EMC Testing Challenges Beyond 40 GHz

Jeremy Cline
Product Manager

ROHDE&SCHWARZ
Make ideas real

Speaker Introduction

Jeremy Cline
Product Manager
EMC Products/Systems

2019 — Primary representative, ANSI C63 Committee

Product Manager

2015 — M.S. Medical Device and Diagnostic Engineering

2013 — Application Engineer

Sales Engineer

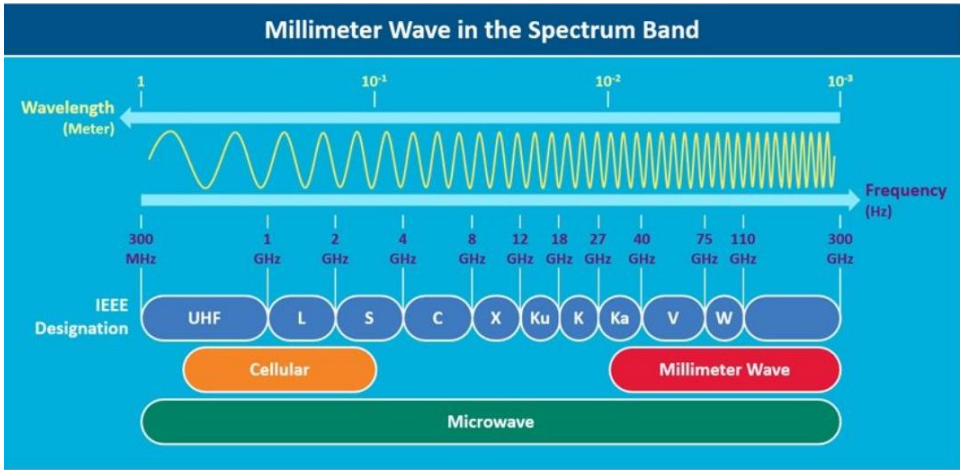
2010 — B.S. Electrical Engineering

Agenda

- 5G is everywhere!
- Standards are evolving
- Cybersecurity concerns
- I/Q record and replay
- Q&A

Industry Trend #1: 5G is everywhere!

- **We must test higher and higher frequencies**
  - Radiated Spurious Emissions (RSE) up to 200 GHz
  - (Automotive) Radar testing up to 77 – 300 GHz
  - CE106 requirements up to 100 GHz



[1] everythingRF: "What are Millimeter Waves?"

Radiated Spurious Emissions (RSE) Testing

- RSE is typically performed within a chamber (**radiated**) to determine if an intentional radiator (**spurious**) is creating energy at harmonics that is beyond a defined limit line (**emissions**).
- CE106 and RE103 requirements have very similar wording to this

5.6.2 CE106 limits.

Conducted emissions at the EUT antenna port shall not exceed the values given below.

a. Receivers: 34 dBµV

b. Transmitters and amplifiers (standby mode): 34 dBµV

c. Transmitters and amplifiers (transmit mode): Harmonics, except the second and third, and all other spurious emissions shall be at least 80 dB down from the level at the fundamental. The second and third harmonics shall be suppressed to a level of -20 dBm or 80 dB below the fundamental, whichever requires less suppression. For Navy shipboard applications, the second and third harmonics will be suppressed to a level of -20 dBm and all other harmonics and spurious emissions shall be suppressed to -40 dBm, except if the duty cycle of the emissions are less than 0.2%, then the limit may be relaxed to 0 dBm.

5.19.3 RE103 test procedures.

5.19.3.1 Purpose.

This test procedure is used to verify that radiated spurious and harmonic emissions from transmitters do not exceed the specified requirements.

5G Testing Specifications

- **Two basic frequency ranges (FR1 and FR2) are used in 3GPP specifications**
  - FR1: 450 MHz to 6 GHz
  - FR2: 24.25 to 52.6 GHz for 3GPP Release 15

3GPP NR Specification Overview	
Series	**Title**
38.1xx	RF test specifications (UE and BS)
38.2xx	Layer 1 (physical layer) specifications
38.3xx	Layer 2 / Layer 3 specifications
38.4xx	Core network specifications and fronthaul interface specification (F1)
38.5xx	UE conformance testing specifications for RF, RRM and protocol testing
37.324	E-UTRA and NR; Service Data Adaptation Protocol (SDAP) specification
37.340	NR; Multi-connectivity; Overall description; Stage-2

5G FR2 Test Requirements

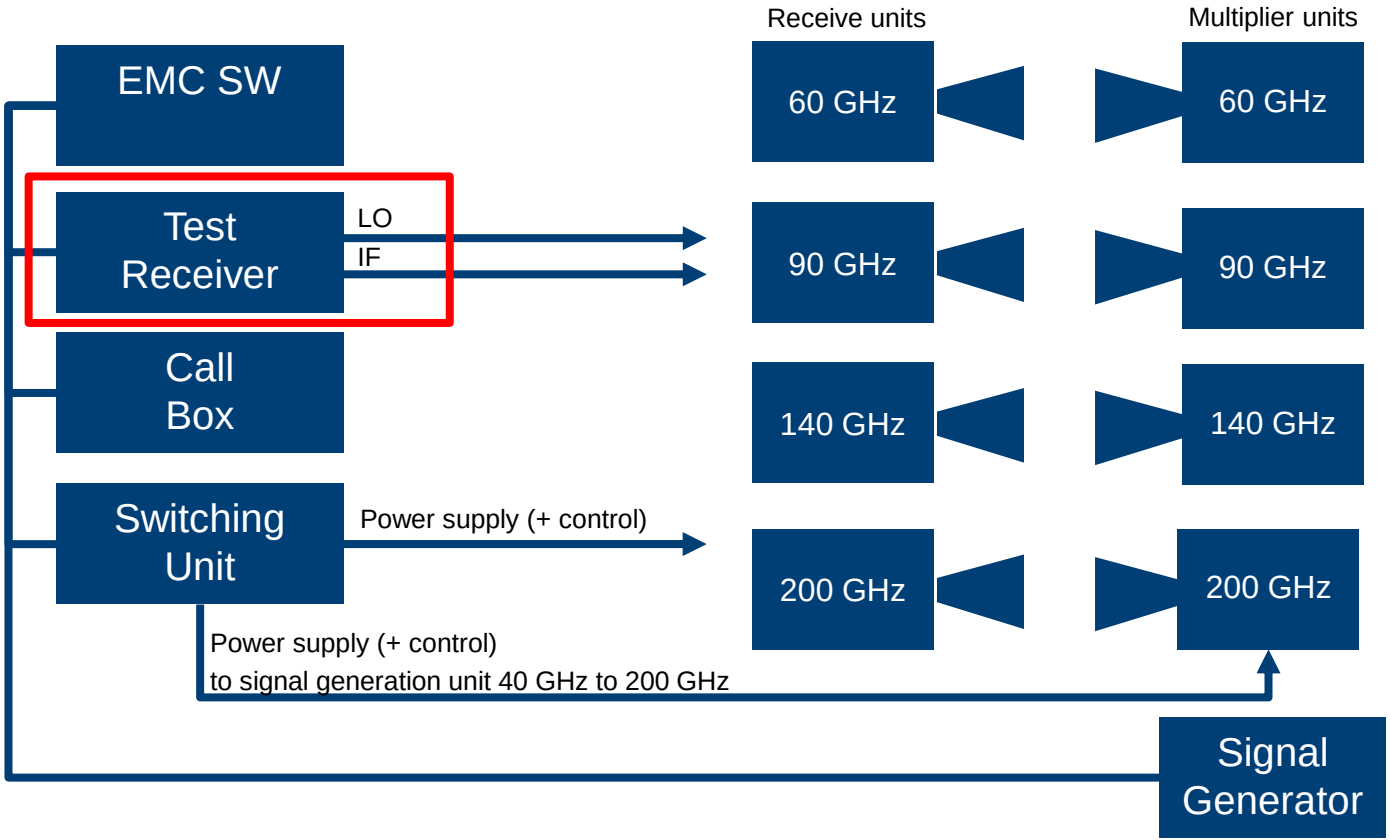
3GPP / RAN4:

- RSE specification 9 kHz to 2nd harmonic
- RSE test requirement 6 GHz to 2nd harmonic
- Limit -13 dBm, Method: TRP
- Details of TRP measurement and limit under discussion

FCC 47 CFR Part 30, KDB 842590, April 2019:

- 30 MHz up to 5th harmonic / 100 GHz (devices < 30 GHz), 200 GHz (devices > 30 GHz),
- Limit -13 dBm, Method: TRP
- Early exit criteria for EIRP, TRP only for failing frequencies
- Test distance ≥ $2D^2/\lambda$, D: Max. dimension DUT antenna and measurement antenna, spurious: only measurement antenna
- Procedure acc. ANSI C63.26 below 40 GHz

5G FR2 Solution Including System Verification



Radar Echo Simulator

Measurements beyond 44 GHz

- **Harmonic mixers** extend the frequency coverage of testing equipment up to 500 GHz.

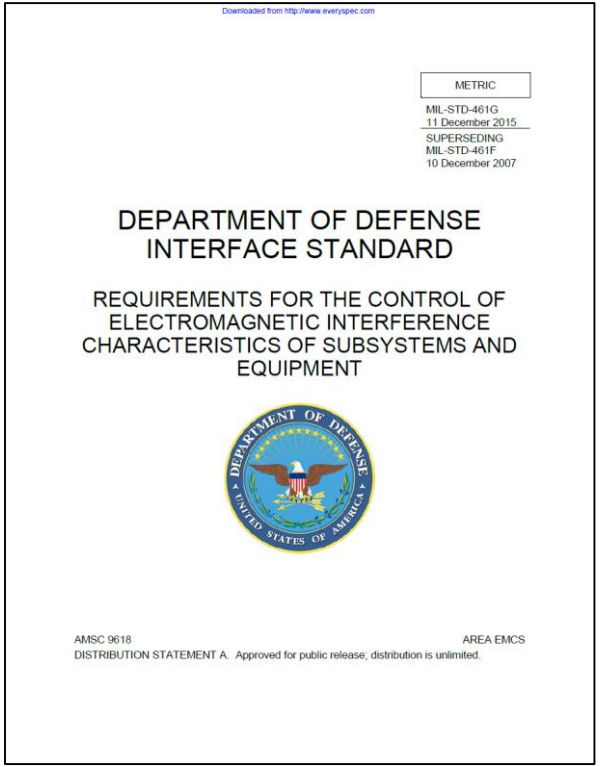
- **Common use cases:**
  - FCC compliance test up to 5th order harmonics
  - 3GPP compliance test up to 2nd order harmonics
  - Radar testing e.g. 77 – 300 GHz
  - A&D applications analyzing interferers up to 110 GHz or higher

Agenda

- 5G is everywhere!
- **Standards are evolving**
- Cybersecurity concerns
- I/Q record and replay
- Q&A

EMC standards are evolving

- **New NATO SDIP-27 TEMPEST standard coming**
  - Might drive frequency requirements up to 40 GHz
- **DO-160H is under development**
  - There has been discussion of emissions requirements up to 18/40 GHz and beyond
  - There is heavy discussion about accepting FFT into the standard
- **MIL-STD 461H**
  - There has been discussion about including requirements around automated visual inspection

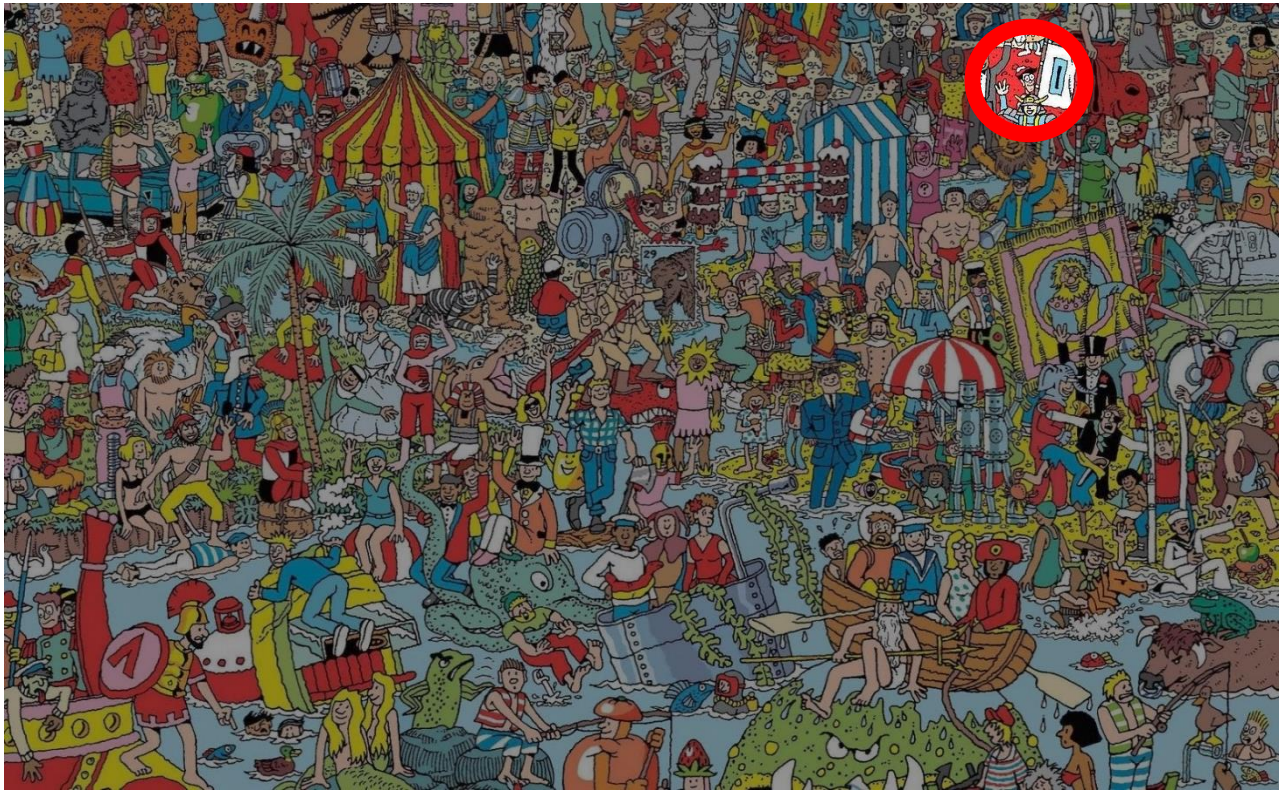


History of MIL-STD 461

- **Major revision released every 6-8 years**
- **New A&D programs starting 2015 or later are using MIL-STD 461 Rev. G**
- **Draft is underway for MIL-STD 461 Rev. H**
  - CE106 up to 100 GHz?
  - Visual inspection requirements?

1967	**461**
1968	**461A**
1969	**461 A Notice 1 / 2**
1970	**461 A Notice 3**
1971	**461 A Notice 4**
1973	**461 A Notice 5 / 6**
1980	**461 B**
1986	**461 C**
1987	**461 C Notice 1 / 2**
1993	**461 D**
1999	**461 E**
2007	**461 F**
2015	**461 G**
202?	**461 H (Draft)**

What is visual inspection?

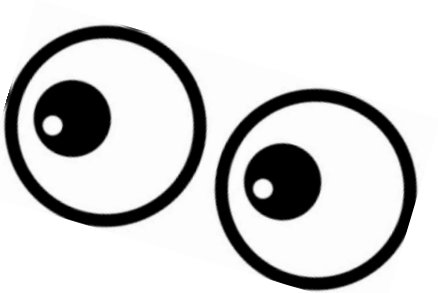


[3] Knight, Shawn. 13 Aug 2018. TechSpot.

Equipment Under Test (EUT) Monitoring

Manual observation

- Time consuming
- Exhausting
- Boring
- Error-prone



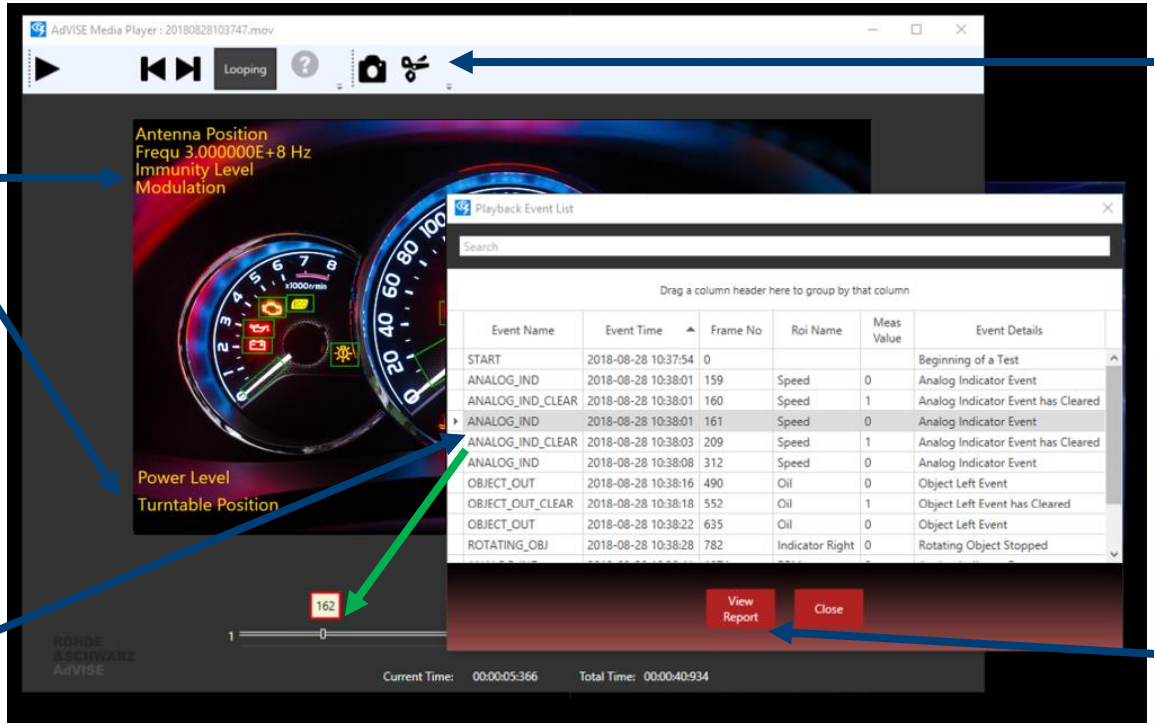
Automated Visual Inspection

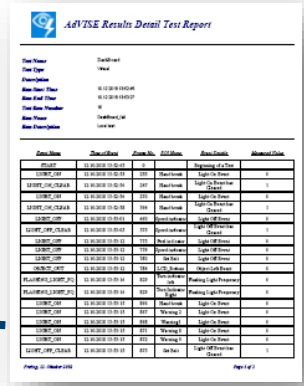
Superimposed EMS test information

Event controlled video player

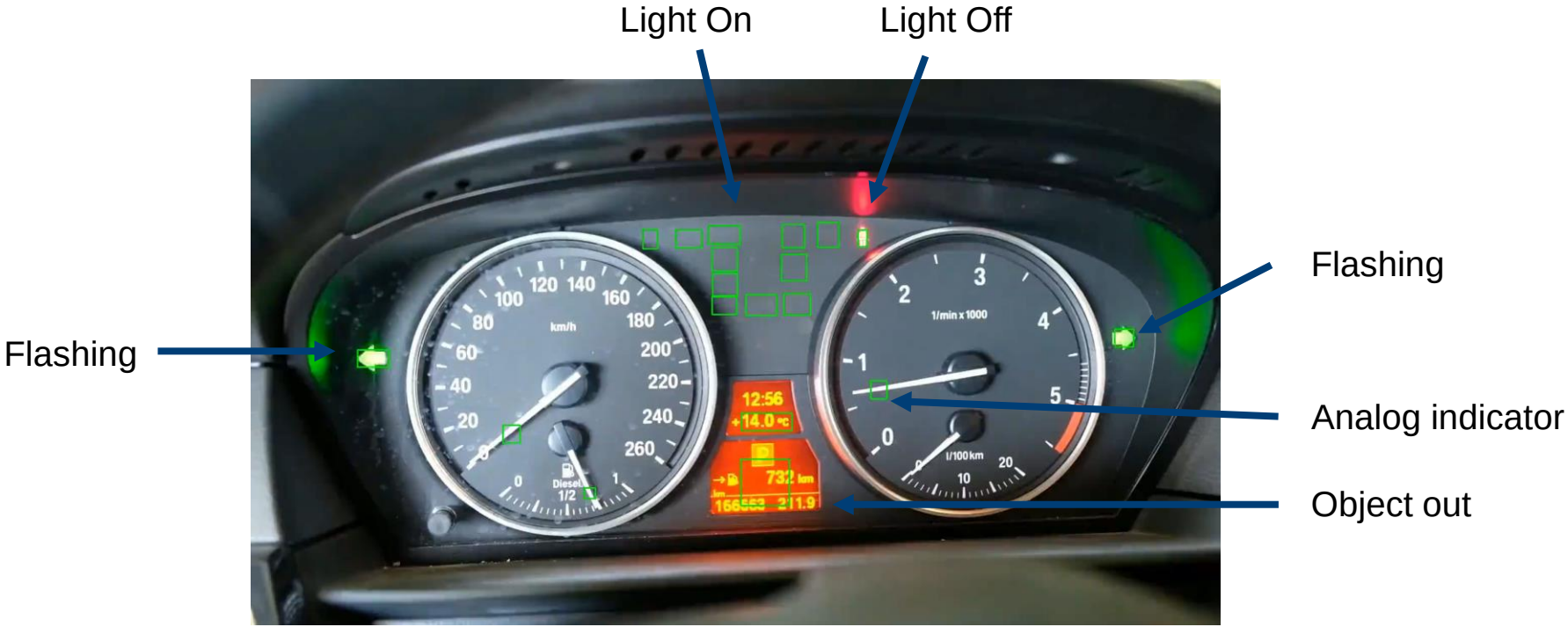
Image or Video extraction

Test report





Automated Visual Inspection



Agenda

- 5G is everywhere!
- Standards are evolving
- **Cybersecurity concerns**
- I/Q record and replay
- Q&A

Industry Trend #3: Cybersecurity concerns have increased

"I think it's more than likely we're going to end up, if we end up in a war - a real shooting war with a major power - it's going to be as a consequence of a cyber breach of great consequence and it's increasing exponentially, the capabilities," Biden said during a half-hour speech while visiting the Office of the Director of National Intelligence (ODNI). (July 27, 2021)

[4] Reuters. Bose, Nandita: "Biden: If U.S. has 'real shooting war' it could be a result of cyber attacks."

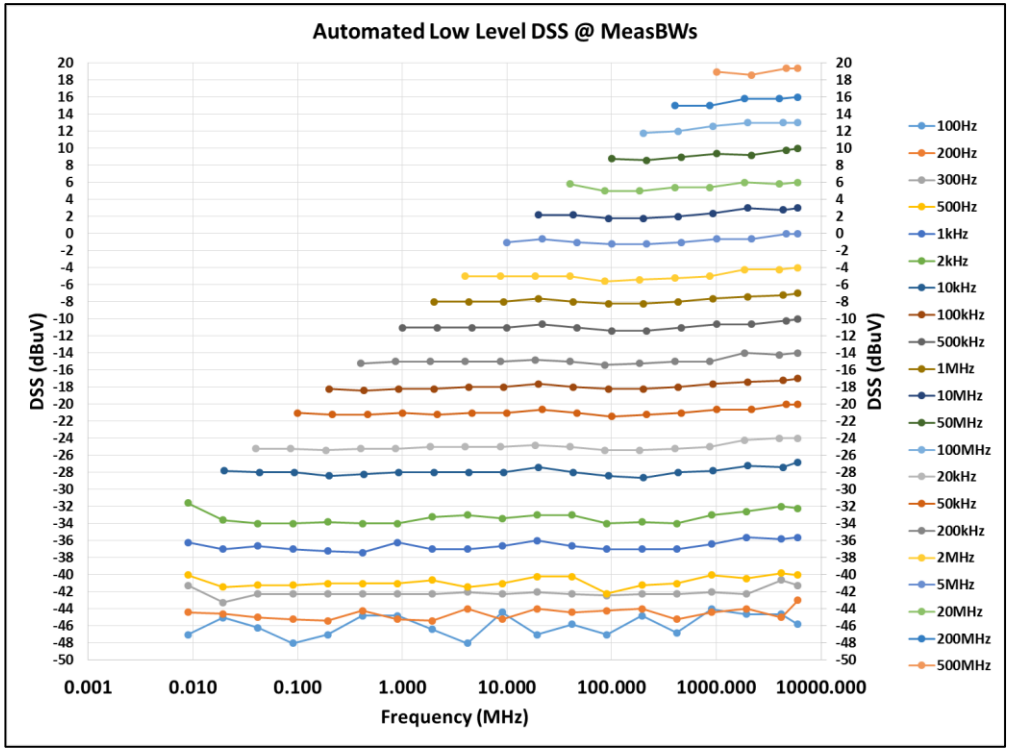
What is TEMPEST?

- Officially, “TEMPEST” does not stand for anything
- ~~Tiny ElectroMagnetic Particles Emitting Secret Things~~
- Telecommunications Electronics Material Protected from Emanating Spurious Transmissions

- **“Compromising Emanations”**
  - TEMPEST is the art & science of verifying that classified information is not inadvertently modulated onto a signal that could be publicly disseminated
  - It is an extension of surveillance and EMC
  - TEMPEST is more than finding the signal as in EMI; it is about finding and then demodulating the signal and determining if classified information is present

TEMPEST Test Challenges

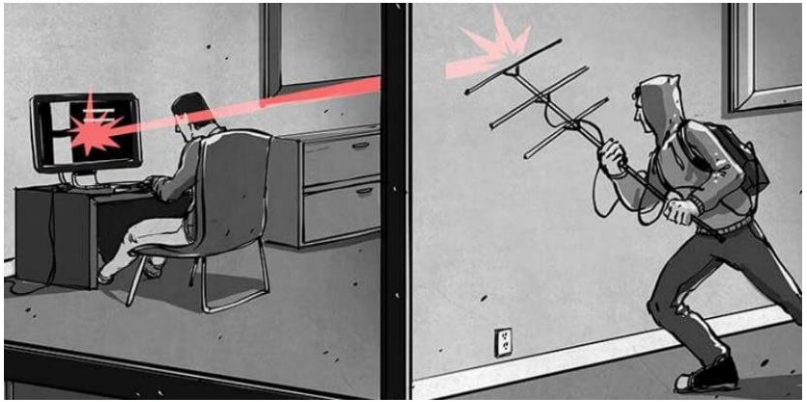
- **Dynamic range (DSS)**
- **Video rastering**
- **Signal analysis / recording**



Example measurement for Detection System Sensitivity (DSS)

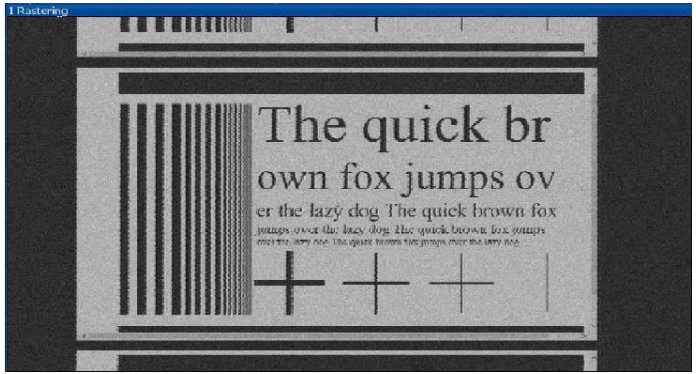
What is rastering?

- A **raster** is a dot matrix data structure that represents a generally rectangular grid of pixels that are viewable via a monitor, paper, or other display medium.
- PC monitors and video screens emit electromagnetic radiation, which may reveal the displayed content.
- Rastering is the process of recreating this content over the air using an unintended RF emission.



Fictional scenario involving a hacker recording RFI from a remote PC.

[5] "Using an RTL-SDR and TEMPEST To Attack AES." RTL-SDR.com.

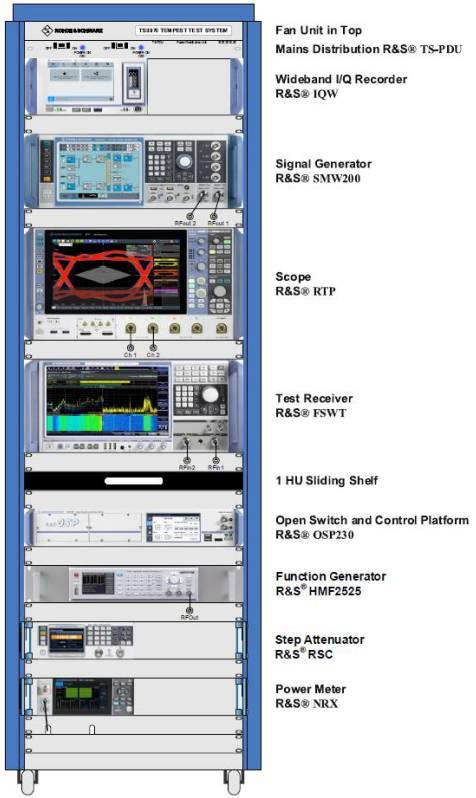


Video rastering example

TEMPEST Solutions

- **Specialized test receivers**
- **Antennas**
- **Test systems**

Active antenna system



TEMPEST rack system

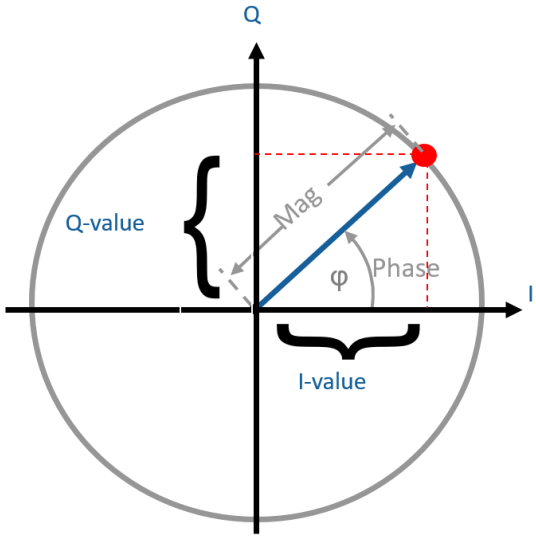
Agenda

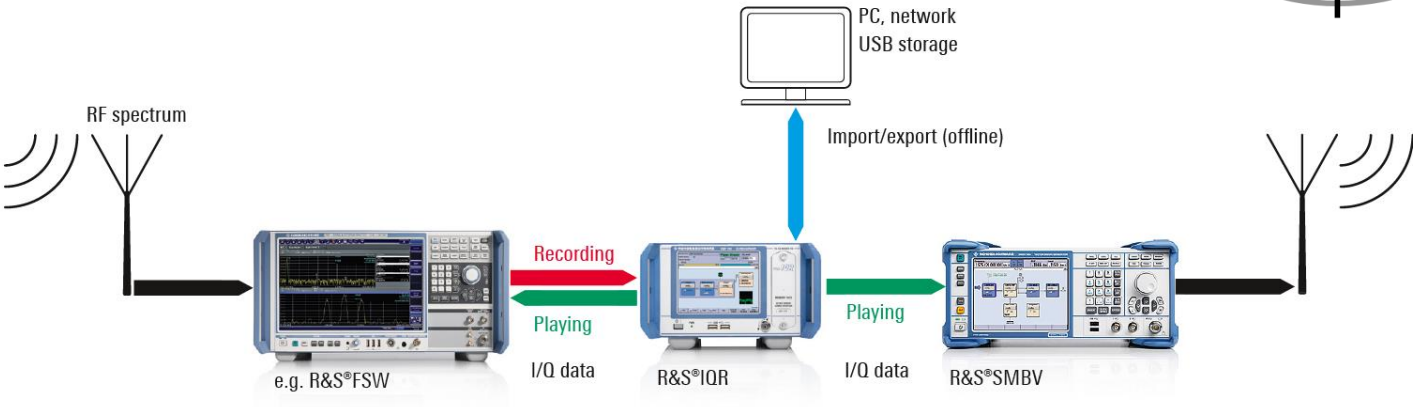
- 5G is everywhere!
- Standards are evolving
- Cybersecurity concerns
- **I/Q record and replay**
- Q&A

Industry Trend #4: I/Q Record and Replay

- **I/Q steaming (i.e. record and replay)** is the ability to record the RF environment and replay it for stress testing

- Long-term recording is very helpful when we want to precisely reproduce an RF environment or scenario





Testing Challenges

- **Coexistence and spectrum refarming**
  - How do signals interact?
  - Can higher frequencies work better?

- **Improvised explosive devices**
  - 5G commercially-available modules
  - How do you stay safe?

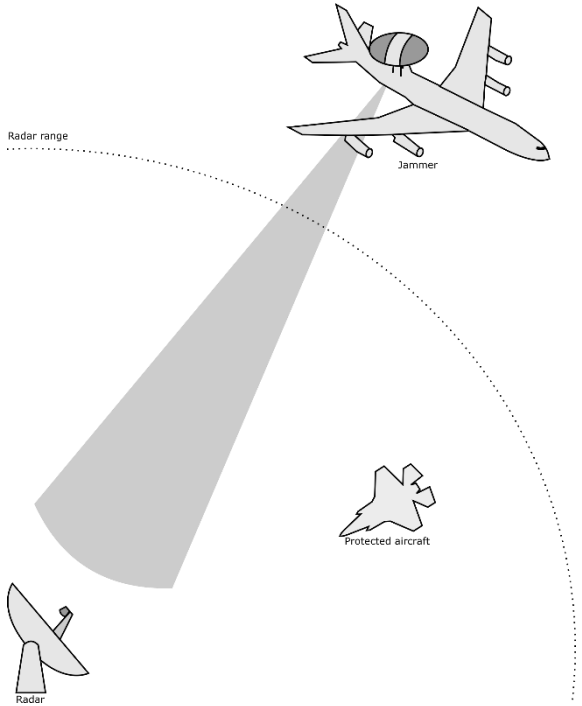
[6] Mcity Test Facility

[7] Improved Explosive Device (IED) using a cell phone

Testing Challenges

- **Electronic countermeasures**
  - Jammer development
- **TEMPEST**
  - Characterize compromising emanations

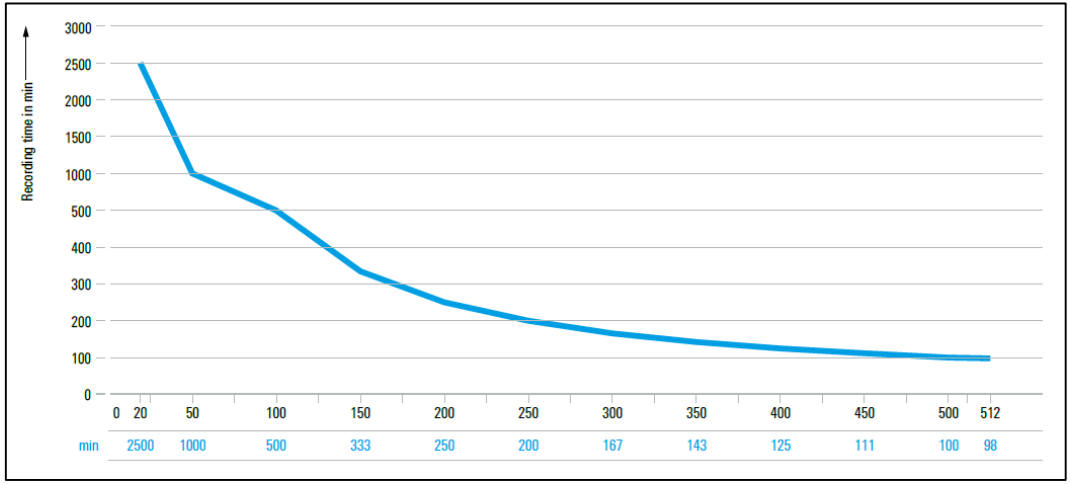
[8] 5G and GPS jammer



[9] Radar jamming example

I/Q Testing Solutions

- **Record the RF environment**
  - Dedicated I/Q recorders
  - Very large hard drives (3 TB+)



Recording time as a function of bandwidth for a 15TB hard drive

MHz	20	50	100	150	200
mins	533	213	106	71	53

3.2 TB

MHz	20	50	100	150	200	250	300	350	400	450	500	512	1000
mins	1066	426	213	142	106	85	71	61	53	47	42	41	27

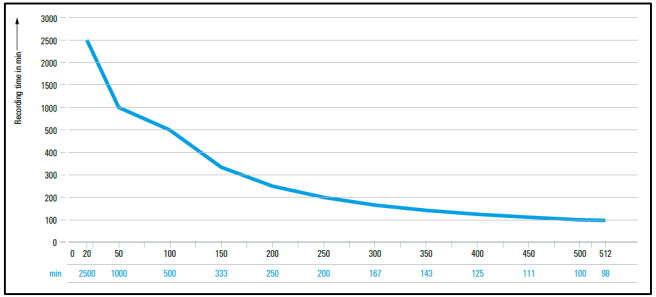
6.4 TB

MHz	20	50	100	150	200	250	300	350	400	450	500	512	1000
mins	2500	1000	500	333	250	200	166	142	125	111	100	97	65

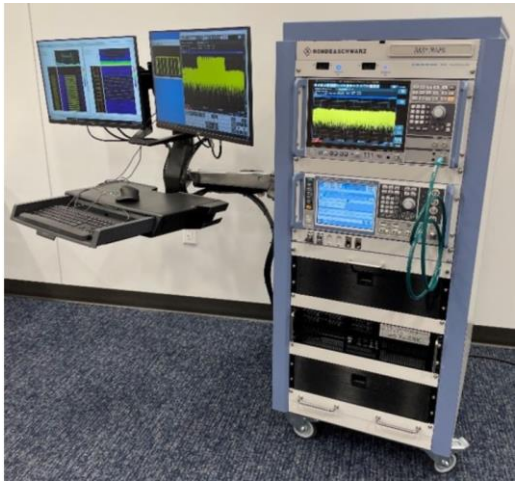
15 TB

I/Q Testing Solutions

- **Record the RF environment**
  - Dedicated I/Q recorders
  - Very large hard drives (1-3 TB+)
- **Analyze the signals**
  - Constellation diagrams
  - Vector signal analysis software
- **Replay the signals**
  - Signal generators w/ ARB
  - Antenna



Recording time as a function of bandwidth



Integrated Record, Analyze, Replay System (IRAPS)

Wrap up

- Industry requirements are going up to 300 GHz and beyond
- Emerging applications include 5G RSE, radar testing, TEMPEST, and more
- MIL-STD 461H effort is underway, may include visual inspection

Thank you for your attention!

…any questions?