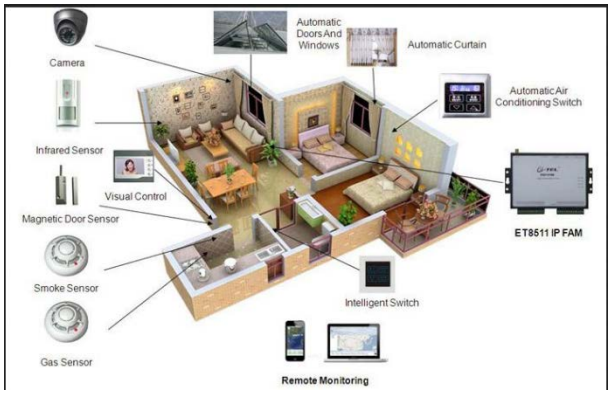
Saving our Spectrum: Handling Radio Layer Vulnerabilities in Wireless Systems

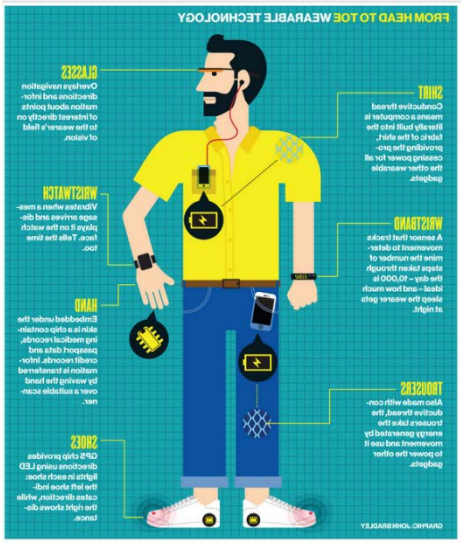
Opening Keynote
Julius Knapp, Chief
Office of Engineering and Technology
Federal Communications Commission

October 10, 2019

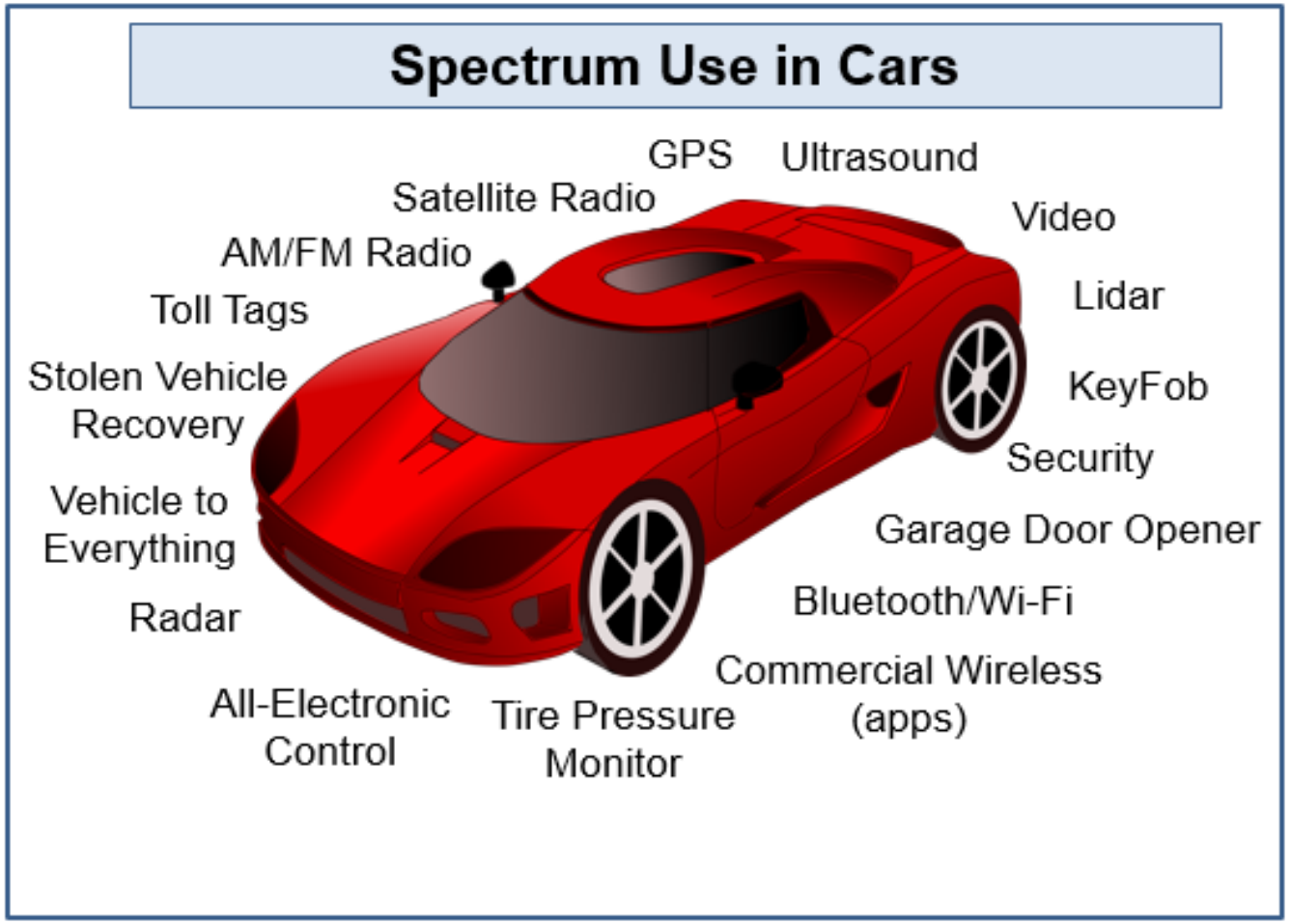
Note: The views expressed in this presentation are those of the author and may not necessarily represent the views of the Federal Communications Commission

The World is Going Wireless!

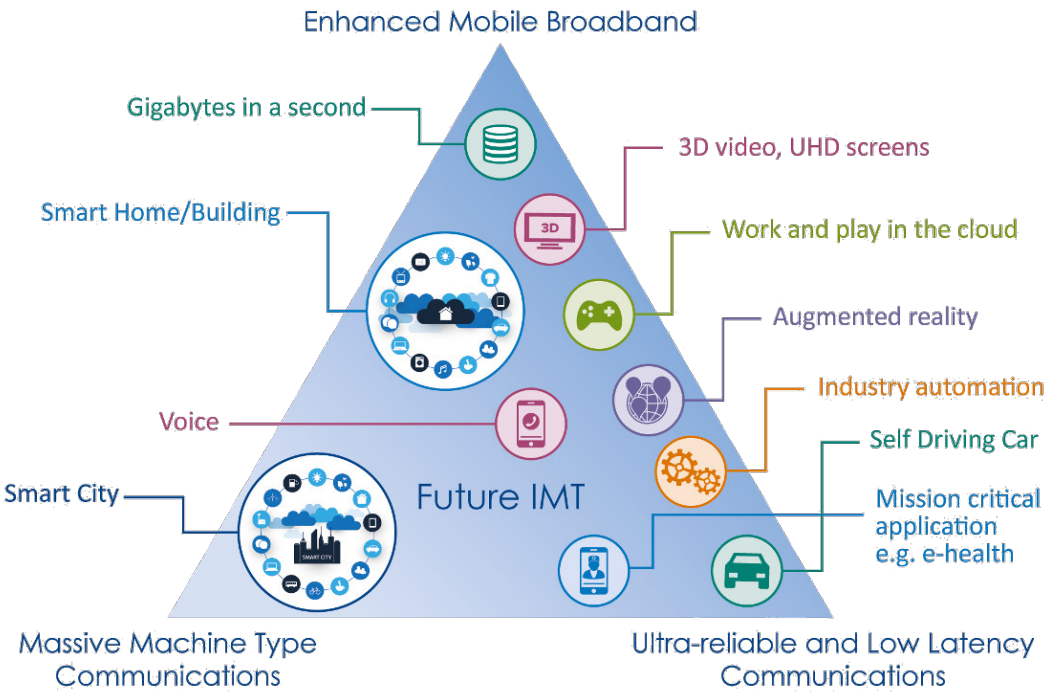




Focus: Radio Technology in Cars



5G Will Greatly Expand Use Cases



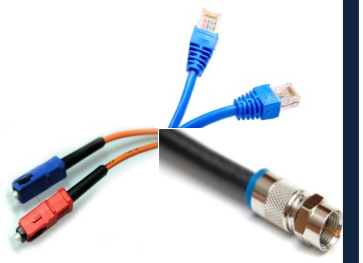
- Public Safety
- Transportation
- Healthcare
- Education
- Energy
- Media
- Smart Cities
- Agriculture
- Building & Home Automation
- And Others . . .

Connectivity Technologies

Source: Courtesy Bill Morelli, IHS Technologies
Presentation to FCC Technological Advisory Council

Wired

- Ethernet, Coax, Fiber, etc. considered as a single category



WPAN

- ANT+
- Bluetooth – Classic & Smart Ready
- Bluetooth Smart

- ZigBee PRO
- ZigBee RF4CE
- ZigBee Multi-Protocol
- EnOcean
- ISA100.11a
- WirelessHART
- Z-Wave
- Other 802.15.4

WLAN

- 802.11a/b/g
- 802.11n
- 802.11ac
- 802.11ad
- Other 802.11
- DECT ULE
- Other 2.4GHz
- Other Sub-GHz

WWAN

- 2G Cellular
- 3G Cellular
- 4G Cellular

Added to original slide:

- *5G Cellular*
- *Satellite*

Spectrum Options For Connectivity

Licensed

- Existing commercial wireless bands allow flexible use
- Recently made available:
  - AWS-3 – Auctioned
  - AWS-4 – Mobile Satellite S-band spectrum made available for terrestrial use
  - 600 MHz - TV Incentive Auction
  - Citizen's Broadband Radio Service at 3.5 GHz (Priority Access Licenses)
  - New licensed bands in millimeter wave spectrum at 24 GHz, 28 GHz, 37 GHz, 39 GHz and 47 GHz
  - 2.5 GHz band transformation
- Proposed: C-band at 3.7 GHz & additional millimeter wave bands

Unlicensed

- Existing unlicensed bands allow flexible use:
  - 915 MHz (902 – 928 MHz)
  - 2.4 GHz (2400 – 2483 MHz)
  - 5 GHz (Total of 555 MHz)
  - 57 – 64 GHz (7 GHz)
  - Overlay in many other bands
- Expansion of unlicensed:
  - New band at 64 – 71 GHz
  - New bands above 95 GHz
  - TV "White Spaces"
  - Citizen's Broadband Radio Service at 3.5 GHz (General Authorized Access)
- Proposed: 5.9 GHz & 6 GHz (shared)

Conclusion: This roundtable discussion was only a starting point, however. More challenges were raised than solutions proposed. The participants agreed that further discussions must take place to assess challenges and develop more detailed solutions on how to address them. There was consensus that a conference or another roundtable that brings together experts in government, industry, and academia is an appropriate next step.

Vulnerabilities

- Workshop objectives:
  - Explore the risks of increasing reliance on wireless systems and access to spectrum, and discuss ways to solve such problems
  - Focus on the radio link rather than conventional cybersecurity issues: the challenges created by radio receivers necessarily being open to incoming signals in order to function
- Examples of Vulnerabilities From Prep Materials:
  - “Spoofing Presidential Alerts”
  - “Protecting GPS From Spoofers is Critical to the Future of Navigation”
  - “New Security Flaw Impacts 5G, 4G, and 3G Telephony Protocols”
  - “Most Dangerous Hacked Medical Devices”
  - “Can “Internet-of-Body” Thwart Cyber Attacks on Implanted Medical Devices?”

Detecting and Understanding Spectrum Vulnerabilities

- **Interference:**
  - Controlling interference is not new - - more on airwaves
  - Defining what constitutes harm
  - Spectrum Management: FCC & NTIA
  - Industry plays a role as well
- **Data collection & sharing:**
  - What to collect
  - Who collects it
  - Reliability of the data
  - Interpreting/analyzing the data

Identifying and Mitigating Causes of Spectrum Vulnerabilities

- **System Design and Complexity**
  - Build protections into the design
  - Anticipate failures - retransmissions
  - Dynamic capabilities can help
- **Standards Setting**
  - Standards now typically consider cyber
  - How to ensure they are thorough & implemented
- **Availability of Harmful Equipment**
  - Would not knowingly certify harmful equipment
  - Take enforcement action
  - What makes it easier: Advertised on the Internet
  - What makes it harder: More avenues for distribution & volume

Jammers Are Prohibited

https://www.fcc.gov/general/jammer-enforcement

Jammer Enforcement

ALERT

Federal law prohibits the operation, marketing, or sale of any type of jamming equipment, including devices that interfere with cellular and Personal Communication Services (PCS), police radar, Global Positioning Systems (GPS), and wireless networking services (Wi-Fi).

"Jamming devices create serious safety risks. In the coming weeks and months, we'll be intensifying our efforts through partnerships with law enforcement agencies to crack down on those who continue to violate the law. Through education, outreach, and aggressive enforcement, we're tackling this problem head on."
-- P. Michele Ellison, Chief, Enforcement Bureau

Jamming Prohibition

The use of "cell jammers" or similar devices designed to intentionally block, jam, or interfere with authorized radio communicati (signal blockers, GPS jammers, or text stoppers, etc.) is a violation of federal law. Also, it is unlawful to advertise, sell, distribut or otherwise market these devices to consumers in the United States. These devices pose serious risks to critical public safety communications, and can prevent you and others from making 9-1-1 and other emergency calls. Jammers can also interfere with law enforcement communications. ***Operation of a jammer in the United States may subject you to substantial monetary penalties, seizure of the unlawful equipment, and criminal sanctions including imprisonment.***

Lessons Learned from Some Past Experiences

Security of Garage Door Openers:
Early Generations had Weak Security

Cordless Phones with Few
Caused False 9-1-1 Calls

Wi-Fi Originally had
Little Security

First Generation Cell Phones
Intercepted via Scanners

Closing Thoughts

- **All stakeholders have a role to play:**
  - Government
  - Network operators
  - Standards organizations
  - Equipment designers
  - Application developers

- **Strive to eliminate vulnerabilities but recognize that some vulnerabilities are probably inevitable**

- **Prioritizing attention to vulnerabilities is appropriate, particularly for safety**

Thank You!