

RADGREEN CONTINUOUS RF MONITORING CASE STUDIES

Here are a few of the many arenas where continuous RF monitoring is not only helpful, but invaluable.

1) Accelerating R&D Timelines by Eliminating "Ghost" Test Failures



RF environment monitoring using the RadGreen RF Monitoring System can identify a localized RF leakage point caused by a degraded coaxial connection or other RF leakage. Real-time alerts are issued for any leakage failure, potentially reclaiming hundreds of lost engineering hours and keeping critical product launch schedules on track.

"Ghost" Test Anomalies Degraded cable shields or RF splitter leakage can raise interference above the ambient noise floor, causing errors during testing or across a batch of tests.

Delayed Project Milestones Intermittent leaks during high-power tests necessitate retesting of a production batch, resulting in delays, missed milestones, and costly schedule slippage.

The Productivity Impact - 5sec Fault Localization Time: RadSys provides automated real-time pinpointing, as opposed to days of manual cable tracking. Continuous, uninterrupted testing with zero ghost anomalies can increase the overall yield by 10-15%. Lab Yield Increase. Continuous RF environment coverage up to 40 GHz covers all critical frequencies, allowing engineers to focus entirely on their product instead of seeking leakage and malfunctions.

Case Study: RF Test Lab. A RadGreen was integrated across the primary test RF lab of one of the biggest cellular operator labs in Europe, for 24/7 continuous monitoring to detect for potential RF leakages. The moment a cable shield degrades, the system alerts in real time — this instant alert enables on-site technicians to detect the fault location and fix it immediately. Fast detection replaced days of manual RF leak troubleshooting with instant, automated fault localization. Fault localization tasks dropped from days to under 5 seconds with the Radys automatic fault detection. Continuous monitoring also eliminates the risk from intermittent leakage events, and provides continuous EHS (Environment, Health, and Safety) to keep personnel safe at all times.

2) Anechoic Chamber Isolation Failure



A shielding breach in a certified anechoic chamber allowed RF signals to exit the chamber and expose personnel to radiation. Additionally, ambient RF signals outside the chamber allowed corruption of sensitivity Rx tests. A RadGreen RadSys Local RF monitoring system was installed to continually check the chamber leakage 24/7. The monitoring device is used in addition to a yearly professional check of the chamber. Installed in front of the chamber, it does not require human resources for continuous chamber leakage detection.

Invalid Tests RF signals near a compromised chamber with a shielding breach can raise the noise floor, and interference can cause corrupt sensitivity Rx testing. High-intensity radiation leaks can raise serious safety concerns in nearby work areas, resulting in severe liability concerns.

A RadGreen RadSys Local RF Monitoring System was placed outside the chamber for 24/7 chamber leakage monitoring. It detected an isolation breach when measuring a leaked signal at -47 dBm instead of -87 dBm. It reflected an isolation error of 40 dB. 24/7 monitoring by the RadSys system saved product batch retesting in this case of leakage. Failures detected in real time eliminate schedule delay, as well as contract penalties. Continuous monitoring helps meet regulation compliance and eliminates liability concerns.

3) Production Schedules and Protecting Delivery Deadlines

A premier high-tech electronics and defense manufacturer integrated the RadGreen RadSys RF Local Monitoring unit next to its 19-inch ATE rack. After a few days, the monitoring system detected RF leakage. The technician paused the test and fixed the problem immediately. As a result, 3 weeks of incorrect tests were saved, helping meet a strict shipment deadline and significantly increasing the project's profit margins. Installing the RadGreen RadSys Local Visual & Voice Monitor device next to an ATE rack provides continuous, real-time RF quality guarantee. The high-speed RadSys sensor detects unexpected high-power RF leakage signals resulting, for example, from a faulty coax cable, a faulty dummy load, or an RF switch. The monitoring system immediately alerts a technician, who can pause the test to prevent inaccurate test results of a batch of devices.



Intermittent Shielding Breach: High-power dummy loads, RF coaxial switches, and instrument interfaces degrade over time due to wear in usage. ATE's with numerous RF connections experience increased likelihood of at least one failure point. As a result, stray leakage can gradually corrupt testing data across production runs.

Costly Quality Loop: Because leakage is sometimes caused by a loose connection, the validation error is only observed during final quality audits — forcing the manufacturer to invalidate weeks of completed tests, leading to delayed shipments and possible contract penalties.

Production Impact By the Numbers: In one situation, three weeks of test data was invalidated, three weeks of completed production runs were also invalidated due to undetected intermittent RF leakage.

Real-Time Leak Detection of unexpected RF signals can be captured instantly by the RadGreen RadSys monitoring device, which can be plug and play deployed in only 5 minutes. The version with no network communication allows the system to pass IT security reviews with minimal hassle, and the system becomes fully operational immediately upon deployment.

100% Shipment Schedule Protection: The RadSys system eliminates rework/retesting caused by RF leakage and helps maintain delivery schedules and profit margins.

Proven Business Value:

Schedule Risks Eliminated. Testing has to be paused at the exact moment a failure occurs - fixing the problem, and continuing to work, eliminates delivery schedule risks.

Maximized ATE Asset Utilization: Using the RadSys system prevents the test environment from corrupting critical product measurements, optimizing production line yield and maintaining asset uptime.

Continuous EHS Compliance: Workspace exposure monitoring keeps personnel safe at all times, and satisfies EHS (Environment, Health, and Safety) requirements.

4) Cybersecurity

Organizations invest heavily in firewalls, EDR and SIEM, and continuously monitor servers and networks. Yet one critical attack route often remains unmonitored: the RF environment. Rogue access points, Evil Twin attacks, unauthorized wireless transmitters and RF anomalies can provide attackers with a path into an enterprise before conventional cyber defenses ever see the attack. Visibility against wireless and RF attacks is often overlooked. MITRE ATT&CK identifies Evil Twin / Rogue access Point attacks (T1557.004) as a recognized adversary technique. CISA warns organizations about wireless Man-in-the-Middle attacks and Rogue Access points. MiM attacks are when adversaries broadcast signals that mimic legitimate corporate networks. By projecting an identical SSID at higher power, attackers lure client devices into connecting — enabling data interception, credential harvesting, and lateral-movement tracking. Nation-state threat groups have used such wireless attack techniques during espionage campaigns.

In 2024, Australian authorities dismantled fake airport WiFi operations, used to steal travelers' credentials. The growth of WiFi 6/6E/7, private 5G, Bluetooth and IoT has rapidly expanded the scope of enterprise RF attacks. According to IBM, the average global cost of a data breach is around \$4.9M and 83% of organizations have experienced more than one breach. One successful RF intrusion can expose intellectual property, confidential product designs, defense programs, sensitive customer data, and manufacturing operations.

RadGreen platforms provide continuous broad wavelength coverage monitoring across the RF spectrum, with no blind spots between inspections. Wideband coverage from 100MHz – 40GHz can be chosen with selected frequency bands. The RadGreen system can detect rogue or unauthorized WiFi and Evil Twin transmissions and abnormal RF power changes. Advanced AI algorithm identify anomalies and suspicious behavior in the RF spectrum, with high accuracy and low false

positives. Real-time, instant alerts can be sent to SOC, email, SMS or local visual/audio alarms for rapid response. Complete RF event logging and reporting is provided for investigations, compliance, and trend analysis. The RadGreen platform can detect the following threats: rogue access points, Evil Twin attacks, unauthorized Bluetooth, IoT and cellular devices, hidden wireless transmitters, RF reconnaissance, wireless data exfiltration, RF interference and signal jamming, GPS/GNSS spoofing, drone communication signals, or many other suspicious RF anomalies. RadGreen sensors can detect, analyze, locate, and protect in the RF arena, and are especially designed for critical infrastructure and mission-critical environments such as Power & Energy, Water & Wastewater, Transportation, Telecoms, Defense Vendors, Aerospace and Secure manufacturing, etc.

Conclusion: RadGreen RadSys RF Monitoring Solution Advantages

- Three solution types – Indoor, Outdoor, and Local & Visual
- Low-SWaP (Size, Weight, and Power) devices designed for dense deployment
- Plug and Play
- Local & Visual Versions: no communication and no memory – suitable for defense
- Non-Chinese controllers and CPUs – suitable for defense customers
- Fast response detection: pulses narrower than 1μSec – radar application
- Competitive price, especially at higher frequencies
- Wide frequency coverage: 100MHz – 40GHz, band-selective
- Maintenance-free operation – no periodic calibration required
- 24/7 continuous monitoring, early detection, with no manual measurements needed
- Centralized multi-site management
- Proven at tier-1 defense and telecom customers
- Built-in data logging and historical reporting

Strengthen your operational resilience, protect your IP, and reduce cyber-risk with RadGreen's RF monitoring solutions! For more information, contact Saelig Co. Inc. at support@saelig.com or visit www.saelig.com/category/radgreen.htm