
Terrorists Win
Ace! Totally Dubbed killed the entire enemy team.
$4950
Killer Hz

Cyber Mercenary
30+ years



CISO / Co-Founder

SIEMonster

DEFCON 23



I WILL KILL YOU

DEFCON 24



HOW TO OVERTHROW A GOVERNMENT

Where have all the good Terrorists gone ?













GLOBAL TERRORISM INDEX 2022

MEASURING THE IMPACT OF TERRORISM



2022 National Intelligence report had Terrorism as

1. China
2. Russia
3. Iran
4. .
5. Health and Security
6. Climate Change
7. .
8. .
9. .

Footnote: Terrorism

2016 National Intelligence report had Terrorism at #1 as the world biggest risk.

Deaths from Terrorism down 89% (MENA) in the last 3 years.

Terrorists Attacks in the West down 68% since 2018.

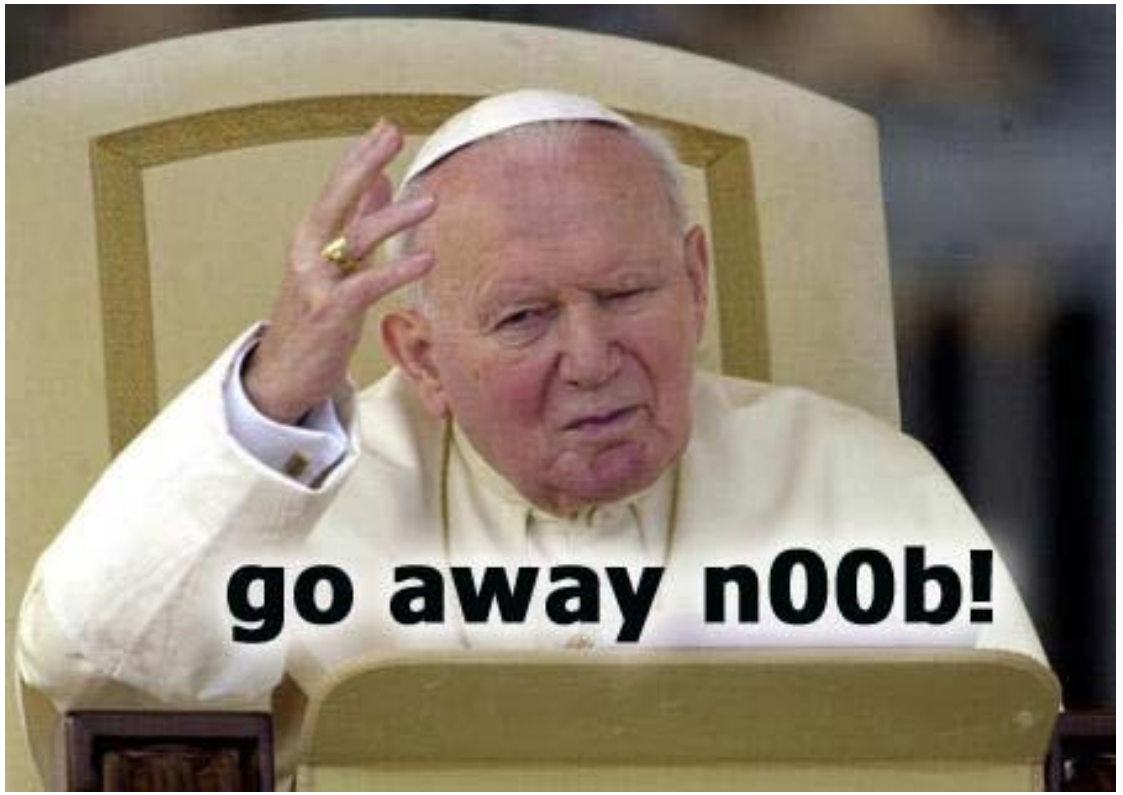


Priest Installs Cellphone Jammer in Church to Decrease Interruptions During Mass

December 22, 2014 Item Media

EMC, EMI, News





Vatican installs jammers to the Sistine Chapel to protect next Pope announcement.


EMBAJADA
LANDON
PLACE

THE TIMES

MONDAY JUNE 27 2022

Thieves using 'jammers' to block alarms

Rise in burglars with high-tech devices which disrupt intruder alerts and phone signals during break-ins

MONITORED ALARM systems installed in homes, shops and businesses are being "blocked" by organised crime gangs using electronic devices.

The devices, known as GSM jammers, emit a powerful signal that blocks intruder alerts sent by alarm systems to monitoring stations.

Jammers











3G
4G LTE
WiFi
GPS
LO JACK
UHF
433 MHz

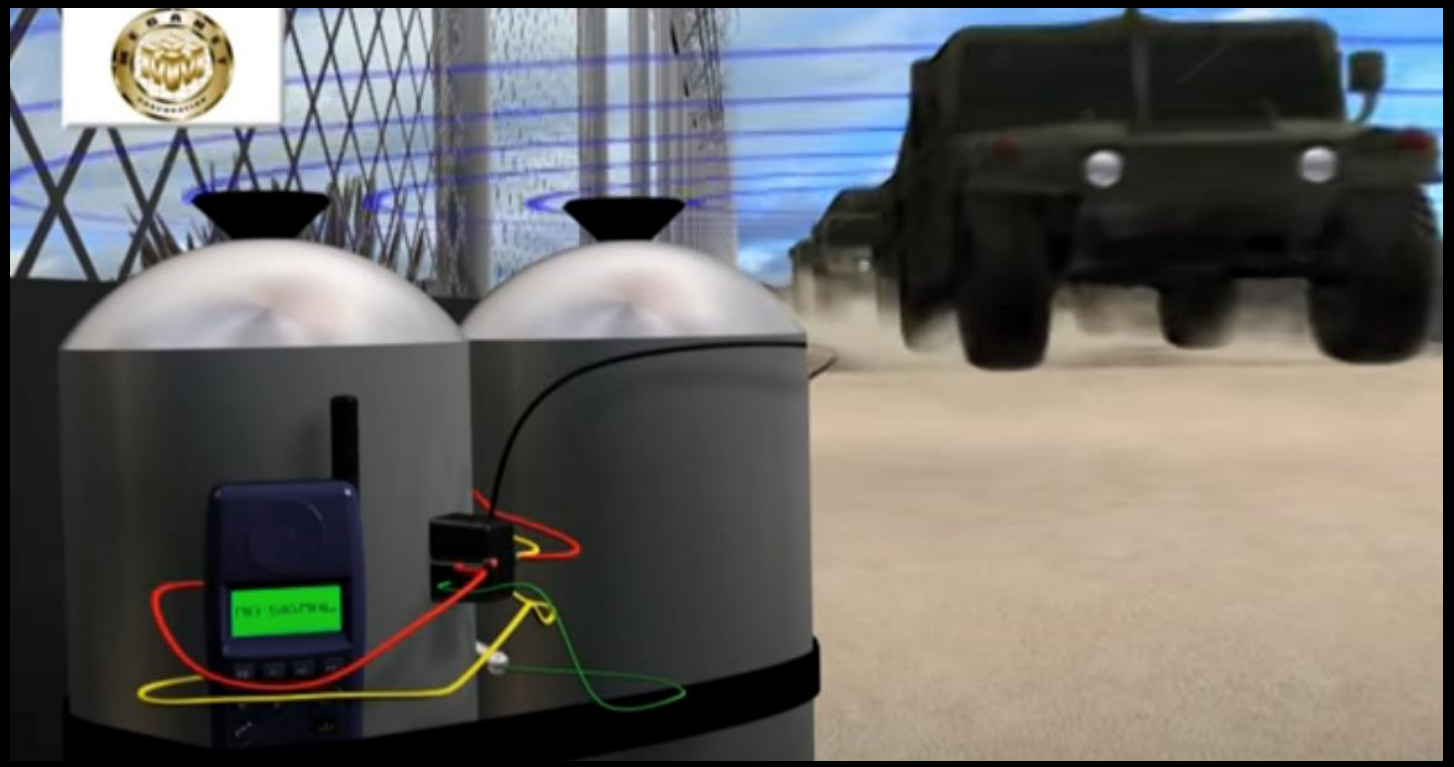




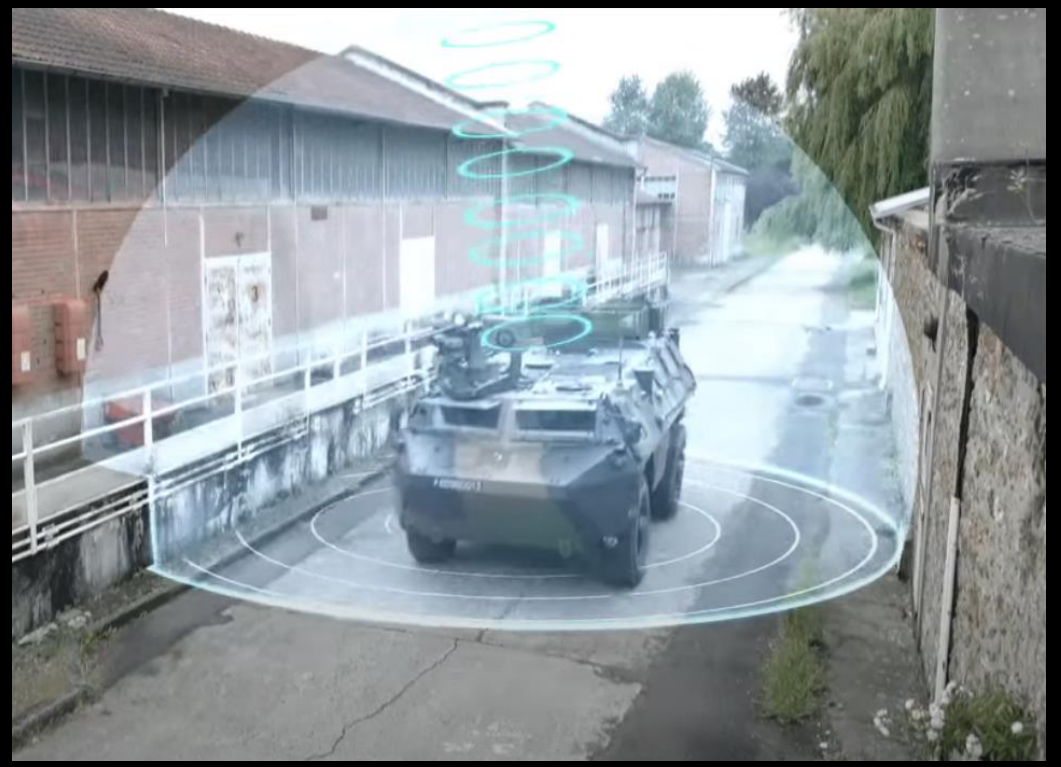




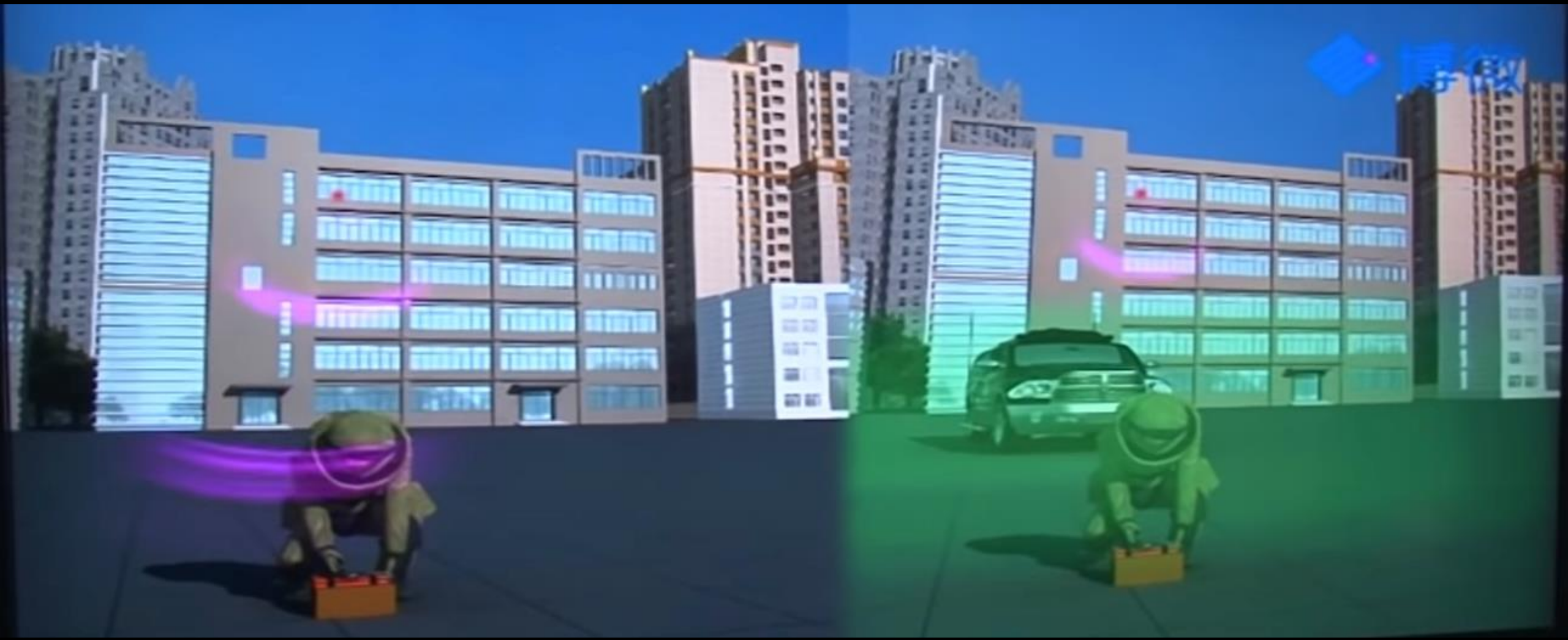
Humvee Jammer



Thales Eclipse



Jammer Protection



Manufacturers









Counter IED market is a 2-billion-dollar Industry

USMC Counter Radio-Controlled Impro
Electronic Warfare (CREW) 3.1 Thor III

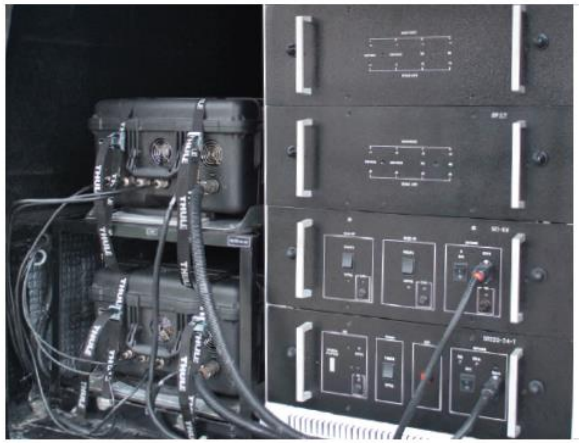
System Characteristics:

TAMCN:	A0326
NSN:	5865-01-580-4854
Technology:	Digital
Spectrum:	Classified
Orientation:	Adjustable position for Antennas
Mobility:	Man portable / Dismounted CREW
Power:	18 to 32VDC, 2.5A maximum (Low) 18 to 32VDC, 4.5A maximum (Mid) 18 to 32VDC, 5.0A maximum (High)
Distance:	Classified
Operational Mode:	Standby – System is idle, no scanning or jamming Operate – System is scanning and jamming as programmed.
Encryption:	N/A
Quantity Fielded:	0
AAO:	823 systems + spares (Pending SON) 336 systems (Original AAO) + 50 Spares per SONs



Military grade jammers

MCSV-3500W High power convoy jammer with communication windows setting



FEATURES:

- Over 1000W power at antenna output
- Independent 13 main channels covering 20-3500 MHz with 650W
- Additional 6 channels for cellular bands of total 358W
- 38 communication windows programming ability
- AC mains or vehicle power supply
- Suppression of entire bands without gaps
- Modular system allows customization on request

The MVCS-3500W jamming system is the military grade solution that can be used as stationary or convoy protection unit with ability of programming communication windows and channels on/off settings.

The MCSV-3500W provides minimum continuous wave signal of 1008W power on antenna output. The jamming range in between 20-3500 MHz is divided without any gap by 13 main channels and 6 additional channels especially for cellular communication frequency bands.

An operator can program up to 38 frequency windows within 13 main channels. The windows quantity and width depend on the channel.

The delivery set includes antennas for the whole frequency range. The power supplied via 22-30V on-board network. The power consumption is not more than 5kW. TThe MCSV-3500W can be stationary installed and connected to the 380V AC mains.

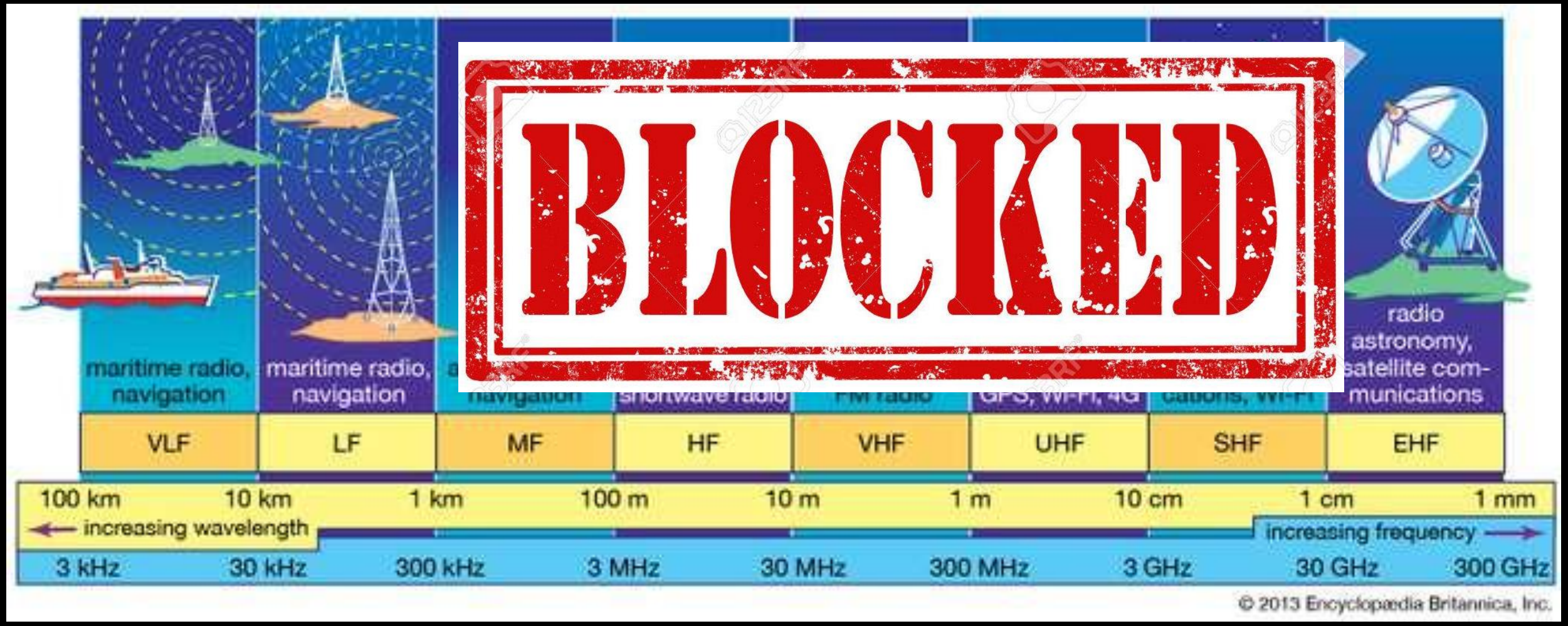
The device employs the maintenance control algorithm that activates the alarm in case of any operation failure or wire disconnection will automatically turn off the amplifier.

The delivery set includes all the antennas and installation kit. The manufacturer's team can install the jammer on the customer request.

PRODUCT SPECIFICATIONS

Operating frequency bands / Min output power	Total coverage of 20-3500 MHz by divided 19 channels					
	Ch1	20-60 MHz	60W	**Ch11**	1700-2000 MHz	50W
	Ch2	60-130 MHz	60W	**Ch12**	2000-2700 MHz	15W
	Ch3	130-180 MHz	100W	**Ch13**	2700-3500 MHz	15W
	Ch4	180-250 MHz	60W	**Ch14**	791-894 MHz	100W
	Ch5	250-400 MHz	100W	**Ch15**	925-960 MHz	100W
	Ch6	400-500 MHz	100W	**Ch16**	1805-1880 MHz	60W
	Ch7	500-750 MHz	40W	**Ch17**	2110-2170 MHz	60W
	Ch8	750-1000 MHz	50W	**Ch18**	2400-2500 MHz	25W
	Ch9	1000-1400 MHz	50W	**Ch19**	2500-2700 MHZ	13W
	Ch10	1400-1700 MHz	50W			
Total output power	1008W					

Jammers



20MHz – 6500 MHz

IED Overview



Precursor Chemicals

(e.g., Fireworks, Black Powder)

Explosive Materials

Container

Shrapnel

Switch

Power Source

Initiator

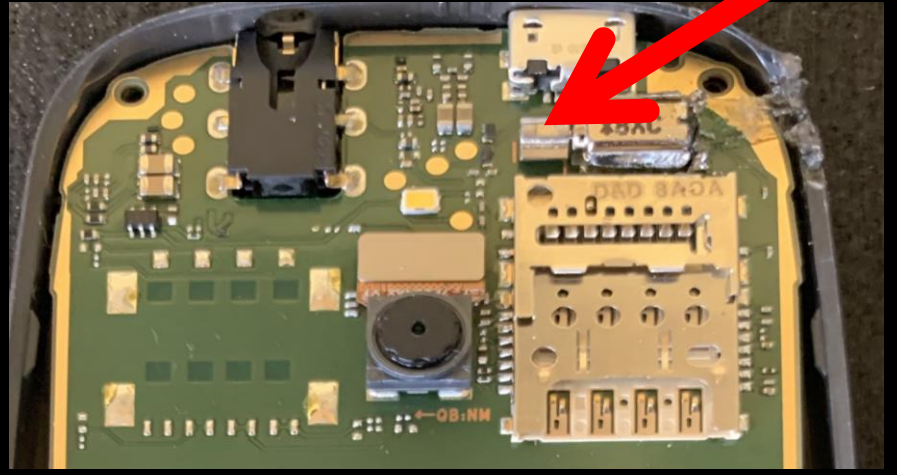
Booster

Main Charge

Improvised Explosive Device

SWITCH

- Firing Switch
- Arming Switch
- Command
- Time
- Victim Operated







Command

- Command Wire
  - Push Button
  - Rocker Switch
  - Relay Board + Rocker Switch
  - Push Button + Dead Man Switch
- Pull
  - Clothes Pin
  - Motorcycle Brake Switch
- Radio Controlled
  - With DTMF
    - Consumer Electronics
      - JDQBA
      - RC Toy
      - Garage Door Opener
      - Door Bell
    - Hand Held Radio
      - PMR
      - ICOM
    - Non-Hand Held Radio
      - Taxi Radio
      - Trunk Mount Radio
    - Cordless Phone
      - LRCT
      - HPCP
    - Mobile Phone
      - GSM
      - CDMA
    - Custom RC
      - WICR
      - MOD 1-5
    - Telemetry
      - Lynx
      - Maxstream
- Optical
- Active Infrared
- Command Projectile
  - Plate
    - 2 Thick Copper Plates
  - Membrane
    - Pie Tins

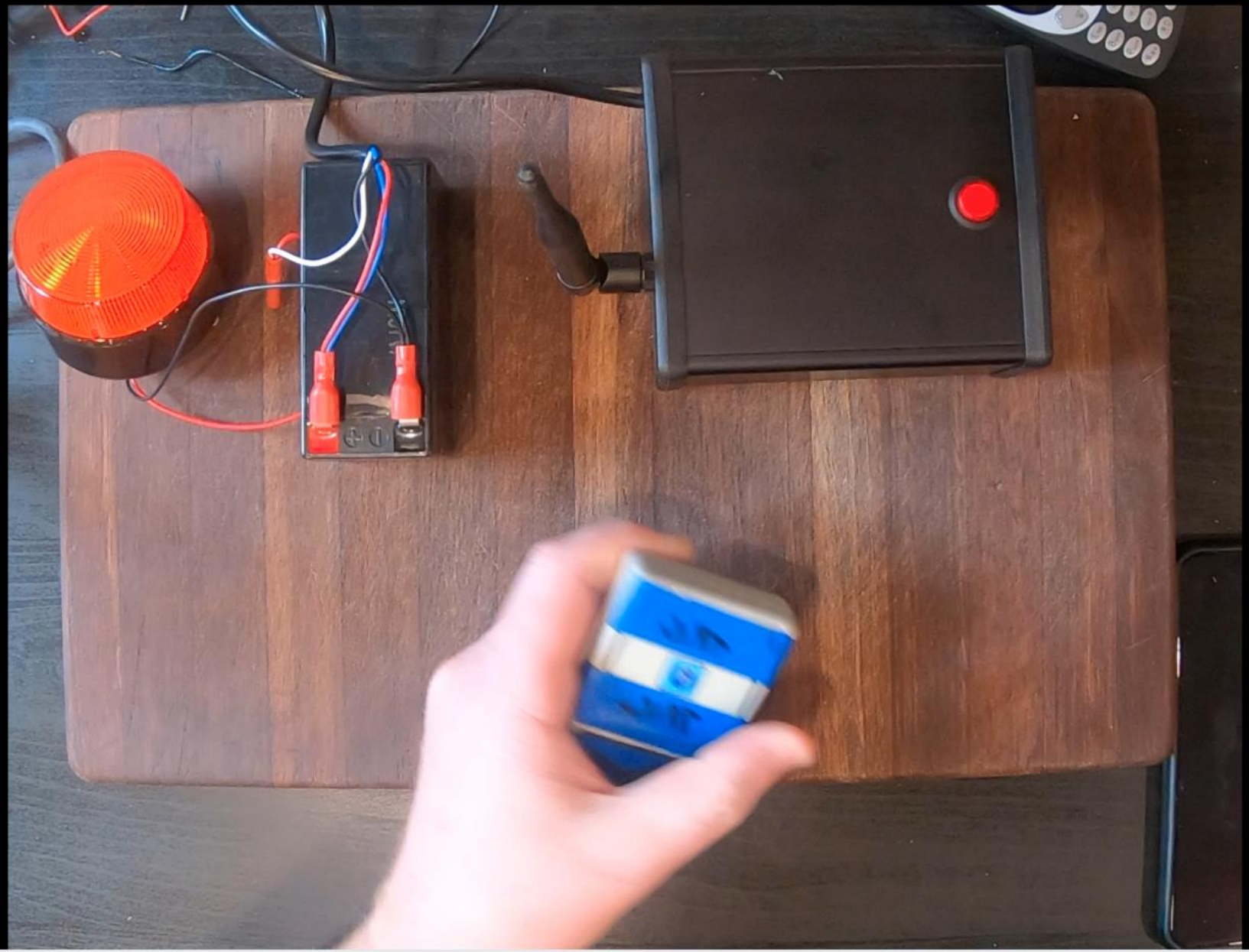
EXAMPLES (Not All Inclusive)



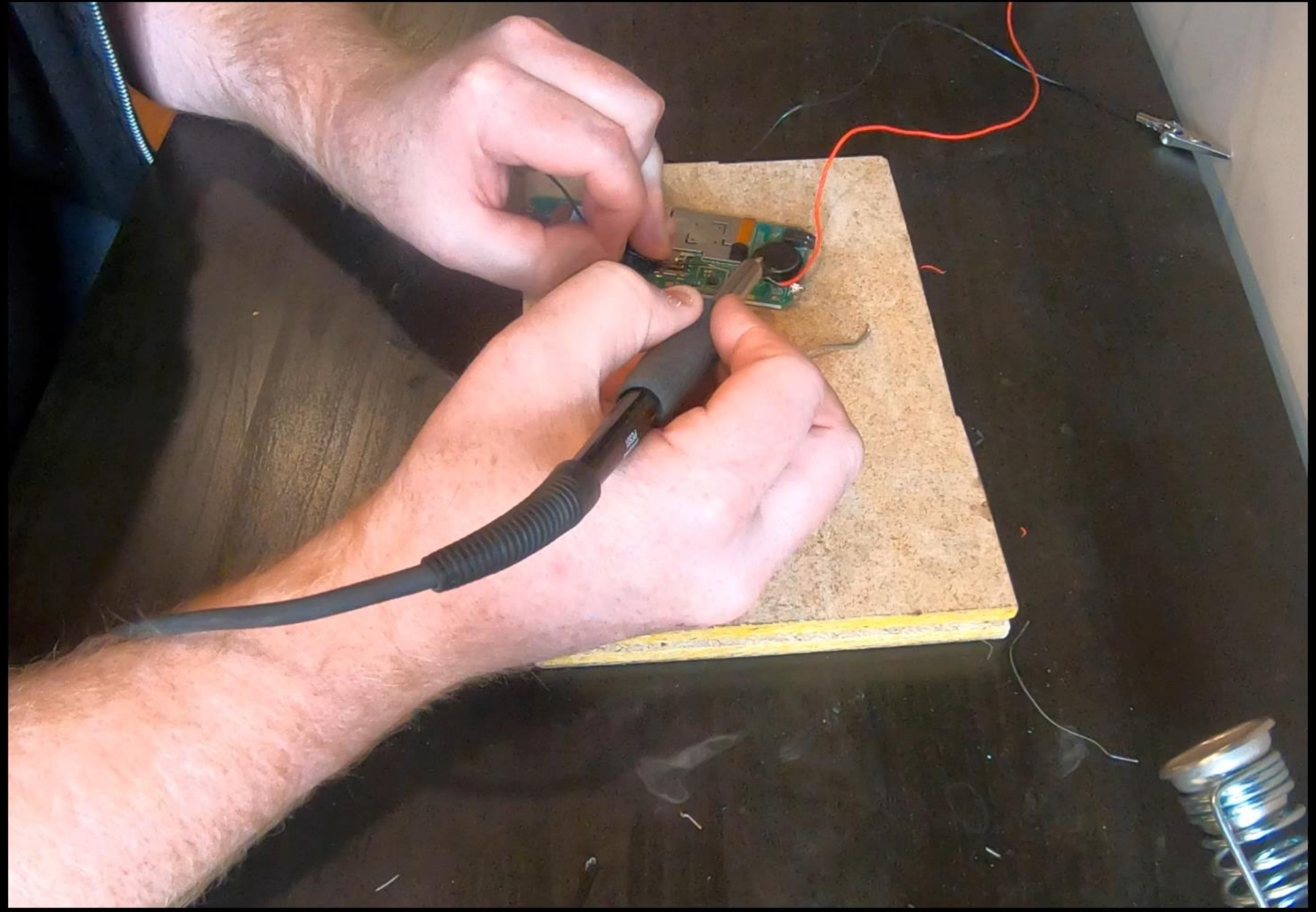








Garage door opener : Frequency 433 MHz

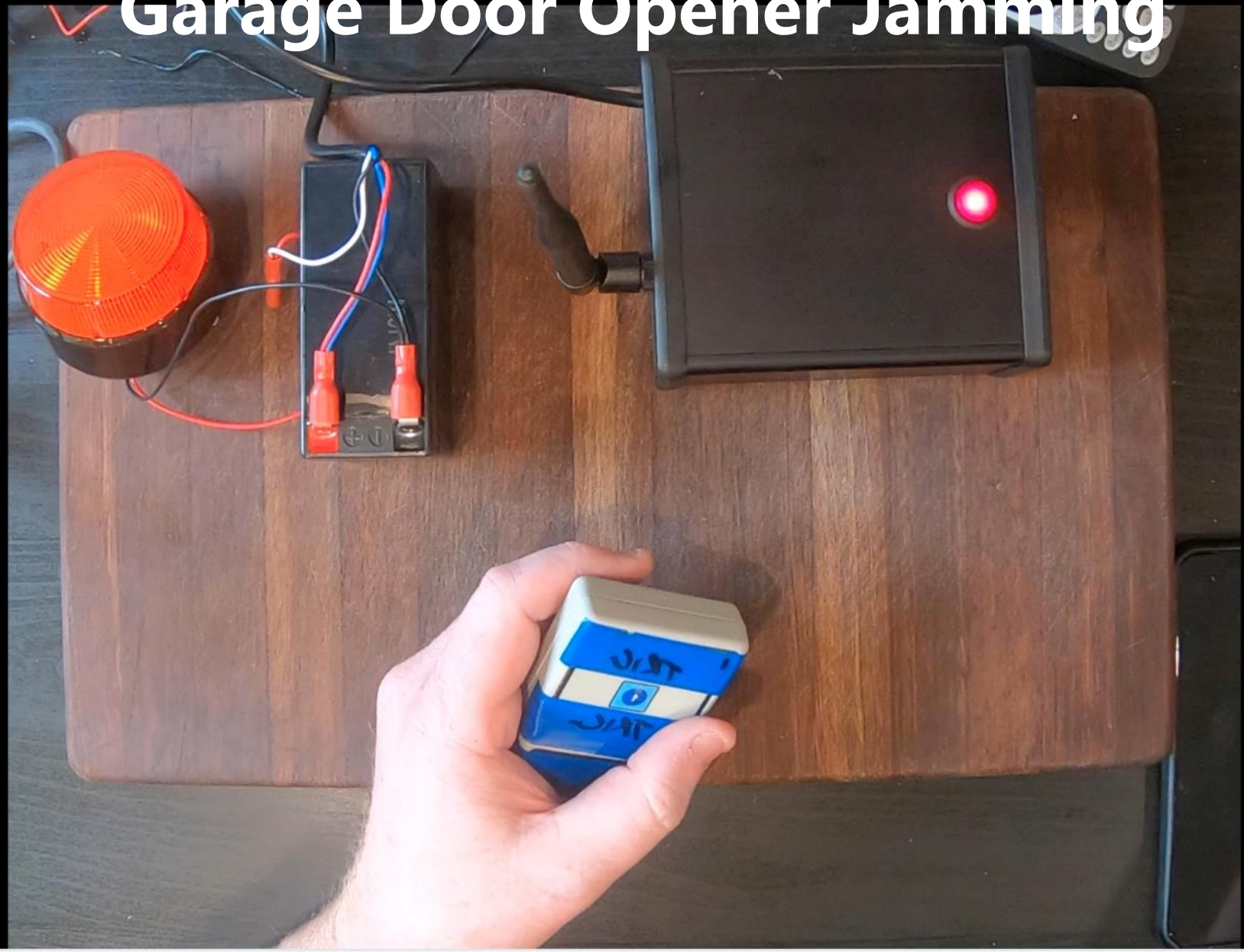


Cell Phone Switch Speaker-Vibrator Soldering



Remote Control IED (RCIED) Electronic Counter Measures (ECM)

Garage Door Opener Jamming



12 Channel Jammer Blocking GSM, Wifi, Bluetooth, 433 MHz and others.


Cell Jamming
Cell Providers
WI-FI/GSM
Terrorists Win
3:02
Mobile Phone: Wifi, 4G, 3G

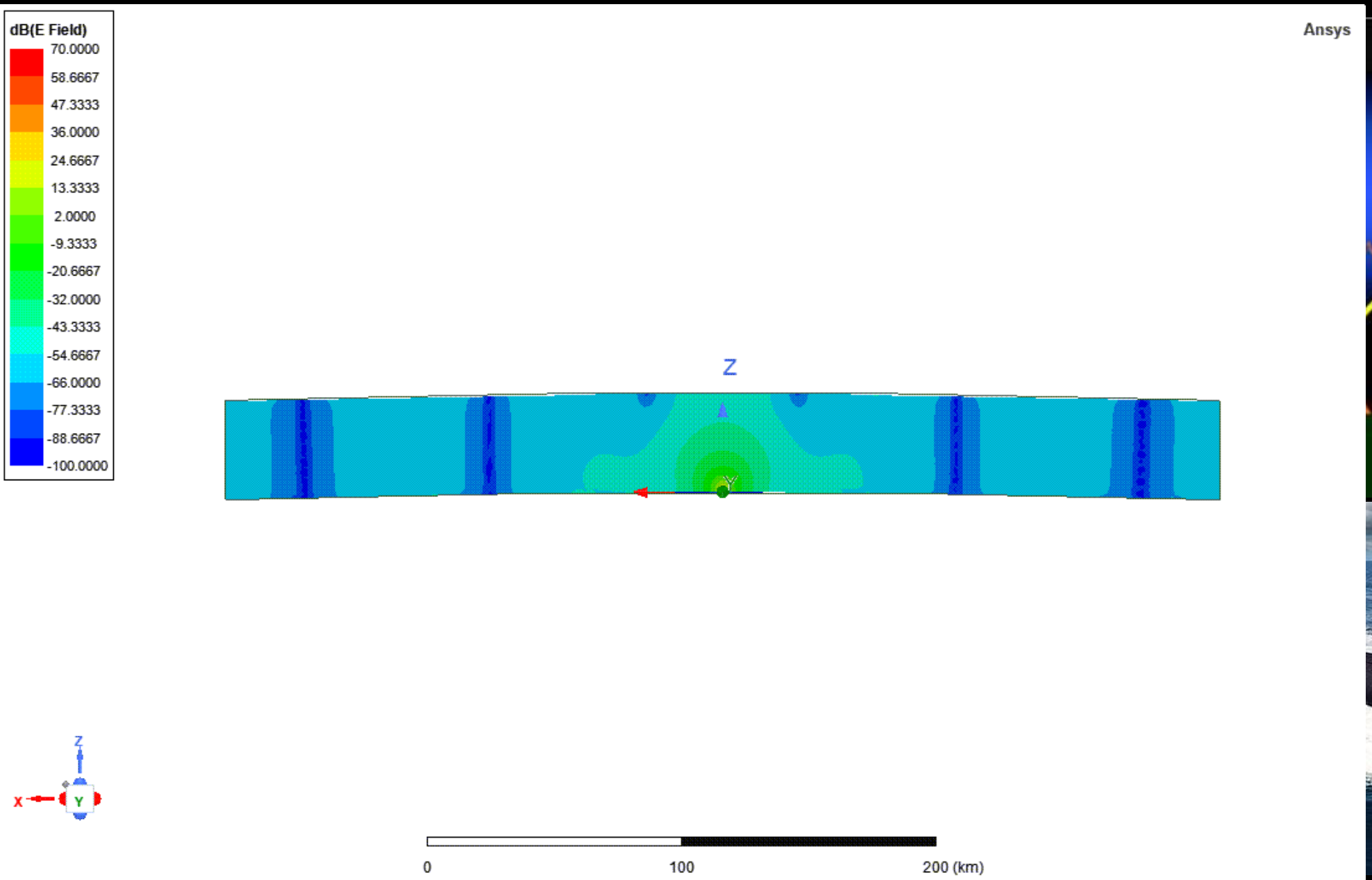


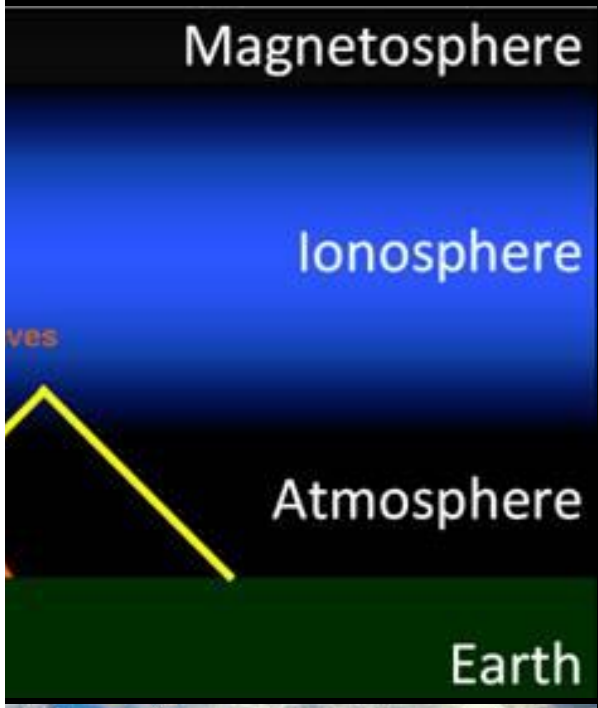
Jammer Gaps ?

Name	Symbol	Frequency Range	Wavelength
Extremely Low Frequency	ELF	3 Hz - 30 Hz	10,000 km – 100,000 km
Super Low Frequency	SLF	30 Hz - 300 Hz	1,000 km – 10,000 km
Ultra Low Frequency	ULF	300 Hz - 3 kHz	100 km – 1,000 km
Very Low Frequency	VLF	3 kHz - 30 kHz	10 km – 100 km
Low Frequency	LF or LW	30 kHz - 300 kHz	1 km – 10 km



VLF / ULF / ELF Military







Ultra Low Frequency (ULF)

Range: 300 Hz – 3 kHz

Wavelength = 1000 to 100km

2 kHz = Wavelength is 150Km

Antenna Requirements 2 kHz

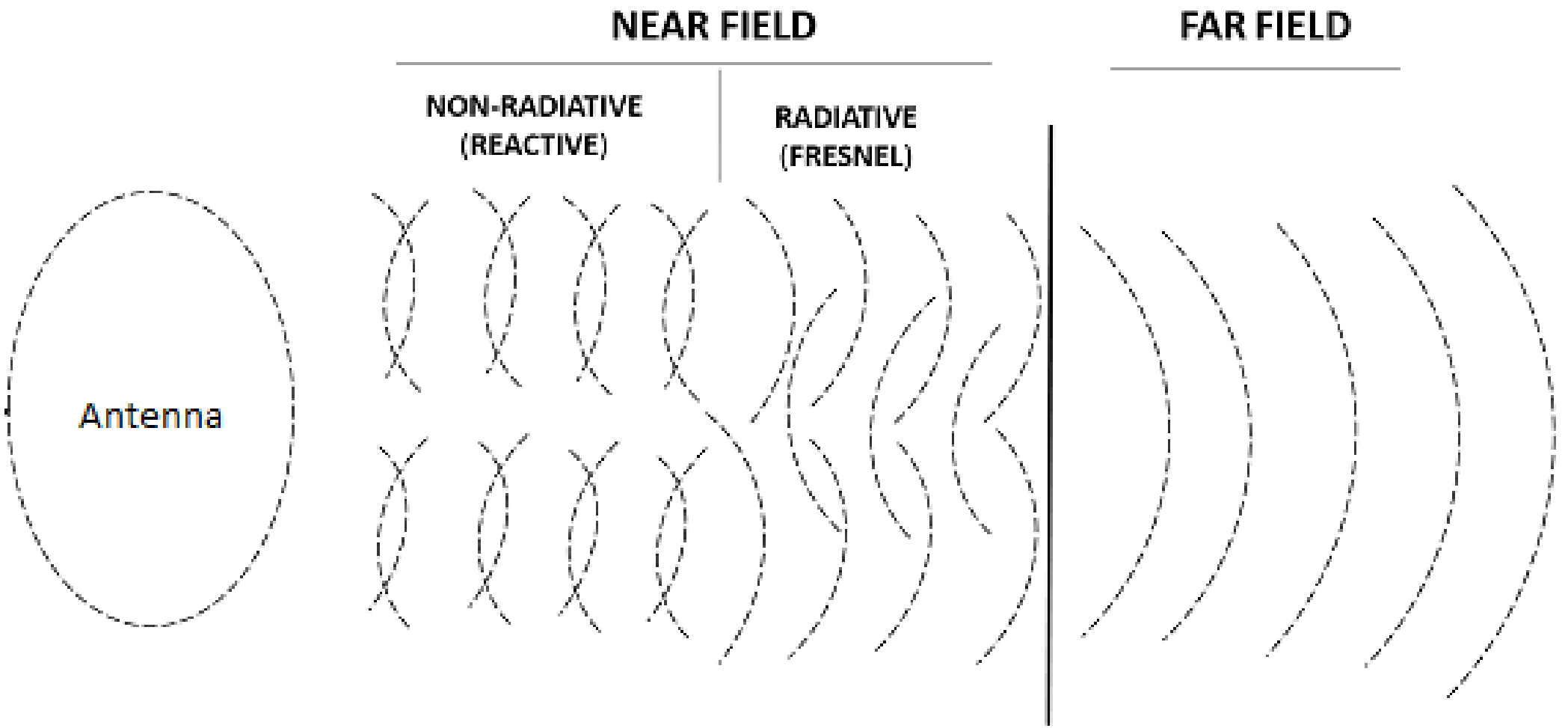
- ½ Wavelength = 75km

Travels through the Earth and Sea Water

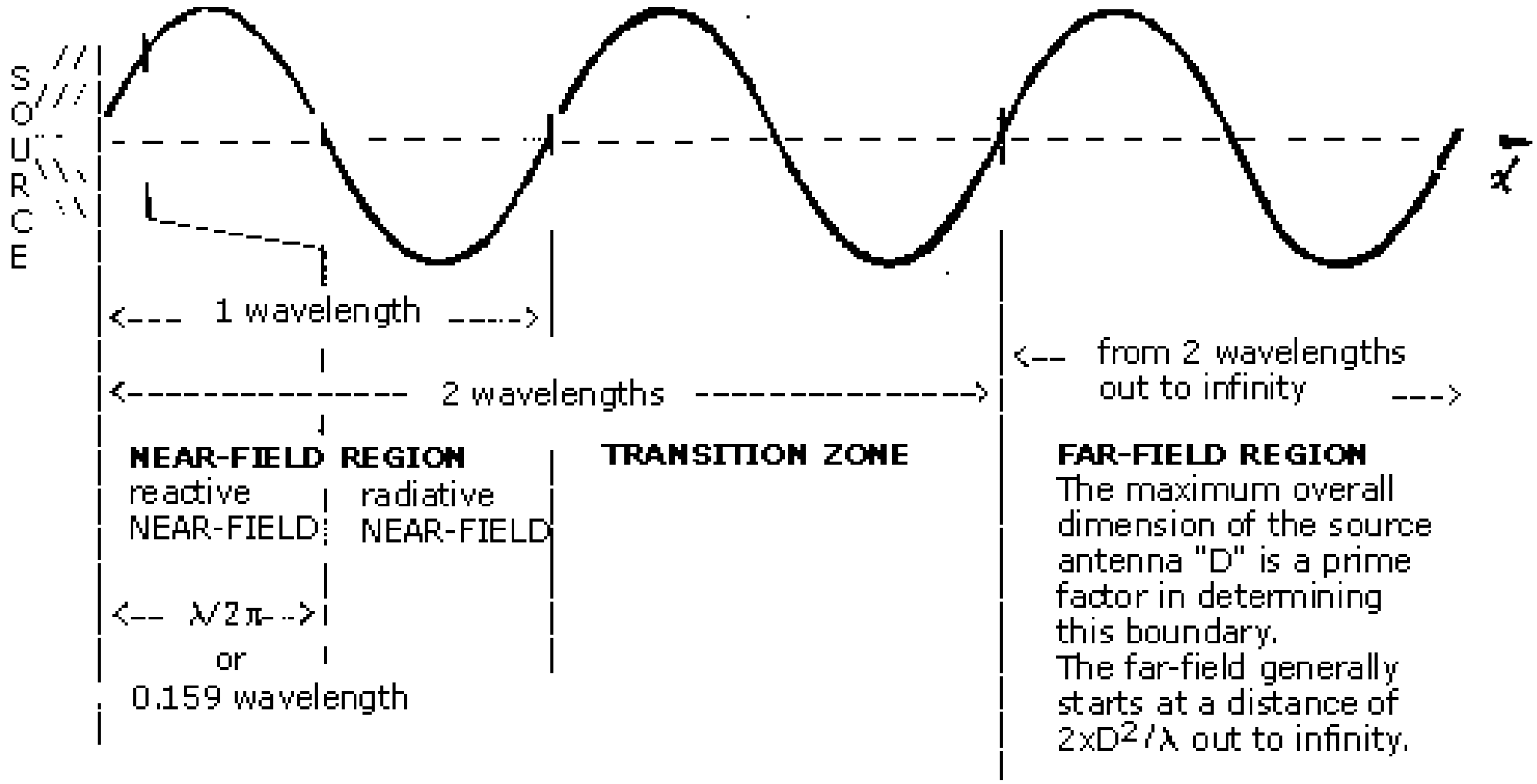
Near Field vs Far Field



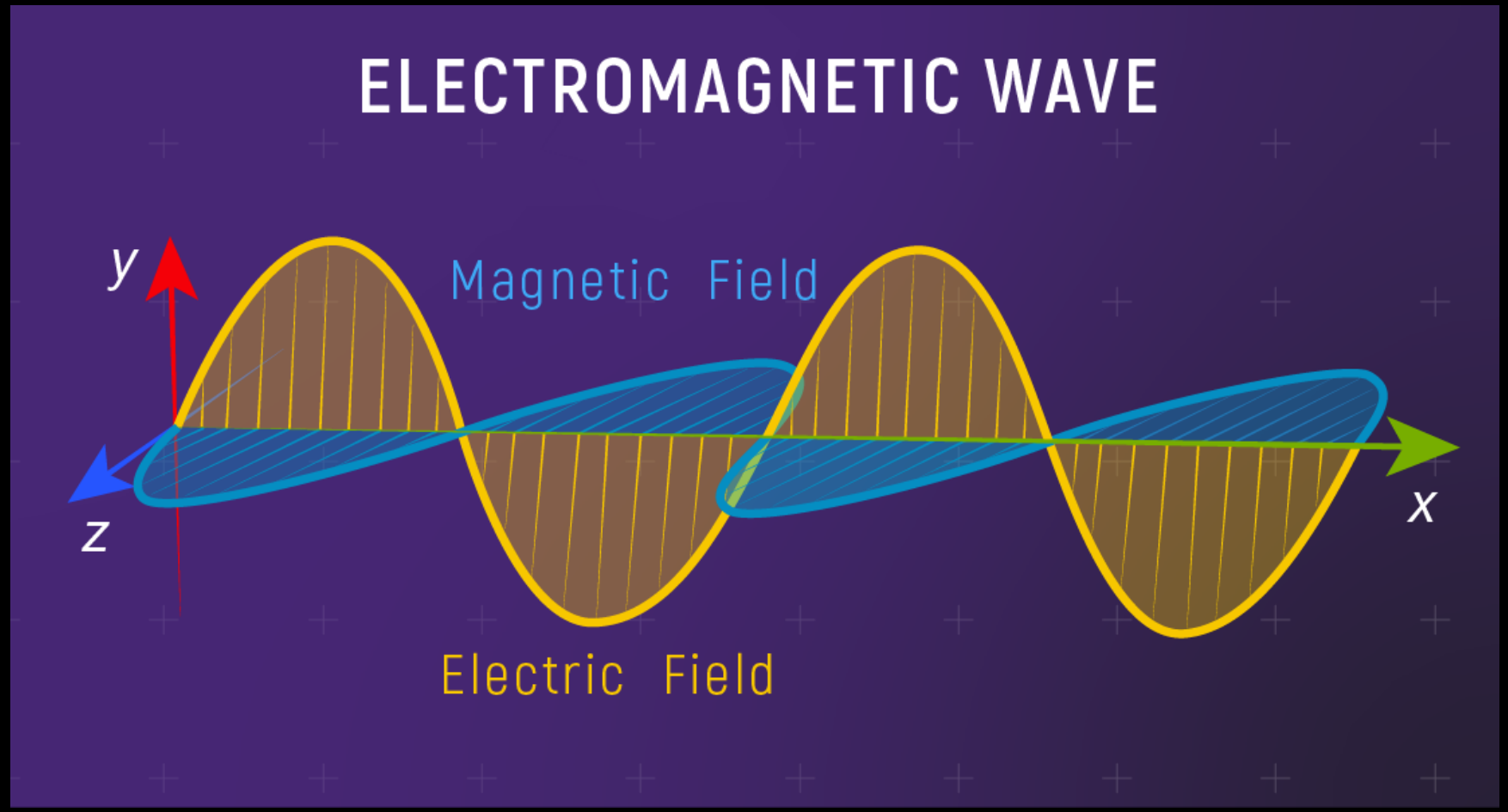
Near Field vs Far Field

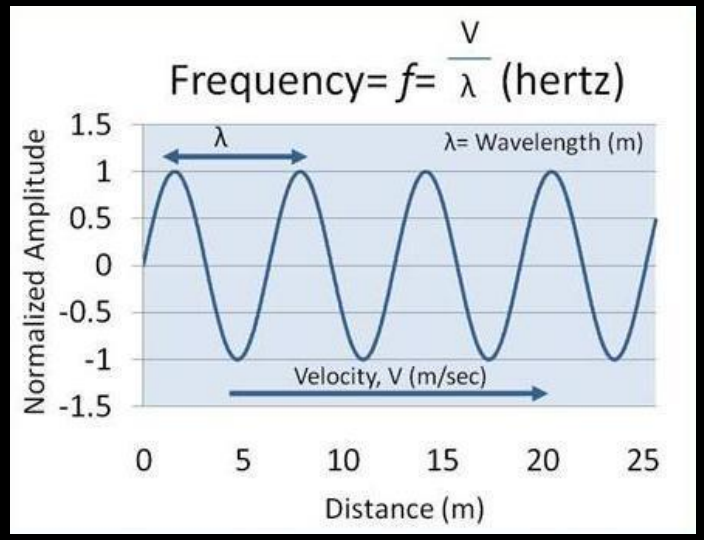


Near Field & Far Field Concept



Radio Waves – Far Field



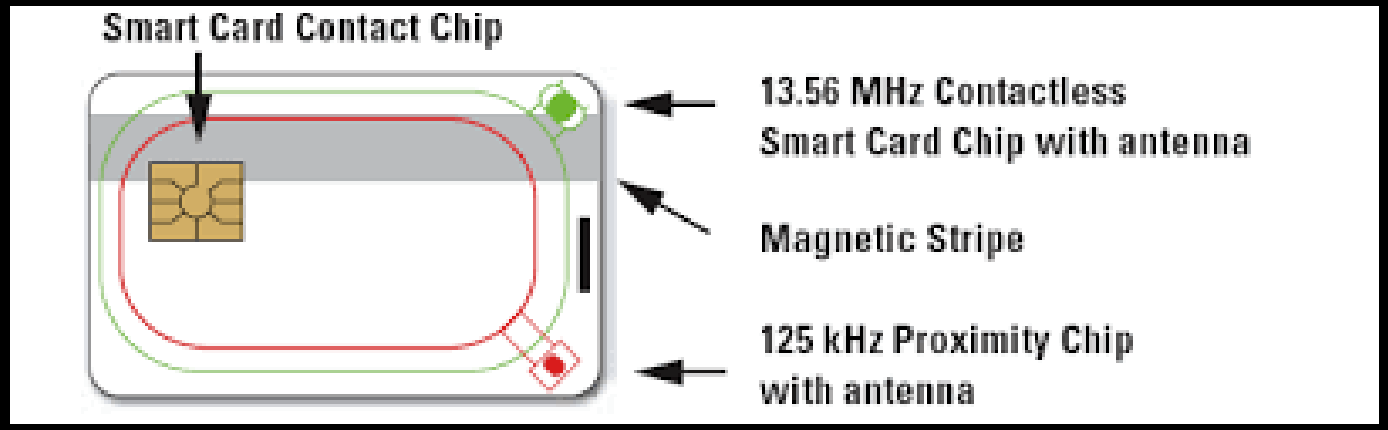


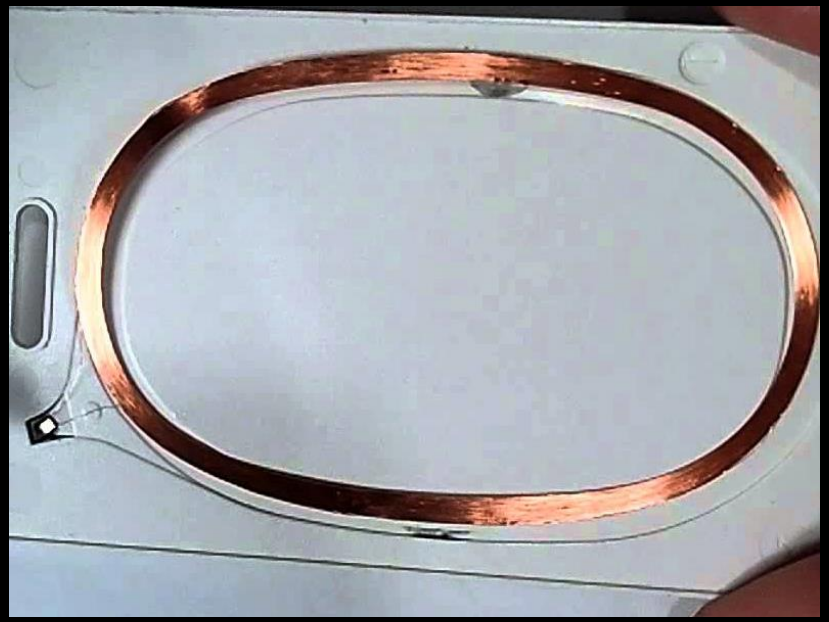
Wavelength = Distance a wave take to complete a cycle.

Frequency = How many repeating wave cycles per second.


CREDIT CARD



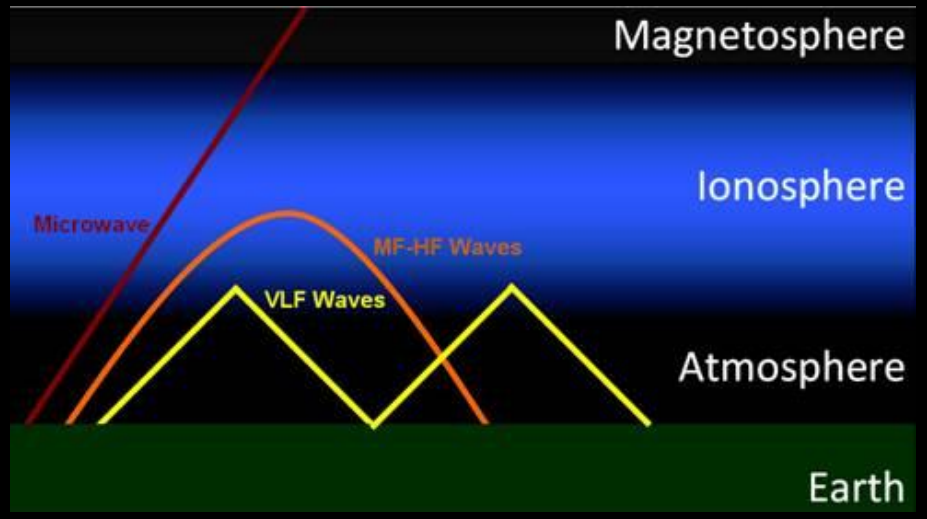

Smart Card Contact Chip
13.56 MHz Contactless
Smart Card Chip with antenna
Magnetic Stripe
125 kHz Proximity Chip
with antenna



NFC Range



13.56 MHz
Wavelength : 22.11 Meters
Near Field Range: 1-5 cm



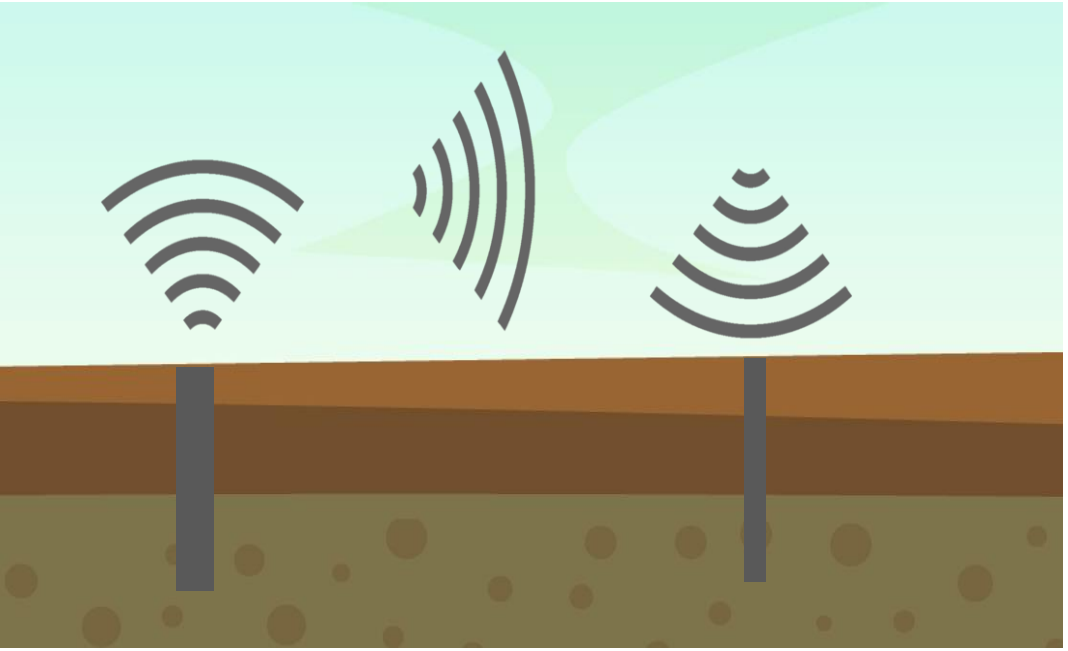
2 kHz
Wavelength : 150 kilometers
Near Field Range: 75 kilometers

How do we create a VLF/ULF Wavelength

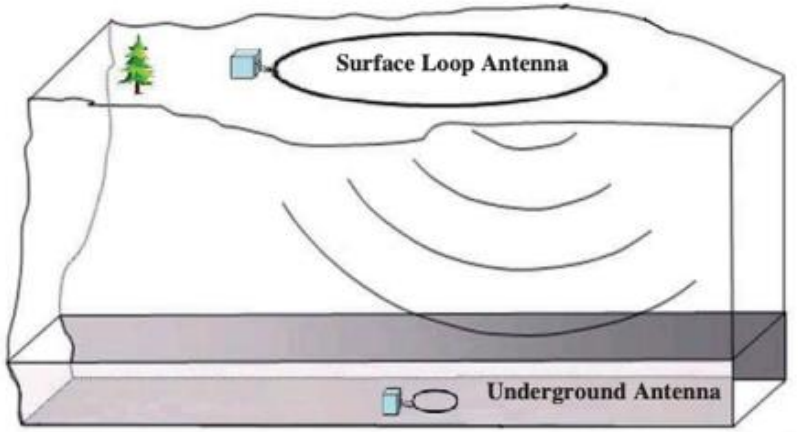
without the massive antenna?

VLF / ULF – Earth Mode

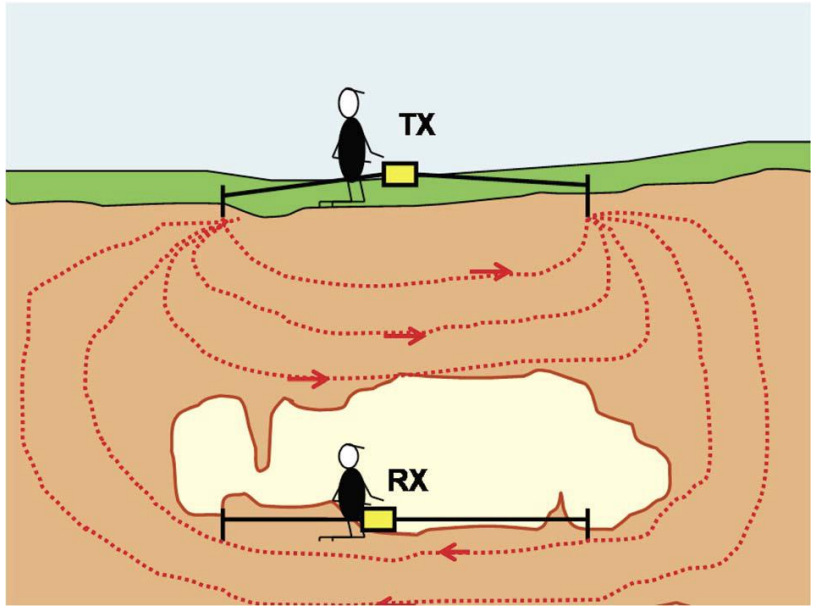
Earth Mode Methods



Earth Current Communication (up – over and down)



Deep Strata – Mining Comms PED



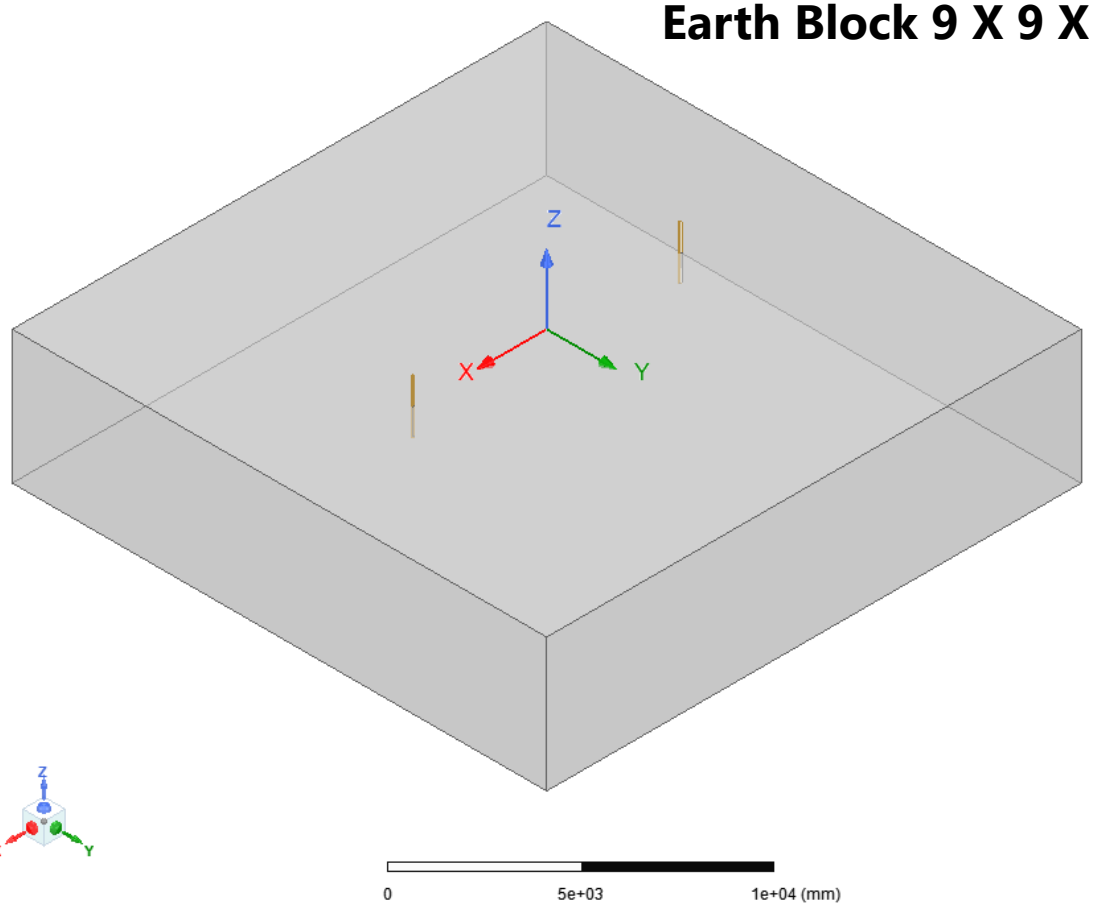
Conduction Current Mode

Simulations

Software Tools

- ANSYS HFSS 3D Electromagnetic Simulation Software
- RES2Mod
- CST Studio (3D EM analysis & Design)

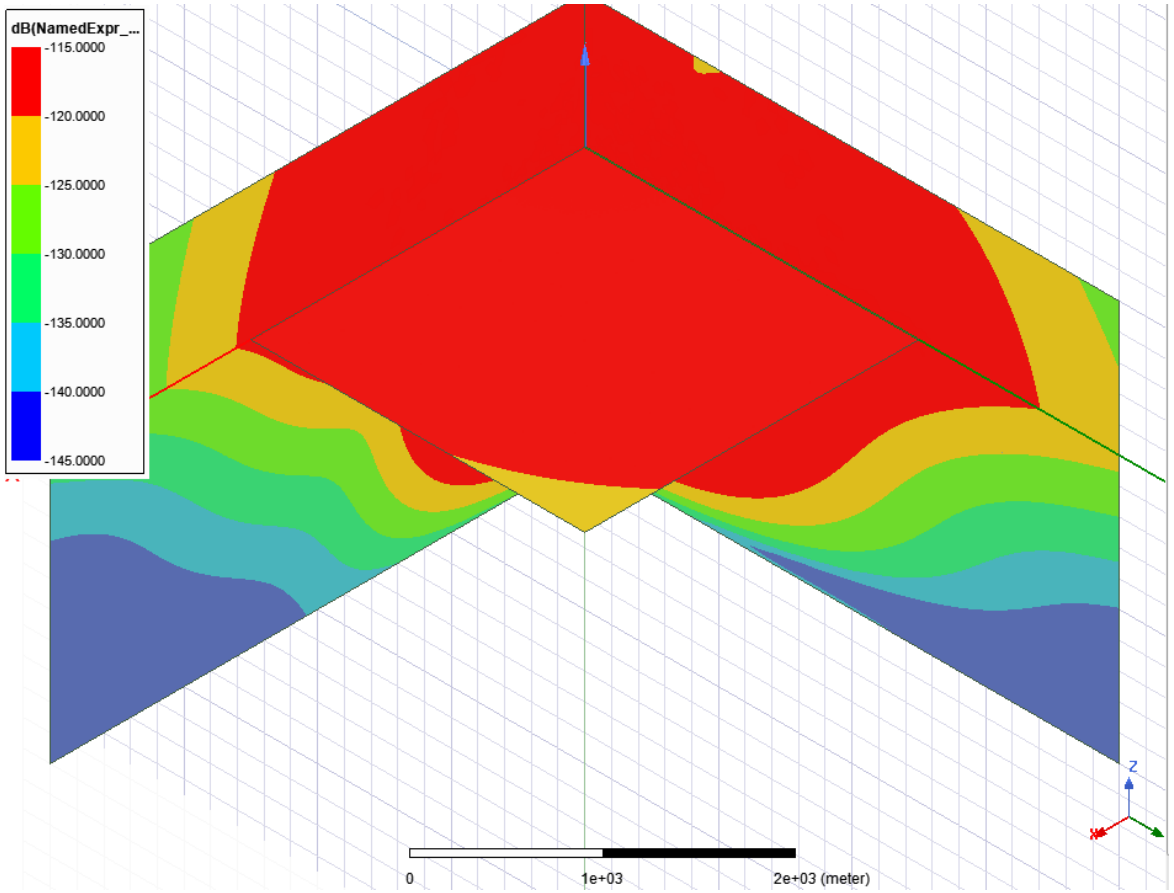
Earth Block 9 X 9 X 2 Km

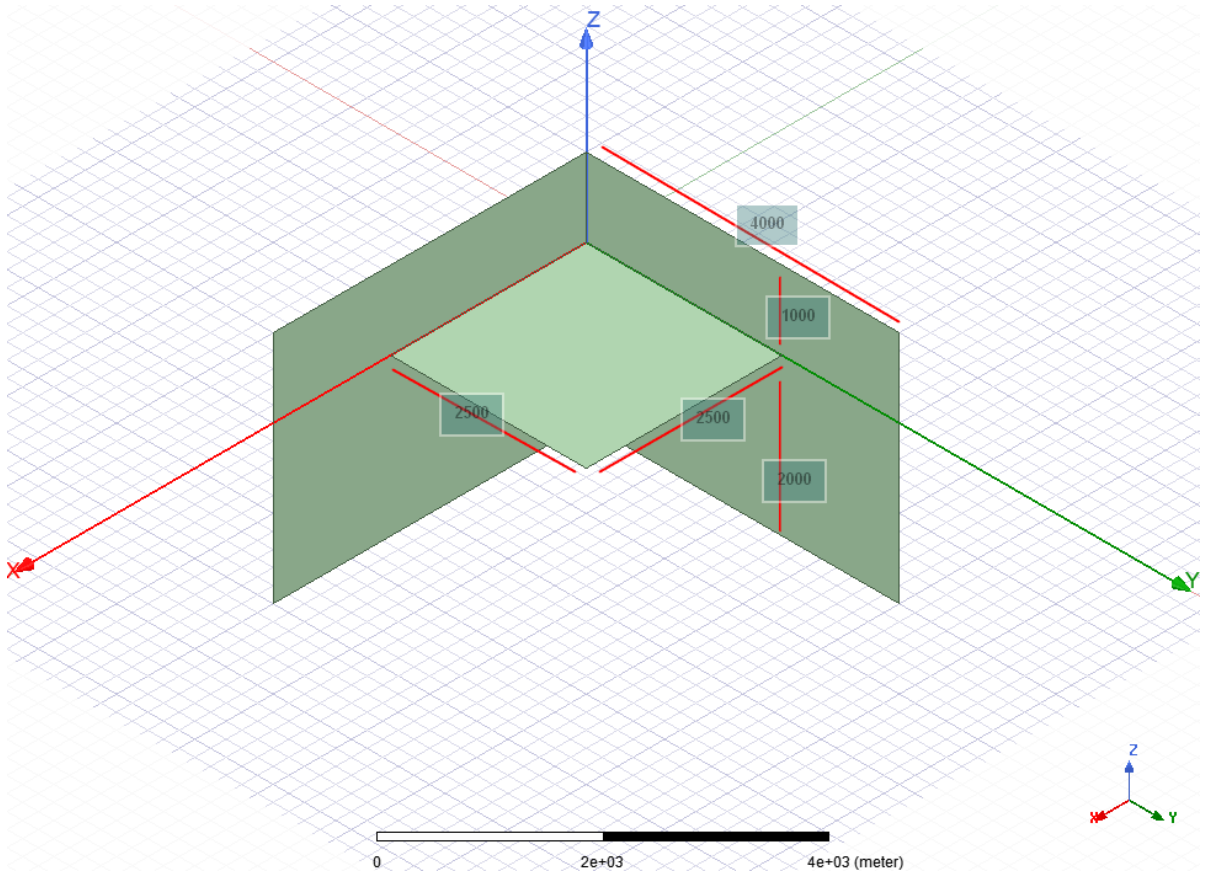


Simulation Values

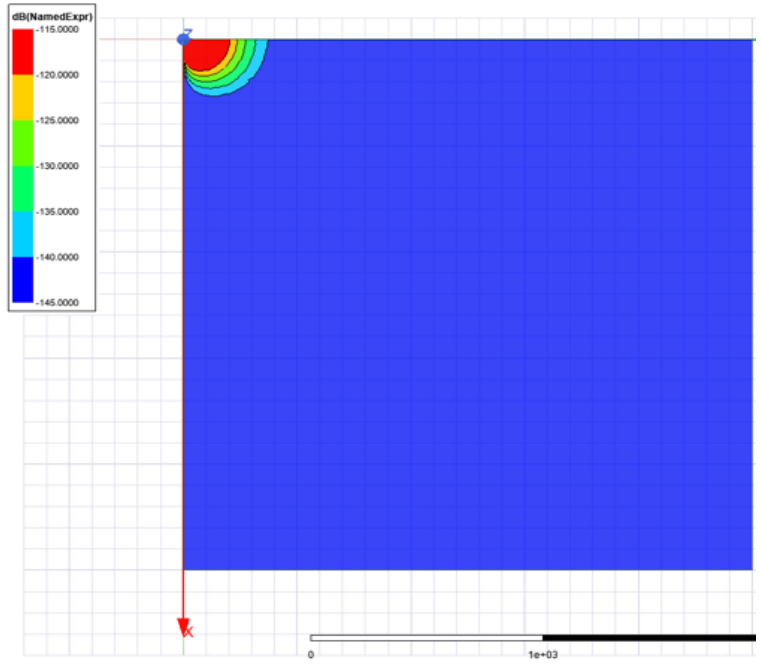
TX Electrodes: Metal 200 X 6 X 6 cm^3 1 meter deep
Conductivity: ~0.01 S/m (wet soil)

Earth mode

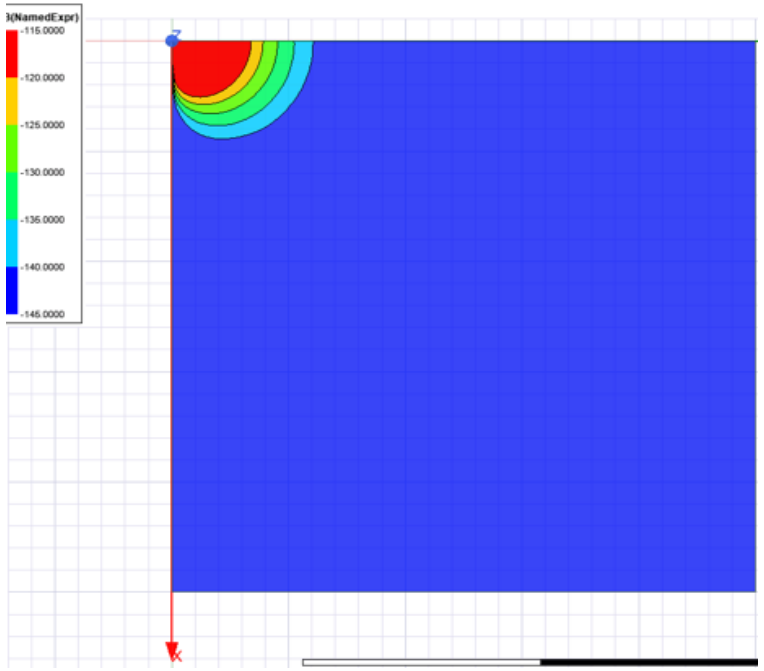

dB(NamedExpr_...
-115.0000
-120.0000
-125.0000
-130.0000
-135.0000
-140.0000
-145.0000
Z
0
1e+03
2e+03 (meter)


Z
4000
1000
2500
2500
2000
X
Y
Z
Y
0
2e+03
4e+03 (meter)

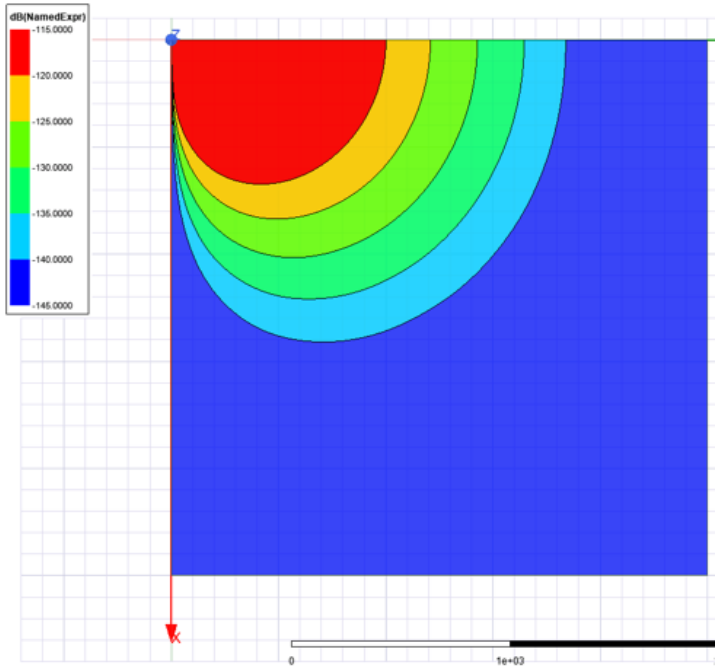
TX Transmission Simulations



Simulation 1: 73 kHz



Simulation 2: 9kHz



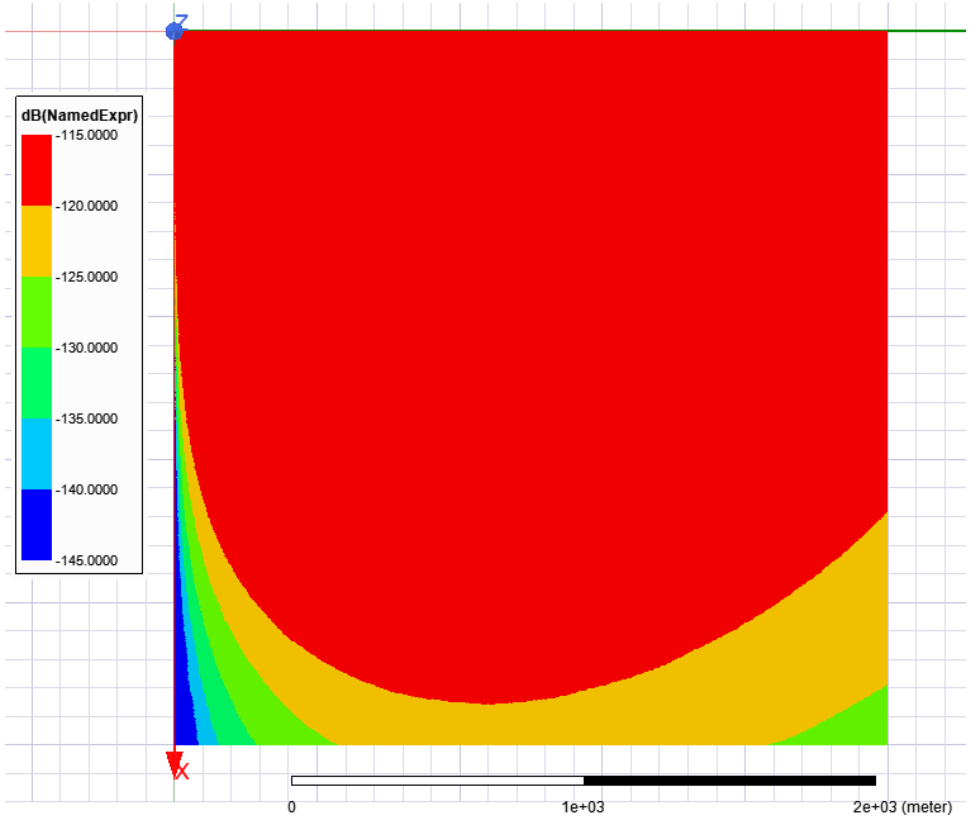
Simulation 3: 0.1 kHz

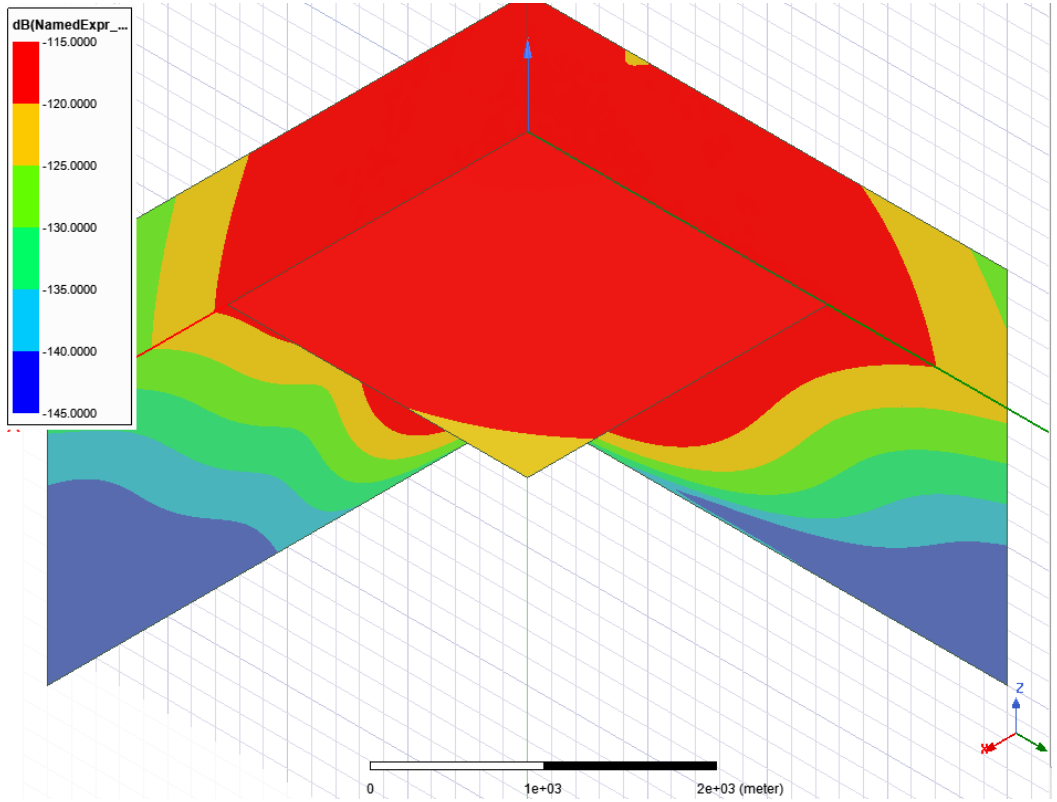
TX Electrodes separation ~10m
Injected power ~ 1A
Distance scale 100m/div.

Initial Random Frequency Results

Frequency (kilohertz)	Electrode Separation (Metres)	Injected Power (Watts)	Operational Range (Metres)
0.1	~ 10	~ 3600	~ 1900-2400
0.1	~ 10	~ 1800	~ 1800-2200
0.1	~ 20	~ 3600	~ 2600-3200
0.1	~ 20	~ 1800	~ 2600-3000
0.1	~ 50	~ 3600	~ 2800-3500
0.1	~ 50	~ 1800	~ 2800-3500
0.1	~ 100	~ 3600	~ 3000-4000
0.1	~ 100	~ 1800	~ 2800-4000
0.1	~ 1000	~ 3600	~ 3800-4800
0.1	~ 1000	~ 1800	~ 4000-5000

TX Transmission Simulations





Frequency: 0.1 kHz
Electrodes: 100 Meters
Power: 3600 Watts

Noise (Natural and Man Made)

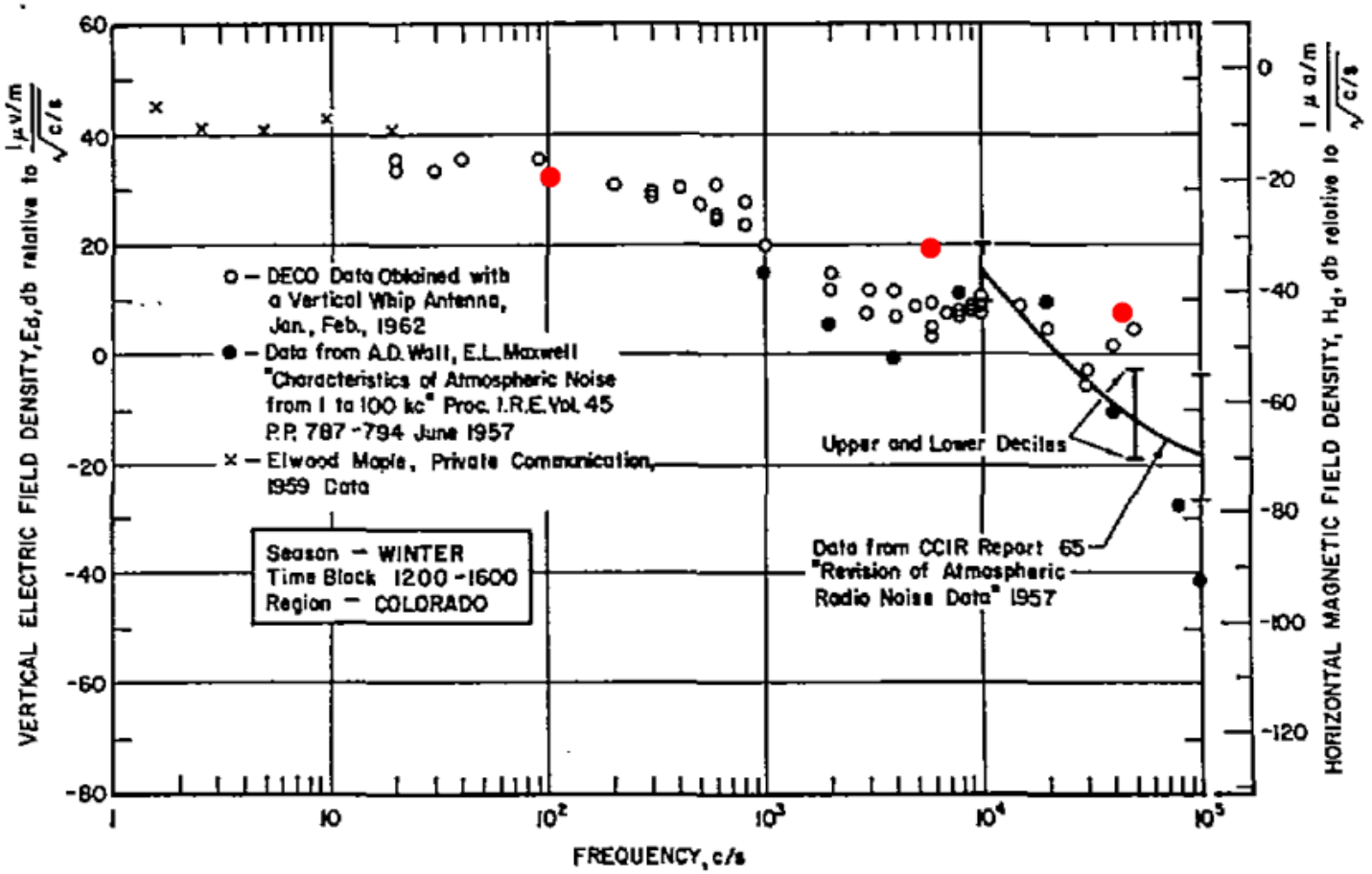


Fig. 1—Natural noise density.



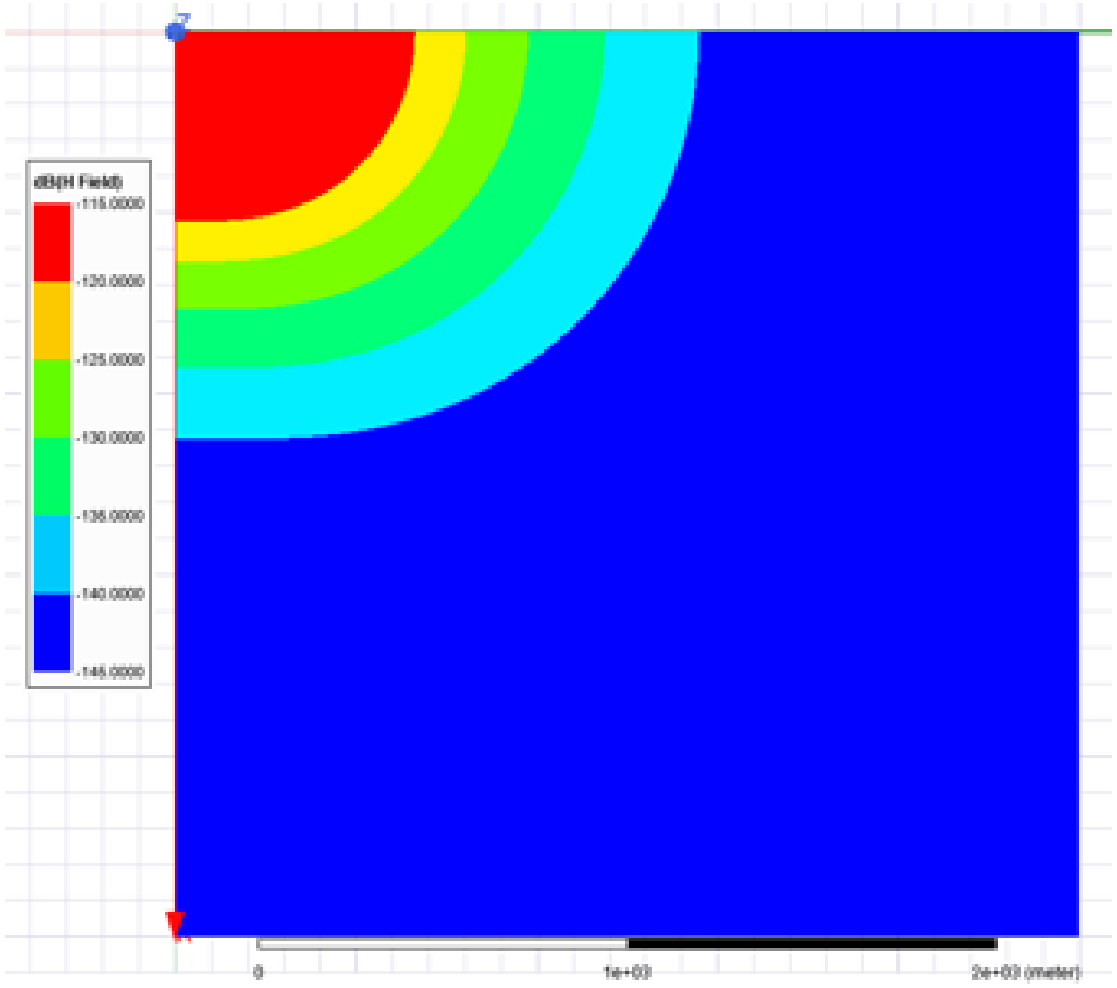
Ideal Range

Frequency: 1-4 kHz

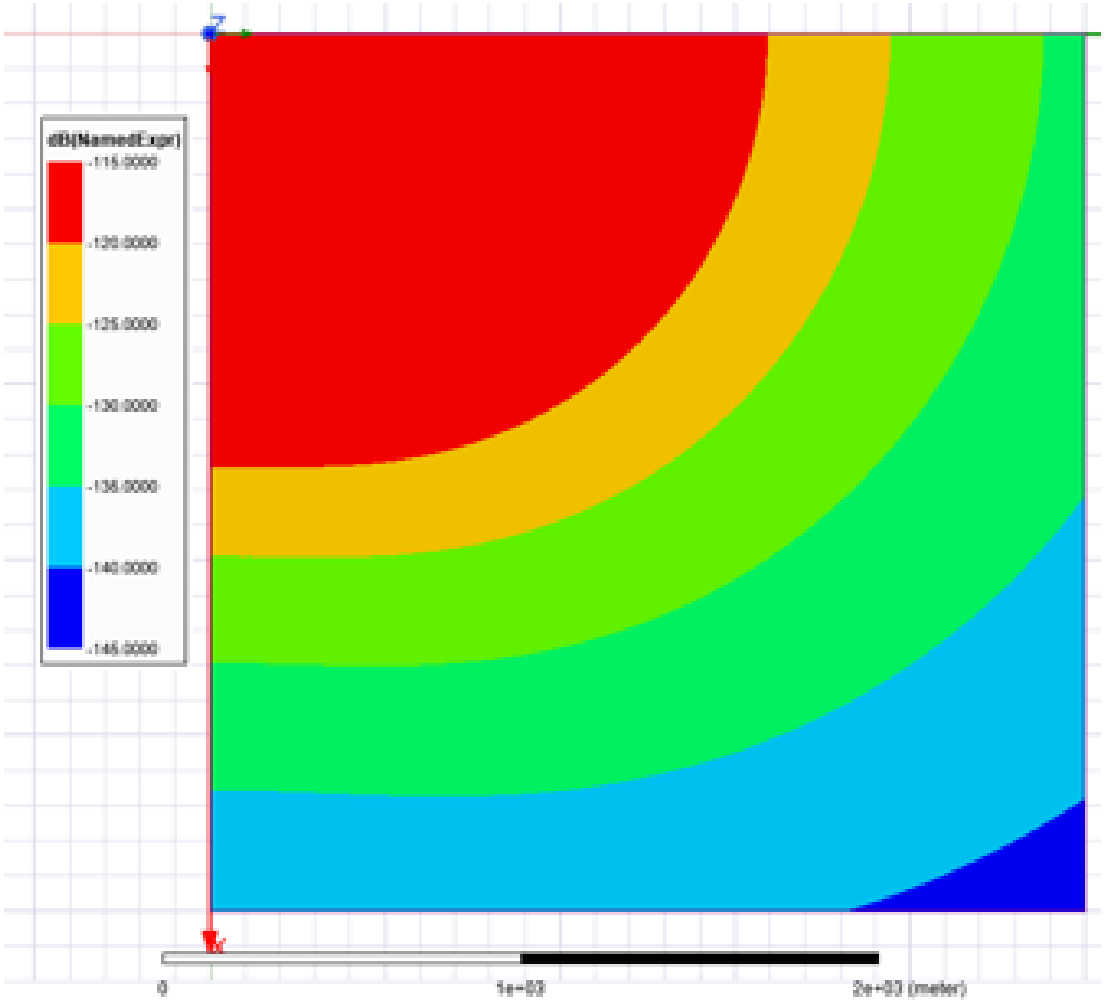
Electrodes: 10-100 Meters

Power: 3600 Watts

Low Power vs High Power

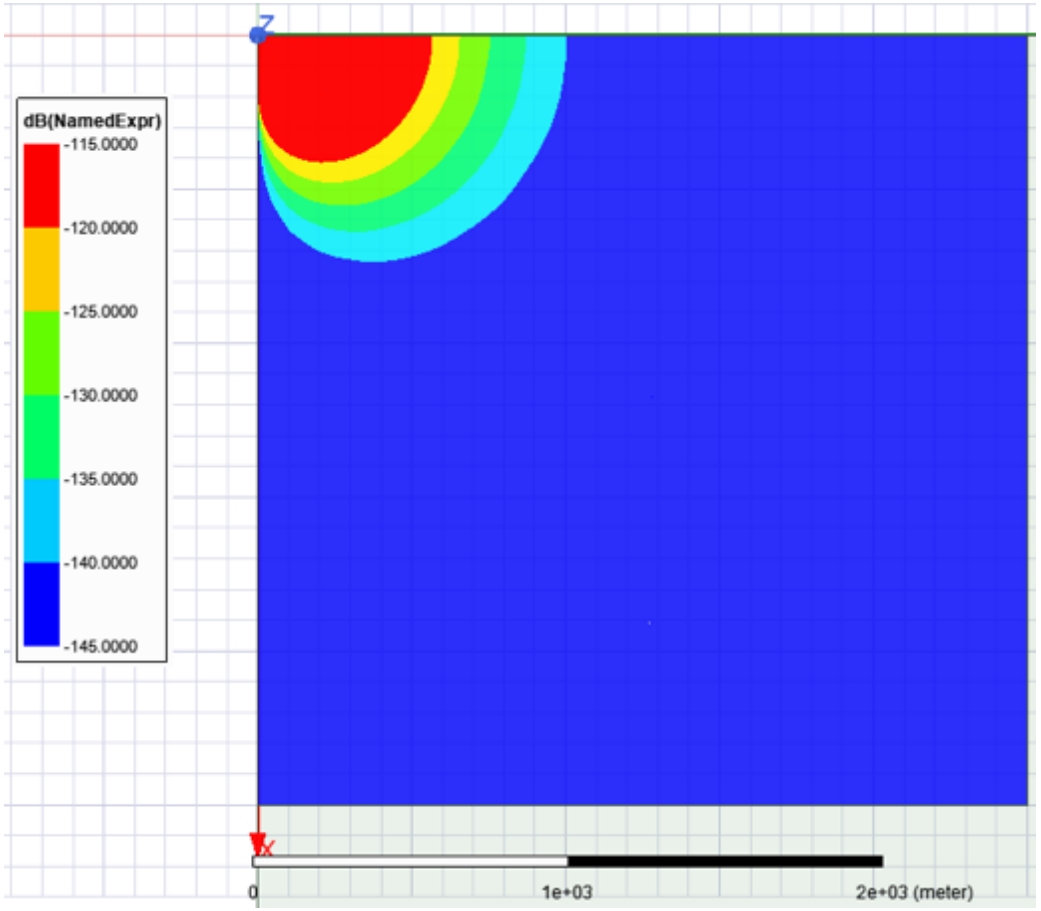


20W, 9kHz,
20-meter Electrodes
Distance **~1km**

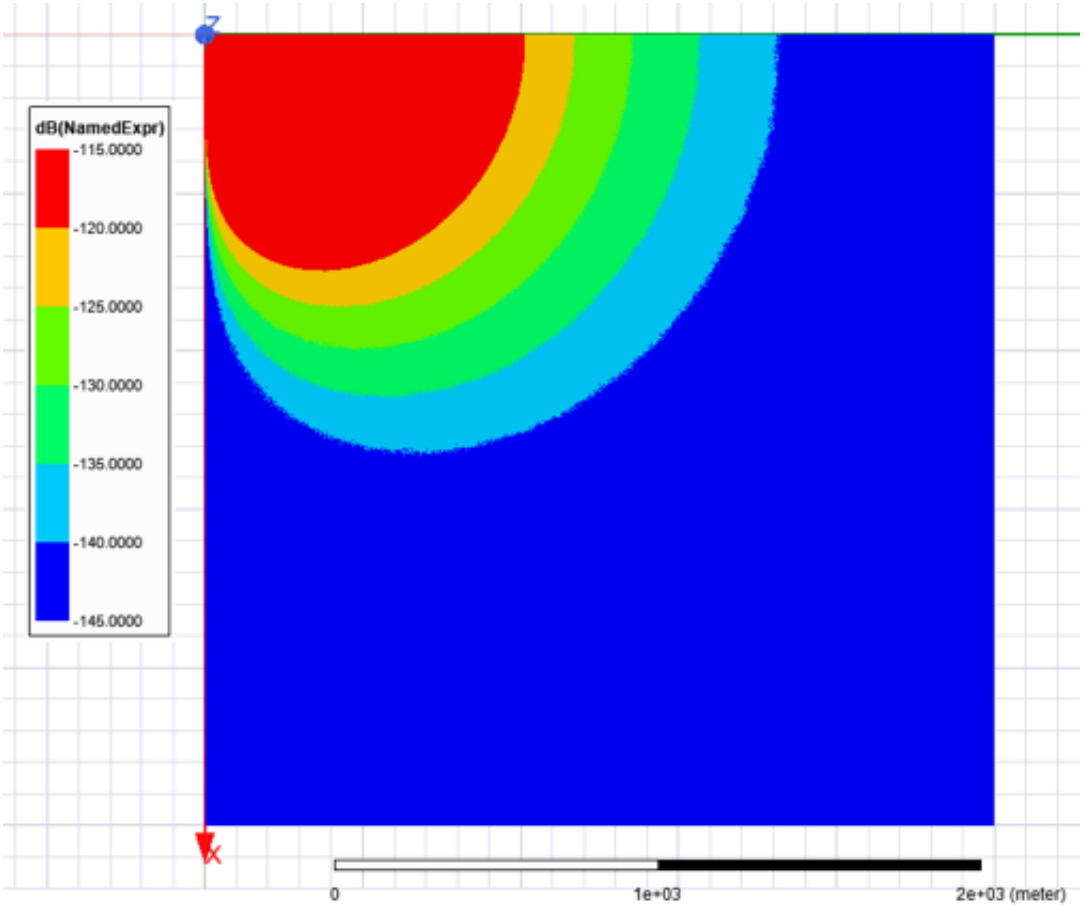


3600W, 9kHz,
20-meter Electrodes
Distance **~2.5km**

Tx Electrode Separation

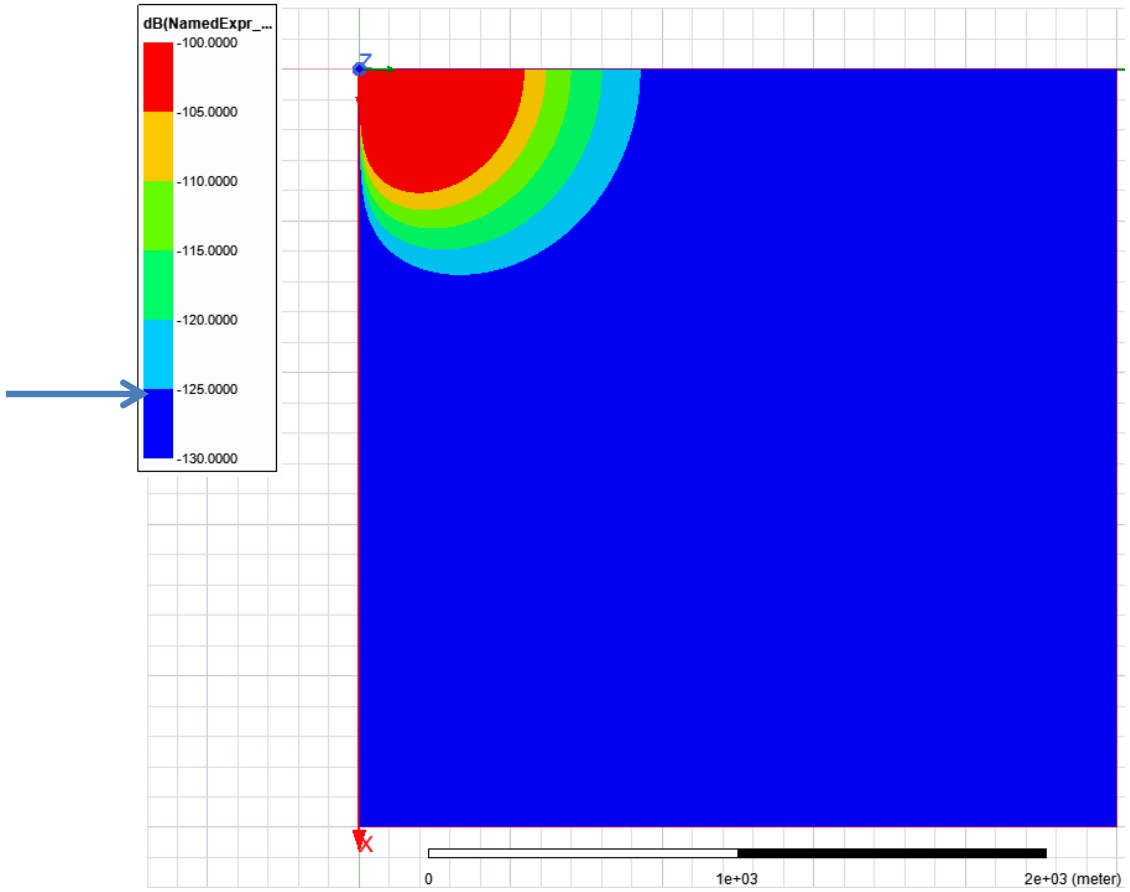


3600W, 9kHz,
10-meter Electrodes
Distance ~1km



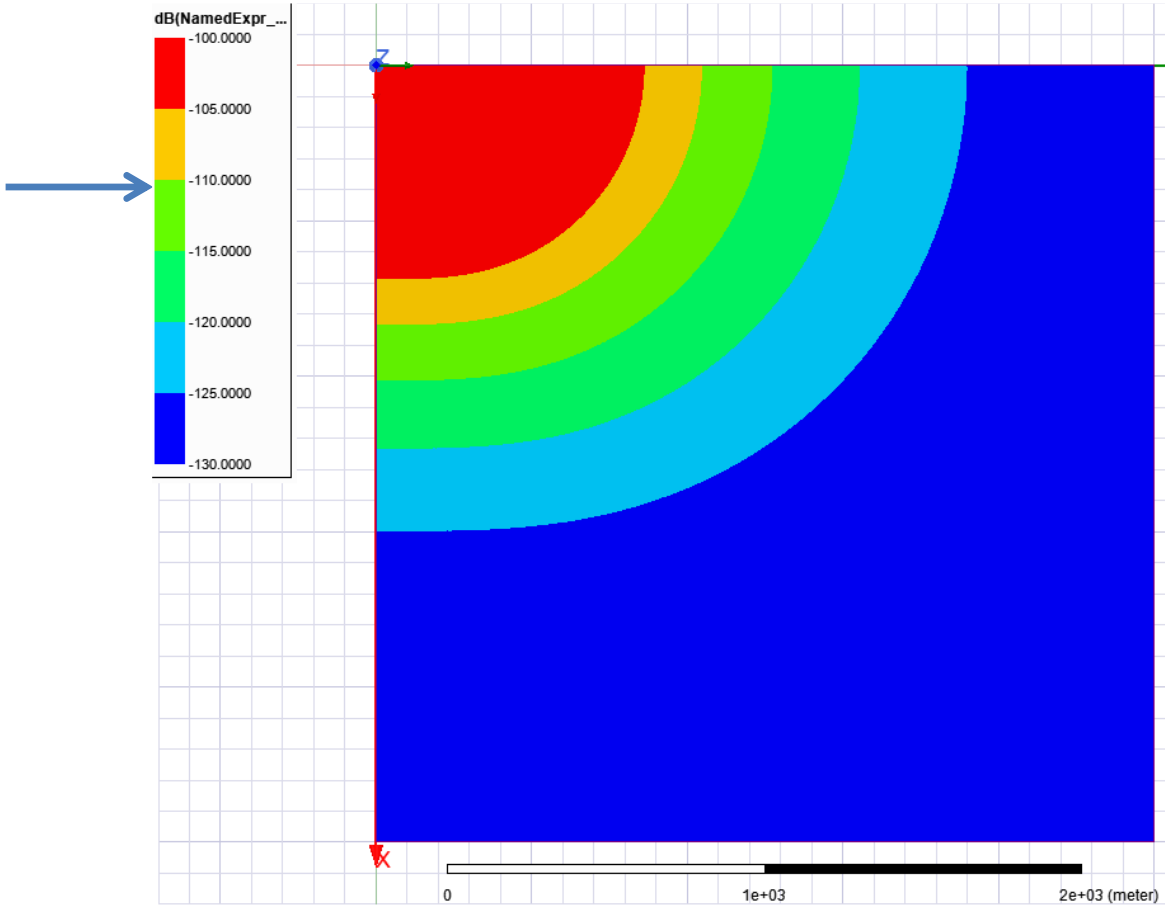
3600W, 9kHz
100-meter Electrodes
Distance ~1.6km

Normal vs Tangential Simulation



Normal

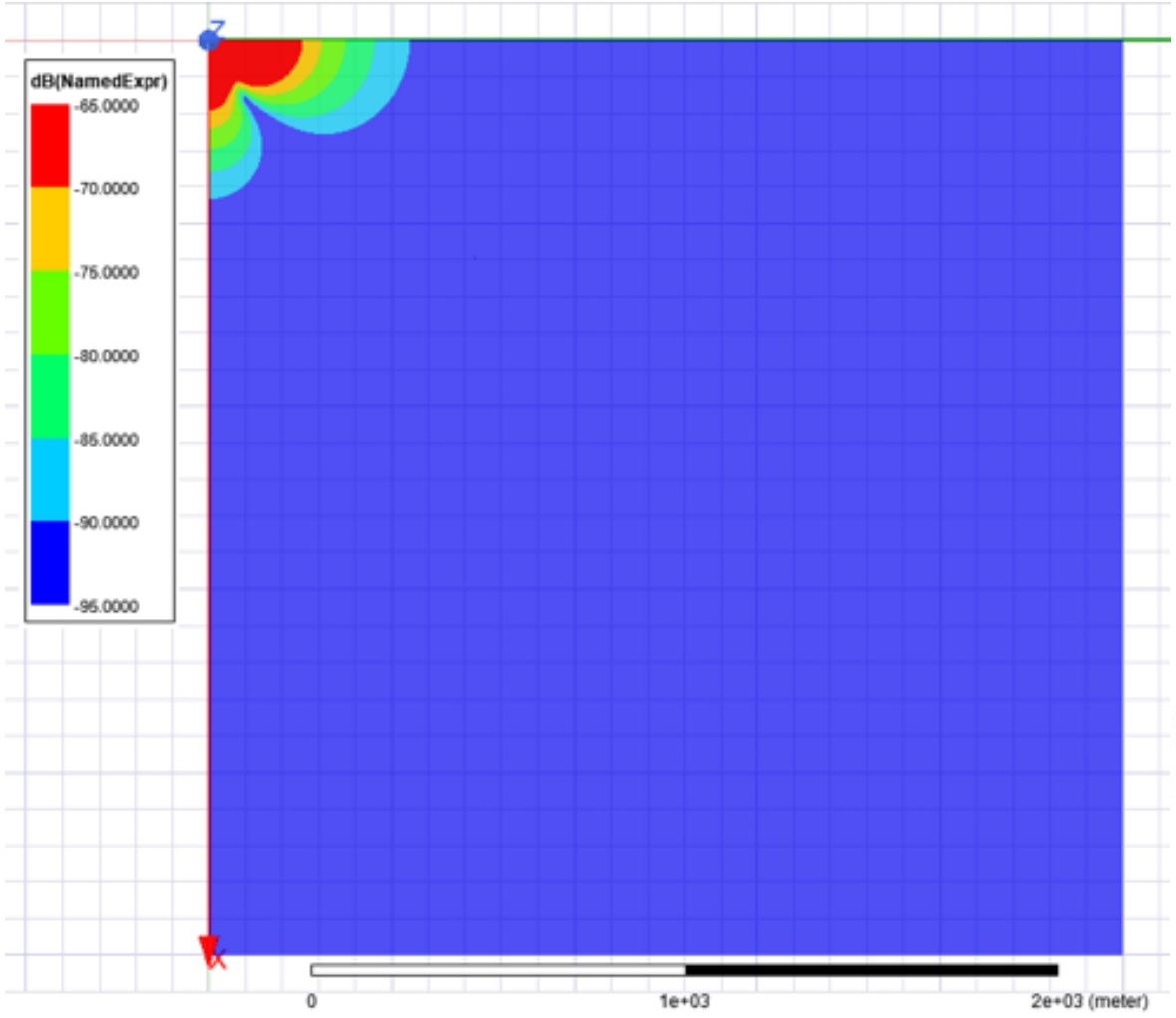
(laying down)



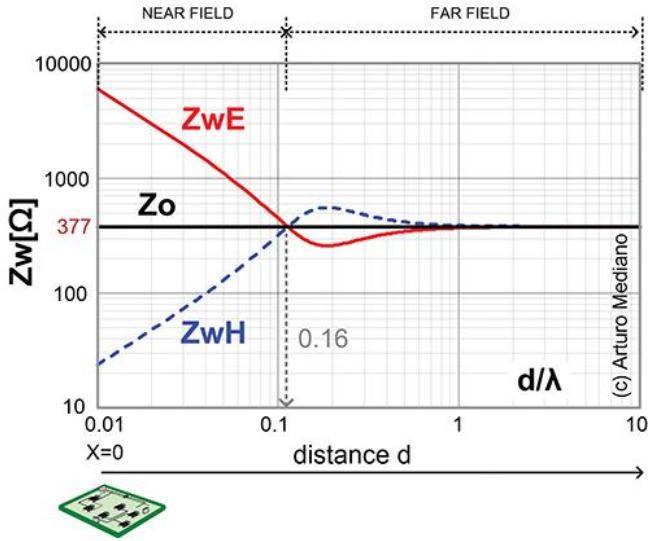
Tangential

(Vertical loop)

E- Field Tests



Frequency: 9 kHz
TX Electrodes separation ~10m
RX Electrodes separation ~10m aligned X-direction
Injected power ~ 3600W. Accepted power ~ 3560W.
Distance scale 100m/div.

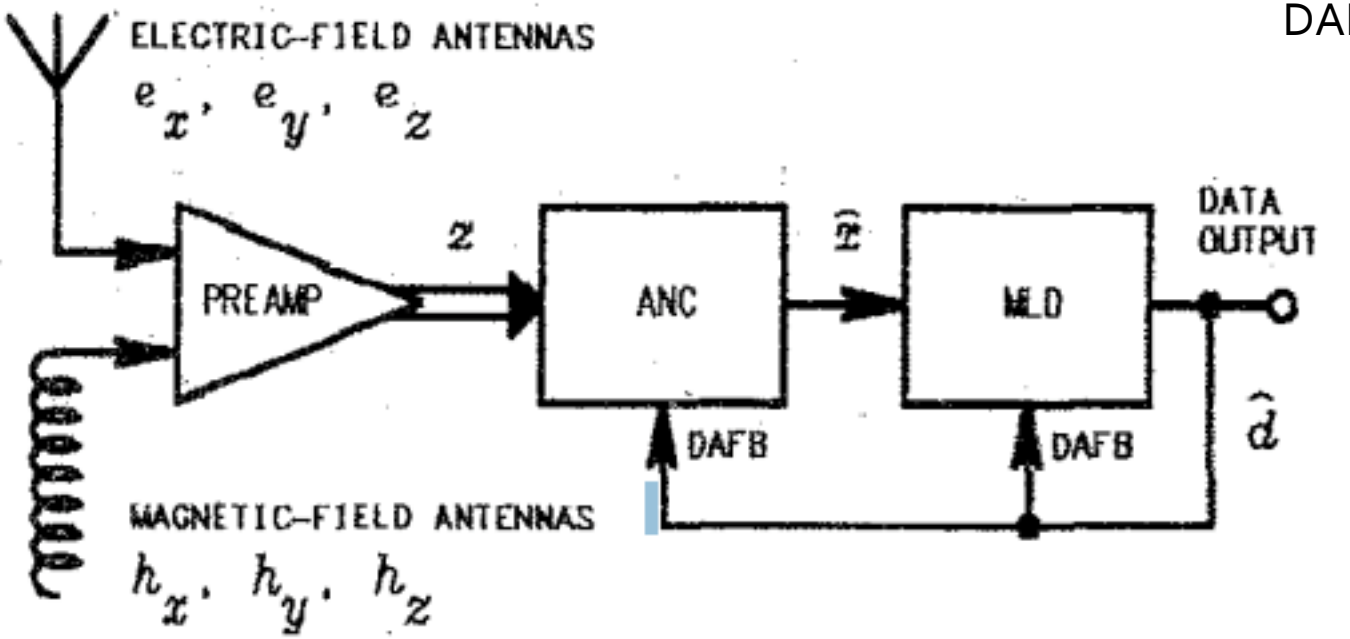


Impedance Matching

Earth Conductivity S/n	0.0001 (Dry)	0.001 (Sand)	0.01 (Soil) Reference Case	0.1 (Clay)
Matched Impedance	**Normal: 2km** **Tangent: 1.5km** Source impedance: ~6000 ohm	Normal: 1.9 km Tangent: 1.85 km Source impedance: ~600 ohm	Normal: 1.4 km Tangent: 1.85km Source impedance: ~100 ohm	Normal: 1.05 km Tangent: 1.9 km Source impedance: ~7 ohm
Non matched Impedance	**Normal: 1.45 km** **Tangent: 0.7 km** Source impedance: ~100 ohm	Normal: 1.75 km Tangent: 1.65 km Source impedance: ~100 ohm		

Modulation Techniques – SNR (Signal to Noise Ratio)

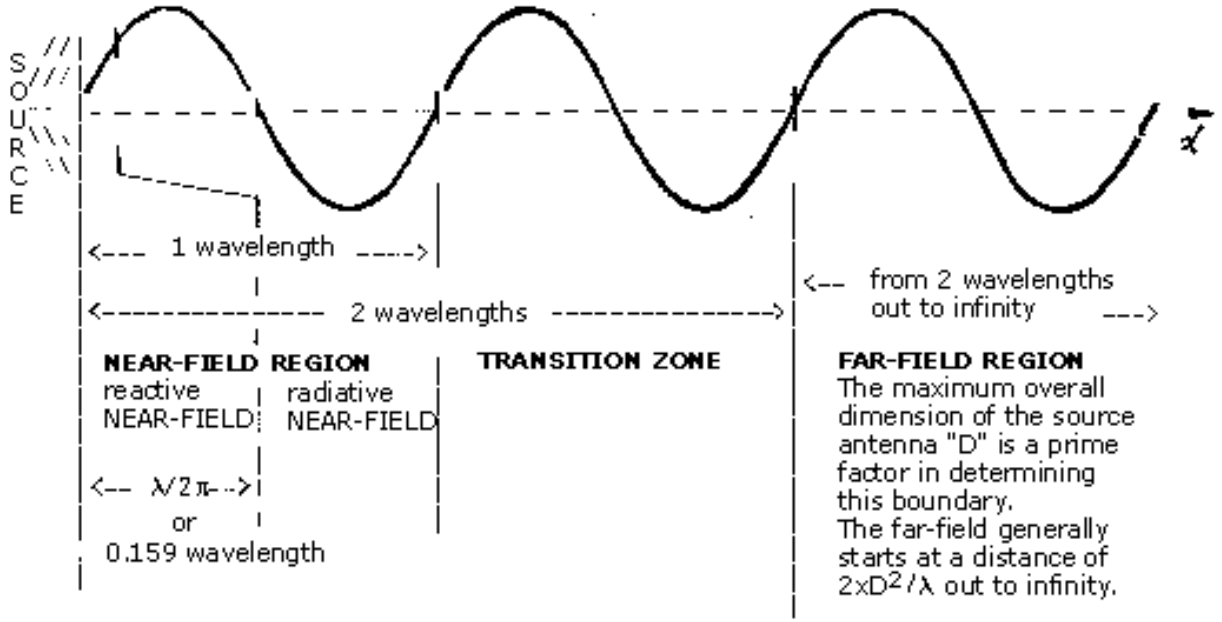
ANC: Adaptive Noise Cancellation
MLD: Maximum Likelihood detection
DAFB: Decision Aided Feedback

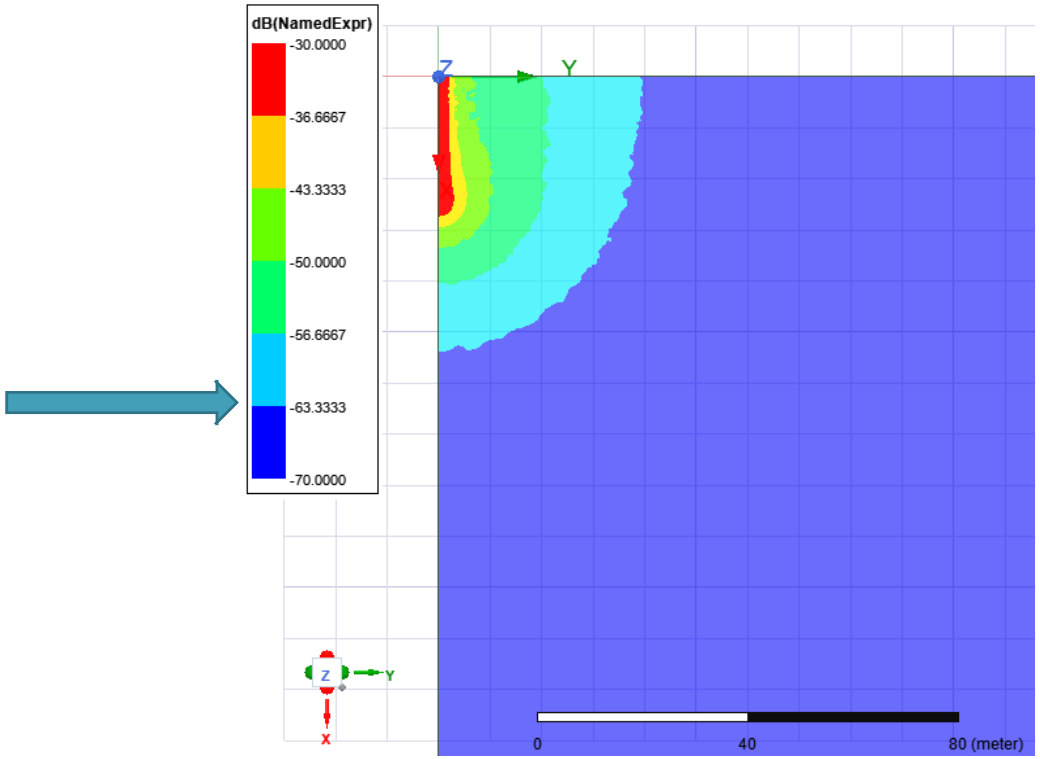


Modulation Choice improves SNR by 10-30 dB in TTE (doubling operation distance)

* Paper includes Schematics for FSK, ASK and MSK modulation.

POE – Power through the Earth



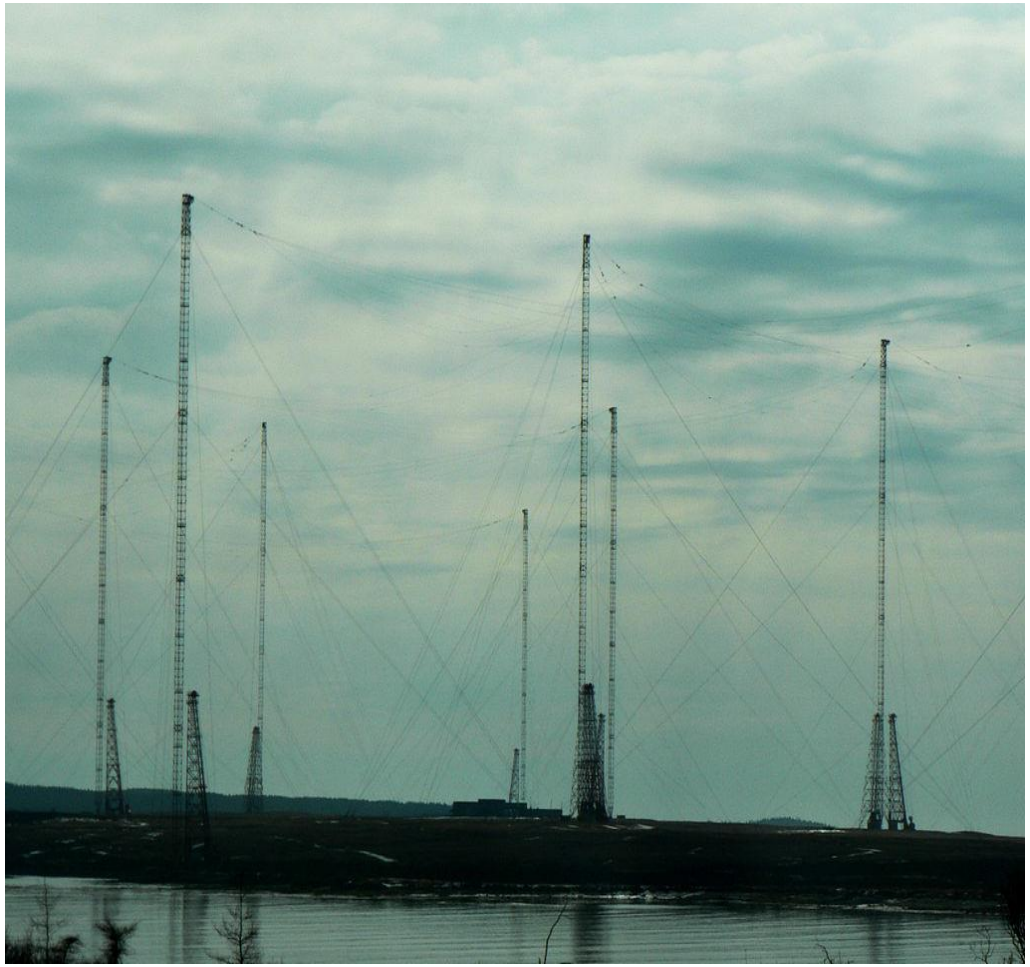


The estimation of the USB DC power supply capability by means of Wireless Power Transfer (resonant NFC coupling) is explained below with simulations.
To provide power ***P*** at a perfectly matched load (USB powered device, for example) the required strength of magnetic field ***H*** is: **~50 meters**

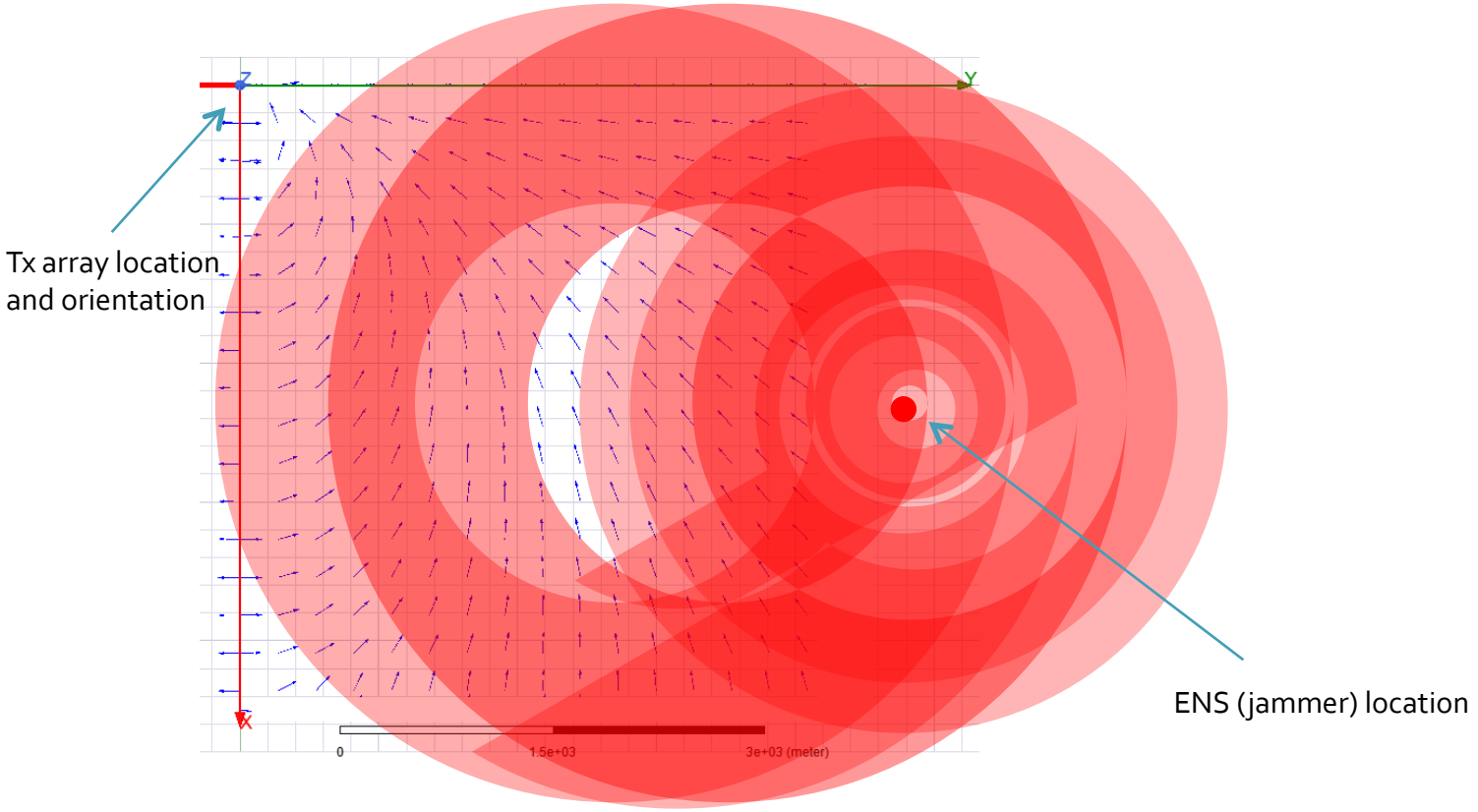
$$H = \frac{4 \cdot \sqrt{\rho}}{f \cdot \pi^{3/2}} \cdot \frac{\sqrt{P}}{\sqrt{S_w} \cdot D^{3/2} \cdot \sqrt{N}}$$

Where:
D – diameter of Rx coil (assumed 1m)
N – number of turns of coil winding (assumed 100 turns)
Sw – cross-section area of wire (0.312 mm^2)
f – frequency of wireless power transfer (2 kHz)
p - resistivity of wire conductor (1.72 x 10^{-8} Ωm)
The estimated required strength of magnetic field ***H is*** -62 dBA/m

Antenna / Near Field / Far Field

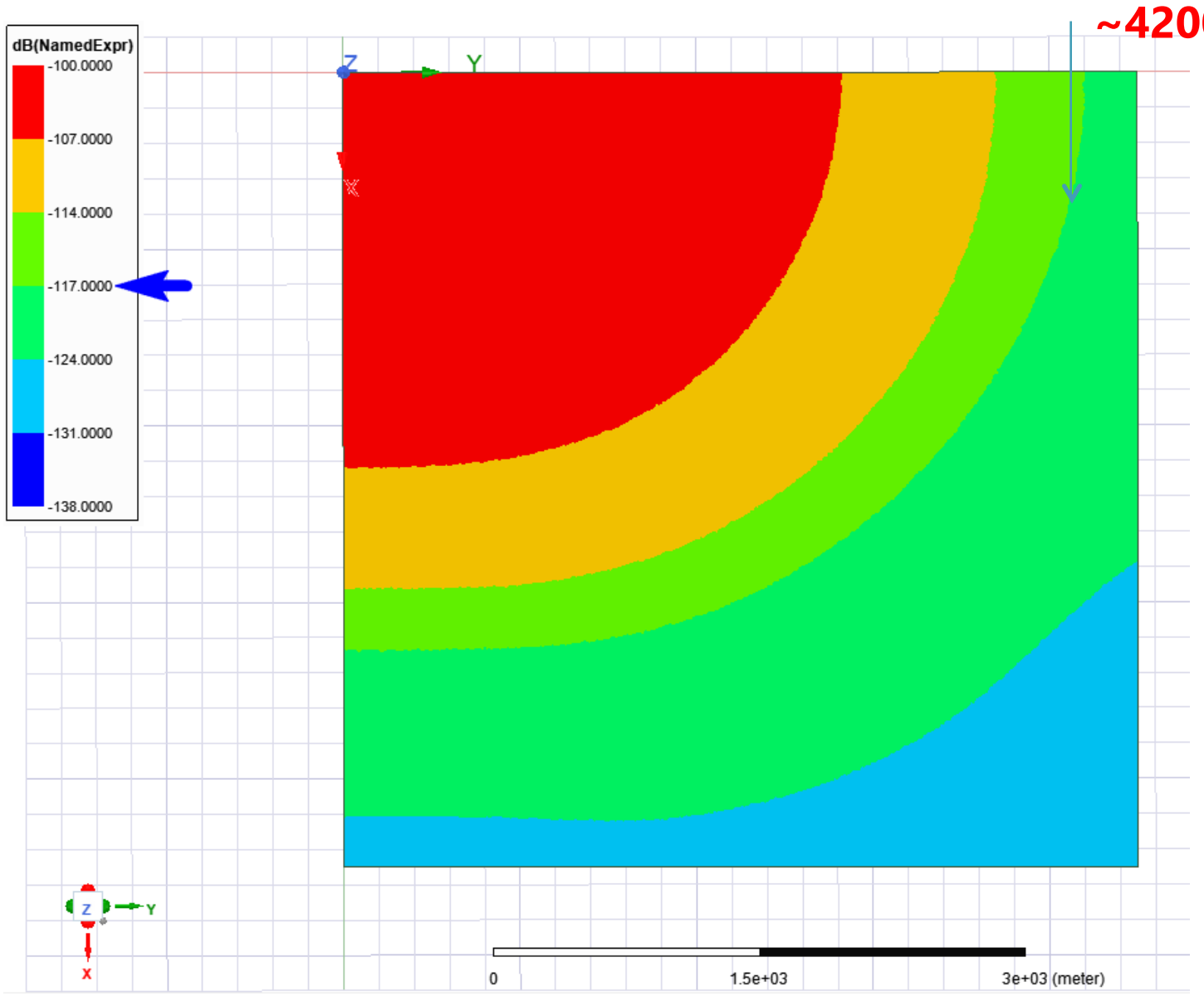


Tangential vs Normal



Normal: Loop Antenna Flat on ground is not affected
Tangential: Is Affected, Required Multi – Rx right angle Vertical Loops
** More details in paper

Playing with the Variables



Frequency 2 kHz
Electrodes: 100m separation
Antenna Tangential
Impedance: Perfectly Matched
Tx power: 20 kW
Rx sensitivity: 5kg Copper Wire

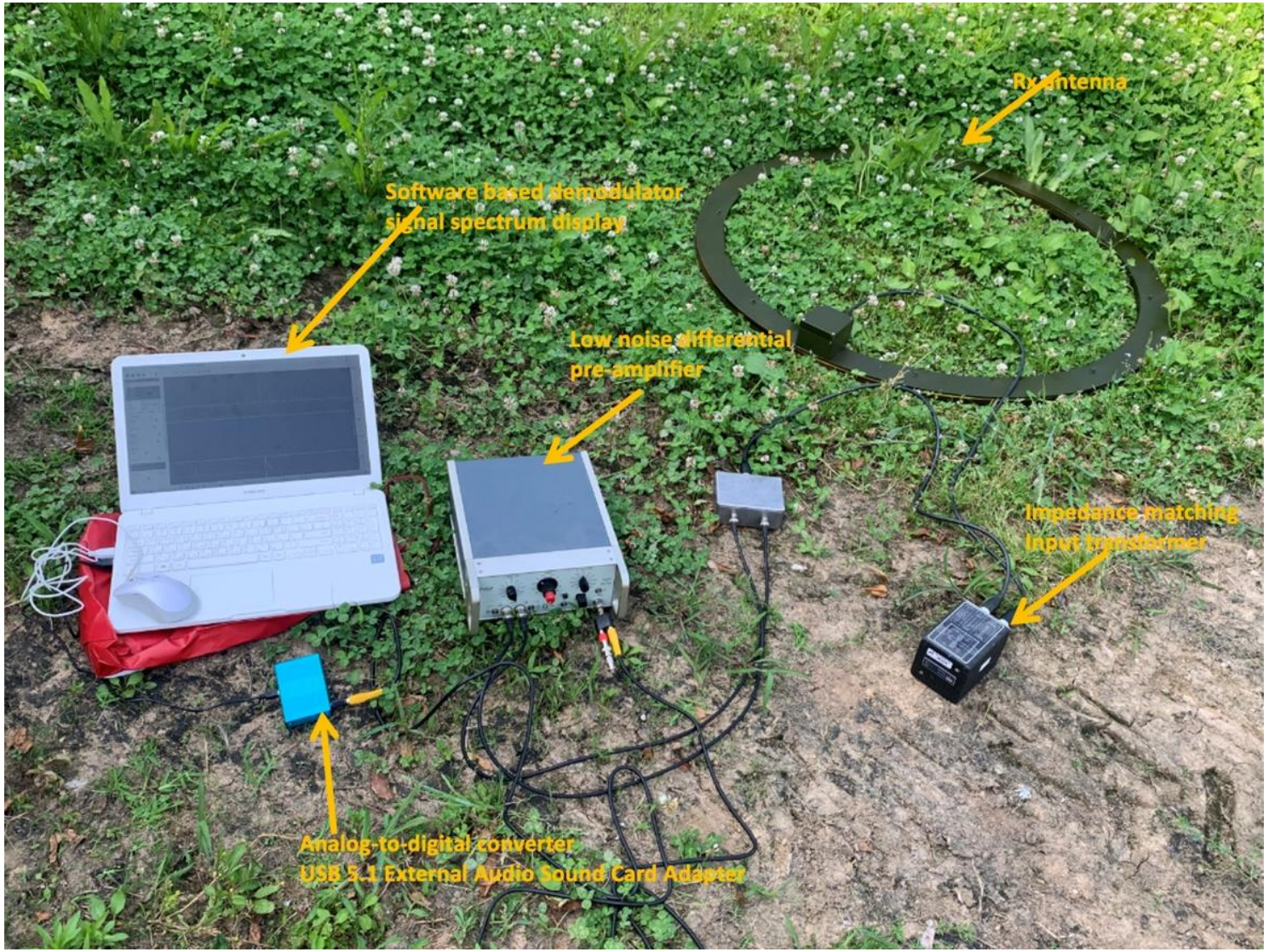
VLF/ULF – Earth Mode Hardware

ECCM – Electronic Counter Countermeasure

Custom Tx/Rx Prototype



Tx



Rx

Custom Transmitter

Prototype



shutdown

Mute toggle and button (for manual amplitude modulation)

fault (short protection)

master/slave

Gain

Load impedance

Commercial Version



Smaller Tx Containing

- **20W+3600W Power Amp**
- **Amp to Tx Antenna Matching**
- **Arduino/Pi (Data post processor/logger/encryption)**
- **LCD Display**

Custom Rx



Smaller Rx Containing

- Rx Antenna Coil
- Band Pass Filter (BPF) input TX matching impedance
- Low Noise Pre-Amp
- Arduino/Pi (Data post processor/logger/encryption)
- LCD Display





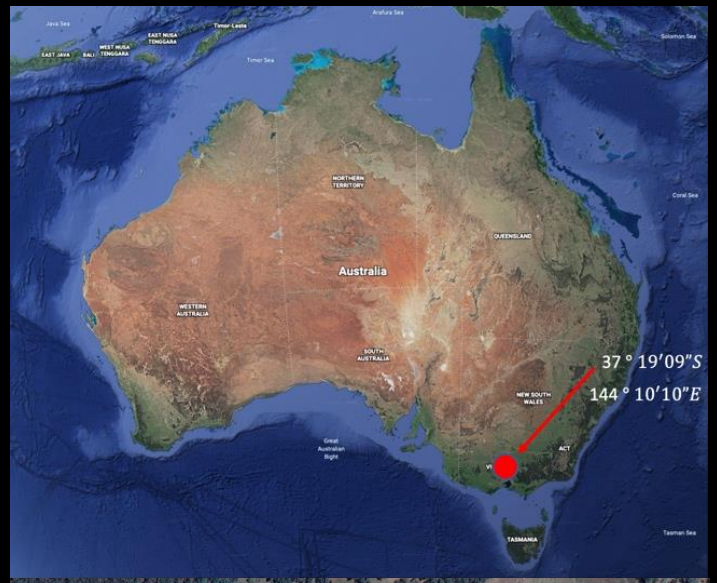
Electrodes and Antenna



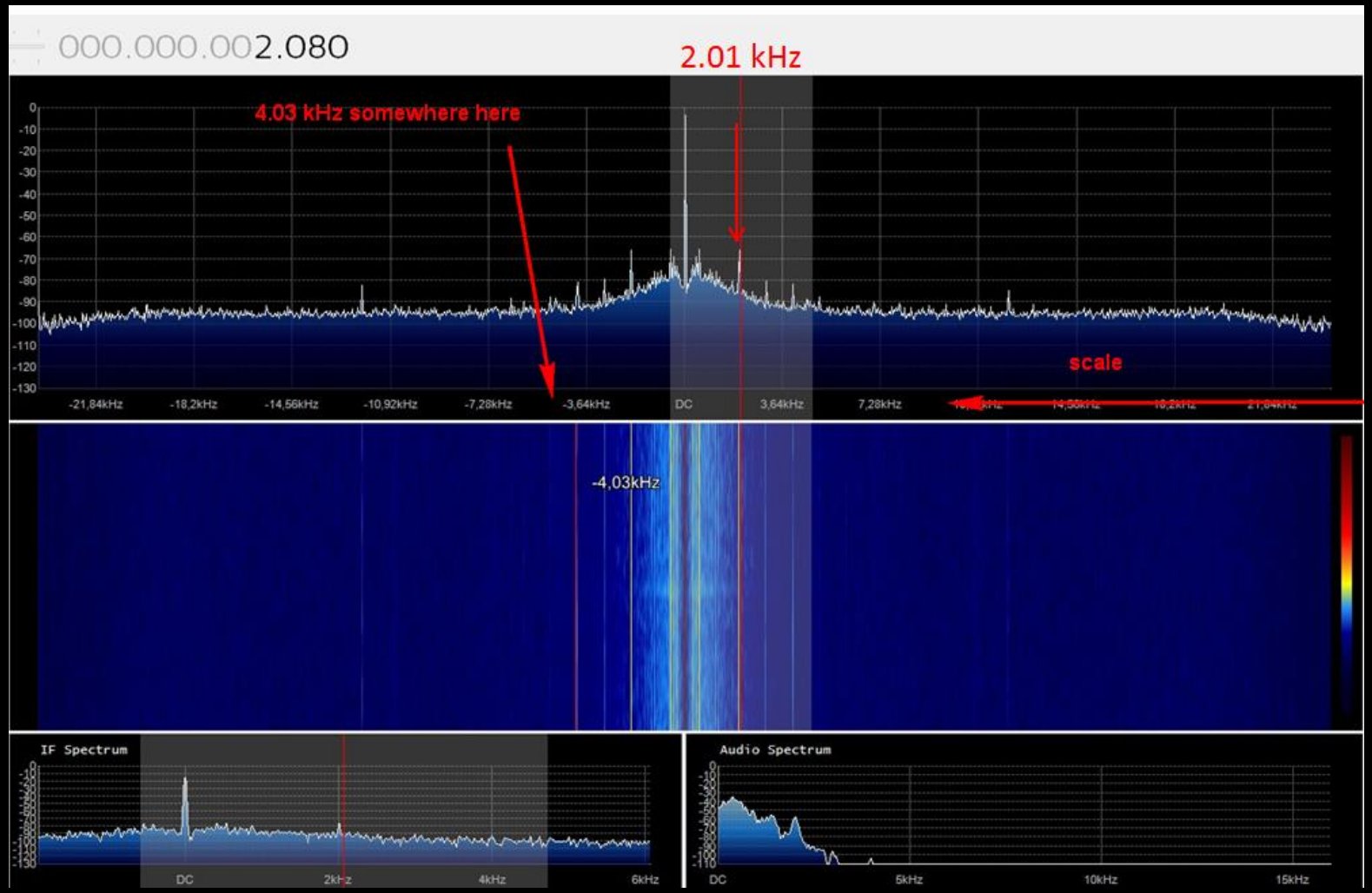
TX Electrodes 1metre Steel Pipe



~2 kHz Test Results





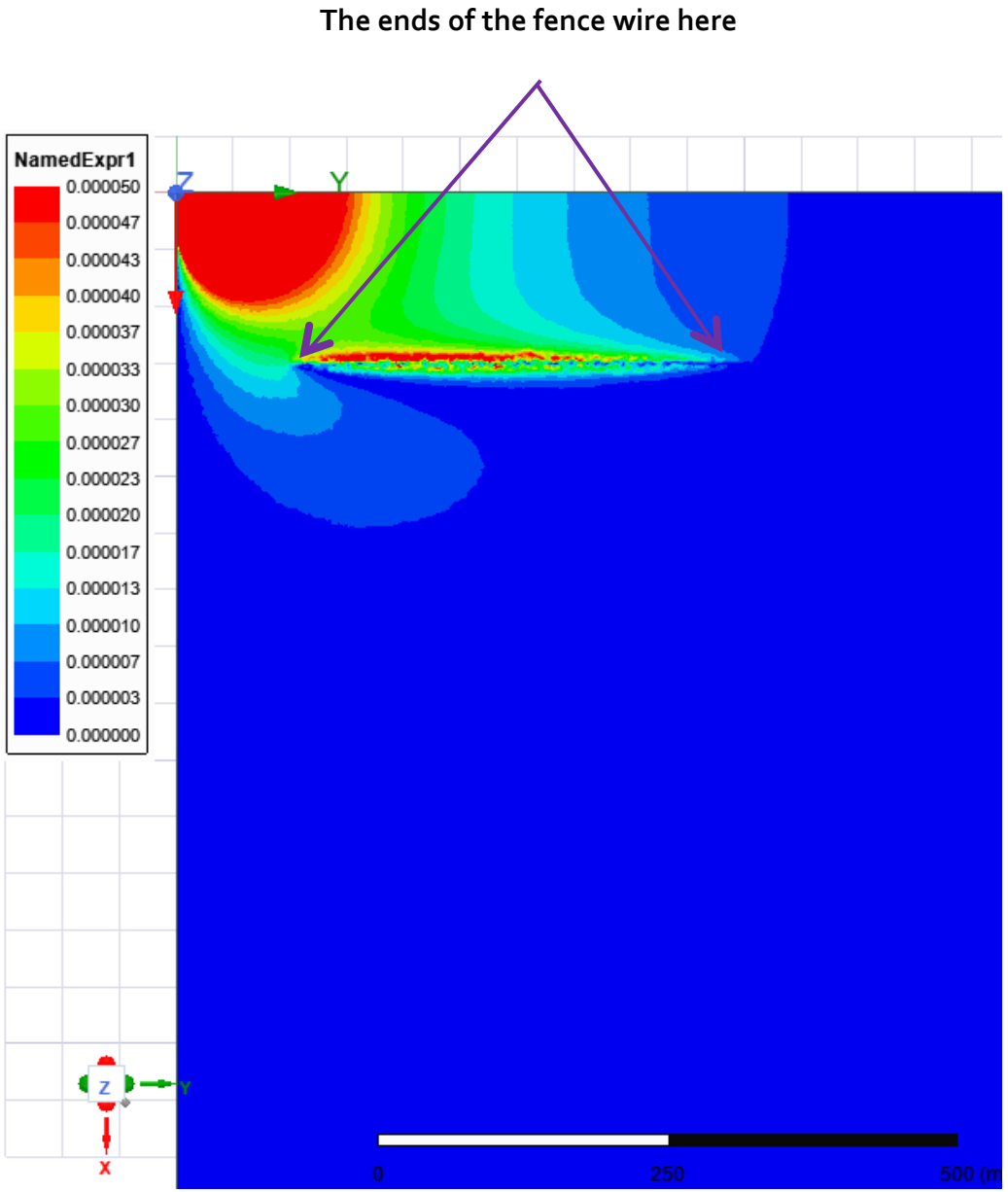


TX: Electrodes 50 meters
Power: **20 W**
Impedance: 100 Ohm
Modulation: ASK

RX: 1 meter diameter coil
Impedance: 100 Ohm
Preamp: AC, LF roll-off – 1kHz, HF roll-off – 1kHz, Gain – 200 (linear).

Distance: 923m

Utilities Assisted Mode



VLF – Utility Assisted Mode

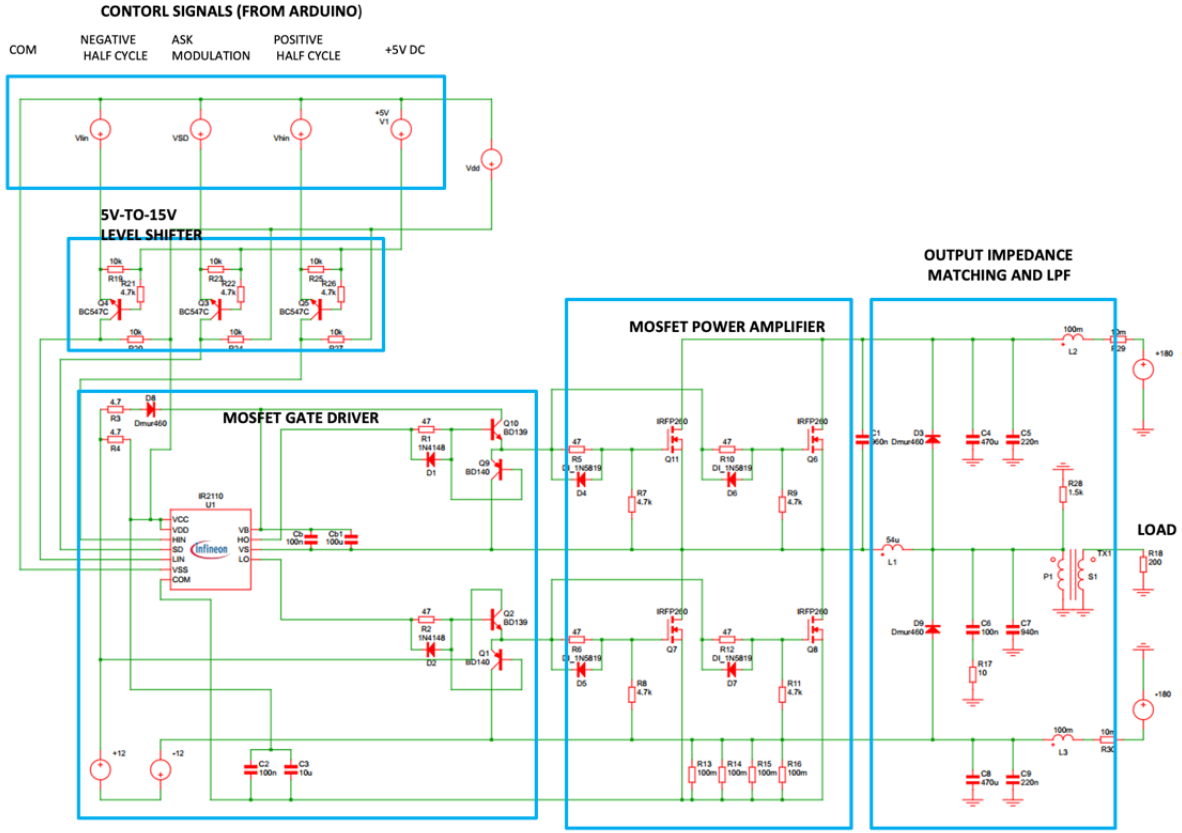
Hobbyists have recorded 2-10km of increased signal detection with underground steel pipes, wires, etc.

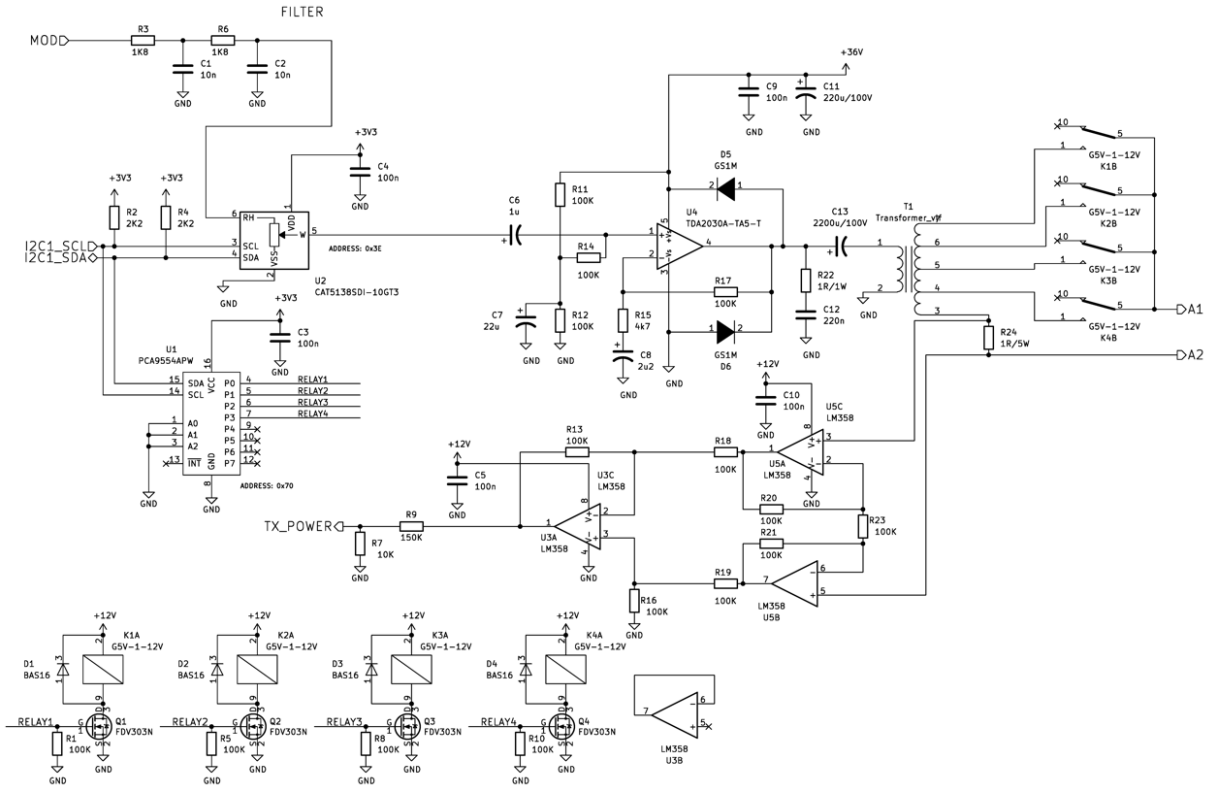
***Will impact Urban distances positively

Home Brew

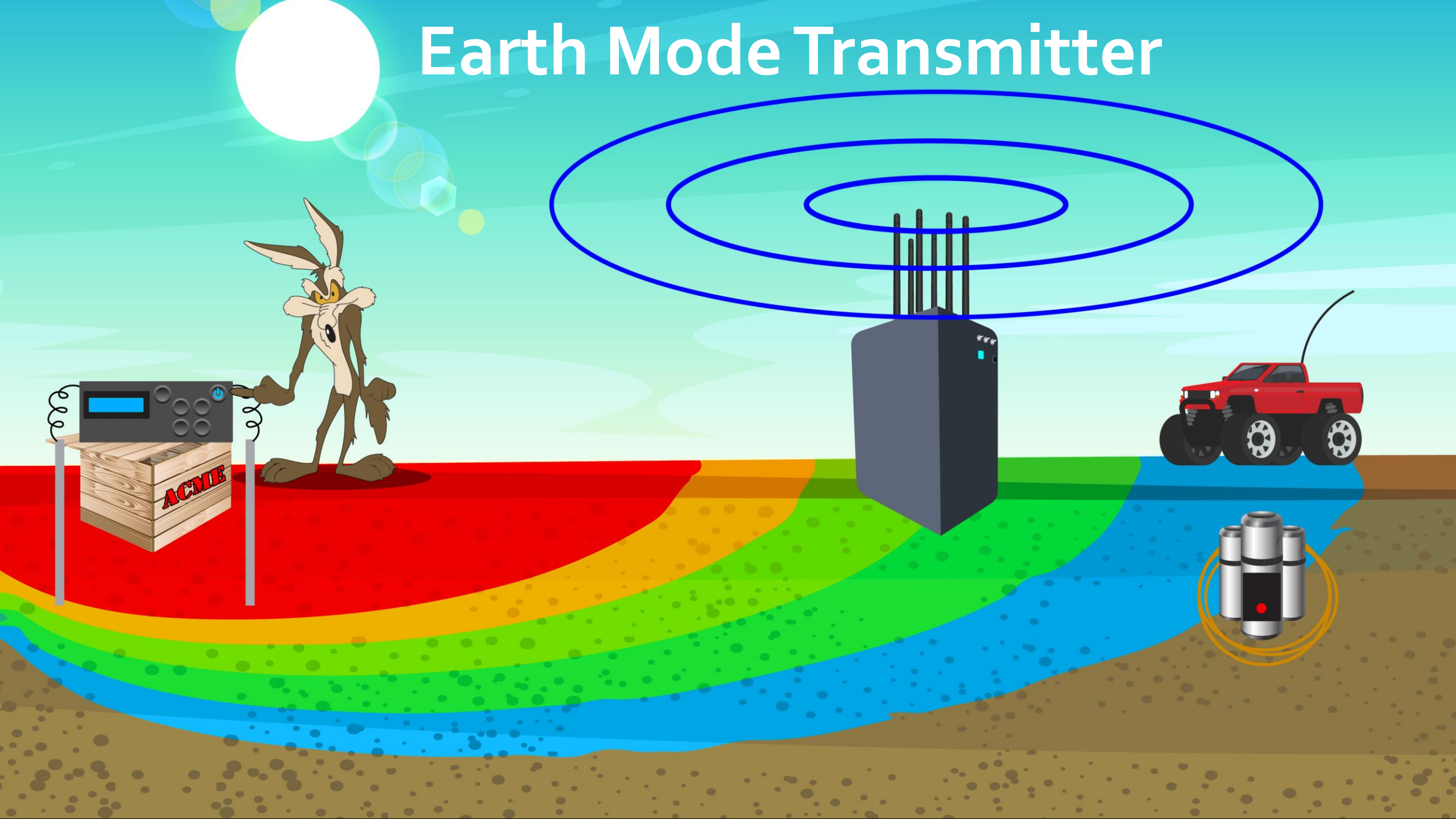
Stage	Materials	Costs	Comments
Base band processor (Arduino)	Arduino Board	$20	Message encoded for Arduino
Tx pre-amplifier (modulator)	Wire, jumpers, switches, modulated with TX ~20W Amp. Can be removed with TX fully synthesized digital source with Arduino above.	$300 / $0	An off the shelf Tx ~20W PA design kit
Tx ~20W Power Amplifier	Enclosure, DC 24V 7A*h rechargeable battery pack	$100	Cutting, drilling, PCB Assembly, and soldering.
Tx amp-to Tx antenna matching	Copper wire, transformer core and coil former	$50	Transformer winding and soldering
Tx Antenna (electrodes)	~55mm ID Steel Pipe 2m ~50mm OD Steel pipe 2m 200x800x3 mm^3 steel plate Bolts and welding clamps	$115	Cutting, griding, bending, welding, and soldering.
Rx antenna (coil)	3 pcs of 1000X1000X10mm ^3 Foam PVC sheet. Copper wire, enclosure, connector, PVC bond	$170	Cutting, bonding, winding, soldering.
Rx BPF and impedance matching or amp below	Low noise input impedance matching transformer or pre amp below (either or)	$2500 new or $200 custom	Rare stock and overpriced new, Replaced with a custom narrow band transformer for $200
Rx low noise pre-amplifier	Differential input low noise preamplifier	$1000 new or $100 custom	Rare stock and overpriced can be replaced with a custom Dual Amp building block chip. (LT1567 Dual ABB) or Preamp LNA10
BPF amplifier and signal conditioner	PCB, components	$50	PCB Assembly
Data post processor and data logger	Arduino Board	$20	Message encoded for Arduino

Home Brew


CONTORL SIGNALS (FROM ARDUINO)
COM
NEGATIVE HALF CYCLE
ASK MODULATION
POSITIVE HALF CYCLE
+5V DC
5V-TO-15V LEVEL SHIFTER
MOSFET GATE DRIVER
MOSFET POWER AMPLIFIER
OUTPUT IMPEDANCE MATCHING AND LPF
LOAD


FILTER
MOD
I2C1_SCLD
I2C1_SDA
TX_POWER
RELAY1
RELAY2
RELAY3
RELAY4
A1
A2
+36V
+12V
+3V3
GND

Earth Mode Transmitter



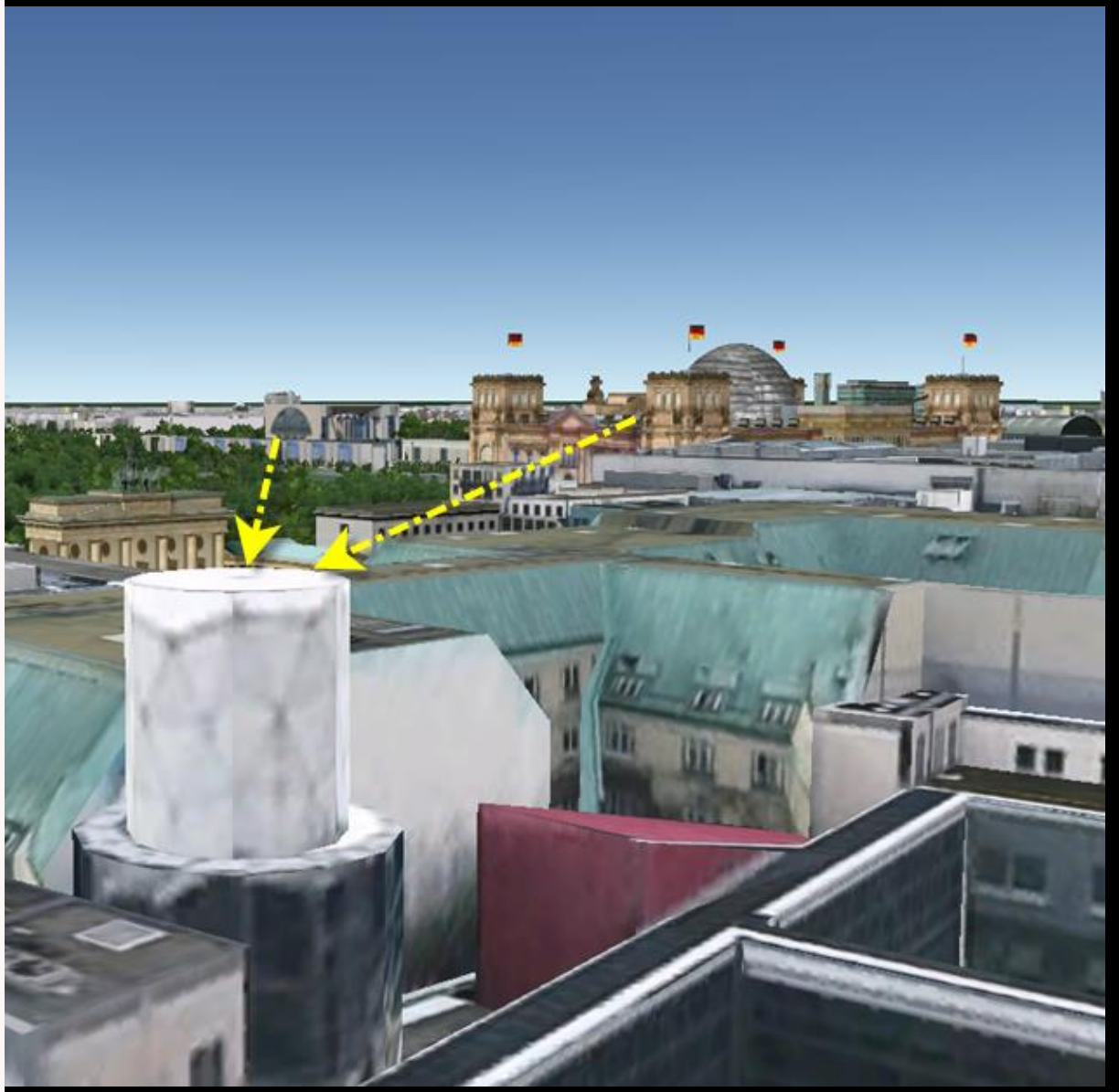


Use Case


State of IoT and Agriculture
BizIntellia
An end-to-end IoT Solution
Auto Spreading
Diagnosis of Disease
Crop Yield Analysis
Smart Data
Soil Erossion
Field Monitoring
Water Stress
Variable Rate of Fertility

Use Case


MAP EXPLAINER
Ukraine
GDP (nominal) $155.6B 54 of 206
Population 43,467,779* 35 of 206
Land Area** 603,628 km² (233,062 sq mi)
Pop. Density ~75/km² (196/sq mi)
*Excluding the autonomous Republic of Crimea and the city of Sevastopol
**About 7% of Ukraine's land area is Russian occupied
Urban Areas (sized by population)
In 1986, Chernobyl suffered the worst nuclear disaster in history. Even today, there is an Exclusion Zone covering an area of approximately 2,600 km² (1,000 sq mi) where radioactive contamination is highest and public access is restricted.
The fourth-longest river in Europe, the Dnieper River, begins in the Valdai Hills of Russia, then flows through Belarus and Ukraine to the Black Sea. A number of reservoirs and hydroelectric dams lie along the length of the river.
Vladimir Putin, Russia's president, officially recognized the Donetsk and Luhansk regions (shown below) as breakaway "people's republics".
Since 2014, upwards of 1.5 million people fled these regions to Russia and other parts of Ukraine.
Ukraine–Russia border
Belarus
Poland
Lviv
Pop. 721,510
Kharkiv
Pop. 1,433,886
Kyiv
Pop. 2,962,180
Kyiv (also known as Kiev) is the capital and most populous city of Ukraine.
Luhansk
Pop. 399,559
Vinnytsia
Pop. 370,601
Carpathian Mountains
Dnipro
Pop. 980,948
Kryvyi Rih
Pop. 612,750
Donetsk
Pop. 905,364
Highest point: Mount Hoverla
Moldova
Zaporizhzhia
Pop. 722,713
Mykolaiv
Pop. 476,101
The largest nuclear power plant in Europe
Mariupol
Pop. 431,859
Conflict Zone
Ukrainian government forces and Russia-backed separatists have been battling for control over this heavily-industrialized portion of the country since 2014.
So far, the conflict has killed more than 14,000 people.
Natural Gas Transit Through Ukraine
120 bcm†
41 bcm†
2001
2021
In the 1990s, most gas that Russia exported to Europe crossed Ukraine. Newer pipelines, like Nord Stream and TurkStream, have diminished Ukraine's gas transit role.
Agricultural land covers 70% of the country. War could send shockwaves through global agricultural markets.
Sea of Azov
Odesa
Pop. 1,015,826
Crimea
Romania
Black Sea
Major Pipelines
Sevastopol
Pop. 464,349
Although not a NATO member, Ukraine is the fourth-largest recipient of military funding from the U.S.
The largest city in Crimea and a major port on the Black Sea. Sevastopol, along with the rest of Crimea, is internationally recognized as part of Ukraine, but has been administered by Russia since being annexed in 2014.
Sources: CSIS, Google Earth, Britannica, State Statistics Committee of Ukraine, New York Times
†Billion cubic meters
visualcapitalist.com

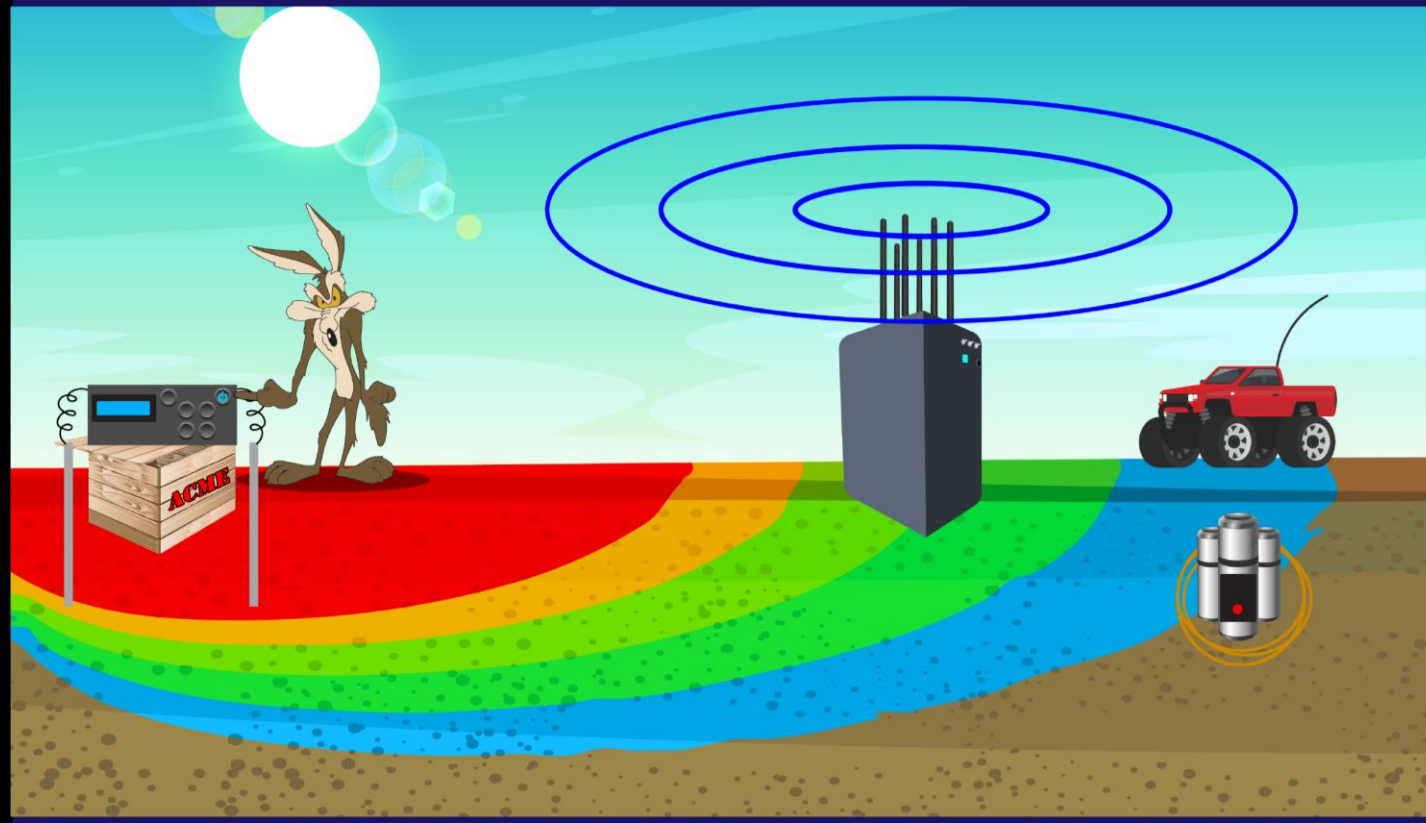


Summary

- Send messages up to 11km (7 Miles)
- Operates at 1- 4 kHz
- Conductive Current Magnetic field ULF
- Runs in Near Field Magnetic Field (H Field) not Far Field.
- TX operate from 20Watts to 3600W power scales to 20 kW
- RX runs on 20Watts
- Impedance Matching Options
- Encrypted messages using Libraries
- Modulation options
- Jammer proof
- Small factor RX Arduino/Pi or can use Laptop PC for messages

The End

CONDUCTIVE CURRENT EARTH MODE COMMUNICATIONS



Radio Frequency Jammer
Electronic Counter Countermeasure