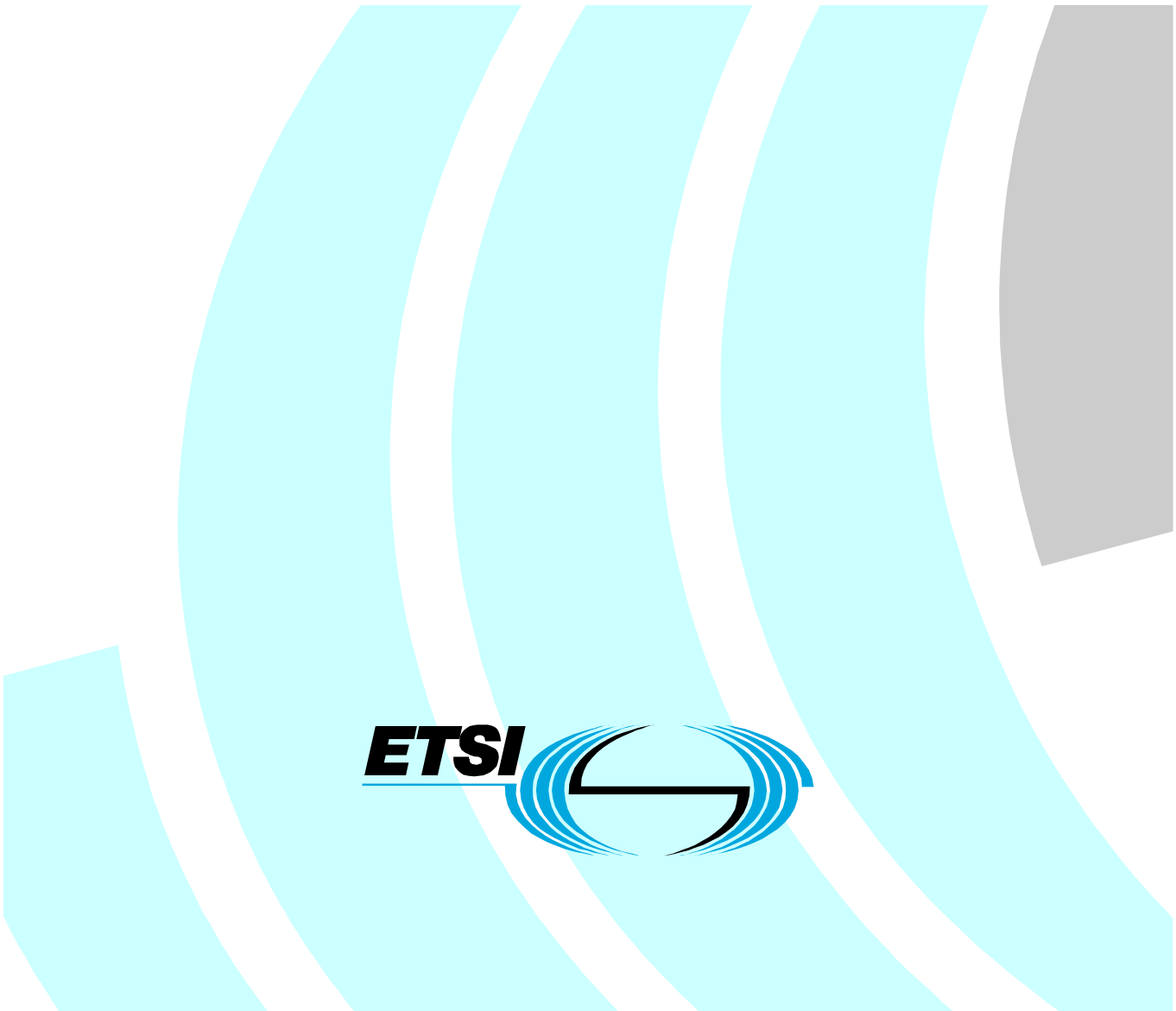
ETSI TR 102 151 V6.0.0 (2003-02)

Technical Report

Smart Cards;
Measurement of Electromagnetic Emission of SIM Cards;
(Release 6)



Reference
DTR/SCP-000286

Keywords
EMC, smart card

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

All published ETSI deliverables shall include information which directs the reader to the above source of information.

Foreword

This Technical Report (TR) has been produced by ETSI Project Smart Card Platform (SCP).

The contents of the present document are subject to continuing work within EP SCP and may change following formal EP SCP approval. If EP SCP modifies the contents of the present document, it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

0 early working draft;

1 presented to EP SCP for information;

2 presented to EP SCP for approval;

3 or greater indicates EP SCP approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

ETSI Project Smart Card Platform (SCP) identified potential problems between mobile equipments and SIM/UICC due to electromagnetic interferences. To allow the analysis of such potential problems it is necessary to define a common reproducible measurement procedure. This allows the comparison of different EMC measurements

The aim of this report is the definition of a standard hardware equipment for EM measurements of smart cards and a common EM measurement procedure.

Further EM measurements are described in the appendix of this report from already existing smart cards used for SIM.

1 Scope

The present document describes:

- a reference test board and TEM cell for EM measurements of smart cards;
- EM measurement procedures for smart card using the reference test board and TEM cell;
- Sample EM measurements of already existing smart cards.

2 References

For the purposes of this Technical Report (TR), the following references apply:

[1] ISO/IEC 7816-3: "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols".

[2] ETSI TS 102 221: "Smart cards; UICC-Terminal interface; Physical and logical characteristics".

[3] ISO 11452-3: "Road vehicles - Component test methods for electrical disturbances from narrowband radiated electromagnetic energy - Part 3: Transverse electromagnetic mode (TEM) cell".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Answer To Reset (ATR): string of characters sent by the card following a reset sequence

card: the smart card, SIM or UICC

clock: the clock provided by the terminal to the card

external clock (e.c.): which has a sinusoidal shape

onboard clock (o.c.): which has a rectangular shape

reader: the hardware used to connect the card to the terminal printed circuit board

TC: metal box used for the measurements

terminal: the handset, ME or UE

Transparent Reader (TR): the terminal used to communicate with the SIM card

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ATR	Answer To Reset
ATT	ATTenuation
CLK	CLocK signal provided by the terminal to the card
e.c.	external clock
I/O	bi-directional communication line between the terminal and the card
NL	Noise Level

o.c.	onboard clock, which has a rectangular shape
PCB	Printed Circuit Board
RBW	Resolution Band Width
RST	ReSeT signal provided by the terminal
SA	Spectrum Analyser
SNR	Signal to Noise Ratio
TR	Transparent Reader
SET	SIM card EMV Test

4 Measurement Equipment

For the EMC measurements the following measurement equipment is needed:

- SET Board: SIM EMC Test board; There are different variations of SET boards available that are described below.
- TEM cell: The needed TEM cell is described below.
- Spectrum analyser that allows the measurements within the different test frequency bands.
- Clock generator to provide the external clock for the SIM.

4.1 Description of the SET Boards

The reference SET board is developed with the following features:

- Power control.
- Special types of plugs for power supply, signal measurements and communication.
- Special filters for reduction of external radiation (p-type filters).
- 6-layer board symmetrical stack up, TEM cell ground only penetrated by signal vias.
- Mobile-specific network inside and outside the TEM cell.
- Different boards with different type of readers.

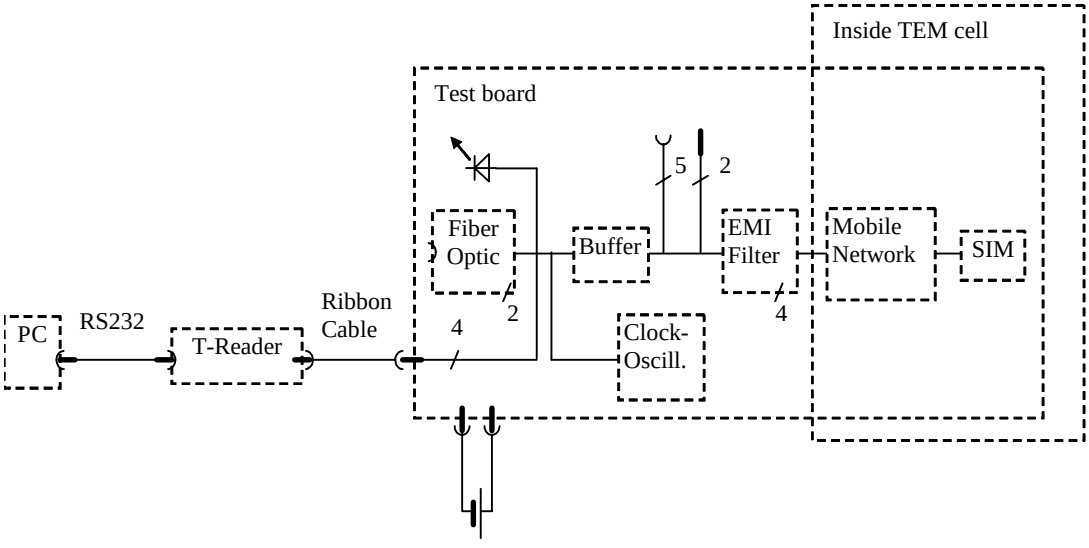


Figure 4.1: Schematic description of the SET board

There are SET boards with different plug-in card readers available. Also the mobile network could be optionally placed outside of the TEM cell. These variation of SET-boards allows the choice of the optimum test condition for a specific problem case.

The following four SET-board versions were used for the generation of the present document:

- Version 1 with Amphenol, No. C707 10 M 006 0012 plug-in reader (6 leads on one side) and mobile network outside of TEM cell.
- Version 2 with Amphenol, No. C707 10 M 006 0492 plug-in reader (three leads on each side) and mobile network outside of TEM cell.
- Version 3 with Amphenol, No. C707 10 M 006 0972 plug-in reader (small version) and mobile network outside of TEM cell.
- Version 4 with Amphenol, No. C707 10 M 006 0492 plug-in reader (three leads on each side) and mobile network inside of TEM cell.

The SET-board can be used in four different operation modes:

- Stand Alone Mode: The card needs only power, reset and clock after the program is started and runs in an endless loop. There is a choice between an onboard clock (rectangular) and external clock (sinusoidal). An onboard reset control is implemented.
- Communication Mode via electrical link: Full communication with a TR.
- Communication Mode via fibre optics: Full communication with a TR.
- Conducted emission: Plugs for measurements are on board.

4.2 Schematic of the Mobile-specific Network

Figure 4.2 shows the mobile specific decoupling network on the SET-board that is either located inside or outside the TEM cell.

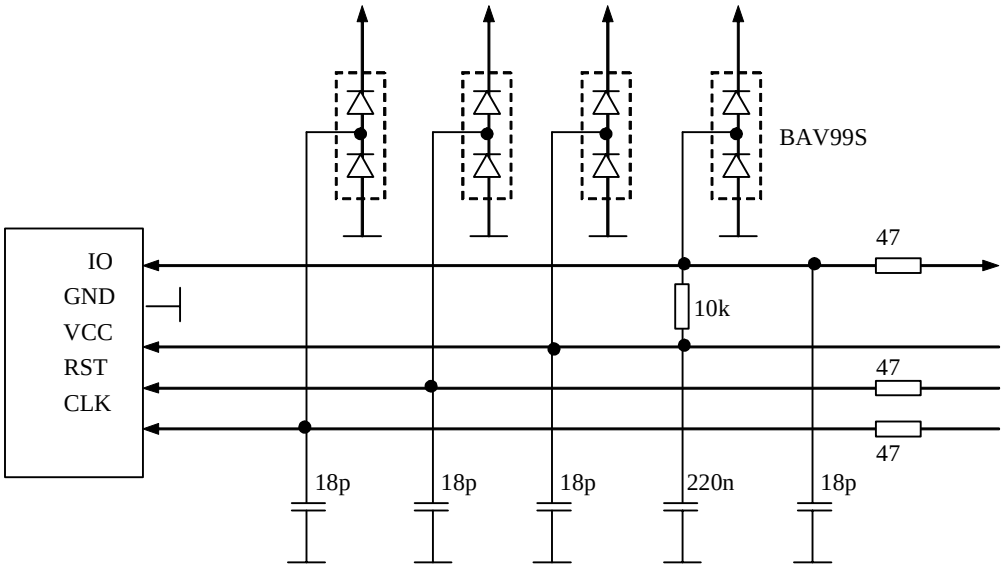


Figure 4.2: Description of the mobile specific network

4.3 Description of the TEM cell

For mounting the SET board at the TEM cell, a TEM cell from Fischer Custom Communication Inc. Model Nr. FCC - TEM- JM3 for the usage up to 2 000 MHz (U.S. Patent Nr. 543 66 03) is used.

Figure 4.3 shows the TEM cell with the SET board.

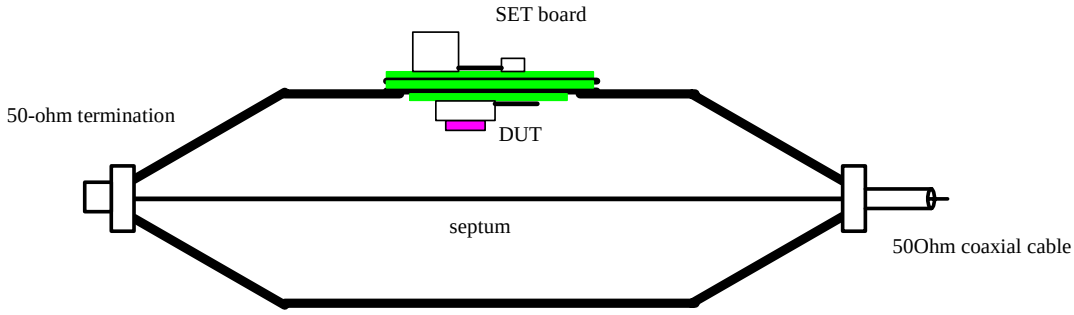


Figure 4.3: Schematic description of the TEM cell

The SET board can be mounted in four different orientations at the TEM cell:

- 0° (12 h).
- 90° (3 h).
- 180° (6 h).
- 270° (9 h).

5 Measurements

5.1 List of test frequency

The following test frequency bands are recommended for the EMC measurements:

- Band 1 (Low frequency): 1 MHz to 100 MHz.
- Band 2 (GSM, EGSM): 800 MHz to 1 000 MHz.
- Band 3 (PCN1800, PCN1900, UMTS): 1 700 MHz to 2 200 MHz.

5.2 Measurement procedure

To allow a correct analysis of the measurement result the following influence have to be checked before analysis of the measurements:

- System dependencies: Therefore the spectrum analyser shall perform measurement with a reference resistance of 50 Ω within the test frequency bands. Typically at each individual spectrum analyser some significant peaks above noise level will occur that should be filtered out for the analysis of the measurements.
- Influence of the measurement equipment: Therefore the spectrum analyser shall perform measurements with a connected SET board mounted at the TEM cell. The SET board shall not be connected to any other electrical signals (Power, clock or I/O) during the measurements. After the measurements it has to be verified if the measurement equipment has a significant influence on the measurement results.
- Influence of the board orientation: Therefore measurement with identical conditions (Same clock, power, SIM, operation mode…) shall be performed with different orientated SET board at the TEM cell. For this measurement it is recommended to use test conditions where a high EM radiation is expected. After the analysis of these measurements it is recommended to use the orientation with the highest EM radiation results (worst case).

- Influence of external clock: Therefore measurements with a not powered smart card shall be performed with different clock shapes to measure the spectrum of the external clock signal. If the smart card hardware can be driven by a sine signal, then it is recommended to use this clock shape to reduce the emitted spectrum of the external clock signal. The spectrum of the clock signal have to filtered out for the analysis of the EM measurement results.

To analyse generally the EM radiation of smart cards the following analysis are recommended:

- Influence of operation mode: Therefore measurements shall be performed with different operation modes of the SIM (stand-by mode, normal CPU calculations, cryptographic calculations, I/O transfer mode…).
- Influence of different SIM chip hardware: Therefore measurements with different SIM chip hardware shall be performed.
- Influence of mobile decoupling network: Therefore measurements under the same test conditions with the mobile network inside and outside the TEM cell shall be performed by exchanging the SET boards.
- Influence of plug-in reader: Therefore measurements under the same test conditions with different plug-in reader shall be performed by exchanging the SET boards.

Annex A:
Sample EM Measurements

A.1 Global Setup

For the measurements shown in this annex the following conditions were used:

- VDD external = 5 V.
- External clock frequency = 3.57.
- Global RBW = 10 kHz.
- Measurements in dBµV.

The following test cards were used:

C#1: SLE 88 CX 720 P, Infineon with 27 MHz internal clock.

C#2: SLE 66 CX 320 P, Infineon with max 12 MHz internal clock.

C#3: SLE 66 C 162 P, Infineon with max 12 MHz internal clock.

The following measurement equipment was used:

- FSP spectrum analyser 9 kHz to 7 GHz from Rhode & Schwarz, Munich.
- Clock Generator; Philips, PM 5193.
- SET boards as described in the present document.
- TEM cell as described in the present document.

A.2 System dependencies

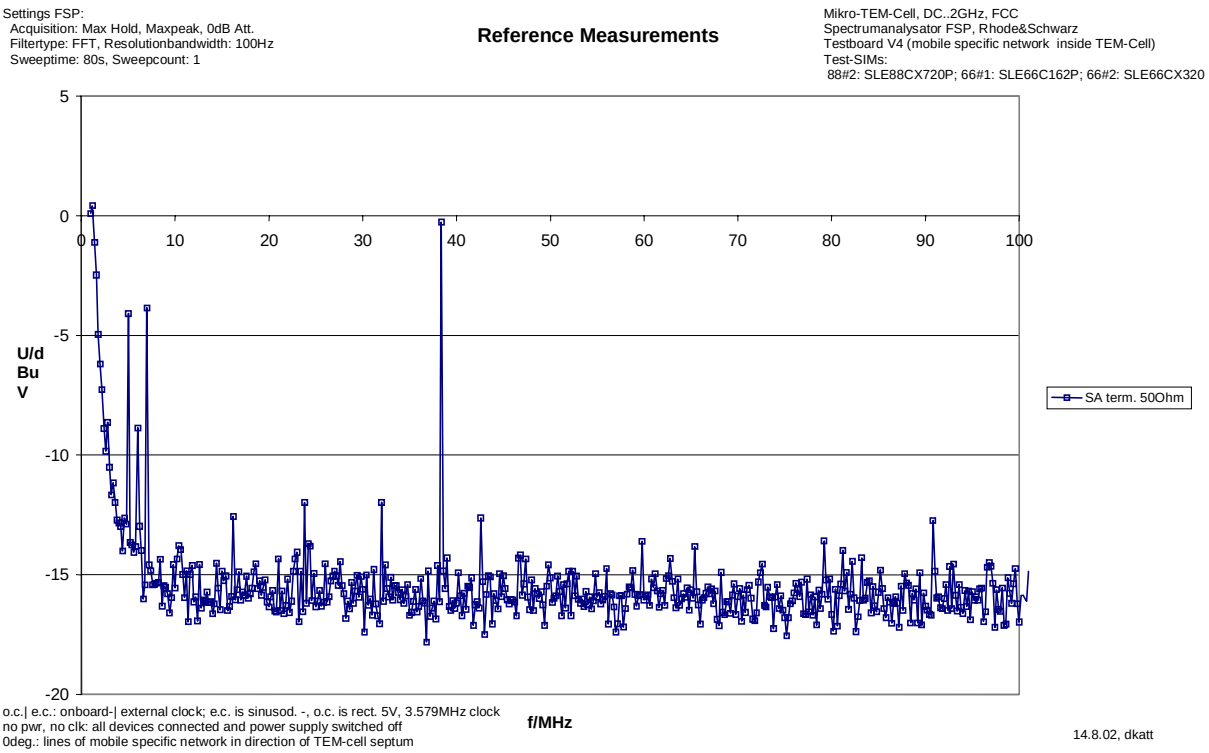


Figure A.1: Best measurement possible

In this measurement the spectrum analyser is terminated with a 50-Ω reference resistance. Four peaks are visible, which are caused by system dependencies of the spectrum analyser. The dedicated frequencies are 5 MHz, 6 MHz, 7 MHz and 38.4 MHz. The spectrum analyser was checked by the manufacturer, who guarantees an ATT of -103 dBm. These peaks are within the specification of the spectrum analyser and are unavoidable. At these frequencies the value was manually set to -20 dBµV to show that we are blind at these frequencies. There are also peaks at higher frequencies, therefore making it necessary to always perform a reference measurement before real measurements.

Conclusion: The NL is -15dBµV with this type of spectrum analyser at an RBW of 100 Hz. This could be improved by using a preamplifier.

A.3 Influences of the measurement equipment

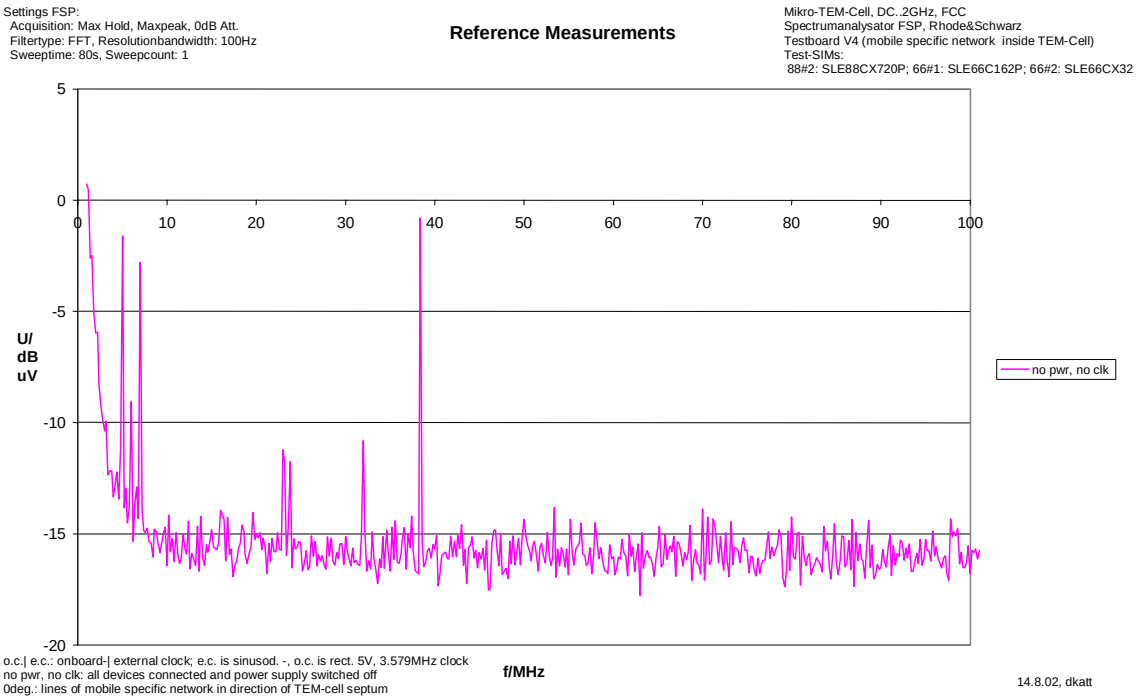


Figure A.2: Influence of measurement equipment

Here the measurement was completely set up (SA, TC, SET board, card), but the device was not under power and there was no clock.

Conclusion: The setup has no major influence on the measurements, peaks under 5 dBµV should not be considered.

A.4 Influence of board orientation

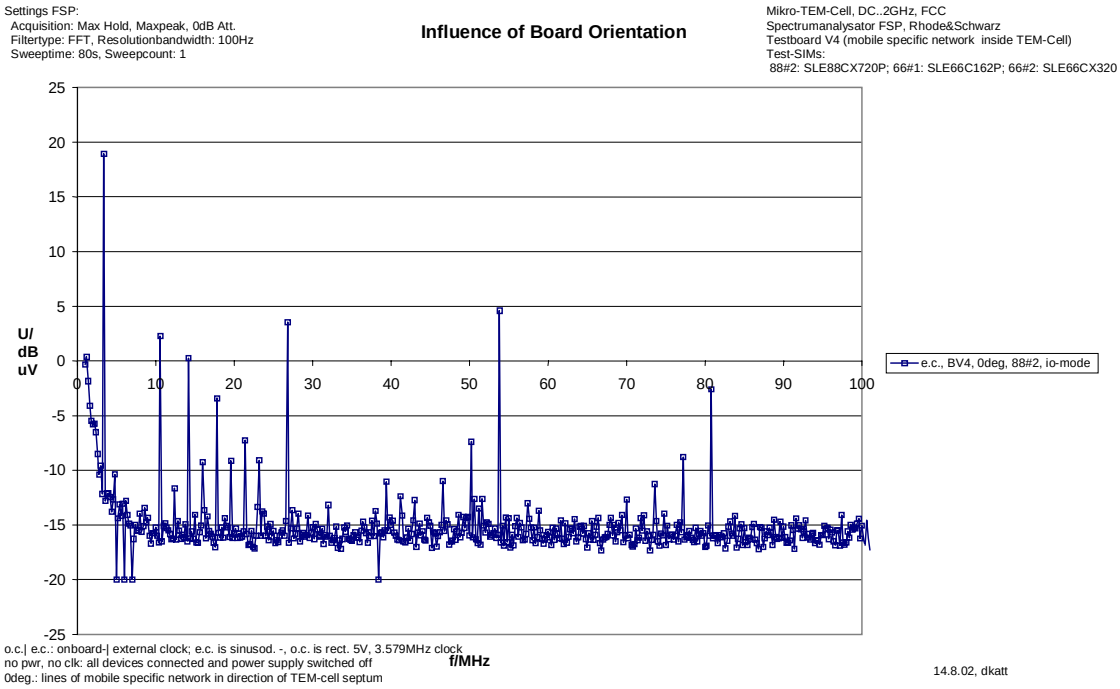


Figure A.3: Influence of board orientation at 0° (SLE 88 CX 720 P, I/O mode)

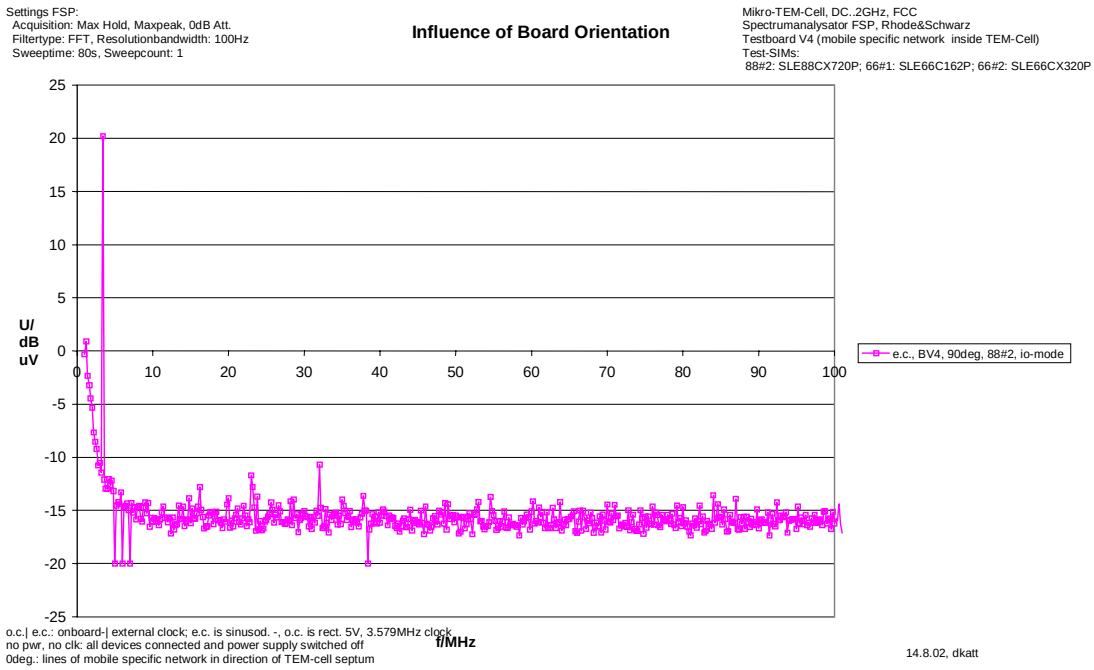


Figure A.4: Influence of board orientation at 90° (SLE 88 CX 720 P, I/O mode)

Conclusion: The orientation of the board has a major influence on the measurements. 0° and 180° show identical results, as do orientations of 90° and 270°. An orientation of 0° was used for all further measurements (representing the worse case).

A.5 Influence of Clock Shape

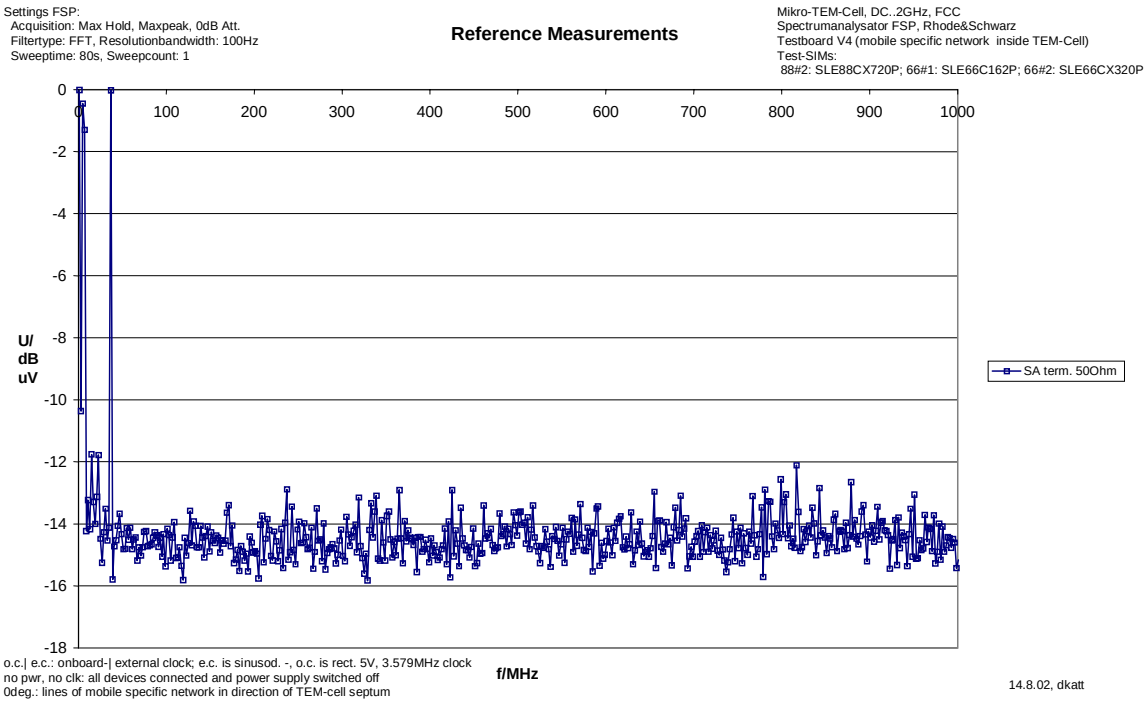


Figure A.5: 1 MHz to 1000 MHz, best measurement possible

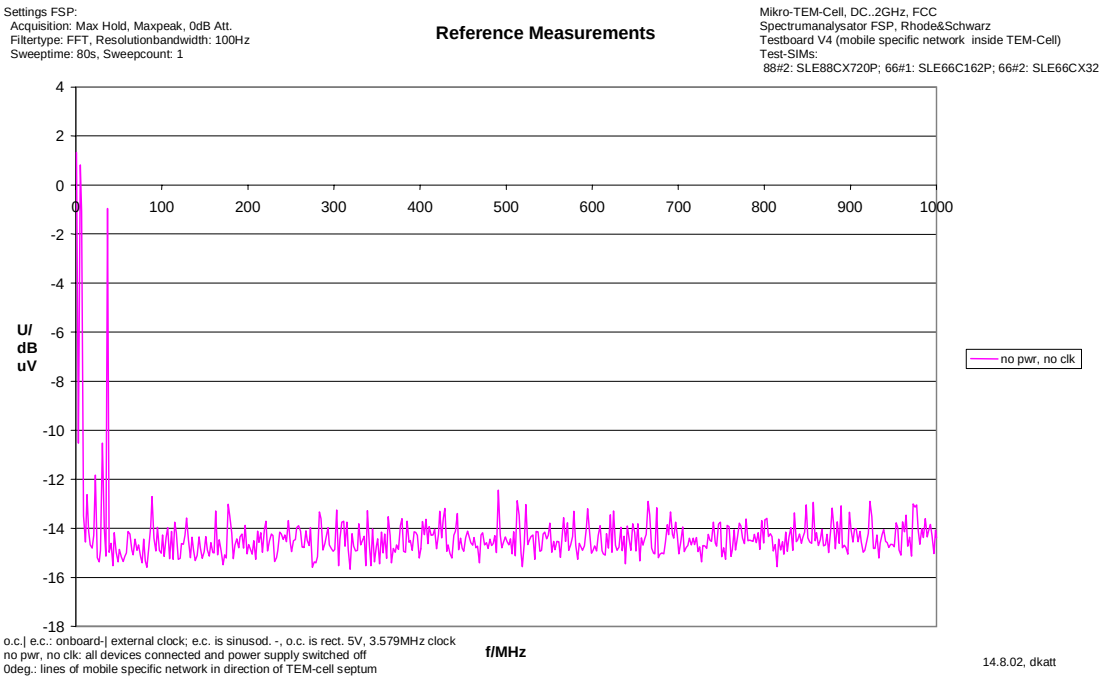


Figure A.6: 1 MHz to 1000 MHz, influence of setup

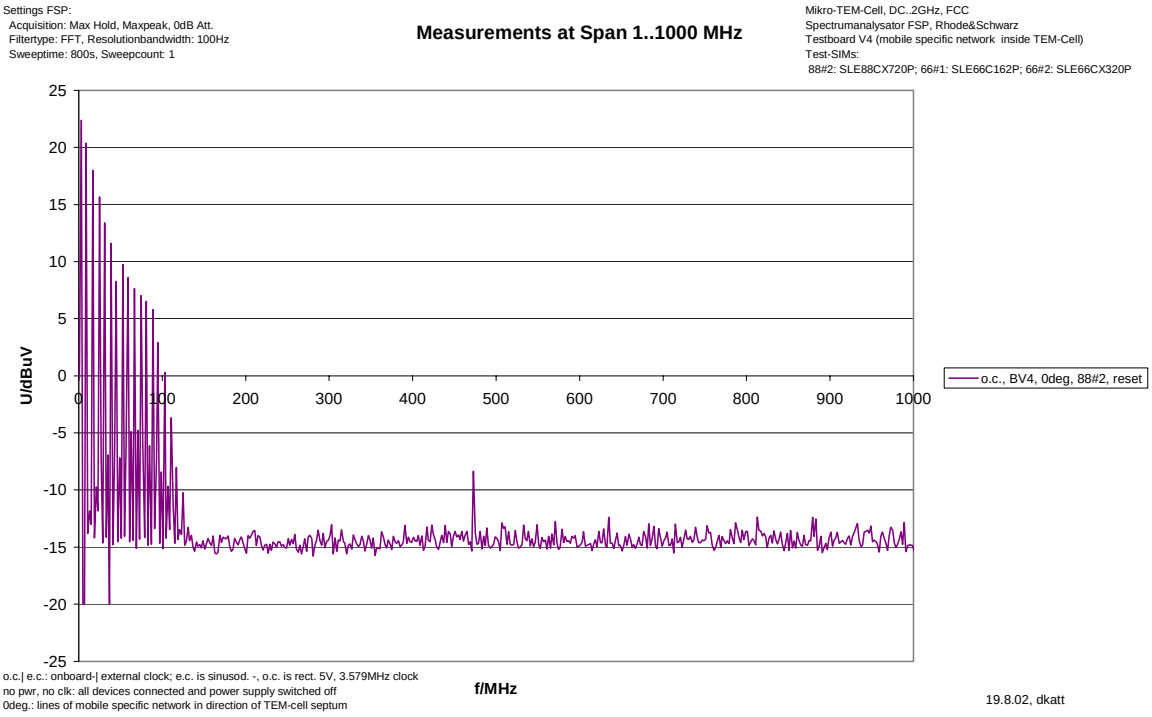


Figure A.7: 1 MHz to 1000 MHz, clock shape rectangular, pll off

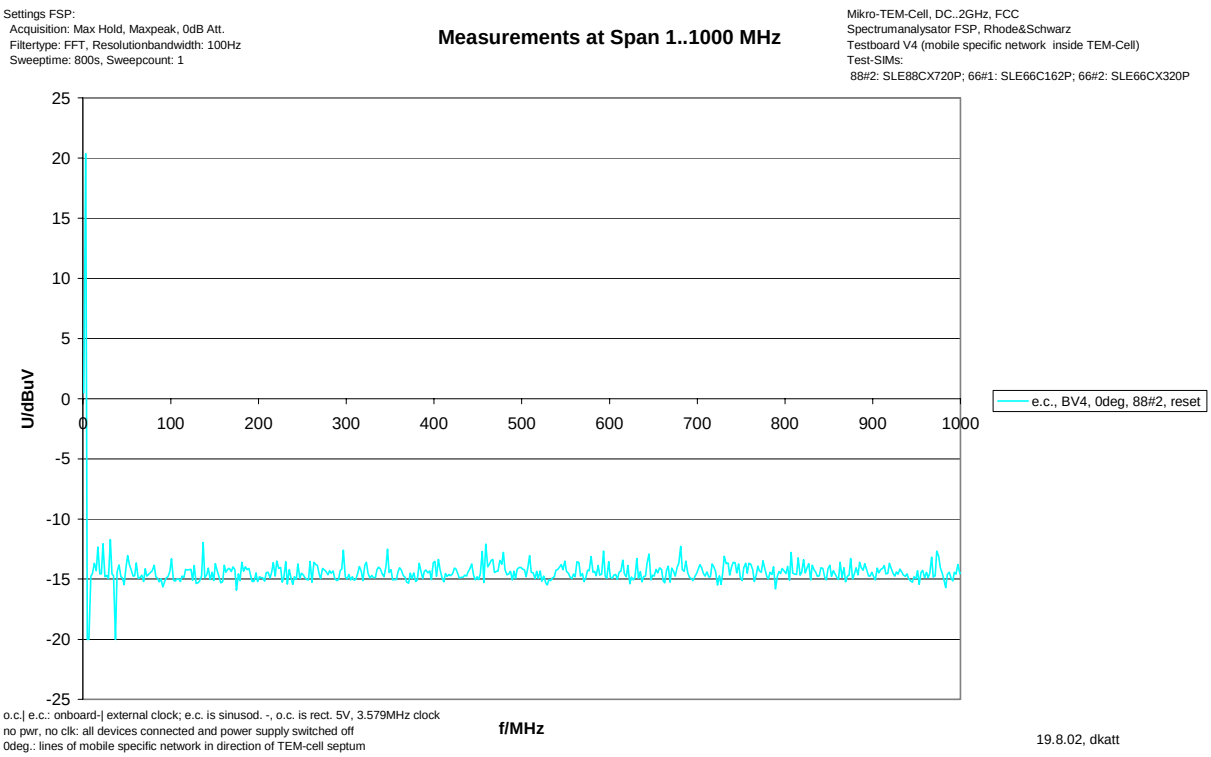


Figure A.8: 1 MHz to 1000 MHz, clock shape sinus, pll off

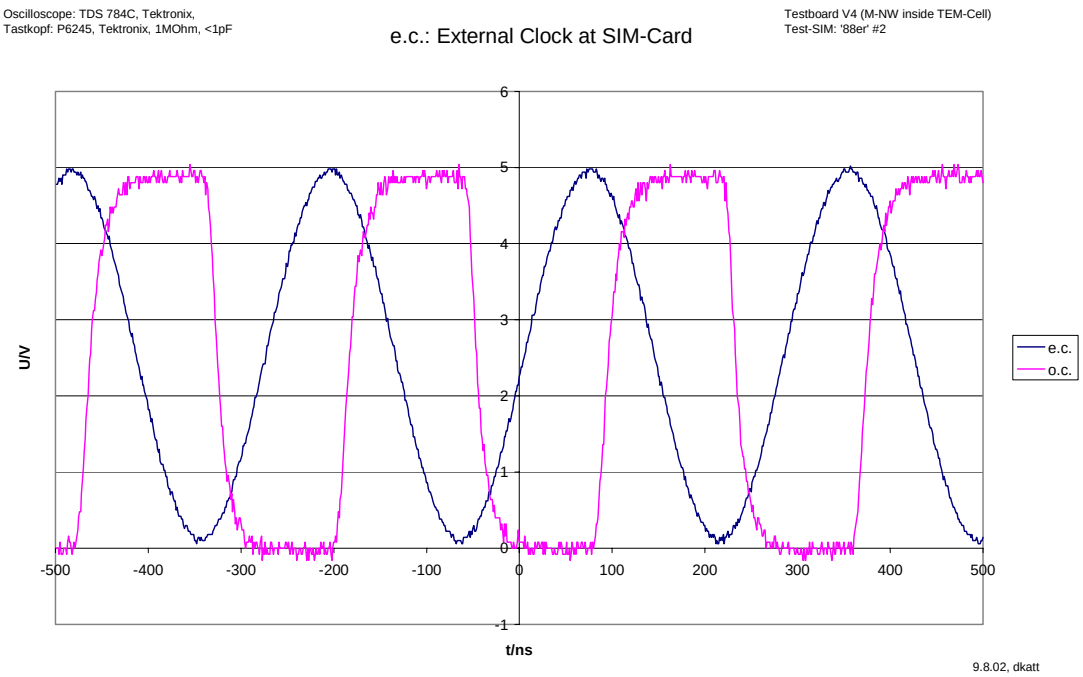


Figure A.9: Clock shape sinusoidal / rectangular

The rectangular clock has many harmonics up to 100 MHz; the sinusoidal clock has only 1 peak at 3.57 MHz and no harmonics. Normally the rectangular clock is used in a handheld. A crystal oscillator is necessary for a sinusoidal clock. The clock pad has a Schmitt trigger inside, so on chip the clock is rectangular again. It makes no difference to the tested smart cards itself if the shape of the clock is sinusoidal or rectangular.

Conclusion: For proof of the radiation of these smart cards a sinusoidal clock is recommended, otherwise the harmonics of the clock would mask the radiation of the chip. All further measurements are done with a sinusoidal clock if not explicitly declared otherwise.

A.6 Influence of the operation mode

For this analysis a card with SLE 88 CX 720 P was used.

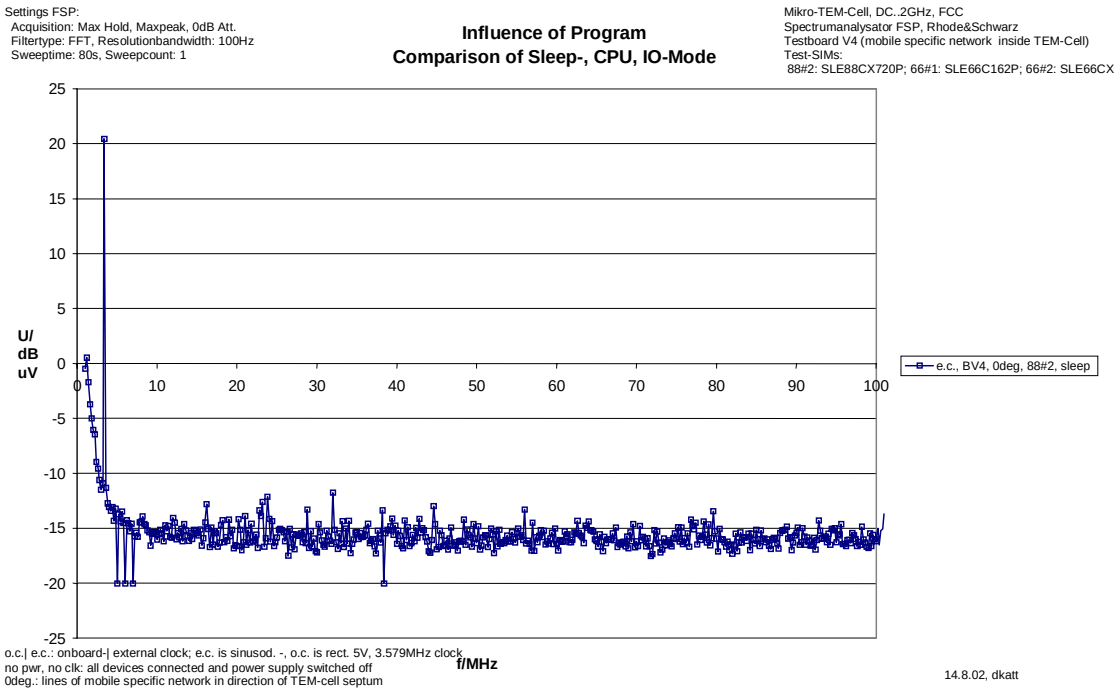


Figure A.10: Sleep mode (no PLL running, SLE 88 CX 720 P)

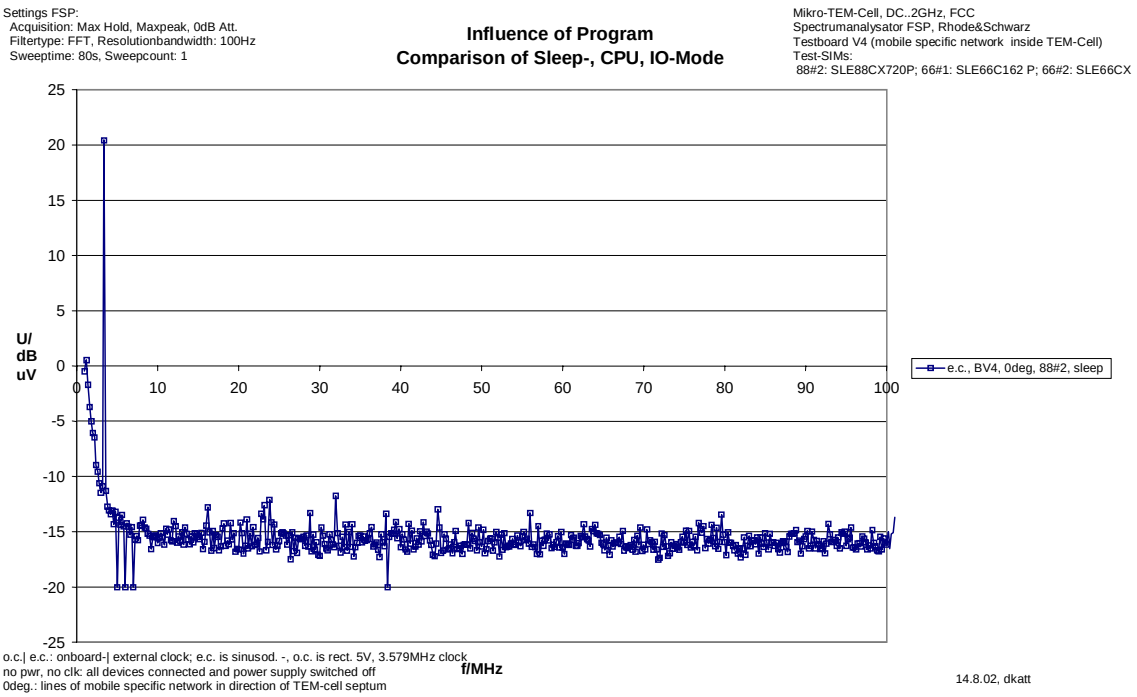


Figure A.11: Sleep mode (PLL running, SLE 88 CX 720 P)

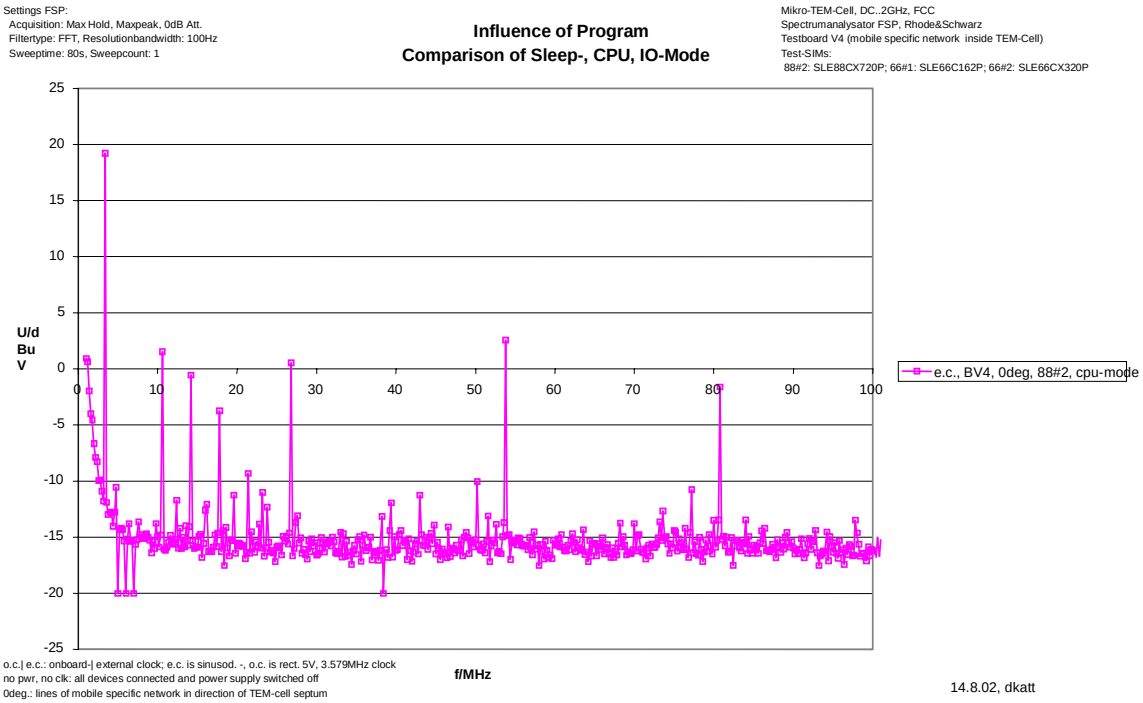


Figure A.12: CPU mode (SLE 88 CX 720 P)

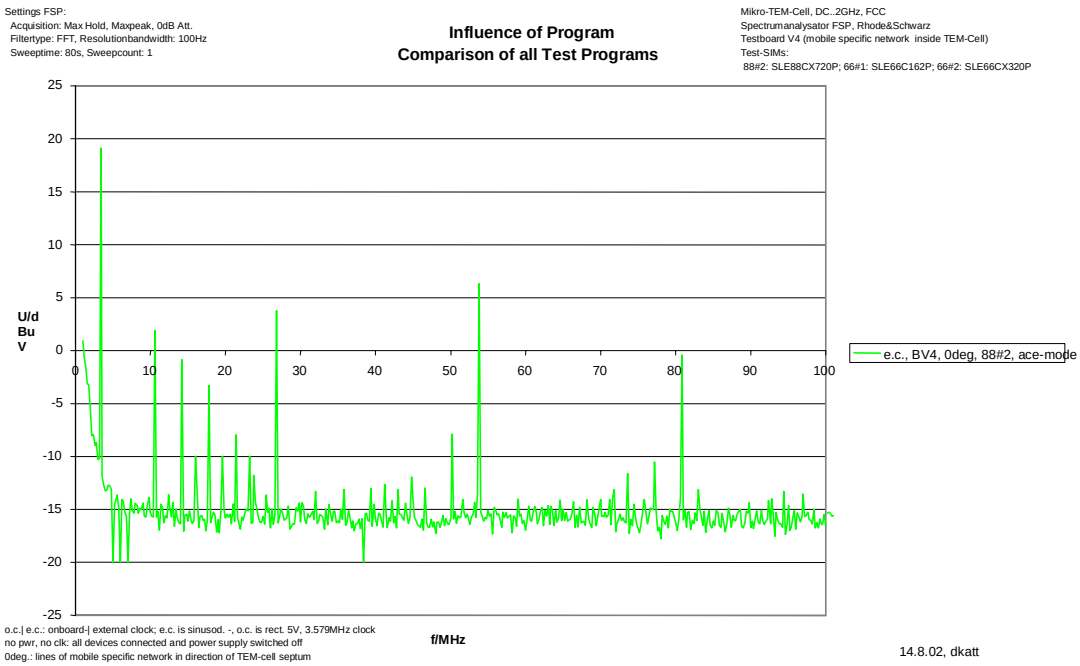


Figure A.13: ACE mode (SLE 88 CX 720 P)

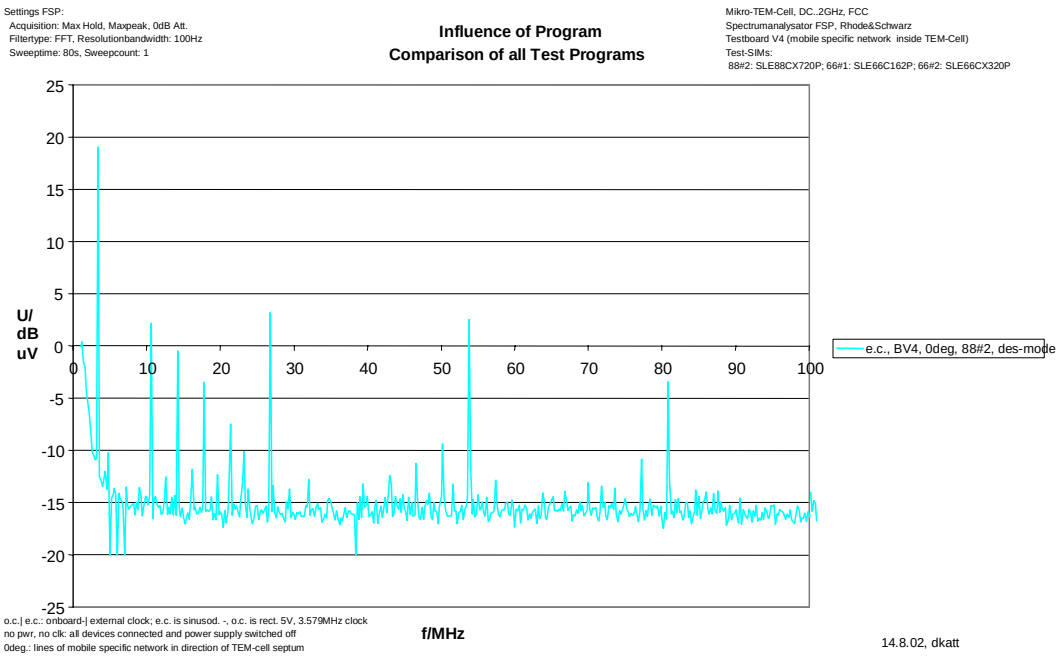


Figure A.14: DES mode (SLE 88 CX 720 P)

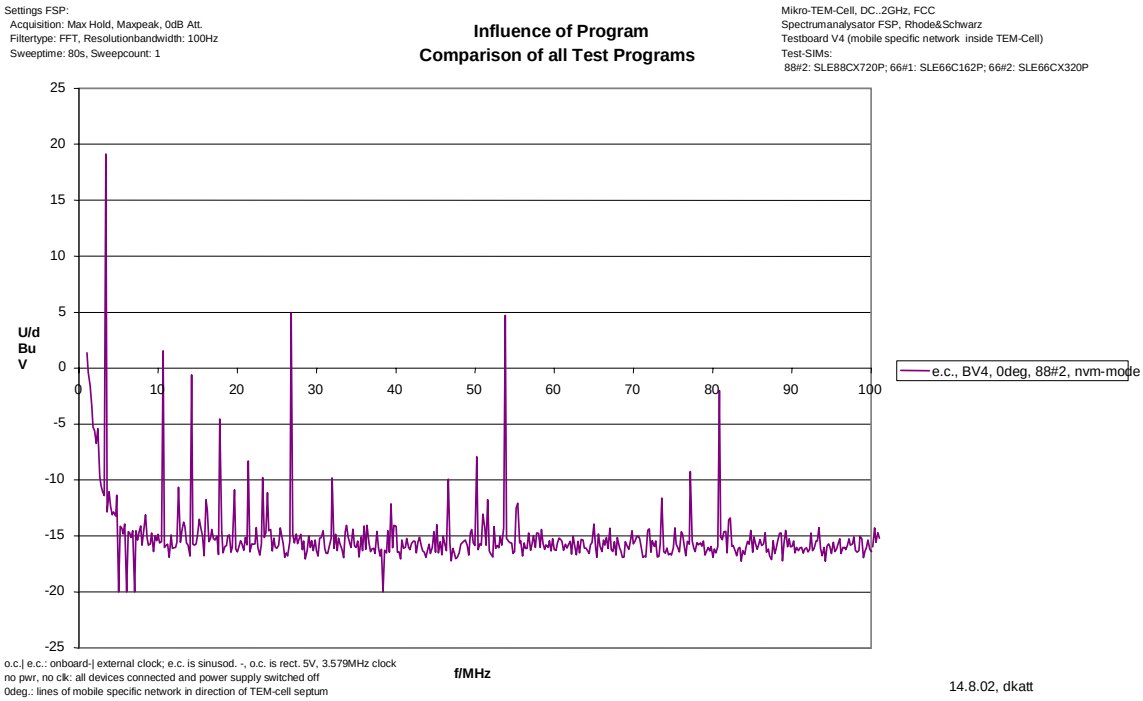


Figure A.15: NVM mode (SLE 88 CX 720 P)

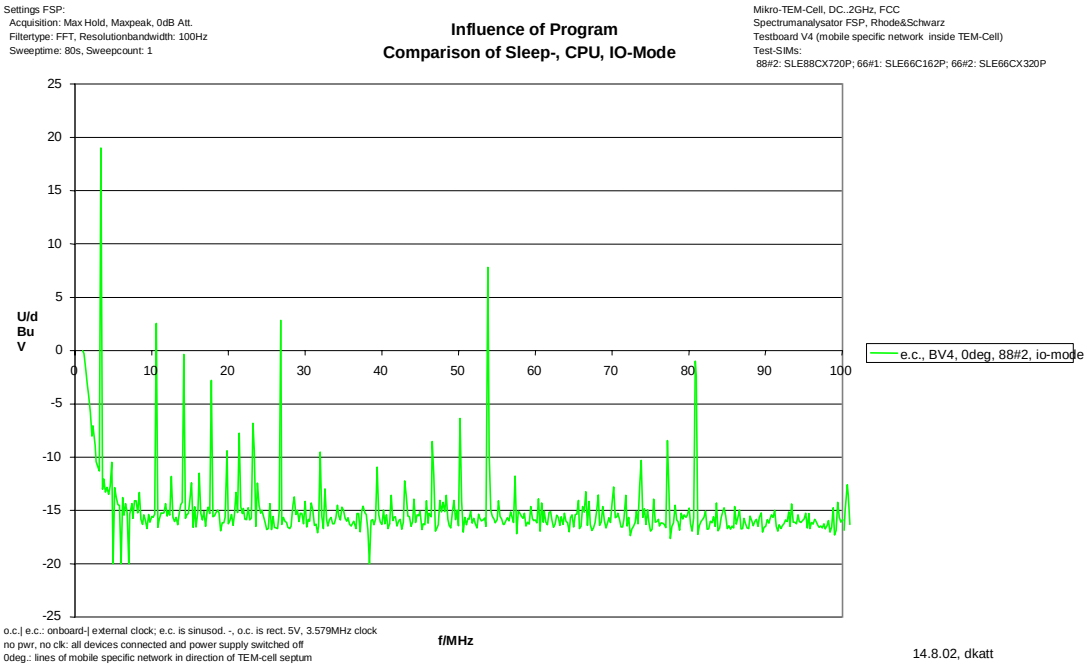


Figure A.16: I/O mode (SLE 88 CX 720 P)

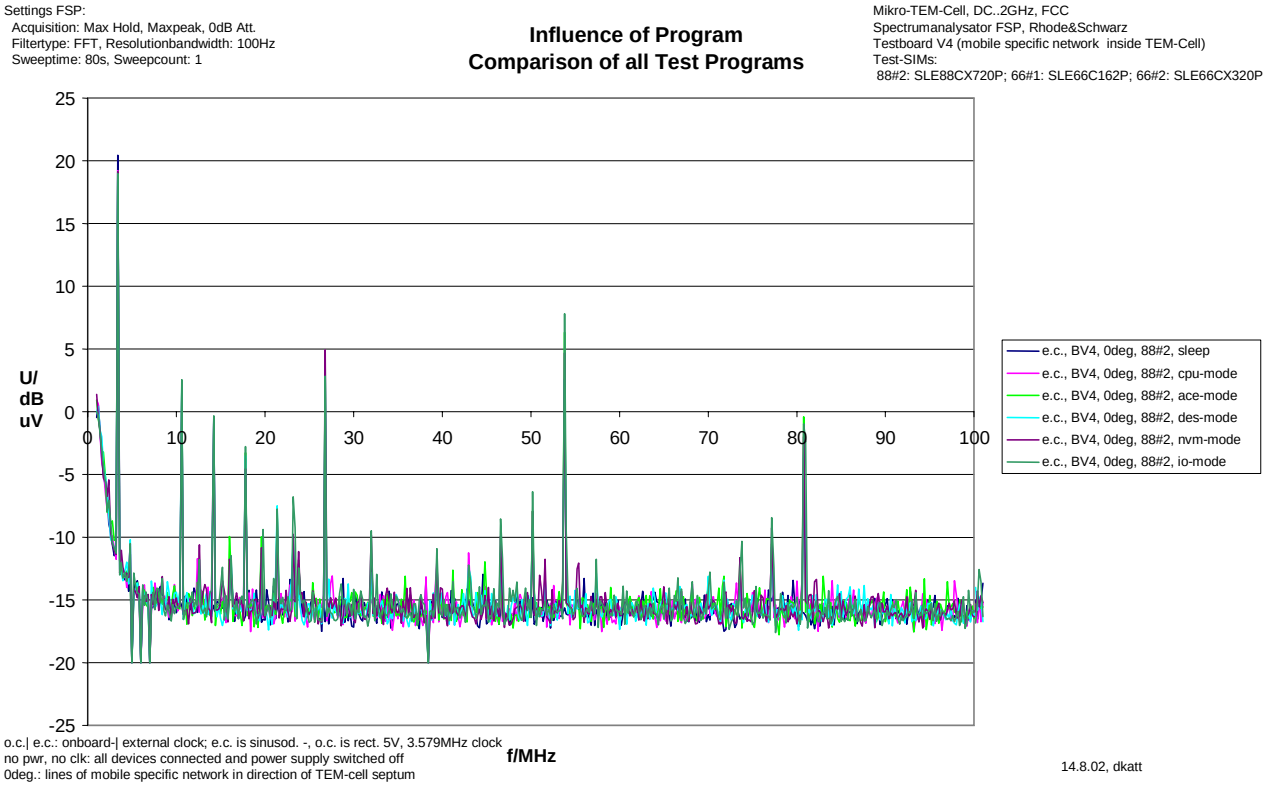


Figure A.17: All modes (SLE 88 CX 720 P)

6 different modes were used (programs running on the chip repeated in an endless loop). They are as follows:

- **Sleep Mode:** There is no activity on the chip, not even the pll is running; this mode was used as the reference mode.
- **CPU:** There is a high level of activity in the CPU.
- **ACE:** Asymmetric cryptographic execution mode.

- **DES:** There is a high level of activity in the DES module and in the chip crypto coprocessor.
- **NVM:** There is a high level of activity in the NVM (non-volatile memory) programming and reading.
- **I/O:** There is a high level of activity on the I/O pin; the chip is permanently sending a byte stream.

Four frequencies have been set to –20 dBµV (here for the first time) according to the system dependencies.

The sleep mode has no significant peaks, only the clock (3.57 MHz) can be seen with 30 dB above NL. This sine wave is clean, there are no harmonics. The I/O mode has the highest peaks. In this mode a second pin is permanently active. The other modes show no major differences. No radiation to be seen above 100 MHz.

Conclusion: There is some radiation in the range under 100 MHz up to 25 dB (6 peaks), the clock shows 30 dB.

A.7 Influence of the chip hardware

A.7.1 SLE 66 C 162 P

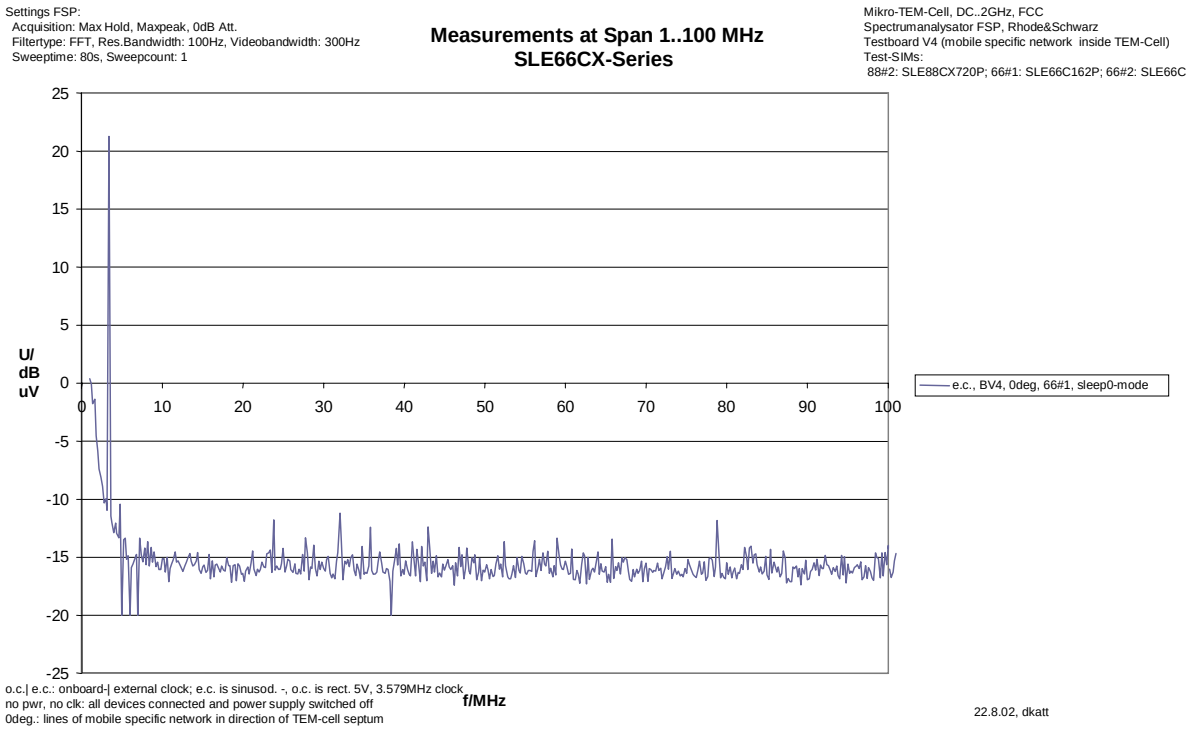


Figure A.18: Reference, sleep mode (no PLL running, SLE 66 C 162 P)

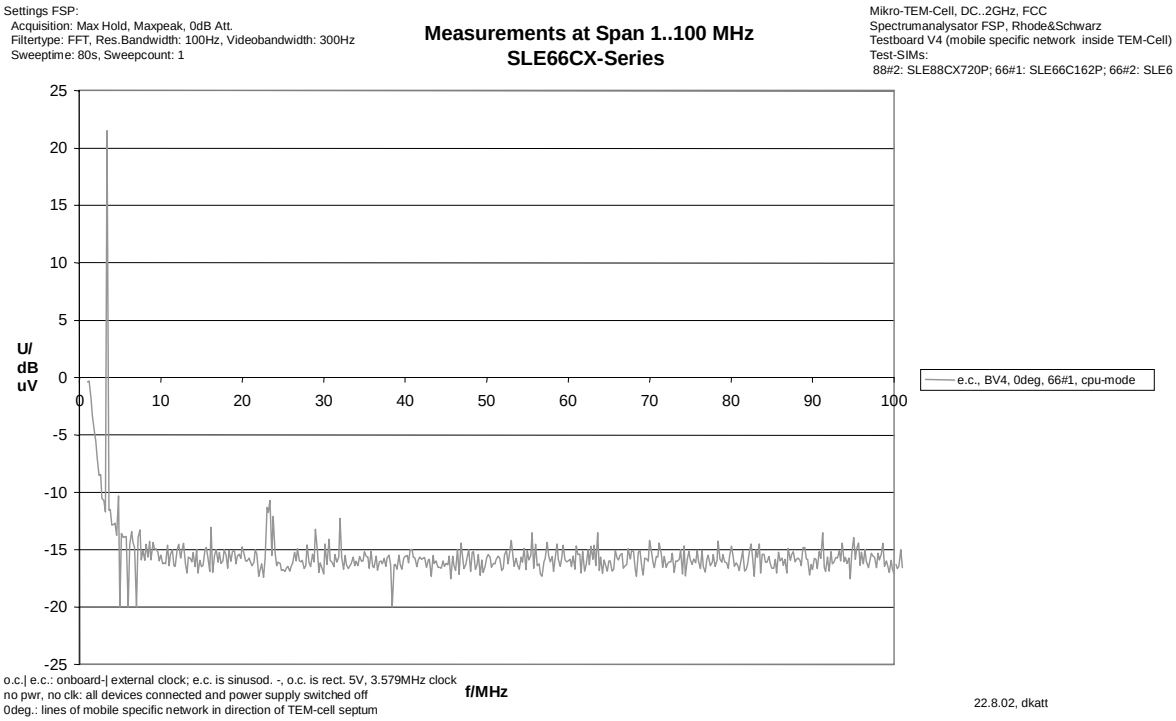


Figure A.19: CPU mode (SLE 66 C 162 P)

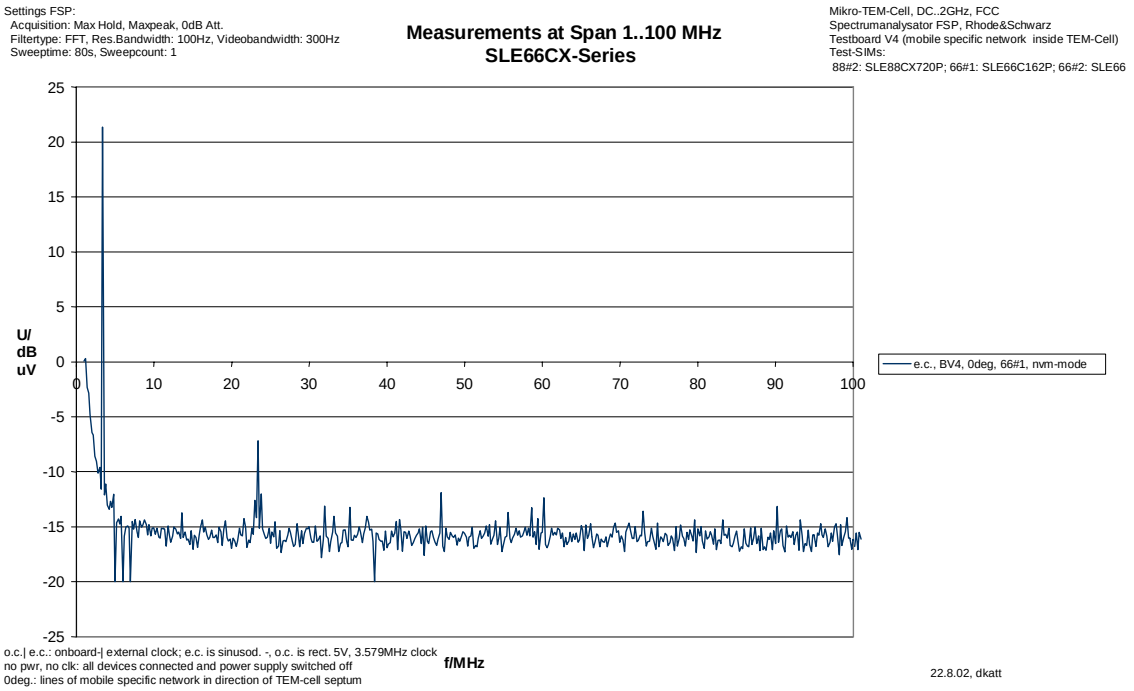


Figure A.20: NVM mode (SLE 66 C 162 P)

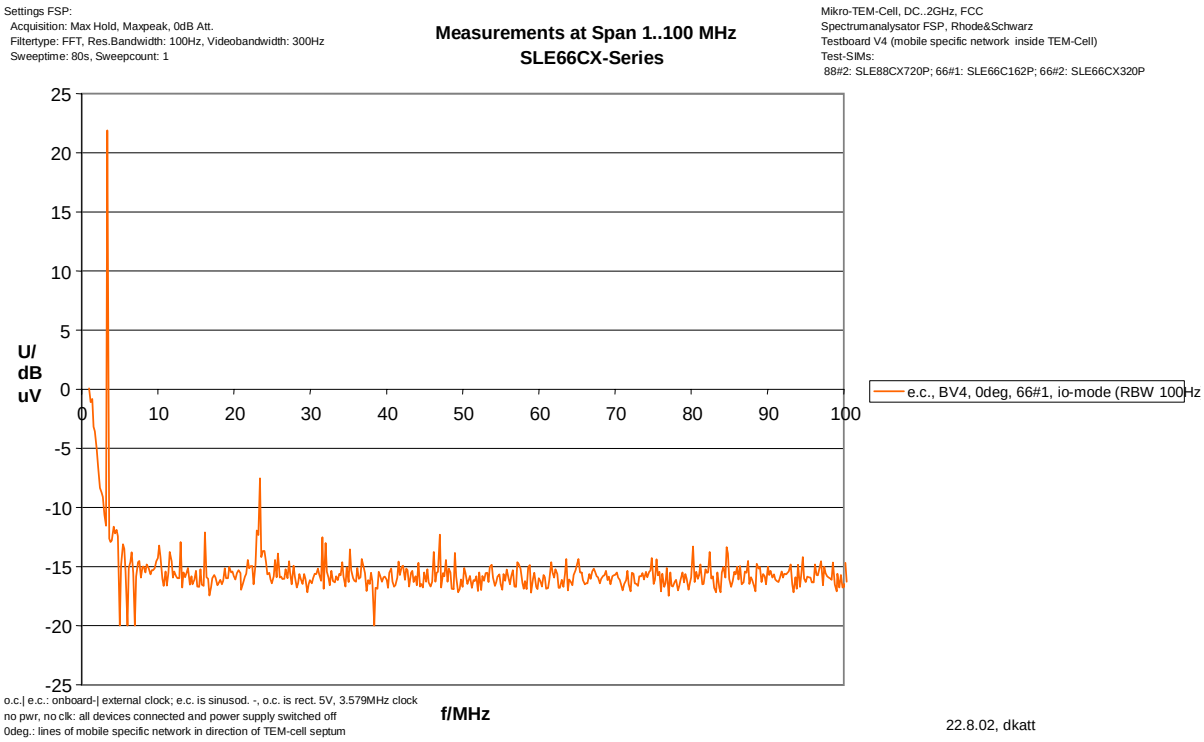


Figure A.21: I/O mode (SLE 66 C 162 P)

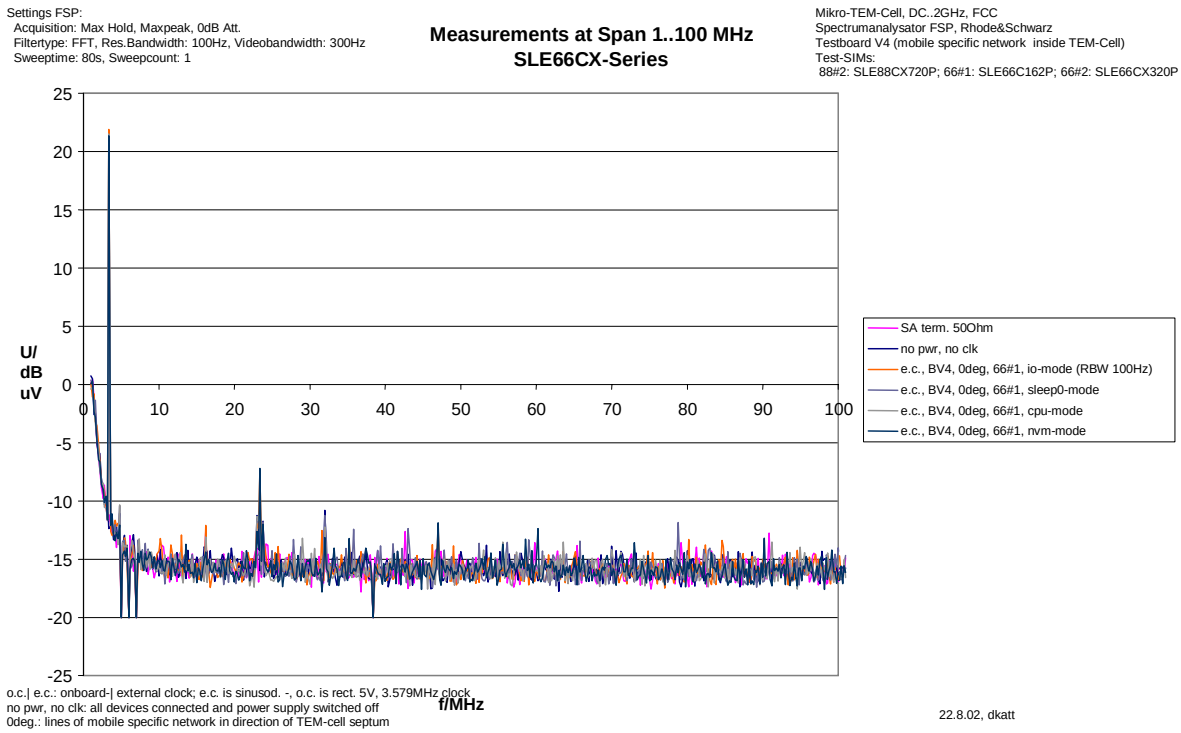


Figure A.22: All modes (SLE 66 C 162 P)

A.7.2 SLE 66 CX 320 P

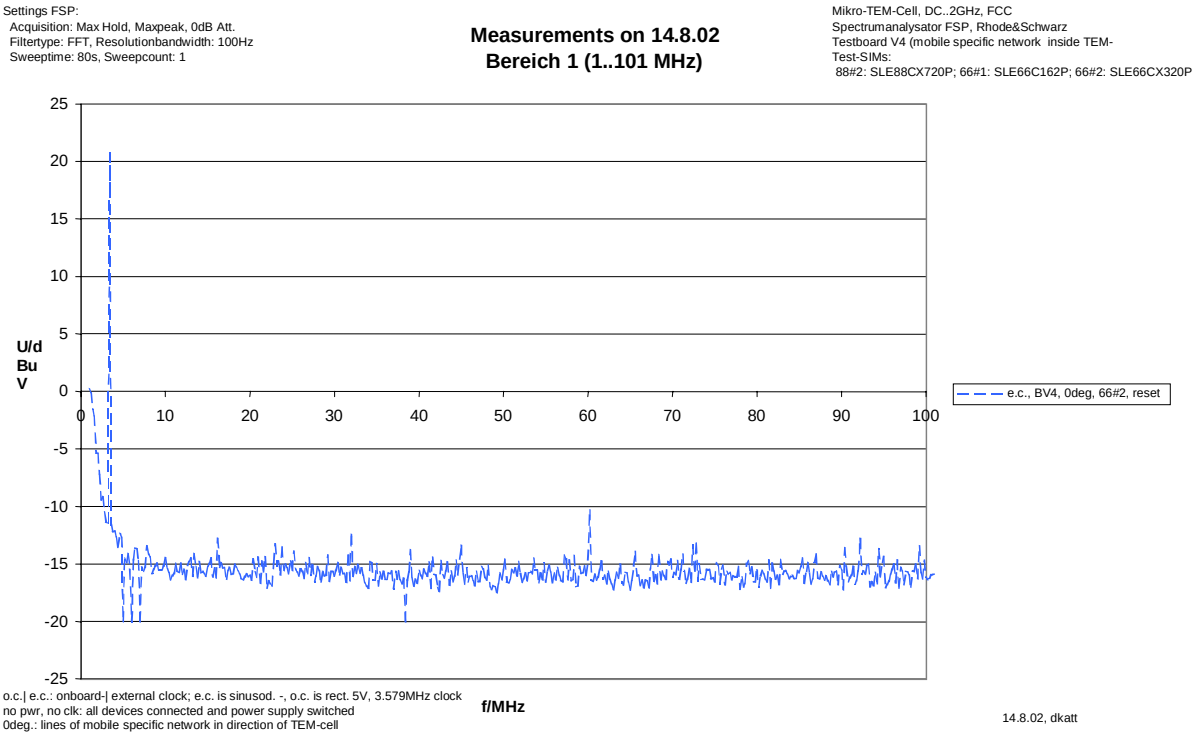


Figure A.23: Reference, sleep mode (no PLL running, SLE 66 CX 320 P)

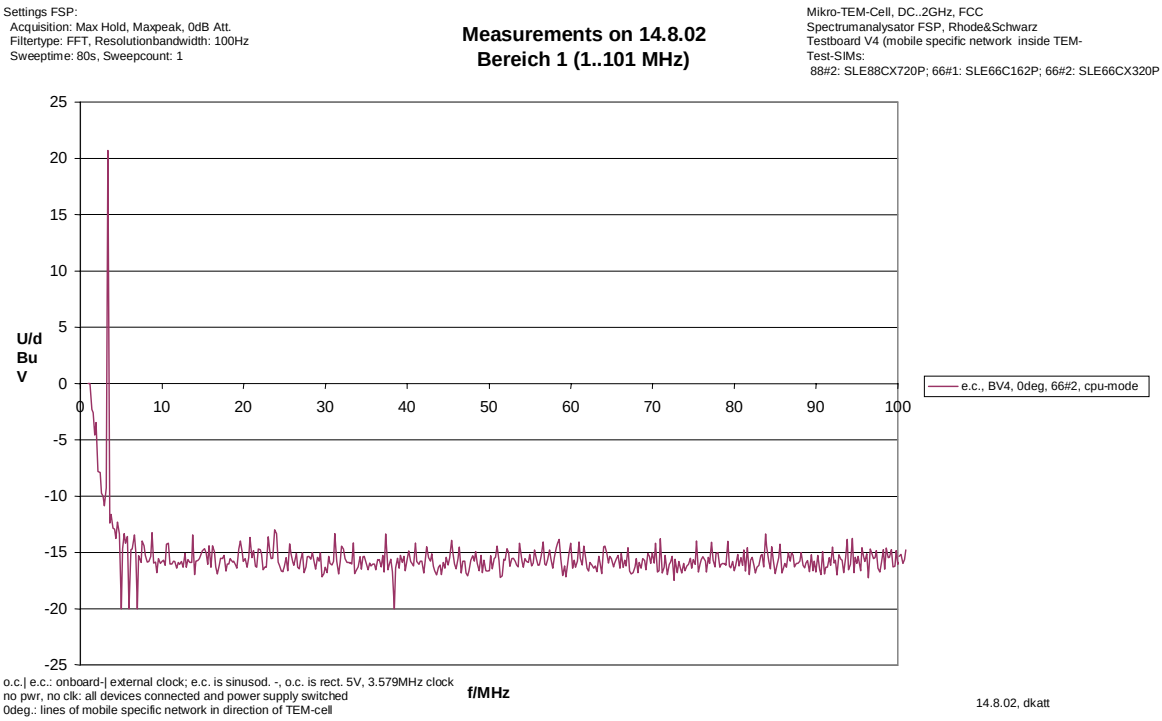


Figure A.24: CPU mode (SLE 66 CX 320 P)

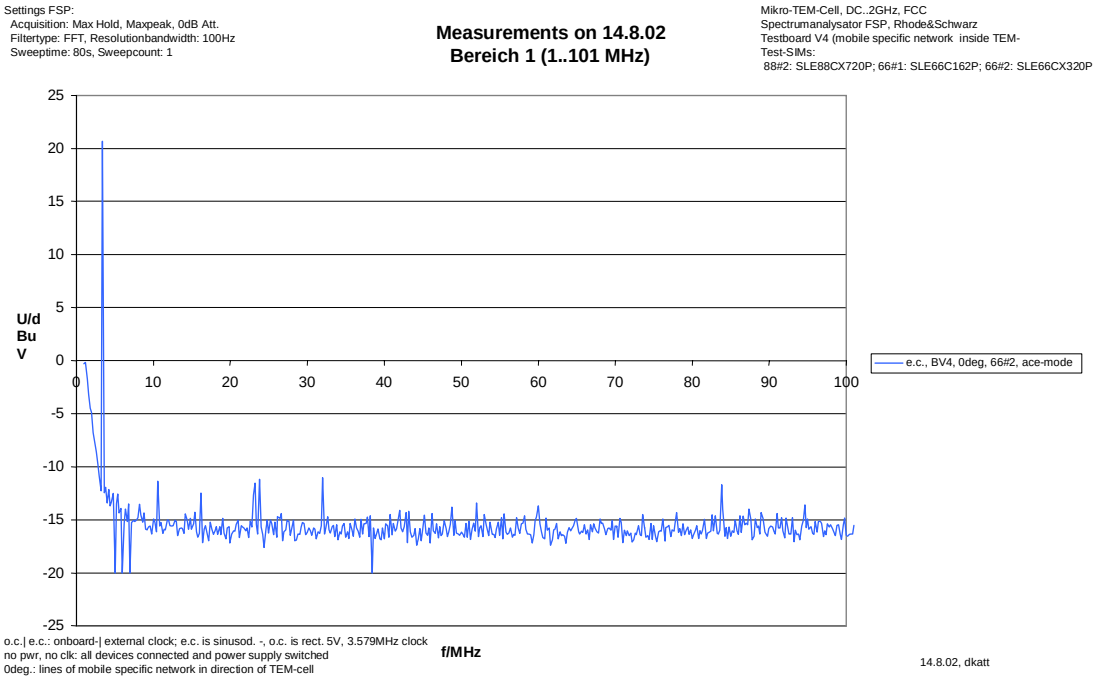


Figure A.25: ACE mode (SLE 66 CX 320 P)

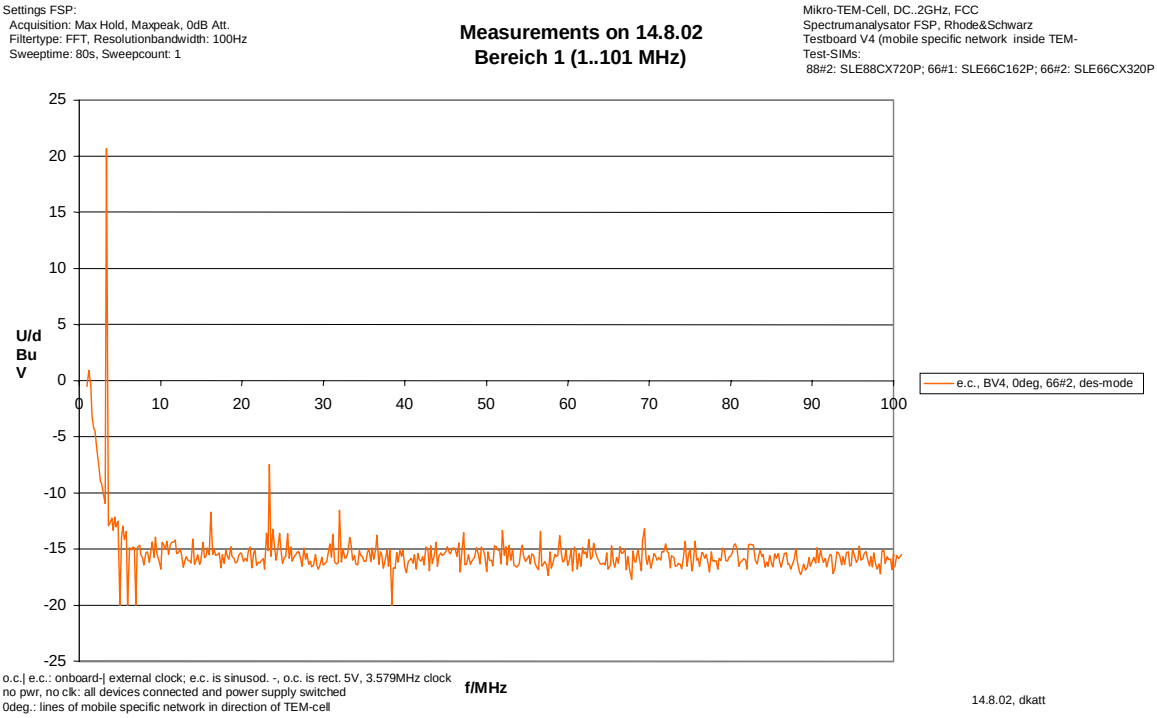


Figure A.26: DES mode (SLE 66 CX 320 P)

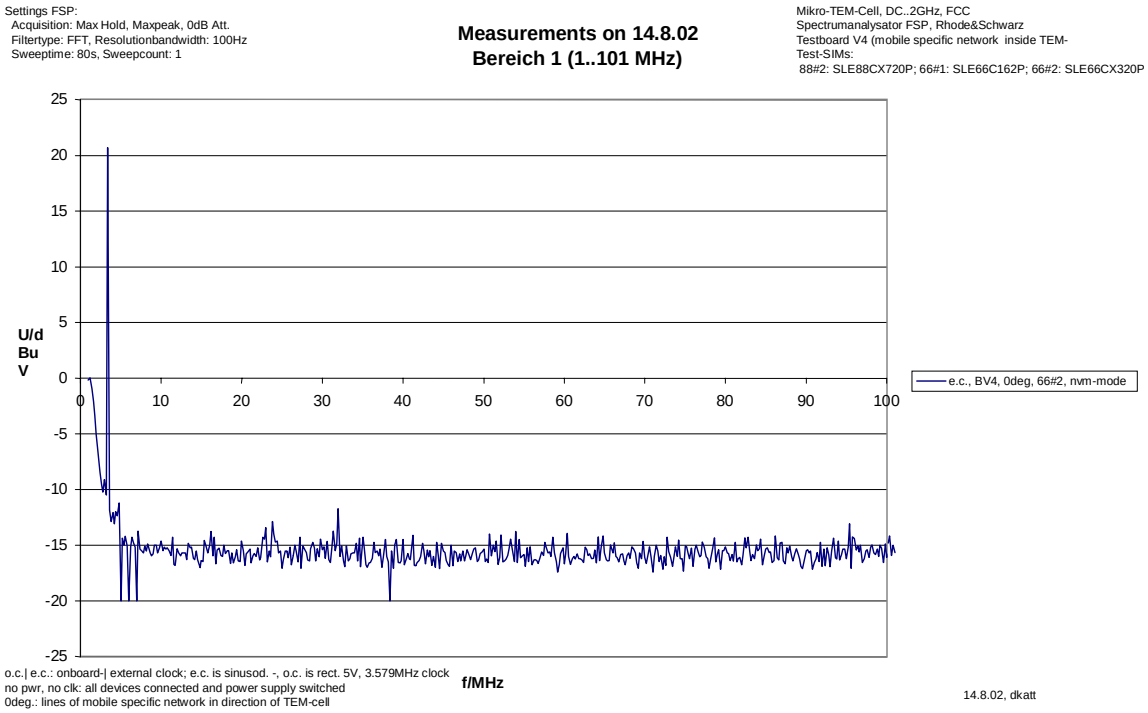


Figure A.27: NVM mode (SLE 66 CX 320 P)

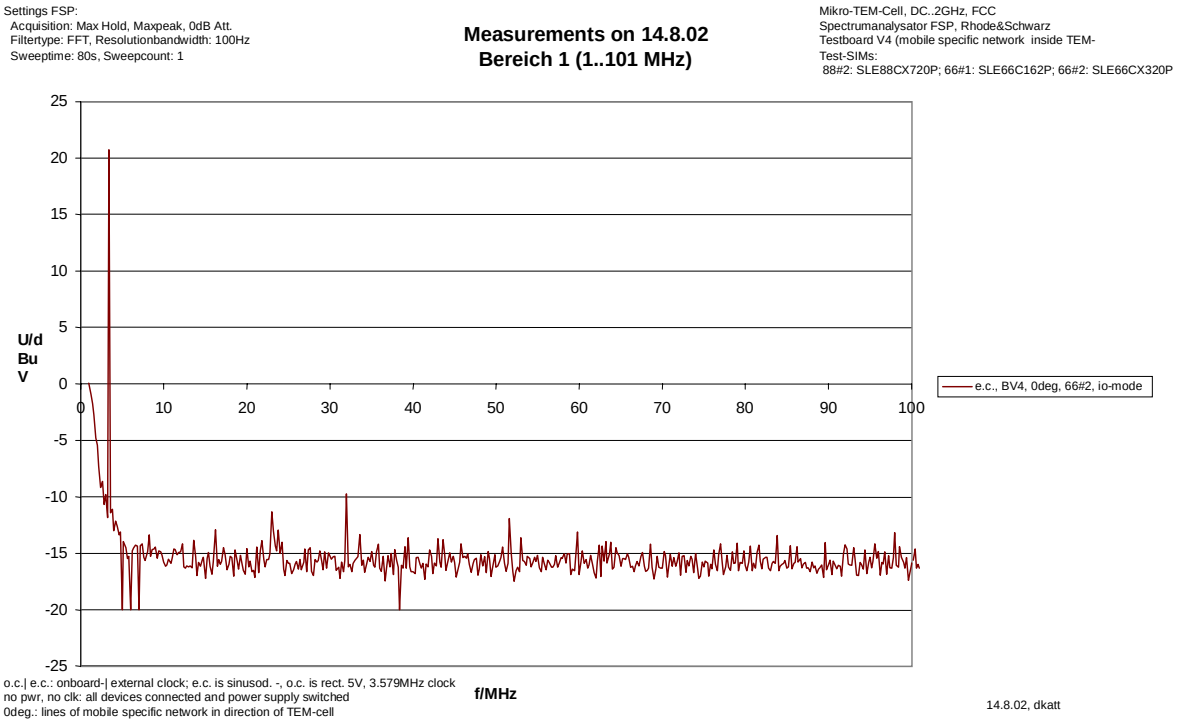


Figure A.28: I/O mode (SLE 66 CX 320 P)

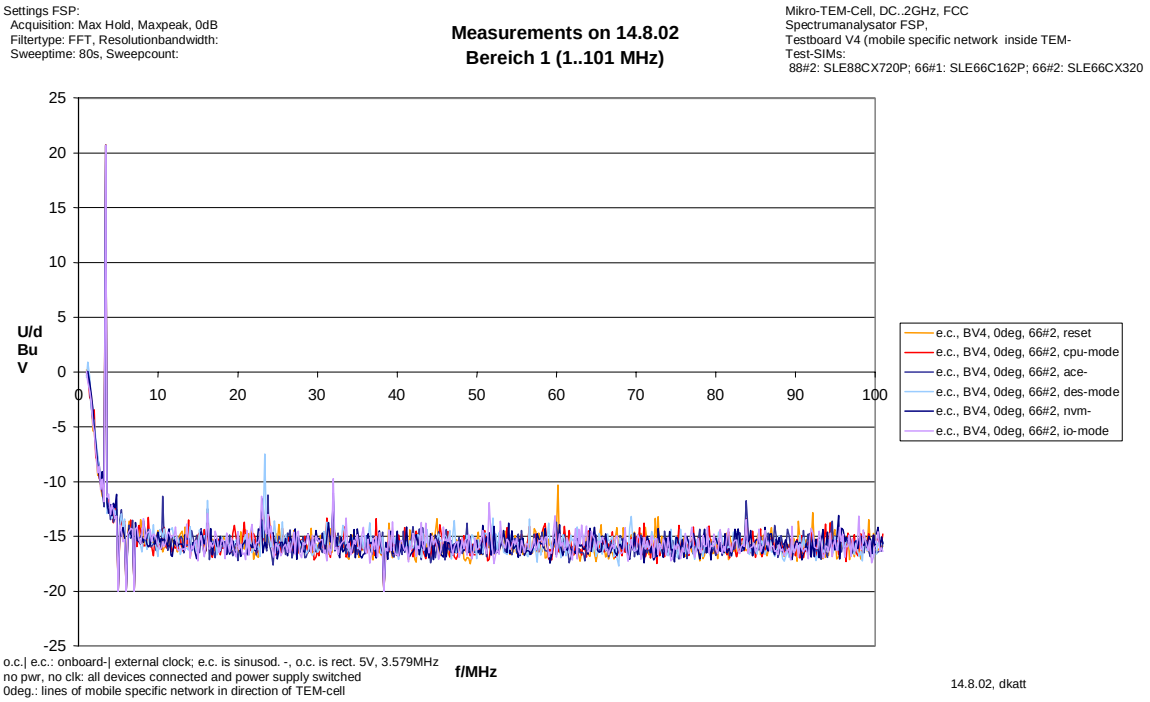


Figure A.29: All modes (SLE 66 CX 320 P)

The "SLE 66 P" family exhibited less radiation in the range from 1 MHz to 100 MHz than the "SLE 88" family. This is reasonable because of the specific chip characteristics.

Feature / Family	SLE 66 P	SLE 88 P
Clock	Multiple clocks	Single phase clock
Max. frequency	12 MHz	27 MHz
Power consumption	Max. 10 mA	Max. 30 mA

Conclusion: An influence is expected due to different smart card hardware.

A.8 Radiation in Bands 2 and 3

A.8.1 Band 2

SA terminated with 50 Ω or with the power supply switched off, no clock, RBW = 10 kHz, 100 Hz, 30 Hz

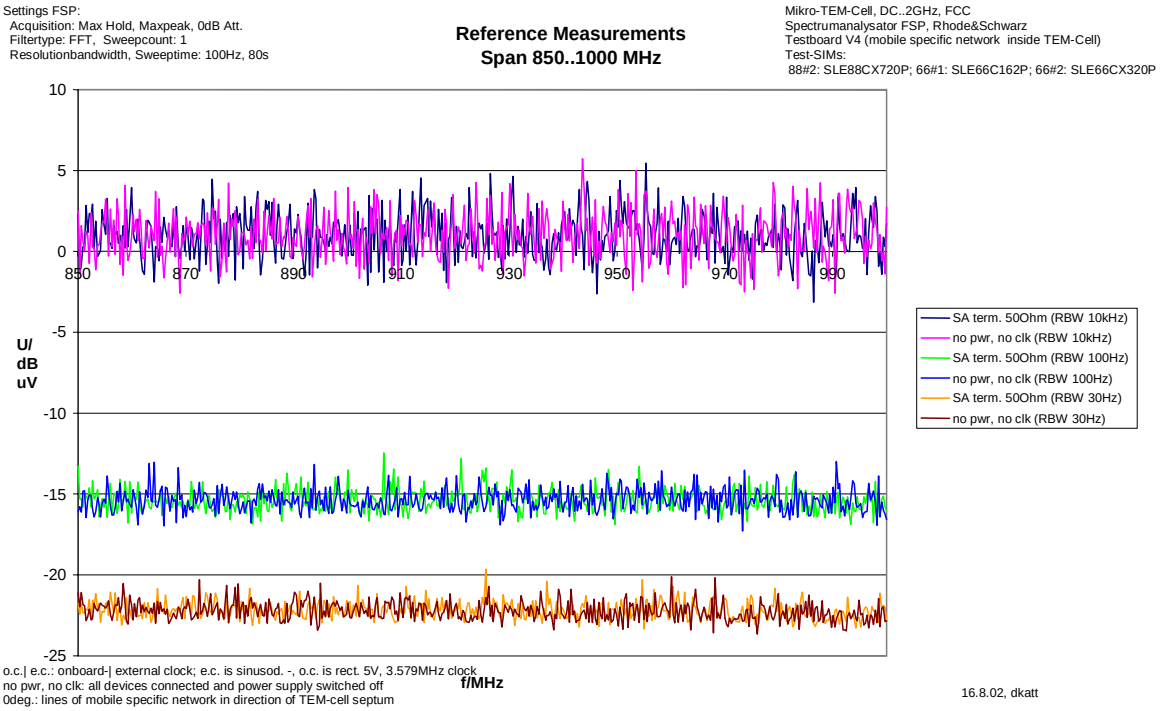


Figure A.30: Reference measurements 850 MHz to 1000 MHz

Narrowing the RBW lowers the NL (10 kHz → 0 dBµV, 100Hz → -15 dBµV, 30 Hz → -22 dBµV).

There is no major difference between the best measurement (SA terminated with 50 Ω) and the no-power measurement.

Conclusion: Setup is appropriate for measurement.

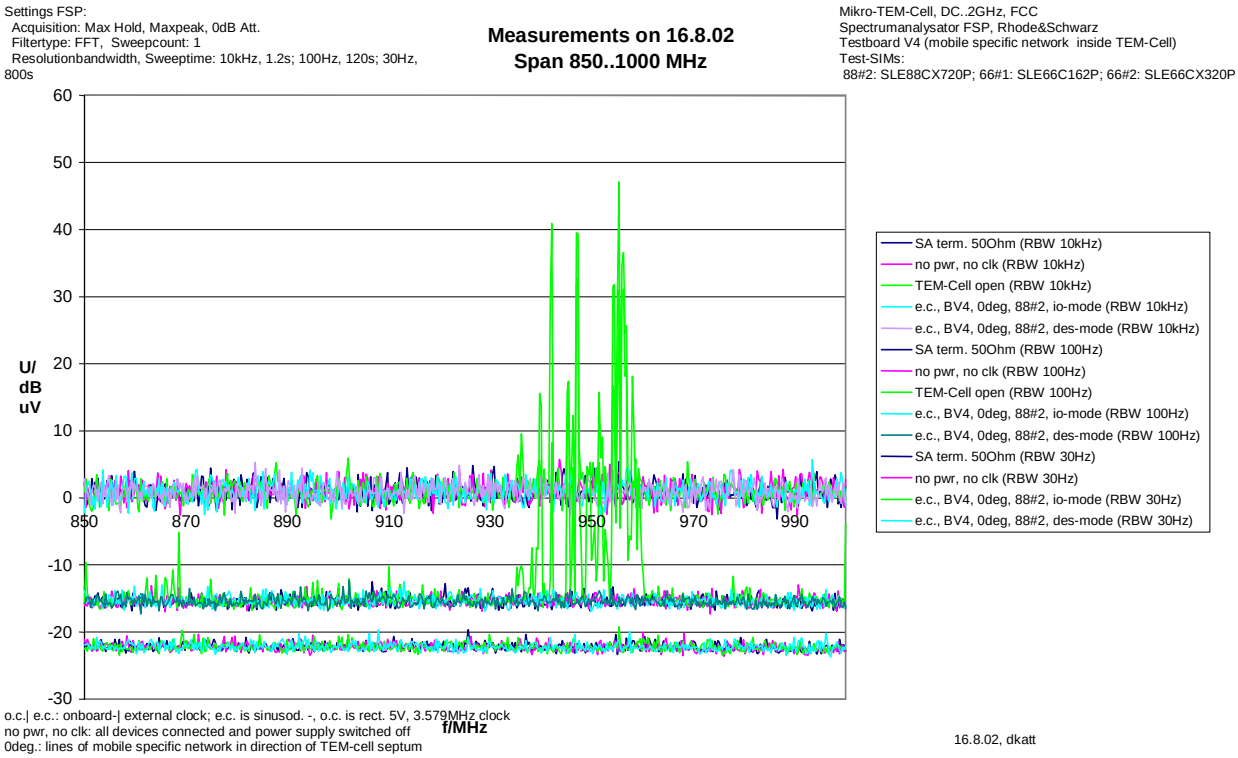


Figure A.31: Open TEM cell

With TC open there is the radiation from the base bands visible. At 100 Hz RBW the signal to NL is about 65 dB.

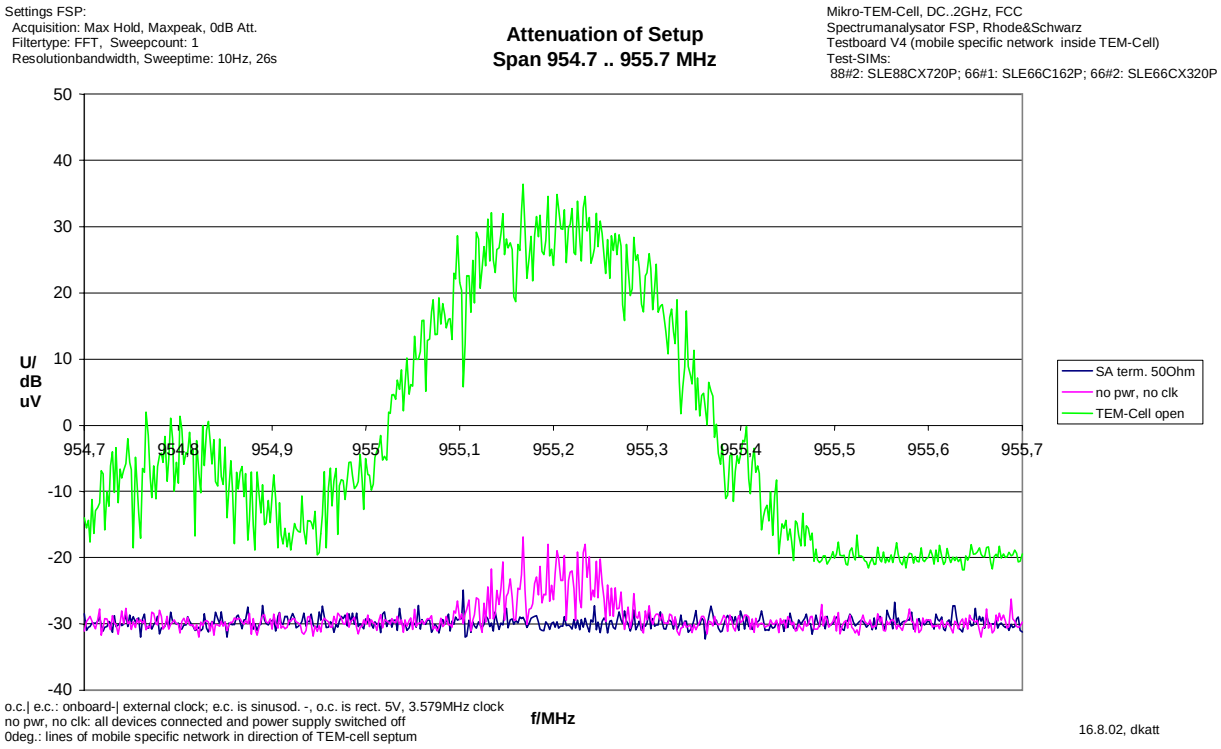


Figure A.32: SNR in the dedicated band in detail

At the centre frequency of 955.2 MHz there is an SNR of 50 dB.

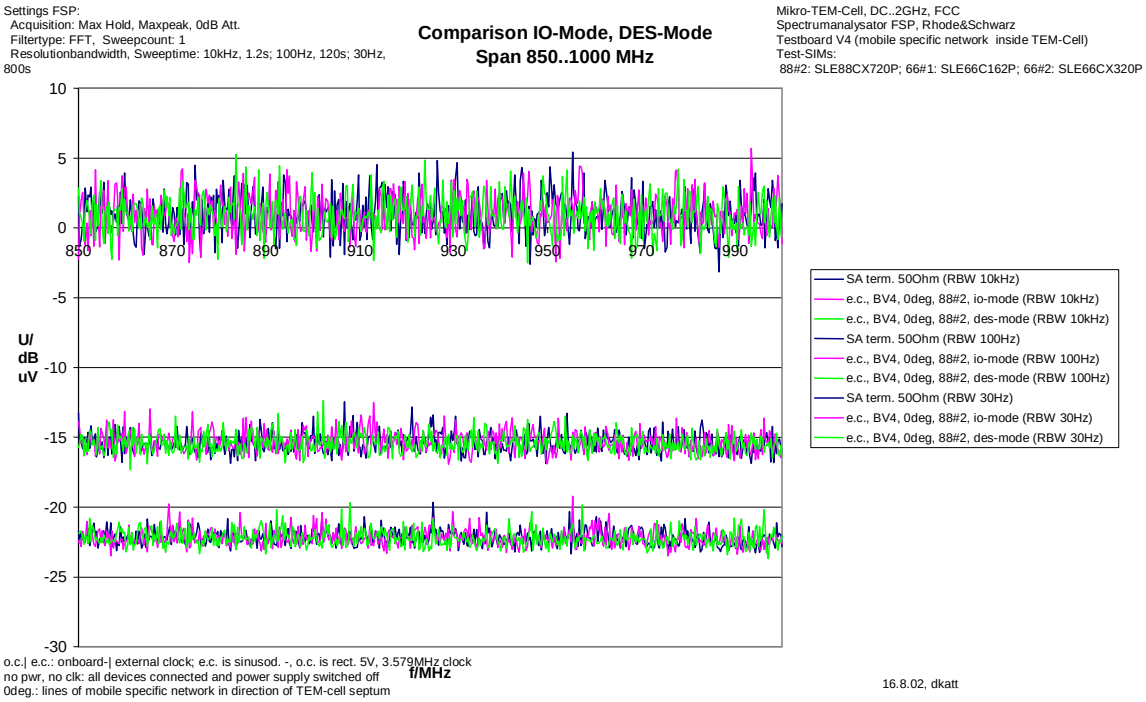


Figure A.33: DES versus I/O mode

There is no visible difference between the DES and I/O modes, neither at 10 kHz RBW nor down to 30 Hz RBW. The I/O mode is therefore used as the worst case programming mode.

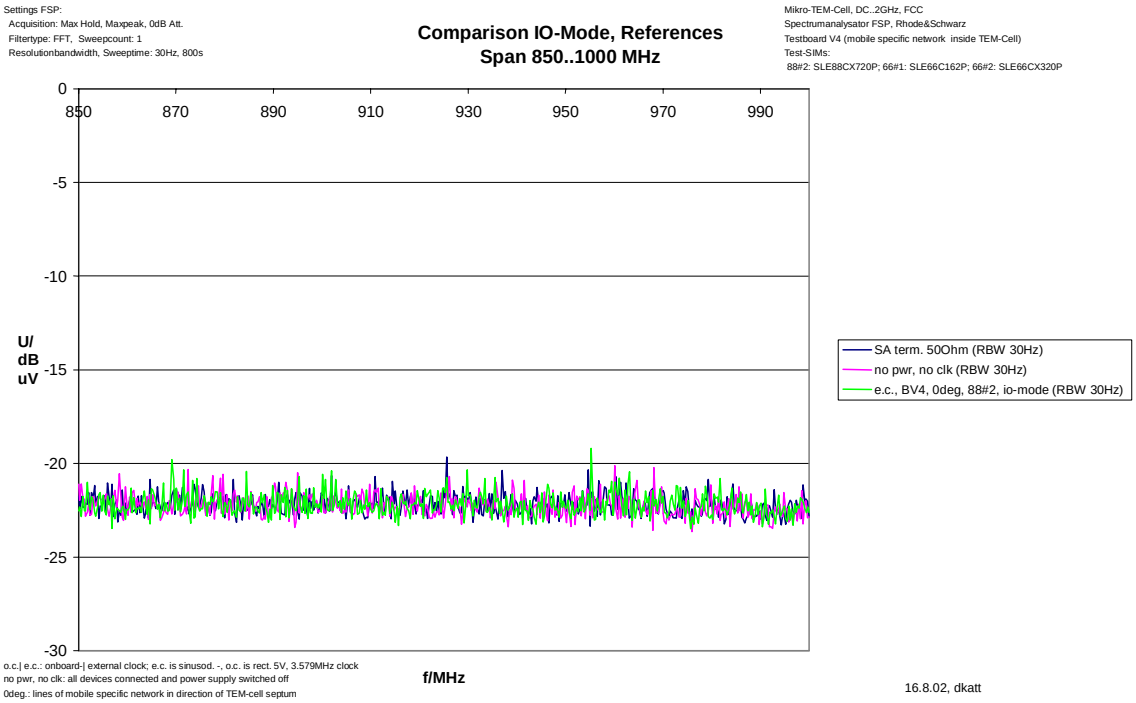


Figure A.34: Reference versus I/O mode

Conclusion: With this RBW (10 kHz, 100 Hz, 30 Hz) no radiation can be detected within band 2.

A.8.2 Band 3

SA terminated with 50 Ω or power supply switched off.

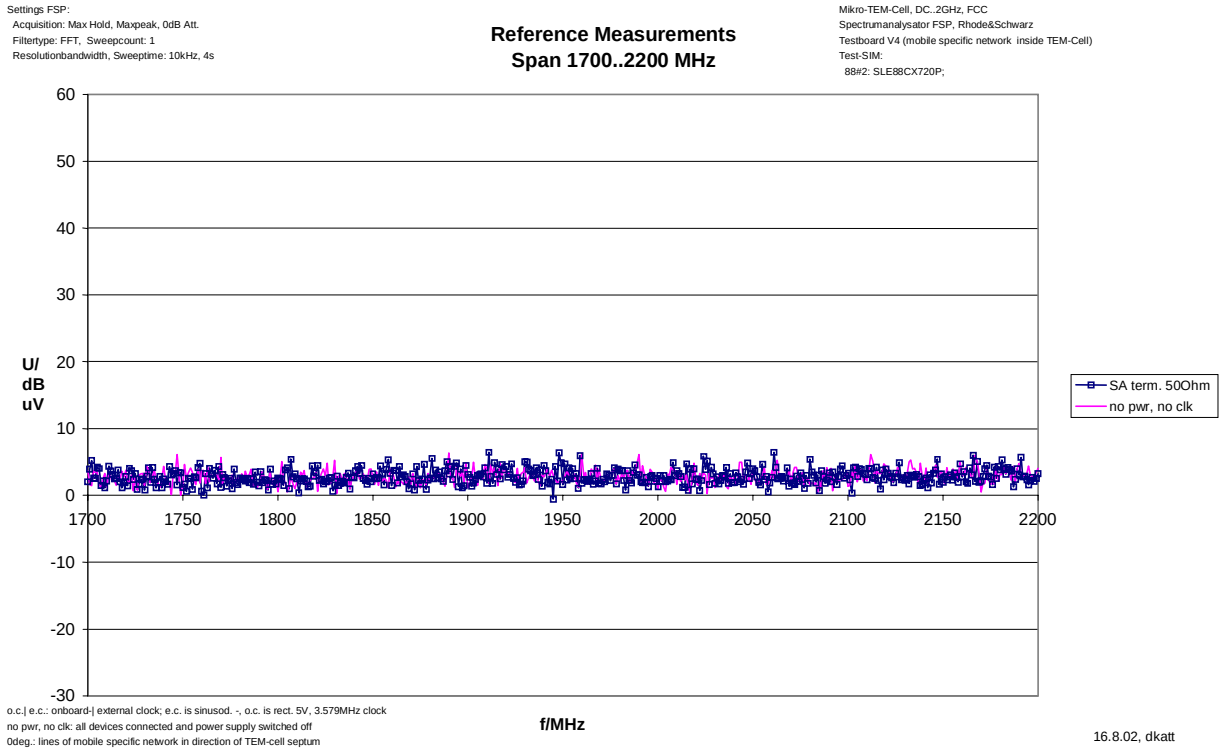


Figure A.35: Reference measurements for 1 700 MHz to 2 200 MHz

NL at 10kHz RBW is around 3dBuV. There is no difference between the best reference (**SA** terminated with 50 Ω) and setup reference (power supply and clock switched off).

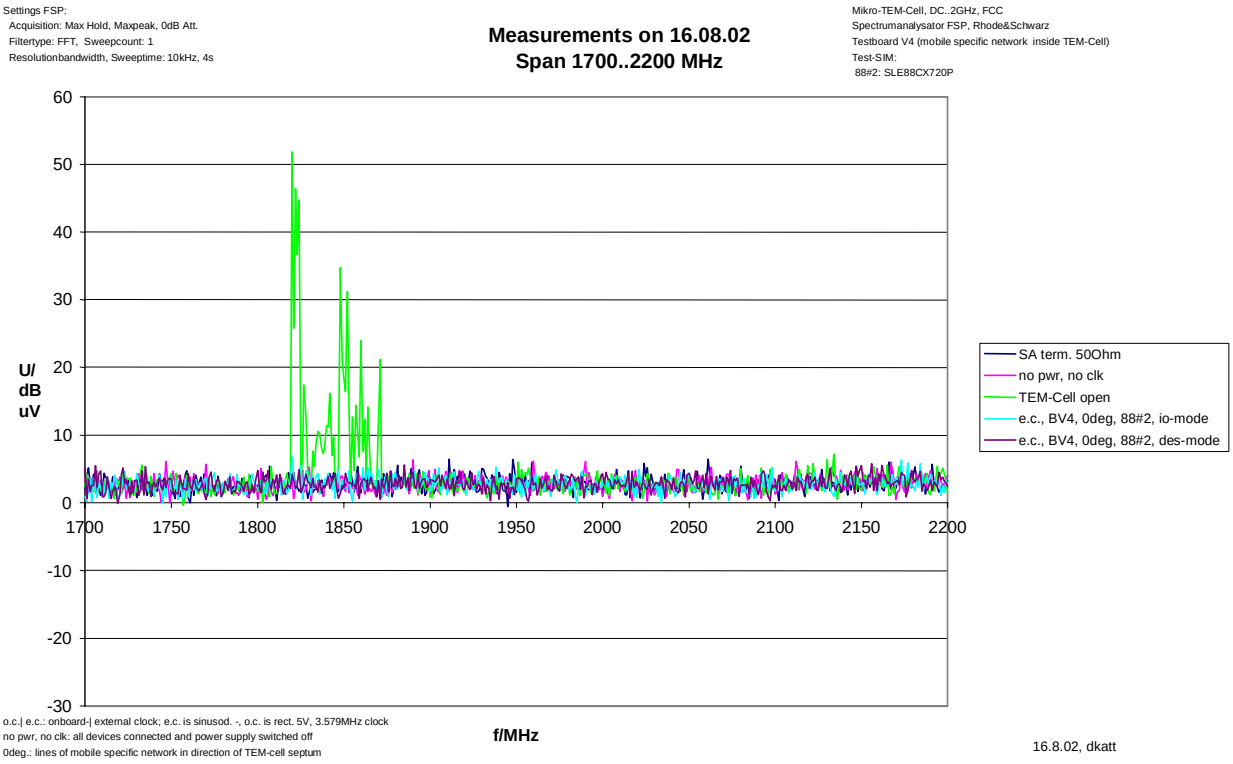


Figure A.36: Comparison of Worst Case Programs

Conclusion: For an RBW of 10 kHz no program-specific spectrum can be detected within band 3. SNR is around 50dB.

A.9 Influence of the Mobile-specific Network

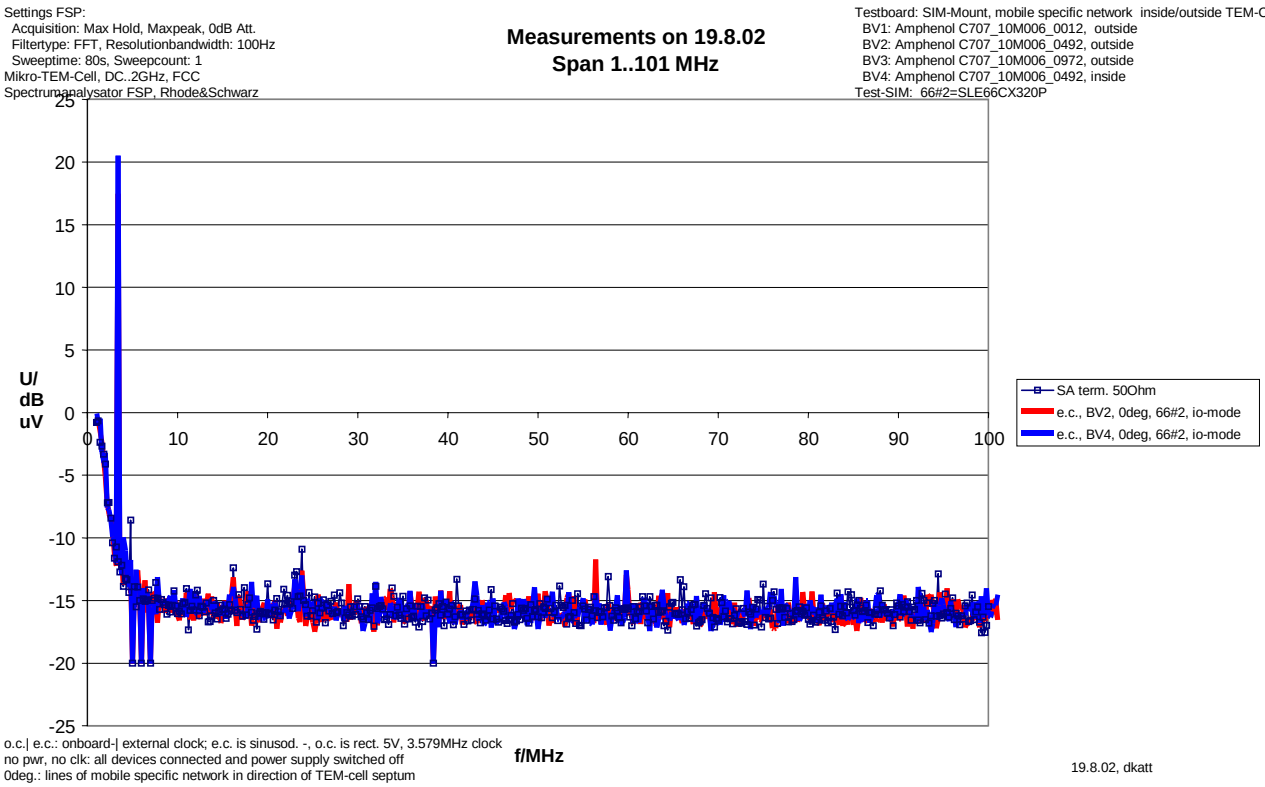


Figure A.37: 1 MHz to 100 MHz, mobile-specific network inside and outside the TEM cell

Conclusion: There are no major differences between the mobile-specific network measurements inside and outside the TC.

A.10 Influence of Readers

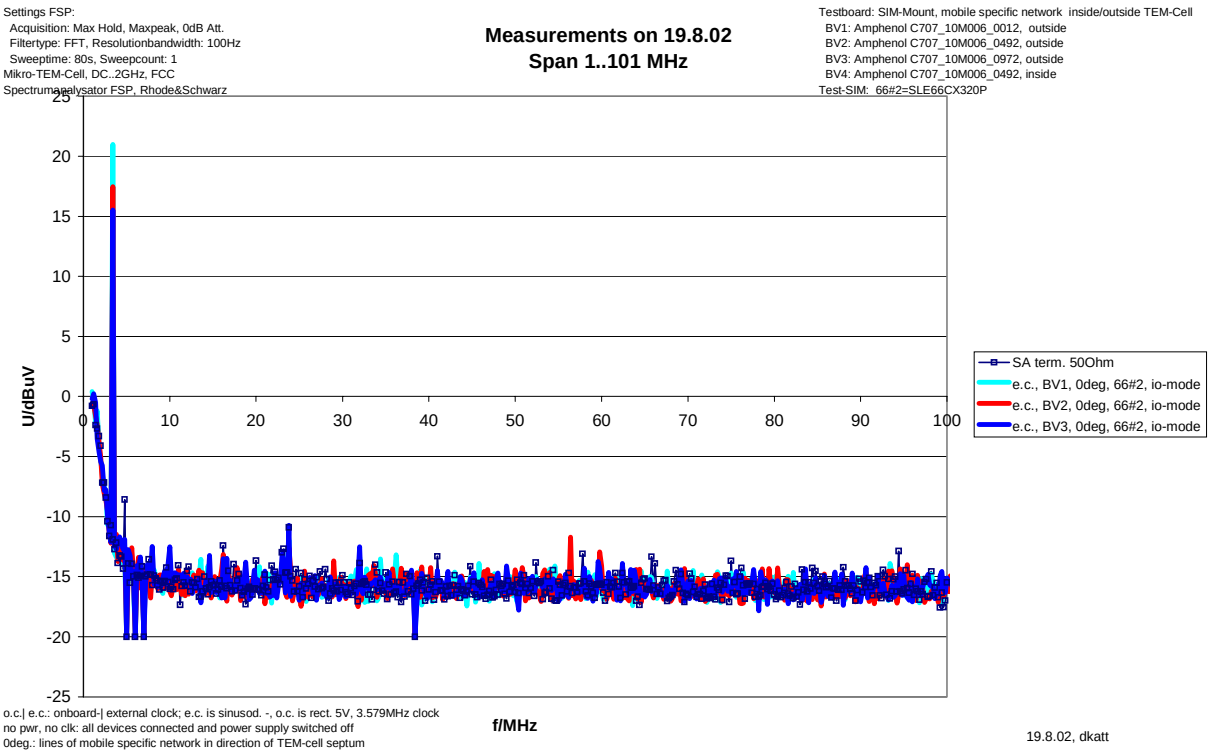


Figure A.38: 1 MHz to 100 MHz, RBW = 100 kHz, reader R#1, R#2, R#3

Conclusion: There are no major differences between the different reader types aside from 5 dBµV between R#1 and R#3 at the 1st harmonic. With a rectangular clock the differences would be more significant.

Annex B:
Change history

The table below indicates all changes that have been incorporated into the present document since it was created by EP SCP.

Change history								
Date	**Meeting**	**EP SCP Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
2003-02	SCP-12	SCP-030013	-		-	Final draft approved for publication		6.0.0

History

Document history		
V6.0.0	February 2003	Publication