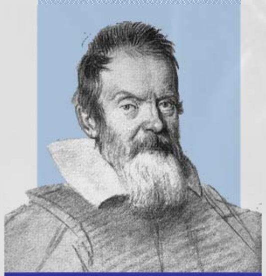
2014 Wireless Innovation Forum European Conference
Rome, 4/6 November 2014

Workshop 1B: Spectrum Sharing and Spectrum Management

November 4th, 2014

Low Cost GSM/GSM-R Interference Detector and PLMNs discovery using Software Defined Radio Technologies



Authors

Ottavio M. Picchi

Marco Della Maggiora

Irene Menicagli

Marco Luise

Outline

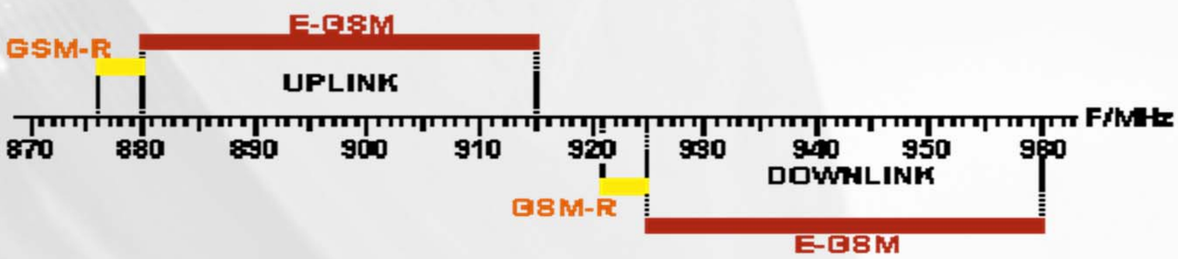
- **Motivations**
- **Proposed solution and target application scenario**
- **Public Land Mobile Network Discovery**
  - *Architecture*
  - *Performance*
- **Interference Detection Algorithm**
  - *Key ideas*
  - *Performance*
  - *Real-time capability*
- **Conclusions and future steps**

Motivations (1/3)

European/Worldwide situation [1]:

• The problem of interference over GSM-R spectrum has become a very sensitive theme since high speed train information is conveyed over GSM-R radio signals. For this reason, the European Union has highlighted the need for some regulations, which foresee an efficient interference detection system as well as a reliable mitigation mechanism.

[1] ECC Report 162, "Practical mechanism to improve the compatibility between GSM-R and public mobile networks and guidance on practical coordination," May 2011.

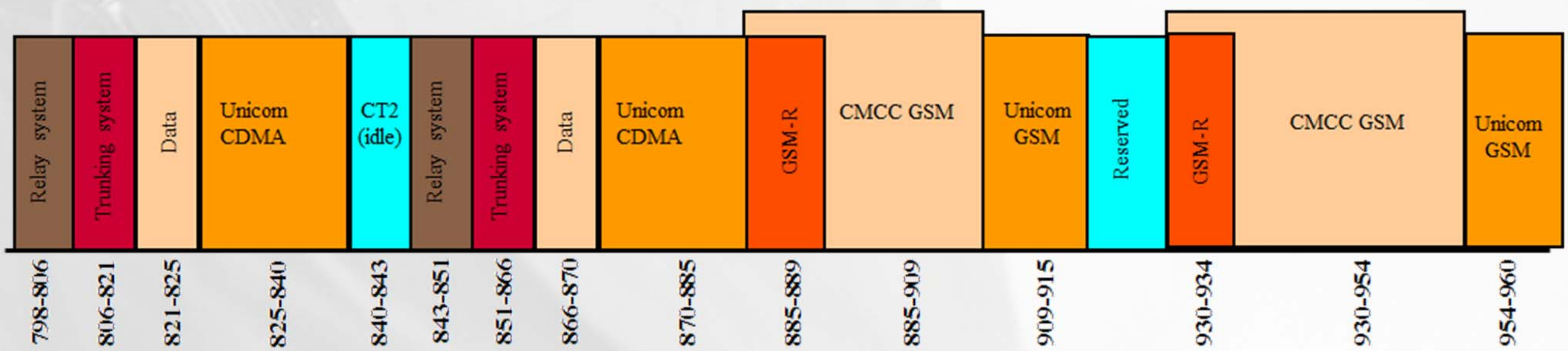


Motivations (2/3)

Chinese specific issue [2]:

• Chinese railways provider does not have the exclusive use of a dedicated spectrum sub-portion (unlike Europe). In fact, the 885÷889/930÷934 MHz EGSM radio resource can be used by both public GSM operators and GSM-R systems depending on different geographic areas. This has led to severe interference conditions and transmission collisions.

[2] L. Zhao, X. Chen, J. Ding, "Interference clearance process of GSM-R network in China," Proc. International Conference on Mechanical and Electronics Engineering (ICMEE), Kyoto, Aug. 2010.



Motivations (3/3)

From IEEE Spectrum, Sept. 2014

- **"In 2012 European Union began funding three projects to deal with assessing EM attacks and protecting critical infrastructure. [...] One project, known as SECRET, is meant to find ways to prevent the jamming of railroad equipment that uses the new GSM-Railway wireless communication standard."**

Proposed solution

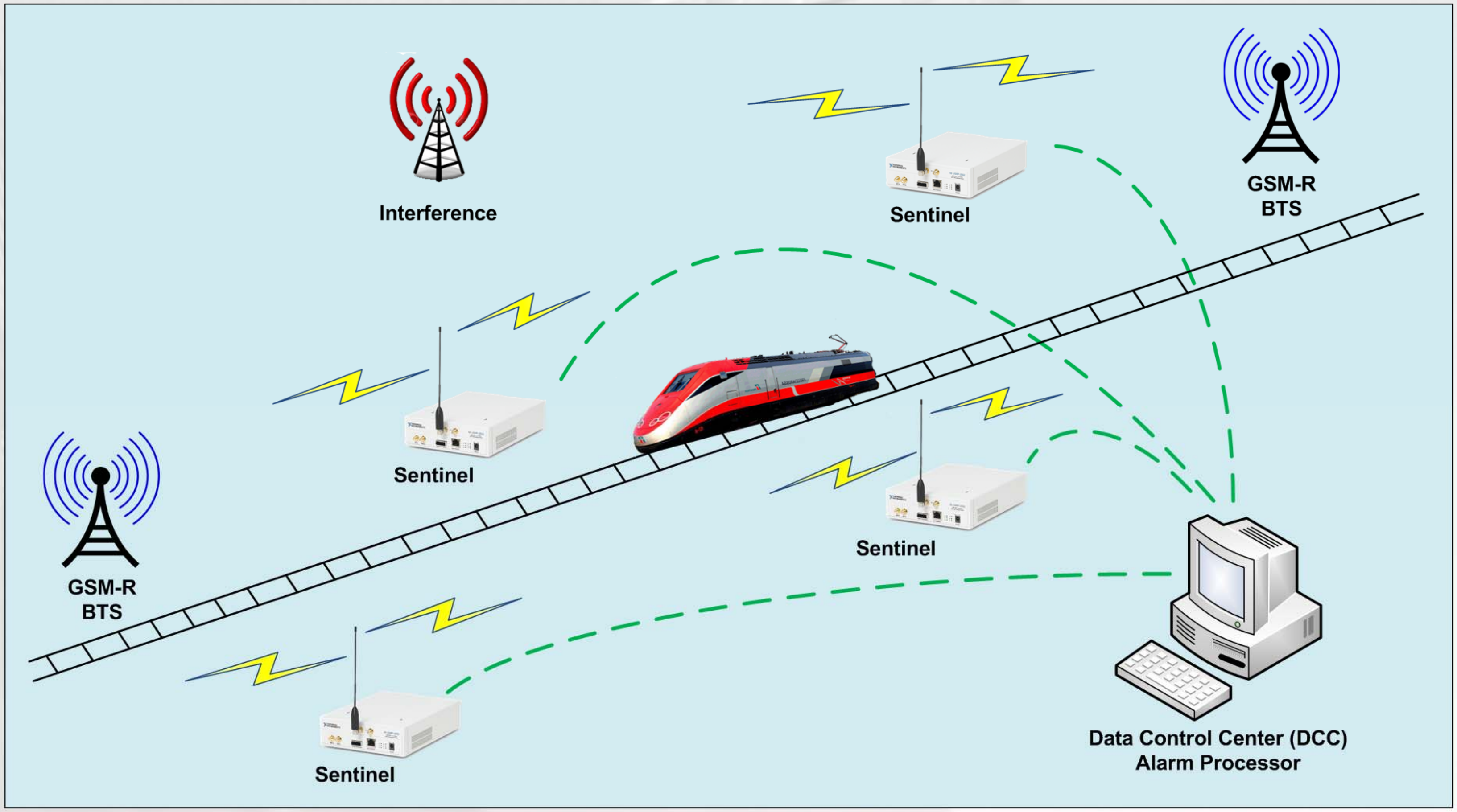
The proposed solution is a sentinel, which is able to monitor the signal integrity and read GSM geographical information, thanks to two SW suites, i.e.

- IDA: ***Interference Detection Algorithm works at PHY-layer level, checking the GSM integrity (downlink).***

- PLMND: ***this set of algorithms works as a GSM SW receiver, which reads GSM geographical information (LAI).***

These SW suites are executed on the SDR-based sentinel and are thought to work cooperatively.

Target Application Scenarios



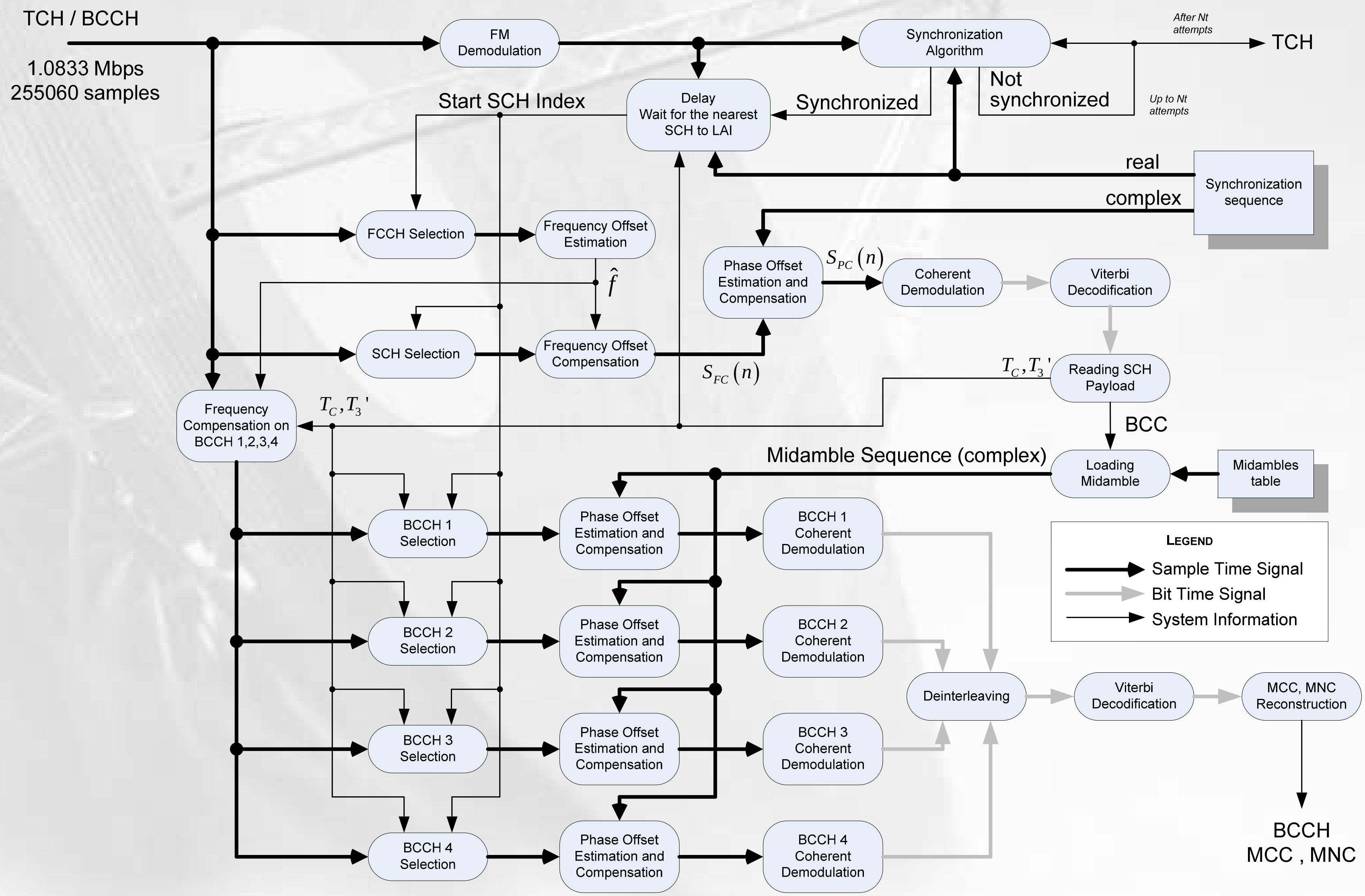
A geographically distributed set of sentinels can be used for interference sources localization.

PLMN Discovery suite

PLMND suite implements all the receiver functions, with the aim of reading LAI. These functions include:

- Channel filtering and decimation functions
- Synchronization algorithm
- Carrier offset recovery and compensation
- Phase offset estimation and compensation
- Coherent Demodulation
- FEC decoder
- MCC and MNC reconstruction

PLMND architecture



PLMND performance

PLMND performance is given in terms of LAI (MCC and MNC) read error rate. Each test starts when the synchronization algorithm succeeds.

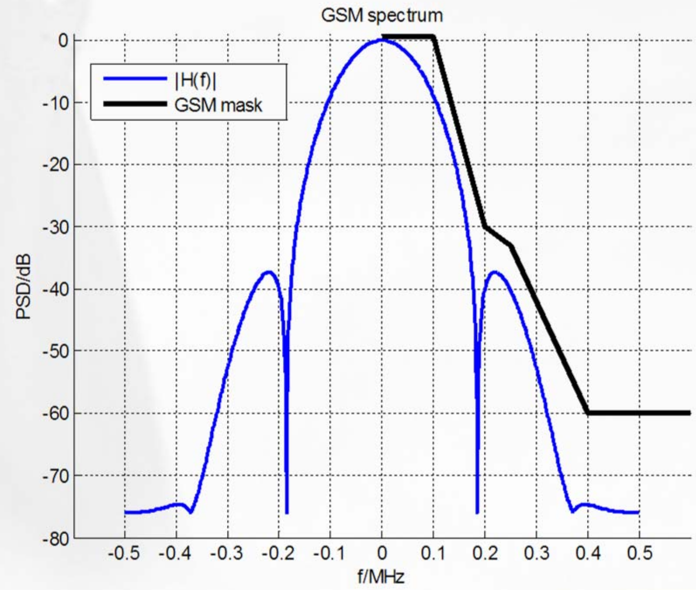
Location	n. Trials	n. Error	Error rate
A	4983	158	0.032128514
B	3571	97	0.027170868
C	722	19	0.026388889
D	8557	302	0.035280374
Summary	**17827**	**576**	**0.032417274**

Each test has been performed as a one-shot read. However, for the working condition of the sentinel it is not crucial to have these values in one shot, but the LAI read may be repeated (if wrong). Hence the error rate might be drastically decreased.

Interference Detection Algorithm suite

The key idea for recognizing BCCH/TCH channels is to check if the signal under analysis meets GSM TDMA constraints.

The GSM tail analysis algorithm checks if potential GSM tail channels are actually tails by checking if their power obeys emission mask. In case the emission mask constraint is fulfilled, the algorithm labels this signal as GSM tails. Otherwise, this signal is identified as an interferer.



How to measure IDA performance?

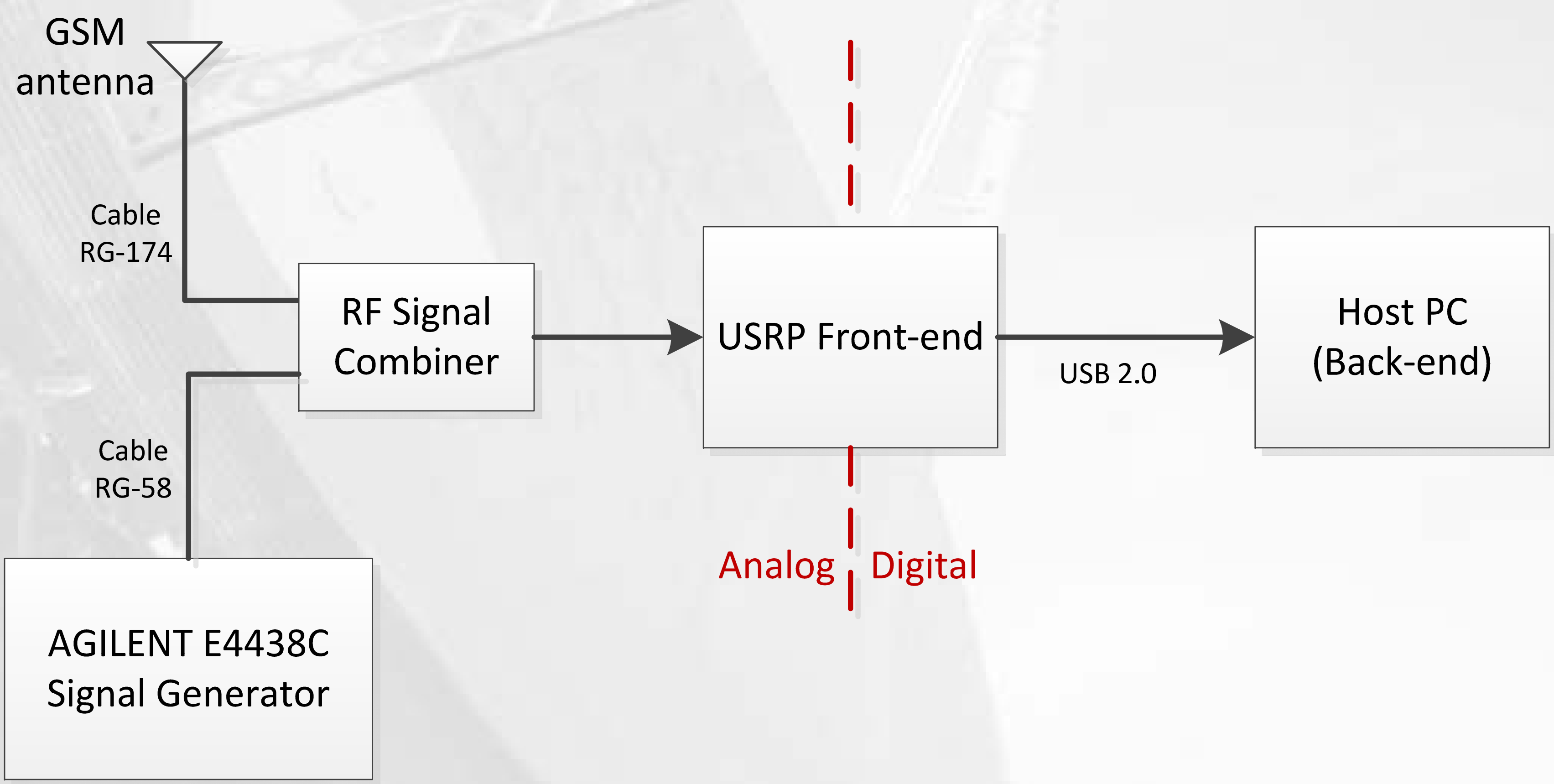
- **IDA tests have been performed on real signals, over which we injected an interference signal. Thanks to a calibration activity, we can set the Interference-to-GSM+Noise-Ratio or the Interference-to-GSM-Ratio, by modifying the interference power.**
- **These metrics are defined as:**

$$IGNR = \frac{P_{Int}}{P_{GSM} + P_n}$$

$$IGR = \frac{P_{Int}}{P_{GSM}}$$

- ***The possibility of tuning IGNR/IGR enables to get a better understanding of the sentinel performance, analysing different interference conditions.***

IDA test set-up



Intelligibility Threshold (1/2)

*Let us define an important parameter, i.e. the **GSM Intelligibility Threshold (IT)**. This parameter states **the minimum interference power, and consequently the minimum IGNR/IGR over which the GSM signal is not readable**, i.e. GSM data are corrupted by the interference signal.*

IT can be empirically measured using PLMND SW suite.

Intelligibility Threshold (2/2)

IT can be measured as follows:

1. Set a very low level interference power;

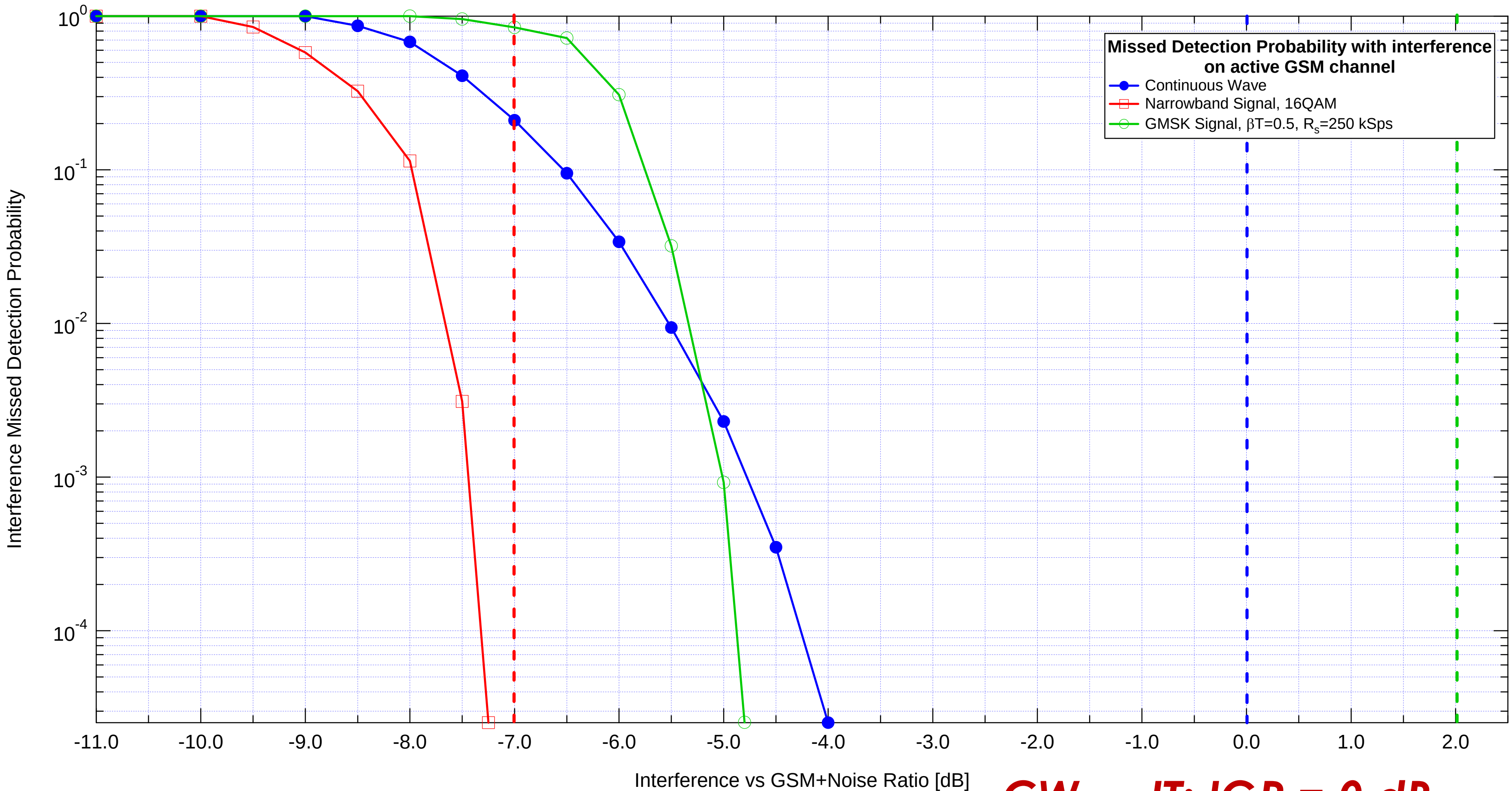
*2. Dump on a file **the composition of GSM signal + interference signal**;*

*3. Try to **read GSM data** (we use our PLMND tool);*

*4. If GSM data are readable, **increase interference power** and come back to step 2.*

*5. If **GSM data are not readable**, IT for the given interference signal has been found.*

IDA Performance

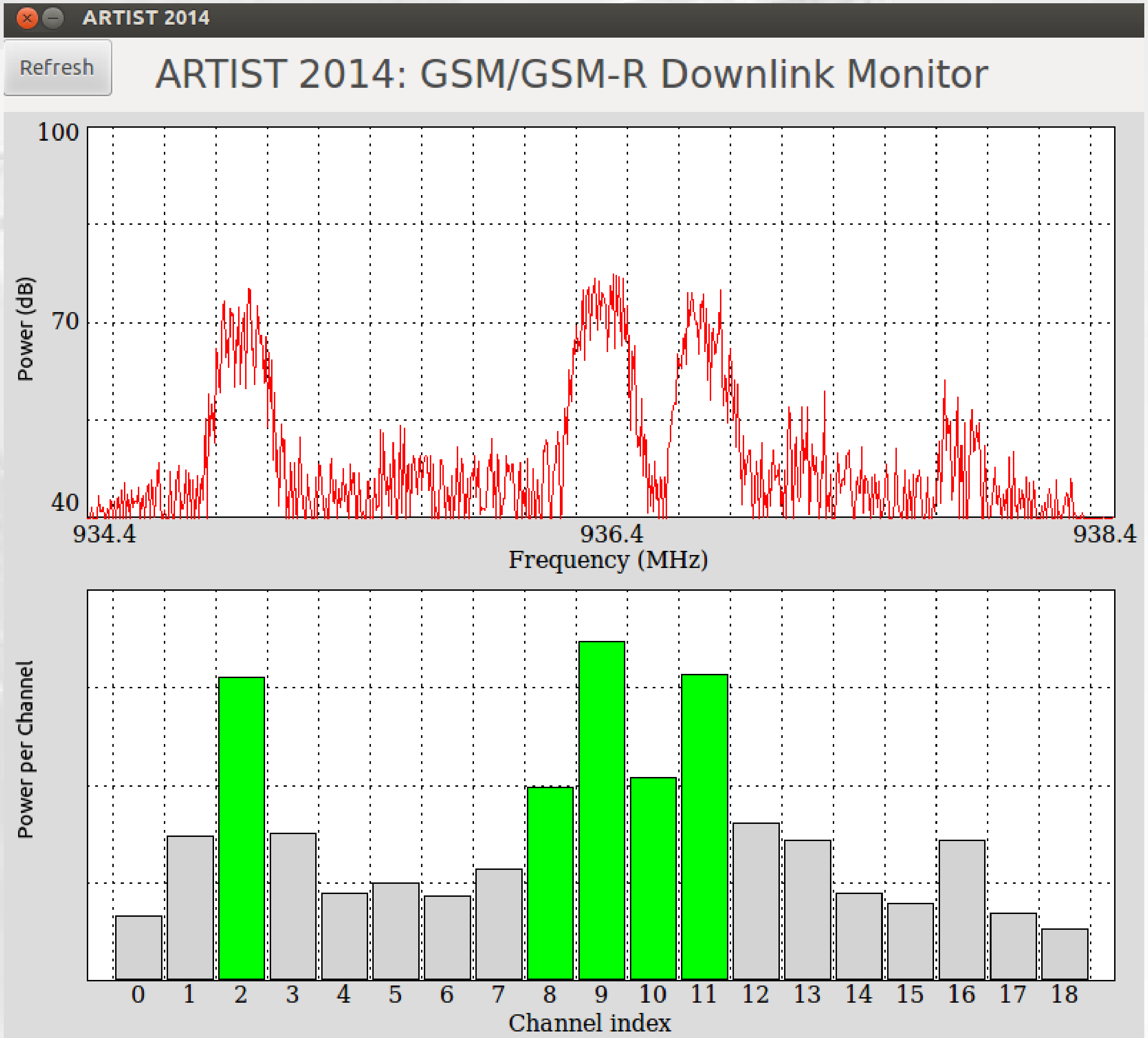


CW → IT: IGR = 0 dB

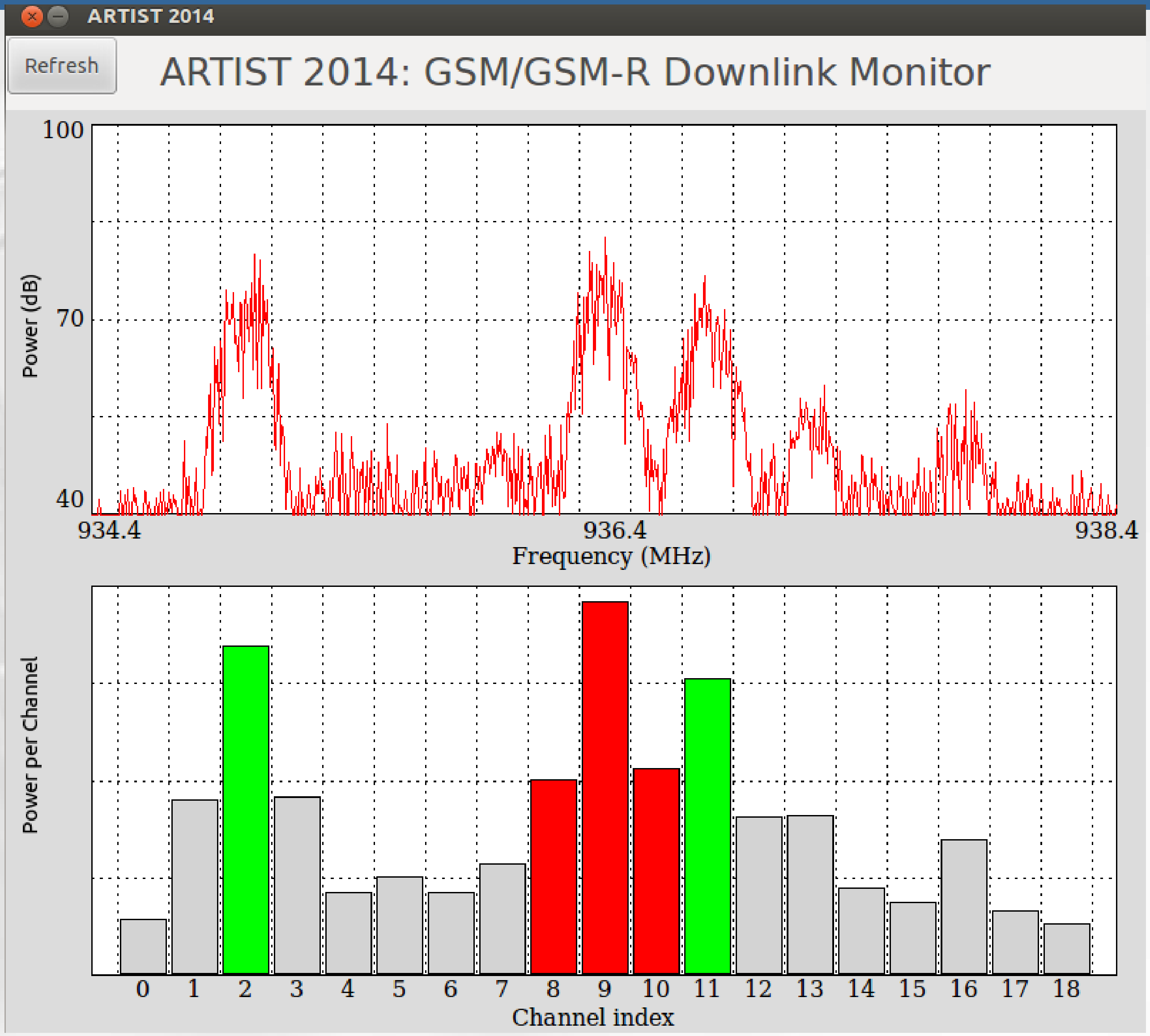
NS → IT: IGR = -7 dB

GMSK → IT: IGR = 2 dB

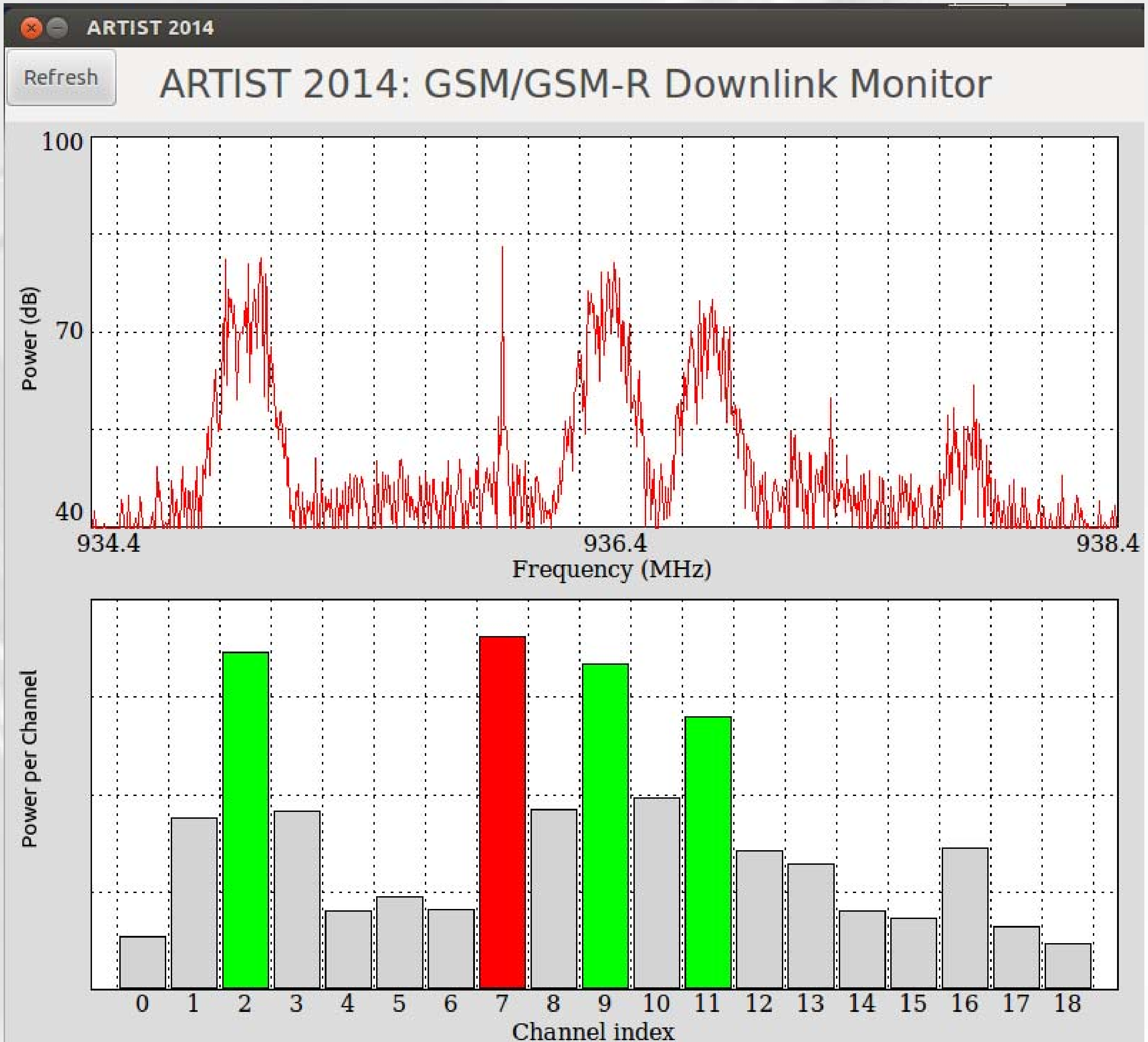
IDA real-time implementation



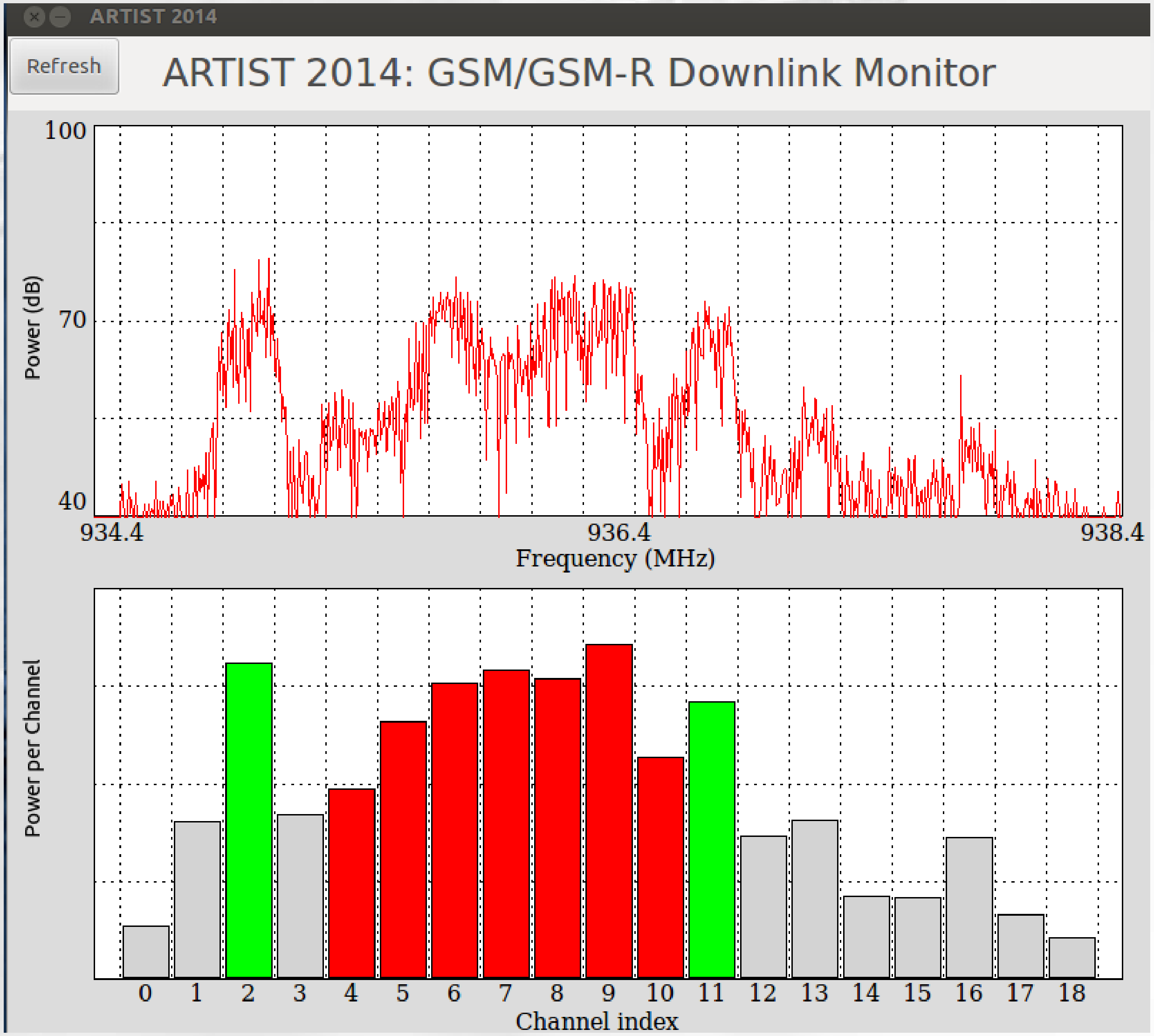
IDA interference detection capability (1/3)



IDA interference detection capability (2/3)



IDA interference detection capability (3/3)



Conclusions

We presented two suites of algorithms: one designed for GSM PLMN Discovery and another for Interference Detection.

- *PLMND suite correctly reads GSM Location Area Identification with an error rate probability < 10^{-2}.*
- *IDA suite identifies several different types of interference signals, including interference with the same modulation format as GSM.*
- *IDA detects the presence of interference, up to an IGR below the Intelligibility Threshold (depending on the interference type).*

Next Steps

Real-time implementation of PLMND set of algorithms

Real-time monitoring of the Intelligibility Threshold

Have a look at our **demo**, available at:

http://www.wiser.it/video.php

Thank you for your attention..

Any questions? ☺

ottavio.picchi@wiser.it