

What's News...

Carriers Say Fixed Wireless Access Can't Match Cable Broadband

The top executives at America's two leading cable companies Comcast and Charter say they think fixed wireless access will never be as good as the cable industry's advanced DOCSIS 4.0 networks. Regardless, Verizon and T-Mobile's collective FWA services accounted for more than 90% of growth in the fourth quarter of 2022. Charter pointed to a test conducted by OpenSignal last year showing that 5G FWA falls short of cable broadband in speed and latency. Not noted, however, was that for most people, gigabit-per-second data rates aren't necessary, and the lower speeds (and cost) of FWA are making it an appealing offering.



Report: Feds Not Following Rules on Call Interception

According to a government audit, the Secret Service and Immigration and Customs Enforcement agencies aren't following the law and official policy regarding the use of cell-site simulators. These devices, typically called IMSI Catchers, make user devices believe they are connecting to their network but are actually decoys set up by law enforcement to intercept metadata or communications and determine a phone's location. The agencies are supposed to get a court order or use a "pen register"

A Word from Sam Benzacar

Healthcare Industry IoT Security Under Threat

By Sam Benzacar



Although IoT allows healthcare professionals to access and exchange patient data and monitor patient health remotely, it also poses significant security threats that can compromise patient privacy, data confidentiality, and system integrity. Healthcare industry is the second-most attacked industry, with the number of ransomware attacks doubling between 2016 and 2021. The result was the theft of massive disruption of healthcare facilities and the theft of millions of patient records.

Wireless networks are inherently less secure than wired networks (although they can also be hacked), and data transmitted over wireless networks can be intercepted by attackers who gain access to the network. Another concern is the proliferation of unsecured devices that lack adequate security measures, making them easy targets for cyberattacks. When these devices are connected to the healthcare network, they can provide a potential entry point for attackers to gain access to sensitive patient data and other healthcare information.

The issue hasn't escaped attention from agencies such as the FDA, federal law enforcement, and Congress, and the first steps toward addressing healthcare security have been taken. Since 2014, the FDA has been issuing recommendations concerning cybersecurity for the healthcare industry, each one updating its predecessor to address the rapidly evolving threat landscape.

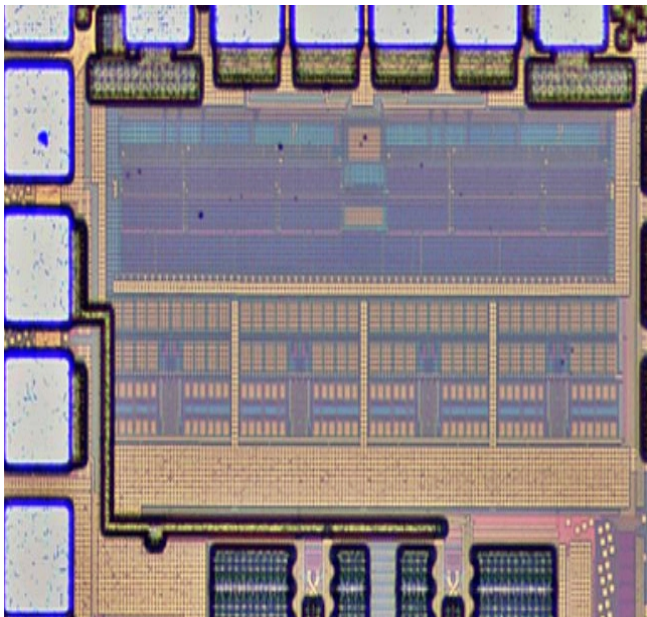
This work resulted in a 49-page document called "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions and Food and Drug Administration Staff." It is very comprehensive and focuses on the deployment of mitigations using a total product lifecycle (TPLC) approach and recommends dozens of actions the industry should adopt.

to record incoming and outgoing calls but in many cases have not been doing so.



MIT Team Finds New Way to Block Interference

Researchers at MIT have developed a device that can actively block high levels of interference with cellular and other wireless signals without traditional filtering and is small enough to be integrated into mobile devices. It's based on a "mixer-first" architecture in which unwanted frequencies are removed before the signal is decoded. It also uses a digital signal processing technique called block-digital filtering that employs capacitors connected in parallel or in sequence to block harmonics.



The Consolidated Appropriations Act for 2023 (the \$1.7 trillion omnibus bill) that funds the federal government through September includes a major addition to the amendments to the FD&C Act that directs manufacturers of "cyber devices" to develop plans to "monitor, identify, and address" cybersecurity vulnerabilities of marketed devices "in a reasonable time." Unfortunately, in the race to get the FDA funded for FY 2023, the agency had to drop almost all its medical device cybersecurity requirements because Senate Republican leadership felt there was not enough time for legislators to review them.

What remains in the budget are FDA requirements for medical device manufacturers to ensure their devices meet minimum standards for cybersecurity and submit a plan to the FDA to monitor, identify, and address post-market cybersecurity vulnerabilities and exploits. They must also submit plans to the FDA for every new product application that demonstrates how the device will address vulnerabilities. Patches to post-market software and firmware are also required.

We can always find a solution!

[Standard Band Pass Filters library](#)

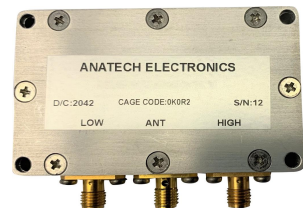
[Standard Low Pass Filters Library](#)

[Standard High Pass Filters Library](#)

[Standard Band Stop/Notch Filters Library](#)

[OR](#)

[send us your specification](#)



Anatech Electronics core business is RF and Microwave filters. Please visit our website to get access to our large database of standard

Researchers Map People Using a Wi-Fi Router

A team at Carnegie Mellon University has created a way to detect three-dimensional shape and movements of human bodies in a room using only Wi-Fi routers by employing a technique called DensePose. This technology maps pixels on the surface of a human body in a photo and was developed by Facebook's AI researchers. After this, a deep neural network maps the signals' phase and amplitude to coordinates on human bodies. Other researchers at MIT in 2013 found a way to use wireless signals to see through walls, and in 2018 another MIT team used Wi-Fi to detect people in another room and translate their movements to walking stick figures. The Carnegie Mellon researchers believe Wi-Fi signals can function as a ubiquitous substitute for standard RGB cameras for sensing people in a room. The benefit of Wi-Fi is that it overcomes obstacles like poor lighting and occlusion that degrade regular camera lenses.



RF & MW filters, as well as the resources to get custom RF and Microwave filters. Just link to our technical dept. or to our easy to follow custom specifications form in our website

WWW.ANATECHELECTRONICS.COM

Anatech Microwave Company

Anatech Microwave Company is a subsidiary of Anatech Electronics manufacturing and offering RF products, such as Directional couplers, Power Dividers, Circulators, Isolators and More.

To learn more about Anatech Microwave Company please link to:

<https://anatechmicrowave.com/>



ANATECH ELECTRONICS INC
RF & Microwave Filters & Products

Happy Holidays from Anatech Electronics



(973) 772-4242



Send us an [email](#)

This email is intended for sam.benzacar@anatechelectronics.com.
[Update your preferences](#) or [Unsubscribe](#)