# Bringing TEMPEST Receivers into the Digital Age

# White Paper

**Products:**

- R&S®FSWT
- R&S®VSE

In the field of TEMPEST, traditional methods of analysis have focused on analog signal emanations from electronic devices. For continued emissions security (EMSEC), there is a need for analysis tools to provide insight into emanations on digital signals. This white paper provides an overview on the digital demodulation basics and delivers an understanding on how to analyze impairments on digitally modulated signals.

White Paper
W. Wangard / D. McCarthy
4.2018 – Version 1.00

ROHDE&SCHWARZ

# Table of Contents

# 1 Introduction

The field of TEMPEST testing focuses on the Emissions Security (EMSEC) of electronic devices. For many years, the TEMPEST community has focused on the unintended modulations of analog signals emanating from their electronic devices. TEMPEST receivers search the entire spectrum with video detectors checking to see if the AM, FM and video output matches their known signal.

Next generation TEMPEST requirements will include digital demodulation in addition to the traditional AM/FM analog demodulation. While digital signals have been around for many years, certain aspects may be new for TEMPEST measurement facilities and test procedures. Next generation receiver and signal analysis solutions need to be future-proofed to include the ability to process digitally modulated signals.

In addition to demodulating digital signals, it is also desirable to determine the Error Vector Magnitude (EVM) in a manner to check for unintended impairments to the digitally modulated signal. By evaluating the signal's Error Vector Magnitude (EVM) over time, one can isolate AM or FM signals that might be included at very low power levels. This signal-on-signal analysis requires a capability to demodulate digital signals and examine the impairments.

This paper includes an introductory overview of digital in-phase and quadrature (I/Q) component modulation theory and EVM measurement theory. We will discuss adding amplitude and phase impairments to better understand your I/Q signals. The R&S®FSWT Test Receiver is a TEMPEST measuring receiver with digital signal evaluation capability. The FSWT offers the best RF performance on the market and was used to help define the next generation TEMPEST requirements (Figure 1). In this white paper, we will show practical results of what may be needed for testing to future TEMPEST requirements.

Figure 1. The R&S®FSWT is helping to define next generation TEMPEST requirements.

# 2 Digital Demodulation Basics

## 2.1 I/Q Modulation

I/Q modulation techniques are very common in digital signals. I/Q modulation is an efficient way to transfer information and is used in most digital formats. An I/Q modulator can create analog modulation techniques such as amplitude (AM), frequency (FM) and phase (PM) modulation.

First, let's remember that a modulated signal has the following form:

$$E(t) = A \cos(2\pi f_c t + \varphi)$$

where both A and φ may be a function of time, t.

We can separate this general form into two components:

$$E(t) = A \cos(2\pi f_c t) \cos(\varphi) - A \sin(2\pi f_c t) \sin(\varphi)$$

We then define $I = A \cos(\varphi)$ and $Q = A \sin(\varphi)$. Then the two-component equation becomes:

$$E(t) = I \cos(2\pi f_c t) - Q \sin(2\pi f_c t)$$

The I signal is considered as the in-phase signal and the Q signal is considered as the quadrature signal.

Now let's consider a Quadrature Phase Shift Keying (QPSK) modulated signal with no impairments. Note that QPSK may also be called 4-QAM (Quadrature Amplitude Modulator).

For QPSK, the A is a constant and φ can take on one of four values, 45°, 135°, 225°, and 315°. We will let A = 1, so the values of I and Q become the following:

| φ | I = A cos(φ) | Q = A sin(φ) |
|---|---|---|
| 45° | 0.707 | 0.707 |
| 135° | -0.707 | 0.707 |
| 225° | -0.707 | -0.707 |
| 315° | 0.707 | -0.707 |

The I and Q values for each of the four QPSK symbols can be plotted in a constellation diagram (Figure 2). Note that the values have not been impaired by noise or interfering signals yet.

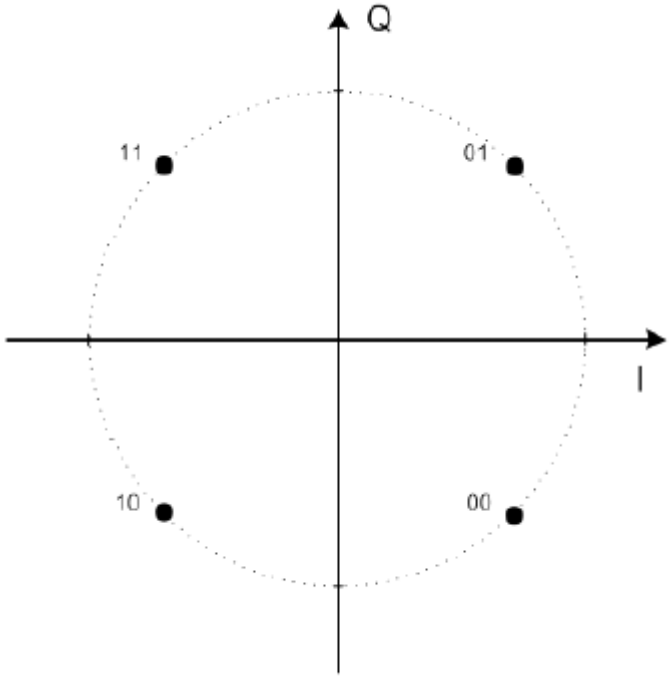



Figure 2. I and Q values for each of the four QPSK symbols in a constellation diagram

Each of the constellation points encode a specific data symbol, which is of one or more bits of data. These constellation diagrams show the location for all the symbols. The number of constellation points is $2^n$ where n is the number of bits per symbol. Knowing the modulation format and symbol rate enables one to demodulate the incoming data by measuring the exact magnitude and phase of the received signal for each clock transition. The layout of the constellation and its symbol locations is defined by the modulation format chosen (QPSK, 16-QAM, 256-QAM, etc.)

In our QPSK example, it transmits two bits per symbol. With 2 bits, four symbols are generated. Each 2-bit code modulates a sine or cosine carrier in a balanced modulator or mixer to produce an in-phase (I) or quadrature (Q) signal. Other modulation techniques will produce even higher levels of modulation. For example, in 16-QAM each 4-bit code group generates one of 16 different symbols (Figure 3). A specific carrier amplitude and phase represents each 4-bit word. These techniques are used to extend to even higher levels, such as 64-QAM and 256-QAM, to increase the data rate in a given channel bandwidth with higher spectral efficiency.

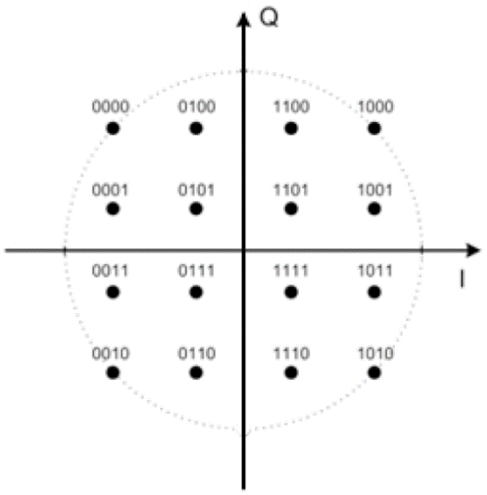



Figure 3. 16-QAM constellation diagram showing each 4-bit code.

An I/Q constellation diagram shows the ideal symbol locations (each marked with a large cross) along with I/Q values measured repetitively at the decision points. The I/Q constellation diagram is a good first place to start in observing signal impairments related to the I and Q signals. Random smearing (or spreading) of the points at the symbol locations indicates noise. But the presence of a pattern such as a line may indicate a spur or interfering tone.

With knowledge of the format of the transmitted data stream, symbol clock timing, and other parameters, a reference signal can be calculated. The reference signal is subtracted from the measured signal leaving a residual error signal (Figure 4). The error can be expressed in a variety of ways including Error Vector Magnitude (EVM), phase error, I-error, and Q-error.

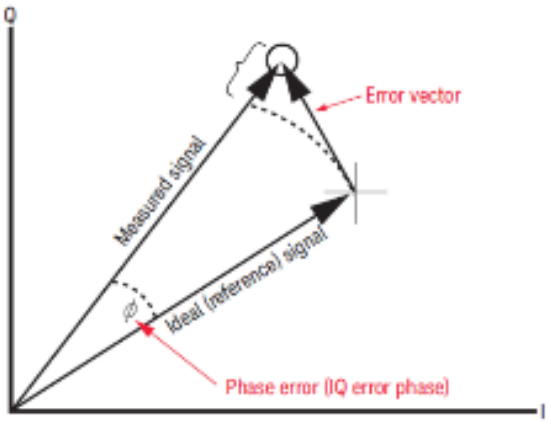



Figure 4. The reference signal is subtracted from the measured signal leaving a residual error signal.

## 2.2 Error Vector Magnitude (EVM)

An issue with complex digitally modulated signals is that circuit imbalance, unintended phase shifts, amplitude differences, and noise may introduce errors that distort the signal. Errors in amplitude and/or phase may cause the signal to be interpreted incorrectly, which leads to bit errors. The greater the number of phase shifts or phase-amplitude symbols used, the more likely there will be errors due to signal impairments.

Error vector magnitude, or EVM, is a measure of modulation quality and error performance in digitally modulated signals. EVM is the root-mean-square (RMS) value of the I and Q errors at the symbol decision times. It provides a quantitative figure-of-merit, as well as offering a methodology for uncovering underlying causes of signal impairments and distortion.

While the error vector has a phase value associated with it, the angle generally turns out to be random. This may be due to the potential randomness of the error itself or because the position of the data symbol on the constellation is random. It is more useful to look at the I/Q phase error between the measured and reference phasors (Figure 5).

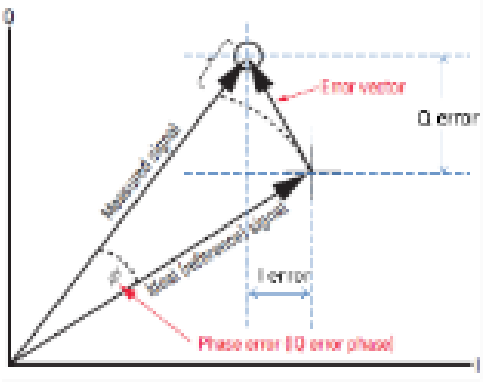



Figure 5. EVM is a measure of modulation quality based on the I and Q errors at the symbol decision times.

EVM is typically represented as a percentage or decibel ratio (dB) of the ideal reference vector magnitude. As a ratio, it is express in negative values and it is important to point out that the lower decibel values represent the best error-free modulation results. For example, an EVM of –40 dB is better than one of –20 dB. In terms of percentage, –40 dB converts to 1% error while -20 dB translates to 10% error.

For the TEMPEST Community, EVM also contains information useful in troubleshooting signal problems. By looking at an EVM over time measurement, you can better isolate the error signal and perform an analysis on it. We'll discuss further how to treat EVM as a signal and demodulate it to determine unintended emanations.

# 3 Understanding Impairments

Residual measurements are very powerful for troubleshooting. Once the reference signal is subtracted, it is easier to see small impairments or signal-in-signal conditions that may have been hidden or obscured by the modulation itself. EVM and phase error measurements are used to determine exactly the type of degradation present in a signal and even help identify their sources. Signal impairments can often be traced back to a component, device, or subsystem of the digital RF communications system.

The error signal can be examined in many ways including the time domain or in the frequency domain by performing an FFT of the time domain error signal. The frequency domain may show details not visible in the time domain. Discrete signal peaks indicate the presence of externally coupled interference. Figure 6 shows examples of EVM vs. time and I/Q phase error vs. time.

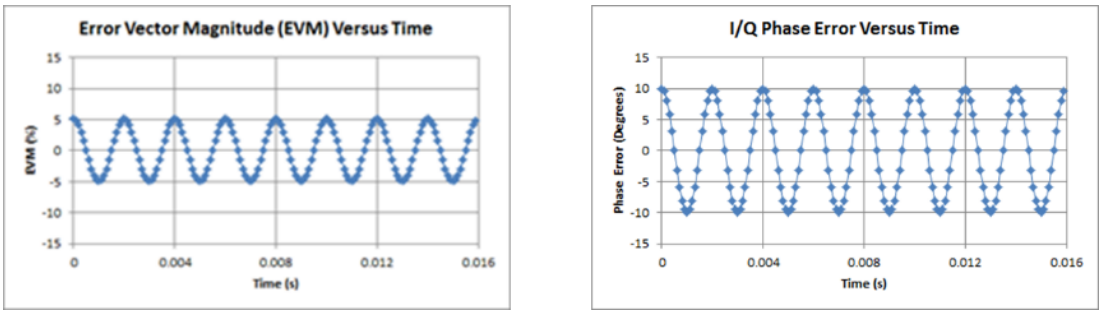



Figure 6. An example EVM and I/Q phase error versus time showing a CW tone coupling.

When the average phase error (in degrees) is larger than the average magnitude error (in percent) by a factor of 5 or more, this indicates that some sort of phase modulation is the dominant impairment error mode. You should look for noise, spurs, or cross-coupling problems in the frequency reference, phase-locked loops, or other frequency-generating stages. When viewed in the time domain, the phase error can reveal sinewaves or other regular waveforms, which indicate an unintended emanation coupled to a desired signal. On the other hand, uniform noise is a sign of some form of phase noise such as random jitter or residual PM/FM.

Residual AM impairment is evidenced by magnitude errors (measured in %) that are significantly larger than the phase angle errors (measured in degrees).

In many cases, the magnitude and phase errors will be roughly equal. This indicates a broad category of other potential impairment problems including compression, clipping, and zero-crossing non-linearities.

Now let's consider different forms of impairments on our example QPSK signal for how best to understand your results.

## 3.1 AM Impairment of the I Signal

Let us define an impairment frequency of $f_i$ with an amplitude of $A_i$ and a phase of impairment of $\varphi_i$. Assume $f_i$ and $\varphi_i$ are constants. If the impairment only imparts amplitude modulation to the I signal, then we can define I and Q as follows:

$I = A \cos(\varphi) [1+m \cos(2\pi f_i t + \varphi_i)]$

$Q = A \sin(\varphi)$

where $m = A_i/A$ which is the modulation index of the impairment signal and

$$E(t) = I \cos(2\pi f_c t) - Q \sin(2\pi f_c t)$$

Figure 7 shows the constellation diagram and the calculated results when the value of m is 0.1 or 10% AM. Note how the measured values for the symbol points are spread parallel to the I axis. We can plot the EVM and phase error versus time as shown. Note the 500 Hz impairment tone.

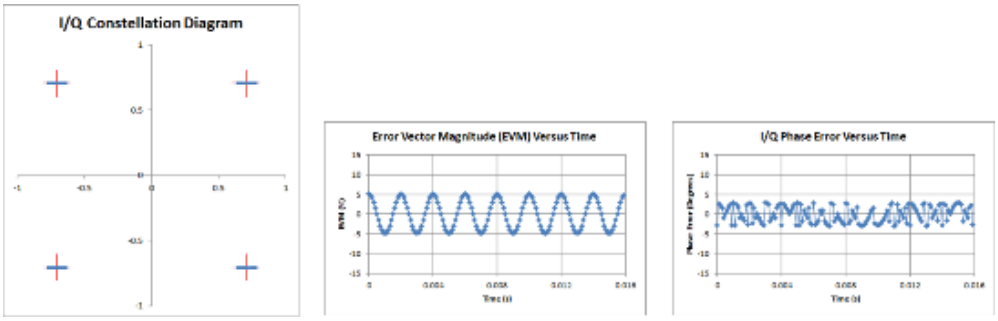



Figure 7. QPSK with AM impairment of the I signal.

## 3.2 AM Impairment of the Q Signal

Let us define an impairment frequency of $f_i$ with an amplitude of $A_i$ and a phase of impairment of $\varphi_i$. Assume $f_i$ and $\varphi_i$ are constants. Now, if the impairment only imparts amplitude modulation to the Q signal, then we can define I and Q as follows:

$I = A \cos(\varphi)$

$Q = A \sin(\varphi) [1+m \cos(2\pi f_i t + \varphi_i)]$

where $m = A_i/A$ which is the modulation index of the impairment signal and

$$E(t) = I \cos(2\pi f_c t) - Q \sin(2\pi f_c t)$$

Figure 8 shows the constellation diagram and the calculated results when the value of m is 0.1 or 10% AM. Note how the measured values for the symbol points are spread parallel

to the Q axis. We can plot the EVM and phase error versus time as shown. Note the 500 Hz impairment tone.

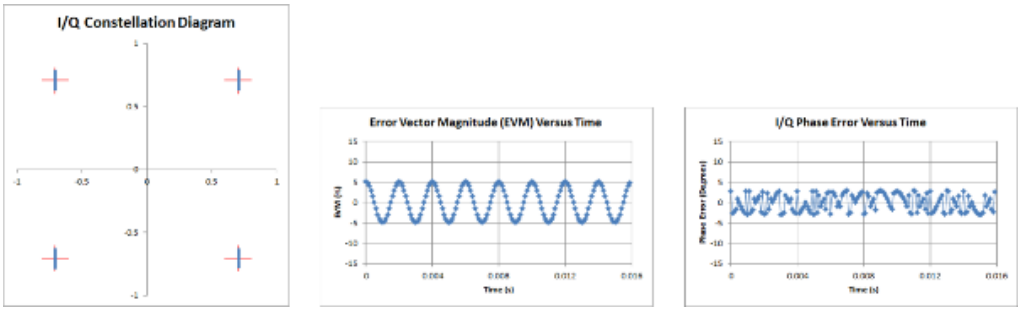



Figure 8. QPSK with AM impairment of the Q signal.

## 3.3 AM Impairment of the I & Q Signals

Let us define an impairment frequency of $f_i$ with an amplitude of $A_i$ and a phase of impairment of $\varphi_i$. Assume $f_i$ and $\varphi_i$ are constants. Now let's have the impairment impart amplitude modulation to both the I & Q signals, then we can define I and Q as follows:

$I = A \cos(\varphi) [1+m \cos(2\pi f_i t + \varphi_i)]$

$Q = A \sin(\varphi) [1+m \cos(2\pi f_i t + \varphi_i)]$

where $m = A_i/A$ which is the modulation index of the impairment signal and

$$E(t) = I \cos(2\pi f_c t) - Q \sin(2\pi f_c t)$$

Figure 9 shows the constellation diagram and the calculated results when the value of m is 0.1 or 10% AM. Note how the measured values for the symbol points are spread at 45° angles to the axes. We can plot the EVM and phase error versus time as shown. The residual error is entirely related to magnitude. Note the 500 Hz impairment tone.

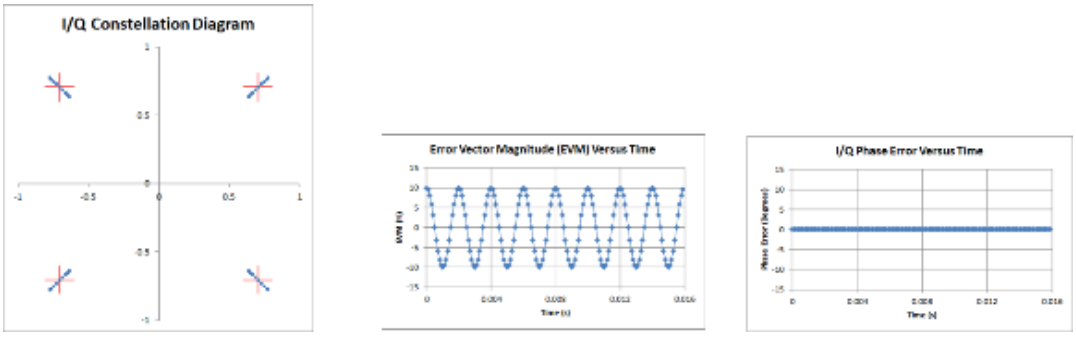



Figure 9. QPSK with AM impairment of both the I and Q signals.

## 3.4 Phase Impairment of I & Q Signals

Let us define an impairment frequency of $f_i$ with an amplitude of $A_i$ and a phase of impairment of $\varphi_i$. Further, assume the impairment is to the phase of the Local Oscillator (LO) in the transmitter that is used to mix the carrier signal with the I signal and the 90° phase shift of the carrier signal with the Q signal. The general equation becomes:

$$E(t) = A \cos[2\pi f_c t + \varphi + m \cos(2\pi f_i t + \varphi_i)]$$

The I and Q components are:

$$I = A \cos[\varphi + m \cos(2\pi f_i t + \varphi_i)]$$

$$Q = A \sin[\varphi + m \cos(2\pi f_i t + \varphi_i)]$$

where m = is the phase modulation index of the impairment signal and

$$E(t) = I \cos(2\pi f_c t) - Q \sin(2\pi f_c t)$$

The constellation diagram is shown in Figure 10. Note how the measured values for the symbol points form a curve. The modulation index is 0.1745 (10 degrees). We can plot the EVM and phase error versus time as shown. The residual error is entirely related to phase. Note the 500 Hz impairment tone.

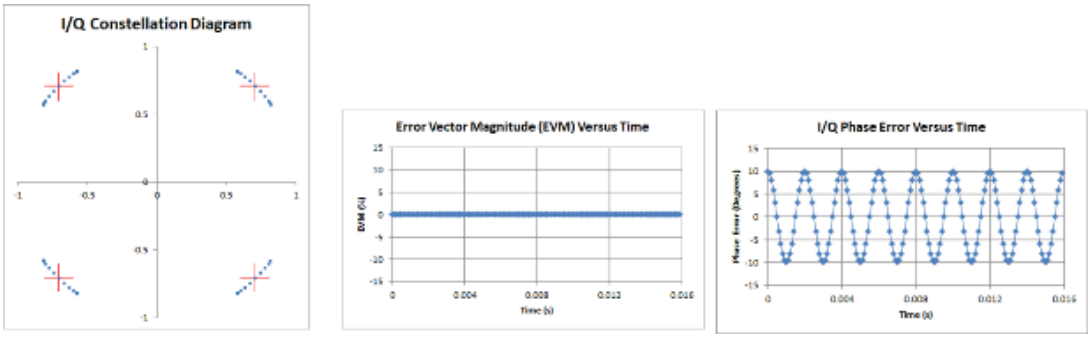



Figure 10. QPSK with phase impairment of the I and Q signals.

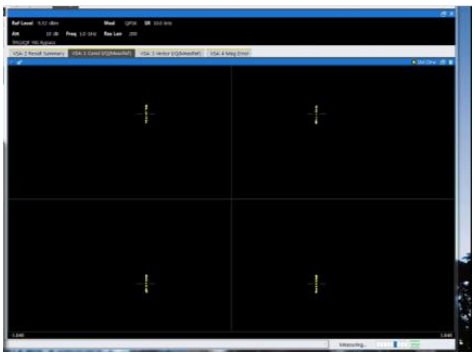
# 4 Rohde & Schwarz Solutions

## 4.1 R&S®FSWT Test Receiver – TEMPEST measuring receiver with digital signal evaluation

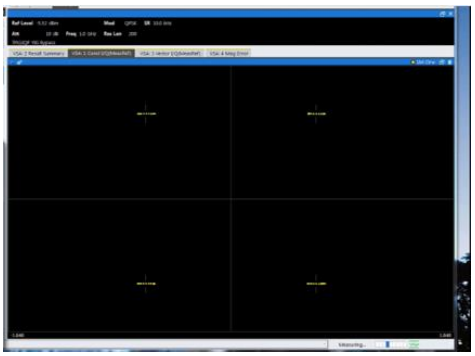
With a digitally implemented measurement bandwidth of up to 500 MHz and very high sensitivity, the R&S®FSWT fulfills the requirements for a TEMPEST measuring receiver. With two equivalent, switchable RF inputs, up to 500 MHz measurement and analysis bandwidth and two independently settable analog outputs for video voltage and demodulators, it fits perfectly into typical test setups and easily replaces older instruments. The FSWT can optionally be equipped with preselection and preamplifier in the base unit. Twenty-one switchable filters with very low insertion loss suppress even strong out-of-band signals. With the preamplifier, the noise figure at 100 MHz is only 1.5 dB. The test receiver measures and demodulates even weak signals reliably.

With its wide selection of measurement bandwidth and detectors, the R&S FSWT is compliant for EMI measurements in line with commercial and military standards. All measurement bandwidths from 1 Hz to 500 MHz are digitally implemented with extremely high accuracy. Video voltage, IF, AM, FM and other signals are exactly reconstructed by two digital/analog converters and fed to two analog outputs. Alternatively, the test receiver can save the I/Q data for offline analysis.

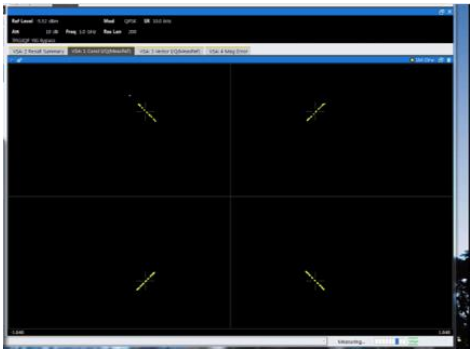
The integrated measurement application demodulates AM, FM and PM. It shows the modulation versus time, the spectrum of the demodulated signal, the RF power versus time and the spectrum of the RF signal. The analog demodulators use the full analysis bandwidth of 500 MHz. Figure 11 shows the measured result equivalents of the impairments shown previously.



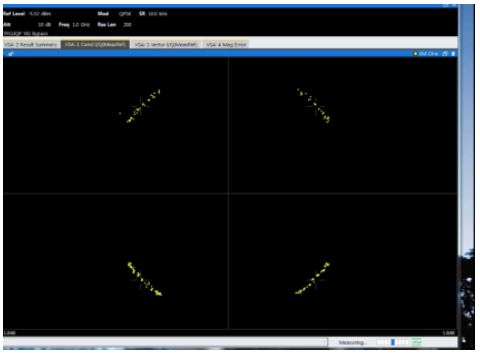
(a) AM impairment on I signal



(b) AM impairment on Q signal



(c) AM impairment on I and Q



(d) Phase impairment on I and Q

Figure 11. Measuring impairments on the R&S®FSWT Test Receiver

## 4.2 R&S®VSE Vector Signal Explorer Software

The R&S®VSE Vector Signal Explorer software brings the experience and power of Rohde & Schwarz signal analysis to your desktop, offering a wide range of analysis tools for troubleshooting on your PC. With this software, you can analyze and solve problems in analog and digitally modulated signals for a wide range of standards using the signal and spectrum analyzers and digital oscilloscopes from Rohde & Schwarz.

With R&S®VSE, you can analyze and investigate a captured signal repeatedly, change parameters, examine the signal in depth and troubleshoot a wide range of signals, from simple BPSK to complex wideband signals such as IEEE 802.11ac and 4096-QAM. Figure 12 shows an example of an EVM measurement over time.

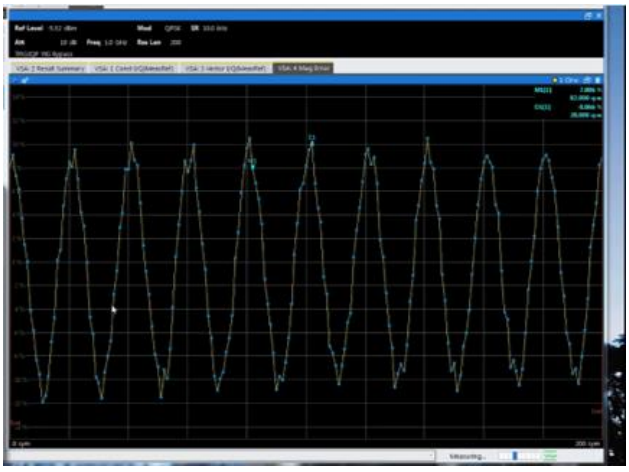


Figure 12. Analyzing EVM over time with the Vector Signal Explorer (VSE) software.

**Rohde & Schwarz**

The Rohde & Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, radiomonitoring and radiolocation. Founded more than 80 years ago, this independent company has an extensive sales and service network and is present in more than 70 countries.

The electronics group is among the world market leaders in its established business fields. The company is headquartered in Munich, Germany. It also has regional headquarters in Singapore and Columbia, Maryland, USA, to manage its operations in these regions.

**Regional contact**

Europe, Africa, Middle East
+49 89 4129 12345
customersupport@rohde-schwarz.com

North America
1 888 TEST RSA (1 888 837 8772)
customer.support@rsa.rohde-schwarz.com

Latin America
+1 410 910 79 88
customersupport.la@rohde-schwarz.com

Asia Pacific
+65 65 13 04 88
customersupport.asia@rohde-schwarz.com

China
+86 800 810 82 28 |+86 400 650 58 96
customersupport.china@rohde-schwarz.com

**Sustainable product design**

- Environmental compatibility and eco-footprint
- Energy efficiency and low emissions
- Longevity and optimized total cost of ownership

Certified Quality Management
ISO 9001

Certified Environmental Management
ISO 14001



**Rohde & Schwarz USA, Inc.**
6821 Benjamin Franklin Drive | Columbia, MD 21046
Phone +1 410 910-7800 | Fax +1 410 910-7849

www.rohde-schwarz.com