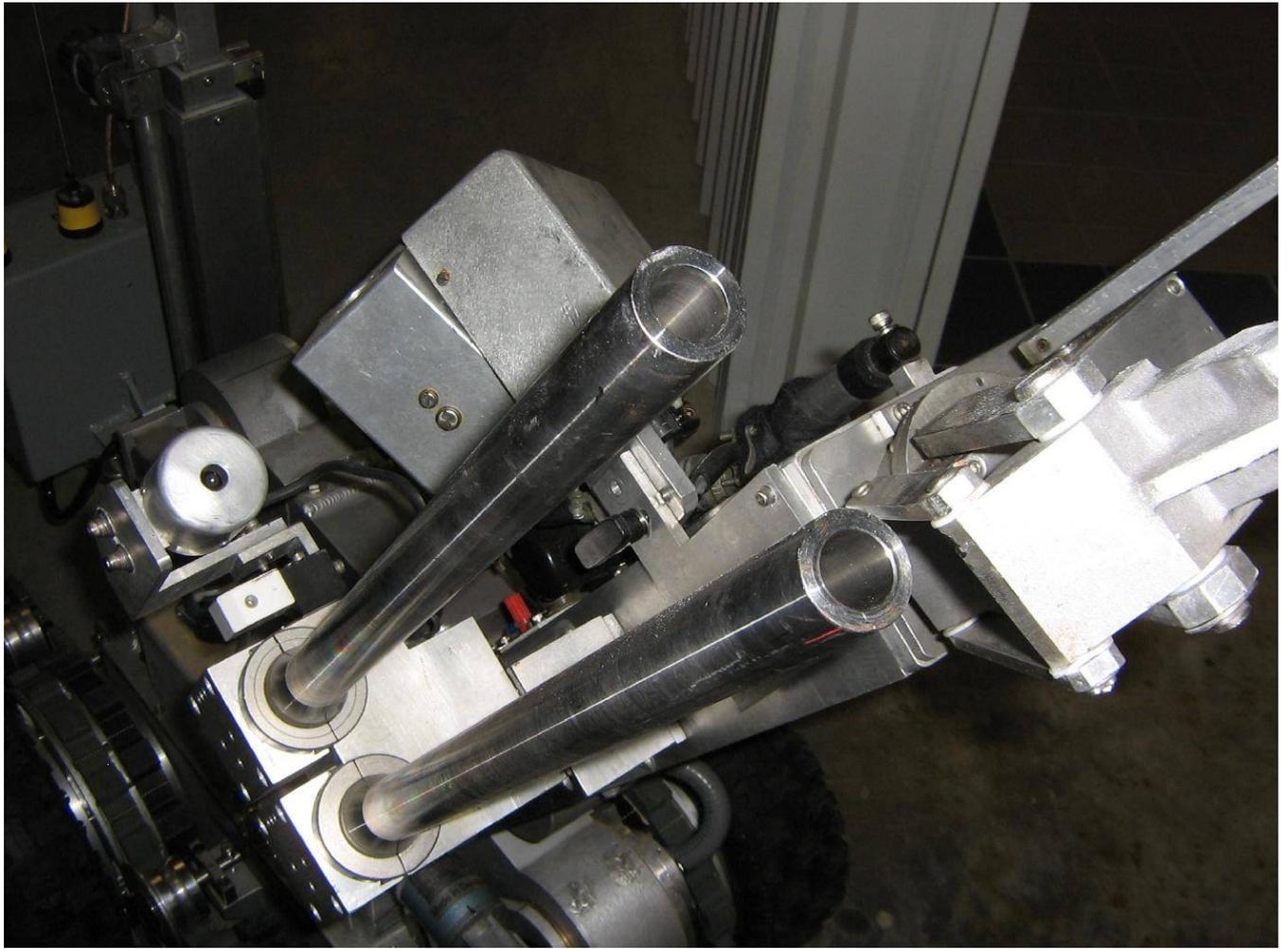
Rear track view.



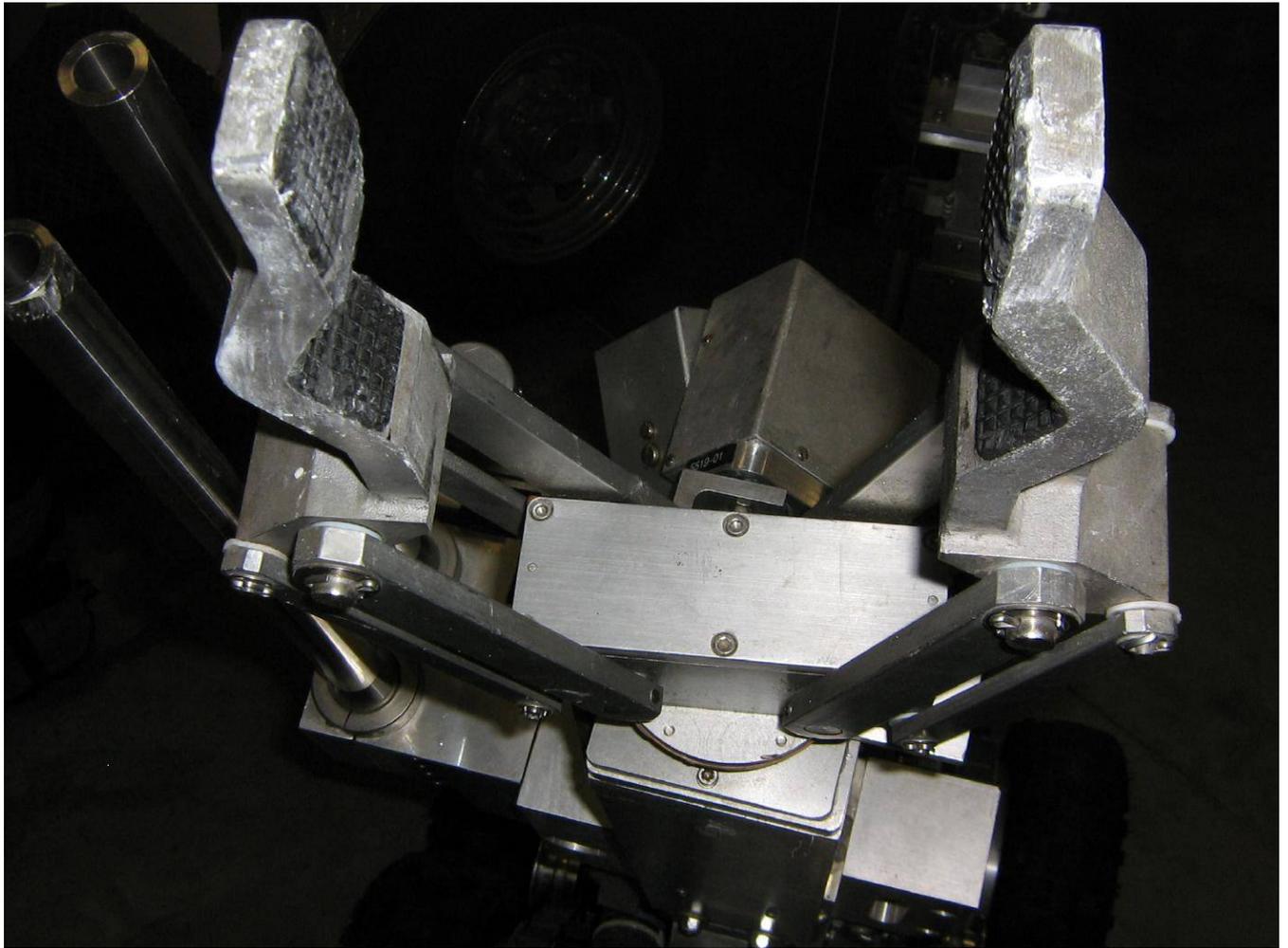
Manipulator arm servos.



Camera and water disruptors on the manipulator arm.

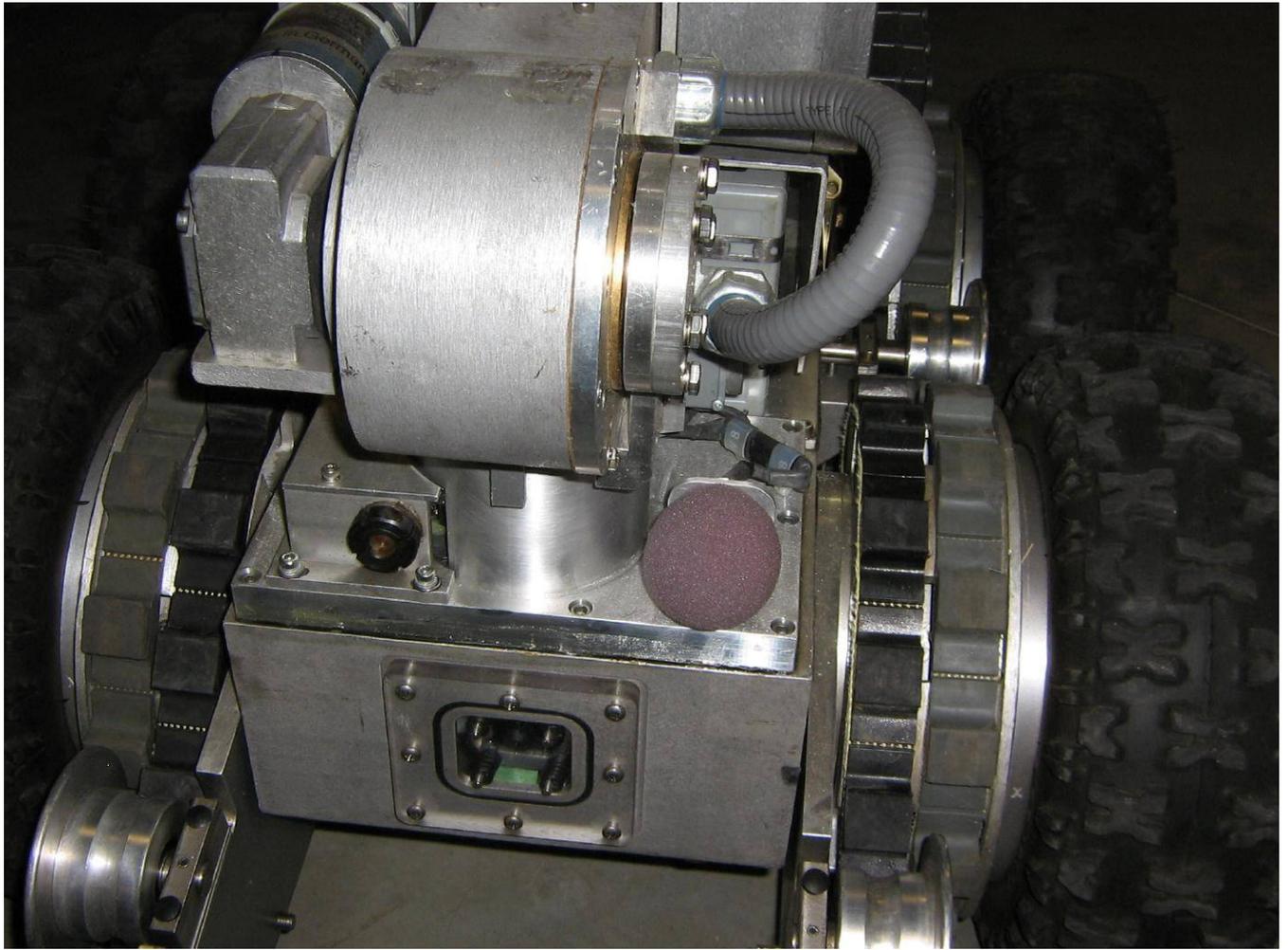


Barrel view of the dual water disruptors.

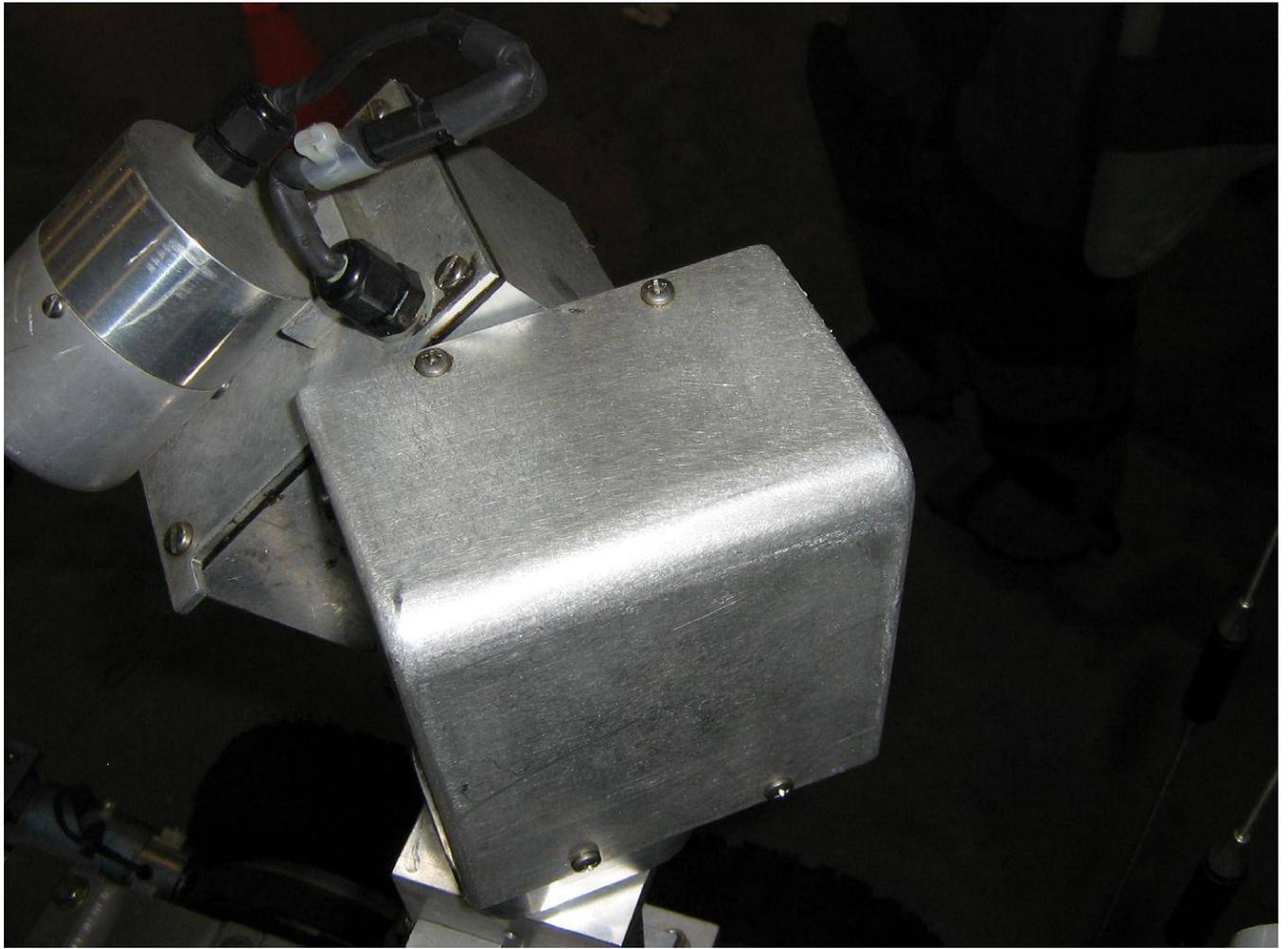


Gripper on the manipulator arm.

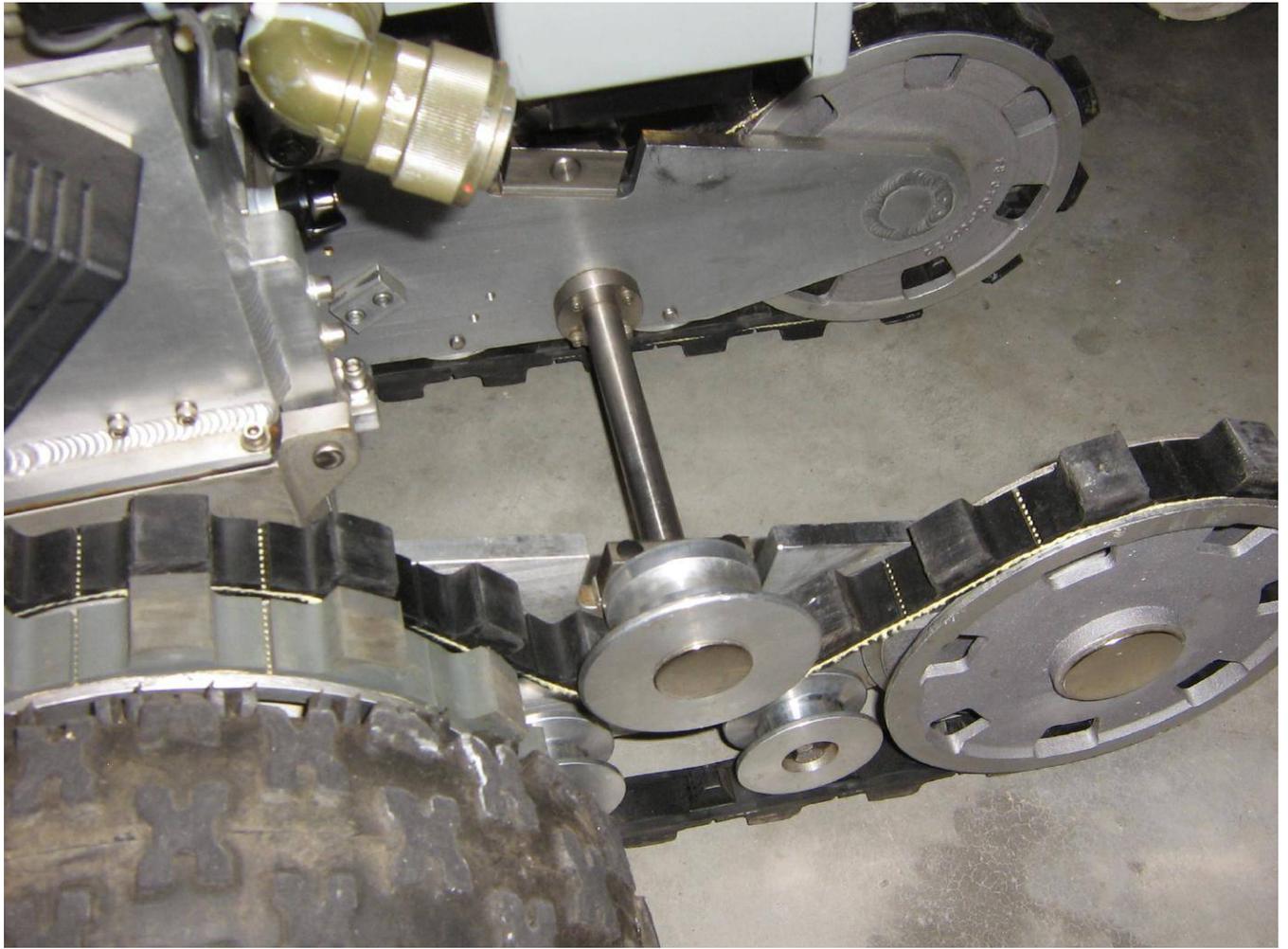
It opens to around 12 inches and has up to 50 pounds of pressure. Its lifting capacity varies with how far the arm is extended.



Front track view showing several cameras and the microphone.



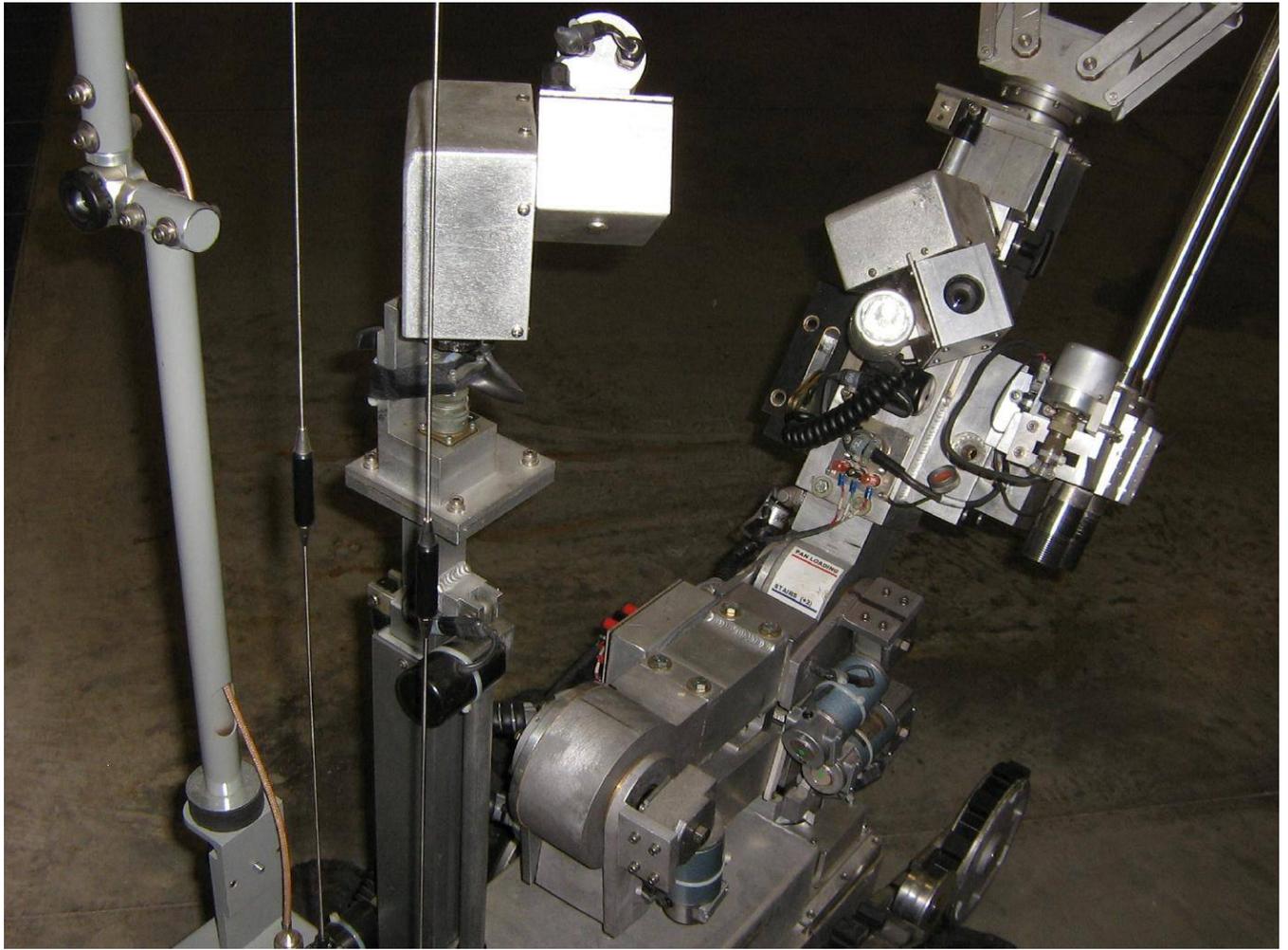
Pan, tilt, zoom video camera.



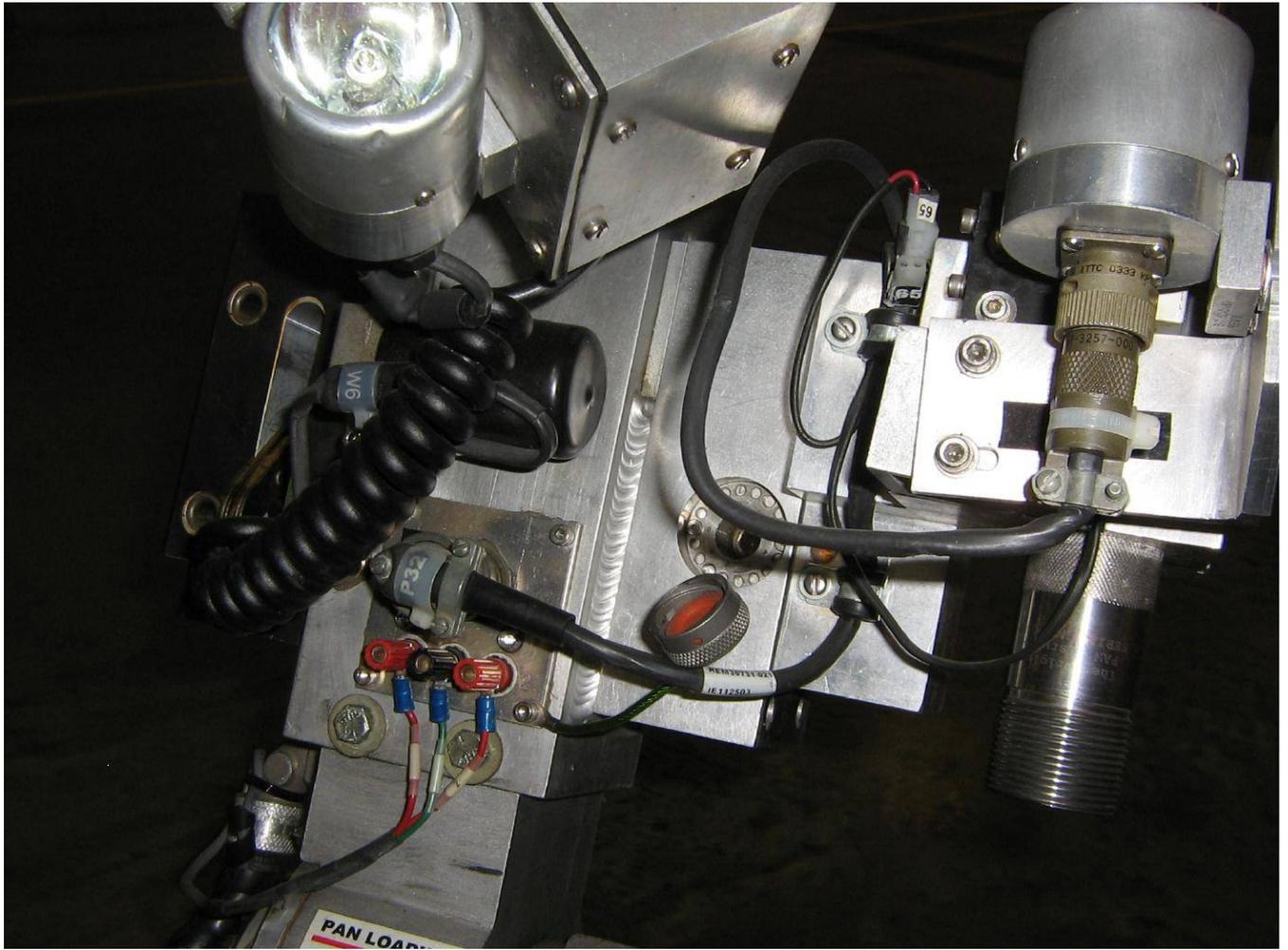
Track guides.



Track guides, alternate view.



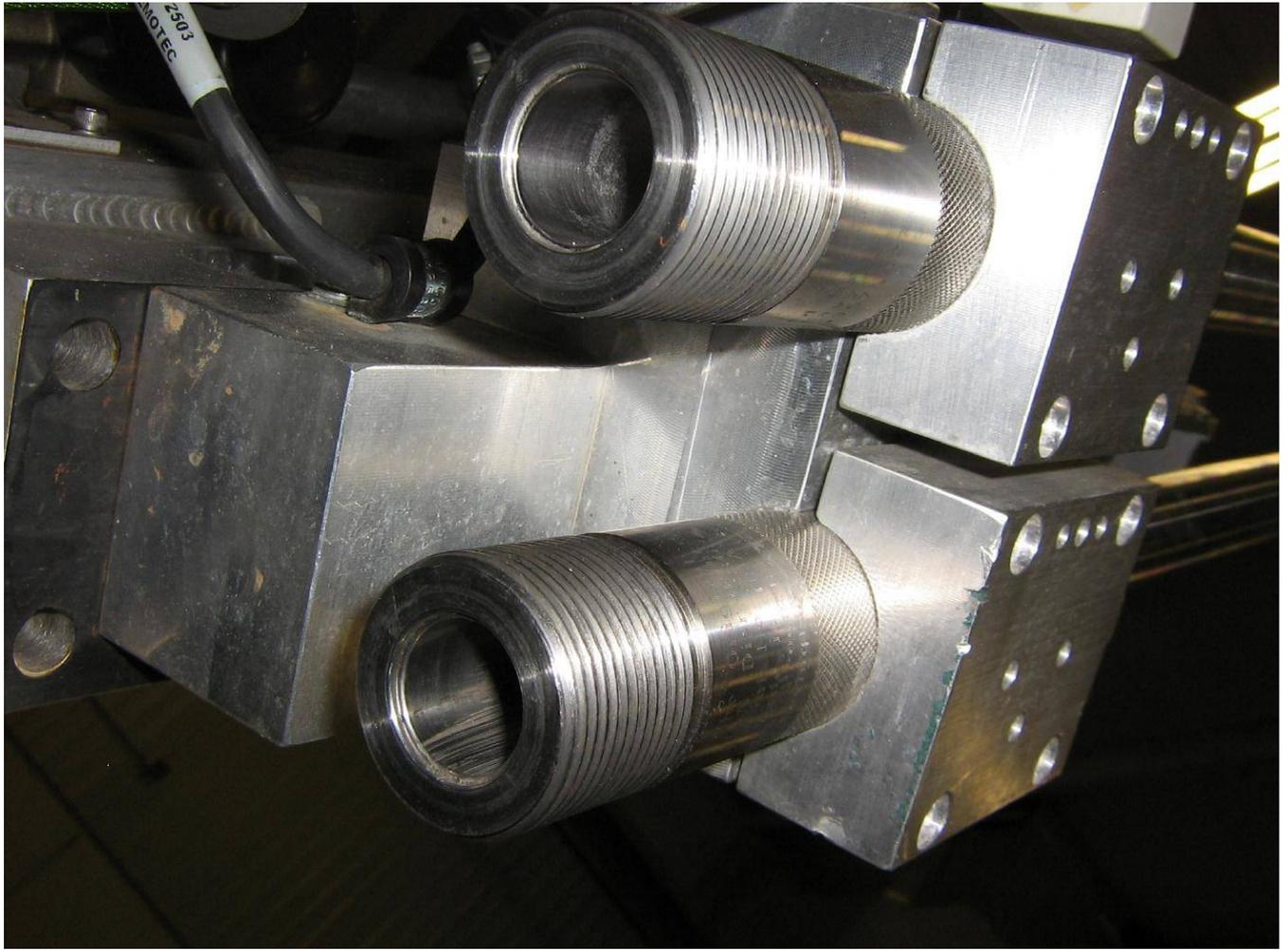
Overview of the antenna mounts, rotating camera, and manipulator arm.



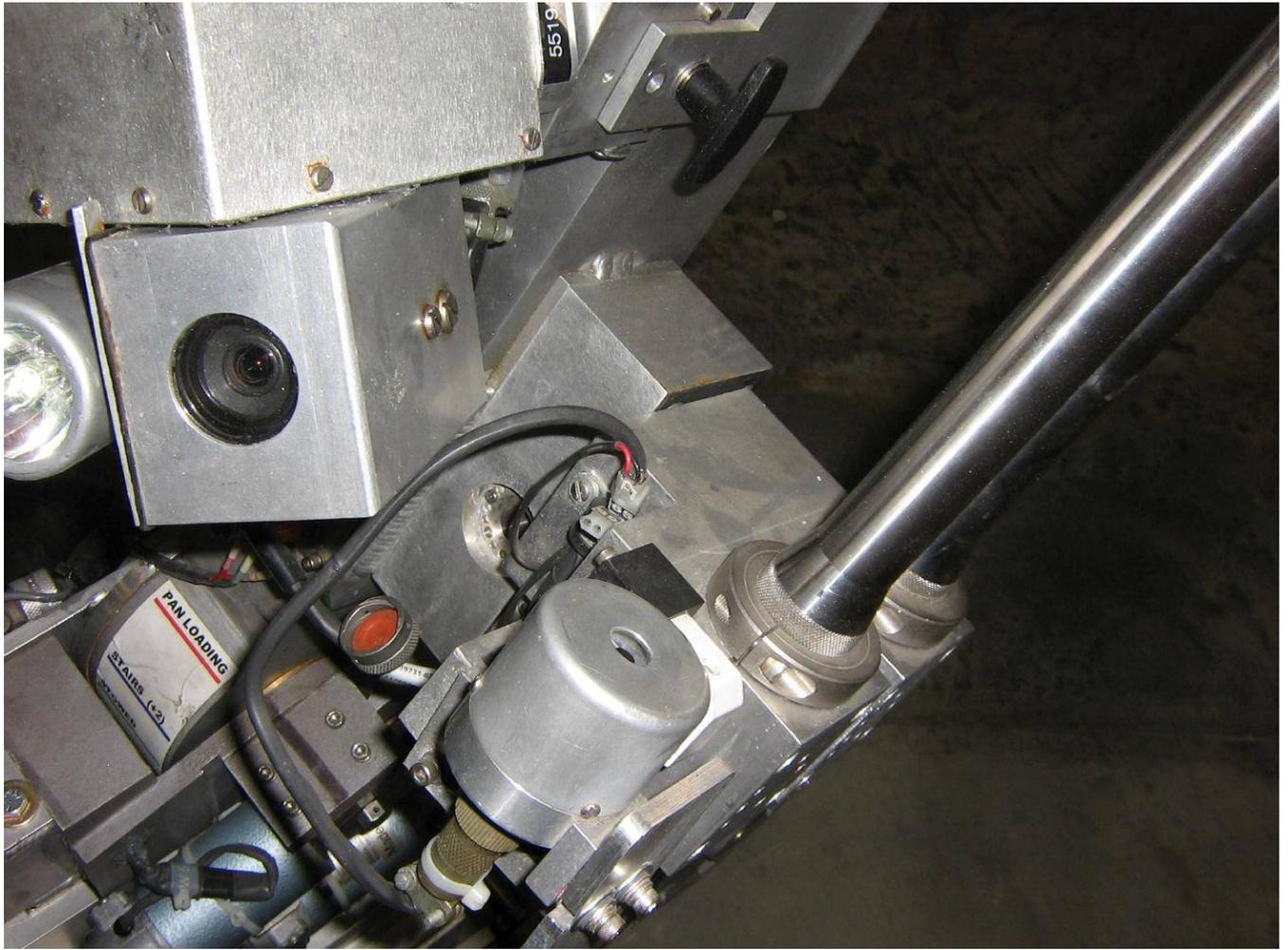
Manipulator arm controls and illumination.



Sealed gel-cell battery box.



Rear view of water disruptors with breech caps removed.



Video camera mounted above the water disruptors.

# Intercepting Older Digital Cordless Phones

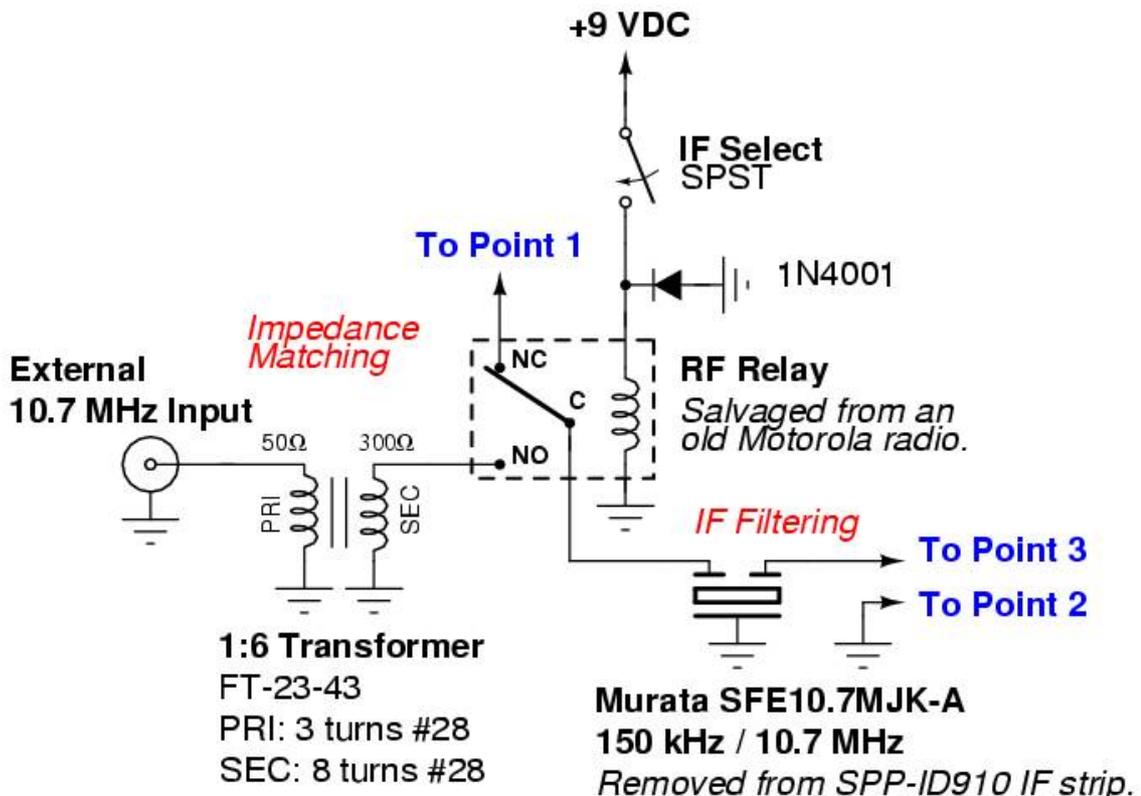
## Overview

This is an experimental project to decode the digital audio modulation used in some older VTech and Sony 900 MHz cordless phones. These phones use a two-level Frequency Shift Keying (FSK) modulation with an unknown audio encoding. Since these VTech and Sony phones (and probably others) tend to use the same AMD AM79C490 controller and encoding chip, it's possible to decode the digital audio by injecting your *own* intercepted target signal into a similar phone's 10.7 MHz IF strip.

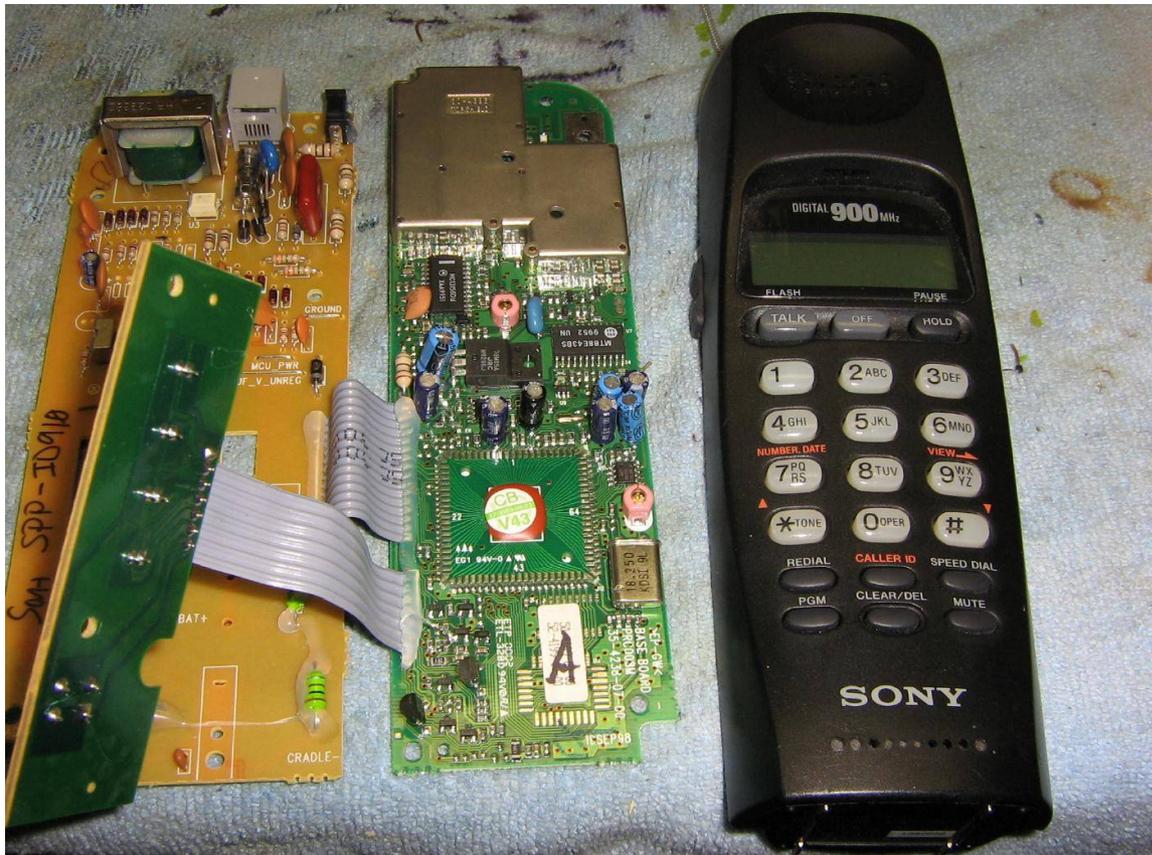
The receiver in those VTech and Sony is based around a Motorola MC13156 wideband IF chip which has an integrated data slicer output. The input frequency to the Motorola MC13156 is at 10.7 MHz, so an external receiver or mixer may be required to downconvert your received frequency.

The MC13156 converts the FSK modulation into a digital bit stream via the data slicer. This bit stream is then sent to the AMD AM79C490 for the proper audio decoding. The audio output from the AMD AM79C490 is in "the clear" and is then sent to the standard analog audio hybrid circuits in the rest of the phone.

The project here consists of a slightly modified Sony SPP-ID910 900 MHz digital cordless phone. A RF relay will be used to switch between the phone's stock 10.7 MHz IF and an external 10.7 MHz IF. The idea is that the phone will be first turned on and "initialized" to the stock handset. This enables all the audio decoding circuits. Then, the RF relay is activated and an external 10.7 MHz signal containing the encoded target modulation is injected into the MC13156 IF strip of the Sony SPP-ID910. The SPP-ID910's audio output is now from your intercepted RF signal.



## Pictures & Construction Notes



Internal overview of a stock Sony SPP-ID910 900 MHz digital cordless phone.

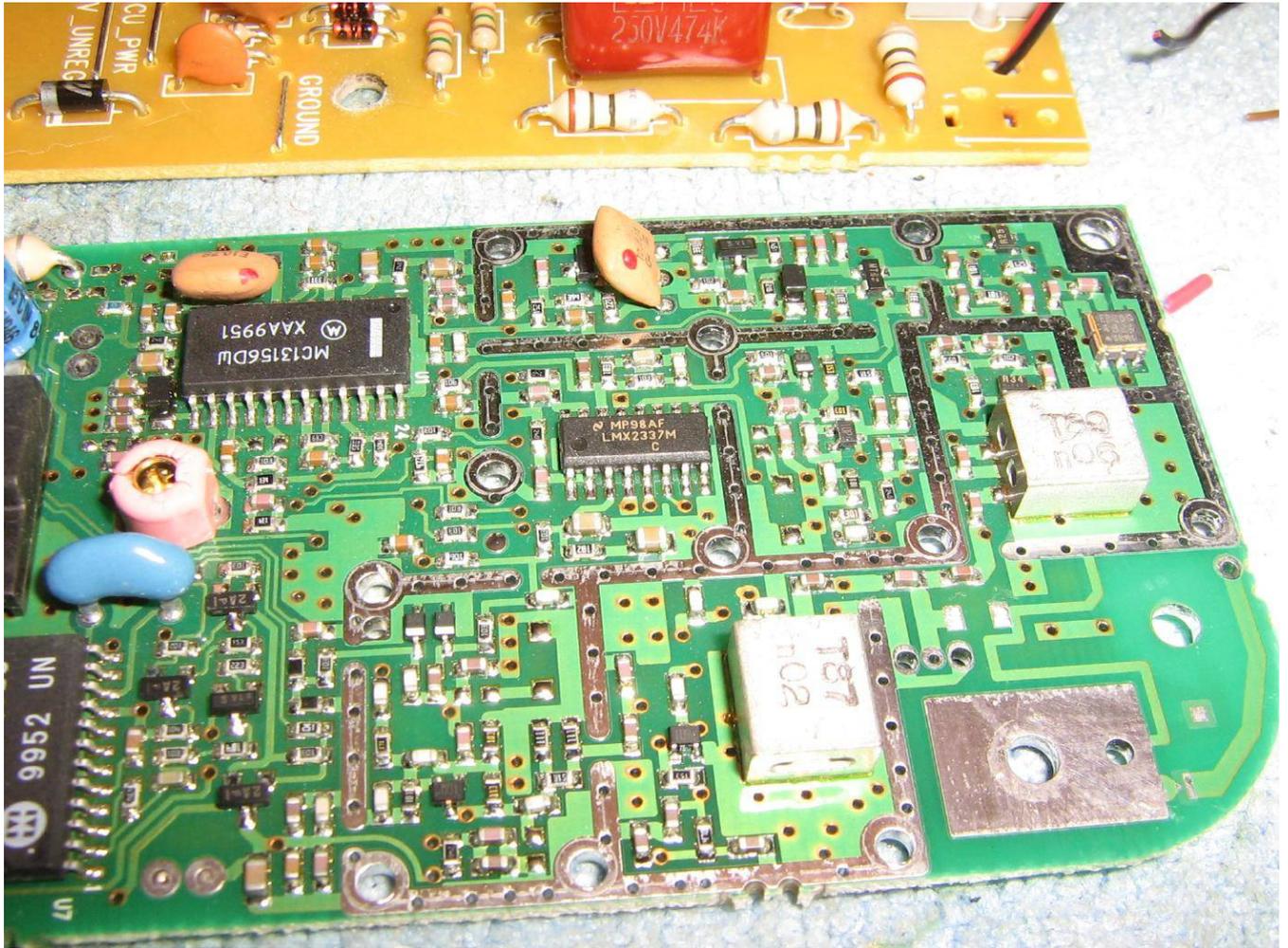
The phone's FCC ID is: AK8SPP-ID910

The active handset and base station center frequencies are:

<u>Display Channel</u>	<u>Handset (MHz)</u>	<u>Base (MHz)</u>
0	925.05	902.3
1	925.35	902.6
2	925.65	902.9
3	925.95	903.2
4	926.25	903.5
5	926.55	903.8
6	926.85	904.1
7	927.15	904.4
8	927.45	904.7
9	927.75	905.0

The handset transmits 22.75 MHz *higher* in frequency than the base station and a new channel is assigned whenever the unit is powered.

It is usually easier to intercept the cordless phone's base station signal as these are stationary and the RF signal won't contain any additional signal losses caused by antenna polarization mismatches from movement.



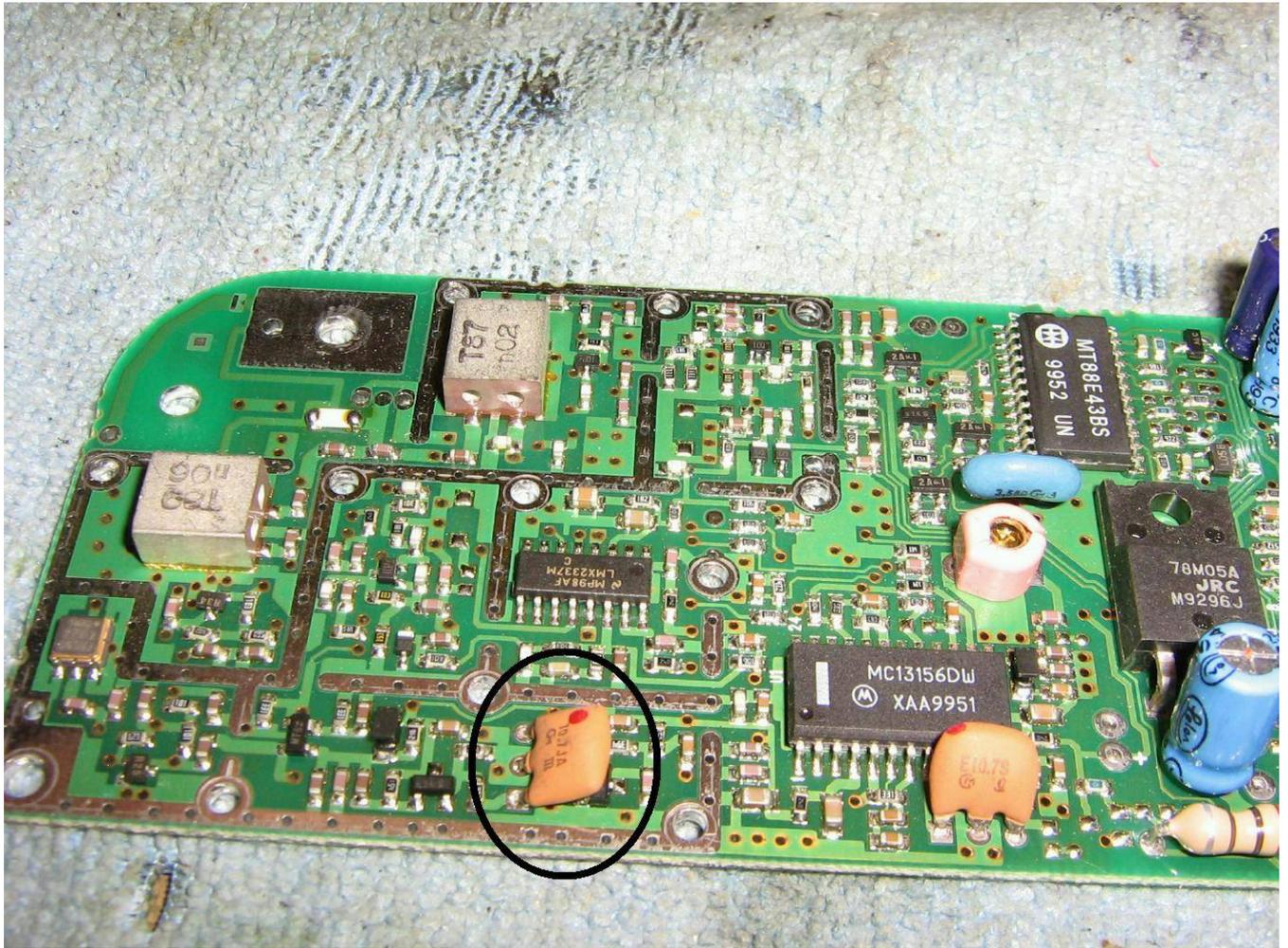
Overview of the RF section of the Sony SPP-ID910.

The antenna input on the lower-right and the two silver squares are the bandpass filters for separating the high/low transmit/receive frequencies.

A National LMX2337 dual-PLL synthesizer controls both the transmit and receive local oscillators.

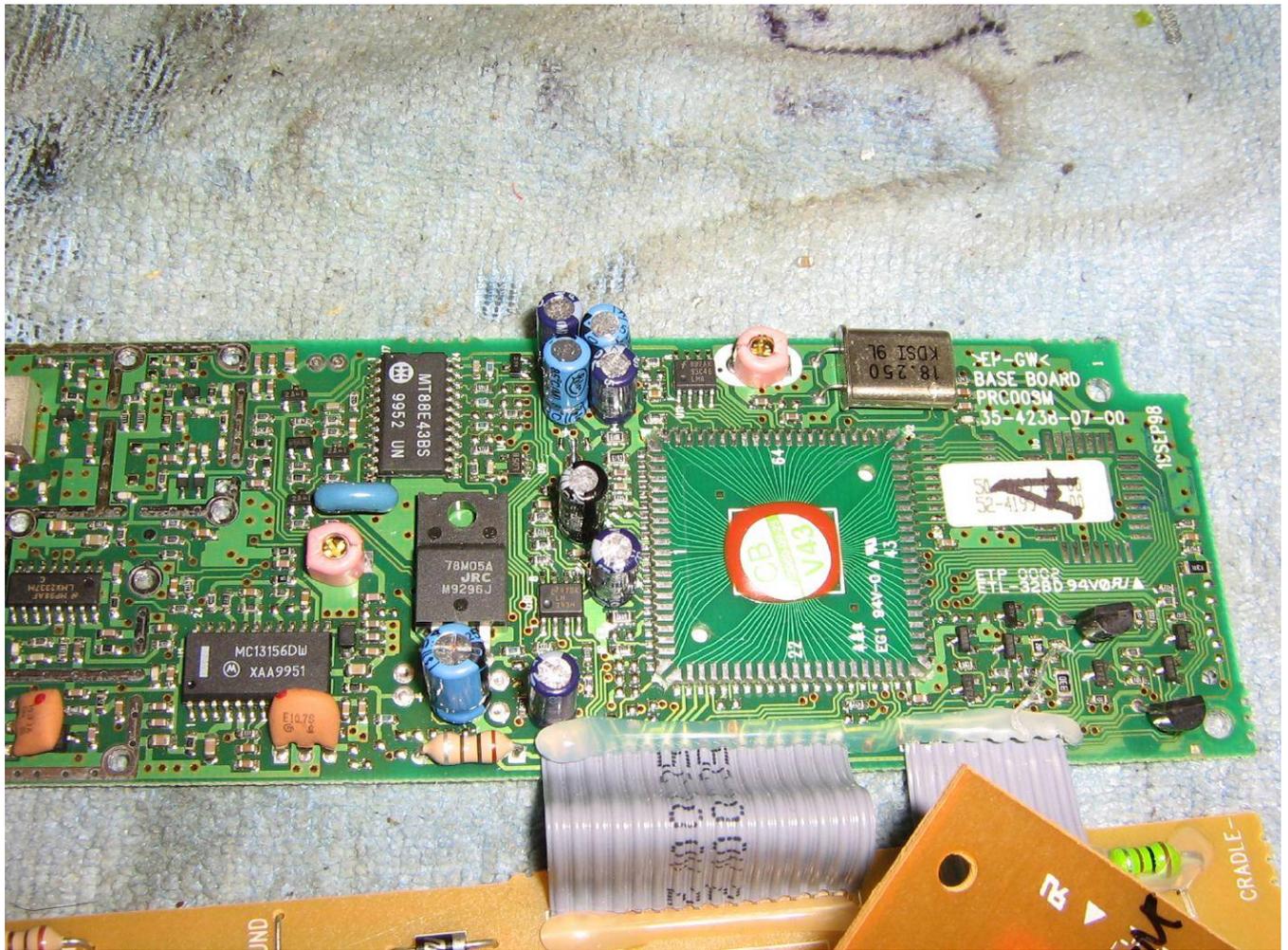
The 10.7 MHz IF strip is based around the Motorola MC13156 (large IC on upper-left) which is specifically designed for receiving narrowband FSK data transmissions.

The data stream output from the Motorola MC13156 (pin 17) is then sent to the AMD AM79C490 for audio decoding and the final coupling to the phone line.



The circled 10.7 MHz IF filter will need to be unsoldered.

The solder pads will then be used to handle the new incoming IF signals.

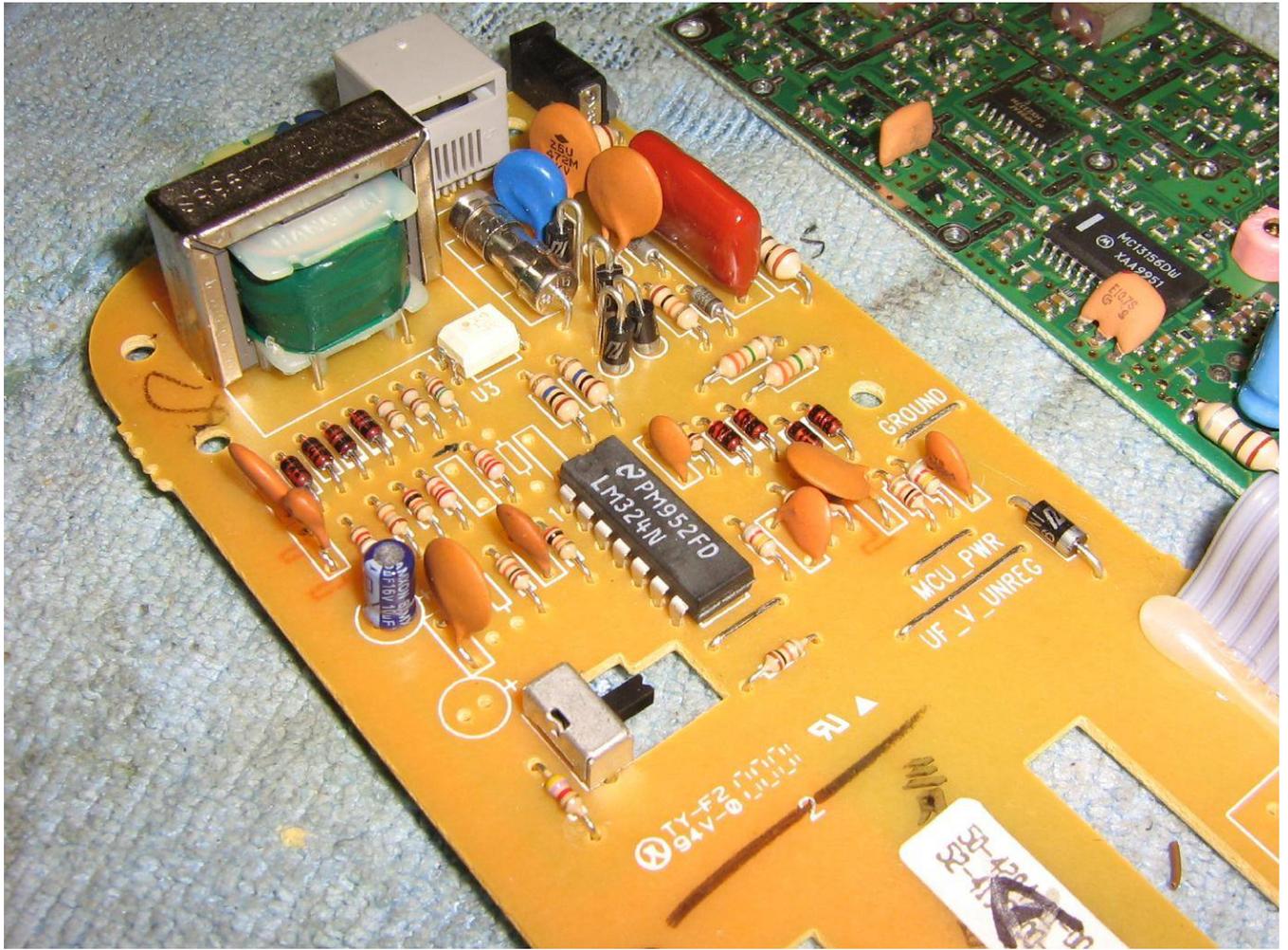


Overview of the 84-pin AMD AM79C490 telephone controller IC.

Details on this IC are difficult to track down, but here's a description of some of the main pins:

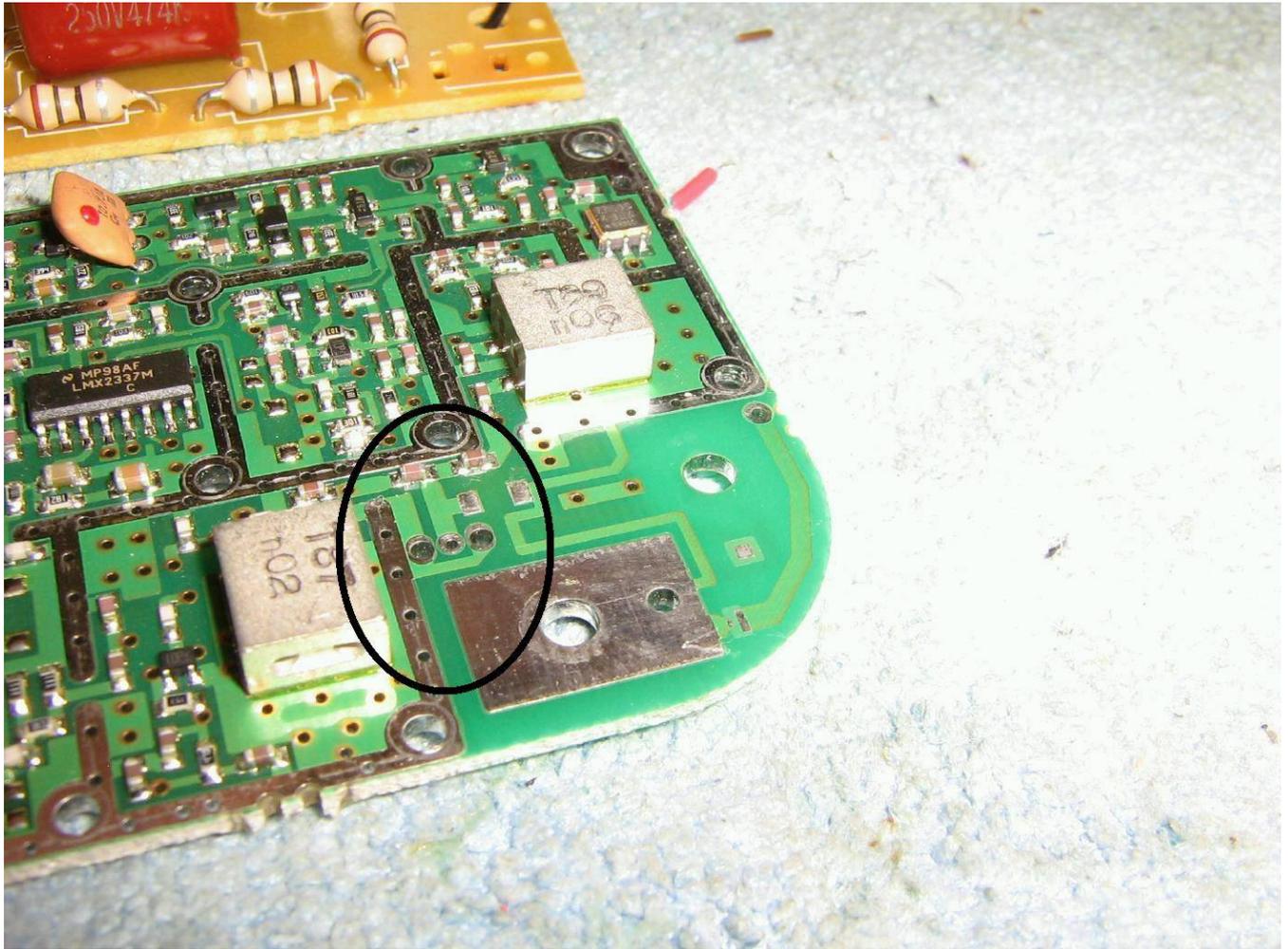
<u>Pin No.</u>	<u>Label</u>	<u>Connection Within the Phone</u>
1	AOP	Audio Output
2	AOM	
3	AIM	Audio Input/Microphone
4	AVss1	Ground
7	AVcc1	+5 VDC
8	TST1	
9	MODE0	
10	MODE1	
84	AVss2	Ground
83	BATMON	
82	AVcc2	+5 VDC
81	/RESET	
80	TST0	
79	MON3	
78	MON2	
77	MON1	
76	MON0	
75	RXBB	Receive Data from MC13156
74	TXBB	Transmit Data to VCO

Note that there appears to be two pins labeled for "test" functions.



Telephone line interface circuit board of the Sony SPP-ID910.

The final decoded audio will be taken from pin 1 of the LM324 shown above and sent to a front-panel BNC jack.

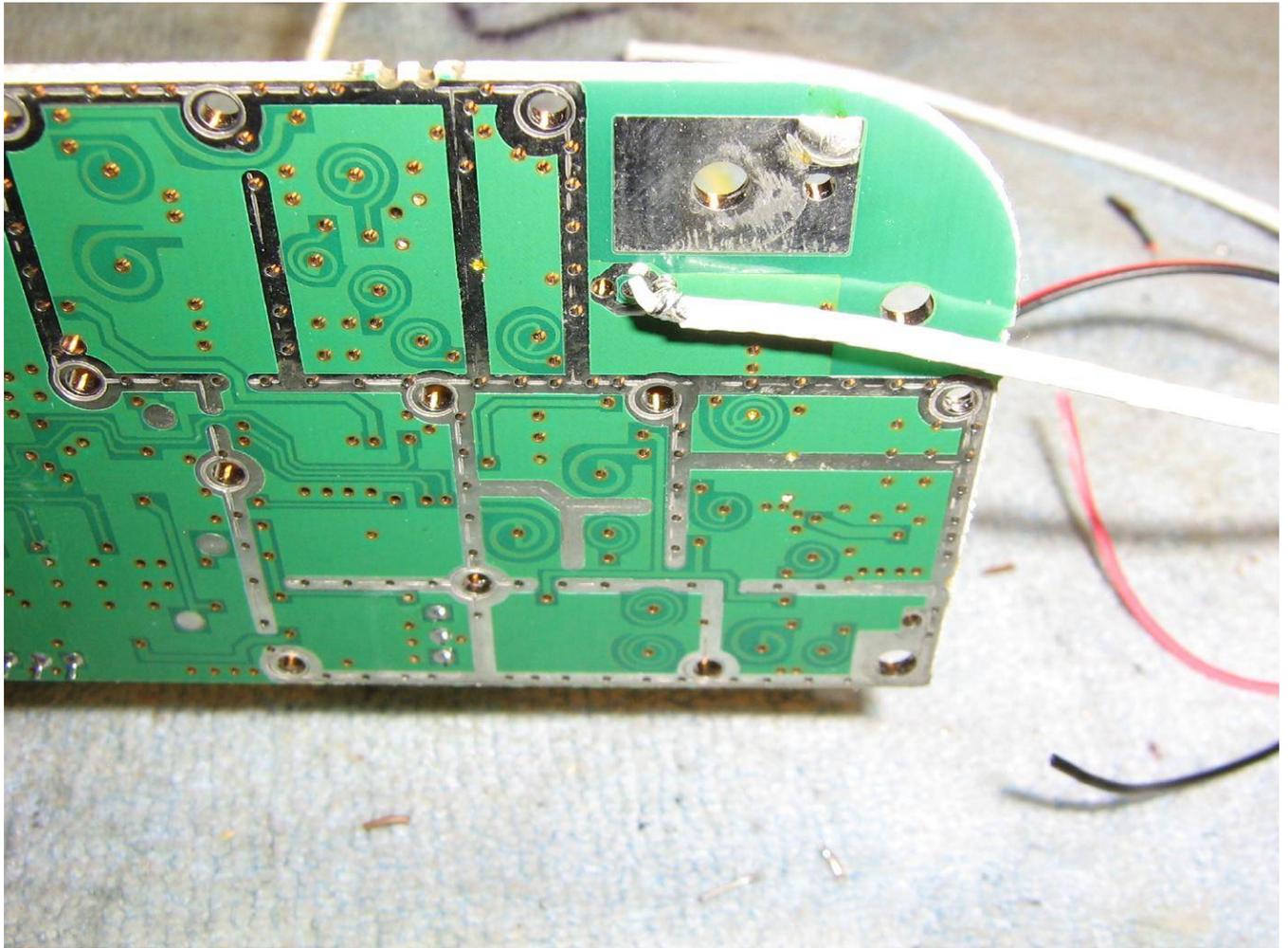


You'll want to add an external antenna to the base station.

Do this by unsoldering the 0-ohm jumper on the circuit board which connected to the pad for the stock "rubber duck" antenna.

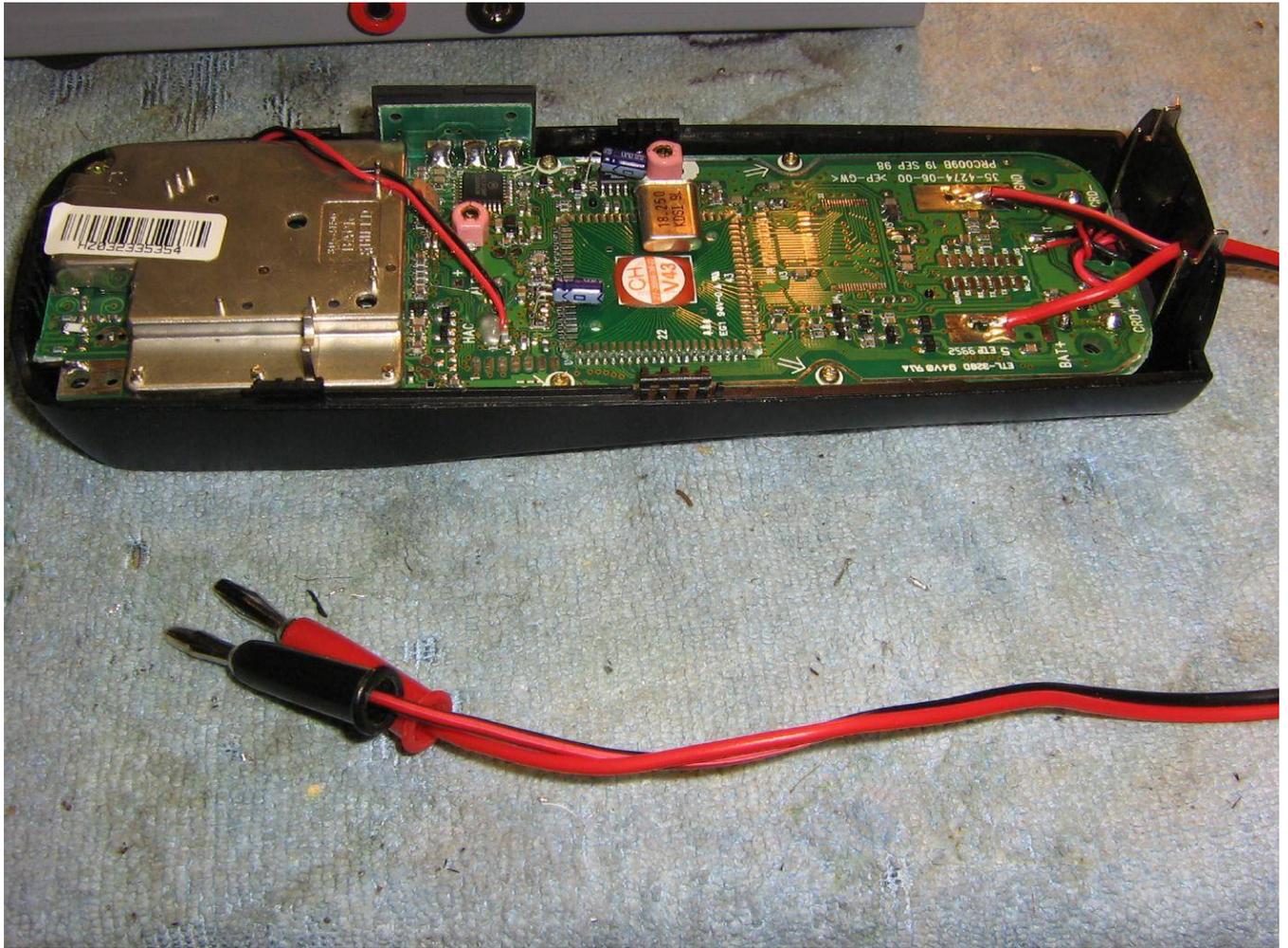
Solder in a piece of small-diameter 50 ohm coax into the plated holes, which are circled above.

The center conductor of the coax should go to the center hole. The other holes are ground and should be soldered to the coax's shield.



Attaching a piece of coax for the external antenna SMA jack.

I ended up soldering the coax to the bottom of the board, which was required for the final mounting arrangement used here.

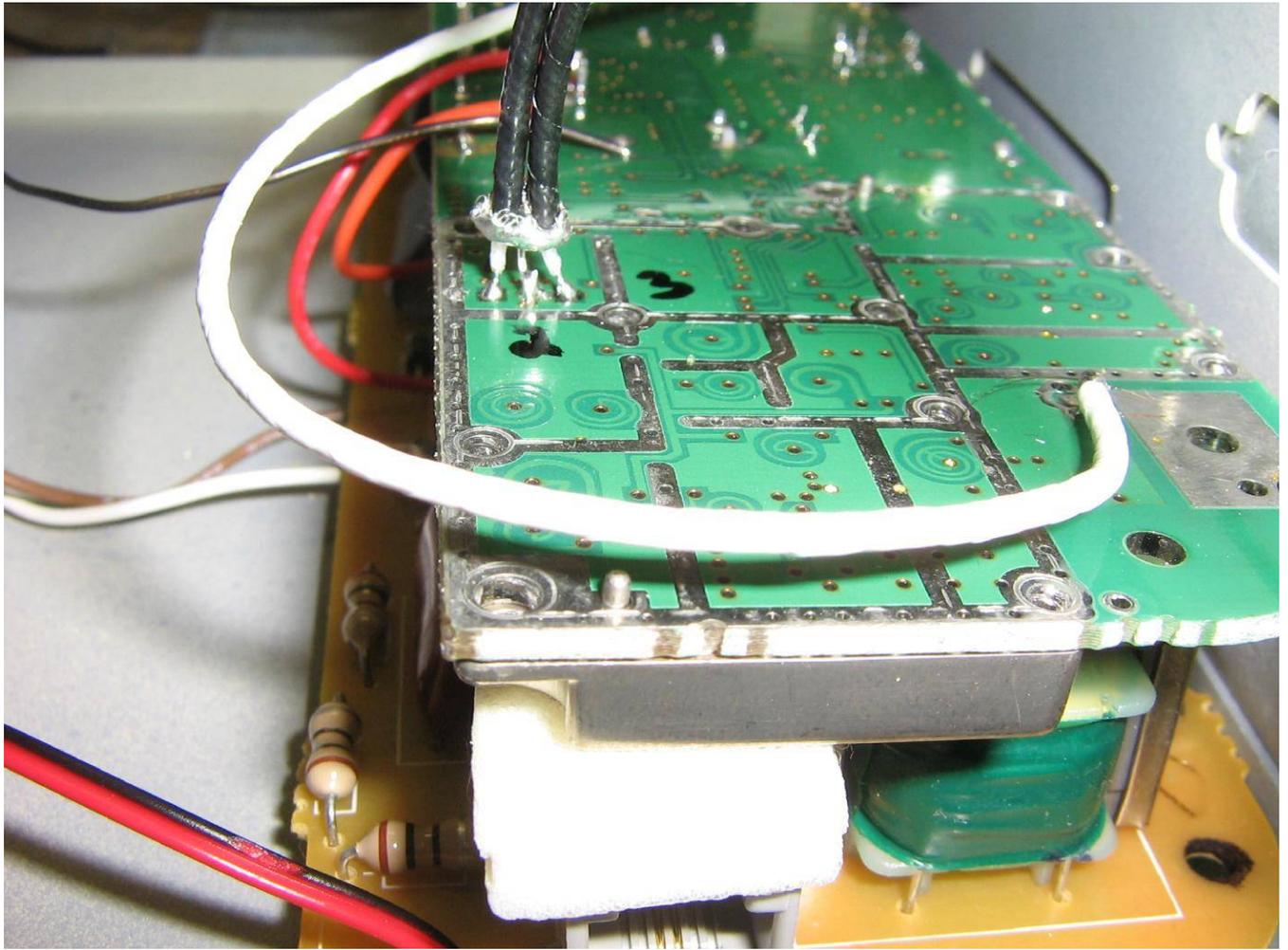


The handset requires no real major modifications.

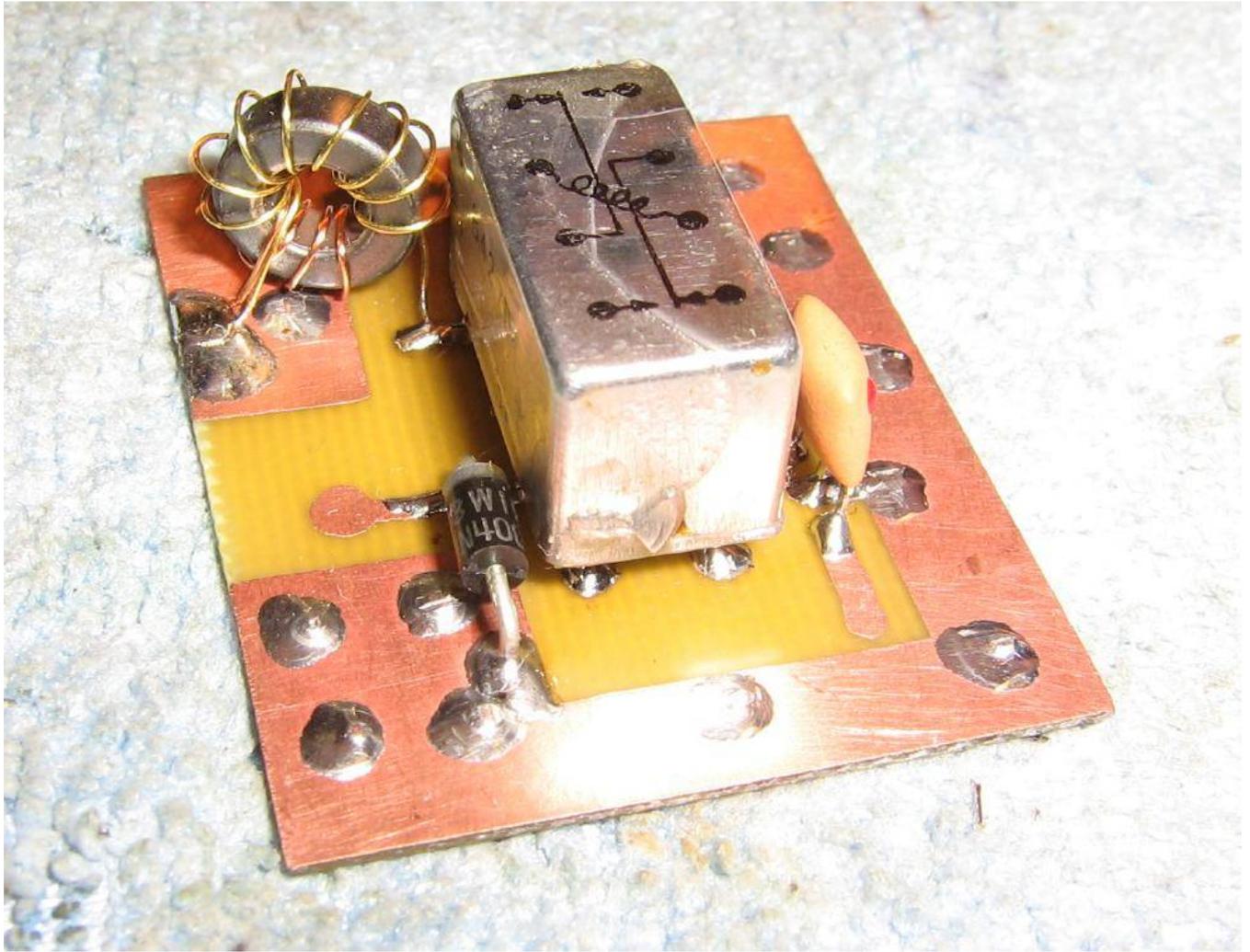
Solder two pieces of wire (with banana jacks) to the solder pads which held the battery springs. This is for applying the handset's required +5 VDC remotely.

Also, the stock antenna was replaced with a short little piece of wire.





Attaching small diameter 50-ohm coaxial cables to the input/output pads where the 10.7 MHz ceramic filter used to be.

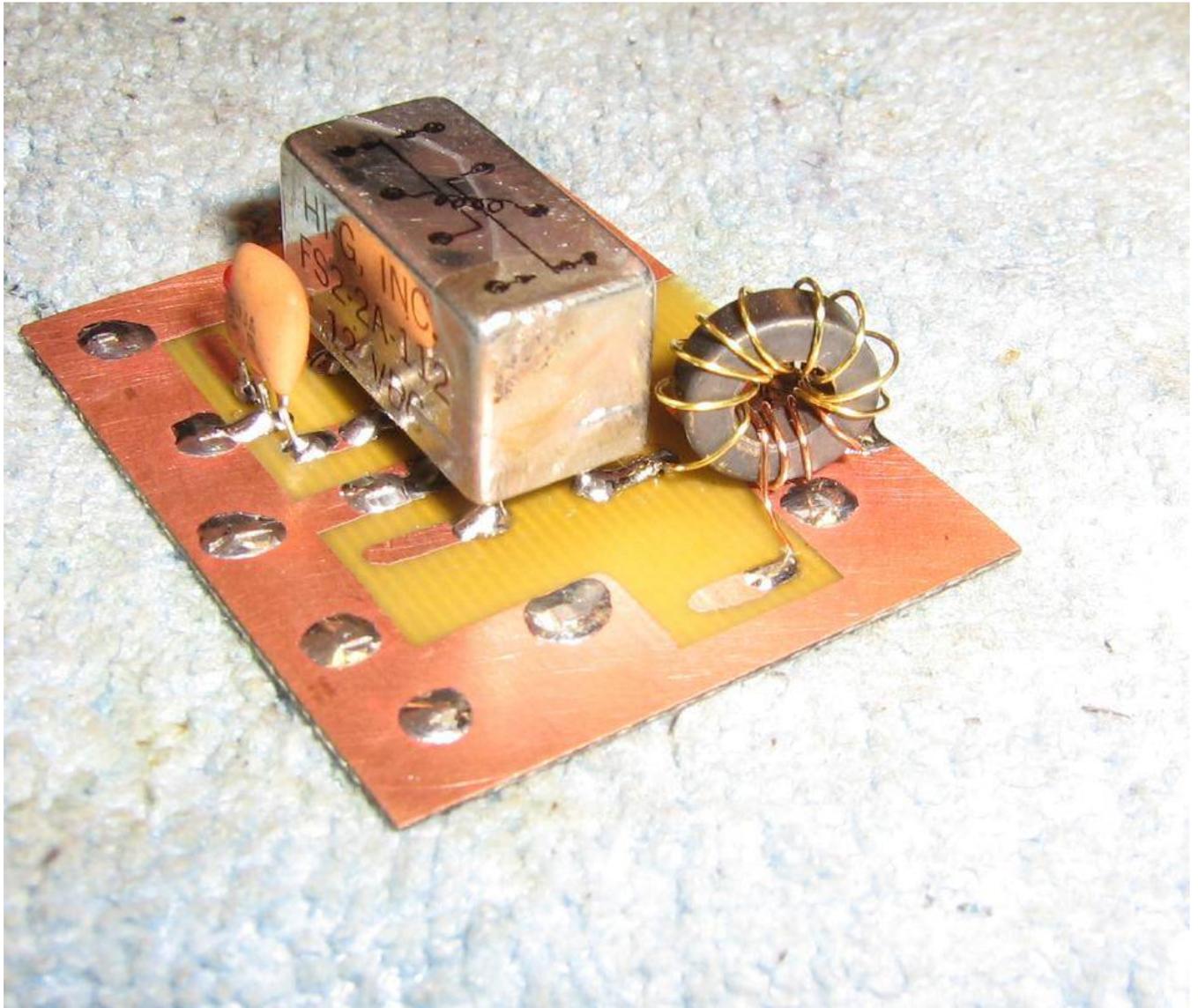


The RF relay which selects between the phone's stock 10.7 MHz IF and an external 10.7 MHz IF.

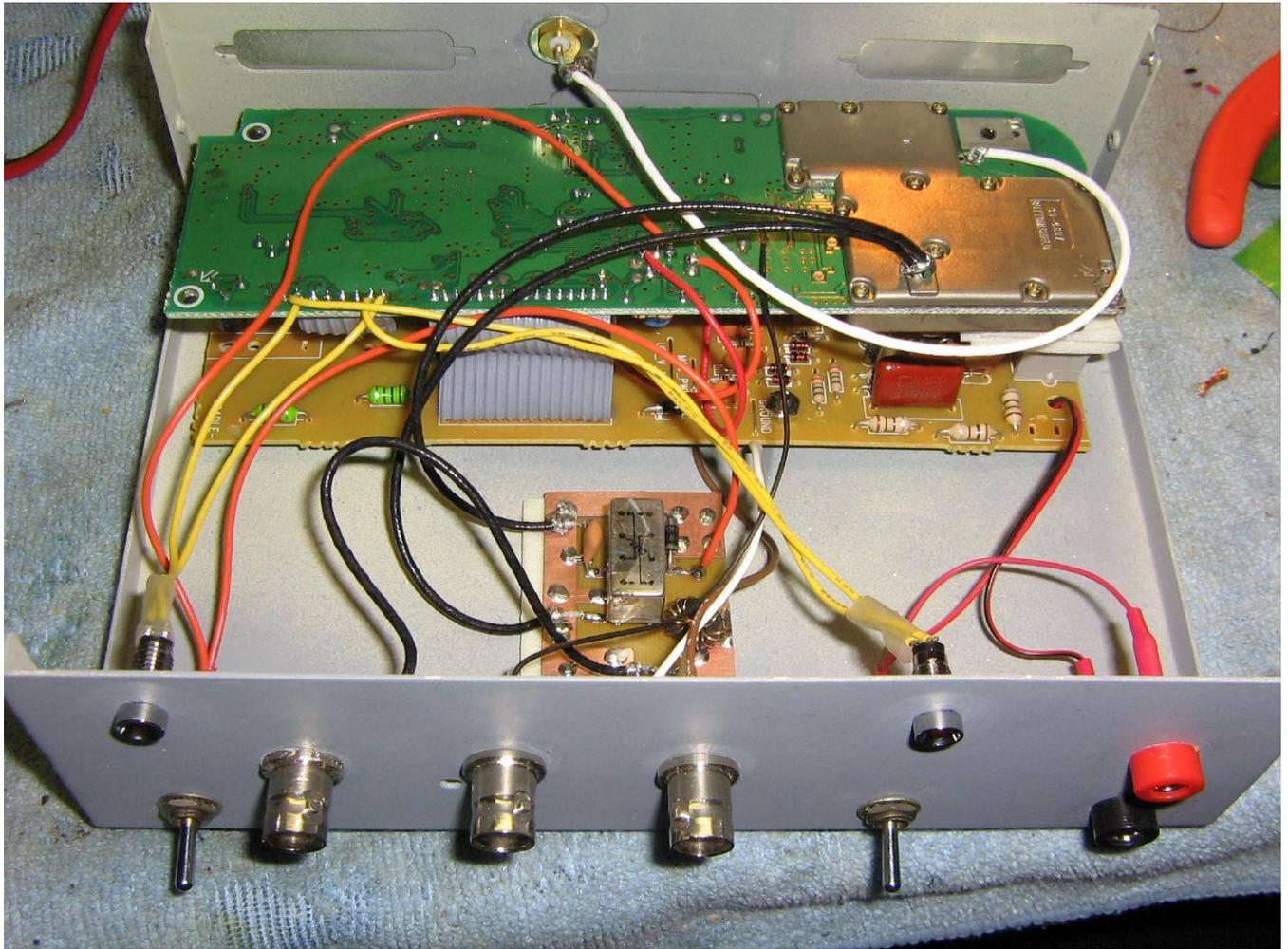
These RF relays can be found in some older Motorola two-way radios.

The input matching transformer is on the upper-left. It's used to convert the 50 ohms input to the 300 ohm impedance of the 10.7 MHz ceramic filter.

The ferrite toroid is an Amidon FT-23-43 with 3 turns of #28 enameled wire on the primary and 8 turns of #28 enameled wire on the secondary.



Alternate view of the RF relay and impedance matching circuit.

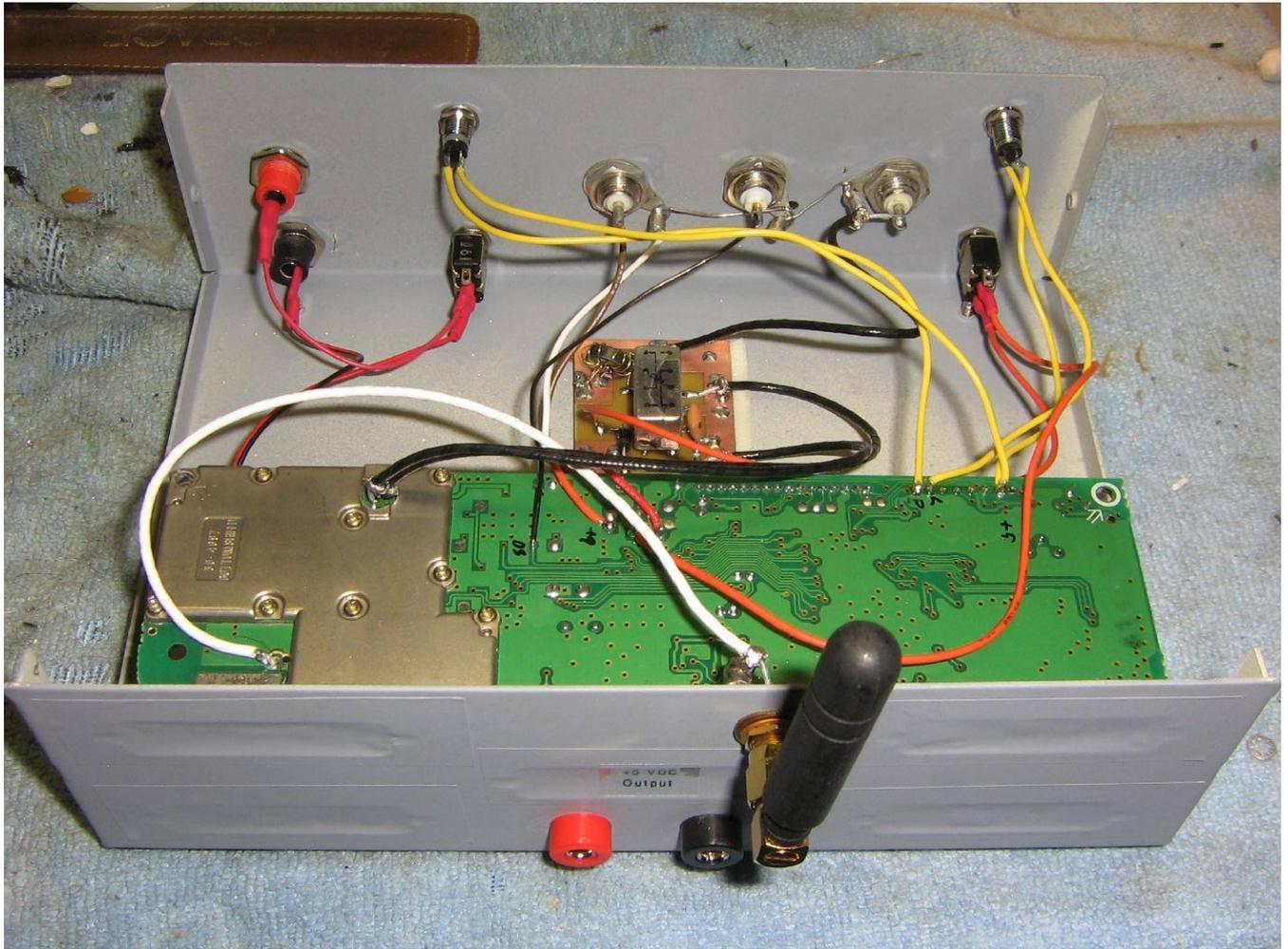


Completed internal view.

The front-panel BNC connectors are for an external 10.7 MHz input, MC13156 data slicer output, and audio output.

The banana jacks on the right are for the +9 VDC power the unit requires.

The LED on the left is from the "Line Enable" on the sub-circuit of the base station. The other LED is a power indicator.



Alternate overview showing the rear panel.

A SMA jack is for an external antenna.

The banana jacks along the bottom provide the +5 VDC output for powering the handset. Tap the output of the 7805 voltage regulator on the base station's main circuit board.

Optionally, tap pin 17 on the Motorola MC13156 (or pin 75 on the AMD AM79C490) to provide a data slicer output signal. This should go to a panel-mounted BNC jack.



Completed overview.

To use this device, apply +9 VDC power to the front-panel banana jacks. This will power both the base station unit and the handset.

Be sure the "IF Select" switch is set to the internal 10.7 MHz IF of the phone.

After a few seconds, the handset and base station should sync, displaying "CHANNEL SEARCHING..." and which channel they are using.

Press the "TALK" button on the handset and the "Line Enable" LED should light. The handset will now display "PHONE ON".

Flip the "IF Select" switch to choose an external 10.7 MHz containing your target data modulation. If it contains audio encoded by a similar Sony/VTech digital cordless phone, the line-level audio will be available on the "Audio Output" BNC jack.

If no audio is available, then it's possible to take the raw data stream from the "Data Output" BNC jack and apply some further external processing via hardware or software. This is should be handy for decoding pagers...

View the MC13156's datasheet for a more in-depth discussion of the MC13156's FSK data decoding possibilities.

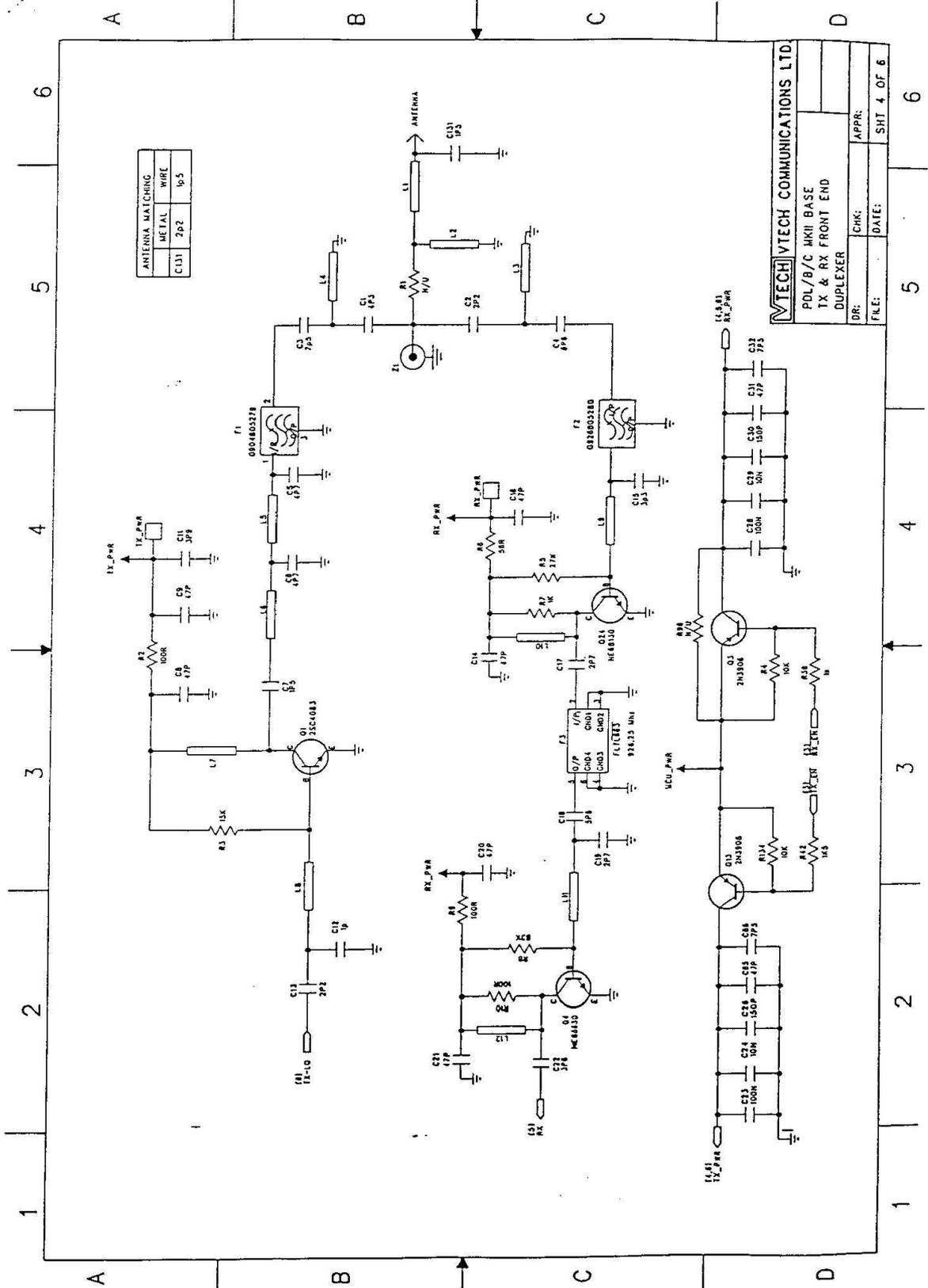


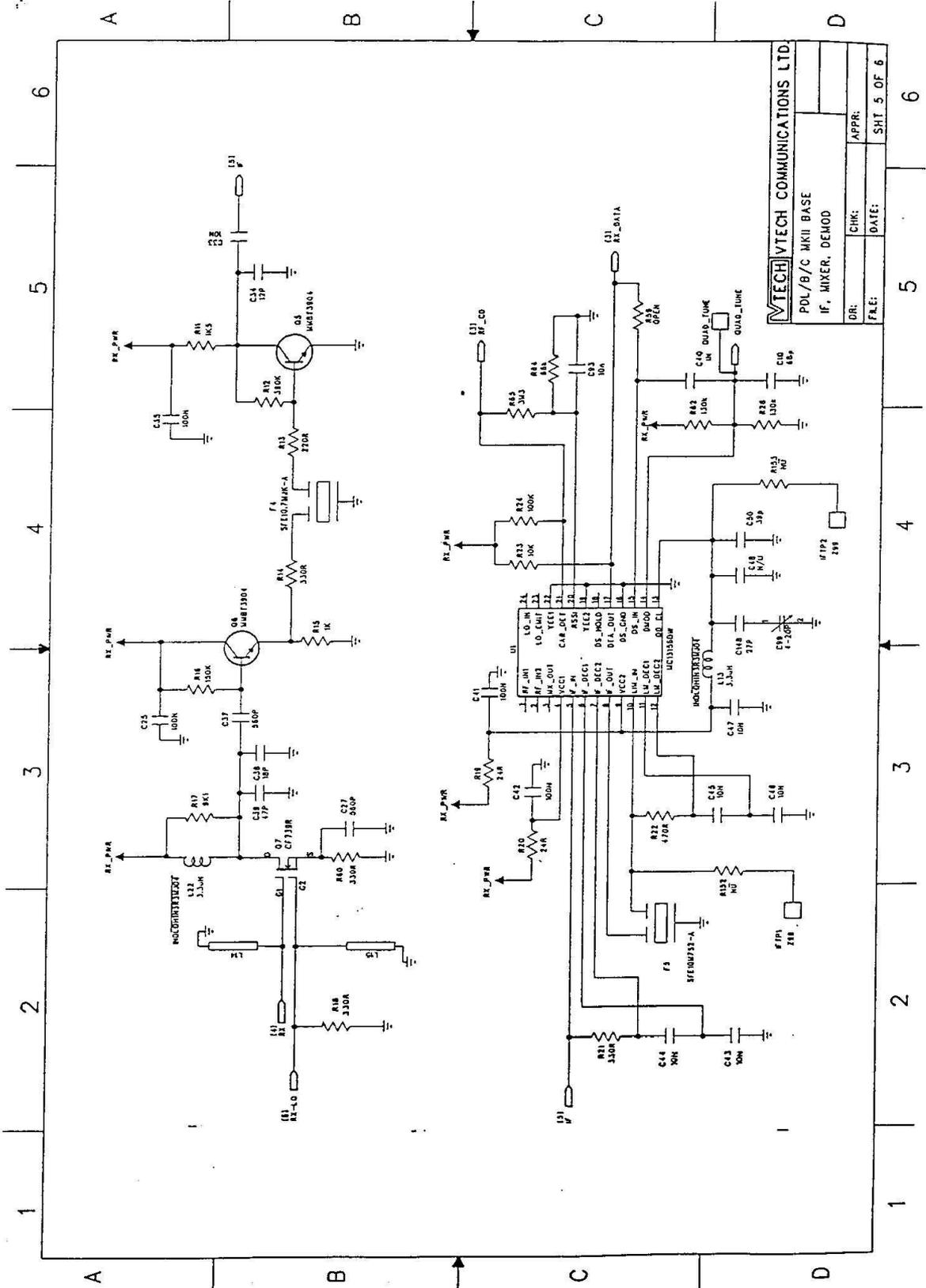
IFR FM/AM-1200S spectrum analysis of a Sony SPP-ID910 900 MHz digital cordless phone in operation.

The center frequency of the base station is at 903.8 MHz. The spectrum display is 20 kHz per horizontal division.

# Sony SPP-ID910 Schematics

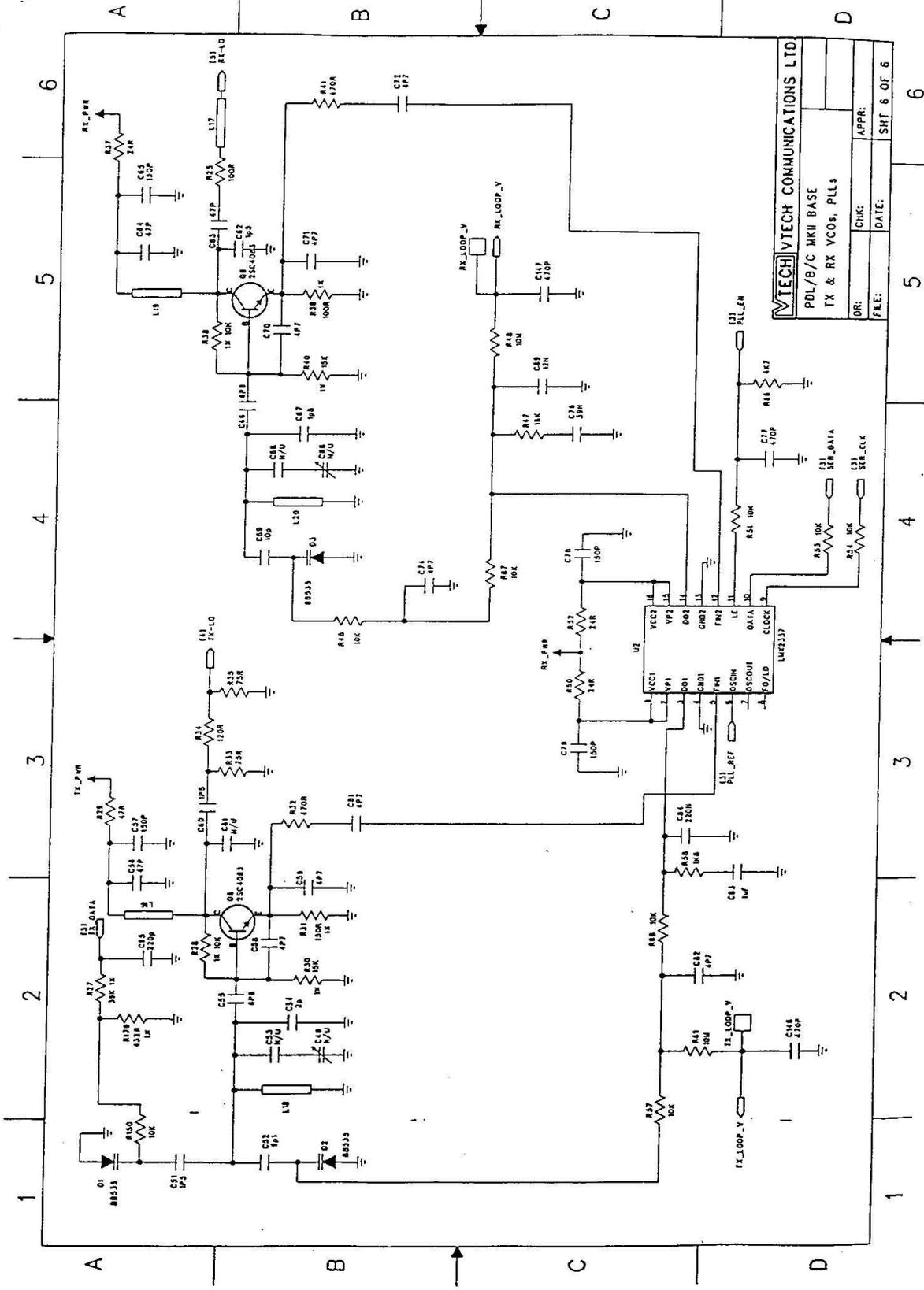
42380000.sch-4 - Tue Jan 6 09:42:02 1998





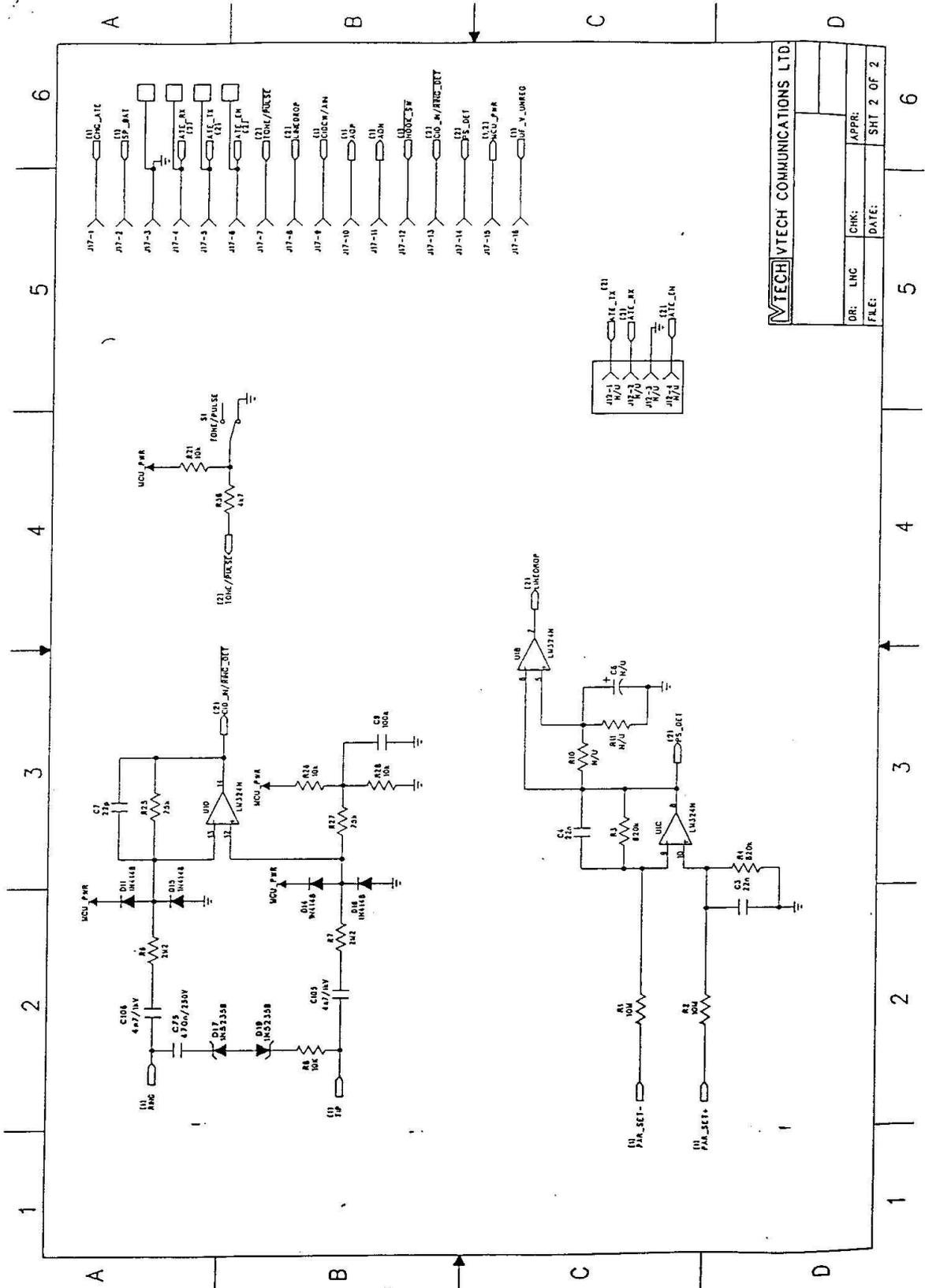
**TECH VTECH COMMUNICATIONS LTD.**  
 PDL/B/C MKII BASE  
 IF MIXER DEMO

DR:	CHK:	APPR:
FILE:	DATE:	SHT 5 OF 6

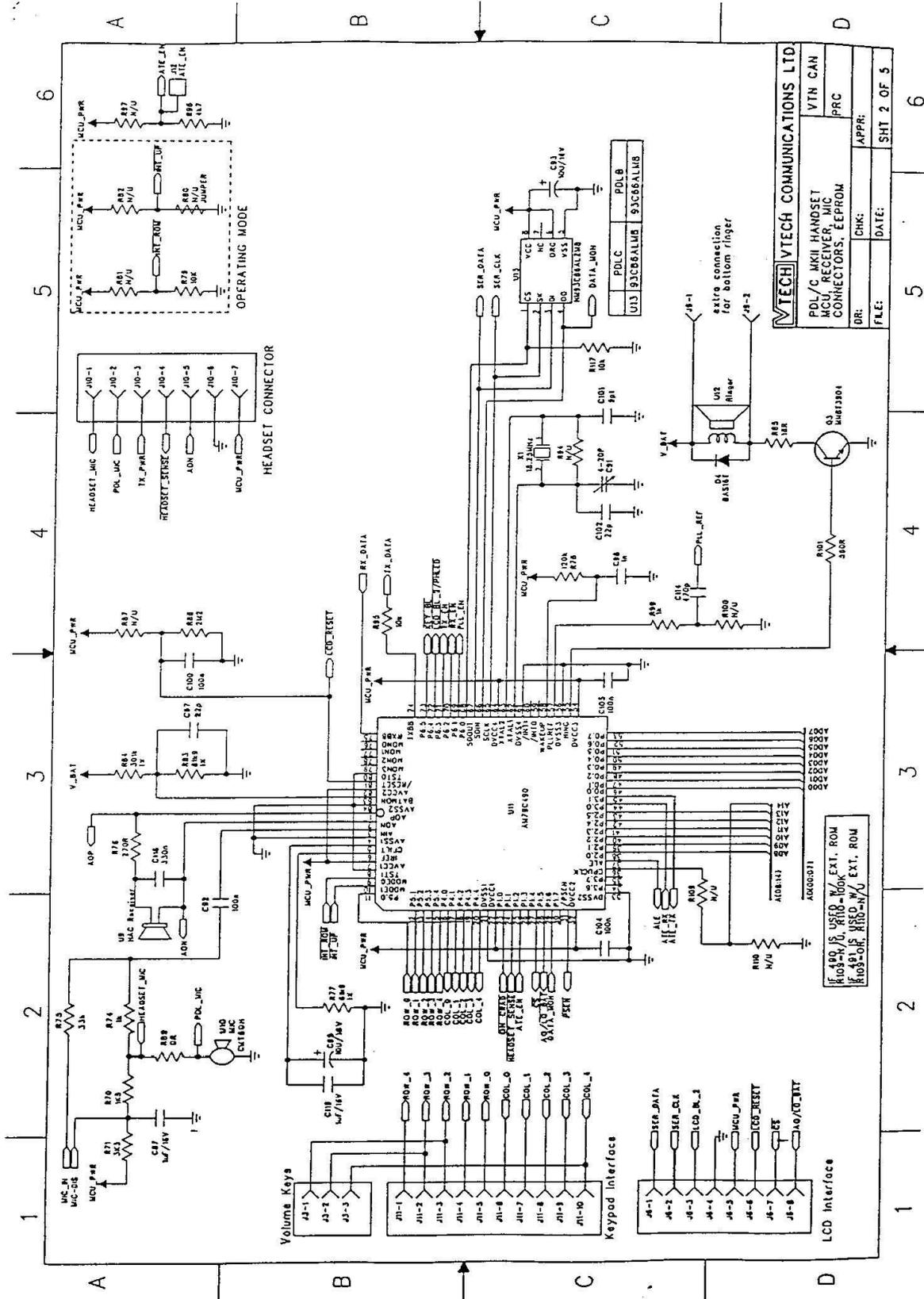


TECHNIVTECH COMMUNICATIONS LTD			
PDL/B/C MKII BASE			
TX & RX VCOs, PLLs			
DR:	CHK:	DATE:	APPR:
F.K.E.:			SHT 6 OF 6









TECH VTECH COMMUNICATIONS LTD	
PDL/C MKII HANDSET	VTN CAN
MCU RECEIVER, MIC	PRC
CONNECTORS, EEPROM	APPR:
DR:	CHK:
FILE:	DATE:
	SHT 2 OF 5

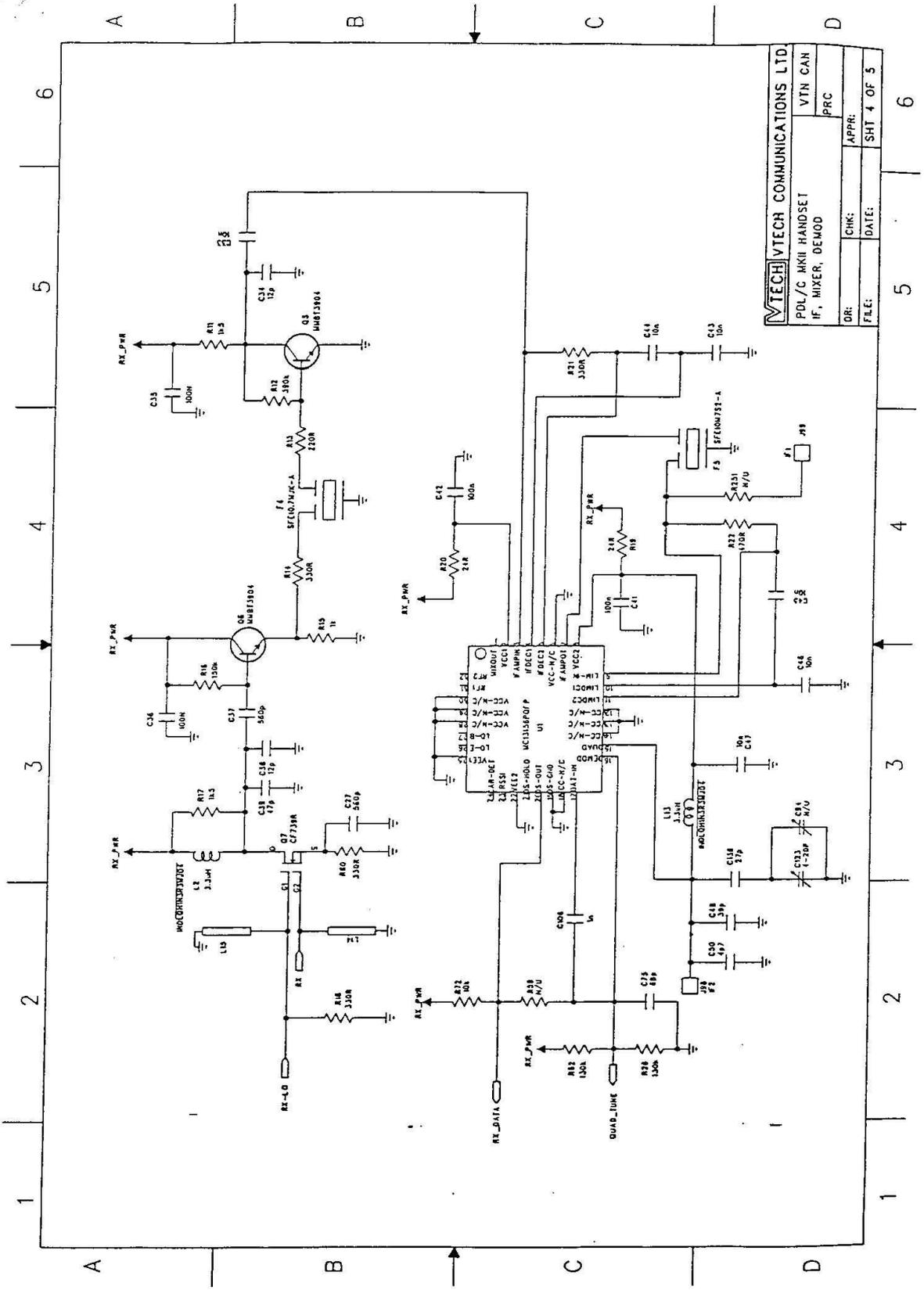
#103=0P, #110=WORK/EXT. ROM  
 #101=1S USED N/ EXT. ROM  
 #103=0P, #110=N/

PDLB	U13 93CB6ALMB 93CB6ALMB
------	-------------------------

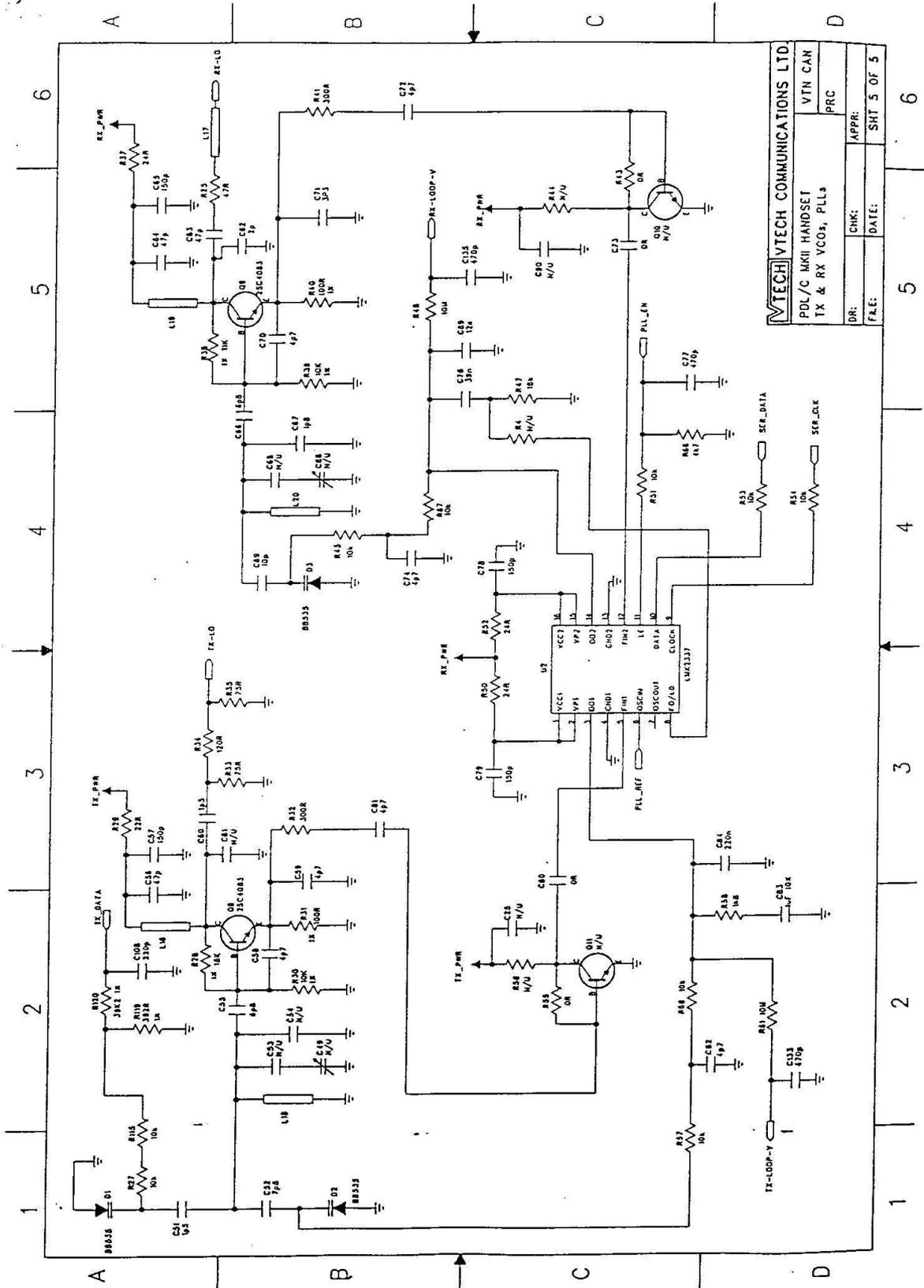
1 2 3 4 5 6

1 2 3 4 5 6





VTECH COMMUNICATIONS LTD	
DR:	CHK:
FILE:	DATE:
APPR:	SHT 4 OF 5
PD/C MKII HANDSET	
VF, MIXER, DEMOD	
VTN CAN	
PRC	



**Bonus**

Michael A. Keller

*Ida M. Green University Librarian  
and Director of Academic  
Information Resources*

*Cecil H. Green Library  
Stanford, California  
94305-6004*

*Michael.Keller@stanford.edu  
telephone 650-723-5553  
fax 650-725-8962*

*The Stanford University Libraries*

11 August 2011

Mr. Eric Hunt  
General Delivery  
280 East 1st Avenue  
Broomfield, CO 80020

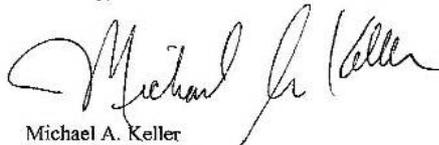
Mr. Hunt:

This letter serves as formal notice that you are not to enter any of the University Libraries, including Green and Meyer libraries, nor are you to be around any Stanford library facilities for any purpose whatsoever.

The Stanford Libraries require that all patrons respect the terms of service of the databases and other research resources we make available. On at least two occasions you have violated those terms of service, thus jeopardizing access to those resources for our patrons. As a private institution, Stanford reserves the right to bar anyone from any or all parts of its premises. You have no affiliation with Stanford University, and there is no reason for you to be in or around any of the Stanford Libraries.

Our Access Services team has been notified of this situation, and you are prohibited from purchasing access privileges to any of SULAIR's libraries. If after being served with this letter you choose to disregard these instructions, you will be subject to legal action, including possible criminal charges for trespass.

Sincerely,



Michael A. Keller  
University Librarian

cc: Laura Wilson, Chief, Stanford Department of Public Safety  
Lauren Schoenthaler, Stanford Office of the General Counsel

Eric Hunt has a documentary project going on called [Last Days of the Big Lie](#). His project is to debunk some of lies and propaganda in the infamous Steven Spielberg documentary *The Last Days*.

Eric Hunt is using **the actual audio & video footage** from USC's "Survivors of the Shoah Visual History Foundation" to debunk some of the myths surrounding the events of the "Holocaust." Hunt has used this information to uncovered numerous instances of lying and witness manipulation in Spielberg's movies.

Above is what Stanford College did when they found out Hunt was using their library. So much for "freedom of speech" or "academic freedom." Contact Michael Keller at the Stanford University Library: [Michael.Keller@stanford.edu](mailto:Michael.Keller@stanford.edu) (650-723-5553) and gently remind him that both Stanford and USC colleges receive taxpayer funding.

## End of Issue #90



Any Questions?

### **Editorial and Rants**

*Welcome to Eric Corley's New York. Now leave your freedoms at the border...*

#### **New York Democrats Argue Free Speech is a Privilege That Can Be Revoked**

October 7, 2011 – From: [dailytech.com](http://dailytech.com)

The First Amendment of the U.S. Constitution clearly states:

*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.*

However, that hasn't stopped state and federal officials to creatively redefine what "freedom of speech" means. Of late there have been multiple attempts to legislate digital censorship, with government officials looking to decide what forms of online speech they feel aren't okay and make them illegal.

The latest effort on this front comes from four Democratic New York state senators, who have published a report entitled "Cyberbullying: A Report on Bullying in a Digital Age." In that report, Sen. Jeff Klein, Diane Savino, David Carlucci, and David Valesky argue that the First Amendment has been long misinterpreted by politicians and courts and really means that free speech is a privilege (not a right), which can be taken away.

They write:

*Proponents of a more refined First Amendment argue that this freedom should be treated not as a right but as a privilege — a special entitlement granted by the state on a conditional basis that can be revoked if it is ever abused or maltreated.*

The argument that free speech was not intended as a protected right seems rather baffling given that the First Amendment is part of the "Bill of Rights."

Of course they argue that state politicians should be tasked with creating laws of what they feel constitutes "abuse" of free speech and grounds for censorship. According to their full report, possible "abusive" speech that they feel should be banned includes:

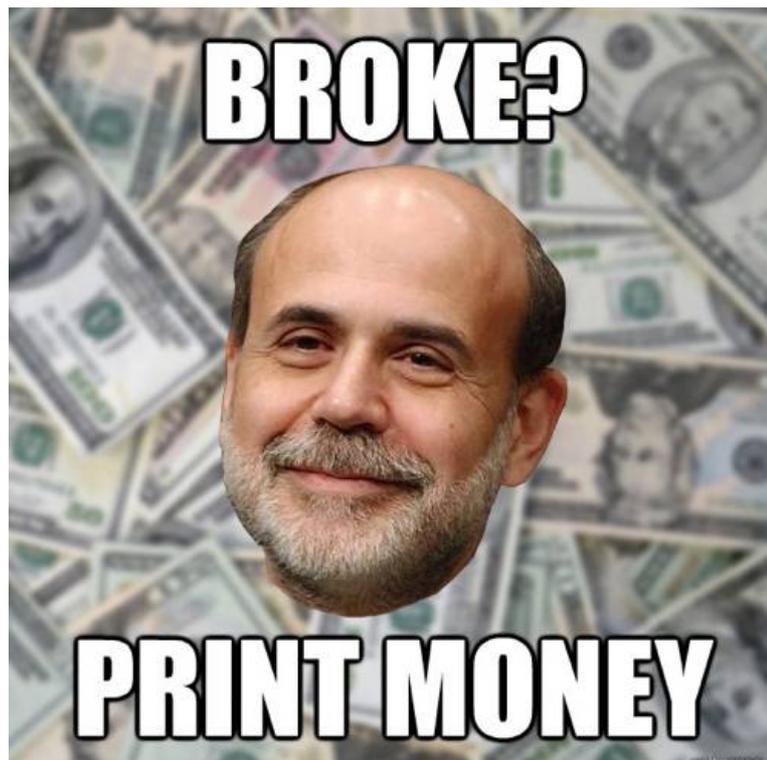
1. Leaving hurtful messages online: "LEAVING IMPROPER MESSAGES ON ONLINE MESSAGE BOARDS OR SENDING HURTFUL AND DAMAGING MESSAGES TO OTHERS;"
2. Flaming people online: "FLAMING (HURTFUL, CRUEL, AND OFTENTIMES INTIMIDATING MESSAGES INTENDED TO INFLAME, INSIGHT, OR ENRAGE);"
3. "Happy slapping" (a 2005 meme that the befuddled Senators appear to mistake for a current problem): "HAPPY SLAPPING (RECORDING PHYSICAL ASSAULTS ON MOBILE PHONES OR DIGITAL CAMERAS, THEN DISTRIBUTING THEM TO OTHERS);"
4. Trolling online: "TROLLING (DELIBERATELY AND DECEITFULLY POSTING INFORMATION TO ENTICE GENUINELY HELPFUL PEOPLE TO RESPOND (OFTEN EMOTIONALLY), OFTEN DONE TO PROVOKE OTHERS);"
5. Exclusion of people: "EXCLUSION (INTENTIONALLY AND CRUELLY EXCLUDING SOMEONE FROM AN ONLINE GROUP)."

Such legislation are perceived by some as an overreaction of extreme recent incidents of cyberbullying. However, it's hard to avoid the possibility that such censorship couldn't be abused by politicians to silence political rivals.

After all, if you can put someone in speech for "trolling" and "leaving hurtful messages on online message boards," does that mean ruling politicians can imprison those who criticize them online? Clearly that's how officials in other countries like China have used similar laws. Is the U.S. headed down a similar road?

The Senators have used their report to draft a proposed law.

Under the proposed law, "offensive" speech would become constitute Third-Degree Stalking, a Class A Misdemeanor. And if someone commits suicide due to online harassment -- or "bullycide" as the report calls it -- the harassers can be charged with Second-Degree Manslaughter, a Class C Felony.



*Note how they dance around the fact that non-Whites are dragging down the SAT scores. Change!*

## **SAT Reading Scores Fall to Lowest Level on Record**

September 14, 2011 – From: [mercurynews.com](http://mercurynews.com)

By Justin Pope

Scores on the critical reading portion of the SAT college entrance exam fell three points to their lowest level on record last year, and combined reading and math scores reached their lowest point since 1995.

The College Board, which released the scores Wednesday, said the results reflect the record number of students from the high school class of 2011 who took the exam and the growing diversity of the test-taking pool — particularly Hispanics. As more students aim for college and take the exam, it tends to drag down average scores.

Still, while the three-point decline to 497 may look small in the context of an 800-point test, it was only the second time in the last two decades reading scores have fallen as much in a single year. And reading scores are now notably lower than scores as recently as 2005, when the average was 508.

Average math scores for the class of 2011 fell one point to 514 and scores on the critical reading section fell two points to 489.

Other recent tests of reading skills, such as the National Assessment of Education Progress, have shown reading skills of high-school students holding fairly steady. And the pool of students who take the SAT is tilted toward college-goers and not necessarily representative of all high school students.

But the relatively poor performance on the SATs could raise questions whether reading and writing instruction need even more emphasis to accommodate the country's changing demographics.

**Roughly 27 percent of the 1.65 million test-takers last year had a first language other than English, up from 19 percent just a decade ago.**

Jim Montoya, vice president of relationship development at the College Board, said the expanding Latino population was a factor, as well as greater outreach to get minority students to take the test. But there are others, too.

"It's a lot of little things," he said. For example, he said, the number of black students taking a solid core curriculum — a strong predictor of success on the test — has fallen from 69 percent to 66 percent over a decade.

The College Board, a membership organization that owns the exam and promotes college access, also released its first "College and Career Benchmark" report, which it said would eventually be used to help show states and school districts how well prepared their students are. Based on research at 100 colleges, it calculated that scoring 1550 or above on the three sections of the test indicated a 65-percent likelihood of attaining a B-minus or above average in the freshman year of college.

Overall, 43 percent of test-takers reached that benchmark.

The SAT and rival ACT exam are taken by roughly the same number of students each year. Most colleges require scores from at least one of the exams but will consider either. In recent years, some colleges have adopted test-optional policies allowing applicants to decline to submit test scores at all.

## BALTIMORE, MARYLAND CA. 1950

75% White, 23.8% African American

Source: "Alabaster cities: urban U.S. since 1950".  
John R. Short (2006). Syracuse University Press.  
p.142. ISBN 0815631057



Then

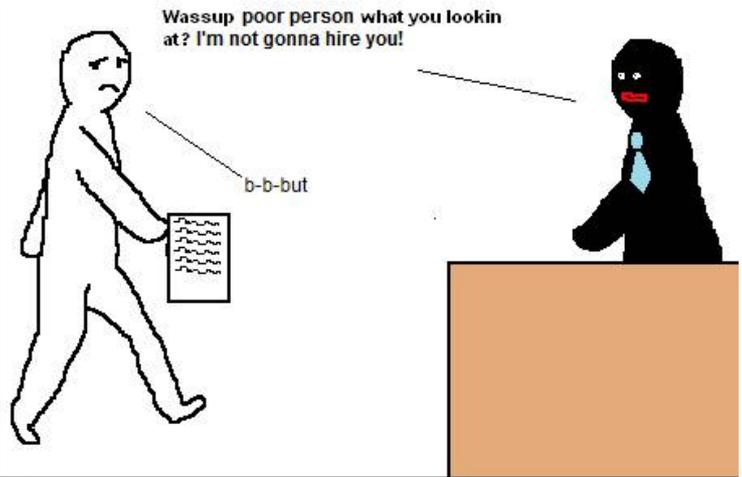
# Baltimore, Maryland ca. 2010

32.5% White, 64% African American

Source: [baltimorehealth.org/infor/HSR/BaltCityDemo.pdf](http://baltimorehealth.org/infor/HSR/BaltCityDemo.pdf)

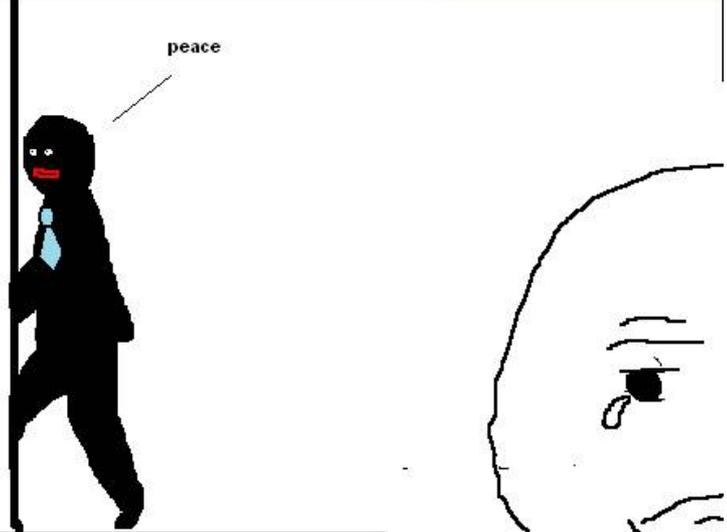


Now



Nah, I'm just kiddn with ya. You only got a degree in art history so you'll only qualify for entry level position, but you can come back Tuesday around noon for an interview.

oh.. uh sure, if that's all you got.. I'll make sure to be there...



LATER...



**/new/ - News**  
Text Boards: [/newnew/](#) & [/newpol/](#)

The One True Communist

This greedy fucking capitalist pig tried to make me into a wage slave the other day and I told them they can't buy me! I hate the richest 1% and all of their stupid libertarian followers there fucking corporate shills I just want to shoot them in their fucking greedy piglike faces when the revolution comes.

..... (Password used for file deletion)

KB, MP3, GIF, JPG, PNG

*It used to be that people helped each other, now it's only the government can help you... See the Jew...*

### **Schakowsky: Americans Don't Deserve to Keep All of Their Money**

September 14, 2011 – From: [wlsam.com](http://wlsam.com)

CHICAGO (WLS) – A lot of reaction Wednesday morning to Congresswoman Jan Schakowsky's interview with Don Wade and Roma.

Schakowsky said that Americans don't deserve to keep all of their money because we need taxes to support our society.

**"I'll put it this way. You don't deserve to keep all of it and it's not a question of deserving because what government is, is those things that we decide to do together. And there are many things that we decide to do together like have our national security. Like have police and fire. What about the people that work at the National Institute of Health who are looking for a cure for cancer," Schakowskysaid.**

Schakowsky also says one reason the 2009 stimulus bill did not succeed was because it was not large enough.

Schakowsky also admitted there are questions about the Obama administration's connection to the now bankrupt Solyndra solar panel company.

The administration approved nearly \$528 million in federal loans to the company, before Solyndra filed for bankruptcy.

Schakowsky sits on the House Energy and Commerce Committee Investigations and Oversight Panel, which is holding hearings Wednesday into the matter. She said she and other Democrats want answers.

"You know, it certainly doesn't sound good. The Democrats are not going to shrink from actually, you know, from any kind of full investigation of that. If there is a problem we're certainly going to support the efforts to get to the bottom of this," Schakowsky said.

Schakowsky did say that even though public money was involved, the Solyndra controversy does not compare to the damage the Enron energy scandal inflicted on the U.S. economy.

Also in the interview, Schakowsky talked about the victory of Republican Bob Turner, in the Tuesday special election to replace ex-Congressman Anthony Weiner. Turner, who is Catholic, won in a district that is heavily Democratic and heavily Jewish, defeating an Orthodox Jewish Democrat.

Schakowsky, who is Jewish, denounced former New York Mayor Ed Koch, for getting involved in the race and criticizing President Obama's record on Israel.

"I thought it was really shameful in talking about Barack Obama as not good on Israel. He has provided more security for the state of Israel than any other president," Schakowsky said.

# THE MEDIA'S GUIDE TO PROTESTORS

