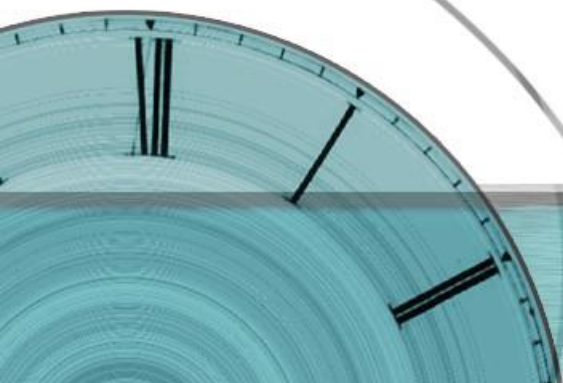


短距离无线系统与航空无线电系统攻击

UnicornTeam 无线电硬件实验室

演讲人：张婉桥





360UNICORNTTEAM

人体移植芯片



Éprouvé - Vérifié

🏠 > All Categories > Firefly Tattoo - Green



Firefly Tattoo - Green

Model Firefly01

Condition New

An implantable subdermal light - Green

Send to a friend

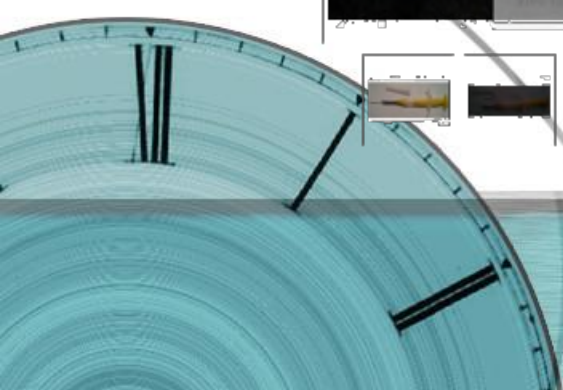
Print

US \$119.00

US \$119.00 per 1

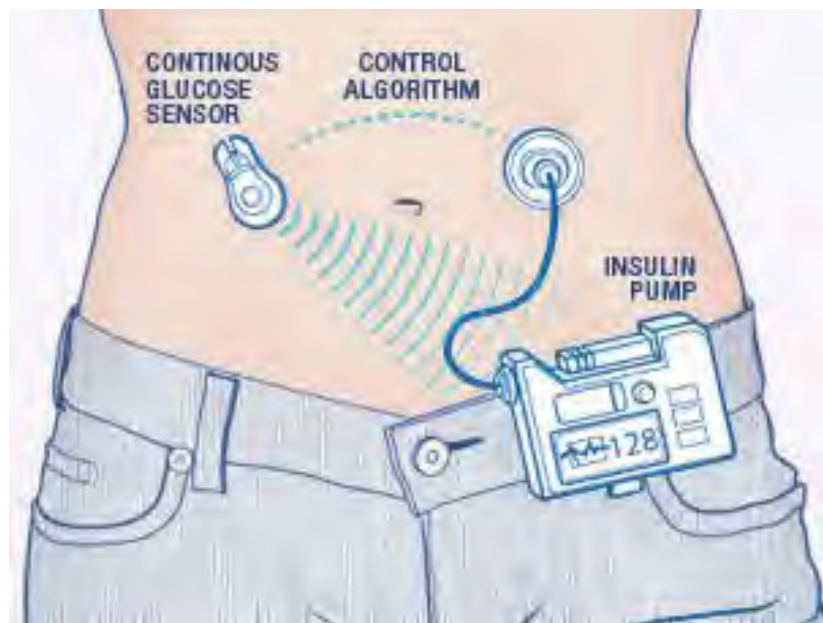
Quantity

Add to cart

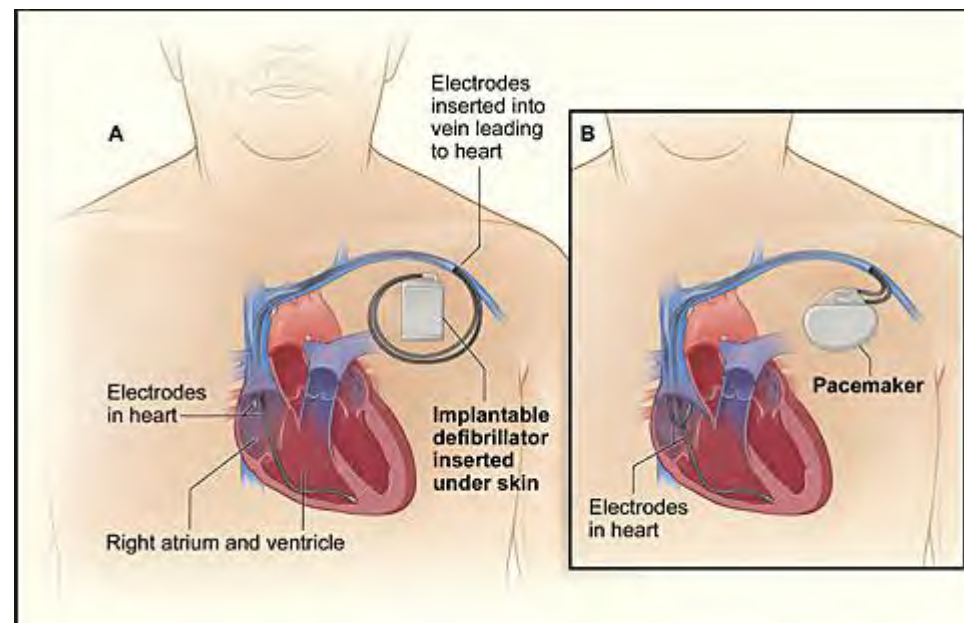


360UNICORNTTEAM

人体移植设备



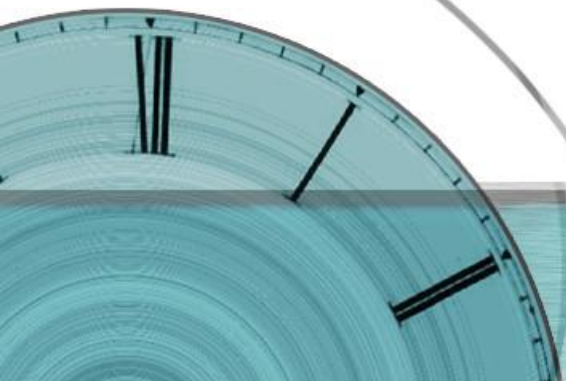
人造胰腺



植入型心率复除颤器



汽车无线控制



IC智能卡

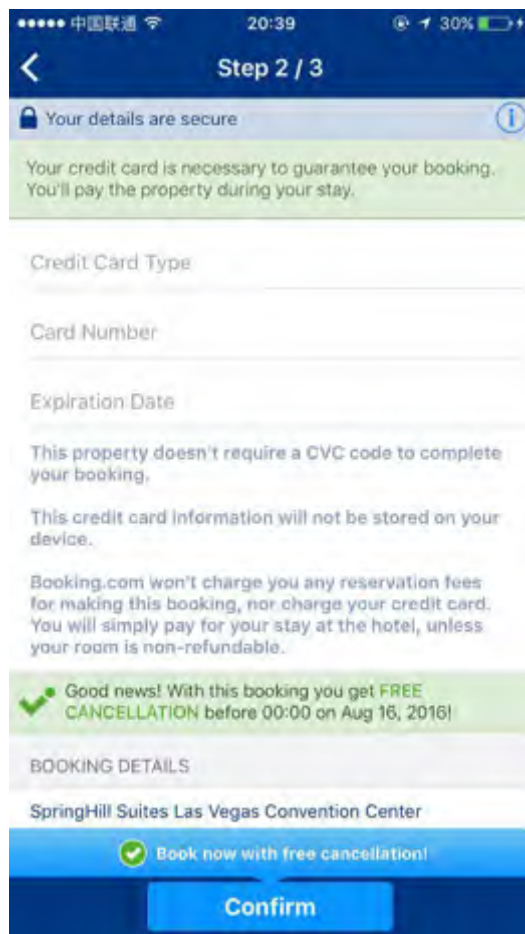


优酷



360UNICORNTTEAM

IC智能卡



芯片银行卡防护



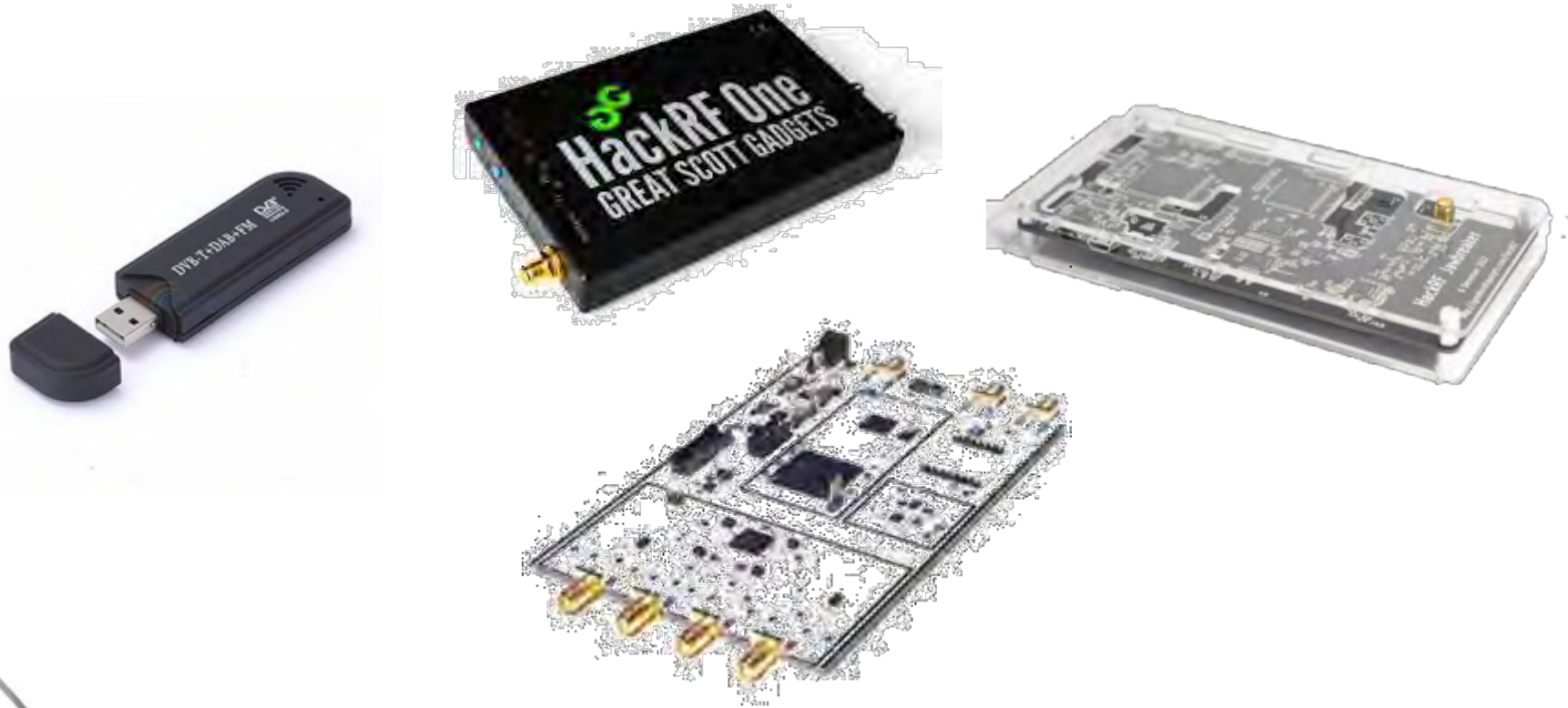
360UNICORNTTEAM

无线电逆向分析

- 短距离无线遥控系统
- 无线传感器
- 航空无线电ADS-B



分析工具——SDR

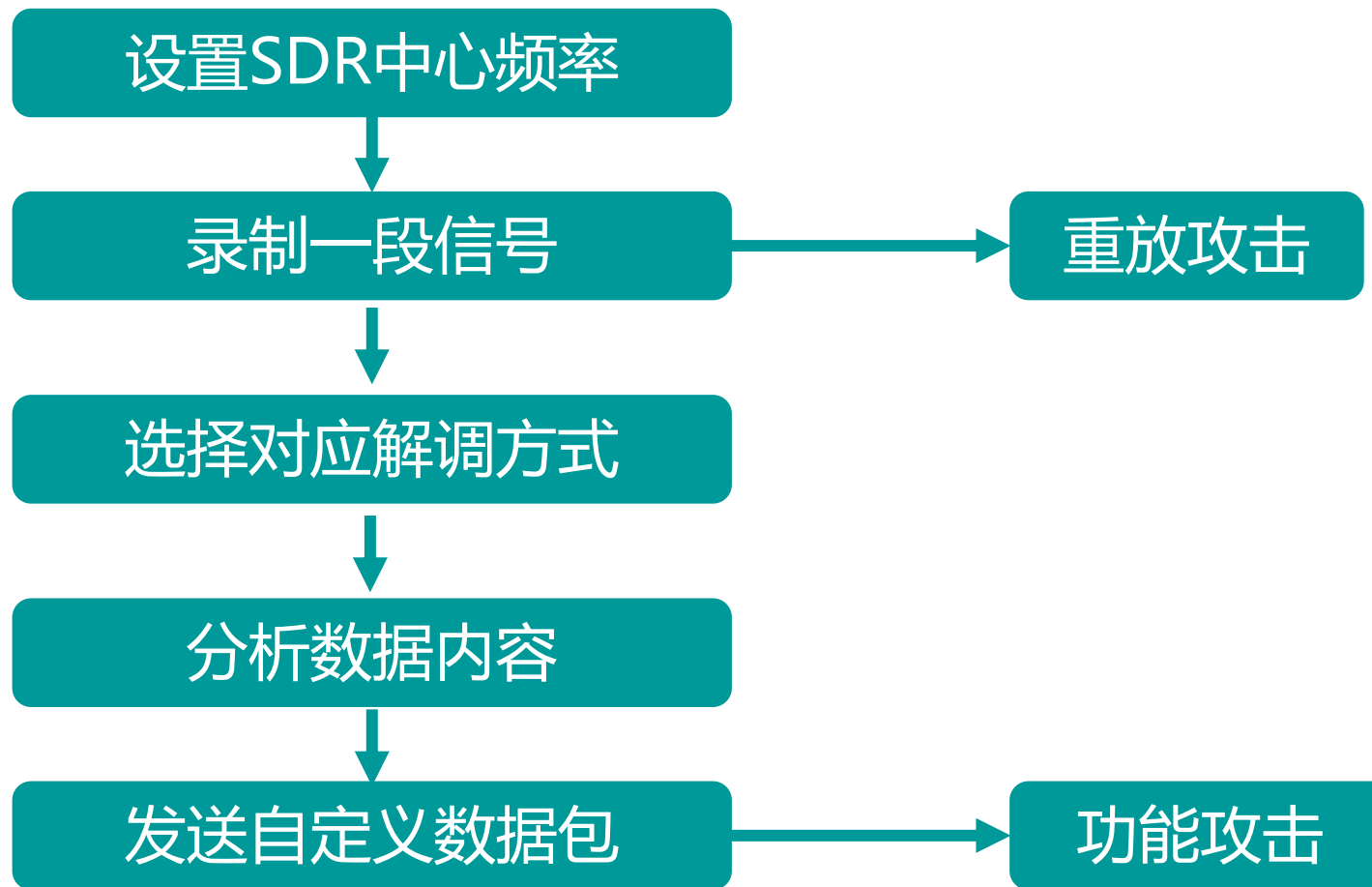


分析工具——SDR

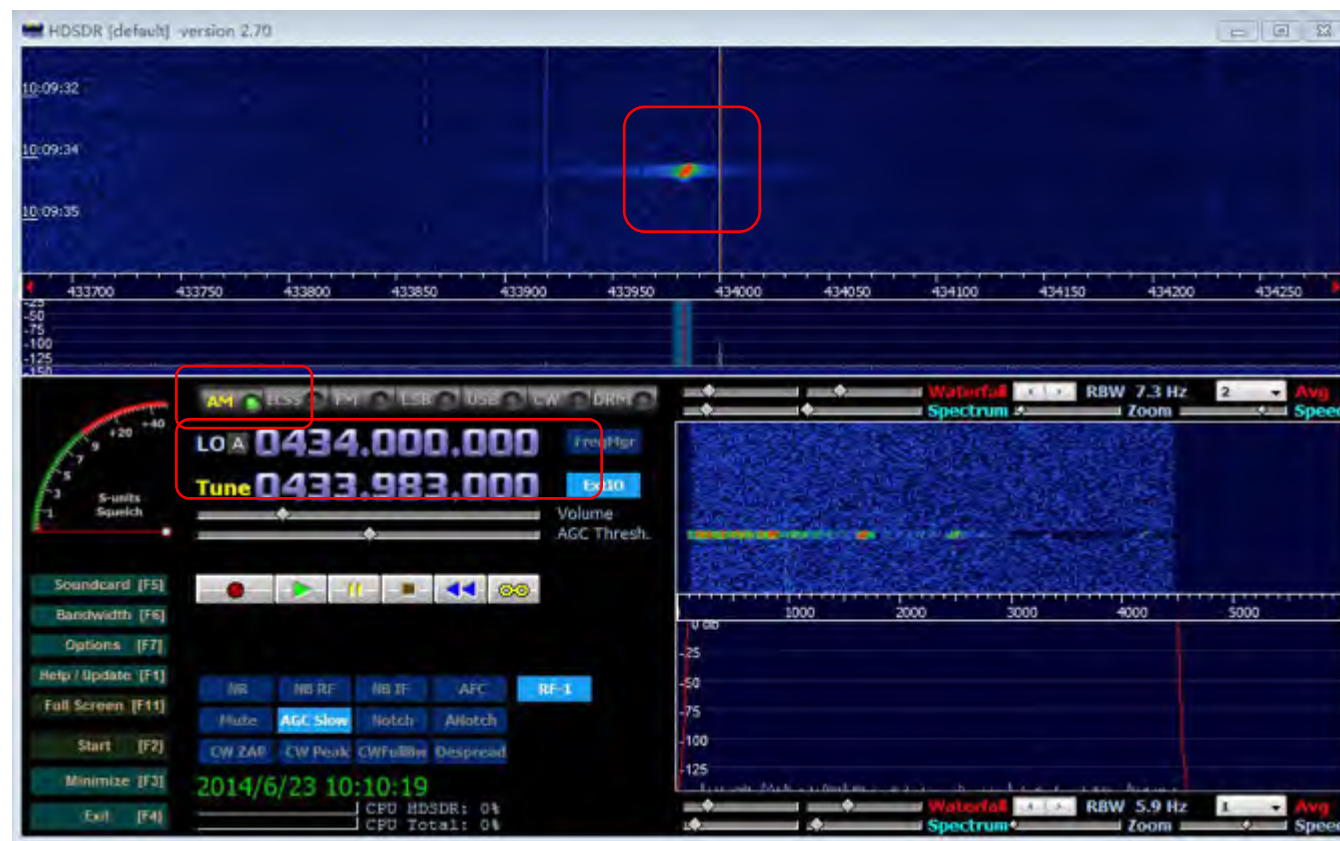
	RTL-SDR	H a c k R F bladeRF x40 One	U S R P B200mini	
频段	52M – 2.2 GHz	1M – 6GHz	300M – 3.8GHz	70M – 6GHz
带宽	2.56MS/s	20 MS/s	40MS/s	56MS/s
双工类型	只能接收	半双工	全双工	全双工
位宽	8-bit	8-bit	12-bit	12-bit
价格	\$20	\$300	\$420	\$675



无线电逆向分析流程



无线遥控信号

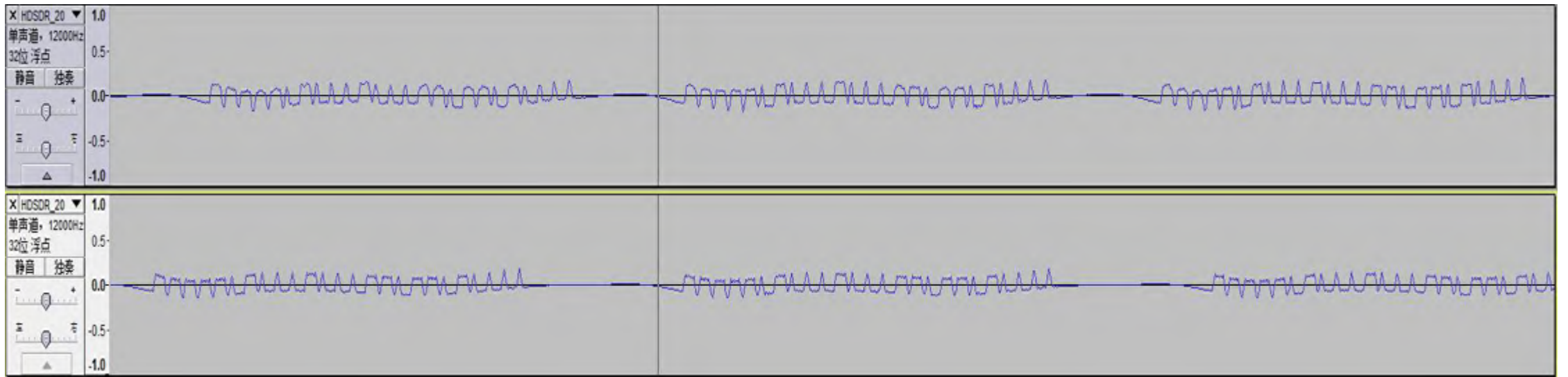


工具：电视棒
软件：HDSDR



360UNICORNTTEAM

无线遥控信号解调后波形图

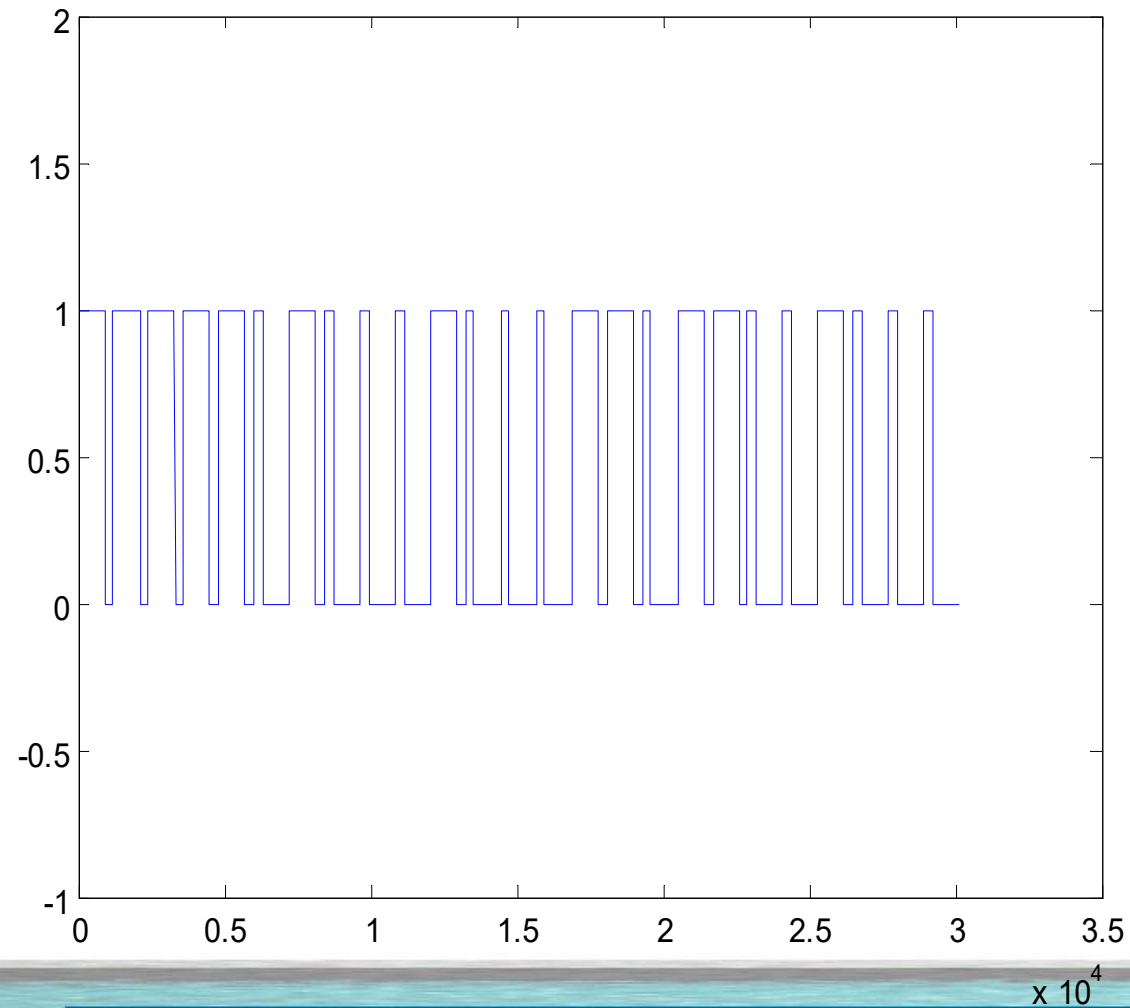


软件：Audacity



360UNICORNTTEAM

分析有效数据内容

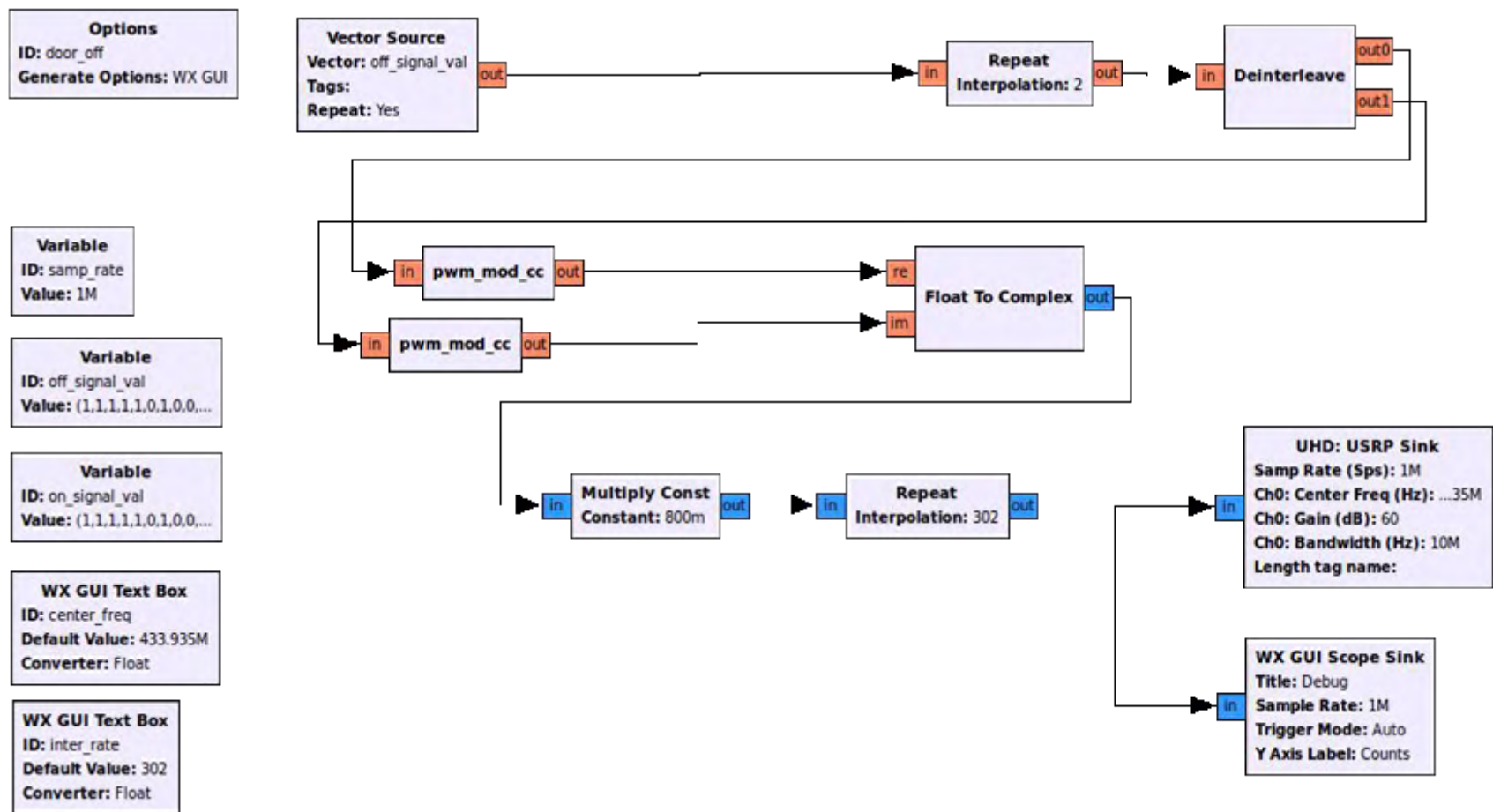


软件：MATLAB



360UNICORNTTEAM

流程图



软件：Gnuradio



手表抬杆

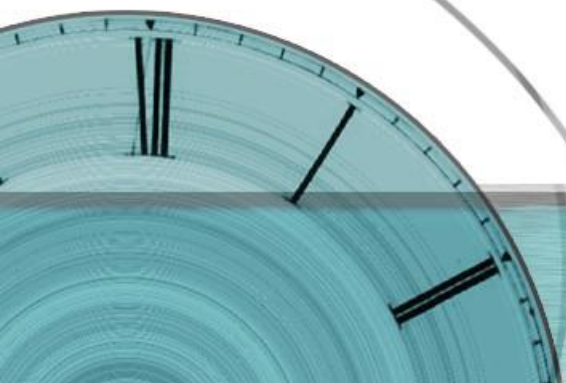


硬件：Chronos手表



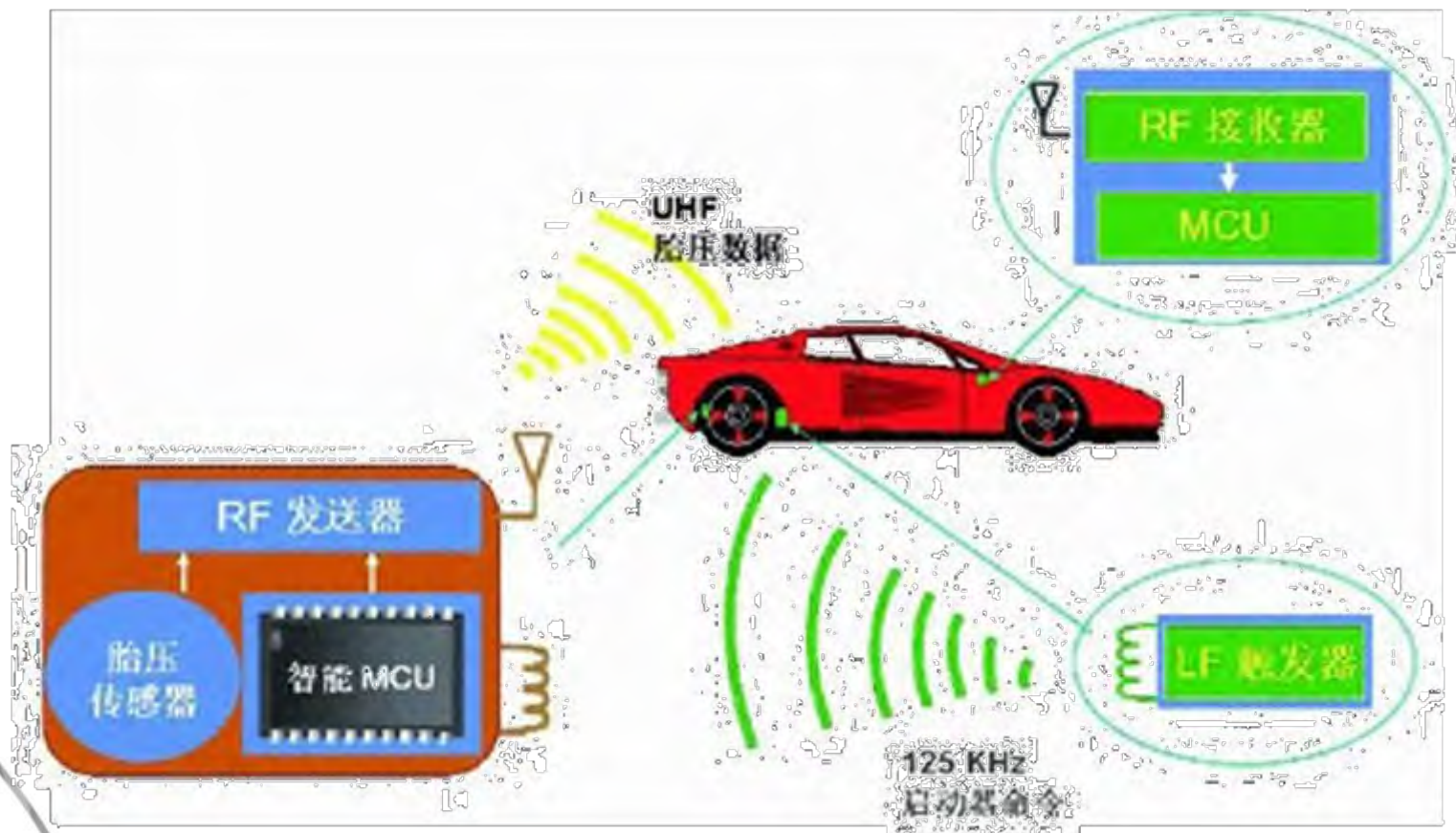
360UNICORNTTEAM

胎压报警器破解

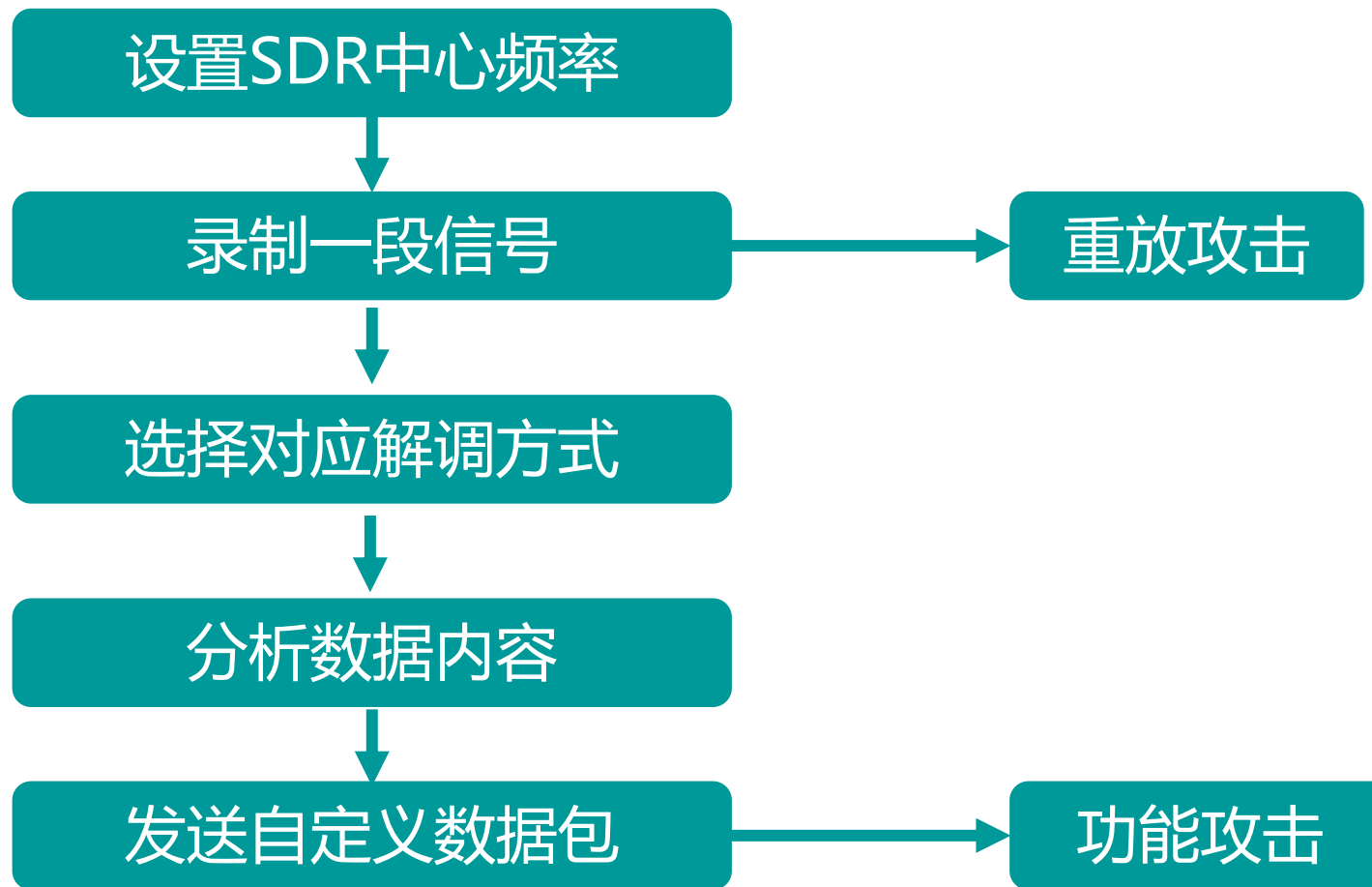


360UNICORNTeam

胎压报警器工作原理

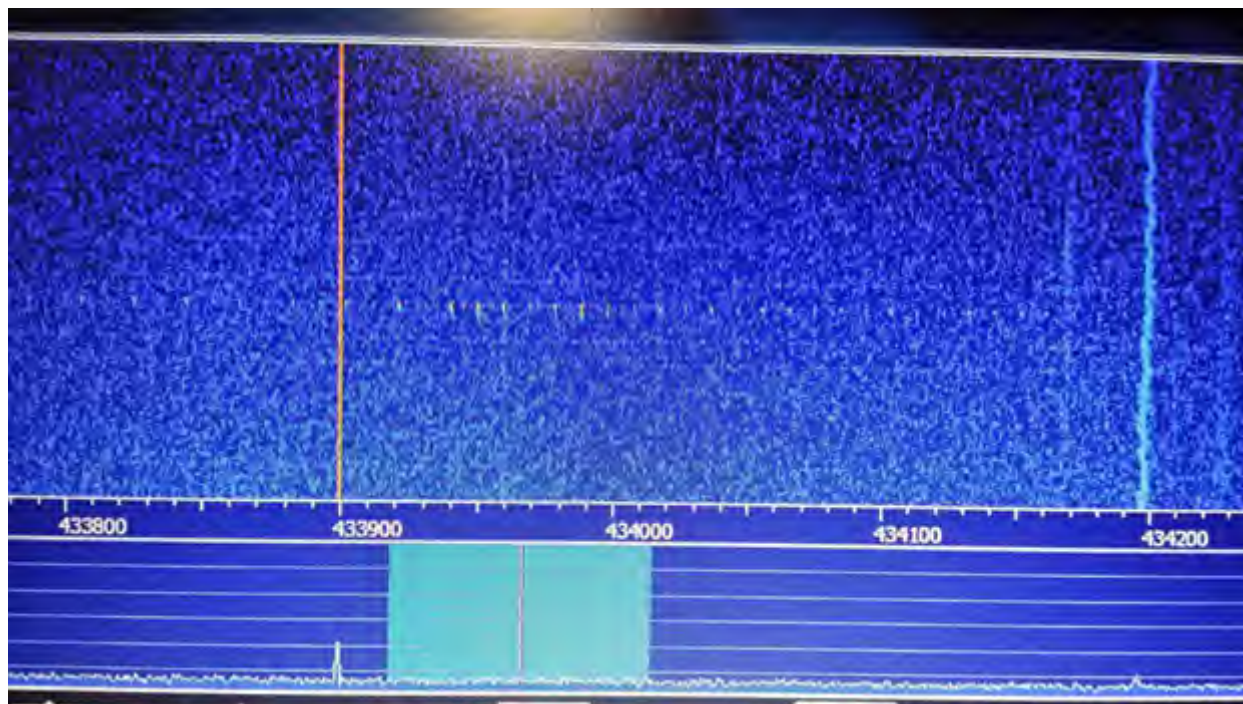


无线电逆向分析流程



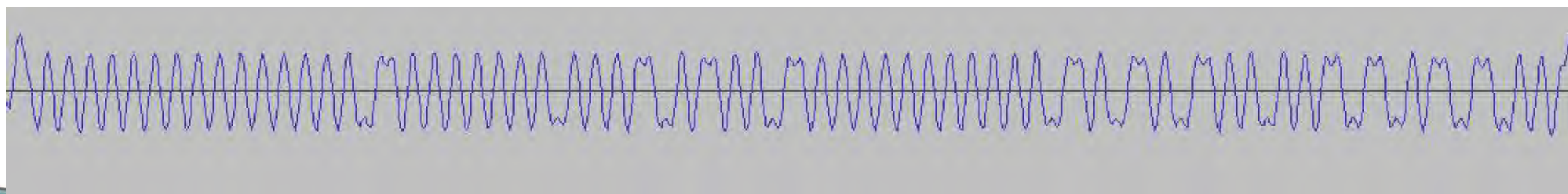
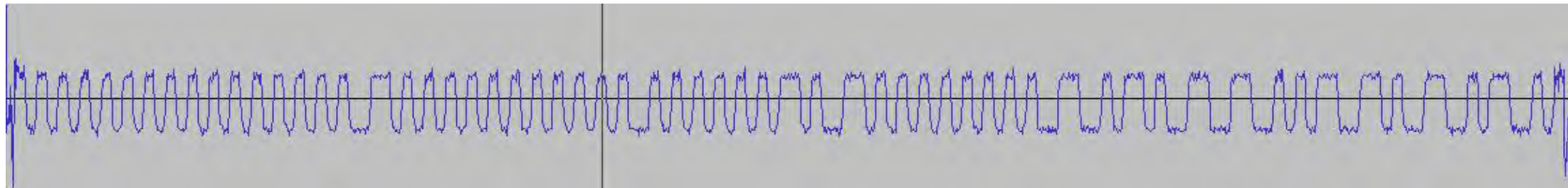
录制信号

- 中心频率 433.92MHz
- 解调：FM
- 比特率9.6Kbps

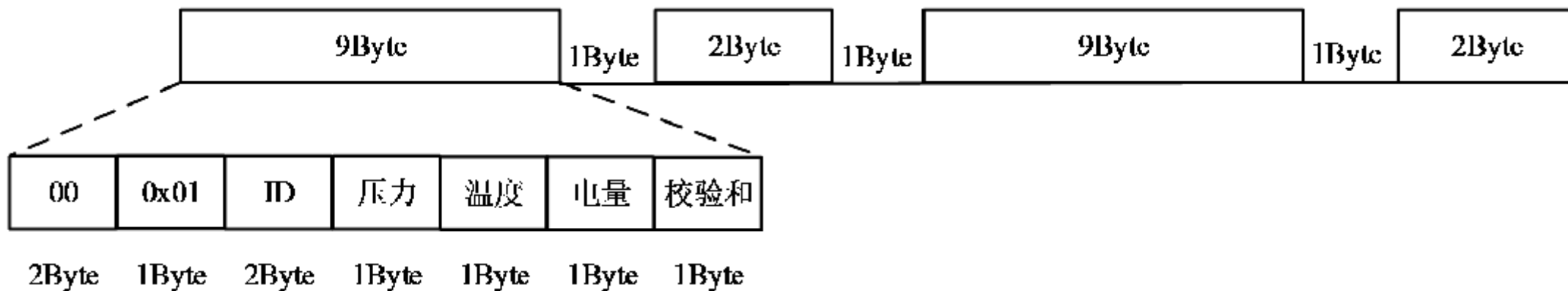


解调后的信号

- 前导码 + 有效码字



逆向分析数据包格式



- 11位有效比特
- LSB模式
- CRC校验 = 前6字节相叠加取低8位



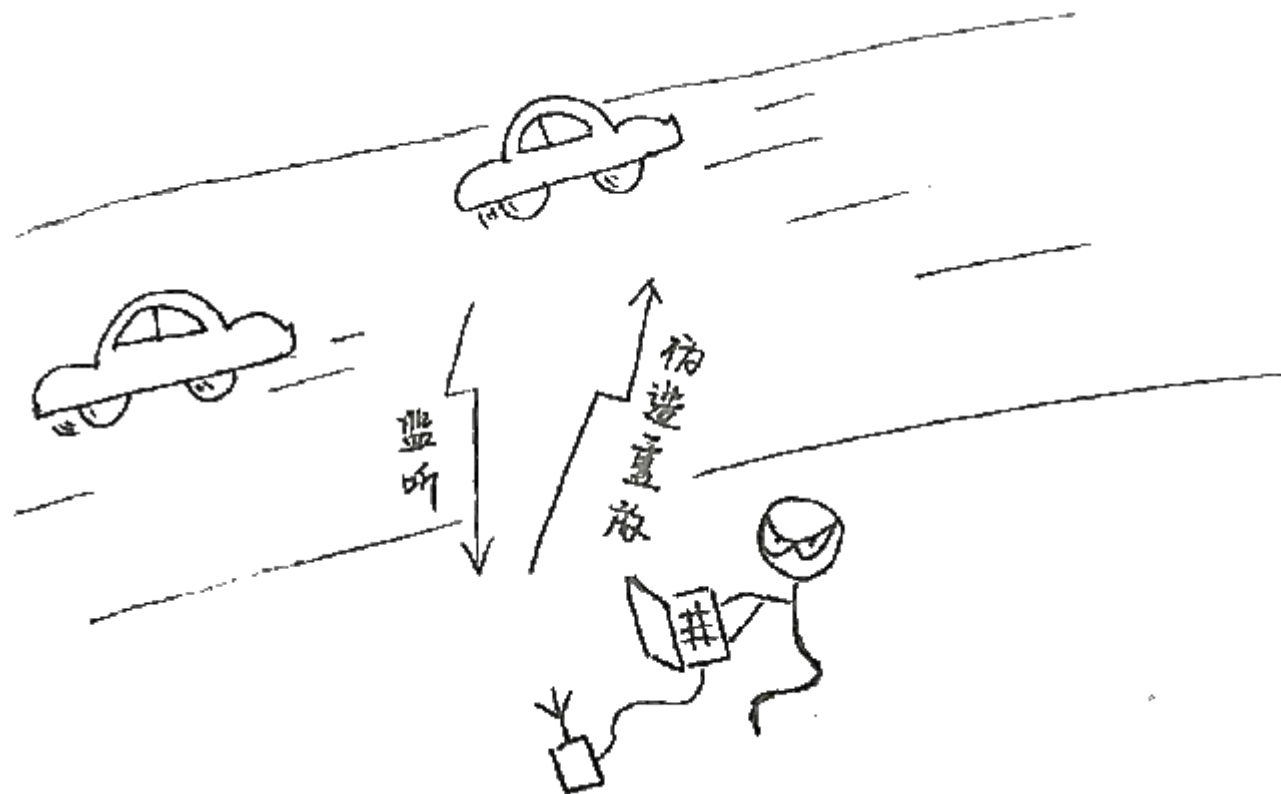
功能攻击效果



高压与低压攻击效果



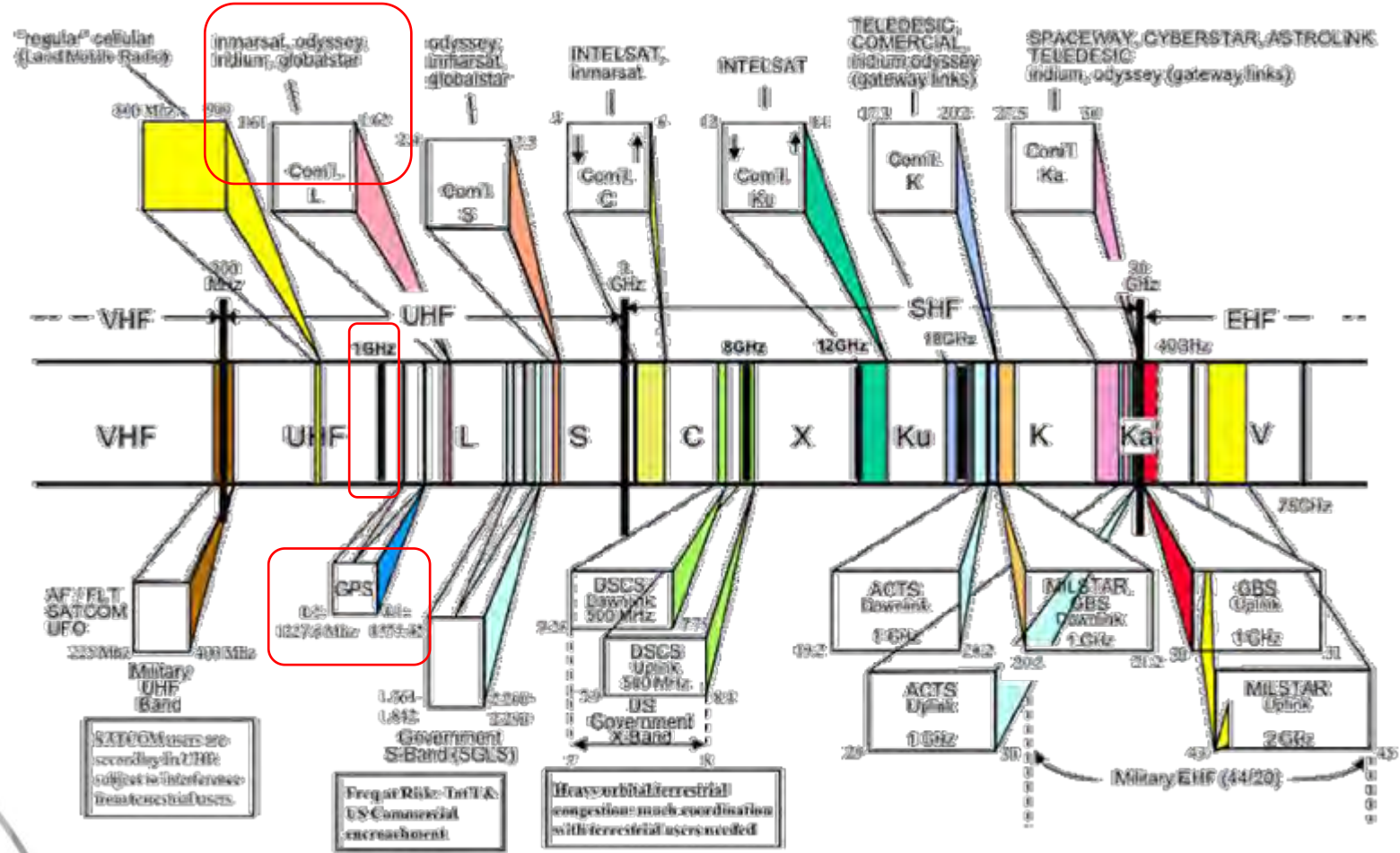
现实中的攻击情况



远距离无线电导航攻击



航空无线电导航攻击

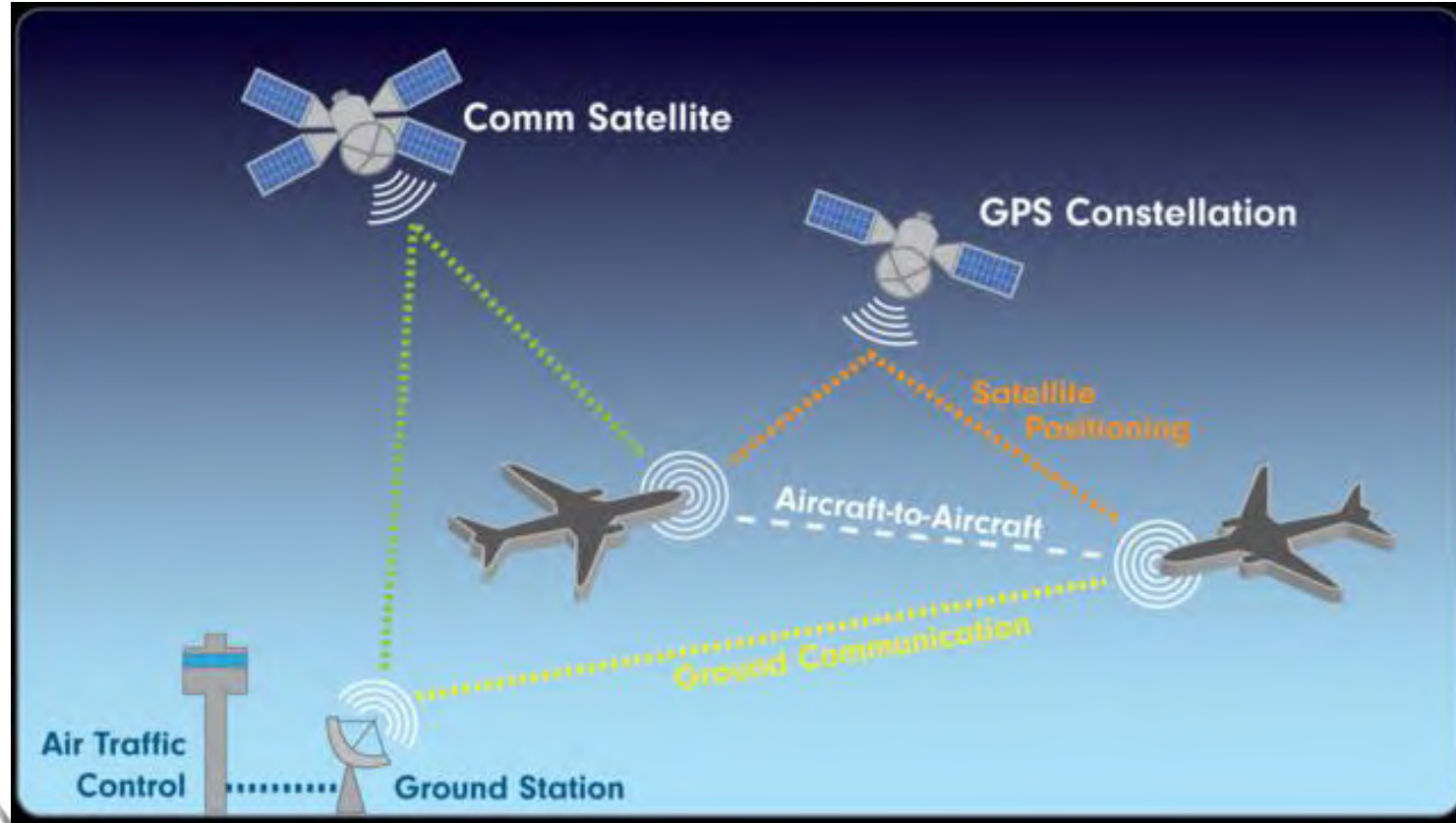


航空飞行涉及的无线电种类

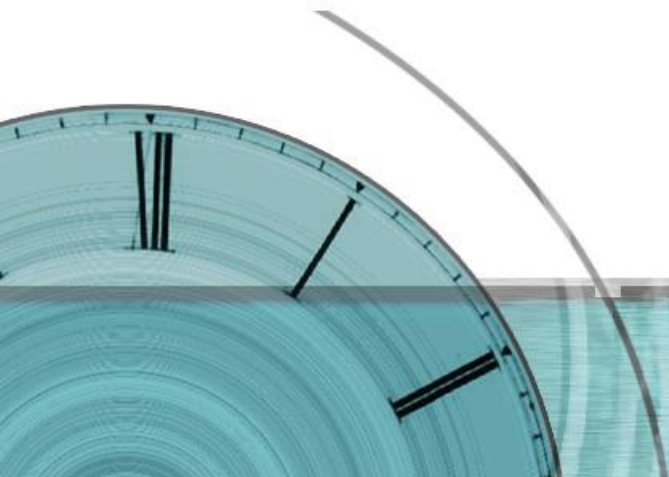
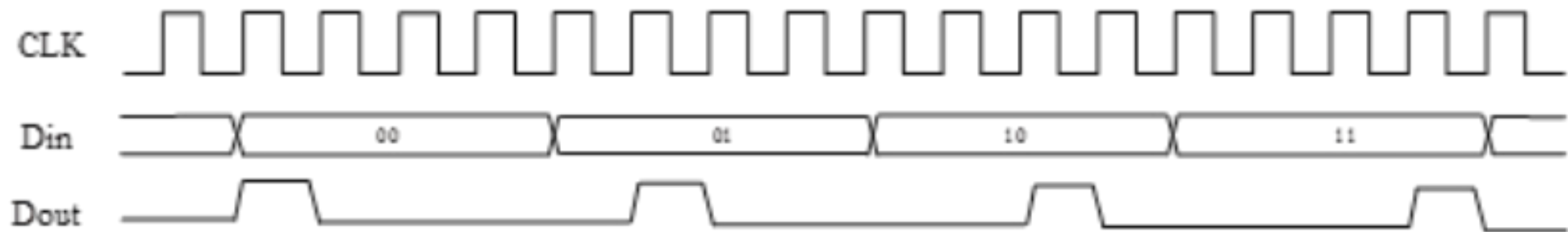
- **通信类：**用于飞机与飞机之间，飞机与地面之间的通信
- **导航类：**主要是卫星导航和地面信标导航



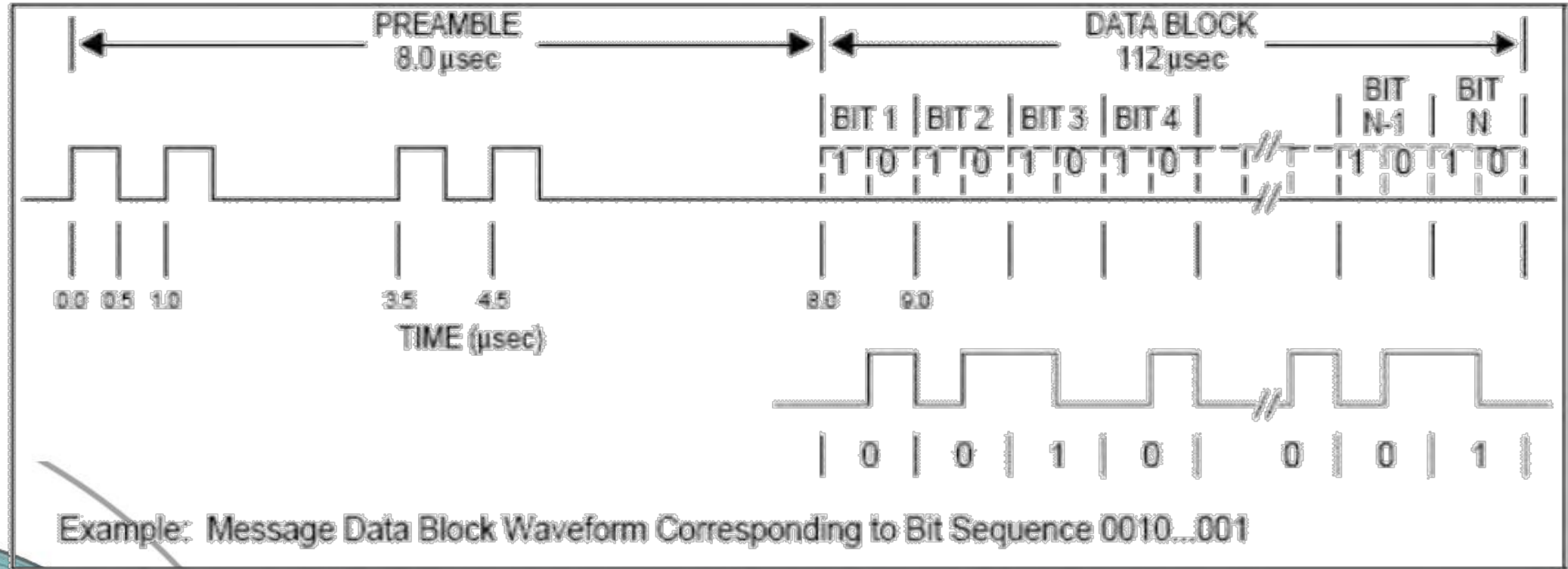
ADS-B 自动相关监视广播



调制方式PPM



ADS-B报文格式

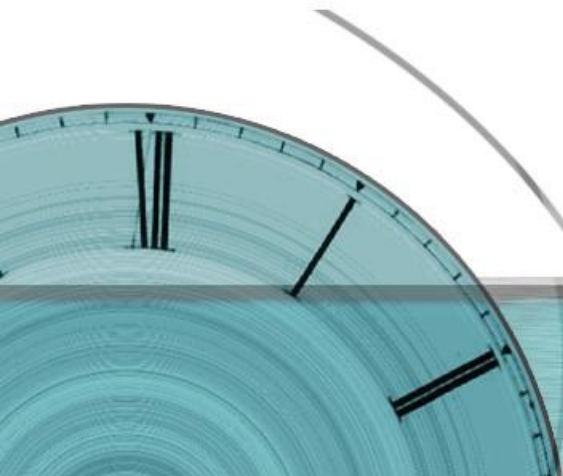


通过虚假的ADS-B信号构造出的飞机



攻防分析

<http://www.flightradar24.com>



360UNICORNTTEAM

更多无线电攻防案例请参考……



视频资料：www.ichunqiu.com



360UNICORNTeam

Thanks & Join us



KUANDI STUDIO 宽地摄影



360UNICORNTTEAM