Susceptibility of COTS sensors to IEMI using pulse modulated signals

Louis Cesbron Lavau[1], Michael Suhrke [1], Peter Knott [2]

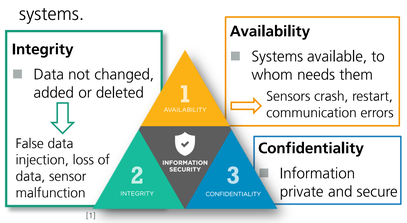
[1]Electromagnetic Effects and Threats, Fraunhofer Institute for Technological Trend Analysis INT, Euskirchen
[2] Chair of Radar Systems Engineering Institute of High Frequency Technology, RWTH Aachen
Fraunhofer Institute for High Frequency Physics and Radar Techniques FHR, Wachtberg

Fraunhofer INT

Background

Sensors show up in every aspect of life
- Use growth
- Multiple applications

IEMI [intentional electromagnetic interference] : intentional malicious generation of electromagnetic energy introducing noise or signal into electrical or electronic systems, thus disrupting, confusing or damaging these systems.



[1]

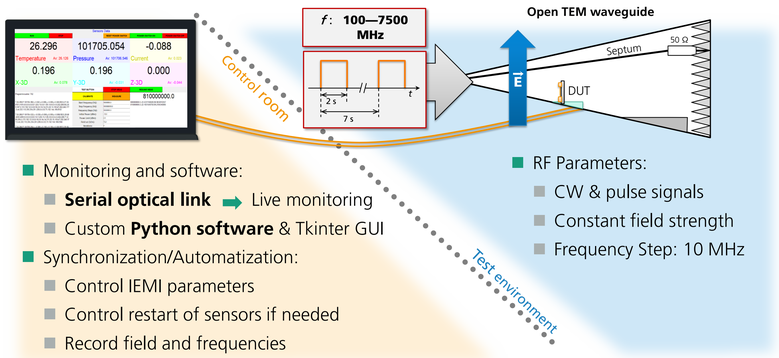
Objectives

Aim: Investigate the susceptibility of **stand-alone sensors** with privileged access to the hardware and software

General Setup
- 3 sensors: Magnetometer, Barometer and Current Sense sensor
- 1 Microcontroller

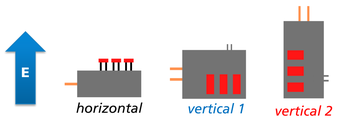
Required features:
- Easy access to raw data for future diagnostics
- Only irradiation of the sensors (shielded box)

Methods



- Monitoring and software:
  - **Serial optical link** ➡ Live monitoring
  - Custom **Python software** & Tkinter GUI
- Synchronization/Automatization:
  - Control IEMI parameters
  - Control restart of sensors if needed
  - Record field and frequencies
- RF Parameters:
  - CW & pulse signals
  - Constant field strength
  - Frequency Step: 10 MHz

- Three DUT orientations:



- Susceptibility measurements:
  - Identification of vulnerable frequencies
  - Classification of errors
  - Use of multiple pulse parameters

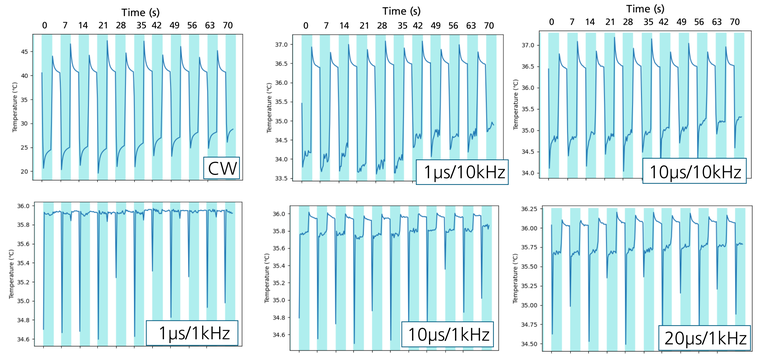
Error	Description
1	Loss of data link under exposure
2	Loss of data link requiring restart
3	Raw sensor values out of tolerance
4	Sensor status errors

Results

Summary of the main differences between CW and pulse signals

Sensors\ Signal type	Magnetometer	Barometer	Current Sense
CW	Multiple crashes at 300-500MHz range starting from 40 V/m Data link loss around 400MHz -> I2C communication affected Forced restart needed everytime	Status errors around 1 GHz Erroneous values at 2.6-2.8 GHz & 5.4-6.2 GHz up to +50°C with 400V/m Steady increase of field strengths leads to new measured standby sensor value	No errors detected
Pulse signals	Higher field strength to cause crashes at 300-500 MHz	Status errors and crashes at 1GHz, 2.5-3GHz causing forced restart Erroneous values at the same frequencies but with lower values (up to 2-3°C maximum)	Erroneous values and status errors at 2.9 & 5.8 GHz

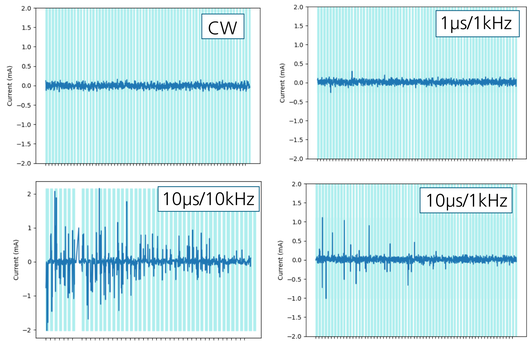
Influence of pulse parameters on the measured temperature (barometer)



Frequency range: 5900 – 6000 MHz
Field : 400 V/m
RF exposure: 2 seconds (plot:)
Signal parameters:
1. Continuous Wave (CW)
2. Different pulse parameters:
   - pulse width : 1µs, 10µs & 20µs
   - pulse repetition rate (PRR) : 1 kHz & 10 kHz

Results:
- Erroneous values only during exposure
- No status errors
- Significant changes of indicated temperature with CW signals
- Various influences of pulse parameters:
  - Shorter pulse width -> narrower peak
  - Higher PRR -> similar behavior to CW qualitatively, not quantitatively

Influence of pulse parameters on the measured current (current sense)



Frequency : 5600 – 6050 MHz
Field : 400 V/m
RF exposure: 2 seconds (plot:)
Results:
- No errors with CW signals
- Influence of PRR
- Value errors & Status errors

Errors occured also at 2900MHz
- Open questions:
  - Influence on the SPI clock?
  - Resonance frequency ?

Discussion & Next Steps

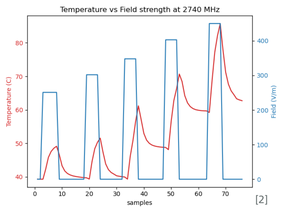
- Limits to measurements:
  - Communication ports exposed
  - Serial connection interrupted
- Influence of the DUT orientations
  - Same vulnerable frequency range
  - Some specific errors only with some orientations (Crashes, Current Sense status errors)
  - Coupling path between sensor and microcontroller?

➡

- Identification of coupling paths:
  - Shielding of ports or possible coupling paths
- Repeatibility of the results
  - Use of other temperature sensors
- Observation of communication with bus analyser
  - Understanding I2C or SPI errors communications

- Possible "smart" pulse attacks:

In EMC Europe 2021 Paper [2], CW signals with field strength above a certain threshold caused a permanent change in the indicated temperature until restart.
Can we use short pulses to achieve the same behaviour?
Which field strength level would it require?



[2]

Conclusion

Threat to sensors
- Systems depend on sensor data
- Information Security needed

Availability under IEMI
- Communication errors
- Forced restart

Integrity under IEMI
- Manipulation of sensor readings

➡

- Better understanding of physical phenomena
- Suitable protection measures

1 Image: https://blog.jamestyson.co.uk/the-cia-and-dad-triads

2 Cesbron Lavau, Louis & Suhrke, Michael & Knott, Peter (2021). Susceptibility of Sensors to IEMI Attacks. EMC Europe 2021 (to be published)

RWTH AACHEN UNIVERSITY

Fraunhofer FHR