

IOT / M2M COOKBOOK

HARALD NAUMANN

How to develop a device based on
Wireless Wide Area Network modules

First edition:
Copyright © 2015 Harald Naumann, Neustadt
Ludwig-Kaufholz-Weg 4, 31535 Neustadt, Germany
E-mail: harald.naumann@gsm-modem.de
Phone: +49-5032-8019985

The book has been finalized and will be further updated as necessary. All purchasers and sponsors will receive free PDF updates regularly. Any comments, requests, tips and suggestions related to the book or download zone are welcome.

New chapters are **marked with an update date** and major changes are **formatted with green text**. This approach is meant to help owners of previous editions to identify the changes and additions more quickly.

Table of contents

1	Why Did I Write the IoT / M2M Cookbook?	5
2	Fundamental considerations before starting the IoT / M2M project	6
3	Certifications and approvals	6
3.1	Examples for Radio approvals in EU and US	6
3.2	Examples for Radio approvals in US and Canada (PTCRB)	7
3.3	Examples for automotive related approvals in Europe	8
3.4	SAR - Specific Absorption Rate	9
4	Cellular data communication (GPRS, USSD, SMS, CSD, DTMF)	10
4.1	Voice communication	10
4.2	Modem / acoustic coupler / encryption	10
4.3	DTMF (Dual Tone Multi Frequency)	11
4.4	GPRS (General Packed Radio Service)	11
4.5	SMS	11
4.6	USSD (Unstructured Supplementary Service Data)	12
4.7	Comparison of power consumption (SMS, USSD and GPRS)	13
4.8	CSD (Circuit Switched Data)	14
5	Supply voltage	14
5.1	Power on timing and waiting	15
5.2	Cellular module in power save mode	15
5.3	Internal resistance of batteries and linear voltage transformers	15
5.4	Switched mode voltage regulator	17
5.5	Simulation of a switched power supplies with LT Spice	17
5.6	Capacitors at power supply and cellular module	19
5.7	Supply voltage for GNSS antenna	19
6	Antennas for IoT / M2M devices	19
6.1	Monopole and dipole antennas	19
6.2	Nothing will interfere with your embedded antenna?	20
6.3	Why the embedded chip or patch antennas are resonant on the frequency?	21
6.4	How will the ground plane affect your embedded antenna?	21
6.5	How to connect your embedded antenna with your wireless module	23
6.6	How to design an antenna matching circuit	24
6.7	Free of charge software to generate a matching circuit automatically	25
6.8	How to switch between an internal and external cellular or GNSS antenna cheap?	26
6.9	Which GPS antenna shall be used for a tracking device?	27
6.10	Which embedded antenna to select for a Bluetooth / GNSS application?	27
6.11	Dos and don'ts during embedded antenna design	30
6.12	Example: Embedded PCB antenna inside a vending machine	31
6.13	Example: Embedded antennas at Telematic device IN1 of GPSoverIP	32
7	Simulation of an embedded GSM PCB track antenna	32
7.1	Definition of the antenna simulation project	32
7.2	Description of the inverted F antenna	33
7.3	3D model of the simulation	34
7.4	Optimization - determination of antenna shape	35
7.5	Typical requirements of a quad band GSM antenna	35
7.6	Optimization of the quad band antenna GSM antenna shape	38
7.7	Directional characteristics of the antenna for two GSM frequencies	39
7.8	Influence on the antenna characteristics of the housing	41
7.9	Influence of the ground plane on the antenna characteristics	42
7.10	Optimisation of the simulated antenna with matching circuit	43
7.11	Design in of the simulated antenna to special GSM / GPS tracker	44
8	Components around the cellular module	45
8.1	SIM card	45
8.2	SIM card subscription	46
8.3	Low ESR capacitor	46
8.4	ESD protection	47
8.5	Loudspeaker and microphone	47
8.6	Firmware update at final PCB	47

9	Examples for mistakes and errors during M2M development	47
9.1	Power down reset	48
9.2	SMS errors	48
9.3	CSD errors	49
9.4	IP connection errors	49
9.5	Analysing of a maximum of design mistakes in one M2M design	49
9.6	Analysing of mistakes at PCB track antenna for GSM	50
9.7	Analysing of GSM chip antenna on small ground plane	51
9.8	Analysing of a Swiss GSM watch	52
9.9	Analysing of embedded LTE antenna in detail	52
10	Radiation noise, maximum spurious, antenna radiation	53
10.1	Antenna radiation versus radiation noise	53
10.2	Conductive noise	55
10.3	Conductive noise transformed to radiated noise	55
10.4	Radiated noise transformed to conductive noise	55
10.5	Prevention against radiated noise	56
11	How to use a vector network analyser for IoT M2M development	57
11.1	Quick Start Guide Vector Analyser MiniVNA Tiny	59
11.2	Explanation S11, VSWR, return loss, reflection coefficient and antenna bandwidth	61
11.3	Unearth the truth - four cellular antennas tested with MiniVNA	63
11.4	A comparison of three Vector Network Analysers	70
12	Testing your M2M device	75
12.1	TX power peaks by cellular module test mode	75
12.2	Pseudo load of 2 Ampere peak load with self-made function generator	76
12.3	TX power peaks by GSM tester	77
12.4	Testing of the sensitivity	77
12.5	Testing of the radiated TX power	77
12.6	Where to get a cheap cellular tester?	77
12.7	Example of a measurement report by GSM test equipment	78
12.8	Ripple and peak voltage - visible by GSM test equipment	83
12.9	How to test an UMTS module on foreign band	83
12.10	Test with UMTS testers	84
12.11	How to test an LTE module on foreign bands	85
12.12	Expected trouble with LTE modules worldwide	85
12.13	Testing the GNSS module	86
12.14	Measurement of the cellular antenna in 3D	86
12.15	Summary of testing	87
13	AT Commands	87
13.1	AT commands during power on your cellular module evaluation kit	87
13.2	Hello World in GSM - AT commands to send a SMS	88
13.3	AT commands and logic loops for set up a communication channel	89
14	Project descriptions of IoT M2M devices	90
14.1	Project description of a long-term tracking device	90
14.2	Project description of a bendable tracking device of bank notes	91
15	Thank you	93

1 Why Did I Write the IoT / M2M Cookbook?

I have worked in the Wireless M2M for more than a quarter of a century. Twenty-five years ago, we didn't even have a word for "M2M" or IoT. We developed Machine to Machine devices without knowing that decades later these creations would be called "M2M devices". Twenty-five years ago, the GSM network for wireless data communication did not exist. I made my first steps in wireless data communication with Frequency Shift Keying (FSK) on Private Mobile Radios (PMR). On PMRs we achieved communication speeds of 3600 bits per second. A little later we started using public analogue trunked radios. These trunked radio systems provided local terrestrial wireless networks on FSK. Years ago, the final public analogue trunked radio network in Germany was taken out of service. GSM jumped in with its Short Message Service (SMS) and Circuit Switched Data (CSD). CSD provided us 9600 bits per second. We could use SMS and CSD for countrywide data communication easily. Later on GSM roaming offered us worldwide data communication. Today, GSM/GPRS is being gradually phased out and is being replaced by 3G and 4G technology. In the US, the cellular operator AT&T does no longer accept new M2M applications on GSM/GPRS. AT&T will accept applications on 3G and 4G (UMTS, HSPA, LTE) only. Some people try to differentiate between M2M and IoT. Call it IoT or M2M - it does not matter. Applications for IoT or M2M often use the same wireless technology. IoT is the umbrella for a number of subsets of wireless data communications. M2M is one out of these subsets and maybe one of the oldest subsets as well.

This IoT / M2M Cookbook describes how to develop a tracking device based on cellular and GNSS modules. You can create a telemetric device by ignoring the GNSS aspect. Typical devices without GNSS include cellular routers with Ethernet ports or a cellular to Wi-Fi bridge. Nevertheless, the navigation system for trucks described in this book already uses six different wireless technologies (2G, 3G, GNSS, Classic Bluetooth, Bluetooth Low Energy and NFC) with five different antennas within one enclosure.

Cellular networks for GSM, HSPA and LTE are the popular Wireless Wide Area Networks (WWAN). However, in some regions we have WWAN over CDMA and WiMax.

Sometimes it is not easy to come up with the appropriate English word for the terms in this book. The common word for SMS in UK is "text message". In this book, we will consistently use the term "SMS". A prepaid SIM card in UK is called a "Pay as you go SIM card". I will typically use the common words specified by ETSI - I will call it a prepaid SIM card. If I use the term "GSM module", this will cover 3G and 4G modules as well, because the fall-back of UMTS, HSPA and LTE is still 2G (GSM/GPRS). GPS is fundamentally an incorrect term. The Global Positioning System (GPS) is just one out of several Global Navigation Satellite Systems (GNSS) that provide the functionality we refer to as "GPS". We can currently access the Russian GNSS called Glonass. The Chinese GNSS is called Beidou. At some point we will be able to access the European GNSS called Galileo.

The IoT / M2M Cookbook is intended to help developers of wireless application save some time and perhaps provide some inspiring ideas. It is a book for makers and summarizes the collective experience across my different jobs. By leading a team of developers required to design a mobile GSM/GPRS tracking device, I learned to think like a developer of an IoT / M2M device. In over fifteen years of working with manufacturing and distribution, I provided the same hints and recommendations to developers of wireless applications again and again. The origin of this book was a 14 page application note written in July 2010. In May 2012, I made the decision to convey the story that I deliver weekly to customers within a book. The goal of this book is to guide developers from the concept of an IoT / M2M device to the final mass-produced product. This book will not provide introductory detail support such as how an inverted F antenna works. To explain those concepts, I will provide links to relevant supporting information. In any case, this book will provide you with information that is often omitted in the official radio module and antenna manufacturers' documentation. This book shows an inverted F PCB antenna for GSM in detail. It explains how to redesign it with your own PCB and how to encapsulate the whole design in epoxy resin. It also explains how to integrate a chip or PCB antenna with coaxial cable.

Some power supply concepts including LT Spice modules for DC/DC regulators and load generator for the 2 Ampere peak currents are included in the book, too. It should be noted that the power down reset is still the main fault in designs with cellular modules.

I hope you will enjoy reading the book and I hope it will save you some time as well.

11.4 A comparison of three Vector Network Analysers

A VNA (Vector Network Analyser) is a very useful instrument for the IoT M2M hardware developer, because it helps you to measure and to check the most important part of the hardware design - the antenna and its transmission lines. It is one of those tools you do not know you are missing until you've got one. One that will save you a lot of time solving problems you are even not aware of, but that can have a serious impact on the quality of your design, like unnecessary high battery drain, malfunction, impaired range,...

It measures complex (transfer) impedances of 1-port (and depending on instrument also on 2-port networks) And RF is all about "matching impedances" and "getting networks to work together", so you can imagine that a VNA can save you really a lot, lot of time.

But until recently VNAs costed a lot of money, like starting at 20K Euro, not the amount of money your manager would spend if you can not promise in writing it will save him or her money.

The good news is that those instruments are available now well under 5000 Euro, suddenly a lot of RF-engineers start looking at them as a tool they can really afford.

Therefore this chapter on usability for those RF design engineer, specially engineers designing the bulk of today electronics: consumer electronics and industrial electronics in IoT and M2M. This chapter will compare VNAs for lab table use going up to at least 3 GHz and covering the most used frequency bands in use for wireless IoT M2M devices (e.g. NFC 13.42 MHz, GSM at 900/1800 MHz, UMTS at 2150 MHz, Bluetooth at 2450 MHz) in the price range under 5000 Euro.

5000,- because under that limit you often do not need to walk all the way up to the CEO to get approval. (and which will be very difficult to explain to someone not involved with RF)

Still, we included a VNA from R&S not because it is a very low cost unit (around 20.000,- Euro), but just because R&S is well settled when it comes to RF-T&M gear.

Well to be honest in fact it is the low-cost R&S table top solution. Which shows low-cost is relative.

Comparison of three VNA:

- mRS: **miniVNA-Tiny** (approx. 430 Euro, 1 ... 3000 MHz)
- MegiQ: **VNA-0440** (2900 Euro, 400 ... 4000 MHz)
- Rohde & Schwarz: **ZVL6** (20.000 Euro, 9 kHz ... 6000 MHz)

Conclusion:

mRS miniVNA Tiny: cheap, low quality; just useful for the radio amateur who has patience and expertise to interpret results. Phase information not very useful in VHF and UHF range.

Rohde & Schwarz ZVL6: Professional quality, all round VNA, rather difficult to operate, very expensive.

MegiQ VNA0440: Professional quality, for the RF designer, easy to use, low priced.

11.4.1 General overview

MegiQ: For a few thousand Euro the MegiQ solution is a bit out of the budget of most radio amateurs, but seen the performance it is a very nice instrument for the professional. Also the frequency range, 400 MHz - 4 GHz is targeted at professional use in design of the consumer electronics of today. But as a design engineer I am interested in that range of 400 - 4000 MHz and within this frequency band we found the unit to give results comparable to the Rohde & Schwarz unit at a fraction of the costs; really amazing.

Operation is easy and straight forward, and it has a lot of unexpected extras.

miniVNA: Nice thing is that you get coverage up from 1 MHz up to 3 GHz for very little money. But of course, for the price you can not expect a lot. The miniVNA looks and feels like a solution for the radio amateur. Advantage is that it is light and really tiny.

It is sensitive to warming up so you need to switch it on timely. It is useful for measuring scalar parameters, like of Return Loss and SWR. It is incredibly noisy and not useful at all for any measurements where phase is involved, so if it comes to phase measurement it is not really a vector network analyser. Yes, it can display a Smith Chart, but as an engineer I would not dare to really develop circuits based on those noisy measurements. It is maybe more a kind of scalar network analyser than a vector network analyser. And then a spectrum analyser with a tracking generator is maybe the better solution.

Rohde & Schwarz: If you go for general specs, the R&S is the best, but well, you can buy a nice car for that money. The frequency range is 9 KHz up to 6 GHz, it is a two port VNA. It is a one

box solution, so with display and knobs on the front panel, but it is impractical to work with without external mouse and keyboard. It “feels” like a German car, it is sturdy. But it is also heavy and bigger than the other solutions, which can be an disadvantage in some occasions. For me that is travelling around and is testing antennas in customers office, this heavy machine is a no go. The results are what you would expect from a 20.000 Euro machine, but front panel operation is cumbersome and very confusing.

operation

MegiQ: The instrument is controlled over USB by a desktop user interface that gives a good overview of measurement results, settings, saving/recalling. Operation is intuitive even with the many features, like stepping through bias voltages in multiple sweeps, automatic calculation of matching networks, etc.

The MegiQ user interface is by far the most pleasurable to work with. The manual gives a good overview but you will hardly need it.

The instrument is running under Windows XP, 7 and 8 and there are people using it on an Apple computer.

Their web site says: “designed by and for RF-engineers”, and I got impression that the user interface has really been developed in close cooperation with actual RF-engineer users.

It remembers where you left while closing the application, so when you start again you do not need to choose all those parameters again. The Session Manager is a very powerful but simple tool to group, save and recall your work: graphs, instrument settings, measurement data, calibration data, etc. I met the developer at an exhibition in Appledorn. They spend two hours to educate me and we measured some PCB antennas with coaxial cables together. Just to let you know, that the out of the shelf antennas was resonate on frequency range and/or showed a poor return loss as well. The MegiQ VNA is designed by engineers that has to develop RF circuits and antennas daily. They developed a tool including accessories like the “sandbox” and help engineers with skills in electronic to design RF electronic. They help not just with a good VNA - they help with some documentation and accessories (sandbox) for self-education. If you combine it with the free of charge software Atyune, then you get a very powerful combination. With the MegiQ VNA you measure the antenna, store the Touchtone file to your laptop, load it to Atyune and calculate the matching circuit by mouse click.

miniVNA: At first glance at the user interface you get an impression of the instrument, but if you look closer, it is not that obvious what the state of the instrument is. Does not look like one consistent program, but more like loose parts working together. If you e.g. want to see the Smith Chart, it opens in a different window and disappears to the background every time you hit the sweep button. And then you must save it using the “gif” button on the graph, A complete different procedure from saving the Return Loss graph -it is confusing. If, after performing an OSL calibration, you forget to hit the knob to actually use that calibration, you can start over again; and calibrating is really slow. The advantage is that the software is in Java and will run without installation. The three helical antennas tested and listed in former chapter I measured with the miniVNA. The result is on the server for download. At the scalar parameters VSWR and Return Loss the miniVNA shows a nice graph, but if you switch to Smith Chart, then you can detect that the graph is jumping around wild. If you then try to optimise an cellular PCB antenna shape multi resonate in GSM 850, 900, 1800, 1900 and UMTS 2150 then you will detect that the Smith Chart is cycling around in several time, what is common and necessary and on top the graph is jumping as well.

Rohde & Schwarz: The instrument is normally controlled on the front panel although there is the possibility for remote control. To use it without a mouse and external USB keyboard is not easy. It runs under windows, but the controls to access features like saving pictures (and where they actually go) are very difficult to find. Perhaps somewhere in the hundreds of pages of manual. And there are only two USB ports, so when using a keyboard and mouse, where does the memory stick to save the pictures go then...

There are a lot of features, and the push buttons an context sensitive menus that pop up on the side of the screen are not very intuitive (and that's an euphemism), so setting up the instrument before you can make a measurement is a tedious job. A seasoned RF engineer had to ask a colleague using the instrument daily for clues how to operate it. Myself got lost. There are to many buttons on the front panel and there are to many pages to read.

But of course once set it works fine. The problem is that when you switch the instrument off, it looks like it got a complete amnesia and next time you start it up, it comes back in an complete

other mode, other frequencies, etc. Sure there must be a setting for the defaults somewhere, but I could not find it. The transmission line and the antenna in a IoT M2M device are the most important part, but the time you spend to get a VNA up and running has to be realistic.

Yes it is a nice instrument, but for the price it costs you would expect a better user interface, one that is designed in cooperation with engineers who really have to use the instrument daily.

11.4.2 Graphical presentation of results

Besides the “technical specs”, graphical presentation of the measurement data is of importance. If you are doing a lot of measurements a day you want a display that gives overview and in depth information in one glance. And if you are only making a measurement every now and then, you want something easy interpretable.

MegiQ: The MegiQ user interface is far out the best when it comes to graphical presentation of the results. You are completely free to arrange all kinds of graphical representations of the measurement data on the screen. And it is easy to do. And if you save and then recall a measurement, you can still rearrange the graphs, switch markers on and off.

While making settings, the displayed measurement stays visible.

The graphs are easy interpretable, also after you print them, since beside markers there are labels along the trace lines. So also after printing a Smith chart, you can still see at what frequencies you are looking along the trace. Amazing that nobody else does this, even not the very expensive R&S.

miniVNA: You have one graph to display the results. You can choose what parameter you want to display in that graph, except the Smith Chart. For this there is an extra graph, but that one disappears to the background every time you hit the sweep button. It was not easy to set multiple markers. The software for miniVNA is a freeware by third party.

Rohde & Schwarz: Without an external screen, the graphical presentation is a bit messy. The screen is too small to display multiple graphs in a useful way.

11.4.3 Save / recall

MegiQ: If it comes to saving and recalling your work, setting etc, the MegiQ solution is the most powerful and at the same time the easiest to operate. It has a Session Manager where you group your settings, measurements, calibration tables in a very simple way and then save those groups in Session Files. For example a file for each project, or a file for each kind of measurement.

So you do not save a “picture” but the complete state of the instrument together with the measurements. From there you can of course choose to export the data in other formats to integrate in your report. But the big advantage is that when you want a different graph on the same data, or reposition the markers a week later, you can still do that (since you have the the complete dataset at hand and get it back into the instrument) and then export it to your report.

The MegiQ VNA was from beginning planned to be connected to a laptop/PC and is using all benefits that you can expect on a PC based VNA. Really everything and any data including the settings are saved in one file. The measurement data, the markers, the calibration of the VNA are stored together. If you power it of on Friday you just power it on and load on Monday and can go ahead without to loose time.

miniVNA: There are several ways to export measurements, but is is not in a structural way. So you can export e.g. to excel, csv, pdf, jpg, ... but that are all separate files, so you got to remember very well what went where...

Rohde & Schwarz: Very unclear what you are saving where. If you look it up in the manual, you can do it, but one month later I had really forgotten how and had to solve the puzzle again. You can save the actual data and recall it, but it is cumbersome and you need to go through different menus for that. Remember that the first Rohde & Schwarz VNAs was stand alone machines without interface to a laptop. Later on they got interfaces for floppy disks.

11.4.4 Exporting

MegiQ: You have a print button that easily saves the measurement with a comment to EMF, which is a standard vector format, so you can scale it in your report without losing resolution.

It uses the graphical representation you had put on the screen, so the combined graphs and markers, the complete overview you had in mind for the measurements. You can recall previous measurements, change the graphical representation, add markers, etc. and then again export the results.

A method to export the graphs individually, is to use the right mouse button and copy&paste the individual graphs into an other application, like Office.

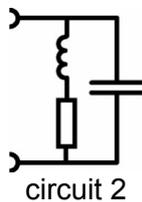
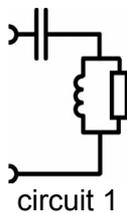
Exporting the measurement data in Touch Stone format is easy too, to import it in Excel or directly into your favourite RF simulation package. (there are three columns: freq, real and imaginary impedance)

miniVNA: You save the Return Loss graphs separately from the the Smith Charts. The latter can only be saved as a GIF. For the Return Loss graphs I had to rename the graphs in Windows every time, which is tedious. There is also the possibility to save the RL graph in a PDF, but you can not manage to combine the RL Graph with the Smith chart in one file for easy reporting. Truly spoken I export Touchtone and import it to Atyune. Atyune is much more handy what is logical because the developer of the software is developing embedded antennas daily.

Data can be exported in Touchtone (SP1), CSV, Excel or XML format.

Rohde & Schwarz: Of course you can export in all kind of ways, but each cumbersome: a lot of menu's to go through, and hard to remember one month later. It is just not obvious. I'm happy I could get the graphs out of the instrument in order to use them in this report, but I had to ask someone who is using the instrument daily. For my daily job it is not just to expensive, it is not very user friendly as well. If you do not use it daily, then you will forget fast how to use it.

11.4.5 Some actual measurements



Of course in the end it is very important that the instrument really does the job, so we compared two simple RCL circuits, both on all three VNAs. The test will show graph of the Return Loss and a Smith chart.

miniVNA: When we see the Smith chart from the miniVNA we see it is very noisy and it only gives an indication of the impedance at best. As a “plus” you get spurious peaks, which are rather annoying: they are around the GPS frequency band.

As with the R&S, (and many others) you can not see from the plot at which frequency you are looking (only start and stop freq are clear). During the measurement you can put markers, but once printed you can only guess.

The Return Loss plot looks more useful, although it is rather “bumpy”. You do not see those bumps with the MegiQ and the R&S. The line should be smooth.

MegiQ: A very clean Smith chart, very comparable to the data out of the R&S box.

In one glance you now realize the advantage of the labels along the trace: you see where you are about, also after saving it into a report!

The Return Loss plot looks nice, and gives the same results as the R&S VNA. No artefacts (bumps) that should not be there.

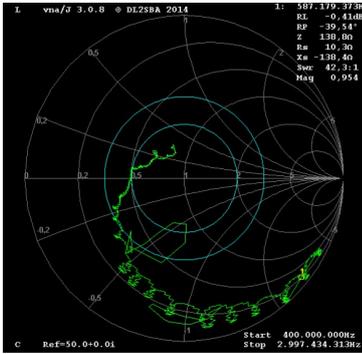
Rohde & Schwarz: As you would expect from R&S a clean Smith chart, comparable to the MegiQ graph. However to interpret the data after saving the picture is not very easy, since we only know the start and stop frequency. Looking at one point on the trace, you must make a very rough guess at which frequency you are looking: There are no frequency labels along the trace.

The Return Loss plot looks nice, and gives the same results as the MegiQ VNA.

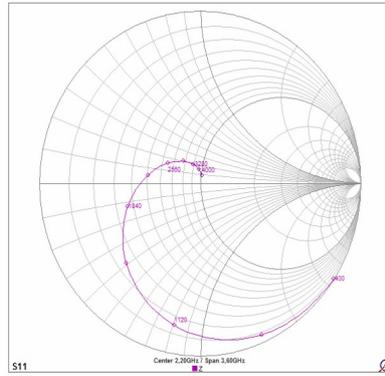
Let the graphs on the next pages speak for themselves...

11.4.6 Measuring LCR circuit 1

This is a capacitor in serie with an inductor shunted with a resistor.



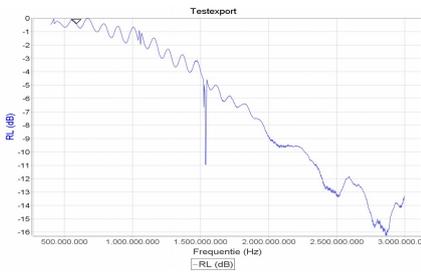
tinyVNA, circuit 1
400 ... 3000MHz
*Note the graph is very noisy,
and only gives an impression of
impedance.*



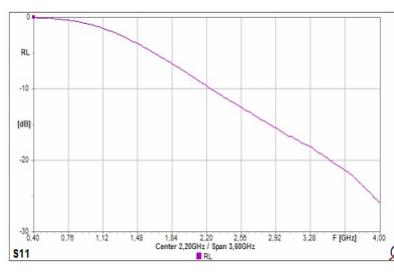
MegiQ, circuit 1
400 ... 4000MHz



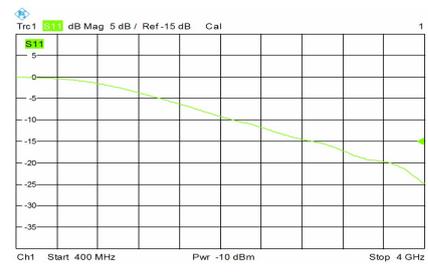
R&S, circuit 1
400...4000MHz



miniVNA
1 ... 3000MHz



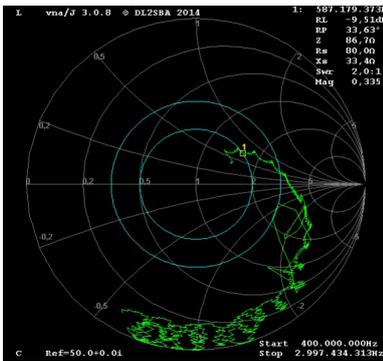
MegiQ
400...4000MHz



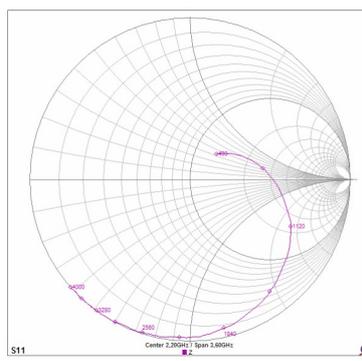
R&S
400...4000MHz

11.4.7 Measuring LCR circuit 2

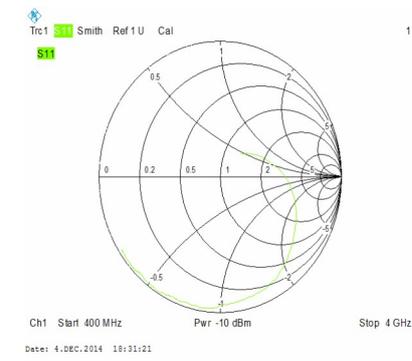
This is a capacitor in parallel with an R and an L in series.



miniVNA, LCR circuit 2
400...3000 MHz
*Note the graph is very noisy,
and only gives an impression of
impedance.*



MegiQ, LCR circuit 2
400...4000 MHz



R&S ZVL6, LCR circuit 2
400...4000 MHz

LCR circuit 2 (return loss graph)