
XDef 2013
第二届
全国网络与信息安全防护峰会
对话·交流·合作

基于软件无线电的
短程无线攻击分析与防护对策

安天实验室微电子与嵌入式研发中心
赵世平（TBsoft）

提 纲

- 短程无线通信
- 软件无线电简介
- 基于软件无线电增强对短程无线的攻击
- 软件无线电增强短程无线攻击的防范
- 结束语

短程无线通信

短程无线通信

- 已成为除3G、Wi-Fi之外的重要工业和物联网通信手段

- 遥控汽车钥匙
- 315MHz
- 433MHz

ISM频段

- ISM频段（工业、科学和医用频段）
  - 433MHz
  - 915MHz
  - 2.4GHz
  - 5.8GHz
- ITU-R（国际通信联盟无线电通信局）定义，免费使用。

短程无线通信特点

- 技术门槛和成本低
  - 315MHz（非ITU-R标准但国内应用广泛）和433MHz短程无线数字通信射频设计难度比收音机还低
    - 单管振荡器发射（国内上世纪80年代技术水平）
    - 单管超再生接收（国内上世纪70年代技术水平）
    - ASK（幅移键控）调制（类似电报）
  - 2.4GHz通信模块5.00元一个

短程无线通信特点

- 通信数据量小
  - 几字节、几十字节到几百字节
- 通信时间短（1s以下）
  - 尽管某些短程无线通信速率很低，但数据量小。
- 通信频点多、调制方式各异
  - ASK、FSK、GFSK……

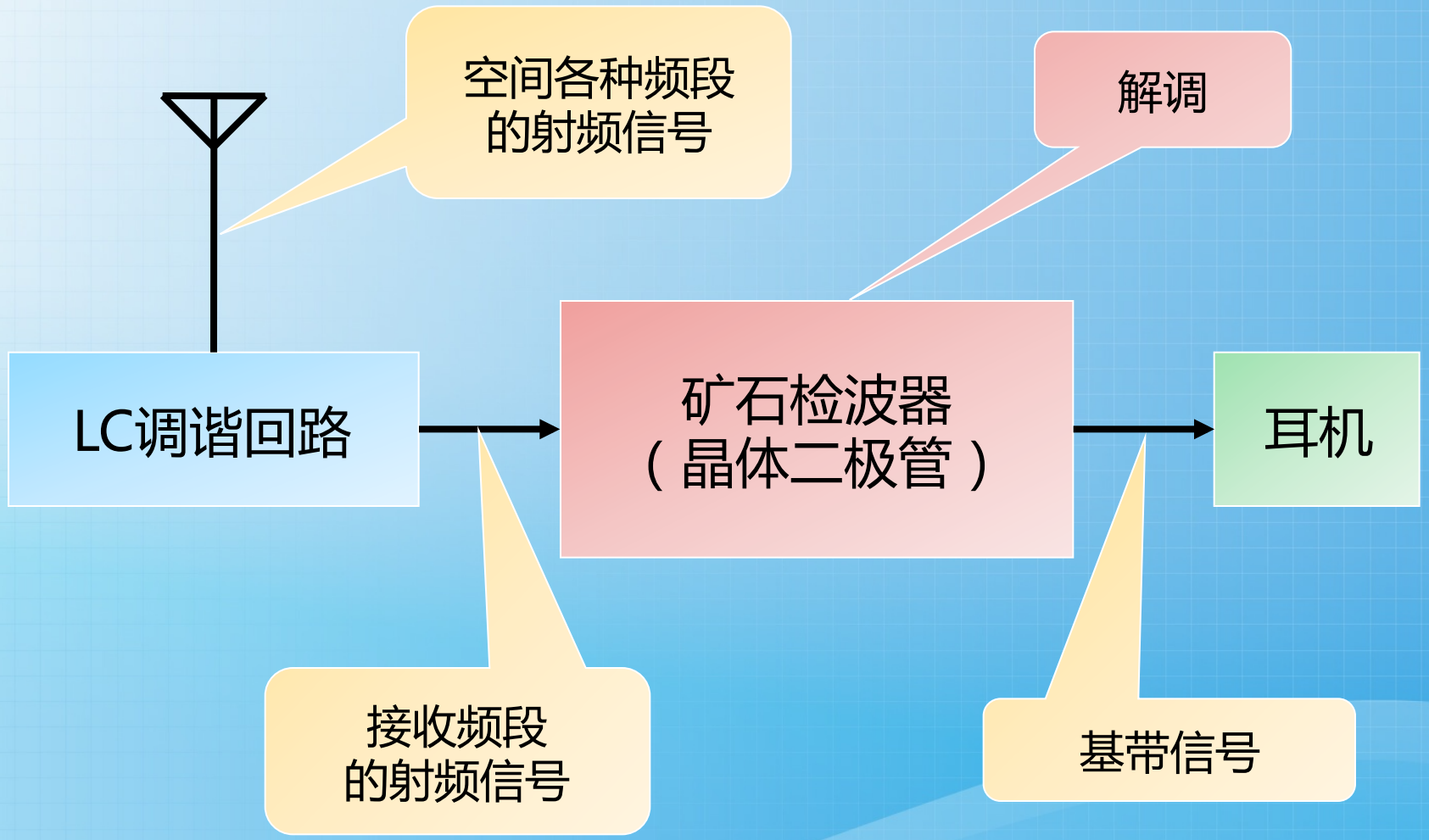
软件无线电简介

矿石收音机

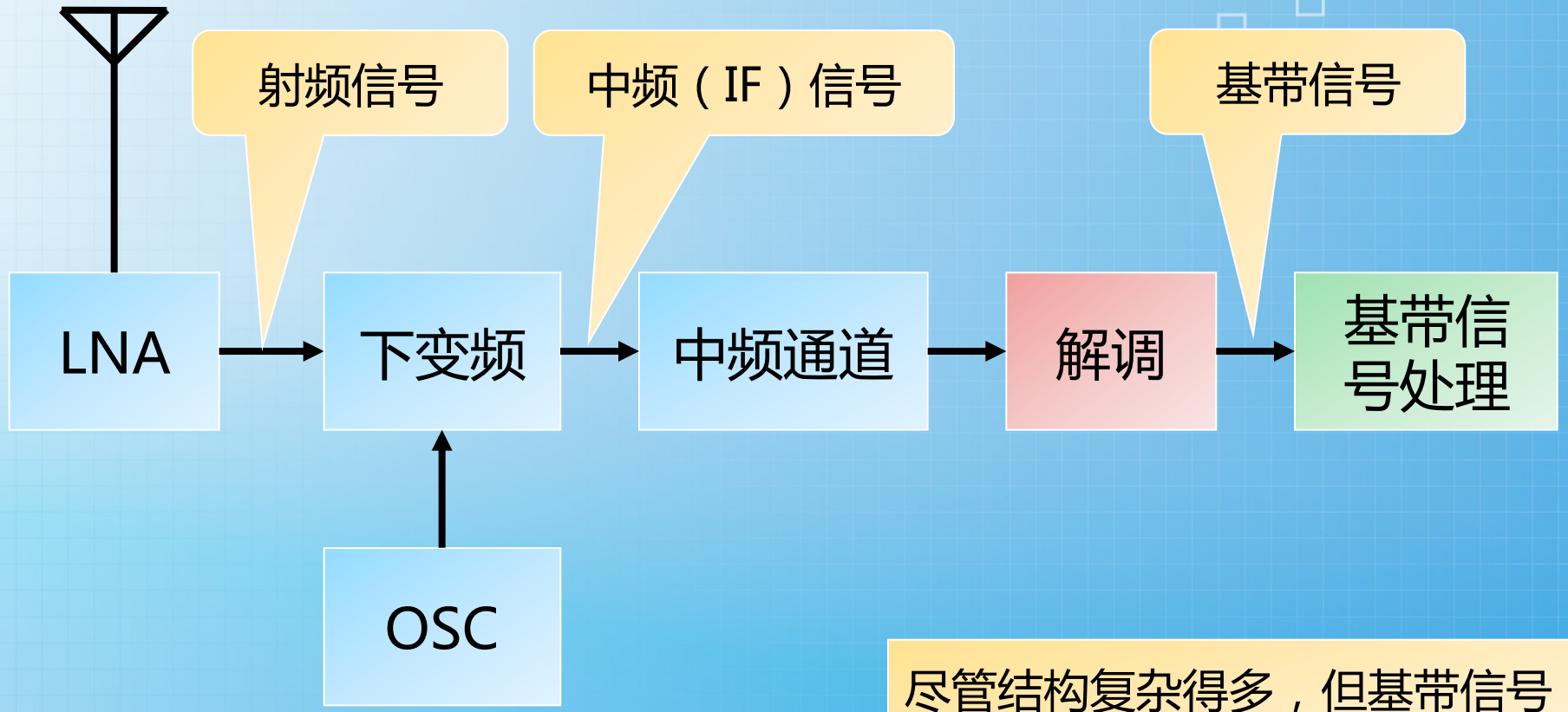
最古老的收音机

上世纪50—60年代中国最流行的DIY

矿石收音机的原理



现代超外差接收机的原理



尽管结构复杂得多，但基带信号处理之前仍然全部是模拟电路。

软件无线电的出现

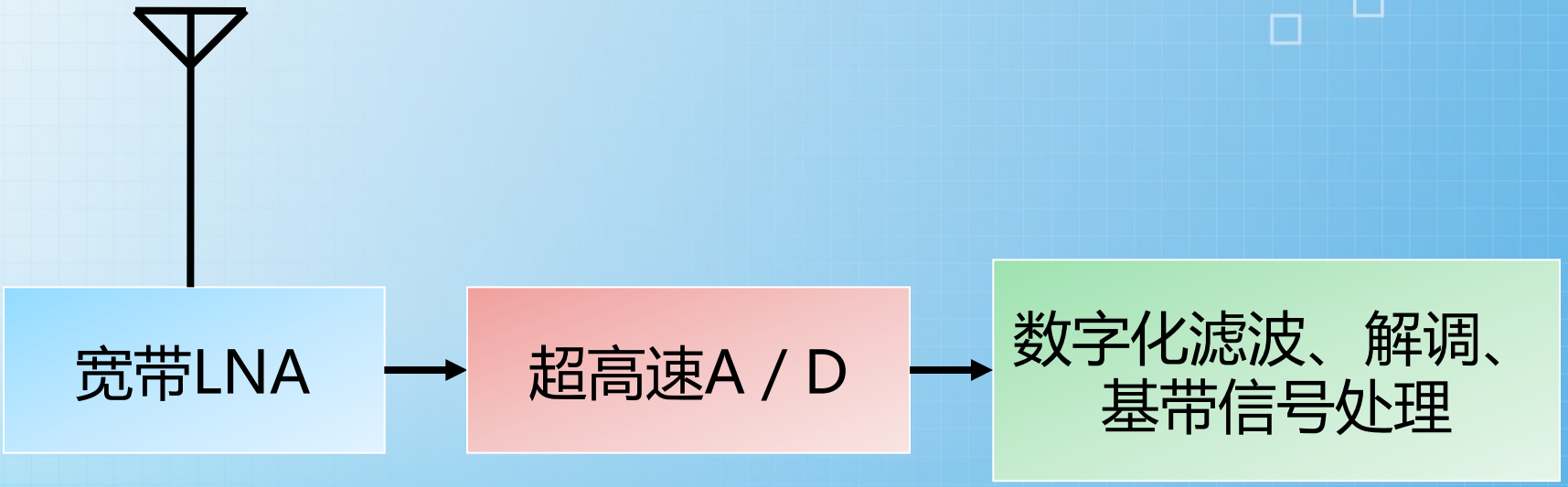
现代超外差接收机存在的问题

- 射频、中频和解调部分仍然依靠模拟电路
- 选频和抗干扰仍然依靠模拟滤波器——LC回路、陶瓷滤波器、石英晶体滤波器等
- 性能难于进一步提升
- 超外差接收机自身存在的问题——组合频率干扰等

如何彻底解决这些问题？

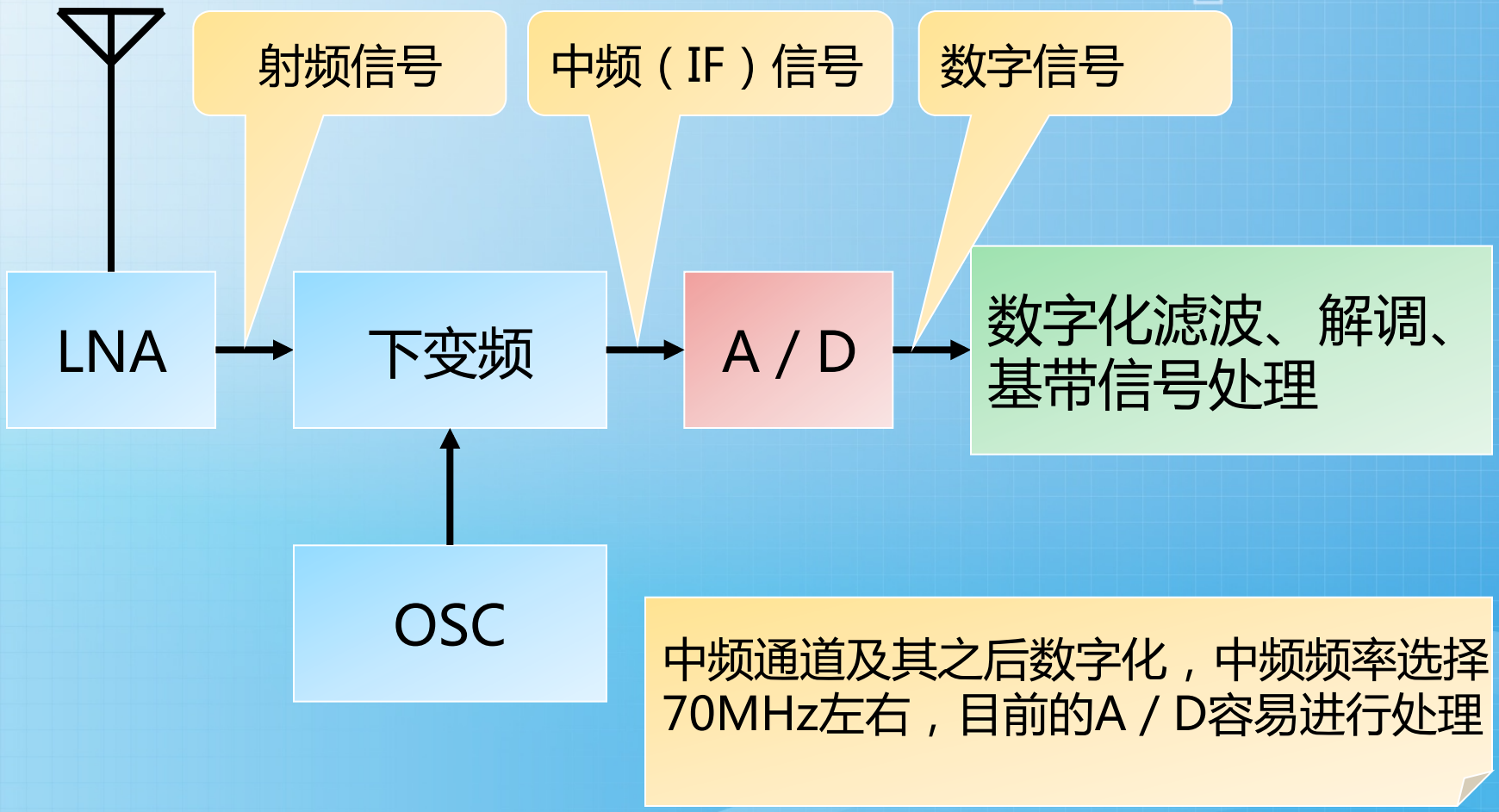
- 软件无线电——将射频信号数字化后处理

理想的软件无线电接收机实现



超高速A / D对于300MHz频段以上的射频信号不容易实现，目前不现实。

目前实际的软件无线电接收机实现



软件无线电核心技术

硬件技术

- 高速A / D
- DSP处理器
- 可编程逻辑器件（FPGA等）

软件技术

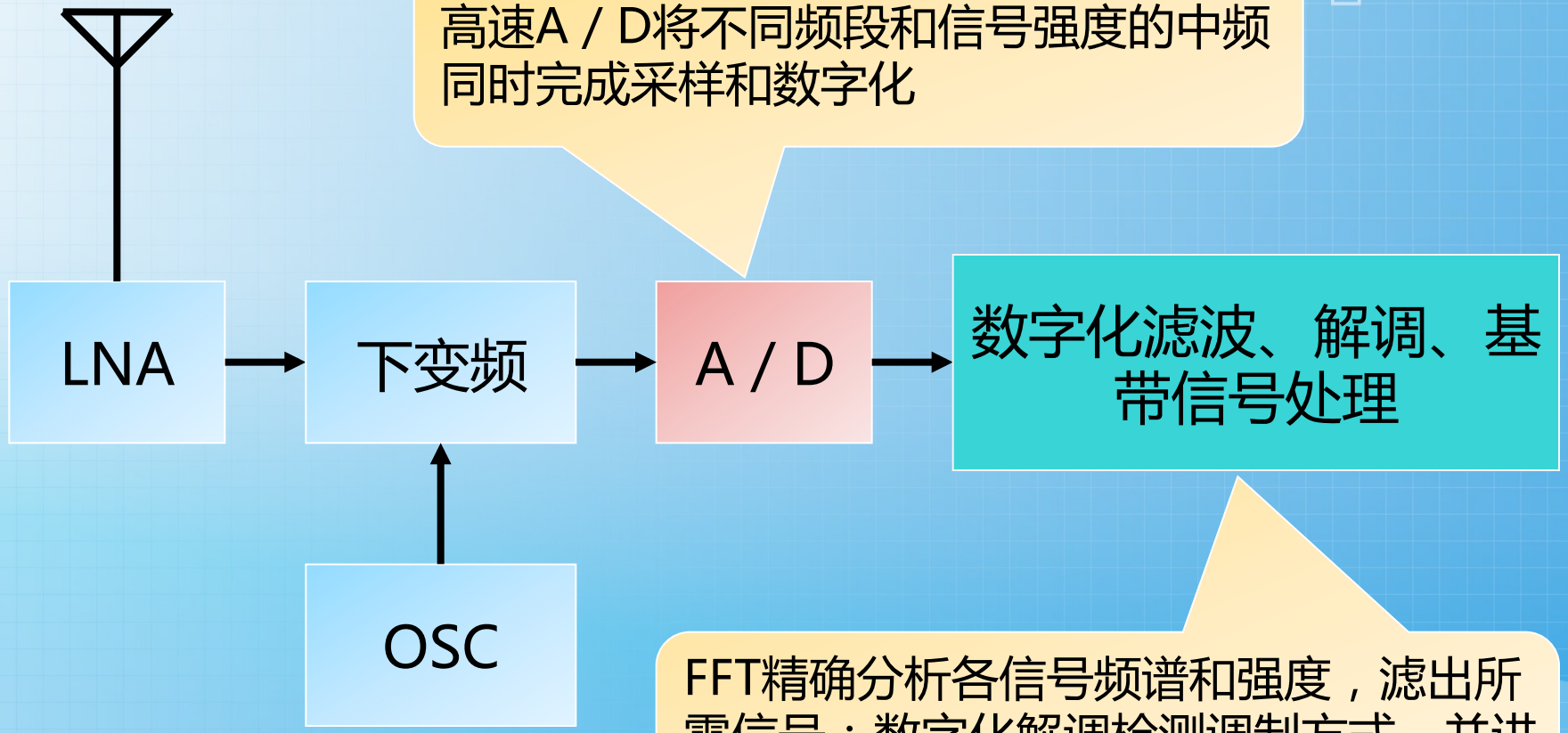
- 数字滤波（FFT、小波等）
- 数字变频
- 数字调制与解调

基于软件无线电增强对短程无线的攻击

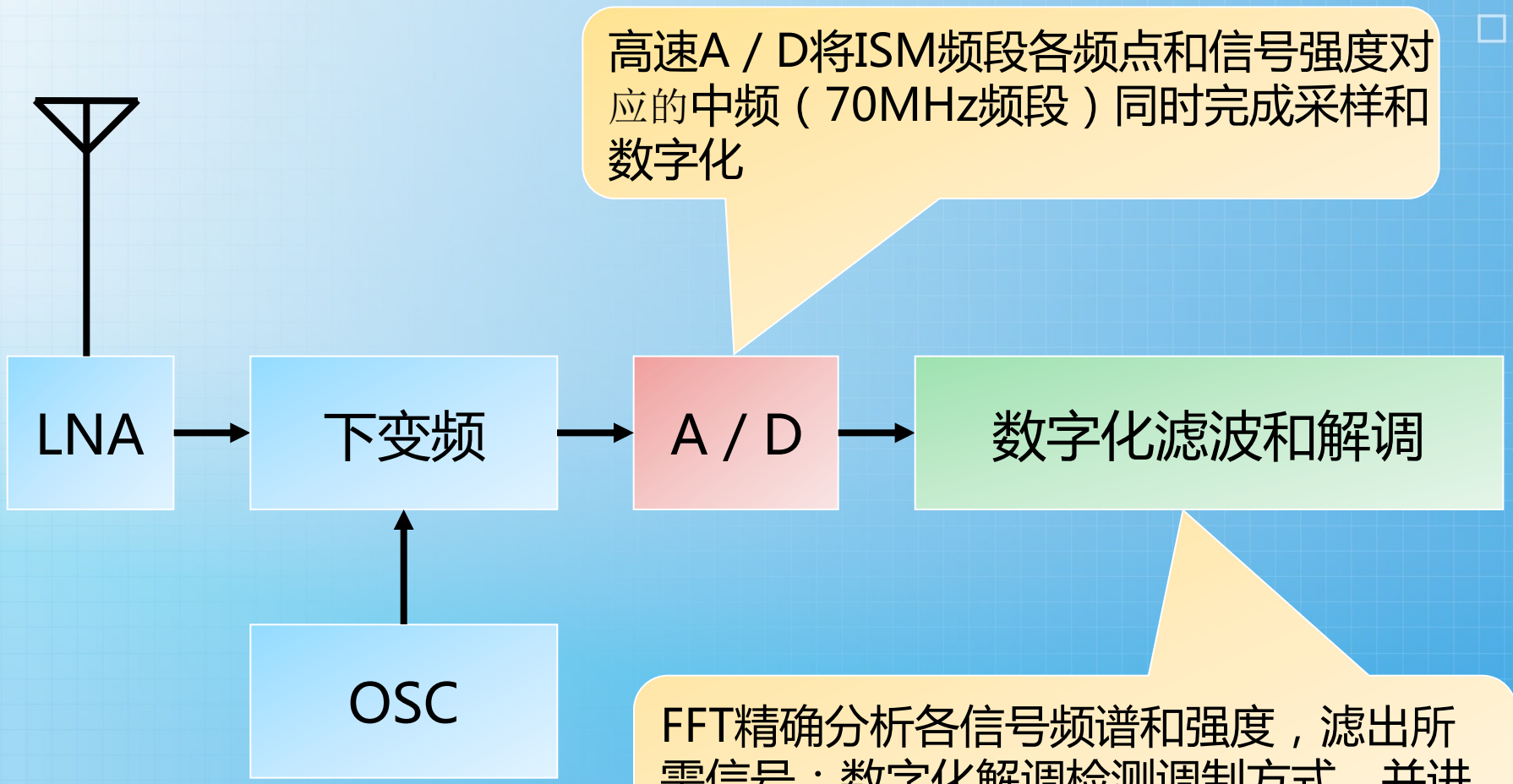
针对无线通信的攻击存在的难点

针对短程无线通信的攻击存在的难点

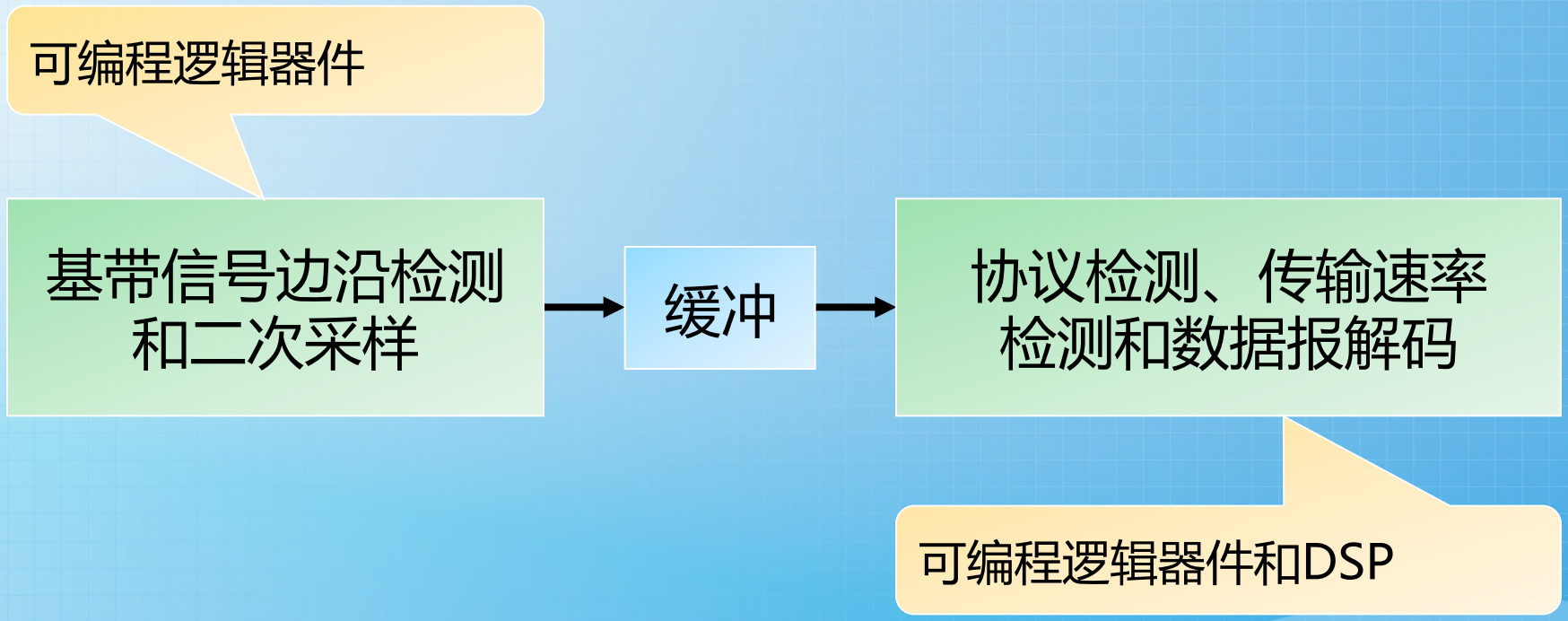
使用软件无线电克服这些难点



使用软件无线电处理ISM频段射频和中频



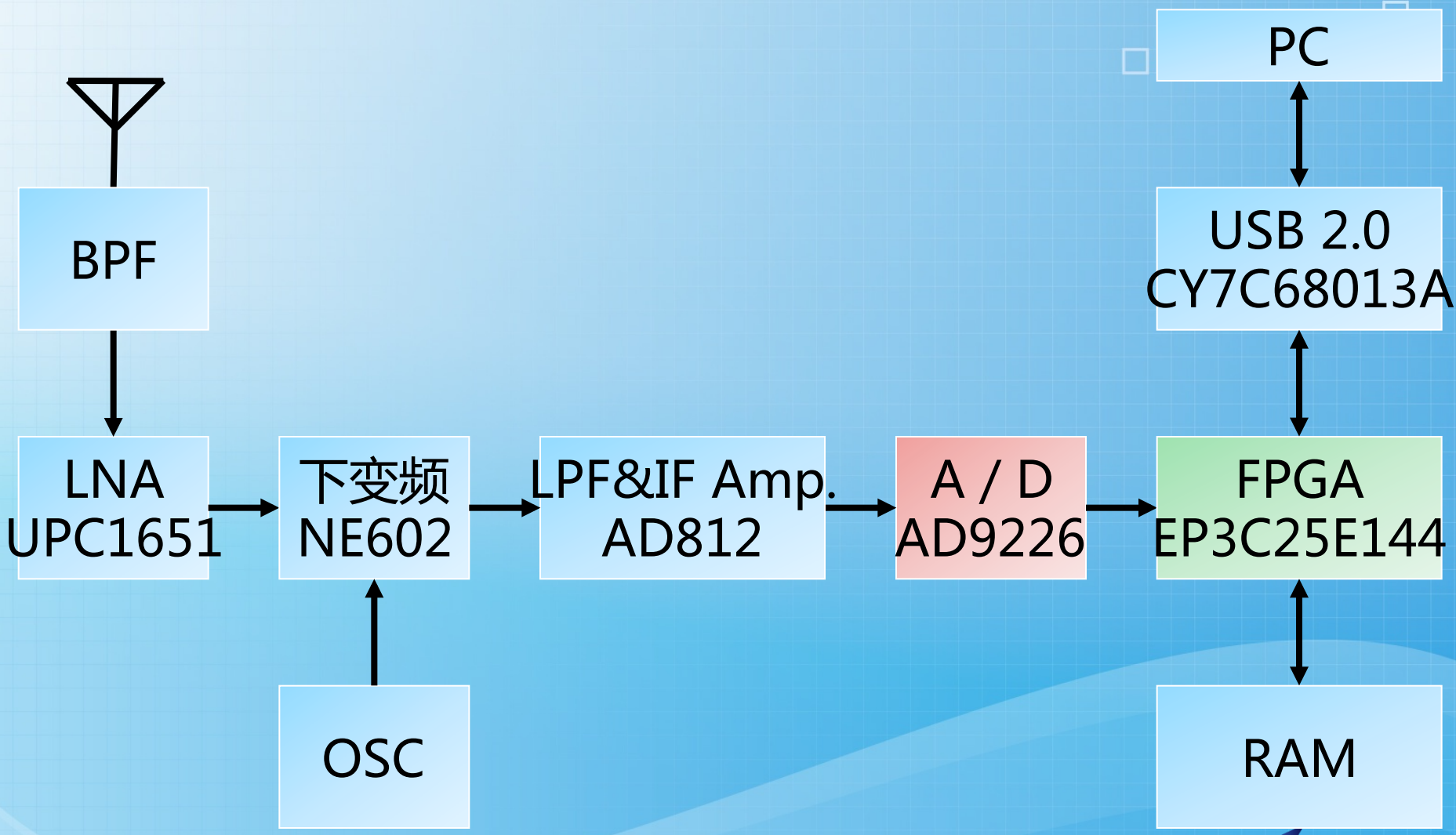
再配合数字化基带信号处理



“不从轮子做起”的方法

- GNU Radio
  - http://gnuradio.org
  - 硬件
  - 软件

“从轮子做起”的方法（433MHz ISM）



软件无线电增强短程无线攻击的防范

软件无线电增强短程无线攻击的防范

- 猝发通信、跳频通信等传统手段对软件无线电无效
- 单一设备监听混杂短程无线通信信号成为可能
- 智能天线和空分多址（SDMA）手段抗监听仍然有效
- 单向通信、明码通信等不应再应用于短程无线通信

结束语

新技术使得短程无线通信安全性面临挑战

- 软件无线电应用的推广和廉价化
- 不要认为“一瞬间”的短程无线通信是安全的
- 明码通信和无法会话验证的单向通信是安全大敌
- 通信信道安全中的“桶板效应”，99%信道安全，1%信道不安全，安全性就由1%决定。

谢谢大家！

tbsoft@antiy.com