RADIO ATTACKS ON NFC, GPS, AND MOBILES

Tomáš Rosa, Ph.D., OK1SFU

http://crypto.hyperlink.cz

SDR
SOFTWARE-DEFINED RADIO

SAMPLING THEOREM

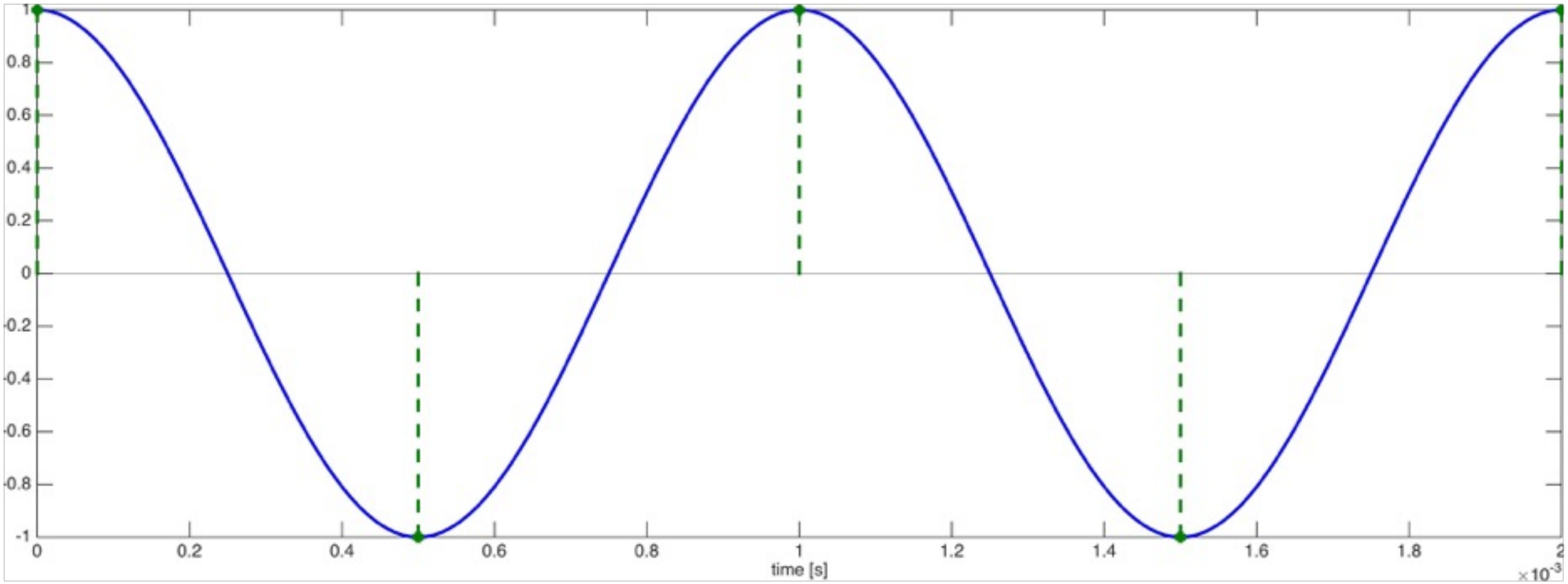
- Let $s(t)$ be a *Fourier-integrable* signal having its highest *non–negligible* frequency $|f_{\max}| < f_s/2 = 1/2T_s$.

- Such $s(t)$ can be then fully reconstructed from its discrete-time samples as:

$$s(t) = \sum_{k=-\infty}^{\infty} s(kT_s) \frac{\sin \pi\left(\frac{t-kT_s}{T_s}\right)}{\pi\left(\frac{t-kT_s}{T_s}\right)} = \sum_{k=-\infty}^{\infty} s(kT_s) \operatorname{sinc}\left(\frac{t-kT_s}{T_s}\right)$$

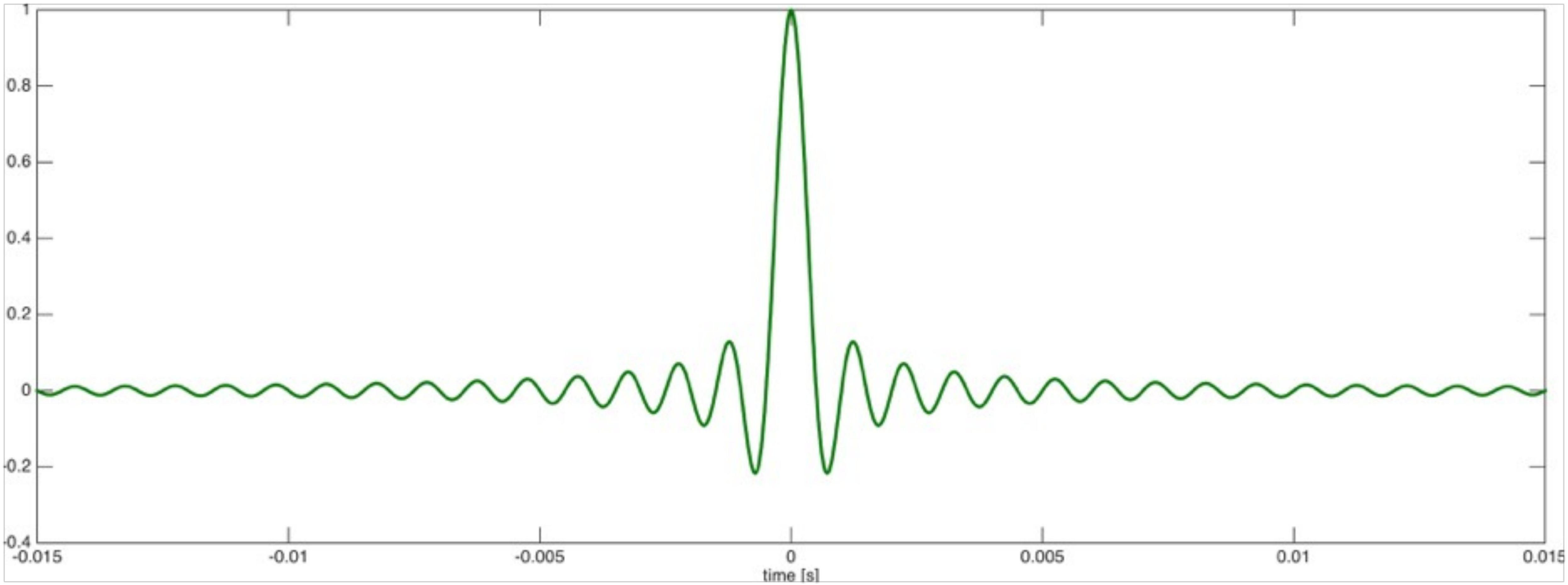
— Kotelnikov, Nyquist, Shannon, Whittaker

NYQUIST RATE SAMPLING



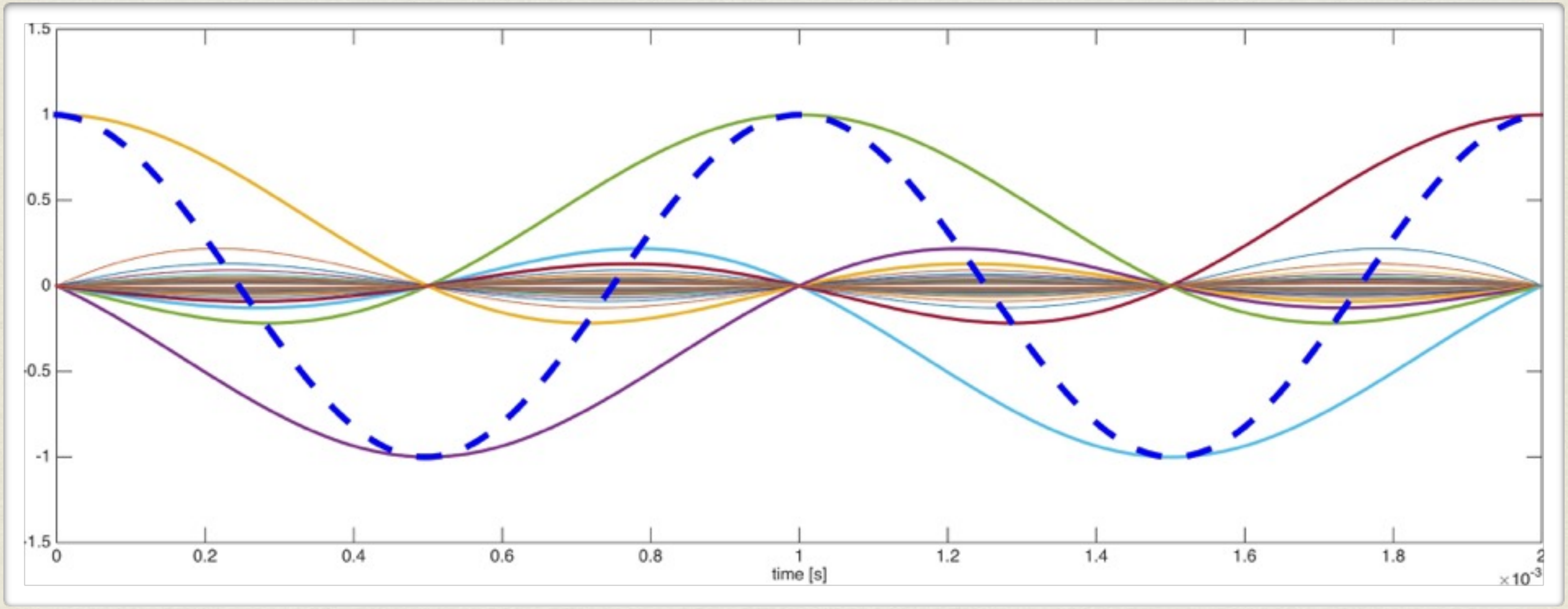
1 kHz @ Nyquist sample rate $f_s = 2$ kHz

SINUS CARDINALIS



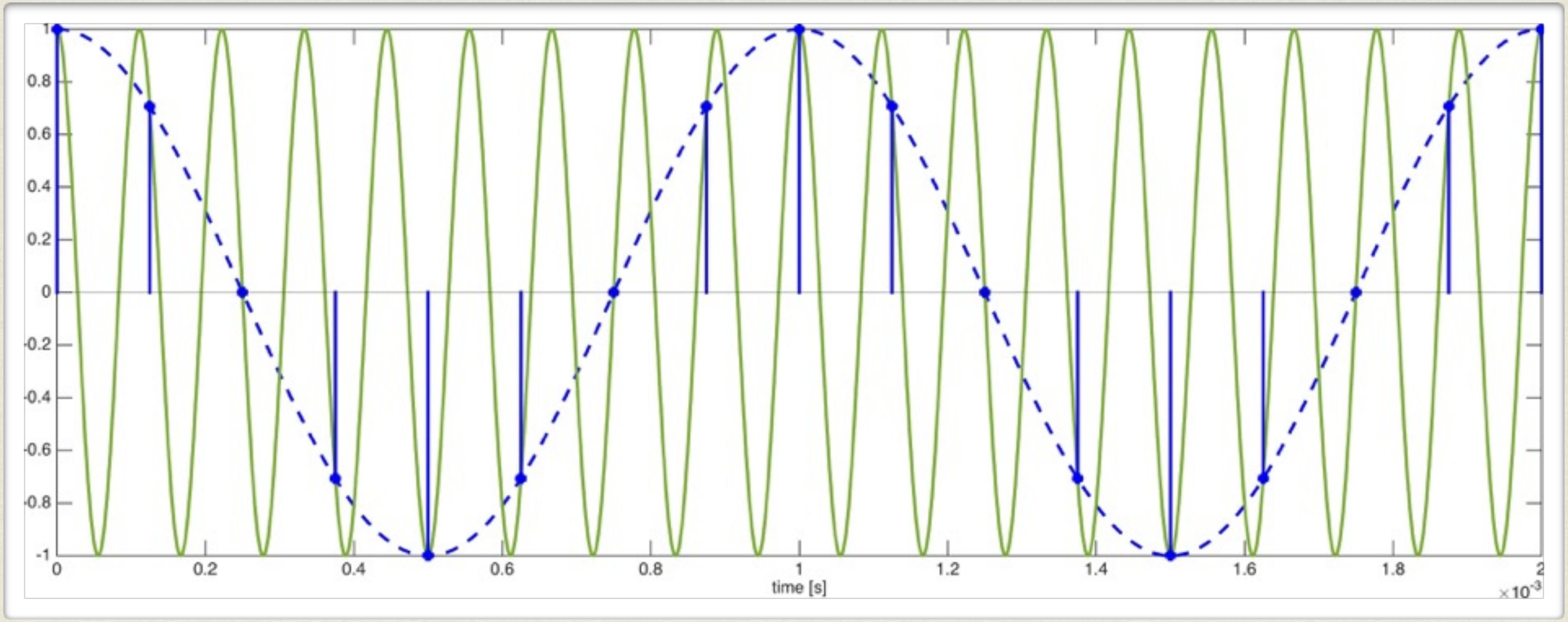
in lowpass filter impulse response scale @ 1 kHz

INTERPOLATION



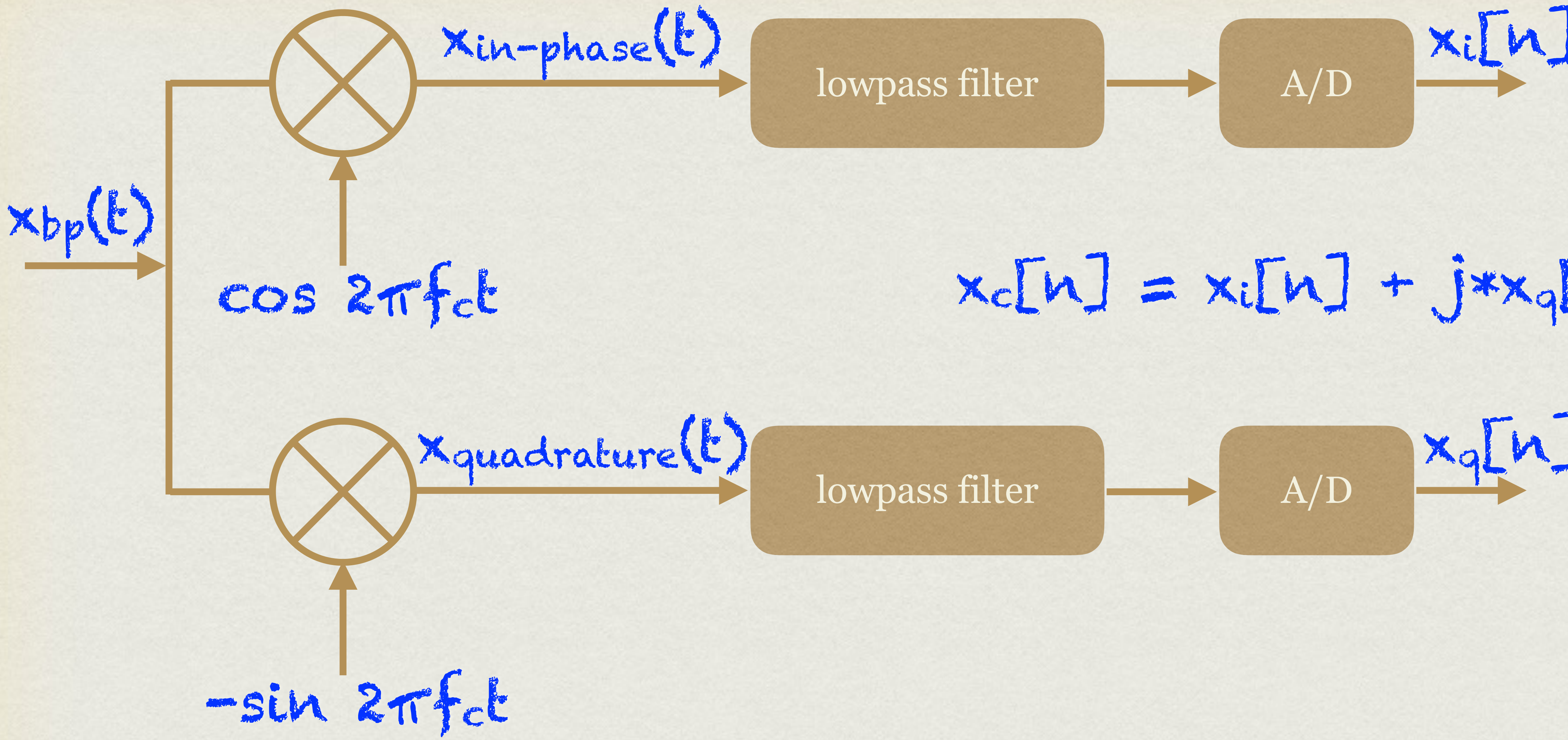
1 kHz recovered @ f_s = 2 kHz with 30-sample delay

ALIASING EXAMPLE



9 kHz -> 1 kHz @ sample rate f_s = 8 kHz

QUADRATURE SAMPLING



$$x_c[n] = x_i[n] + j * x_q[n]$$

bandpass complex signal sampling at $f_s = B$

cf. [Lyons, 2011] for excellent explanation

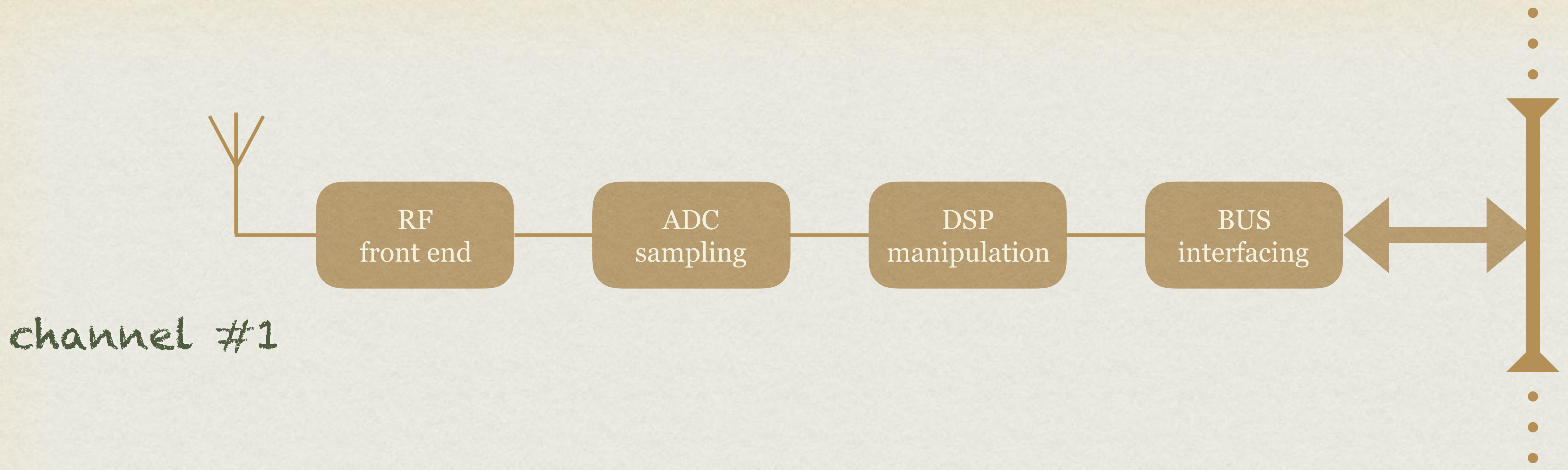
DIGITAL SIGNAL PROCESSING (DSP)

… (thanks to the sampling theorem), uses the correspondence of continuous-time functions and discrete-time sequences to process the input signals by digital operations instead of analog circuits

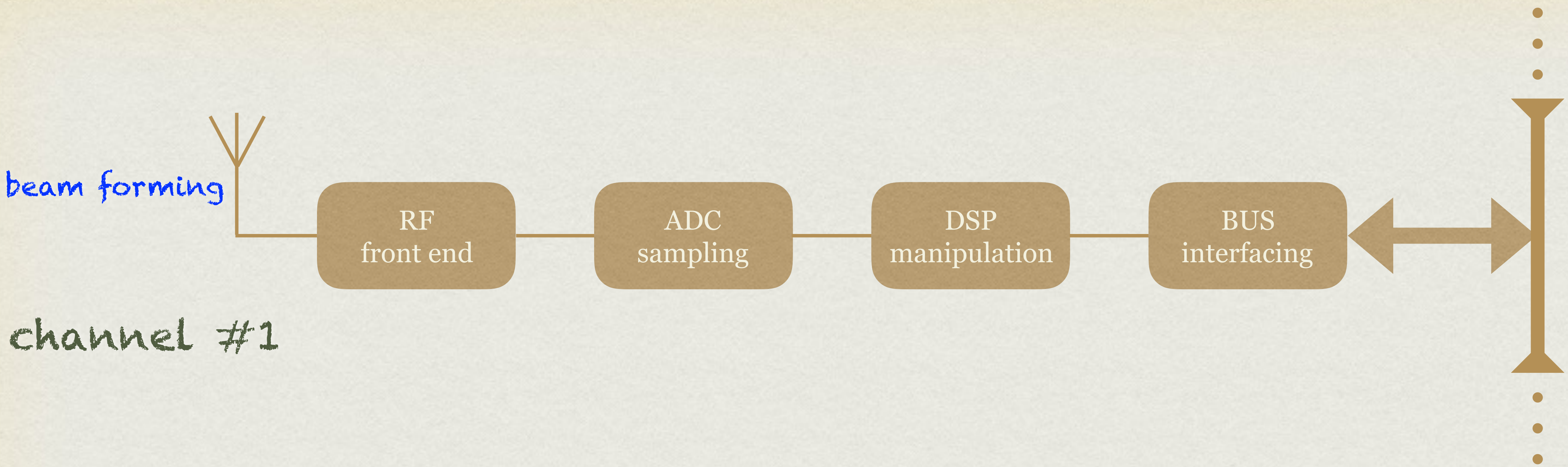
SOFTWARE-DEFINED RADIO (SDR)

... (thanks to the digital signal processing), components that have been typically implemented in (analog) hardware are instead implemented by means of software on a personal computer or embedded system

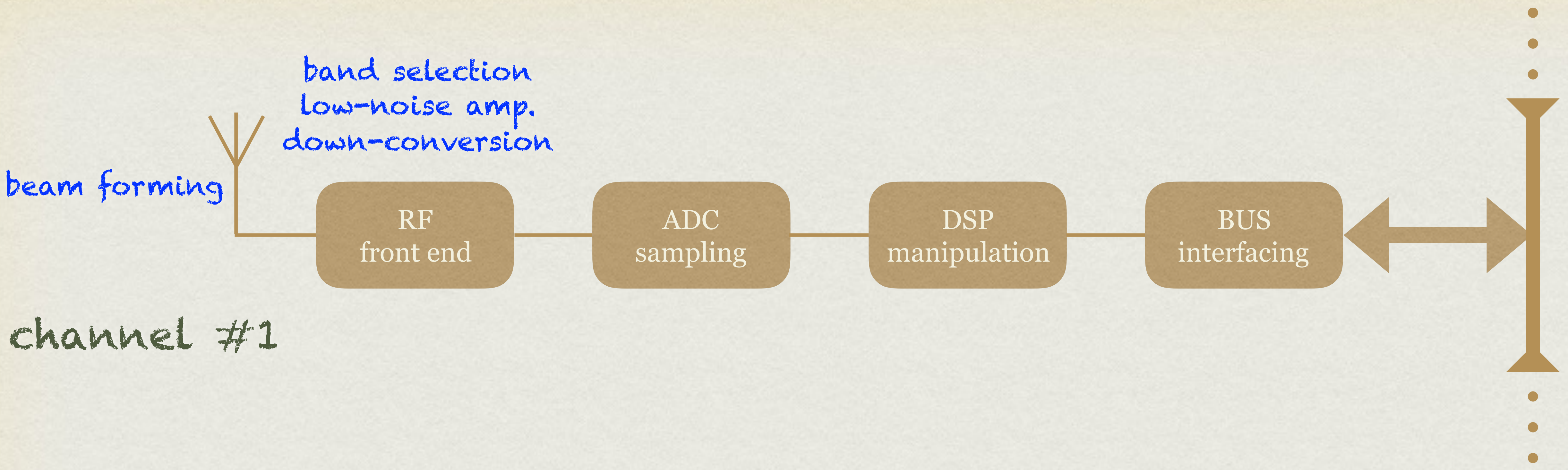
SDR CONCEPT RX PATH



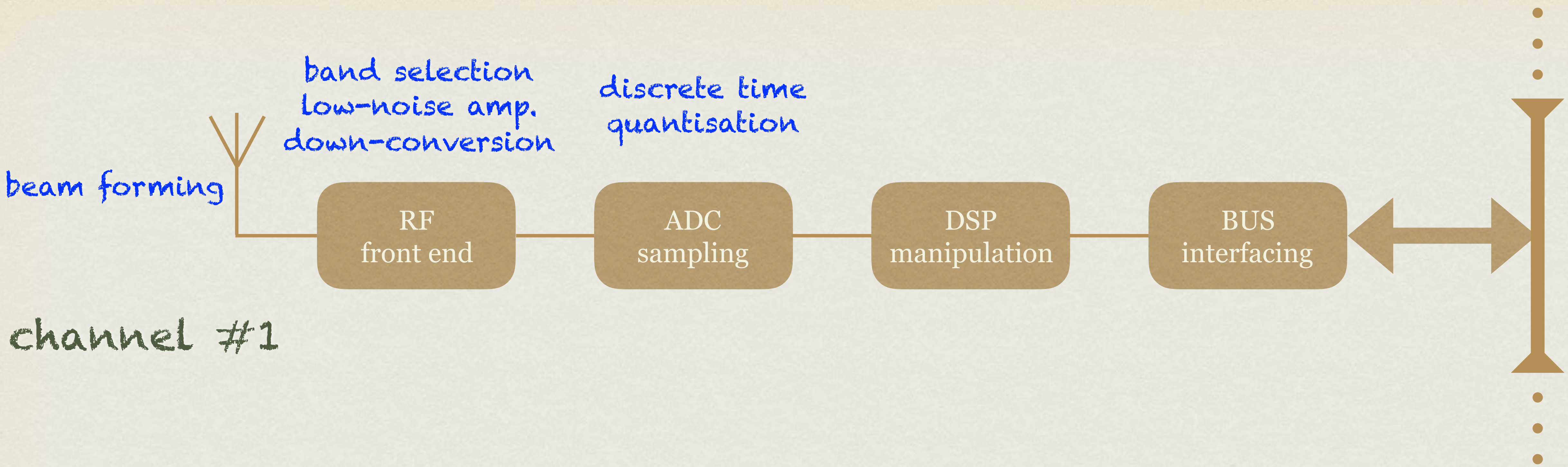
SDR CONCEPT
RX PATH



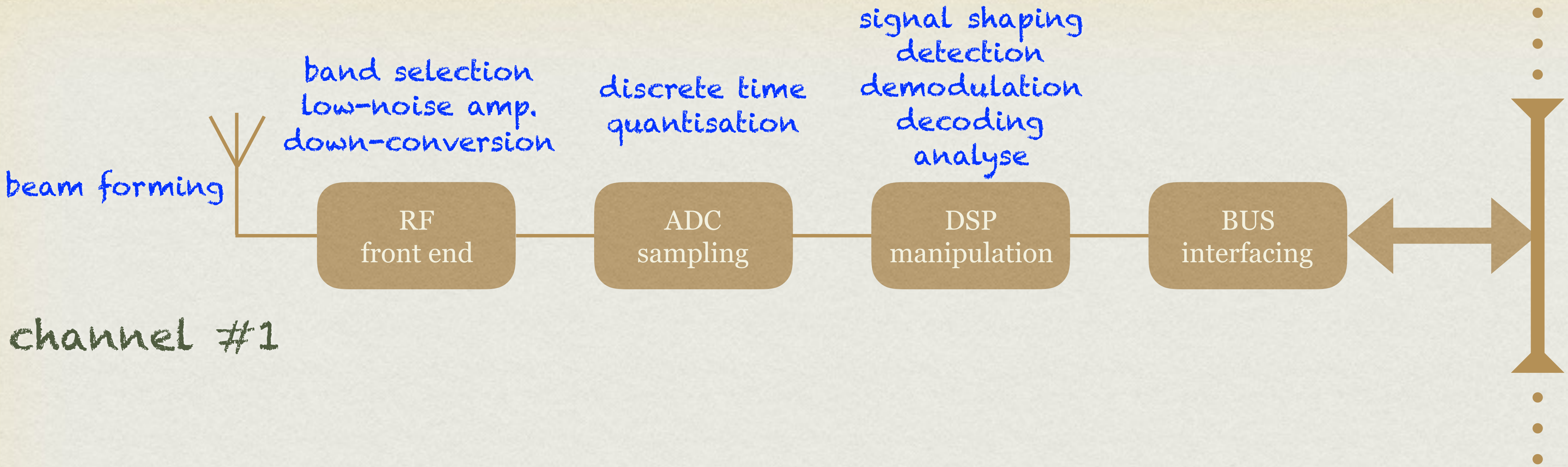
SDR CONCEPT RX PATH



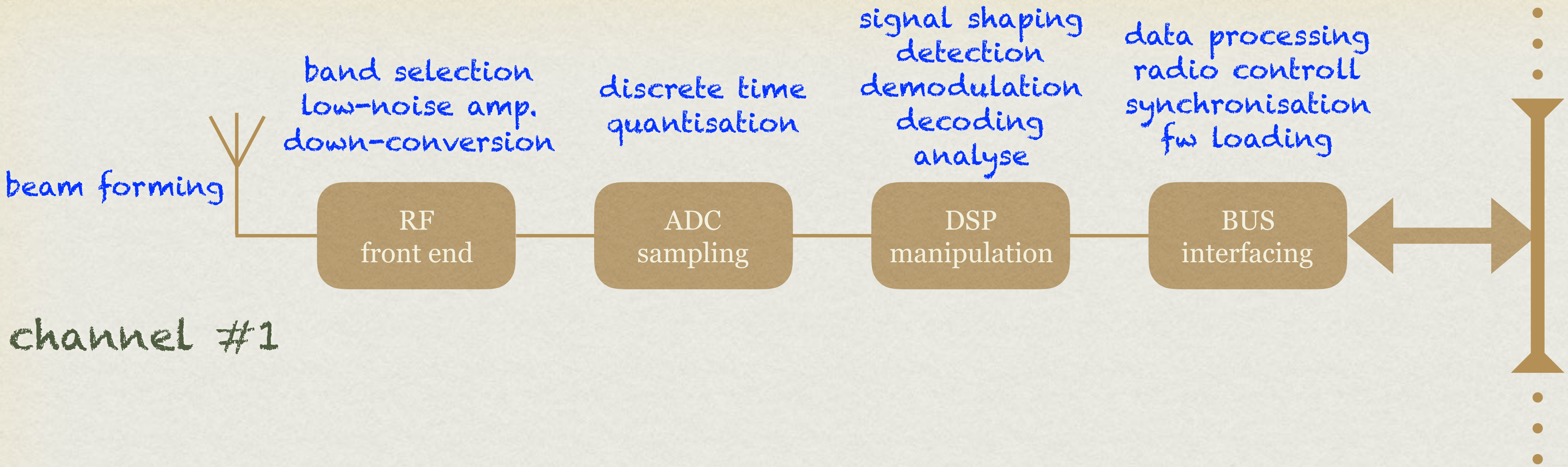
SDR CONCEPT RX PATH



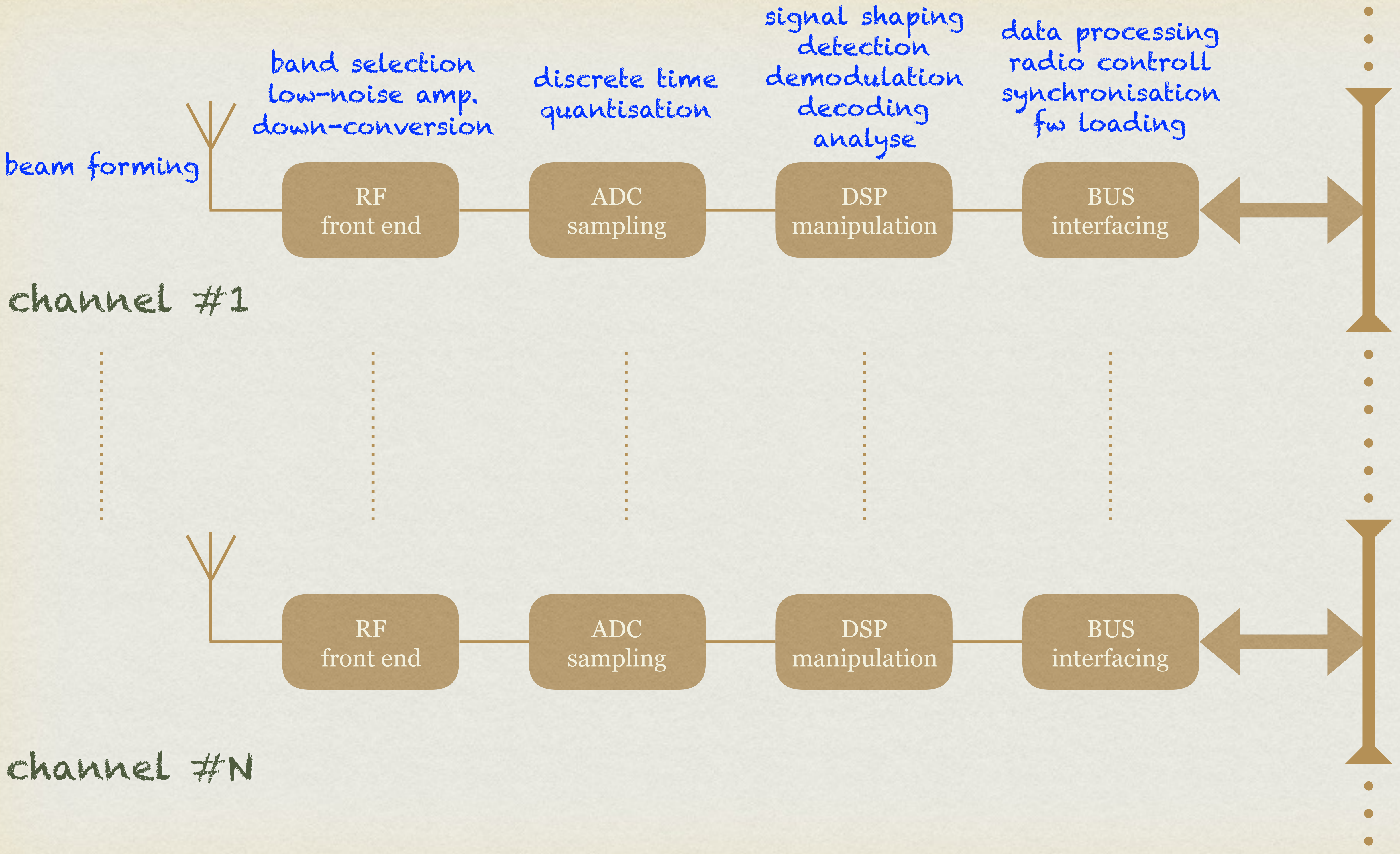
SDR CONCEPT RX PATH



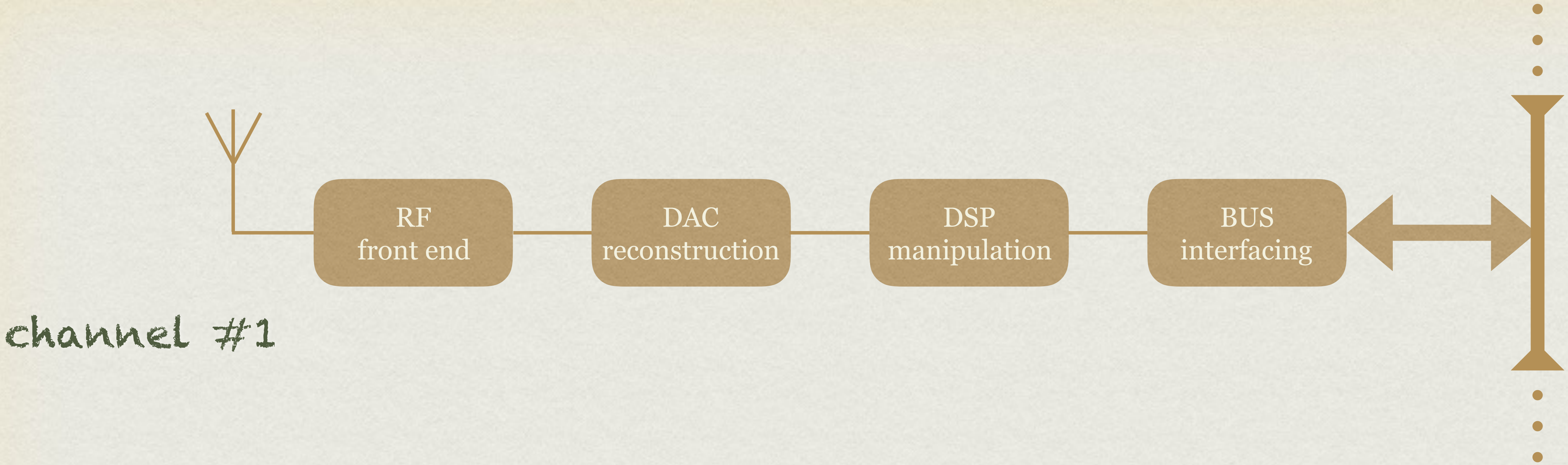
SDR CONCEPT
RX PATH



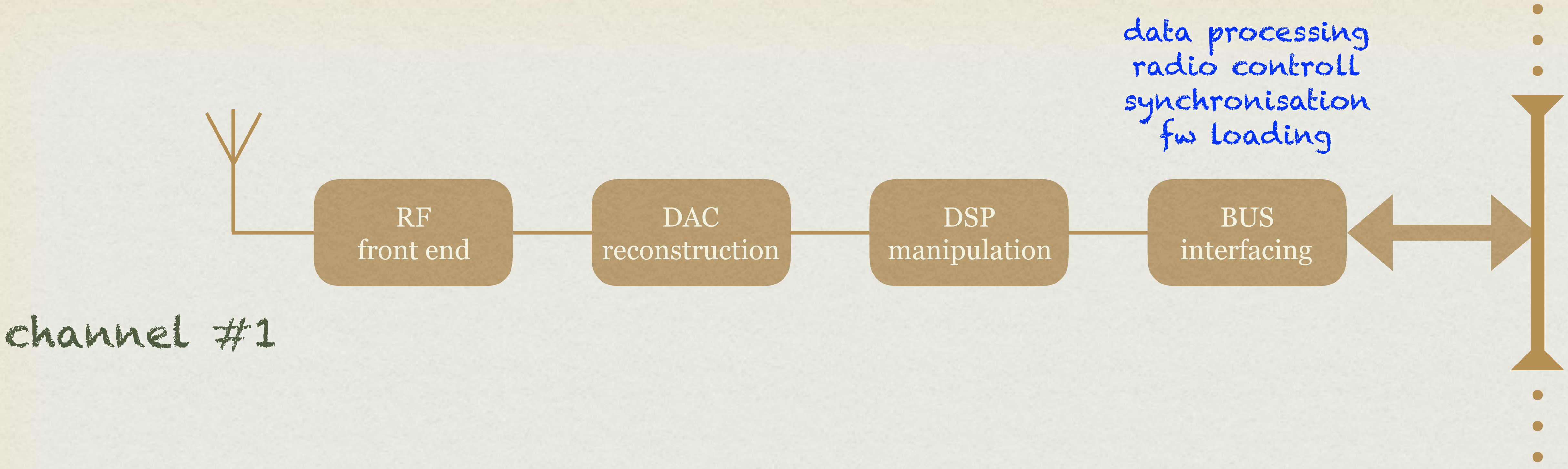
SDR CONCEPT RX PATH



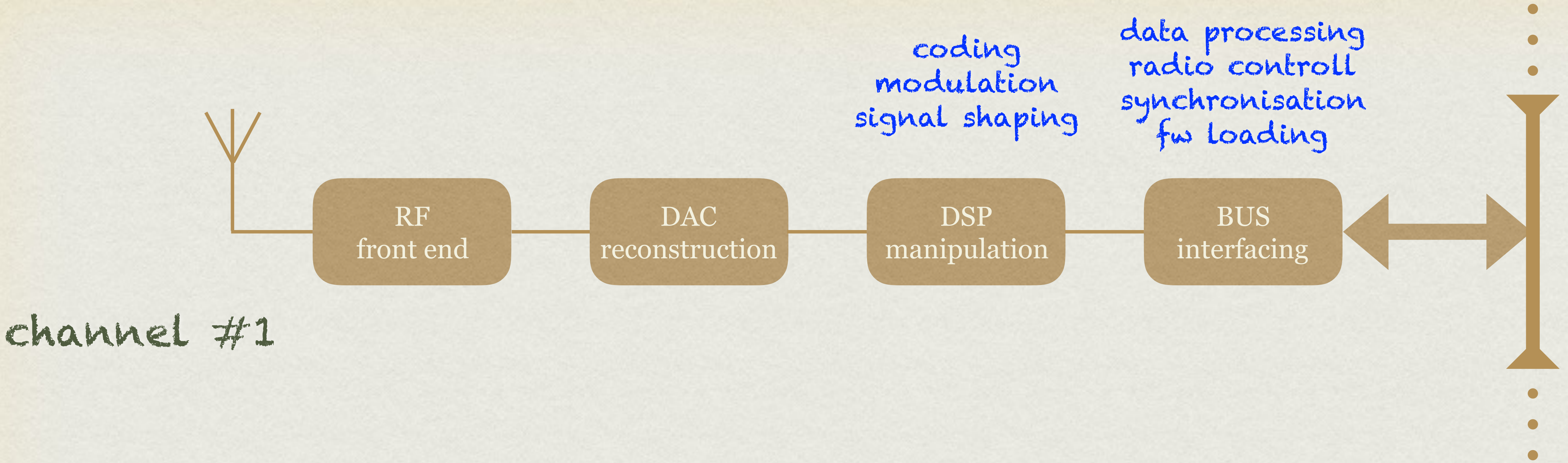
SDR CONCEPT
TX PATH



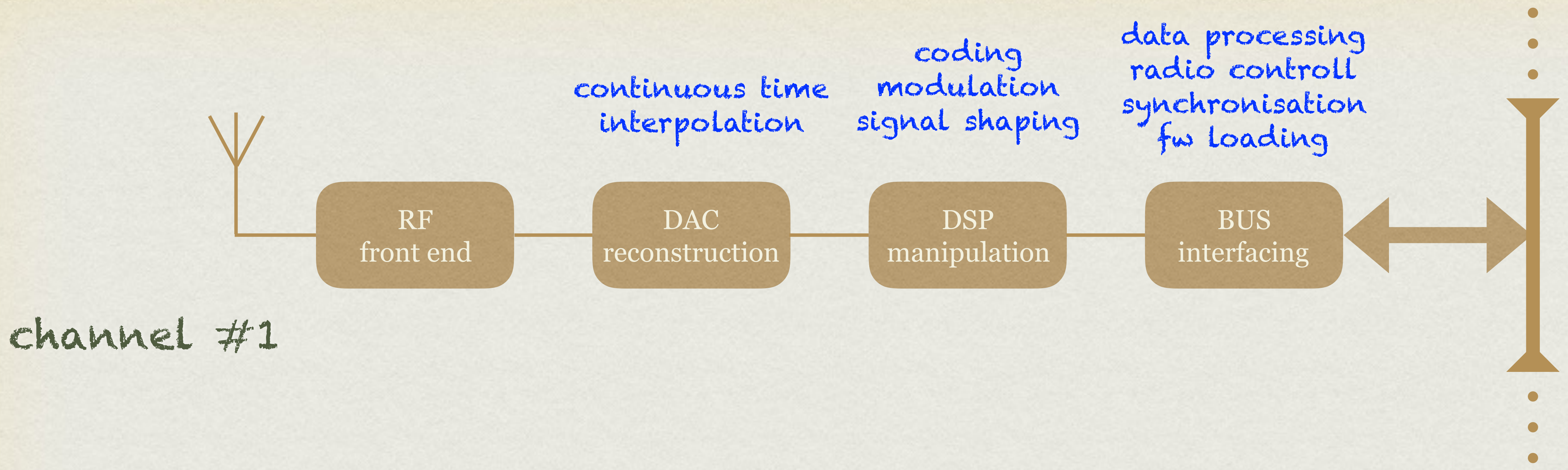
SDR CONCEPT
TX PATH



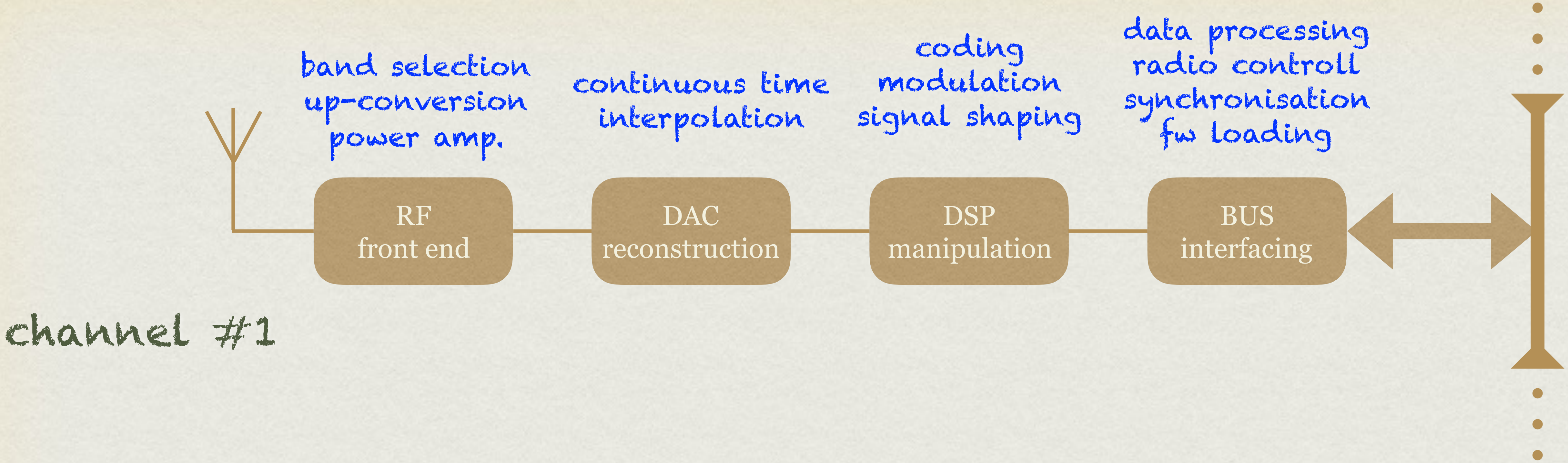
SDR CONCEPT
TX PATH



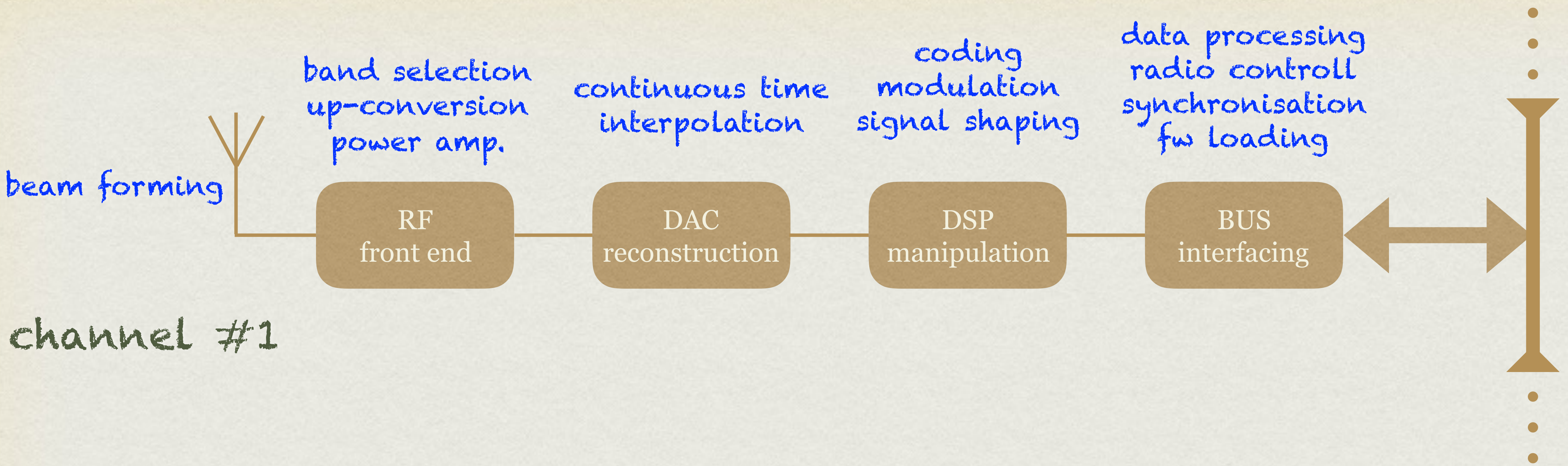
SDR CONCEPT
TX PATH



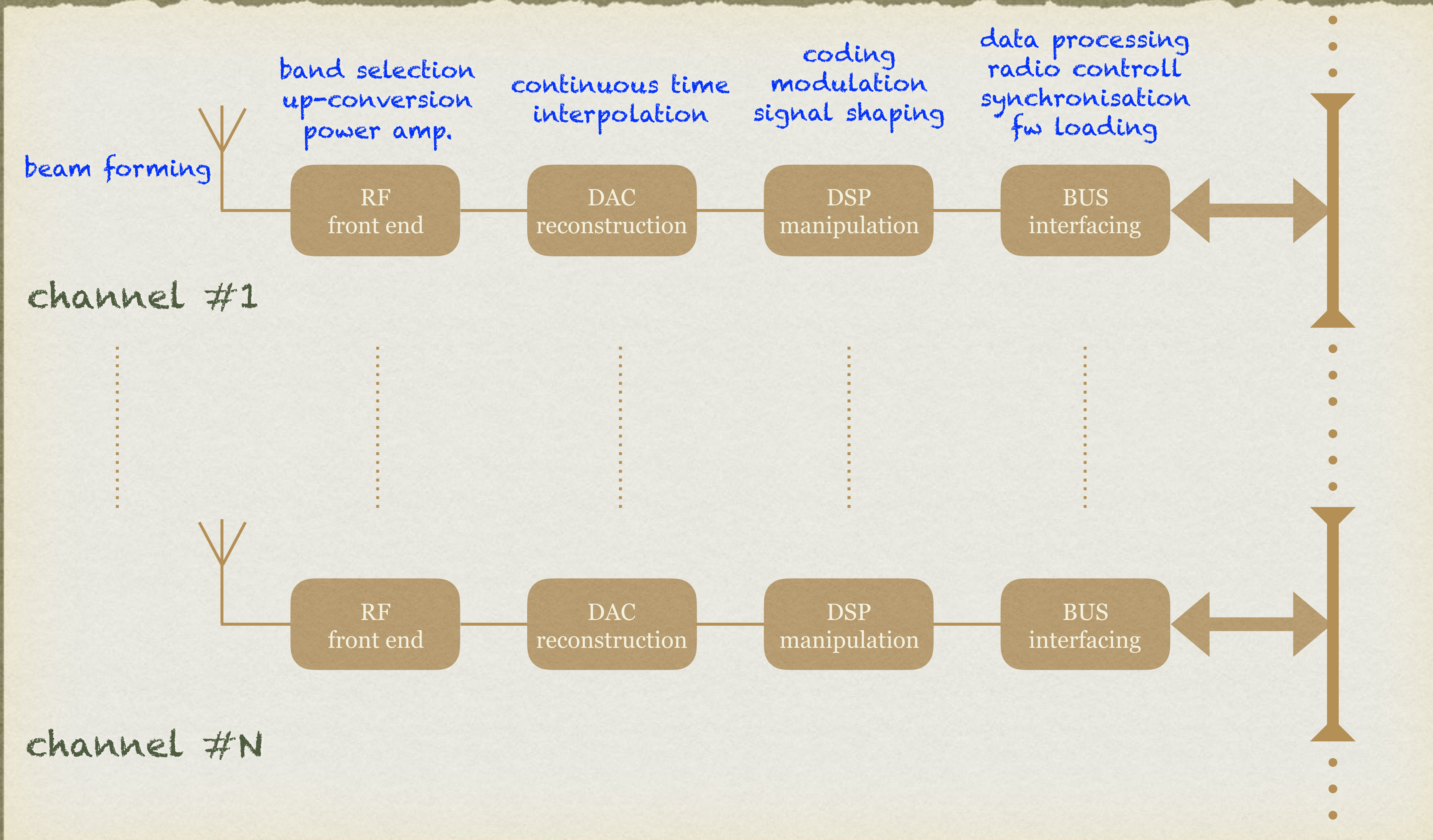
SDR CONCEPT
TX PATH



SDR CONCEPT
TX PATH

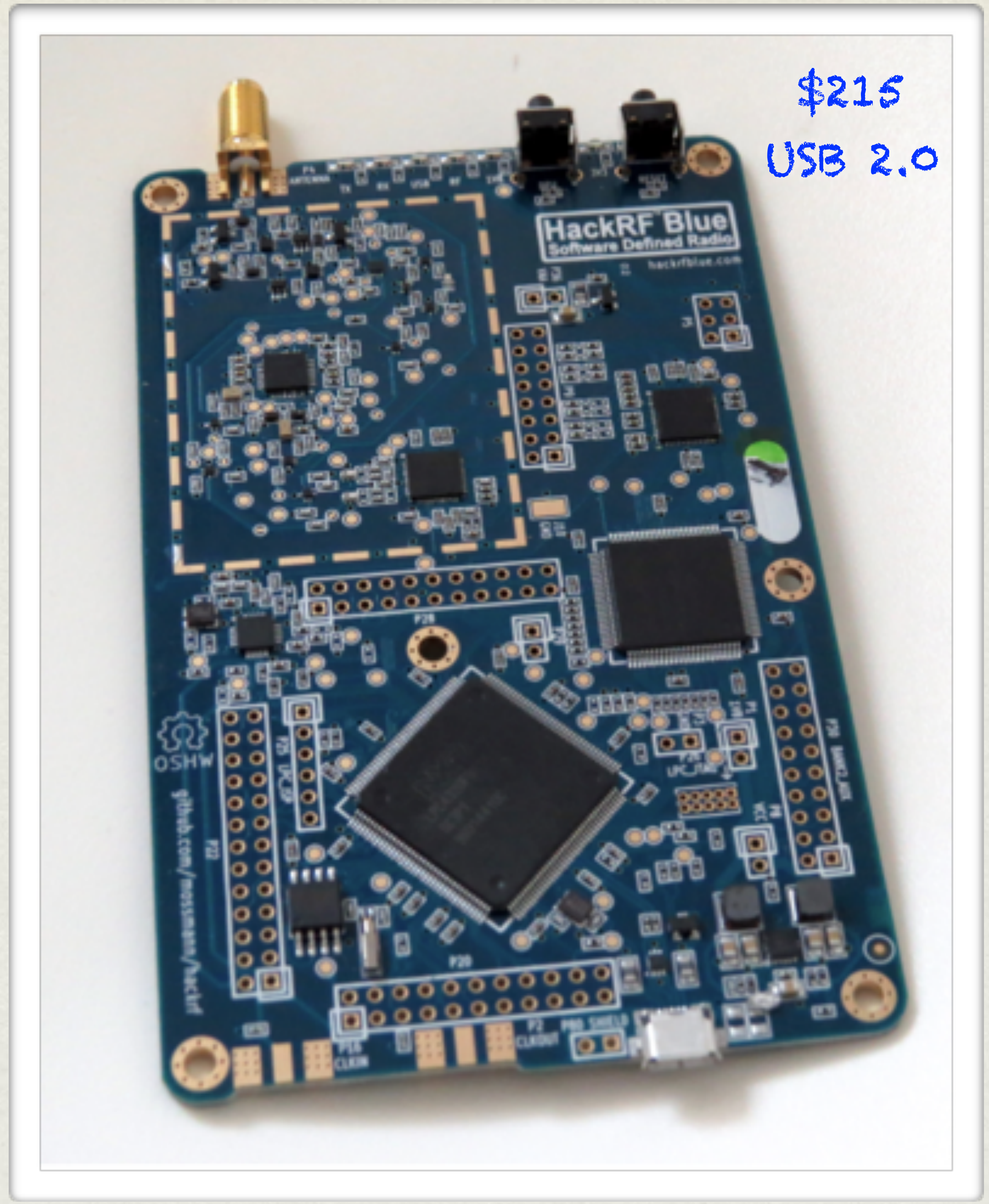


SDR CONCEPT TX PATH

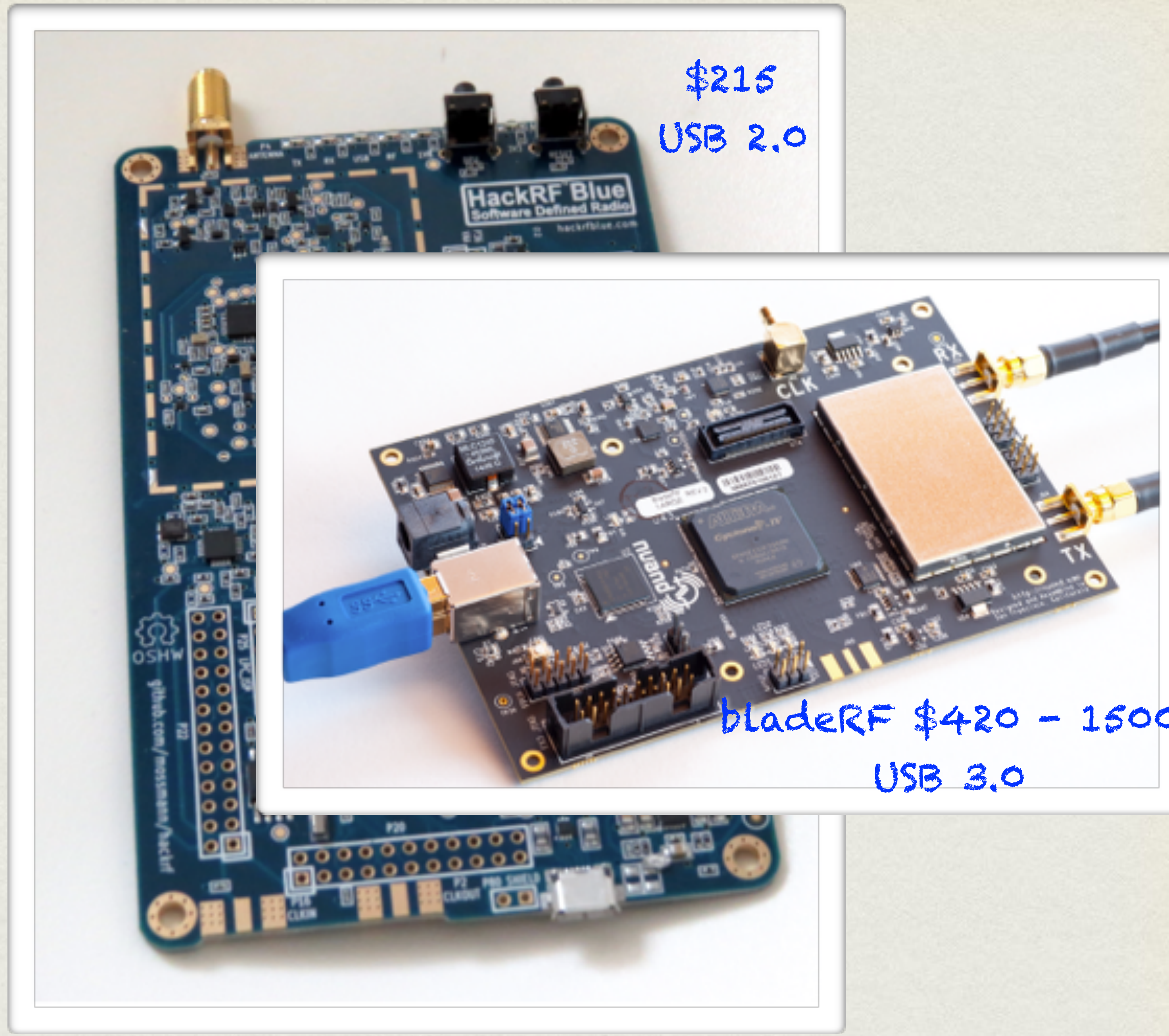


POPULAR HACKING SDR

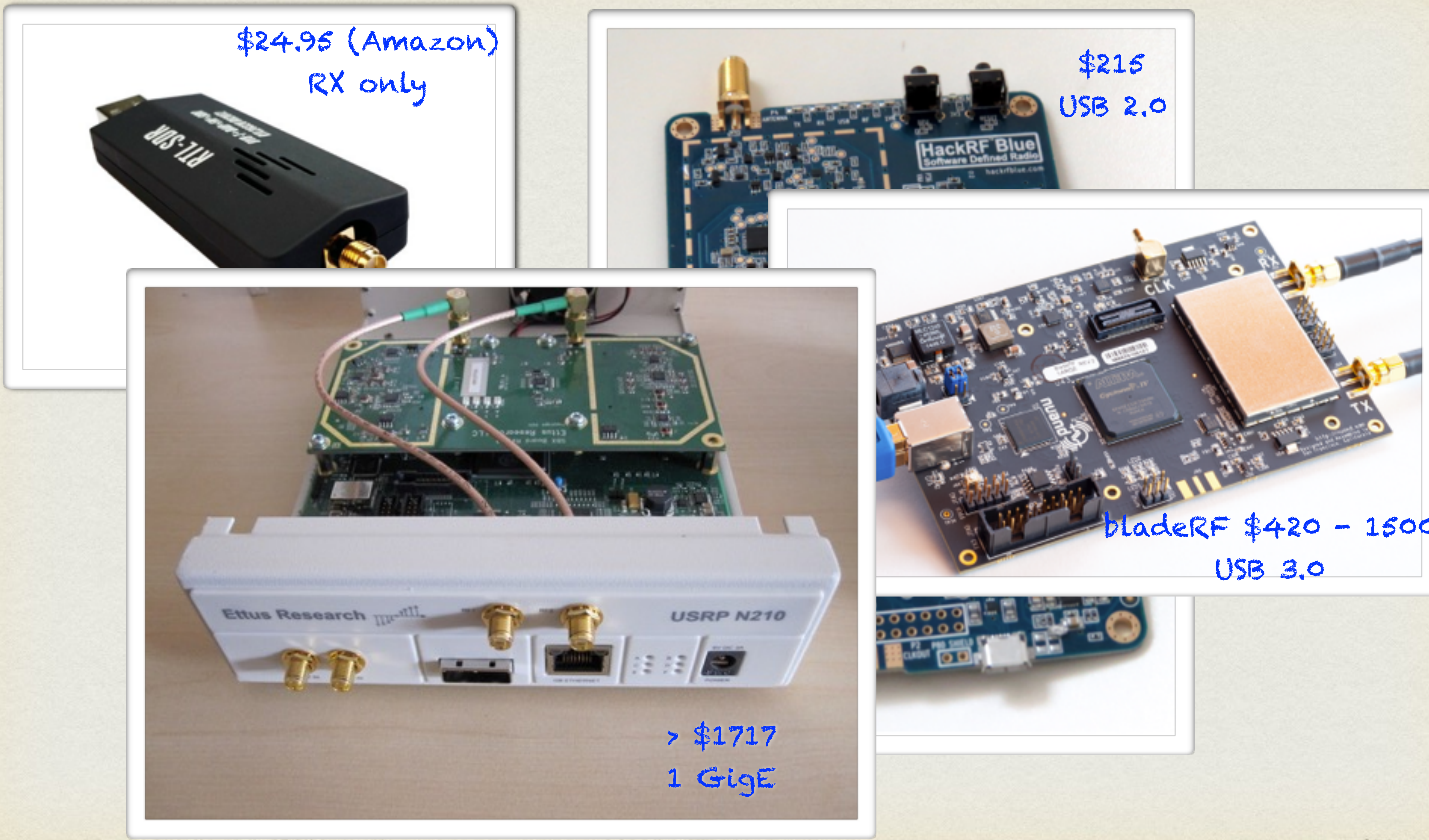
POPULAR HACKING SDR



POPULAR HACKING SDR



POPULAR HACKING SDR



SDR AS A THREAT

DSP routines are SW. This can be shared, installed, and executed all around the world instantly with a very modest background.

Just like any other exploit code.

NFC
NEAR FIELD COMMUNICATION

START WITH SOMETHING FAMILIAR

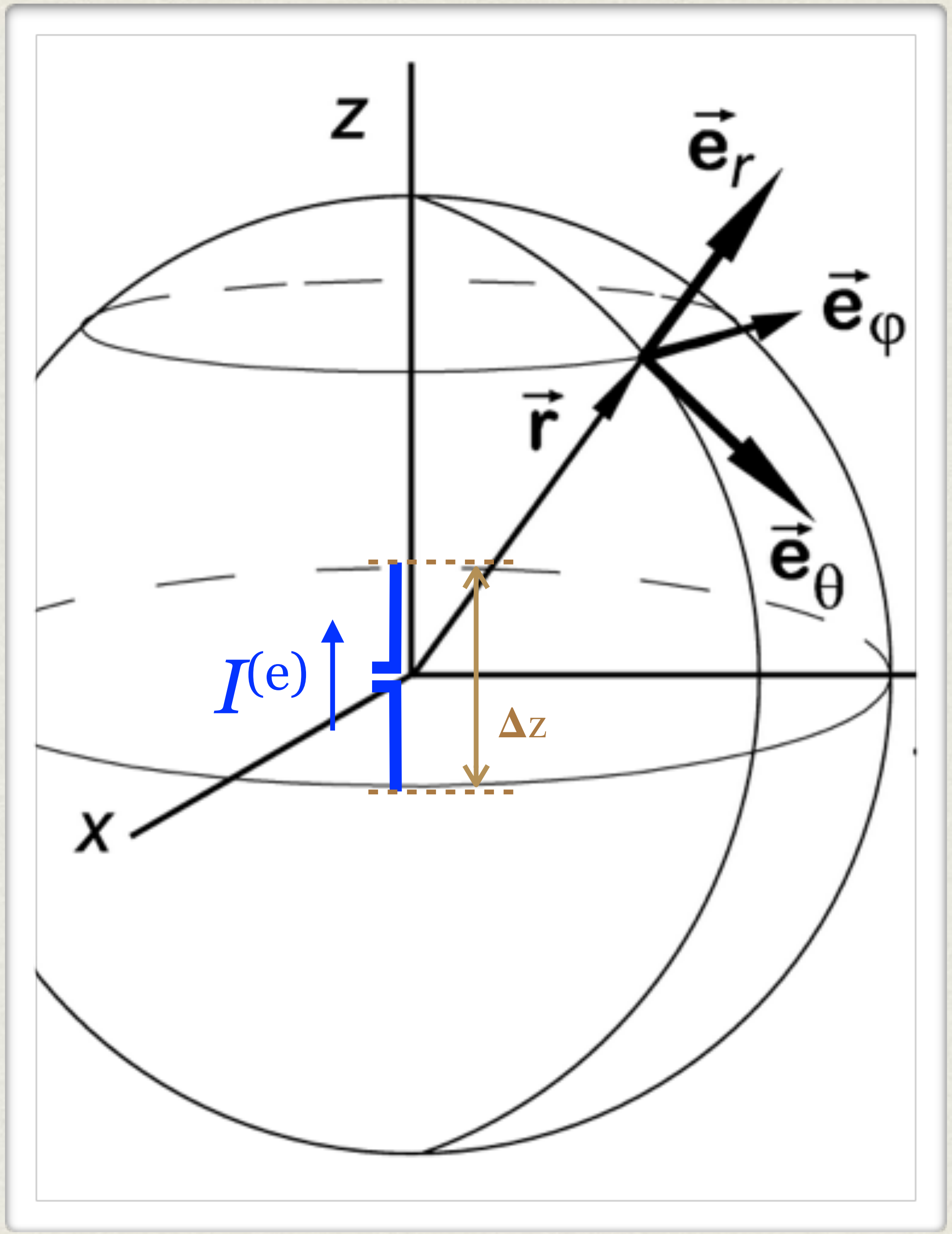
[Buddipole QRV by 5B8AP]

THE IDEAL ELECTRIC DIPOLE

- Electrically small, i.e. $\Delta z << \lambda$, uniform amplitude current element.
  - Ordinary dipole is covered by integration over these elements.
- In the far field, a donut-like pattern bearing the vertical polarisation is produced.
- In general, its field has the following components.

$$\overrightarrow{E}_{edp}(I^{(e)}) = E_{edp,\theta}(I^{(e)}) \cdot \widehat{e_\theta} + E_{edp,r}(I^{(e)}) \cdot \widehat{e_r}$$

$$\overrightarrow{H}_{edp}(I^{(e)}) = H_{edp,\phi}(I^{(e)}) \cdot \widehat{e_\phi}$$



(illustration purpose only)

LONG STORY SHORT

$$\vec{H}_{edp}(I^{(e)}) = \frac{I^{(e)}\Delta z}{4\pi} j\beta(\frac{1}{r} + \frac{1}{j\beta r^2})e^{-j\beta r}\sin\theta \cdot \hat{e}_\phi$$

$$\vec{E}_{epd}(I^{(e)}) = \frac{I^{(e)}\Delta z}{4\pi} j\omega\mu(\frac{1}{r} + \frac{1}{j\beta r^2} - \frac{1}{\beta^2 r^3})e^{-j\beta r}\sin\theta \cdot \hat{e}_\theta$$

$$+ \frac{I^{(e)}\Delta z}{2\pi} j\omega\mu(\frac{1}{j\beta r^2} - \frac{1}{\beta^2 r^3})e^{-j\beta r}\cos\theta \cdot \hat{e}_r$$

$$= \frac{I^{(e)}\Delta z}{4\pi} j\omega\mu(\frac{1}{r} + \frac{1}{j\beta r^2} - \frac{1}{\beta^2 r^3})e^{-j\beta r}\sin\theta \cdot \hat{e}_\theta$$

$$+ \frac{I^{(e)}\Delta z}{2\pi} \eta(\frac{1}{r^2} - j\frac{1}{\beta r^3})e^{-j\beta r}\cos\theta \cdot \hat{e}_r$$

TOWARDS SOMETHING APPEALING

[AlexLoop by Alex, PY1AHD]

THE SMALL LOOP

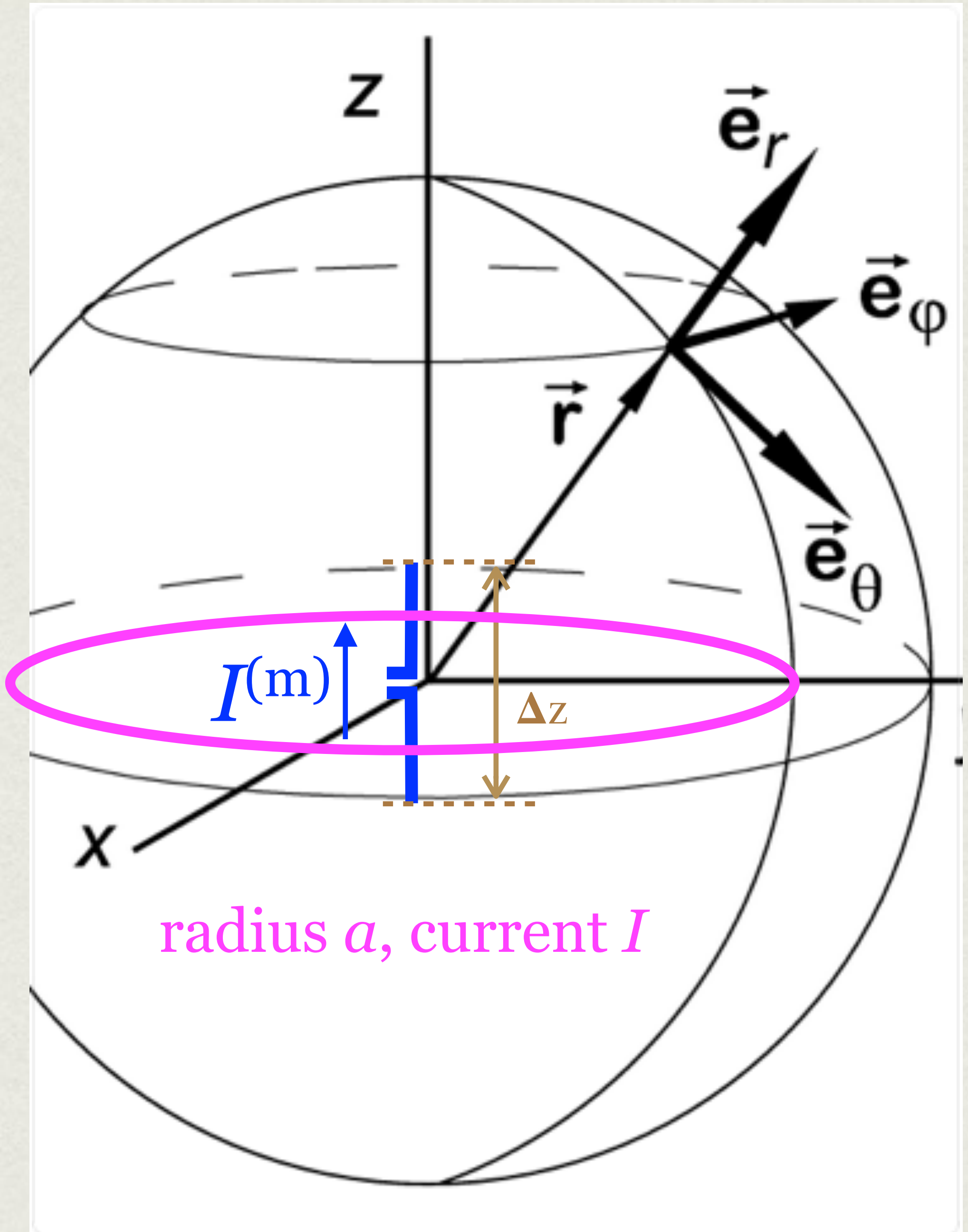
- Electrically small, i.e. $2\pi a < \lambda/10$, uniform amplitude current loop.
- Can be modelled as an ideal *magnetic* dipole which is the theoretical dual of the ideal electric dipole.
- The duality equations follow.

$$\vec{E}_{mdp}(I^{(m)}) \equiv -\vec{H}_{edp}(I^{(m)}),\ \vec{H}_{mdp}(I^{(m)}) \equiv \vec{E}_{edp}(I^{(m)})$$

$$\mu_{mdp} \equiv \varepsilon_{edp},\ \varepsilon_{mdp} \equiv \mu_{edp}$$

$$\beta_{mdp} = \omega\sqrt{\mu_{mpd}\varepsilon_{mdp}} = \omega\sqrt{\varepsilon_{edp}\mu_{edp}} = \beta_{edp}$$

note also $\beta = \dfrac{2\pi}{\lambda},\ v = \lambda f$



(illustration purpose only)

LONG STORY SHORT

$$\vec{E}_{mdp}(I^{(m)}) = -\frac{I^{(m)}\Delta z}{4\pi} j\beta\left(\frac{1}{r}+\frac{1}{j\beta r^2}\right)e^{-j\beta r}\sin\theta\cdot\hat{e}_\phi$$

$$\vec{H}_{mpd}(I^{(m)}) = \frac{I^{(m)}\Delta z}{4\pi} j\omega\varepsilon\left(\frac{1}{r}+\frac{1}{j\beta r^2}-\frac{1}{\beta^2 r^3}\right)e^{-j\beta r}\sin\theta\cdot\hat{e}_\theta$$

$$+\frac{I^{(m)}\Delta z}{2\pi} j\omega\varepsilon\left(\frac{1}{j\beta r^2}-\frac{1}{\beta^2 r^3}\right)e^{-j\beta r}\cos\theta\cdot\hat{e}_r$$

MAGNETIC CURRENT OF THE SMALL LOOP

$$I^{(m)}\Delta z = j\omega\mu IS$$

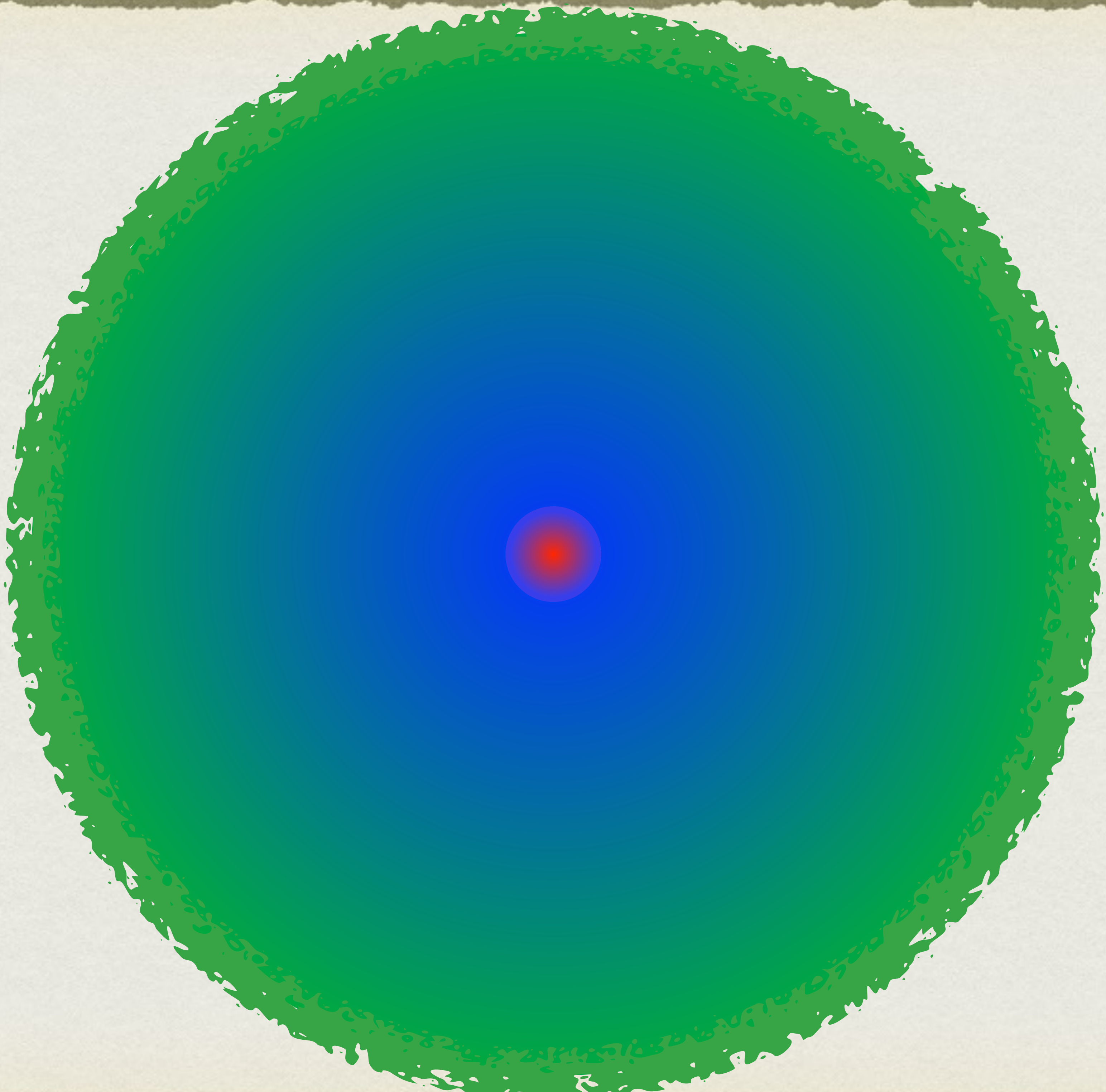
$$S = \pi a^2$$

(based on far field equivalence)

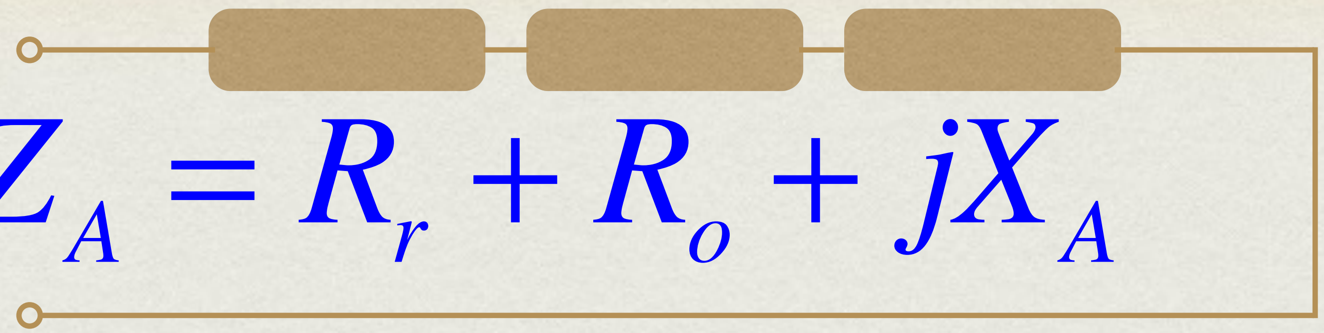
NEAR, FAR

- Basing on the different dominating E, H field terms implying *different dominating field behaviour*, it is useful to distinguish:
  - *Reactive near field* (XNF), where the terms with $1/r^2$ and $1/r^3$ dominate. Energy is mainly stored and exchanged between E and H.
  - *Radiating near field* (Fresnel region), where the $1/r^2$ terms start to dominate, i.e. $r > \lambda/2\pi$. Energy is mainly radiated with unstable patterns, however.
  - *Far field* (Fraunhofer region), where the $1/r$ terms remain to dominate and the plane wave model can be used. Several conditions shall be met: $r > 2D^2/\lambda$, $r > 5D$, $r > 1.6\lambda$, where D is the largest antenna dimension. Energy is radiated with a distance-independent field pattern.

WHEREVER YOU ARE



ANTENNA IMPEDANCE



$$Z_A = R_r + R_o + jX_A$$

- The input impedance Z_A describes the antenna from the lumped circuit parameters viewpoint. *This is also useful to describe the antenna field action observable in those different field regions in a handy condensed way.*
  - R_r is the equivalent radiation resistance representing the energy emanated through the radio waves
  - R_o describes the dissipative energy loss
  - X_A reflects the energy exchanged back-and-forth with the reactive near field

RADIATION OF THE SMALL LOOP

$$P = 10I^2(\beta^2 S)^2$$

$$R_r = \frac{2P}{I^2} = 20(\beta^2 S)^2 \approx 31171(\frac{S}{\lambda^2})^2$$

$$\approx 31171(\frac{NS}{\lambda^2})^2, \text{ for a small } N\text{-turn loop}$$

DAMPING RESISTOR

- For the radiation efficiency analysis, R_o shall also cover any damping resistor R_q used.

- Especially for NFC, a nonzero R_q is often inserted serially to lower the antenna Q to achieve the required bandwidth.

    - Finally, we can expect a very small radiation efficiency for a typical NFC antenna.

    - Interestingly, we may investigate on how to design a yet-usable NFC antenna that is, however, a very poor radiator anyway.

    - *Nevertheless, it does not mean the radiation is zero.*

EFFICIENCY ANALYSIS

- To get a better overview, we can compute the radiation efficiency e_r that can be further used for e.g. gain estimation, etc.

- We do that by comparing the equivalent real resistances from the circuit model of Z_A.

$$R_s = \sqrt{\frac{\omega\mu}{2\sigma}}$$

$$R_o = \frac{a}{c} R_s, \text{ a } \sim \text{ loop radius, c } \sim \text{ wire radius}$$

$$e_r = \frac{R_r}{R_q + R_o + R_r}$$

YES, IT CAN!

- NFC antenna is generally capable of transmitting its signal into the far field region.
- Due to its construction, the radiation resistance is very small leading to a very poor energy transfer.
- Nevertheless, it does not mean there would be no transmission at all.

PARASITIC ANTENNAS

- From the security viewpoint, we shall recognise it may not be the *primary* antenna only that can radiate sensitive data.
- In general, any spatial distribution of a time-varying current modulated (or sensed!) by the internal processing unit is a potential backdoor.
  - We are getting to the well-known phenomenon of the electromagnetic side-channels.
  - Here, we have an extremely high chance this mechanism is exploitable by attackers.
  - In principle, applying anti-RFI techniques for all those patch cables and power lines is a good idea to start with.

INITIATOR RANGE EXTENSION

- Allows RF skimming or wormhole (relay) attacks.
- Due to a very low efficiency and very high power consumption, it is practically limited to the reactive near field region (XNF).
- Antenna diversity separating downlink and uplink channels may help significantly.
- Distance: Decimetres (confirmed), reliably working at around 20 cm. Principal upper limit $\approx \lambda/2\pi$, i.e. circa 3.5 m, is infeasible to achieve practically. So, we are limited to a kind of *bumping attack*.

SNIFFING

- Sensitive data capture, identity theft.
- Works over all zones, from XNF to Fraunhofer region.
- **Often, this scenario induces the most serious risks.**
- For regions outside XNF, the important idea is to look for higher harmonics of the 13.56 MHz carrier.
- Furthermore, antenna design and orientation varies through the regions.
- Distance: Metres to dekametres. Confirmed for both downlink and uplink channels.

ALL YOU NEED IS *LOOP*

SPYING IN THE LANE (STILL IN XNF)

[https://www.youtube.com/watch?v=9QjxwejBPHs]

TARGET RANGE EXTENSION

- Allows covert communication with NFC terminal.
- Combines the techniques for a long range sniffing with the reciprocal problem of an extended-range signal injection into the RF front-end of the terminal.
- Based on direct DSB (Double Side Band) or even SSB (Single Side Band) injection, basing on the particular terminal signal processing.
- Principally possible even from the Fraunhofer region.
- The terminal antenna gain together with its input sensitivity limits the distance.
- Distance: Metres (confirmed). Working from the Fraunhofer region is practically very hard.

TRAFFIC INJECTION

- Allows Man-In-The-Middle scenarios.
- Due to the linear superposition in the EM field, the attacker does not have to be geometrically right in the middle, neither to break the original channel spatially.
- Again, a few turns of a wire around the original reader can be enough.
- Note we can also spoof the Initiator packets, besides the Target responses.
- Covering the path to the Target (downlink) requires XNF. One sided injection can work from the Fresnel or Fraunhofer regions as well.
- Distance: Decimetres (downlink TX covered) up to metres (TX for uplink only). Confirmed indirectly by other experiments together with own observations (cf. below).

INITIATOR LOCATION

- Allows searching for active terminals - for instance, exposing passengers inspection, etc.
- Carrier detection at 13.56 MHz or higher harmonics, possibly also with the communication footprint.
- Distance: Dekametres. Indirectly confirmed by the eavesdropping experiments that can serve as a lower bound.

TARGET LOCATION

- Allows searching for potentially valuable assets.
- Searching based on radio characteristics without querying the higher protocol layers.
- Electronic Article Surveillance (EAS) style to search for the particular resonant circuits.
- Distance: Decimetres (confirmed by the range extension experiments) to metres (estimated).

JAMMING

- Allows DoS attacks at airport, office entry, market centre etc.
- We can use reciprocity theorems to estimate the effect an attacker's (measurement) antenna would have on the terminal input.
- Distance: Metres (confirmed by the range extension experiments) to dekametres (estimated).

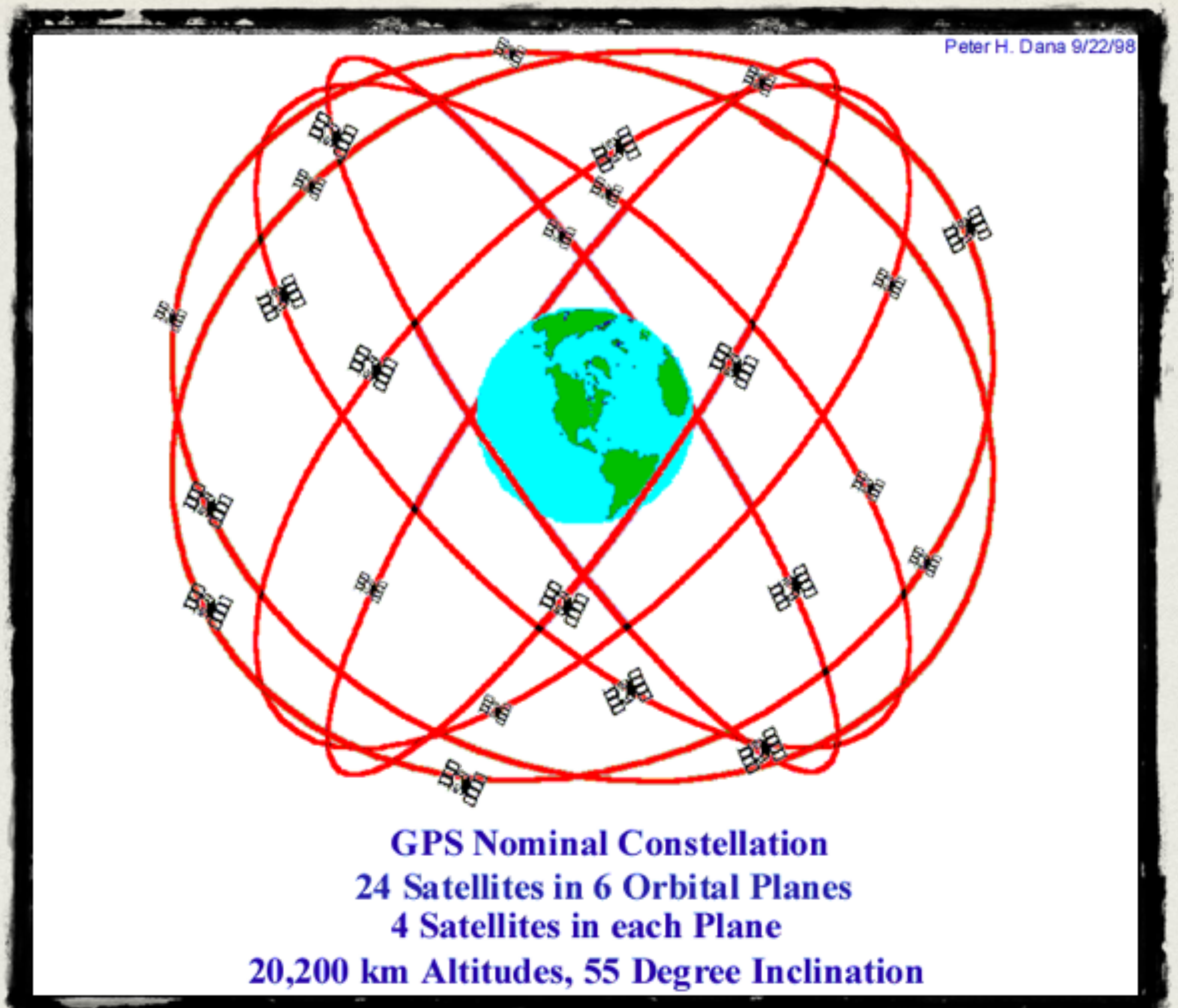
DEVICE DESTRUCTION

- Allows selective DoS on the terminal or transponder.
- In principle, it requires a strong power pulse, so a near field approach is assumed.
- Distance: Decimetres.

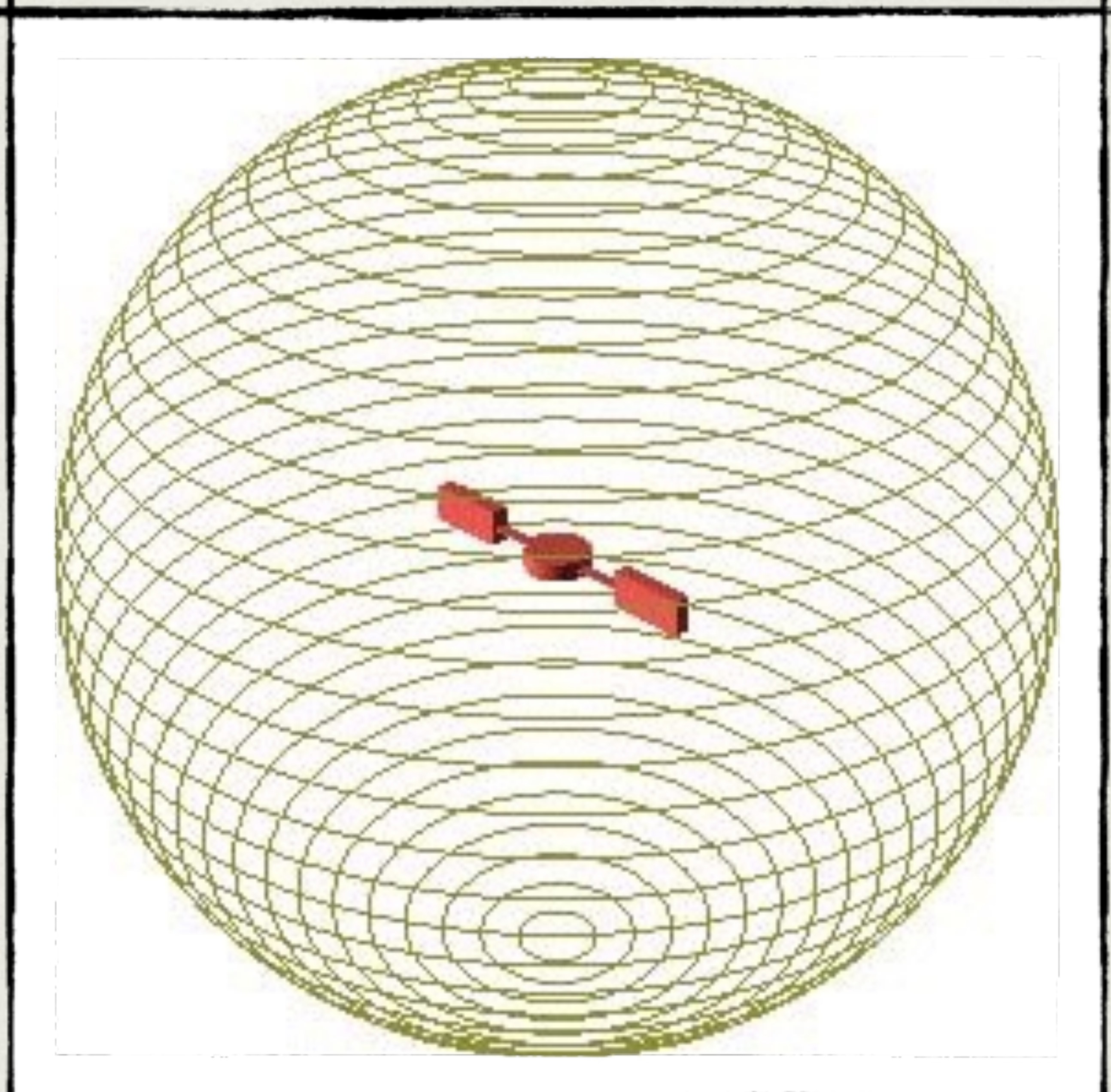
GPS
GLOBAL POSITIONING SYSTEM

artist's illustration of GPS Block IIF satellite vehicle
produced by The Boeing Company, first launch on May 28th 2010

GPS SPACE SEGMENT

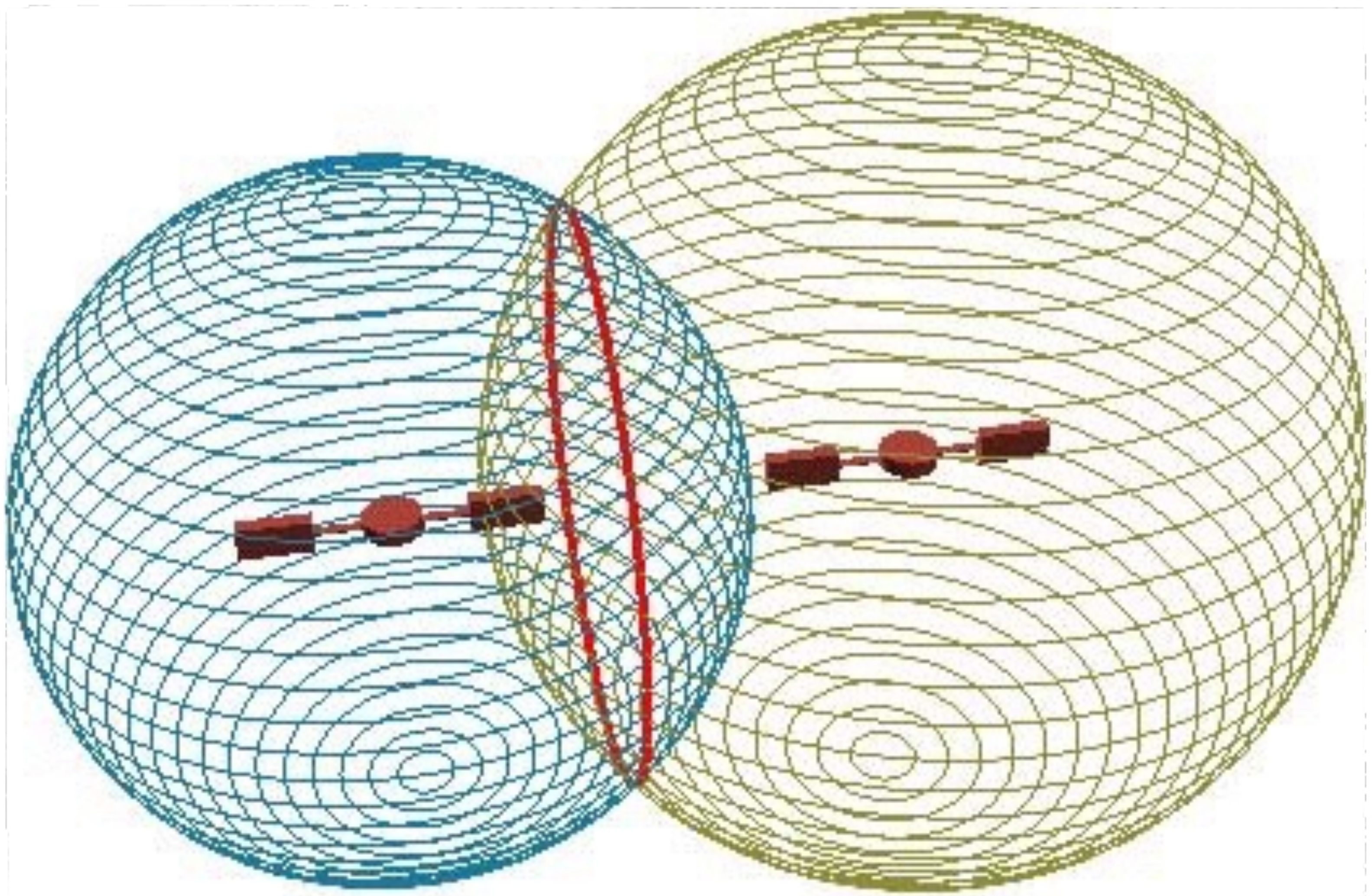


TRILATERATION I



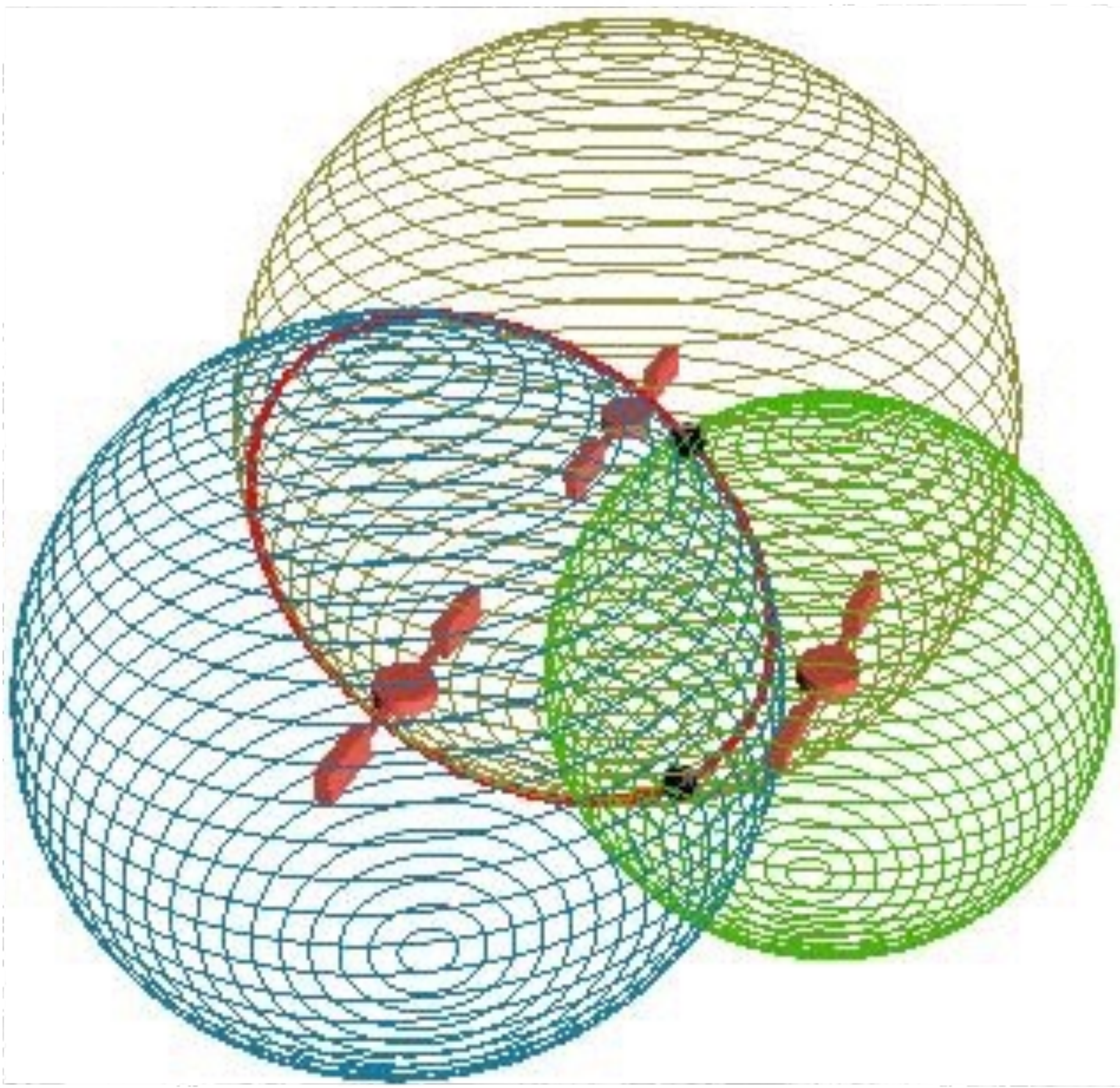
http://courses.washington.edu/gis250/lessons/gps/

TRILATERATION II



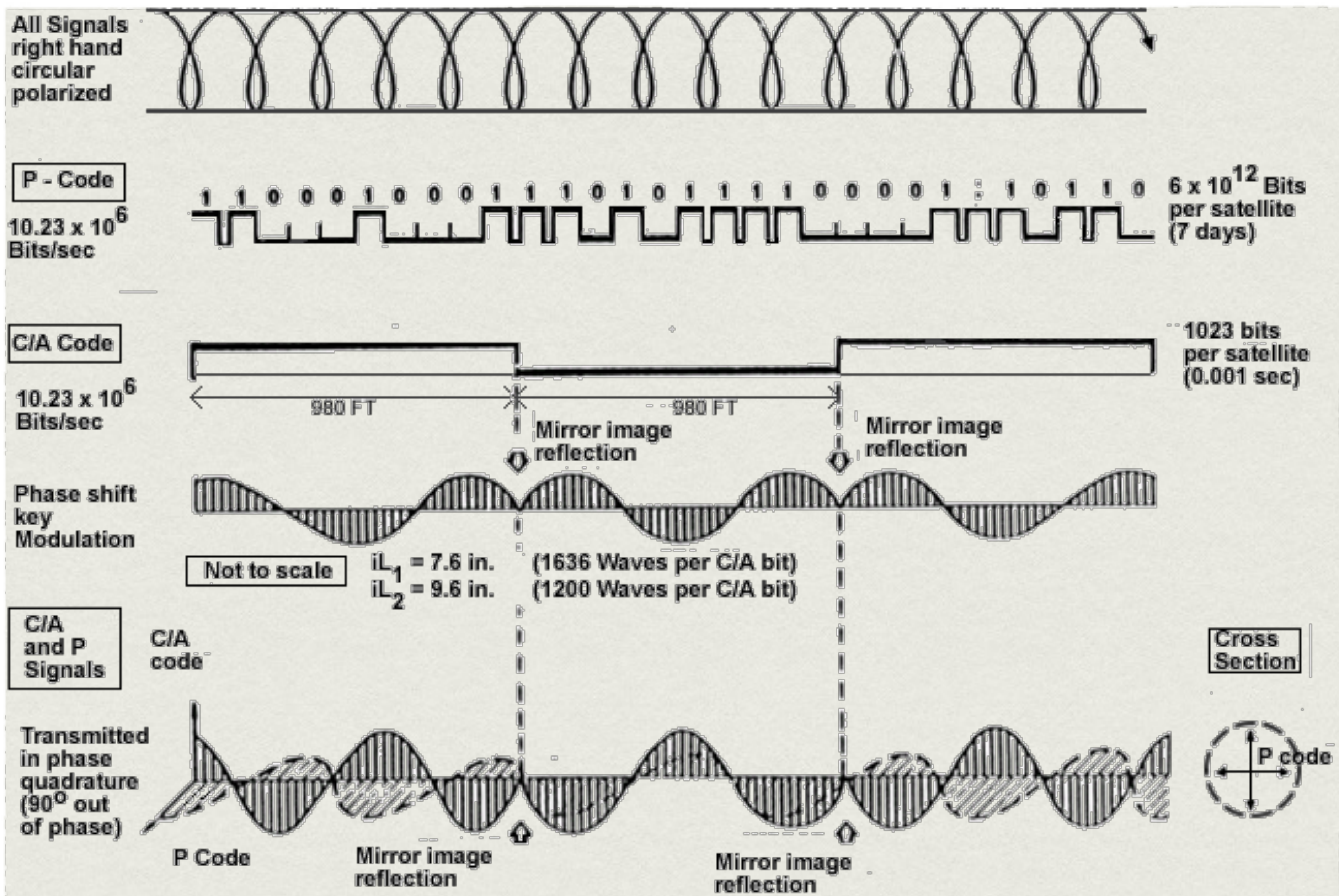
http://courses.washington.edu/gis250/lessons/gps/

TRILATERATION III



http://courses.washington.edu/gis250/lessons/gps/

GPS L1 C/A & P(Y) (ILLUSTRATION ONLY)



Kulshreshta, 1997

SATELLITE CLOCK REPLICAS EXPOSE THE TIME DELAYS

CIVIL GPS IN SERIOUS APPLICATIONS

NTP server

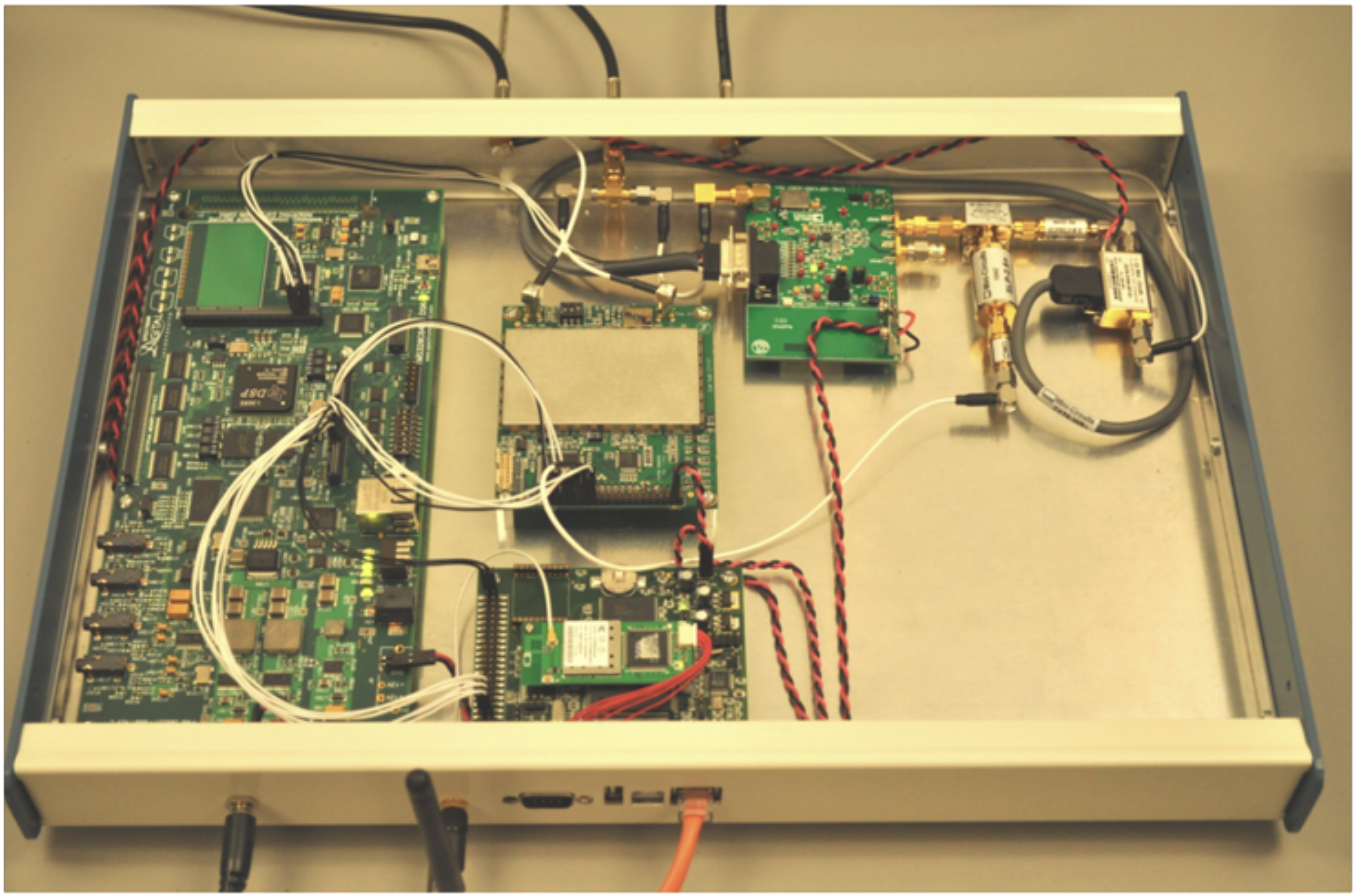
L1 C/A SIGNAL IN BRIEF

- CDMA at the common carrier frequency of 1575.42 MHz
- Satellites distinguished by their unique chipping sequence (Gold codes)
- Allows creation of a delayed replica clock of the particular satellite (implicit time synchronisation)
- Carries 37 500 bits of navigation data for the particular satellite (explicit time synchronisation and position computation)
- Includes corrections according to the General Theory of Relativity
- … does not include any cryptographic protection

L1 C/A SECURITY

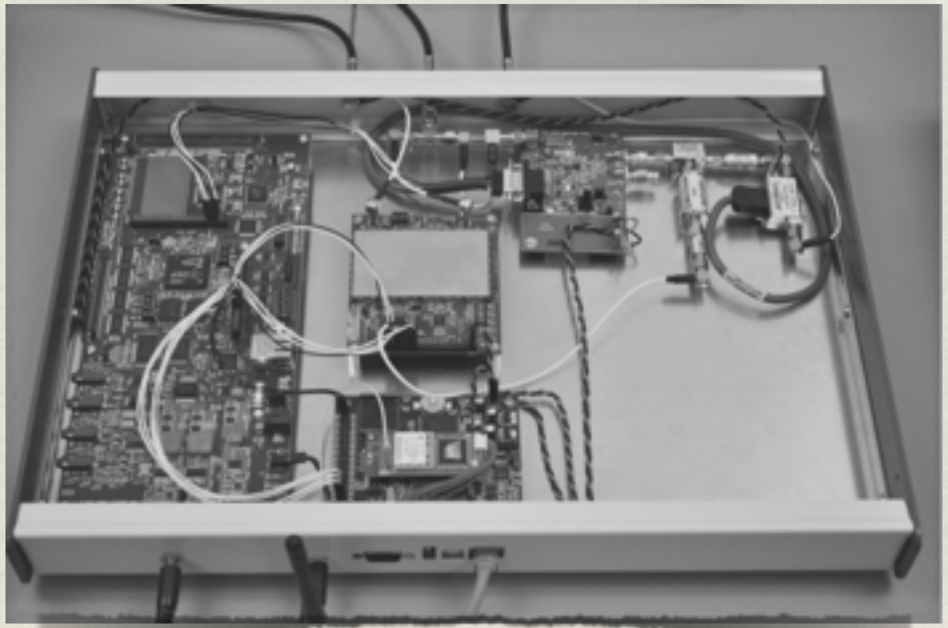
- Position/Velocity/Time (PVT) spoofing is accessible to a moderate-level attacker
  - real-life scenario may (allegedly) be that "**Iran–U.S. RQ-170 incident**"
  - actually, a GPS "replay attack" is a standard advanced tutorial for the LabView platform using the USRP Software Defined Radio (SDR)
- OK, this signal was never meant as a military-grade service and the lack of protection here can hardly be called a "discovery"
- On the other hand, a lot of commercial applications have grown up to be vital parts of our critical infrastructure today…

CIVIL GPS UNDER SERIOUS ATTACK



[Humphreys, Ledvina, and Shepard, 2008-2011]

PRECISE SDR SPOOFER



- receiver-spoofer architecture
- tracks original L1 C/A and L2C
- manipulates individual SV signal channels of L1 C/A (up to 12)
- re-mixes and re-transmits the spoofed signal
- precise phase sync for a smooth take over
- SDR architecture; someday it could be just downloaded and run
- HW parts were off-the-shelf components of approx. $1500 (2008)

[Humphreys, Ledvina, and Shepard, 2008-2011]

THE NEXT TARGET?

- Recall those 37 500 bits of navigation data transmitted on each and every L1 C/A channel
- It has been observed the baseband processors in GPS user modules seldom care about the integrity of this data as well as of the plausibility of PVT results obtained
  - [Sheppard and Humphreys, 2011], [Nighswander et al., 2012]
- Interestingly, this suggests a new infection vector allowing malware installation right into the GPS receiver…
  - shall be covered in the future Cyber Threat Intelligence process

IEMI
INTENTIONAL ELECTROMAGNETIC INTERFERENCE

SMARTPHONE IEMI

audio output is omitted for the clarity,
as we are interested in the input path, now

SMARTPHONE IEMI

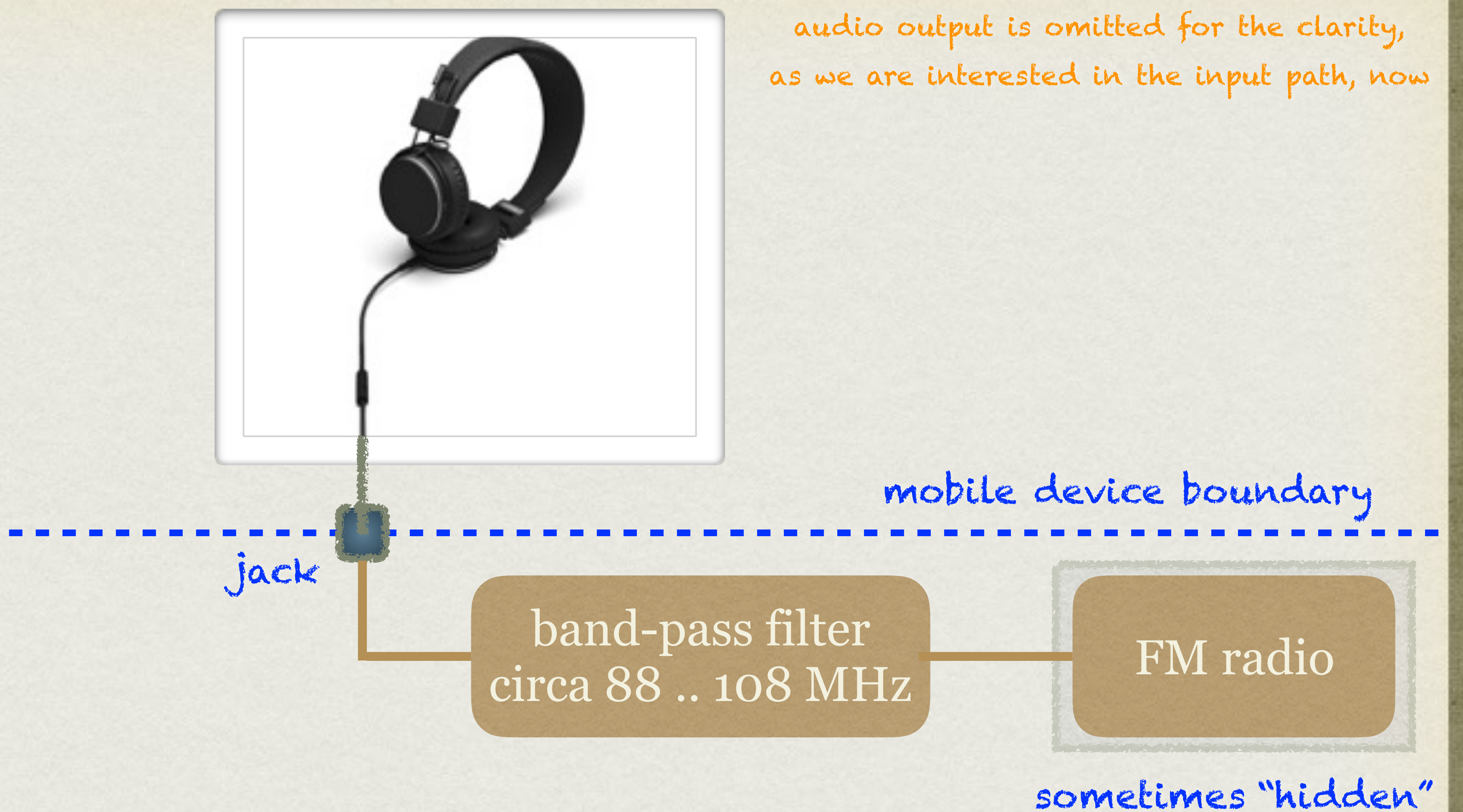
audio output is omitted for the clarity,
as we are interested in the input path, now

mobile device boundary

jack

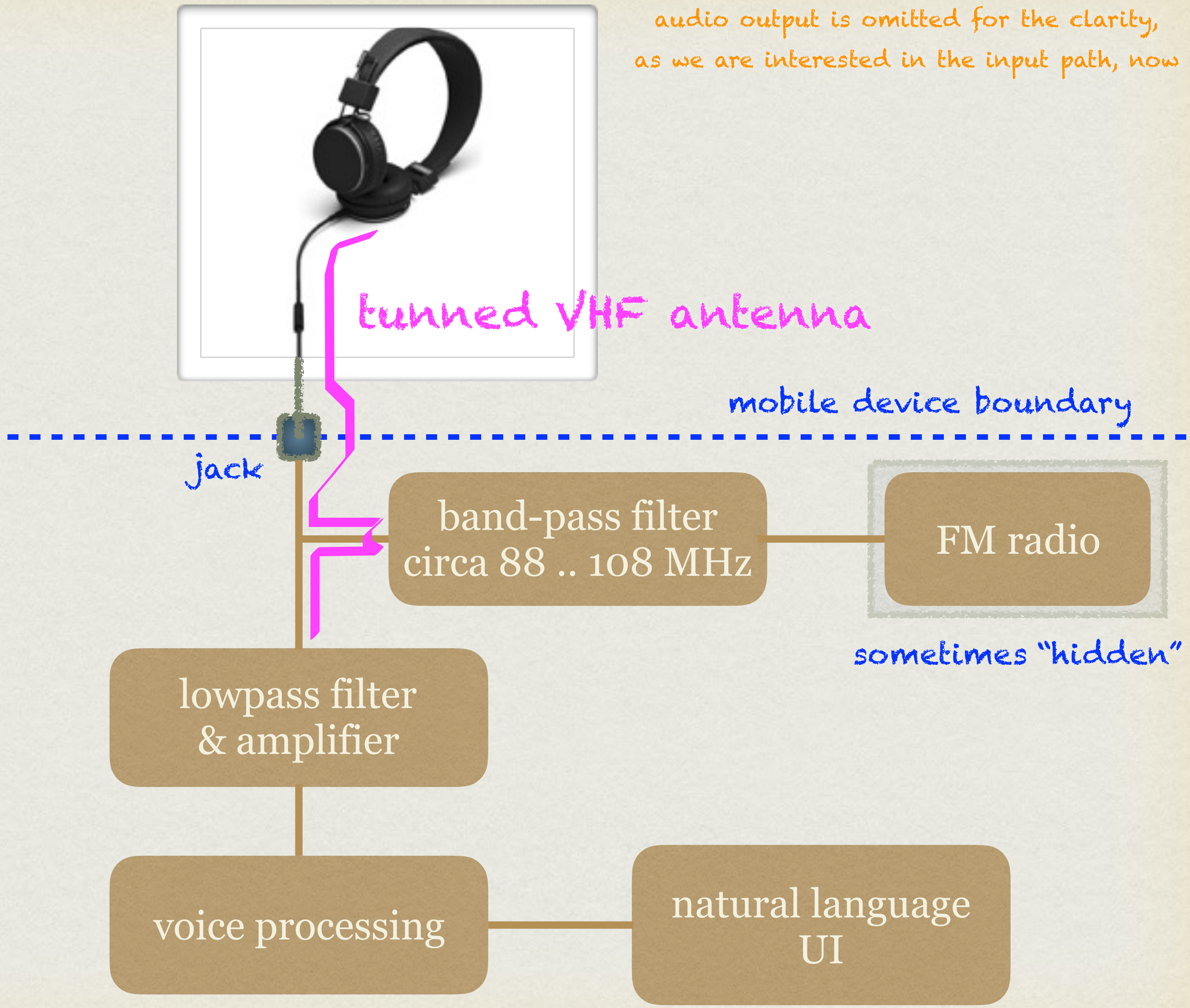
SMARTPHONE IEMI

SMARTPHONE IEMI

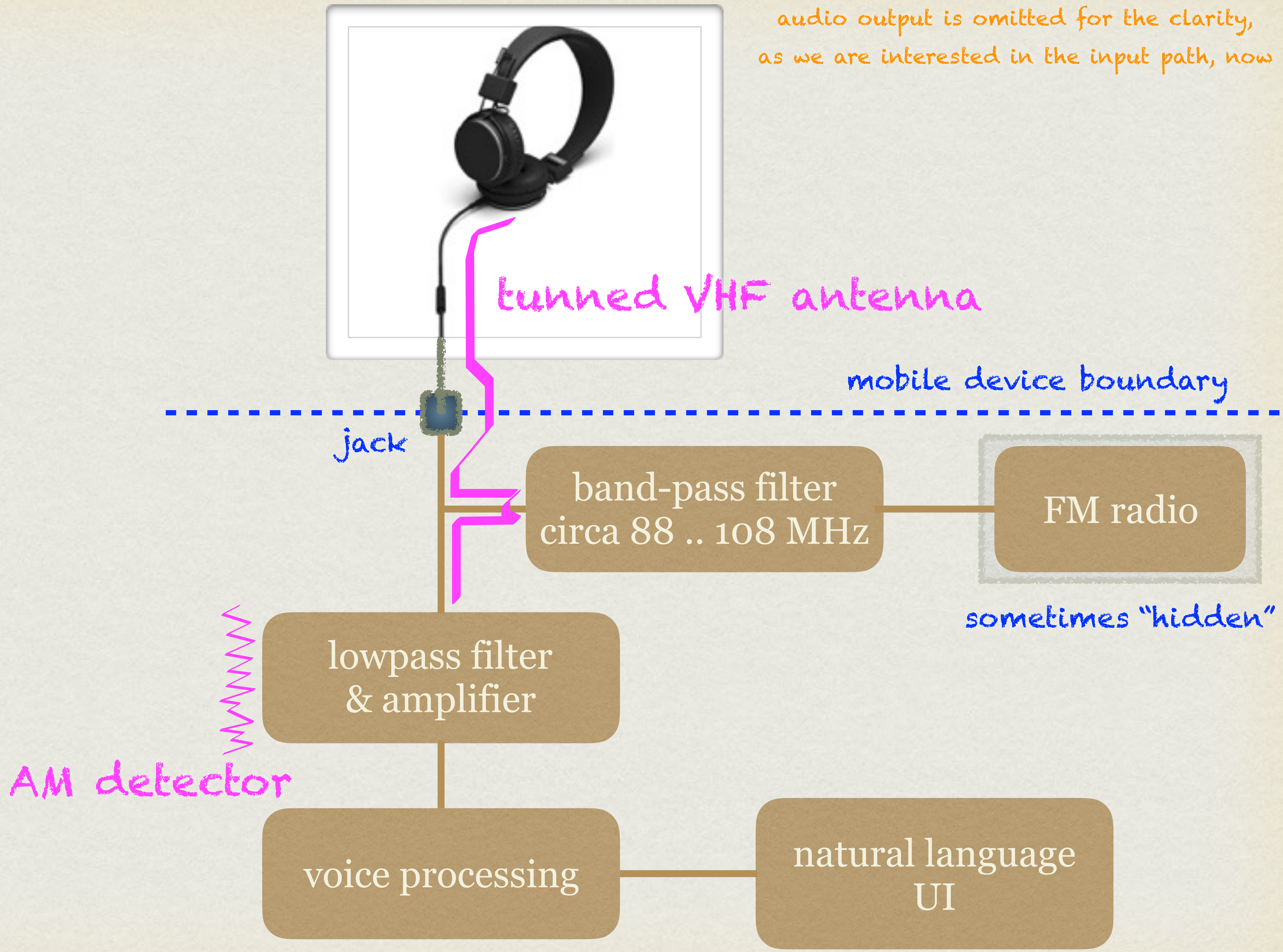


SMARTPHONE IEMI

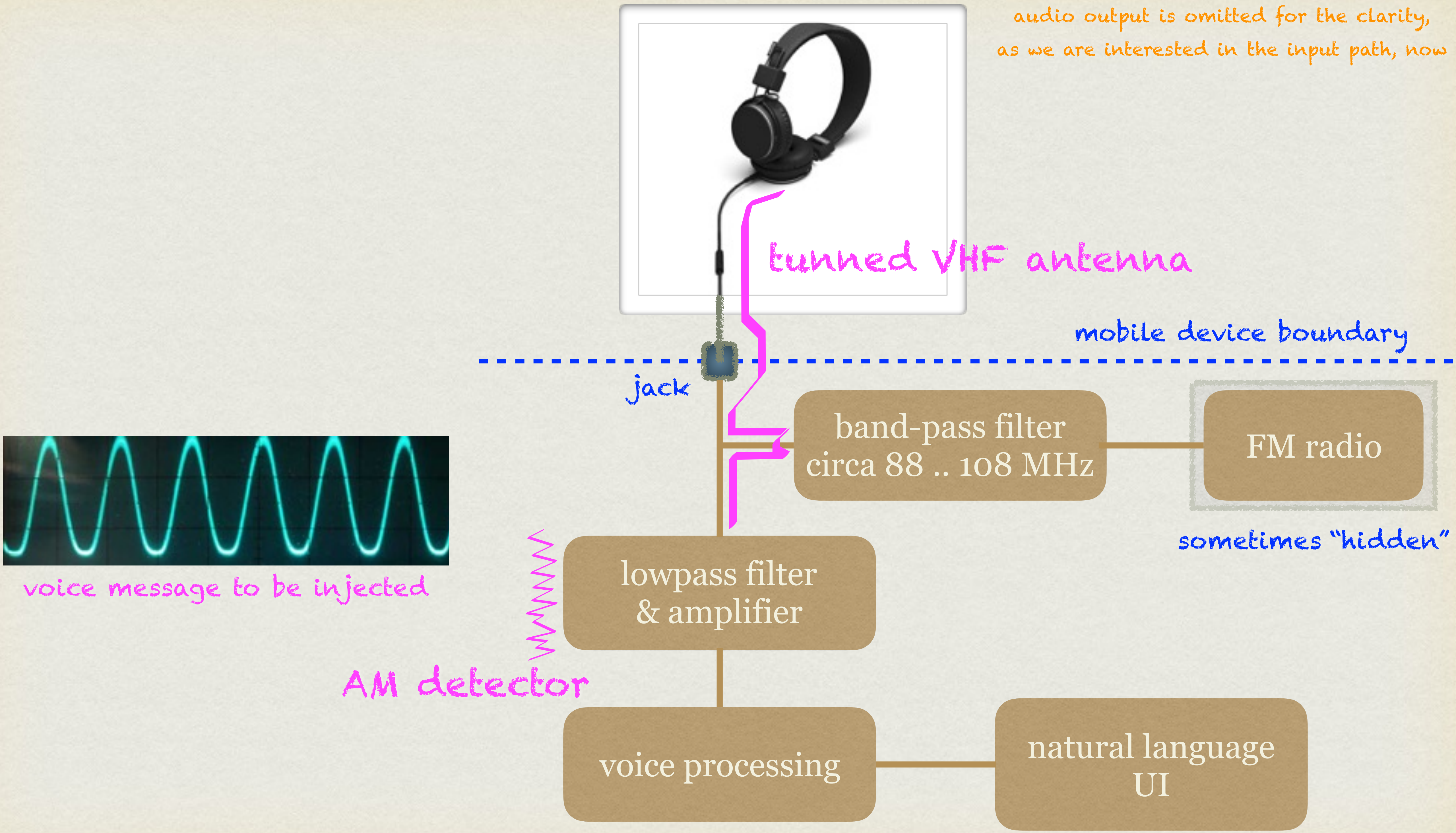
SMARTPHONE IEMI



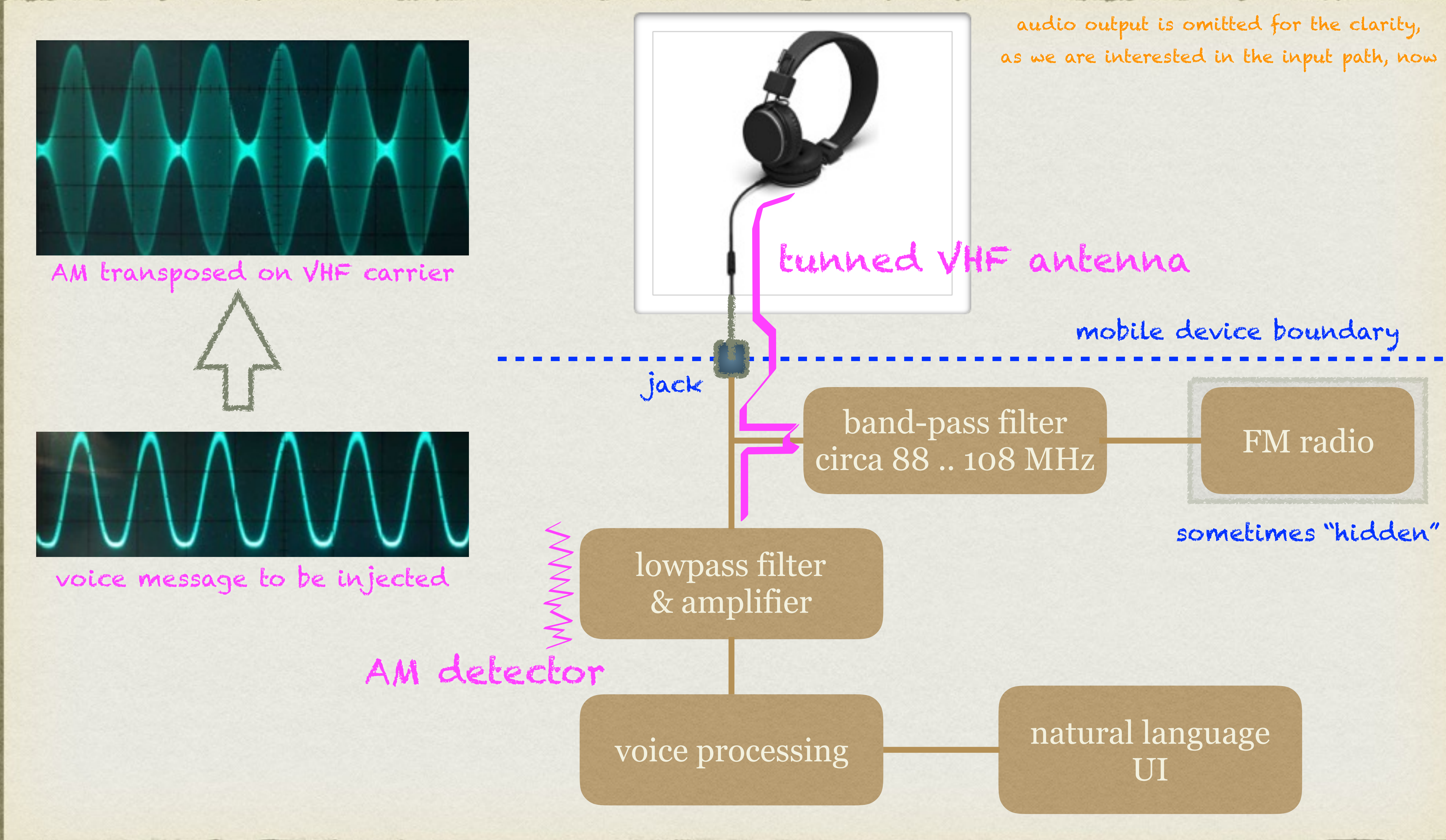
SMARTPHONE IEMI



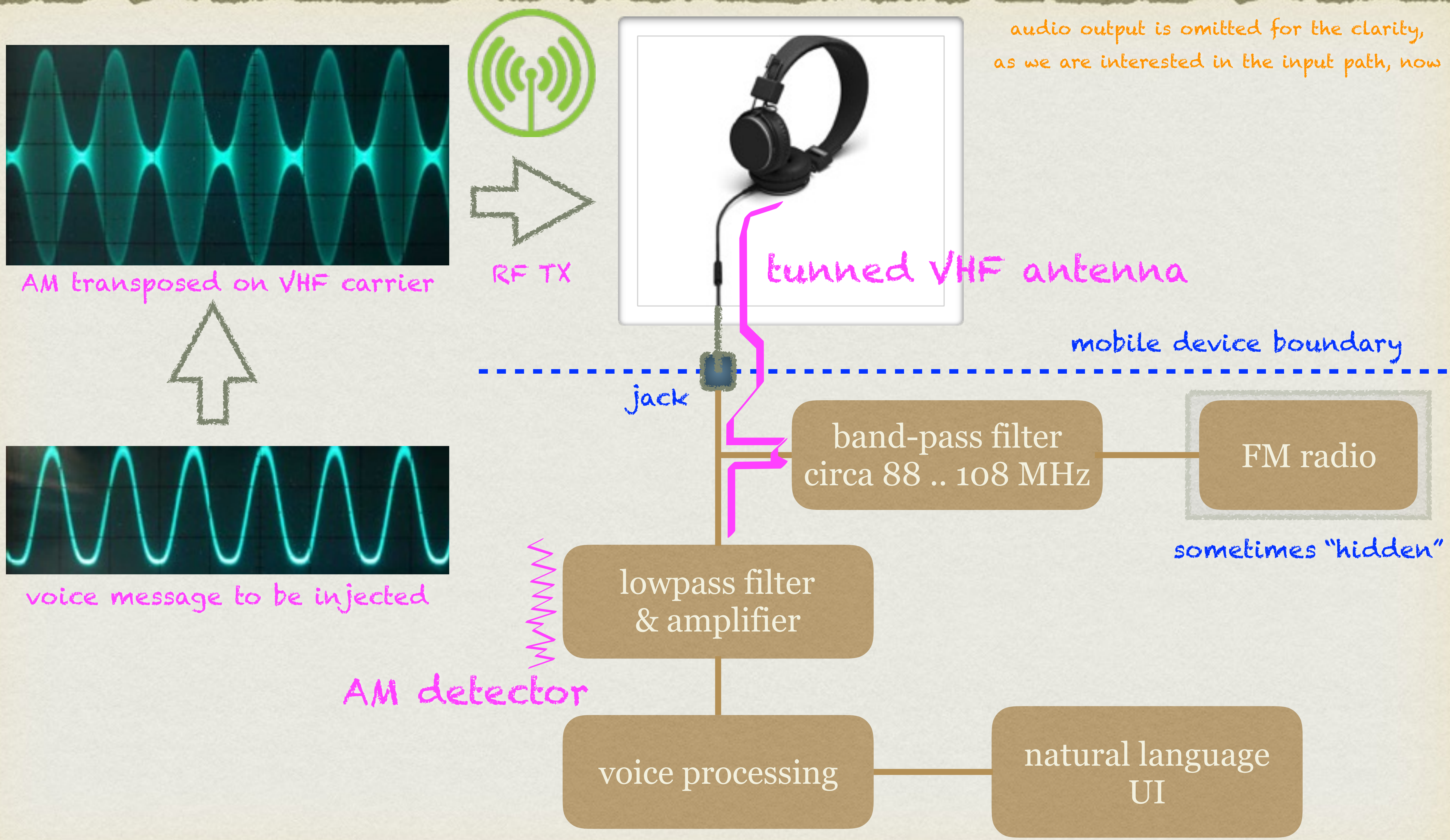
SMARTPHONE IEMI



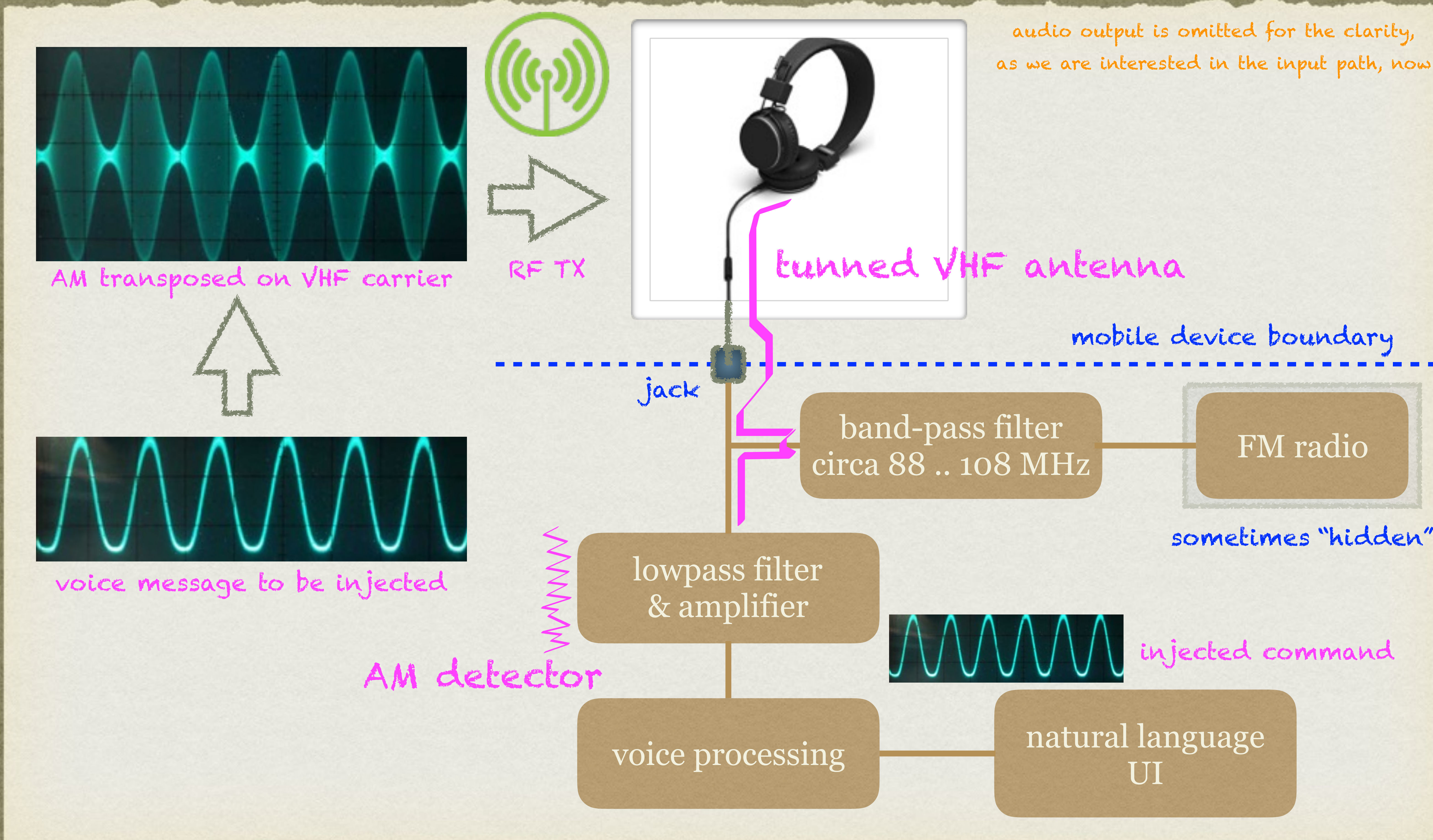
SMARTPHONE IEMI



SMARTPHONE IEMI



SMARTPHONE IEMI



PROOF-OF-CONCEPT

- Described in [Kasmi and Esteves, 2015]
- They were able to inject voice commands into modern smartphones from the far field (Fraunhofer) region in the VHF band
  – the range was, however, still limited to **several metres** with a reasonable equipment
- Required $E_{\mathrm{min}} \approx 25 - 30$ V/m at the victim for the 103 MHz carrier
- Interestingly, in case of the voice assistant did not listen on background, they were even able to "push" the voice command button remotely!
  – this time, it was via FM modulation of the carrier
- They employed the SDR platform with an external power amplifier

THEORETICAL IMPROVEMENTS

- Investigate higher resonant frequencies of the headphones antenna, as they can enhance the energy transfer by an intensive beam forming
- Further exploit the nonlinear distortions of the smartphone input to devise more efficient modulation schemes

CONCLUSION

- RF signals are ubiquitous, we probably cannot live without all that electromagnetic tweeting anymore
- Sometimes, our devices listen even more than they shall
- Often, the relative inaccessibility of the RF interface is the only protection
- SDR phenomenon offers easy access to the whole RF spectrum, while also allowing rapid and massive exploit sharing
- The era of intensive RF hacking is coming and it will go far beyond the usual scope of Wi-Fi and Bluetooth!
- These new attack vectors shall be included into future threat models for RF applications
- We shall require qualified penetration tests and security assessments for each and every critical RF service we have


REALLY, DO THE PENTEST!

REFERENCES - COMMON

1. Balanis, C.-A.: *Antenna Theory - Analysis and Design*, Third Edition, Wiley-Interscience, 2005
2. Boggess, A. and Narcowich, F.-J.: *A First Course in Wavelets with Fourier Analysis*, Second Edition, Wiley, 2009
3. Essick, J.: *Hands-On Introduction to LabVIEW for Scientists and Engineers*, Third Edition, Oxford University Press, 2015
4. Grayver, E.: *Implementing Software Defined Radio*, Springer, 2012
5. Griffiths, D.-J.: *Introduction to Electrodynamics*, Fourth Edition, Pearson, 2013
6. James, J.-F.: *A Student's Guide to Fourier Transforms With Applications in Physics and Engineering*, Third Edition, Cambridge University Press, 2011
7. Johnson, C.-R., Jr., Sethares, W.-A., and Klein, A.-G.: *Software Receiver Design - Build Your Own Digital Communications System in Five Easy Steps*, Cambridge University Press, 2011
8. Kraus, J.-D. and Fleish, D.-A.: *Electromagnetics with Applications*, Fifth Edition, McGraw-Hill, 1999
9. Kraus, J.-D. and Marhefka, R.-J.: *Antennas For All Applications*, Third Edition, McGraw-Hill, 2003
10. Lathi, B.-P. and Green, R.-A.: *Essentials of Digital Signal Processing*, Cambridge University Press, 2014
11. Lyons, R.-G.: *Understanding Digital Signal Processing*, Third Edition, Prentice Hall, 2011
12. Pu, D. and Wyglinski, A.-M.: *Digital Communication Systems Engineering with Software-Defined Radio*, Artech House, 2013
13. Stutzman, W.-L. and Thiele, G.-A.: *Antenna Theory and Design*, Third Edition, Wiley, 2013

REFERENCES - NFC

14. Brown, T.-C.-W. and Diakos, T.: *On the Design of NFC Antennas for Contactless Payment Applications*, 2011

15. Brown, T.-C.-W., Diakos, T., and Briffa, J.-A.: *Evaluating the Eavesdropping Range of Varying Magnetic Field Strengths in NFC Standards*, 2013

16. Diakos, T.-P., Briffa, J.-A., Brown, T.-W.-C., and Wesemeyer, S.: *Eavesdropping near-field contactless payments: a quantitative analysis*, 2013

17. Engelhardt, M., Pfeiffer, F., Finkenzeller, K., and Biebl, E.: *Extending ISO/IEC 14443 Type A Eavesdropping Range using Higher Harmonics*, 2013

18. Finkenzeller, K.: *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*, Third Edition, Wiley, 2010

19. Finkenzeller, K.: *Research Homepage*, http://rfid-handbook.de [checked Nov-23-2015]

20. Finkenzeller, K.: *Known attacks on RFID systems, possible countermeasures and upcoming standardisation activities*, 2009

21. Finkenzeller, K.: *Battery powered tags for ISO/IEC 14443, actively emulating load modulation*, 2011

22. Finkenzeller, K., Pfeiffer, F., and Biebl, E.: *Range Extension of an ISO/IEC 14443 type A RFID System with Actively Emulating Load Modulation*, 2011

23. Francis, L., Hancke, G.-P., Mayes, K., and Markantonakis, K.: *Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones*, 2011

REFERENCES - NFC

24. Hancke, G.-P.: *Research Homepage*, http://www.rfidblog.org.uk/research.html [checked Nov-23-2015]

25. Hancke, G.-P.: *Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens*, 2011

26. Kfir, Z. and Wool, A.: *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems*, 2005

27. Kirschenbaum, I. and Wool, A.: *How to Build a Low-Cost, Extended-Range RFID Skimmer*, 2006

28. Lee, Y.: *Antenna Circuit Design for RFID Applications*, Application Note 710, Microchip Tech. Inc., 2003

29. NXP: *AN1445 - Antenna design guide for MFRC52x, PN51x, and PN3x*, 2010

30. Oren, Y., Schirman, D., and Wool, A.: *Range Extension Attacks on Contactless Smart Cards*, 2013

31. Pfeiffer, F., Finkenzeller, K., and Biebl, E.: T*heoretical Limits of ISO/IEC 14443 type A Eavesdropping Attacks*, 2012

32. Rosa, T.: *RFID Wormholes – the Case of Contactless Smart Cards*, 2011

33. Thevenon, P.-H., Savry, O., Tedjini, S., and Malherbi-Martins, R.: *Attacks on the HF Physical Layer of Contactless and RFID Systems*, 2011

REFERENCES - NFC

34. ISO/IEC 14443-1: *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 1: Physical characteristics*, 2000

35. ISO/IEC 14443-2: *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface*, 2001

36. ISO/IEC 14443-3: *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision*, 2001

37. ISO/IEC 14443-4: *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol*, 2001

38. ISO/IEC 18092: *Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1)*, 2004

39. NFC Forum: *NFC Digital Protocol*, Technical Specification, 2010

40. EMV Contactless Specifications for Payment Systems: *Book D - EMV Contactless Communication Protocol Specification*, 2015

REFERENCES - GPS

41. Bonebrake C. and O'Neil, L.-R.: *Attacks on GPS Time Reliability*, IEEE Security & Privacy, May/June 2014, pp. 82-84, 2014

42. Borre, K., Akos, D.-M., Bertelsen, N., Rinder, P., Jensen, S.-H.: *A Software-Defined GPS and Galileo Receiver (Applied and Numerical Harmonic Analysis)*, Birkhäuser Boston, 2007

43. Chen, J., Zhang, S., Wang, H., and Zhang, X.: *Practicing a record-and-replay system on USRP*, In Proc. of the second workshop on Software radio implementation forum, pp. 61-64. ACM, 2013

44. Doberstein, D.: *Fundamentals of GPS Receivers - A Hardware Approach*, Springer, 2011

45. Fernández-Prades, C., Arribas, J., and Closas, P.: *Turning a television into a GNSS receiver*, In Proc. of ION GNSS, pp. 1492-1507. 2013

46. Huang, L. and Yang, Q.: *GPS Spoofing - Low-cost GPS Simulator*, DEF CON 23, Las Vegas, August 6th - 9th, 2015

47. Humphreys, T.-E., Ledvina, B.-M., Psiaki, M.-L., O'Hanlon, W.-O., and Kintner, P.-M., Jr.: *Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer*, In Proc. of the ION GNSS international technical meeting of the satellite division, vol. 55, p. 56. 2008

48. Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., Lachapelle, G.: *GPS vulnerability to spoofing threats and a review of antispoofing techniques*, International Journal of Navigation and Observation, 2012

49. Kaplan, E.-D. and Hegarty, C.-J. (Eds): *Understanding GPS - Principles and Applications*, Second Edition, Artech House, 2006

50. Malhotra, A,, Cohen, I.-E., Brakke, E., Goldberg, S.: *Attacking the Network Time Protocol*, First public posting manuscript, October 21, 2015

REFERENCES - GPS

51. McMilin, E.-B., Chen, Y.-H., De Lorenzo, D.-S., Akos, D.-M., Walter, T.-F., Lee, T.-H., Enge, P.-K.: S*ingle Antenna, Dual Use: Theory and Field Trial Results for Aerial Applications of Anti-Jam and Spoof Detection*, Inside GNSS, September/October 2015, pp. 40-53, 2015

52. Misra, P. and Enge, P.: *Global Positioning System - Signals, Measurements, and Performance*, Revised Second Edition, Ganga-Jamuna Press, 2012

53. Nighswander, T., Ledvina, B., Diamond, J., Brumley, R., and Brumley, D.: *GPS Software Attacks*, In Proc. of the 2012 ACM conference on Computer and communications security, pp. 450-461, ACM, 2012

54. Shepard, D.-P. and Humphreys, T.-E.: *Characterization of Receiver Response to Spoofing Attack*, In Proc. of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation, p. 2608, 2011

55. Shepard, D.-P., Humphreys, T.-E., and Fansler, A.-A.: *Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks*, International Journal of Critical Infrastructure Protection 5, no. 3, pp. 146-153, 2012

56. Thompson, E.-A., Clem, N., Renninger, I., and Loos, T.: *Software-defined GPS receiver on USRP-platform*, Journal of Network and Computer Applications 35, no. 4 pp. 1352-1360, 2012

57. Tippenhauer, N.-O., Pöpper, C., Rasmussen, K.-B., and Capkun, S.: *On the requirements for successful GPS spoofing attacks, In Proc. of the 18th ACM conference on Computer and communications security*, pp. 75-86. ACM, 2011

58. John A. Volpe National Transportation Systems Center: V*ulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System*, Final Report for the Office of the Assistant Secretary for Transportation Policy, U.S. Department of Transportation, August 29, 2001

59. Wan, X. and Zhan, X.: *The research of indoor navigation system using pseudolites*, Procedia Engineering 15 (2011), pp. 1446-1450, 2011

REFERENCES - IEMI

60. Kasmi, C. and Esteves, J.-L.: *IEMI Threats for Information Security: Remote Command Injection on Modern Smartphones*, IEEE Trans. on Electromagnetic Compatibility, Issue 99, pp. 1-4, 2015

61. Kasmi, C. and Esteves, J.-L.: *You Don't Hear Me But Your Phone's Voice Interface Does*, Hack In Paris, June 18th, 2015 [includes video

THANK YOU