INFRABEL

Security aspects Impacts on networks operation and design

Alex Raviart, Head of I-ICT Networks

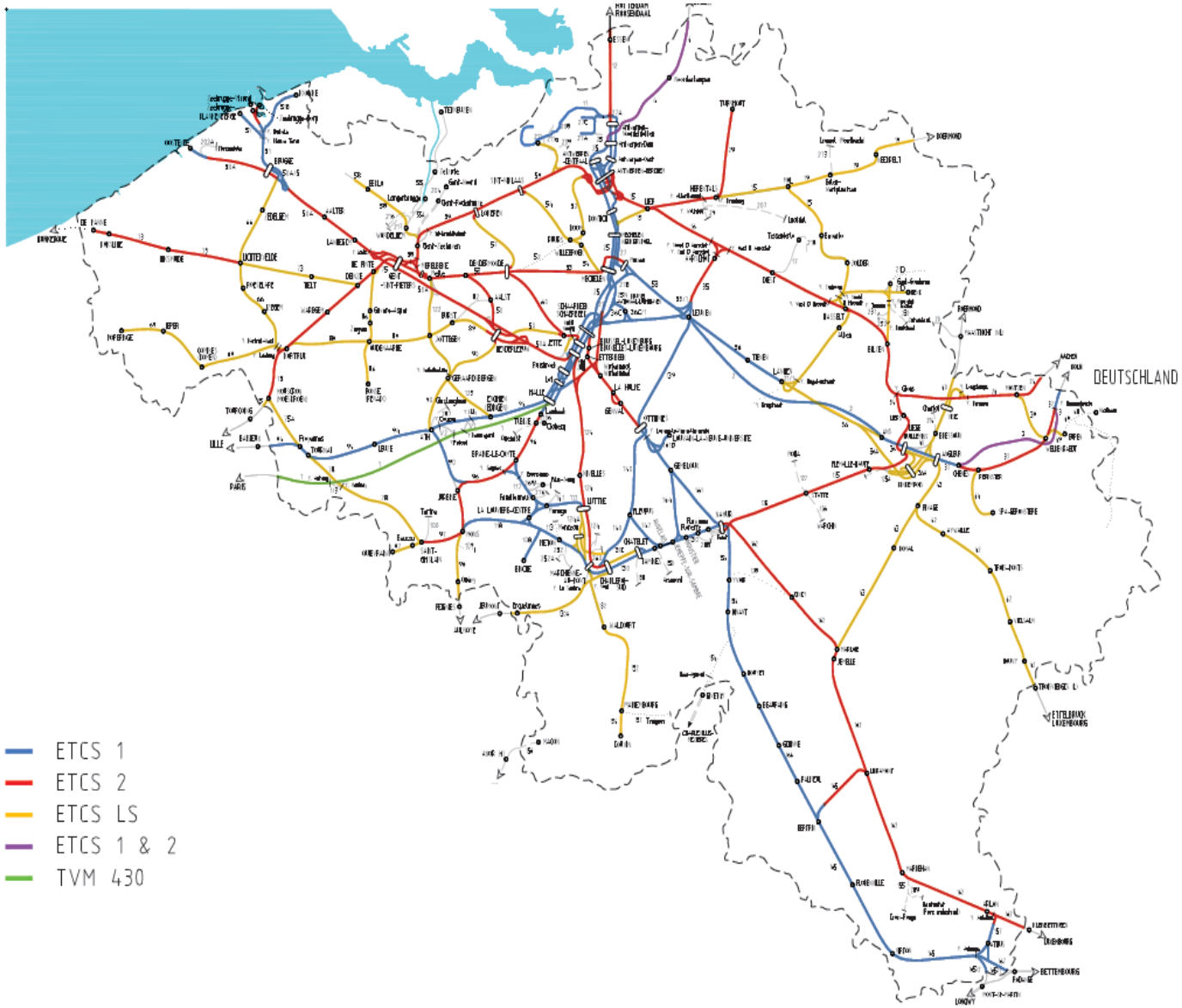
UIC – May 18th, 2017

SAFETY FIRST by Infrabel

Agenda

1. GSM-R in Belgium: context
2. 22 March 2016 : Facts and Lessons learned
3. Jamming & protection measures
4. How to protect GSM-R & business continuity ?
5. Data integration for GSM-R improved operations

GSM-R in Belgium : context



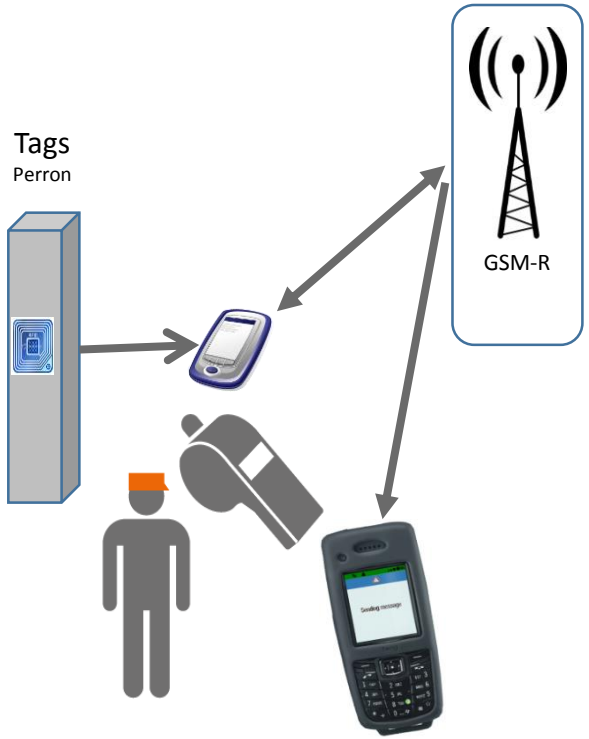
GSM-R in operation since 2009 with 2 high speed lines in ETCS 2

ETCS Masterplan, horizon 2022

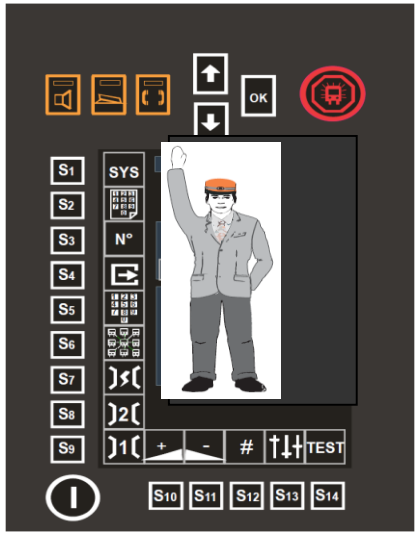
- 1/3 with level 1
- 1/3 with level 2
- 1/3 Limited Supervision

INFRABEL

GSM-R Context overview



In Belgium, the GSM-R will be part of the new procedure for departing trains.



- GSM-R has become vital for the rail-traffic continuity
- The GSM-R monitoring does not limit itself to the monitoring of equipments/systems but evolves towards services monitoring where each transaction is critical

INFRABEL

22 March 2016 : Facts

From 8h00
Air traffic
stopped

Communications
problems due to
network overload

9h30 to 17h00
Stop Rail transport in Brussel from
Stop metro lines + Stop Stations

In this high tension climate, Infrabel management had to deal with a situation with great difficulties in order to receive clear instructions from the authorities:

- It's when they had to communicate in order to take and transmit decisions that the means of communication have been defective!

- GSM is today the default mean of communication between members of management (decision takers) and the responsible authorities

INFRABEL

22 March 2016 : Facts

Communication problems

- Saturation of the GSM Networks in Brussels
- Saturation of Astrid (Tetra) Network in Brussels
- Some information sites where saturated and inaccessible
- The IP Network of Infrabel was also saturated in Brussels by worried staff (download)
- The SNCB information site was saturated (IP network)

How can the decision takers/authorities take the good decisions ?

- Should they stop the traffic ?
- How to stop the traffic ?

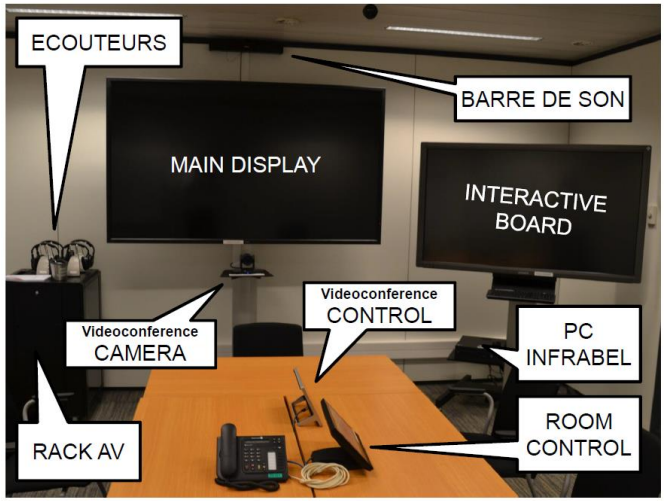
How to inform the users ?

How to transmit instructions ?

22 March 2016 : Lessons learned

- Necessity to have a “Security” crisis plan integrating a “no communications” mode and a “attack of communication means” mode
- Technical measures were taken to guarantee the continuity of information and communication means
- The crisis plan is part of a regular training during which organisational measures and technical measures are tested

  - Crisis rooms autonomous in communication means
  - Portable GSM-R with fixed connectivity
  - IP segregation (Internet, critical applications, web applications, IP surf,….)



INFRABEL

22 March 2016 : Consequences - Jamming

To reinforce the means during anti-terrorist operations, authorities extend the legal frame to use communications network jammers

Consequences :

- This new use of jammers has direct consequences on the good functioning of rail communications, and especially of GSM-R communications
- Disturbed GSM-R communications imply a disturbed rail traffic (ETCS2, train departure,…)

22 March 2016 : Consequences - Jamming

In this new context and with this new risk, we need:

1. To have clear agreements with the authorities regarding the use of jamming
2. That authorities cooperate in case of intervention or use of jamming (the infrastructure manager should be aware before)
3. To reinforce the GSM-R network, in key spots, to avoid as much as possible the possible impact on communications (new sites)
4. To upgrade the means to monitor and detect/undetect jamming

Important remark :

Detection means and classification of interferences on GSM-R should allow to discriminate real disturbances from disturbances due to the legal or illegal use of jamming

22 March 2016 : Consequences - Jamming

It is necessary to know the impact of the usage of jammers on GSM-R

SIMULATION : GENT EXPO - L50A & L75 - ETCS LEVEL 2 LINES

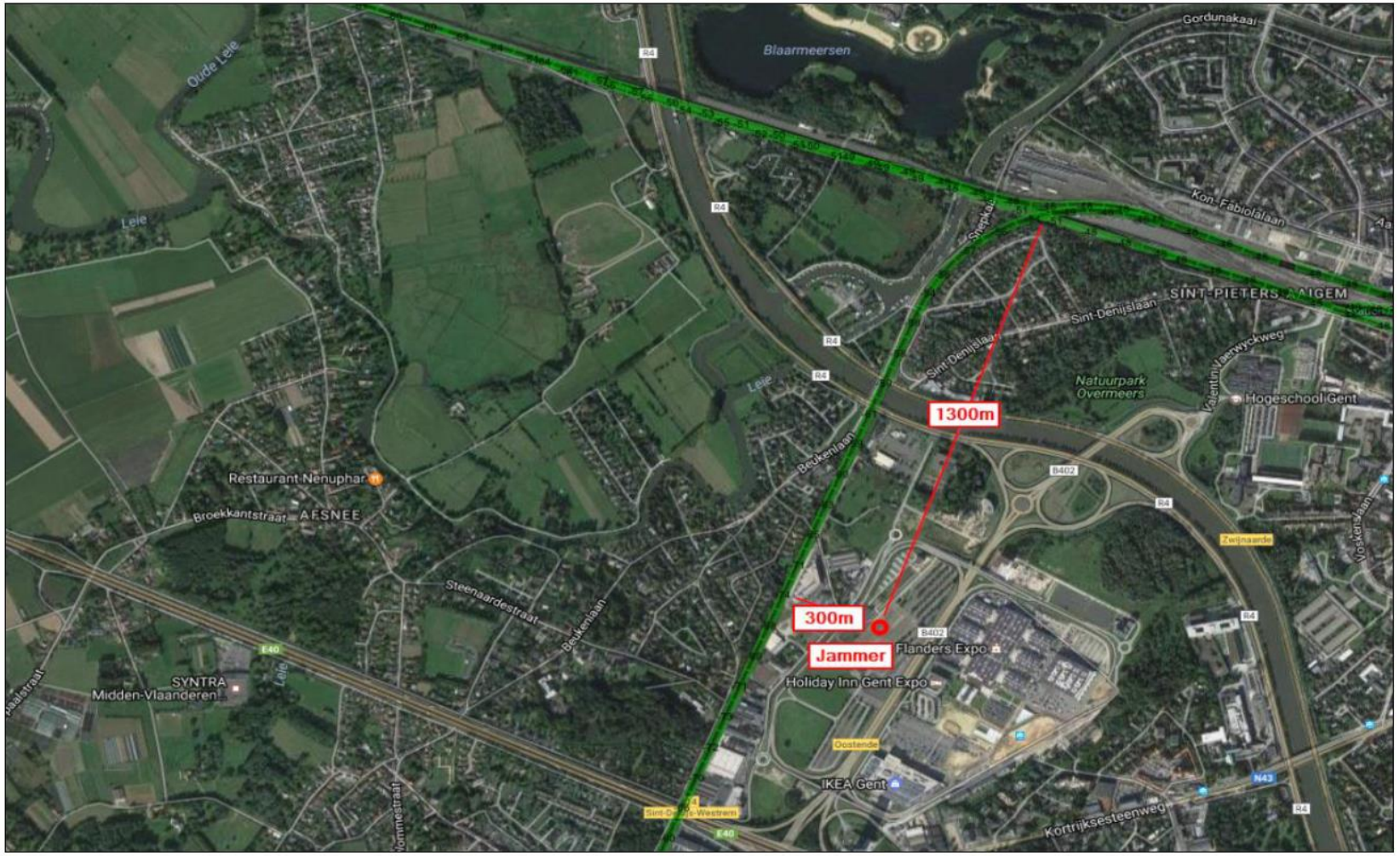
Hypothesis

1. Jammer in an open area on the parking of the Flanders Expo in Gent. Assumption is 50 watts Tx power.
2. Closest railway line is the L75 (300m distance) and L50A (1300m distance).
3. Type of traffic is ETCS L2 with RBC Handovers in the area.
4. Only Downlink disturbance is analysed.

Jammer Power Output	50	Watts
Jammer Bandwidth	30	MHz
Spectral Power	0.33	Watts/200 KHz
Power Jammer	25.23	dBm
Gain Tx Jammer	0	dBi
EIRP Jammer	25.23	dBi
Distance Jammer-Reference Point	300	m
Frequency	900	MHz
Gain Tx Jammer	0	dB
Gain Rx Victim	0	dB
Additional Losses (building,...)	0	dB
Path Loss	81.07	dB
GSM-R Reference Level Taken	-74	dBm
Jamming Level at 300 m	-55.8	dBm
C/I condition	-18.2	dB

Conclusions

1. Total loss of service (negative C/I) on the L75. Evaluation of 1500m of tracks of potential impact on the L75 (ETCS drops with emergency brake).
2. The L50A can be impacted punctually, near the RBC handover zone because of the waveguide effect from the canals that can transfer strong signals (near Blaarmeersen).

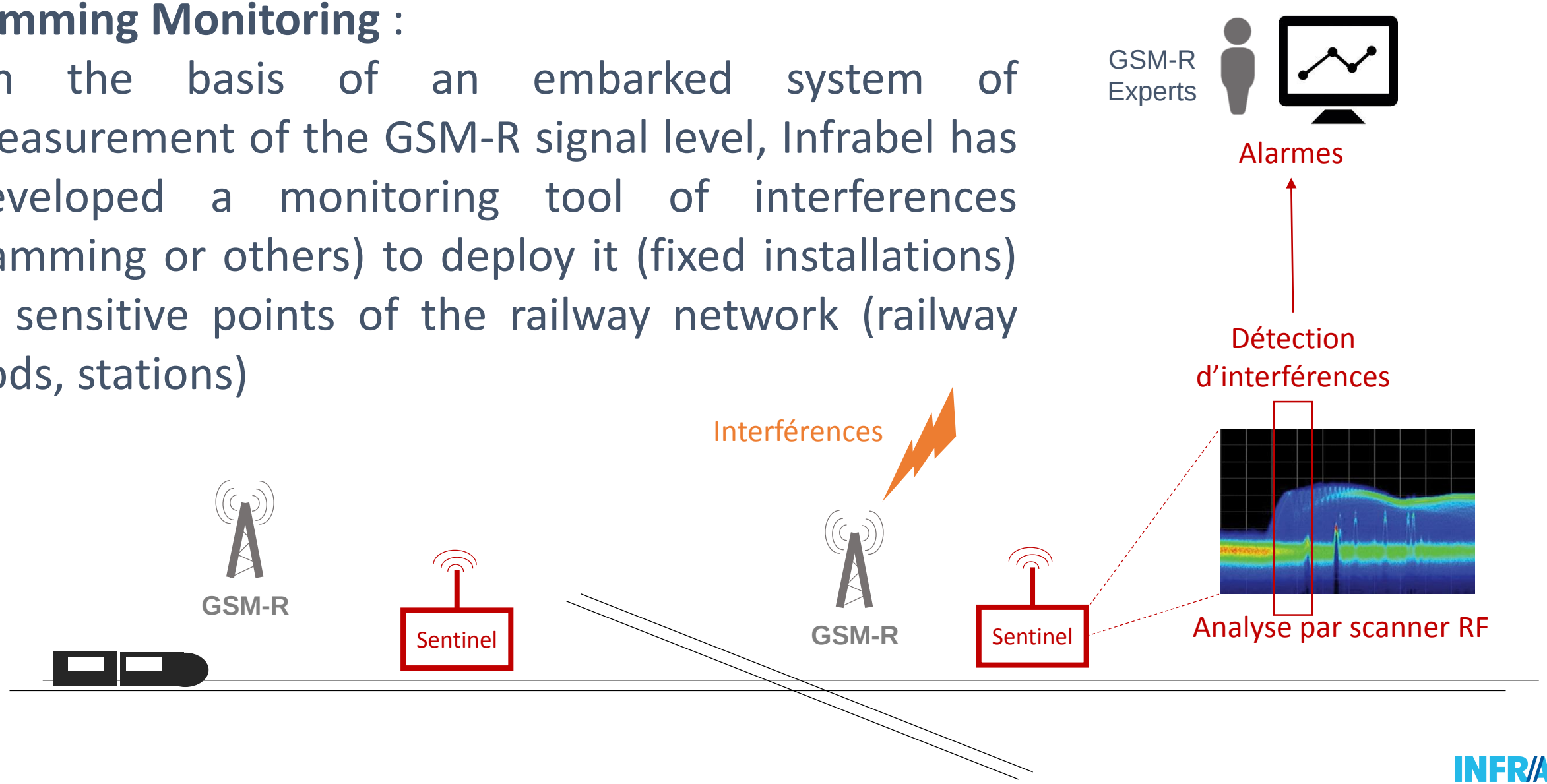


INFRABEL

22 March 2016 : Consequences - Jamming

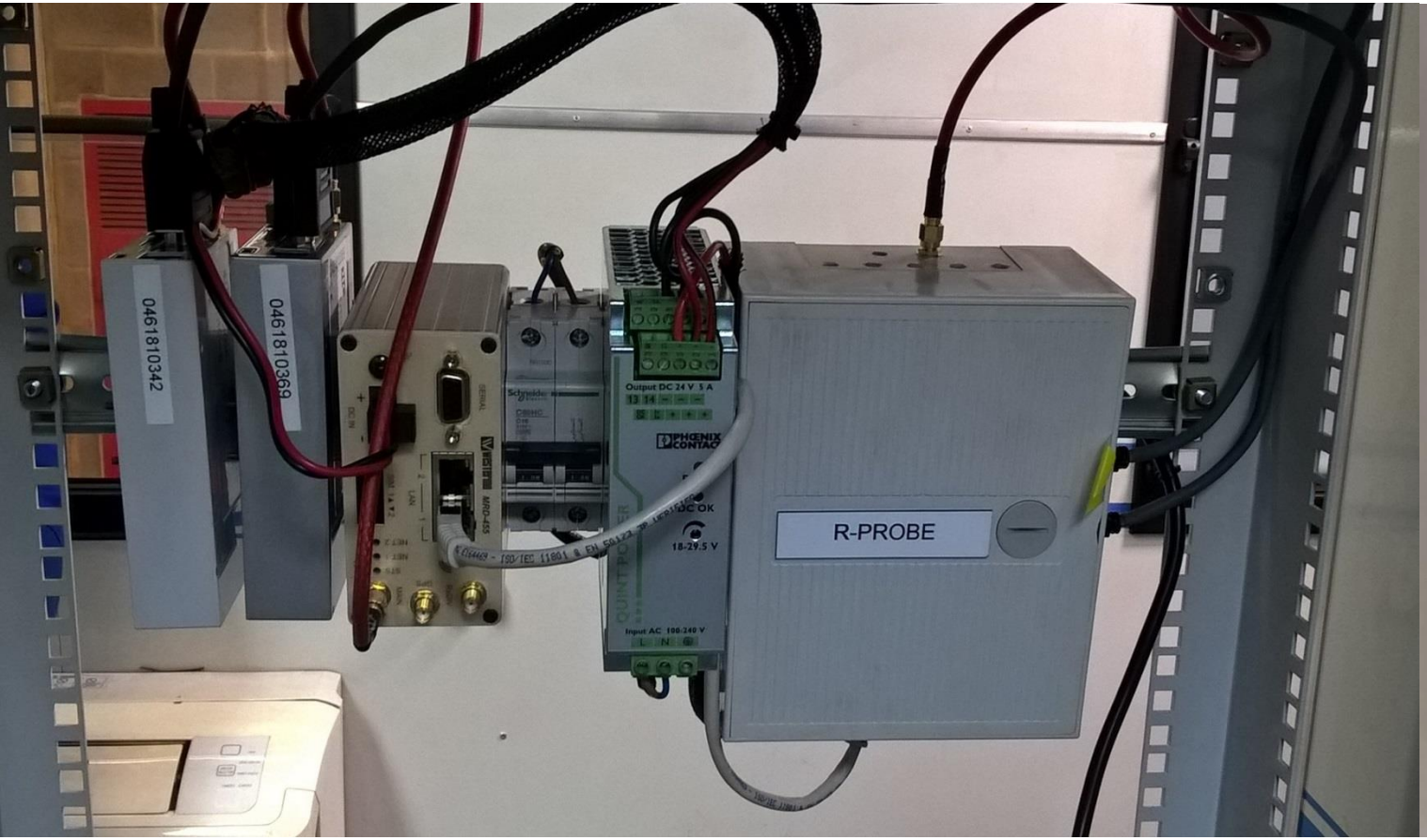
Jamming Monitoring :

On the basis of an embarked system of measurement of the GSM-R signal level, Infrabel has developed a monitoring tool of interferences (jamming or others) to deploy it (fixed installations) in sensitive points of the railway network (railway nods, stations)

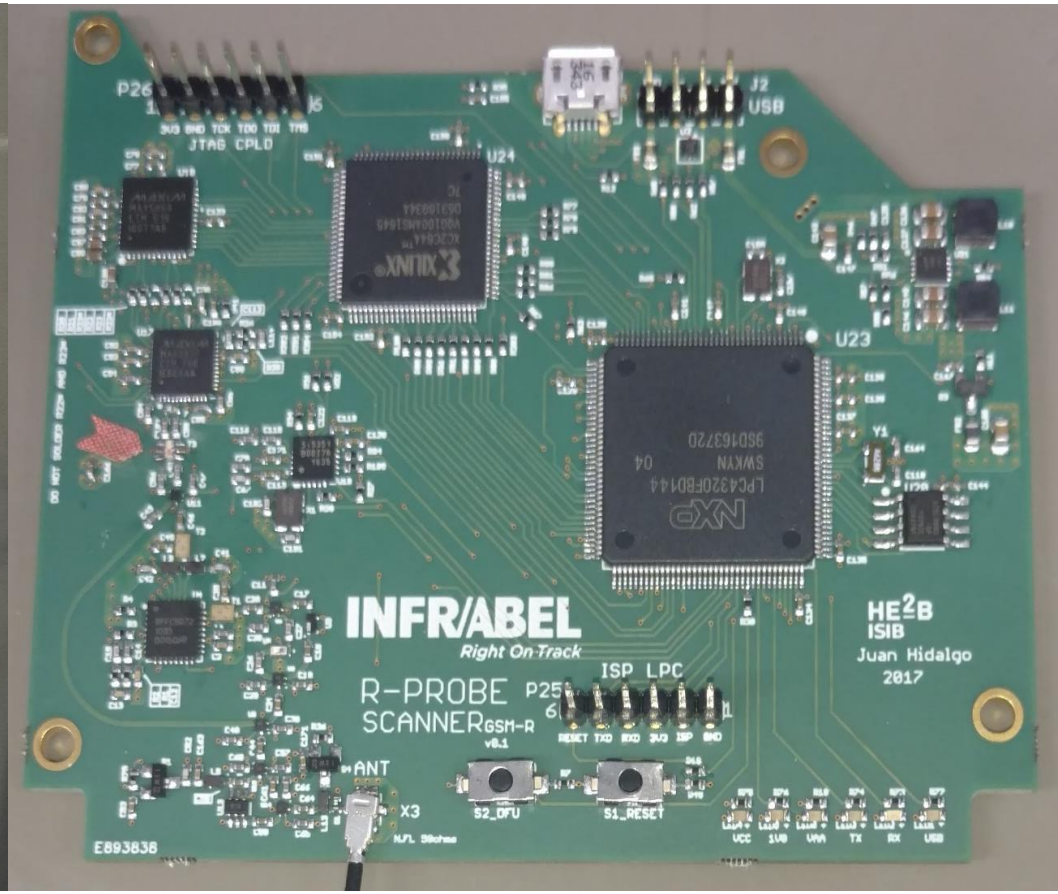


22 March 2016 : Conséquences - Jamming

Monitoring of the GSM-R network : Probes & Sentinel



Rack mounted (in a measurement train) R-Probe unattended measurement system



R-Probe Embedded Scanner for interferences detection (Sentinel)

How to protect GSM-R & the business continuity?

« Risk comes from not knowing what you're doing. »

How to protect GSM-R & the business continuity?

The sentinels remain a punctual mean and should not be deployed everywhere…

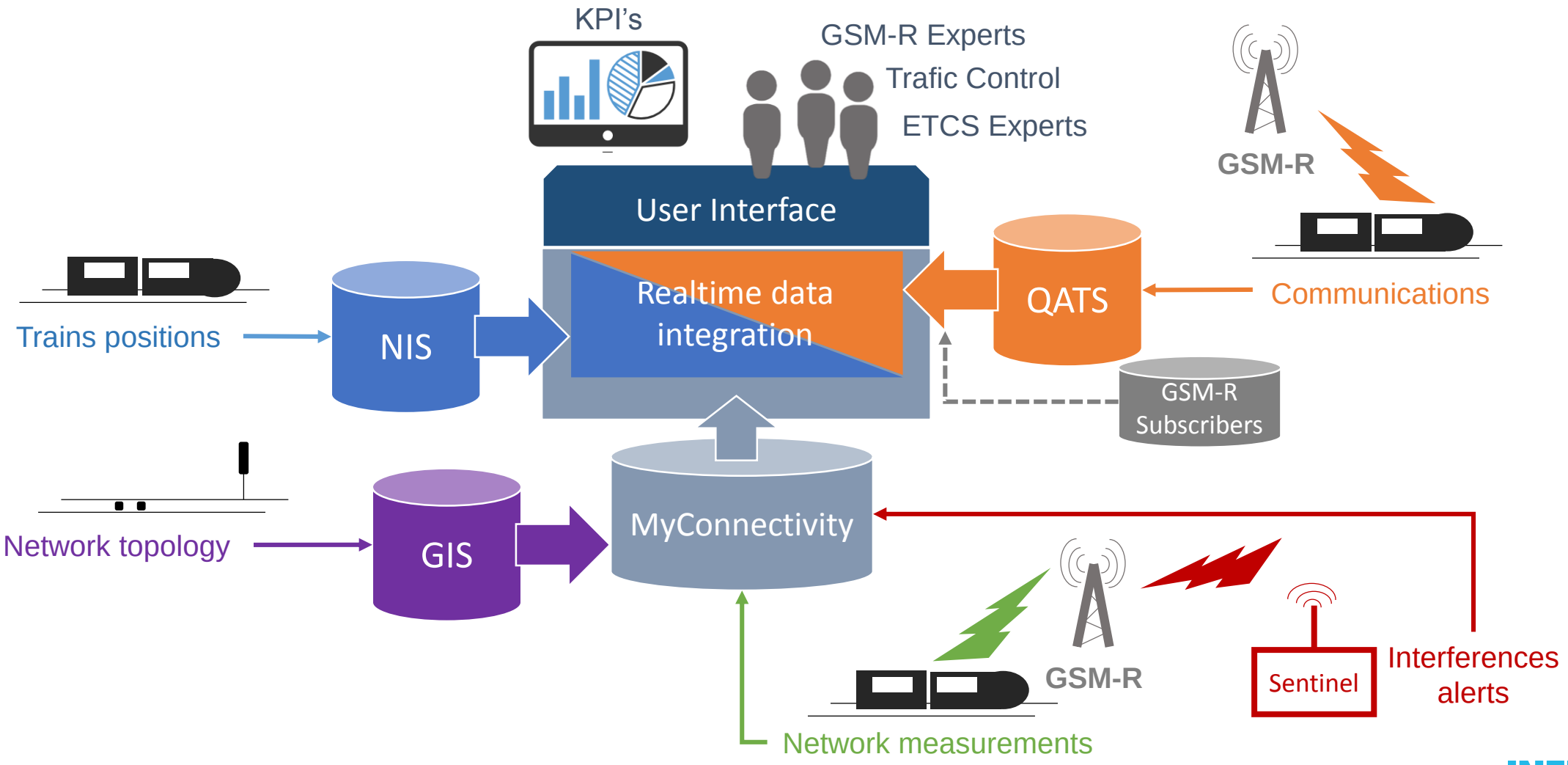
To protect the GSM-R, you need to understand as soon as possible the cause of a malfunctioning service and to identify its origin !

Infrabel pursue a continuous improvement plan of operational management means of the GSM-R network based on :

1. **The integration of datas** (measures, configuration, KPI's, alarms, communications, etc) with reference datas from the railway network (topology, traffic, etc)
2. Greater use of **autonomous systems** (on-board or fixed robots) for measurement of signal levels and detection of interferences
3. **Automatization of the process of treatment of datas with homemade softwares** (MyConnectivity) linked to softwares from suppliers (Netact/Nokia, QATS/Expandium)

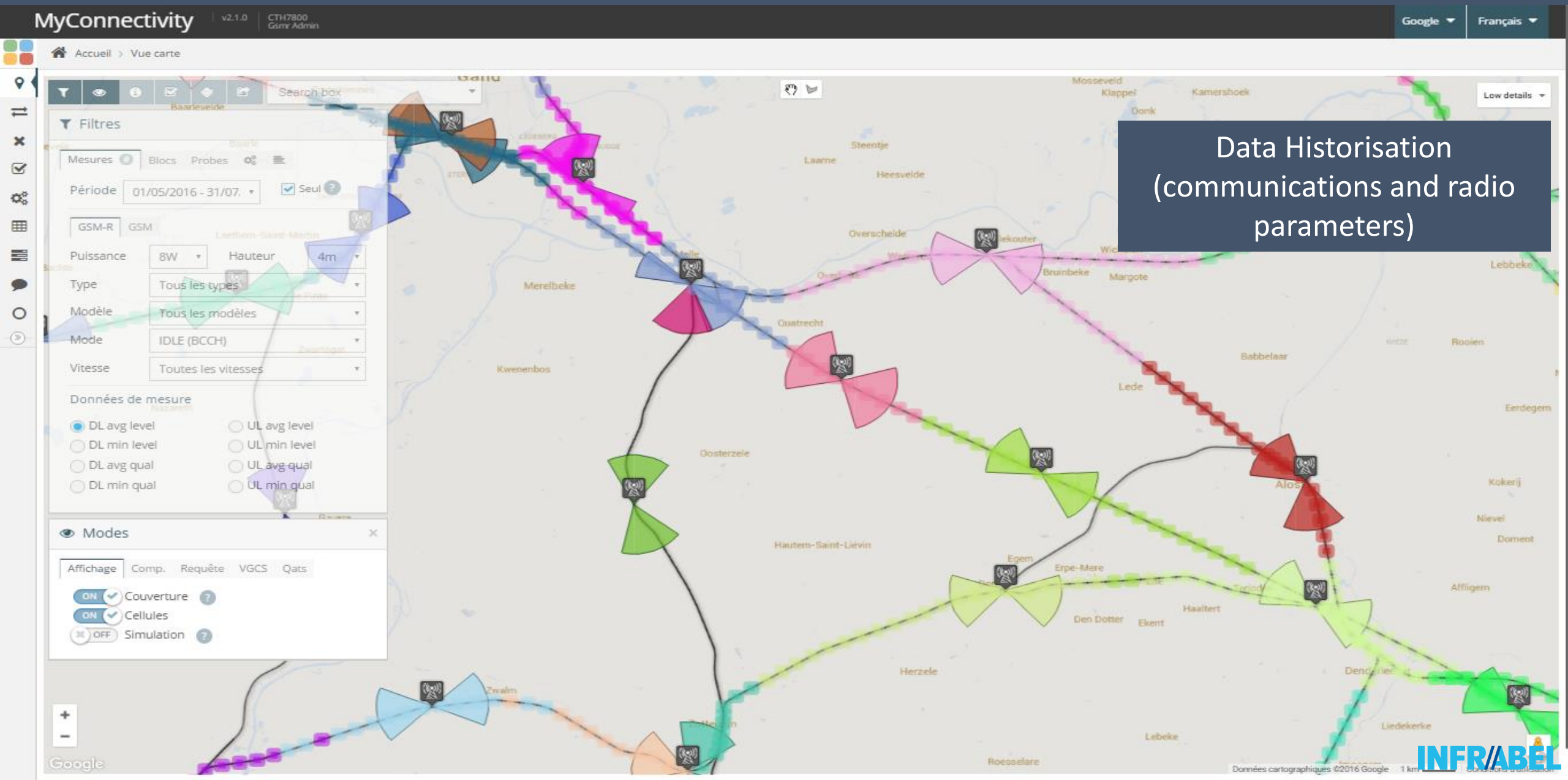
Data integration for GSM-R improved operations

Data integration for GSM-R Improved Operations

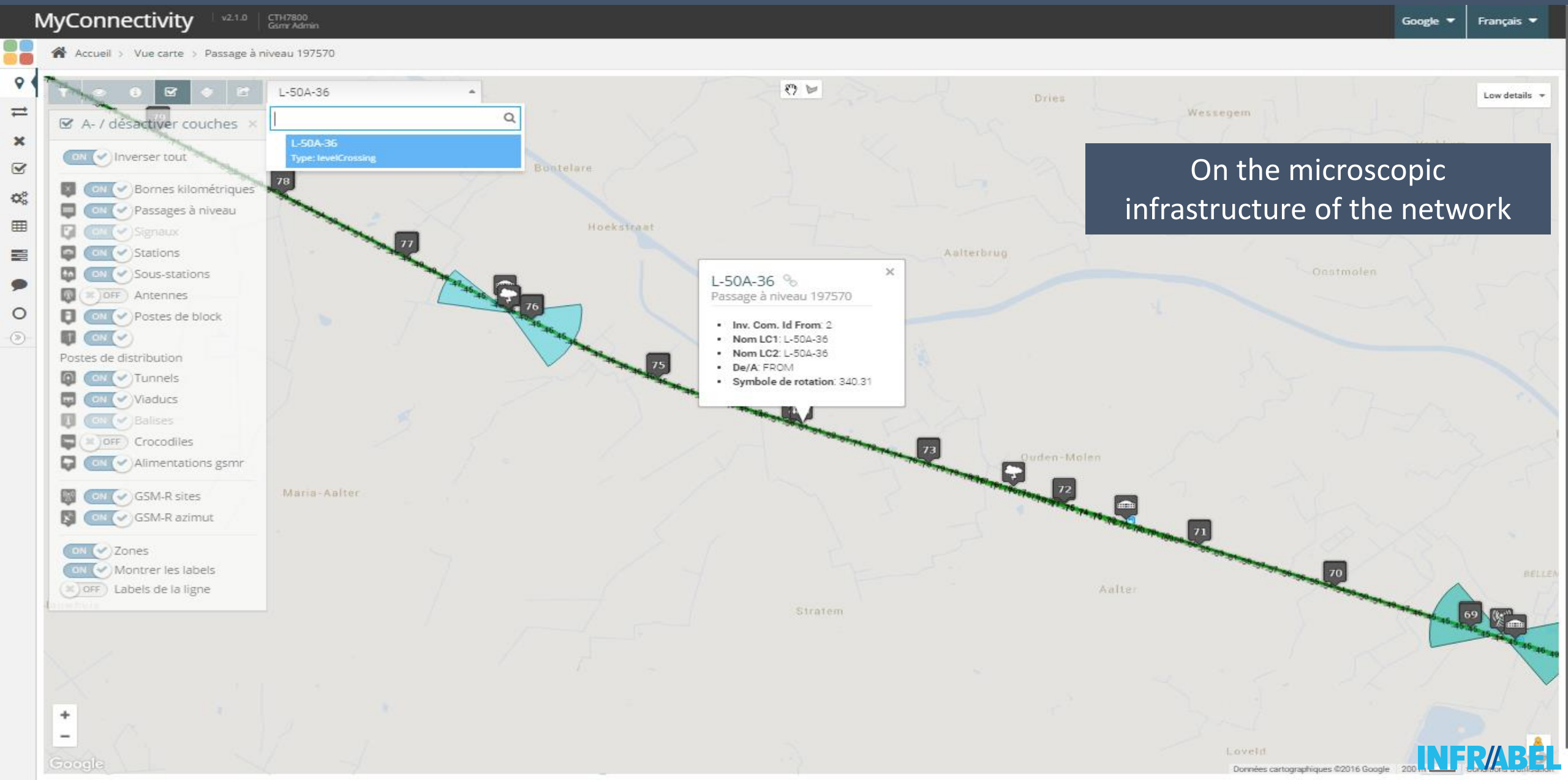


INFRABEL

Data integration for GSM-R improved operations



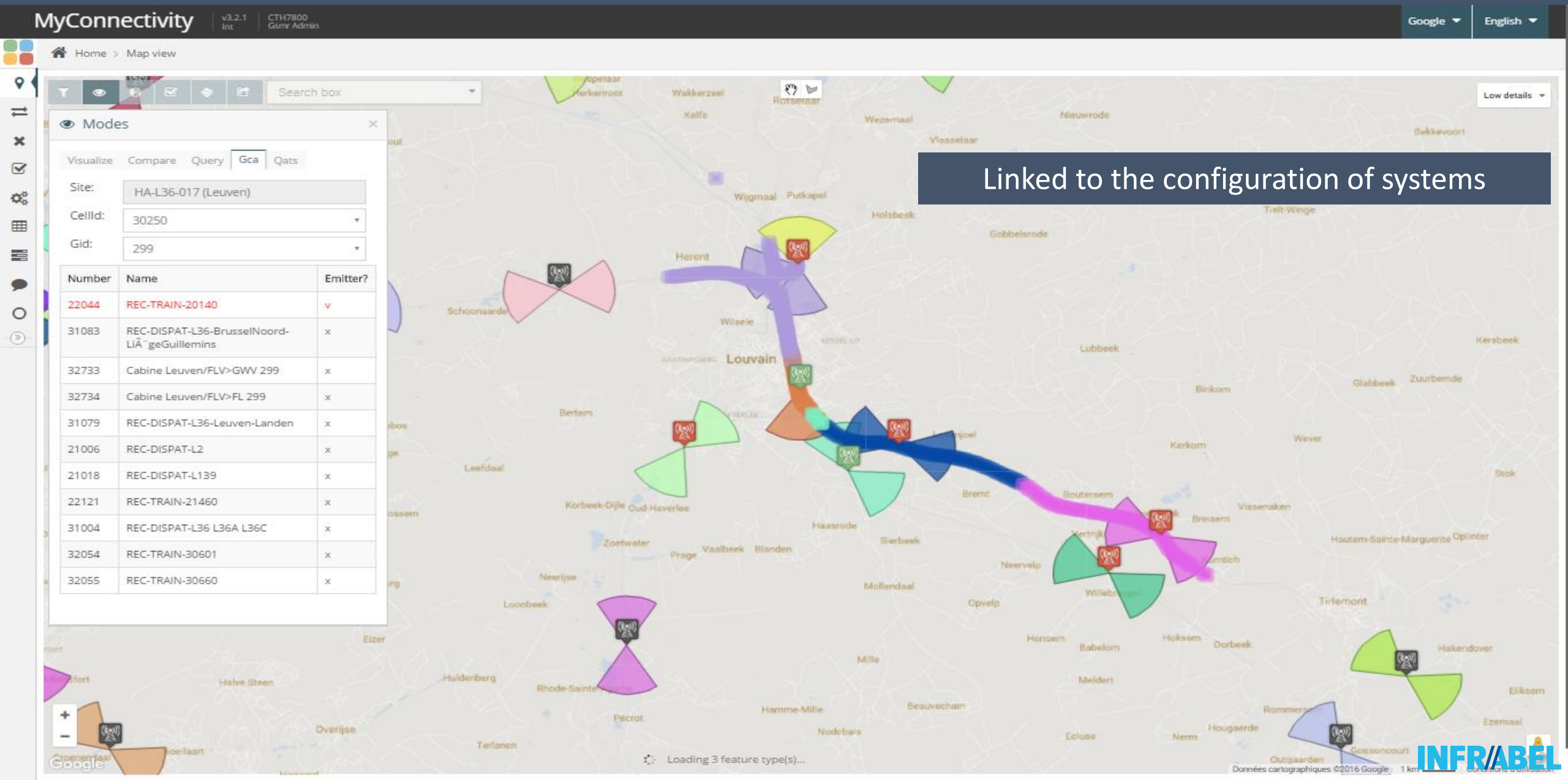
Data integration for GSM-R improved operations



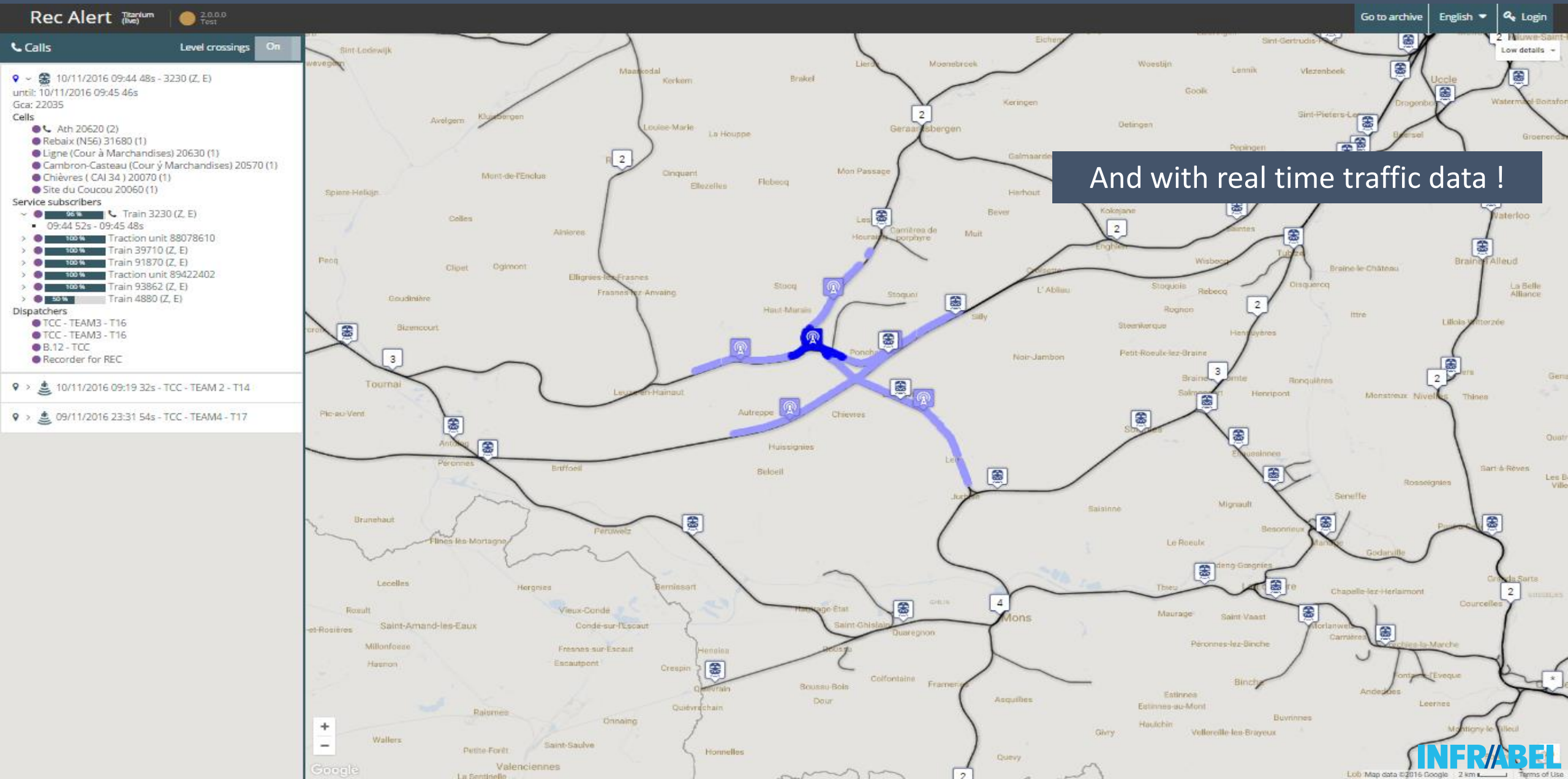
On the microscopic infrastructure of the network

INFRABEL

Data integration for GSM-R improved operations



Data integration for GSM-R improved operations



Thank you for your attention

INFRABEL