KEYSIGHT

Design, Emulate and Test

Transforming Medical Device Innovation and Compliance

Youzhi Li, PHD

Director of MedTech Instruments

A Brief History of Keysight

1939 – 1998
Hewlett-Packard years

The company was founded on electronic measurement innovation.

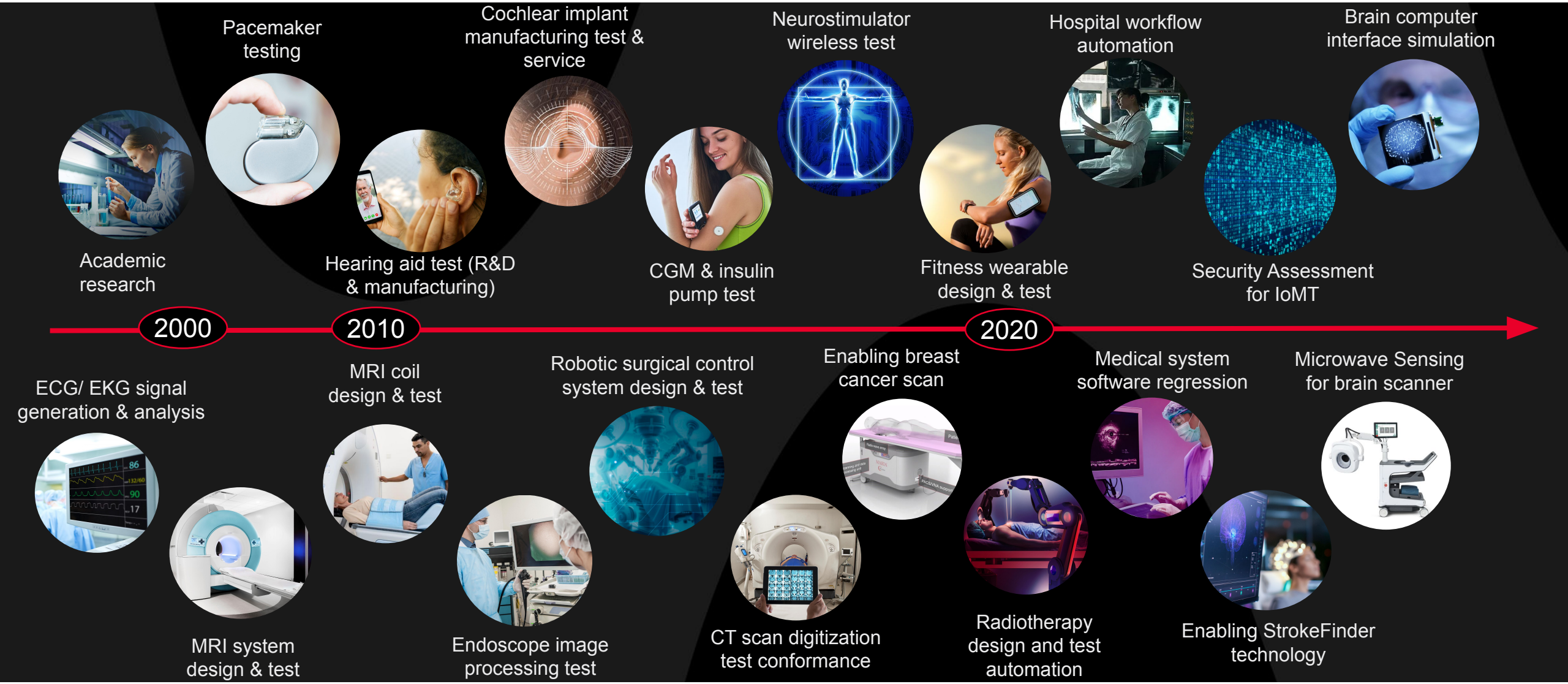
1999 – 2013
Agilent Technologies years

Spun off from HP, Agilent became the world's premier measurement company.
In September 2013, it announced the spin-off of its electronic measurement business.

2014+
Keysight years

Keysight became an independent public company focused on electronic measurement solutions.

Keysight Enables MedTech Industry Innovations



Keysight is an end-to-end enabler for Partners in Healthcare

Keysight partners and coordinates with all players across the ecosystem to enable digital health solutions

MedTech Research & Development

KEYSIGHT

E2E Design & Test Solution

- Wireless compliance & coexistence
- Cybersecurity Compliance
- Software test automation and lifecycle management

Clinical Validation

- Digital twin clinical trials

MedTech Manufacturing

KEYSIGHT

- ICT, functional test, and test automation

PATHWAVE Manufacturing Analytics

Health Information Technology

KEYSIGHT

- Software test automation and lifecycle management
- Cybersecurity

Health Care Systems

KEYSIGHT

- Software deployment test automation
- Digital twin device calibrations
- Cybersecurity

Risk Management for Medical Device

Risk Assessment To Achieve Compliance & Safety Faster

Improves Medical Device Success with Proven Testing Capabilities

WIRELESS COEXISTENCE

KEYSIGHT

Stories from Trenches - Healthcare

“

I don’t expect a new wireless medical device to work, coming into my hospital.

Wireless IT Manager
Medium Sized Hospital

“

My new device worked great in the lab, but then it hit the hospital and fell flat on its face.

Design Engineer
Medical Device Manufacturer

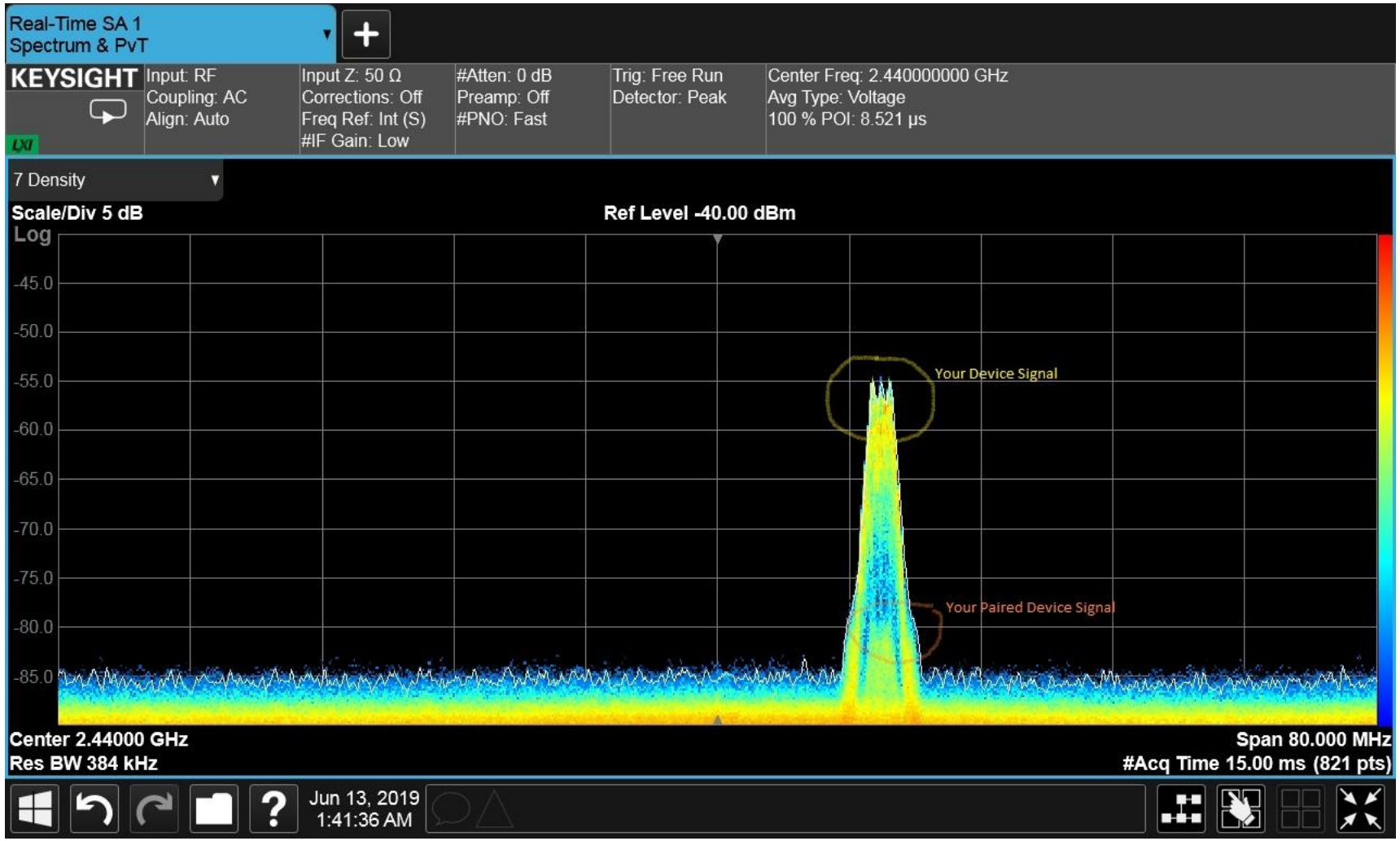
“

I have 950 Wi-Fi devices on my networks and rogue networks coming in the front door every minute. A visitor walks in with a smartphone, a smart watch, a wireless headset, a FitBit, and his phone configured as a Wi-Fi® hotspot.

Wireless IO Professional
Healthcare Facility

But I Tested It!

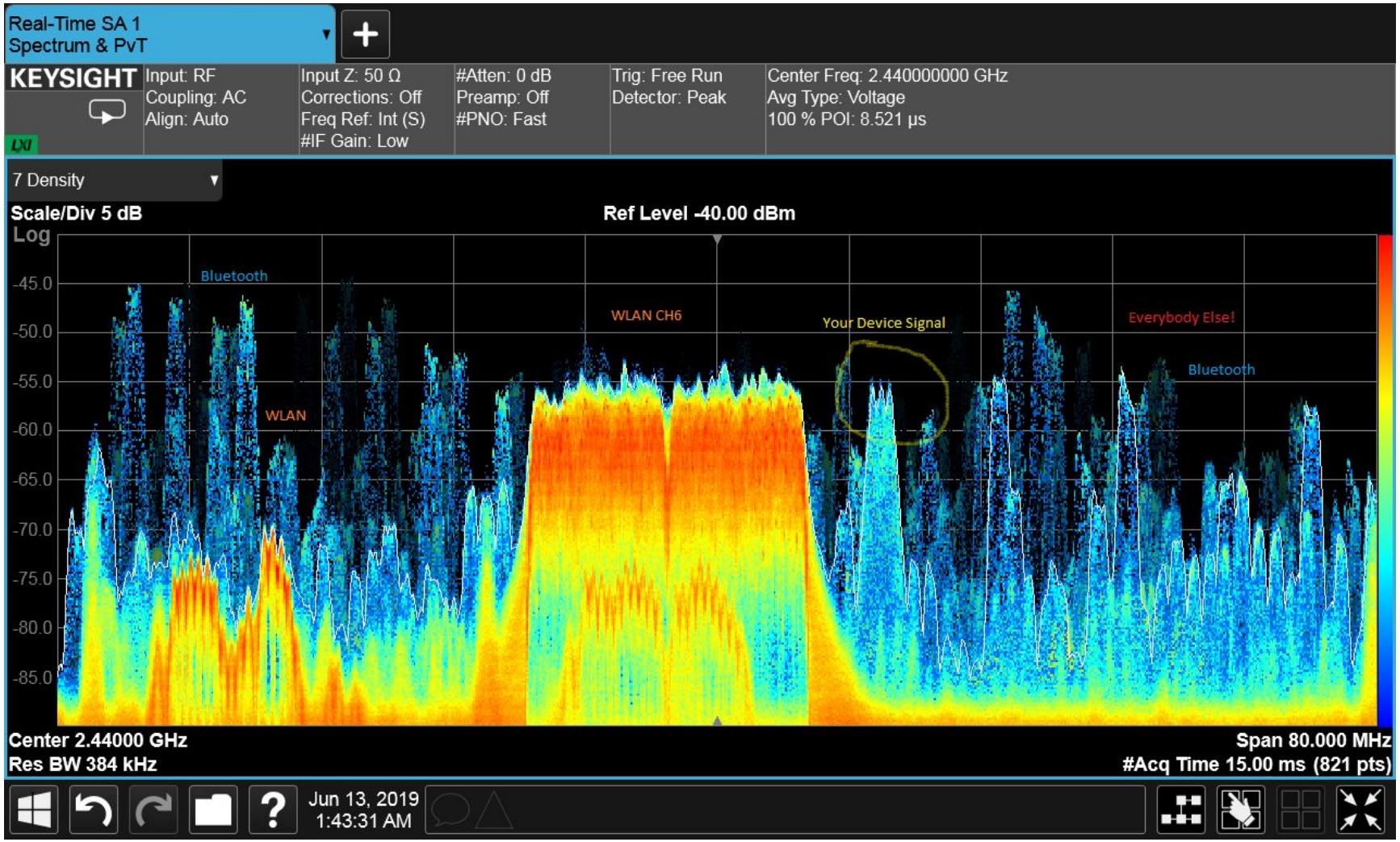
Insufficient Test Conditions



- Quiet Chamber
- No other emitters
- Measure:
  - Unintended signals
  - Susceptibility
  - Protocol Compliance
- Does not measure
  - Performance
  - Interference effects

How You Should Test It

Real World Use Conditions



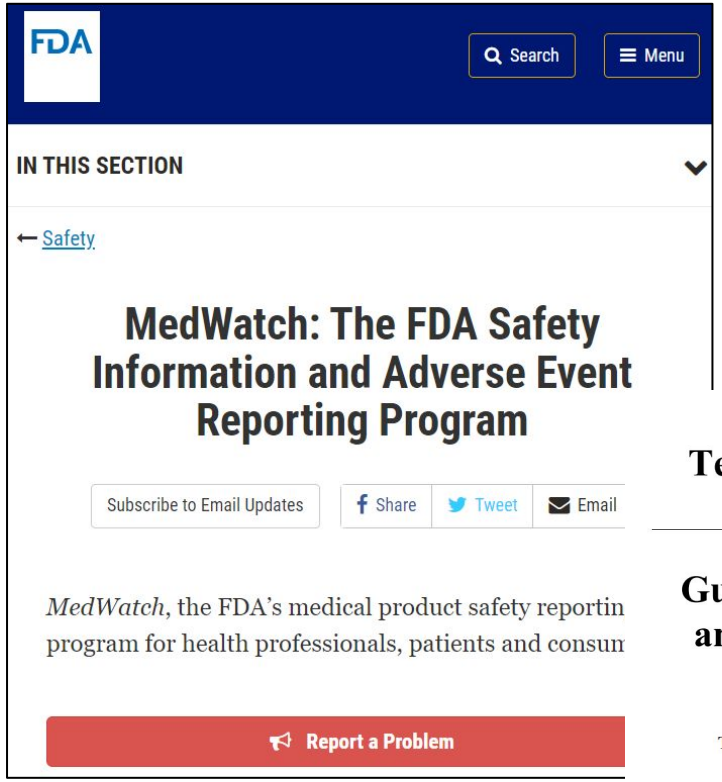
Measure FWP in presence of expected emitters:

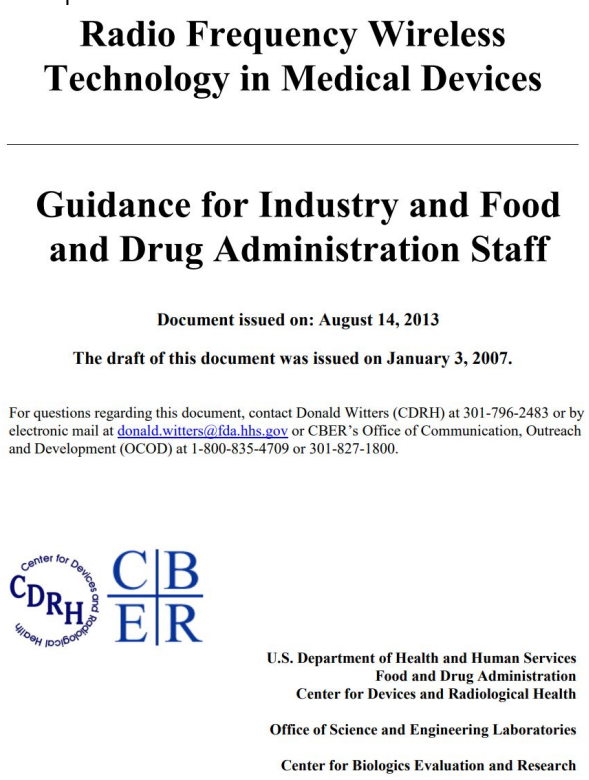
- Active Chamber
- Expected emitters
- Measure:
  - *Performance*
  - *Interference Effects*

Coexistence in Medical Devices

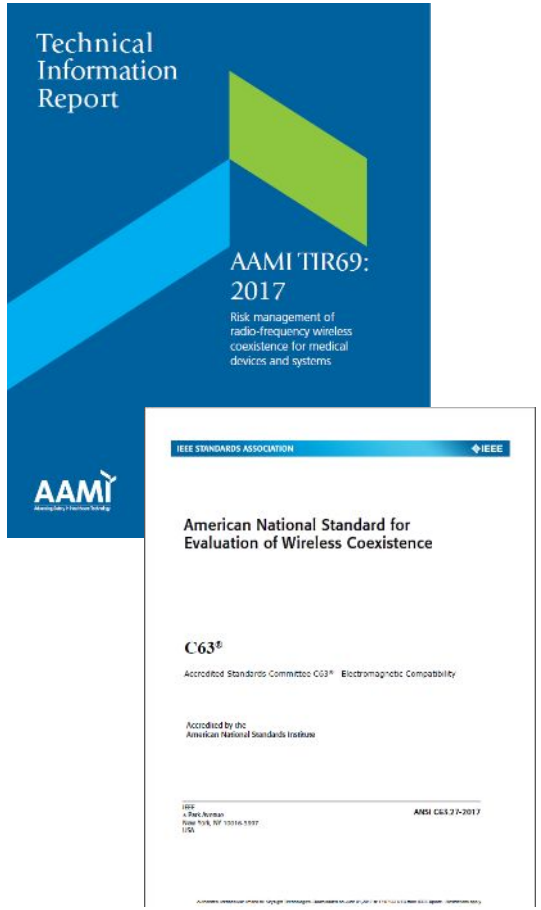
Why is it Particularly Important?

- Patient safety
- Implanted devices
- Devices have long expected service life
- Public reporting of device failures
- Legal costs associated with failed devices
- Additional regulatory consequences (e.g. Form 483)





Industry Alignment: RF coexistence

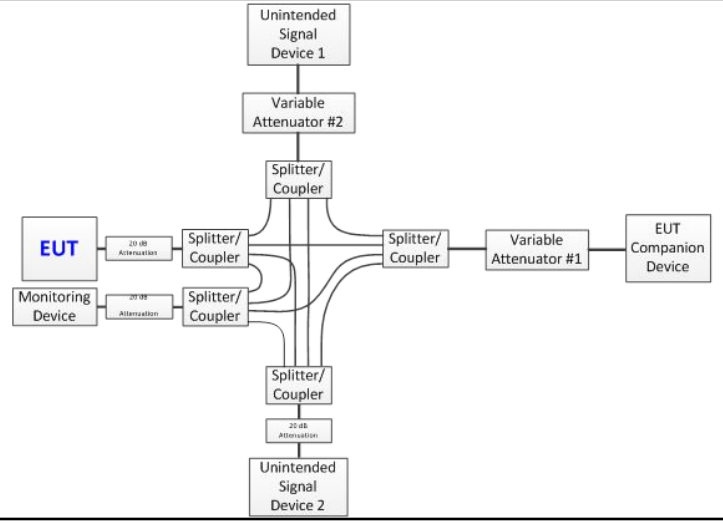


Beyond Regulatory, Why Test?

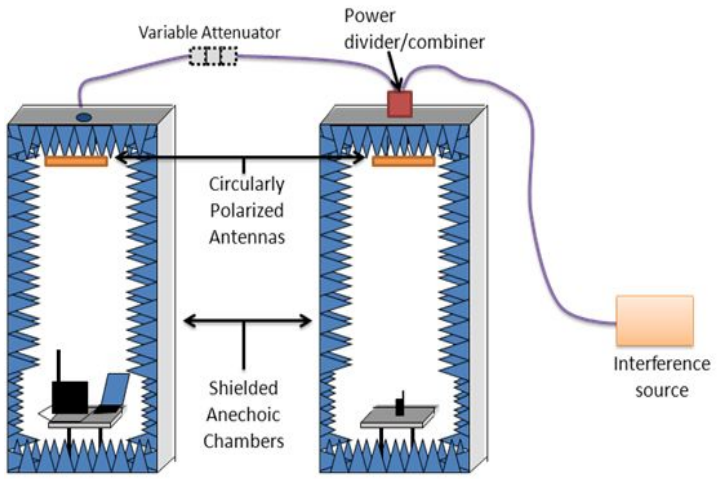
ANSI C63.27: Four Test Setup for Wireless Coexistence

Coaxial, Chamber, Open

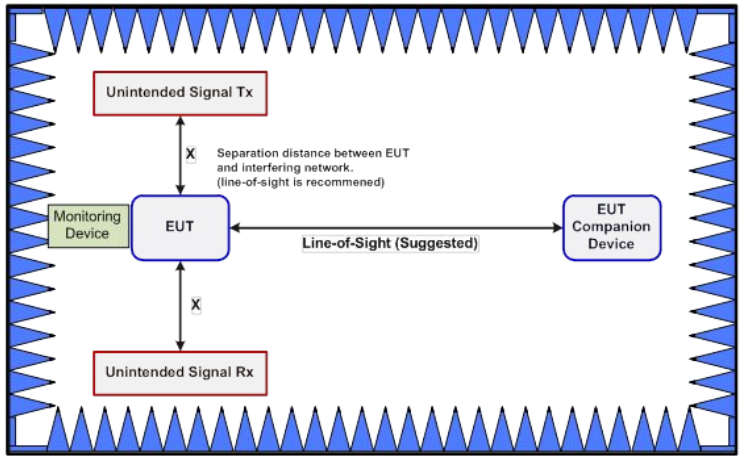
1.



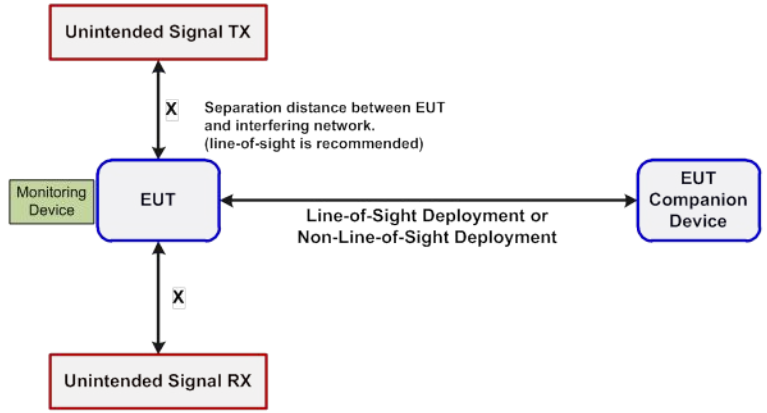
2.



3.



4.



Keysight st Solution

N9917B FieldFox
Signal Analyzer

IOT8720A
IoT Wireless Test
Solution
Companion Device

X8902A-SCU
Signal Conditioning
Unit

5150A
s coexistence test
e

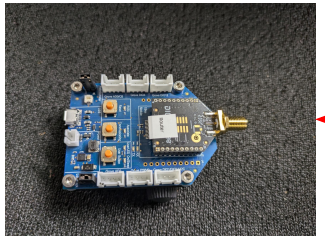
84C
rference Signal Generator

- **Key Features:**
  - Up to 8 independent signals from single port □ easy to create simulated real-world environment.
  - C63.27 compliant signal libraries and test scenarios
  - Test automation
  - Report generation

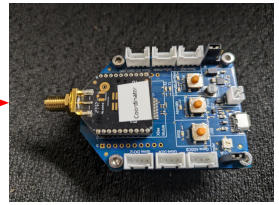
Wireless Medical Device: ZigBee Demo

DUT PC

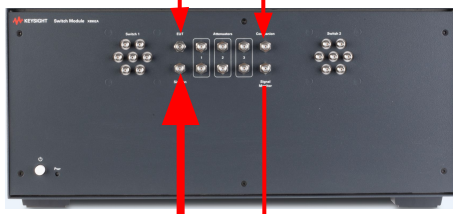
Companion Device
ZigBee Router



ZigBee
Generic Device

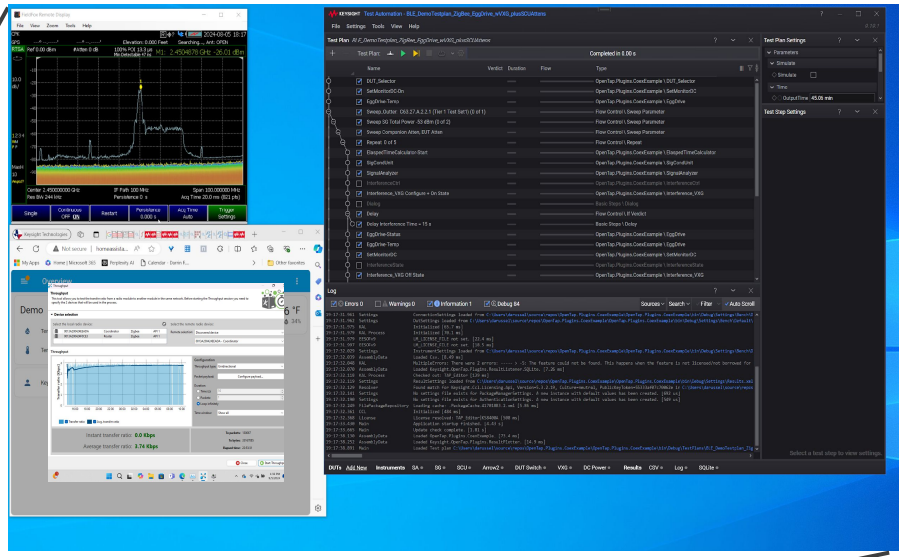


Coordinator



N5182B/N5186A/M9484C

N9917B



Test PC

Test Cases:

- Performance in presence of interference
- Performance vs interference power level
- Recovery Time after interference
- Measure Time to Interference
- DUT interference
- Companion interference
- Performance vs Distance (DUT to Companion)

CYBERSECURITY

Vulnerabilities Discovered in Post-Market Devices

FDA U.S. FOOD & DRUG ADMINISTRATION

← Home / Medical Devices / Medical Device Safety / Safety Communications

- SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication
- Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telem
- URGE Introd
- Certain Medtronic MiniMed Insulin Pumps Have Potential Cybersecurity Risks: FDA Safety Communication
- Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication

- When you discover vulnerabilities, you must scramble to address flaws and rush updates
- You risk brand damage, expensive recalls, compliance risk and potential patient harm

Why Test ?

How to manage the growing risk

IoMT devices are at risk

- 87% increase in IoT malware attacks in 2022[1].
- As of January 2022, **53%** of connected medical devices and other internet of things (IoT) devices in hospitals had known critical vulnerabilities. [2]
- Approximately 1/3 of healthcare IoT devices have an identified critical risk potentially implicating technical operation and functions of medical devices [2].

Organizations lack skills and visibility

- 42% say they lack the ability to detect vulnerabilities on IoT and OT devices[3].
- 64% have low or average confidence that IoT devices are patched and up to date[3].

KEYSIGHT

Security Compliance Is No Longer Optional

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Guidance for Industry and Food and Drug Administration Staff

Document issued on September 27, 2023.

The draft of this document was issued on April 8, 2022.

This document supersedes "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," issued October 2, 2014.

For questions about this document regarding CDRH-regulated devices, contact CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010, or by email at ocod@fda.hhs.gov.

FDA U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

C. Cybersecurity Testing

As with other areas of product development, testing is used to demonstrate the effectiveness of design controls. While software development and cybersecurity are closely related disciplines, cybersecurity controls require testing beyond standard software verification and validation activities to demonstrate the effectiveness of the controls in a proper security context to therefore demonstrate that the device has a reasonable assurance of safety and effectiveness.

Under 21 CFR 820.30(f), a manufacturer must establish and maintain procedures for verifying the device design. Such verification shall confirm that the design output meets the design input requirements. Under 21 CFR 820.30(g), a manufacturer must establish and maintain procedures for validating its device design. Such design validation shall include software validation and risk analysis, where appropriate. FDA recommends verification and validation include sufficient testing performed by the manufacturer on the cybersecurity of the medical device system through which the manufacturer verifies and validates their inputs and outputs, as appropriate.

Security testing documentation and any associated reports or assessments should be submitted in the premarket submission. FDA recommends that the following types of testing, among others, be considered for inclusion in the submission:

- Security requirements;
  - Manufacturers should provide evidence that each design input requirement was implemented successfully.
  - Manufacturers should provide evidence of their boundary analysis and rationale for their boundary assumptions.
- Threat mitigation;
  - Manufacturers should provide details and evidence of testing that demonstrates effective risk control measures according to the threat models provided in the global system, multi-patient harm, updatability and patchability, and security use case views.
  - Manufacturers should ensure the adequacy of each cybersecurity risk control (e.g., security effectiveness in enforcing the specified security policy, performance for maximum traffic conditions, stability, and reliability, as appropriate).
- Vulnerability Testing (such as section 9.4 of ANSI/ISA 62443-4-1); and
  - Manufacturers should provide details and evidence[61] of the following testing and analyses:
    - Abuse or misuse cases, malformed and unexpected inputs;
      - Robustness.
      - Fuzz testing.
      - Attack surface analysis;
      - Vulnerability chaining;
      - Closed box testing of known vulnerability scanning;
      - Software composition analysis of binary executable files; and
      - Static and dynamic code analysis, including testing for credentials that are "hardcoded," default, easily guessed, and easily compromised.
  - Penetration testing;
    - The testing should identify and characterize security-related issues via tests that focus on discovering and exploiting security vulnerabilities in the product. Penetration test reports should be provided and include the following elements:
      - Independence and technical expertise of testers;
      - Scope of testing;
      - Duration of testing;
      - Testing methods employed; and
      - Test results, findings, and observations.

FDA Requirements on Cybersecurity in Medical Devices

Section 524B (a):
Manufacturers submitting for premarket application or 510(k), PMA. PDP, De Novo, or HDE for “cyber device” is required to include information to ensure the device meets cybersecurity requirements.

Documentation Recommended

1) Plans and Procedures (Section 524B (b)(1))

2) Design, Develop, and Maintain Process and Procedures to Prove a Reasonable Assurance of Cybersecurity (Section 524B (b)(2))

3) Software Bill of Materials (SBOM) (Section 524B (b) (3))

Reference: https://www.fda.gov/media/119933/download

How We Help You Test

Keysight automated IoT security testing

Easy

- Automated testing of multiple standards
- Simple user interface and API

Fast

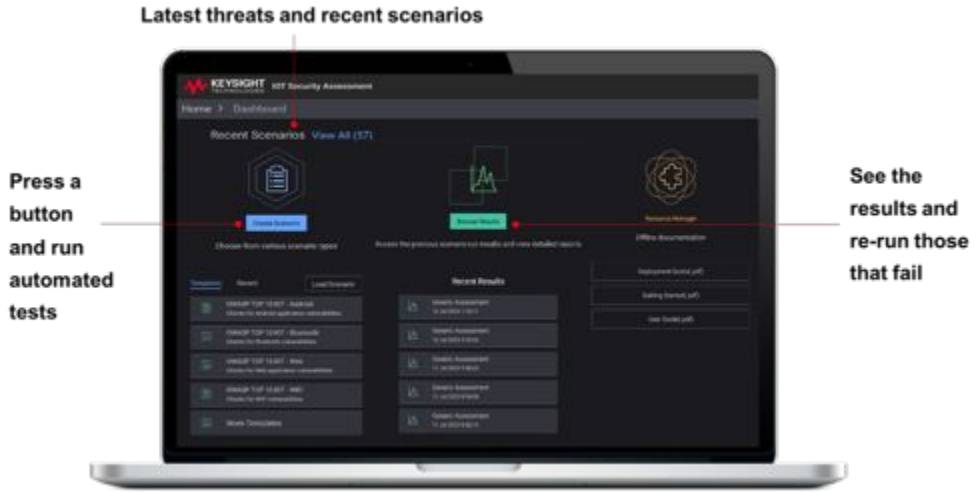
- Quickly finds security flaws

Comprehensive

- Offers updates for the latest threats
- Discovers protocol flaws, weak encryption, guessable passwords, known vulnerabilities
- Scans virtually any device on any network

How Customers Use Keysight IoT Security Assessment

Portfolio of IoT Security Testing



- **Protocol Fuzzing**
  - Industry leading Fuzzing which accelerates discovery of unknown flaws in protocol stacks and chipsets
- **Vulnerability Assessment**
  - Scans devices against a growing list of known threats and vulnerabilities
- **Compliance Testing**
  - Evaluate target against specific requirements such as encryption, open ports, certificate validation
- **Firmware Analysis**
  - Analysis of binary firmware files for generating SBOM, detecting vulnerabilities and weaknesses, and identifying potential 0-days

KEYSIGHT

Keysight Automated IoT Security Testing

Demo of IoT Security Assessment in action.

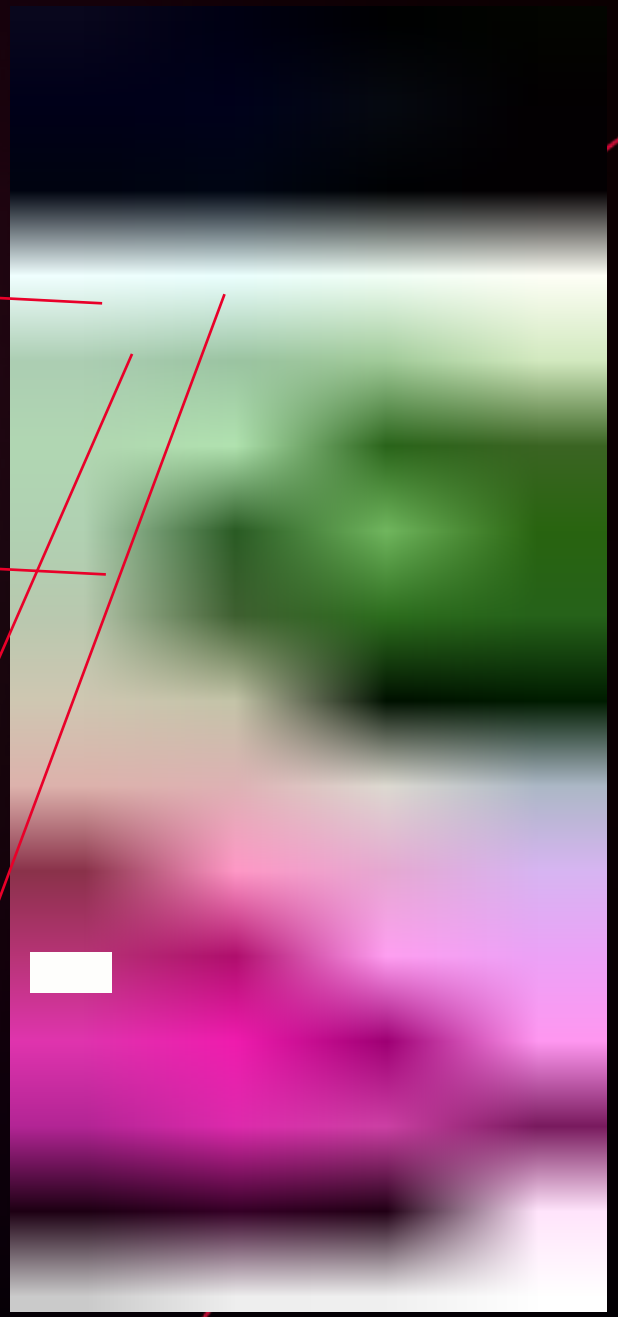
In this scenario we show an attack on an ECG.

User starts ECG test

Fuzzing attack begins

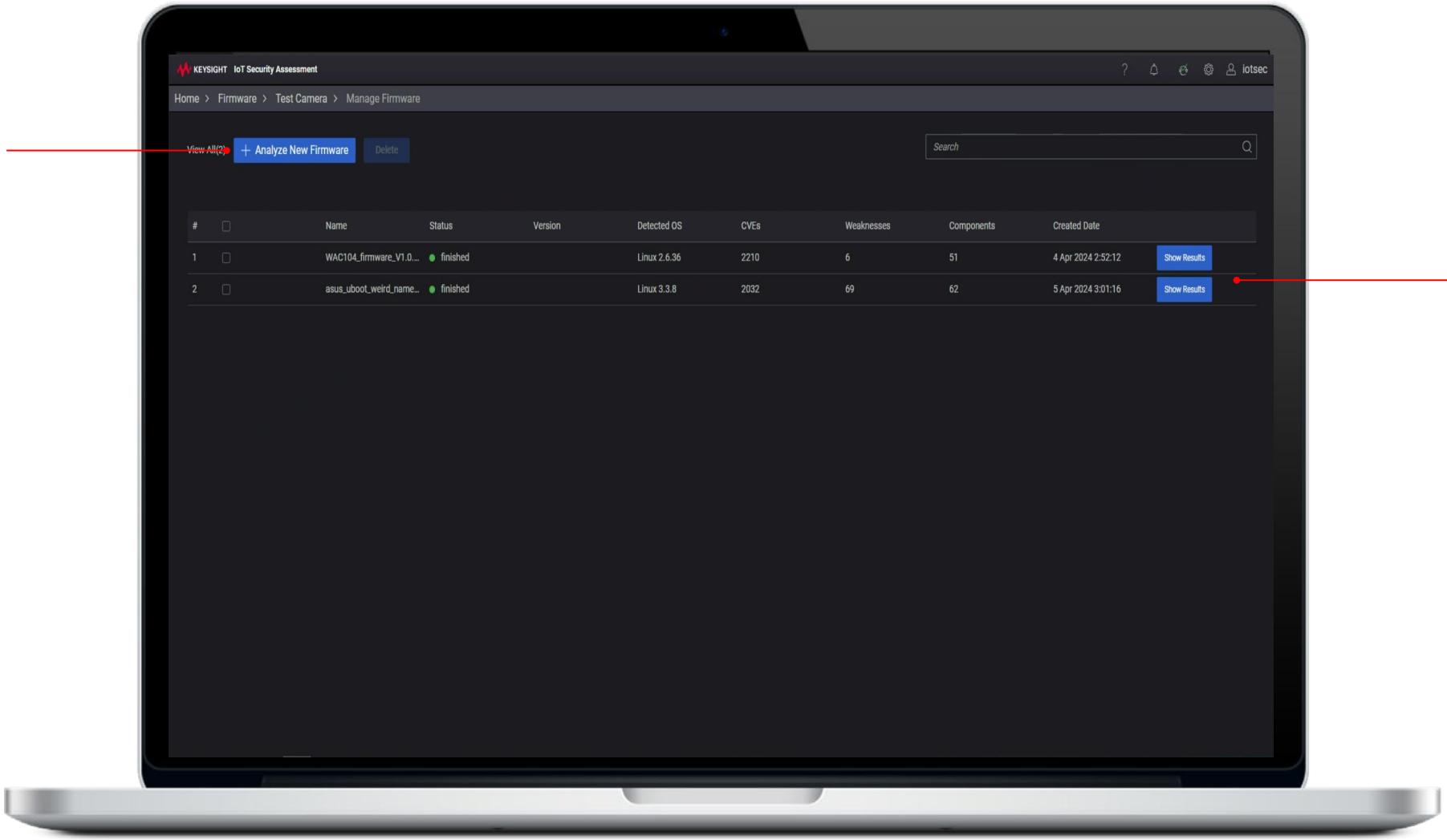
Device reports erratic results

Results interpreted as heart problem



Automated Firmware Analysis UI

Upload a new firmware



See the results

Keysight SBOM Studio

Automated SBOM Management

Validation & Correction of imported SBOMs

Enrichment with Software Supply Chain intelligence

Accelerated Vulnerability Management

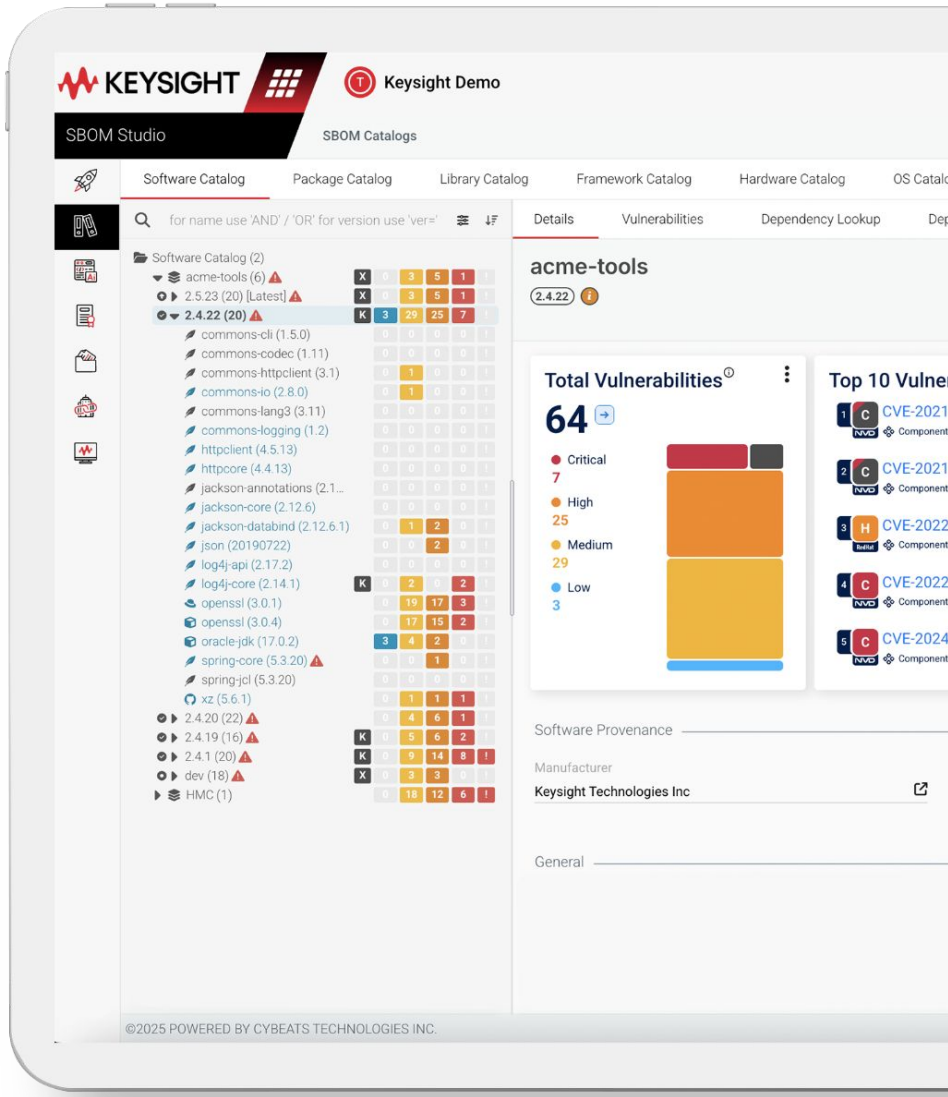
Continuous Monitoring for emerging threats

Rapid Identification of compromised components

SBOM Quality Score

Scoring system to assess SBOM quality and completeness

Enhances trust and readiness for integration



Keysight SBOM Studio

Regulatory Compliance & License Management

Supports GRC compliance and license tracking

Reduces legal and regulatory risk

Secure SBOM Sharing & Exchange

Controlled, format-agnostic distribution

Safe sharing with stakeholders and regulators

Data-Driven Decision Making

Dashboards and reports for forecasting and risk analysis.

Governor View for organization-wide component visibility

Integration & Workflow Enhancement

Seamlessly integrates with CI/CD

User-friendly interface for developers and security teams

+ SBOM Lifecycle
+ AppSec
+ Product Security
+ PSIRT
+ Vulnerability Mgmt
+ Supply Chain Risk

Recommend

Assessment & compliance for **wireless coexistence** & **cybersecurity** are necessary to ensure patient safety & efficacy.

Test & fix early in design phases for faster time to market with safe & reliable products.

Speak to us @ Booth #24

www.keysight.com/find/healthcare