Marek P. MICHALAK[1], Monika E. SZAFRAŃSKA[2]

National Institute of Telecommunications (1), Wroclaw University of Science and Technology (2)

doi:10.15199/48.2018.02.12

EMC in IoT World

***Abstract**. The Internet of Things (IoT) is fast growing part of the market that becomes one of the biggest challenges of contemporary and future electromagnetic compatibility researches. The paper presents discussion on the subject of EMC testing of IoT related equipment. The authors considered different, alternative to classical, approaches to equipment testing for electromagnetic compatibility including those using new technical developments of FFT use in EMC testing. PCB-like testing approach and system approach are also discussed and taken into consideration.*

***Streszczenie.** W artykule przedstawiono dyskusję nad tematyka związaną z badaniami EMC urządzeń tzw. Interrnetu Rzeczy (Internet of Things - IoT), stanowiącego szybko rozwijającą się gałąź rynku teleinformatycznego. Autorzy uwzględnili różne podejścia do zagadnienia badań kompatybilności urządzeń w tym wykorzystujące nowe zdobycze techniki w zakresie badań z wykorzystaniem FFT. Pod dyskusję poddane zostały również podejścia badawcze zbliżone do rozwiązań stosowanych w przypadku PCB oraz podejście systemowe. (**EMC w świecie IoT**).*

Keywords: IoT, EMC, test setup
Słowa kluczowe: Internet Rzeczy, kompatybilność elektromagnetyczna, stanowisko badawcze

Introduction

In the last years the number of smartphones, tablets and “wearable” equipment significantly increased. In 2011 Cisco [1] provided estimation that in 2020 there will be 50 billion Internet of Things (IoT) related equipment in the world. This means a huge number of equipment that must coexist.

Together with the increase of transfer rates the use of wireless communication also increased. That brings questions if the increasing number of wireless devices will influence the rise of problems with Electromagnetic Compatibility (EMC) and if today’s industry is ready for EMC problems connected with IoT development. The statistics alone show that the more equipment influence and interact with each other (what is a basic presumption of IoT), the more electromagnetic compatibility problems can be expected, especially when EMC parameters of the equipment will be left on today’s level.

The problems mentioned above are being razed on international level, the subject is very up to date and in coming years it will undoubtedly be major EMC issue.

How to test the IoT equipment against the EMC?

The dynamic development of IoT equipment contributes to the fact that this equipment is quickly introduced to the market and mass production, what in turn generates the need for testing of this equipment. In most cases the EMC standards fall behind as far as new solutions are concerned. And even if that can be achieved the new problem arises. Most of IoT intended equipment is meant to work in “crowds” – we face the accumulation of equipment in direct proximity. And here another issue arises – very often that equipment was tested according to different standards, therefore in some cases even if on the basis of performed tests single equipment meets the appropriate requirements, the coexistence of the same equipment in specific conditions becomes impossible or generates interactions that influence the integrity and correctness of data transferred by that equipment. Furthermore, if we take into account that IoT equipment works in very close proximity the other issues arise that were not so much important before as far as EMC testing is concerned. Even if since lately it is taken into consideration that electronics is being smaller all the time, in case of IoT equipment we face it in every single issue. For typical equipment for which the influence of devices working in close proximity was observed in the last years, not long ago the IEC 61000-4-39 [2] standard was positively voted for introduction. The solutions proposed in above mentioned standard may introduce some kind of transposition of IoT equipment coexistence into area of the tests. However, if we take into account the time usually needed for introduction of standards we can expect that before the testing methods described in IEC 61000-4-39 are introduced to the product standards it might take several years.

It should be noted here, that because of possible equipment classification and purpose, that equipment may be the subject of different requirement, both emission and immunity. Significantly different may be also the interpretation of these requirements. For example, when we consider gas measurement equipment, especially in case of gases that are dangerous to people, the tolerance for incorrect data is single numbers in percentage, while in cases where the measurement or transmission can be repeated and the measured value is not critical in decision making process, the allowed error level can be even as high as 50%. Off course most of manufacturers that like to be seen as reliable and reputable state much higher requirements for their products. Whichever the case is, there are some (mostly low cost) products that are available in the market that not only do not work properly (in clients opinion) but also do not even comply with basic requirements. It is not possible to avoid situations where non-compliant products are introduced to the market. Even with thorough control and market surveillance this scenario needs to be taken into account.

The other fact that must be noted here is that very often the same level of ignorance of the developers of some solutions can cause significant problems with their products or systems compatibility. Commonly known rule is that even if you use components that are standards compliant it does not guarantee that you end up with the resulting compatible product. The same is still true (and even in higher scale) in the IoT world. Full integration of equipment together with dimensions requirements for IoT devices causes very small (read: almost non-existent) separation between the components (especially when compared with wave lengths).

The question is, how to test IoT equipment against the EMC requirements? Do we test them:

- With classical approach – like other equipment before, according to EN 55022, EN 55024 or EN 55032?
- With real time measurements?
- Like components (or PCBs)?
- Like whole systems (from over a dozen to several hundreds of elements?

Classical approach

The most well-established and current approach on the market for many years has been to test IoT or similar devices according to standards and requirements for typical IT equipment (until recently it were mainly EN 55022 standard [3] for emission measurements and EN 55024 standard [4] for immunity measurements), and in recent times for multimedia equipment (i.e. EN 55032 standard [5], superseding the EN 55022 and some other standards, and waiting for publication is EN 55035 standard which will cover the immunity requirements for multimedia equipments, and among others will supersede the EN 55024 standard – the CISPR 35 Publication is already published, so we probably will not wait for EN 55025 for too long). Using this approach is the closest one to regulatory requirements for introduction to the market of new equipment according to Radio Equipment Directive (RED) [6] or ElectroMagnetic Compatibility Directive (EMCD) [7].

In the case of testing according to the requirements of the above mentioned Directives harmonized standards [3, 4, 5], the tests are performed in tests set-ups strictly defined in the standard. This means that all the set-ups of every single part of equipment are made according to those standards. However, there is always the question whether the measuring system corresponds to the basic need of an IoT device under test, whereby, in principle, those devices have at least a few, a dozen or several hundred components in their basic functionality, each of which may, according to the Directives [6, 7] requires testing as a single item because of being also marketed as a single item.

In a typical tests performed in accordance with the guidelines and requirements of the abovementioned standards, the measuring/testing system is assembled in the way in which there may be multiple components of the device and the auxiliary/associated equipment. An example of such a system prepared for testing with the distinction of individual components is shown in Figure 1.

In the case of most IoT devices we mainly deal with low power devices and most of them are battery powered, so the most interesting scenario for the measurements, and closest to the practical applications of these devices and the most representative of the entire product group are the IoT devices tests in the typical case of radiated disturbances emissions measurements, as most of these devices are not equipped with external wiring that could be potential sources of reception and generation (radiation) of disturbances.

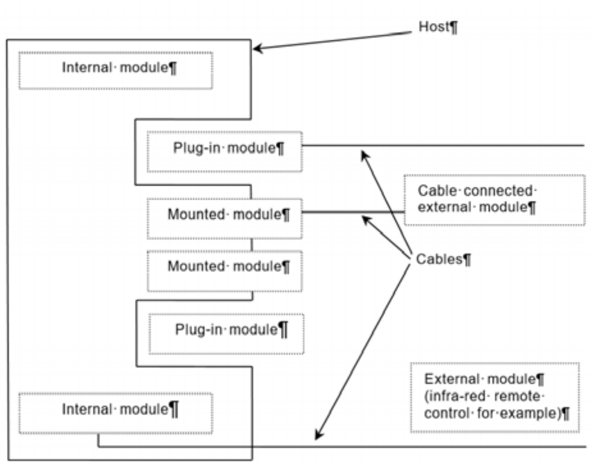

Fig.1. Example of a host system with different types of modules [5]

A typical, standard dictated set-up of several larger systems of devices during radiated emission testing is shown in Figure 2. Such placement of individual test objects can generate problems for devices that require multiple co-operating auxiliaries for their correct operation or consist of multiple modules, linked together. Case studies and divagations on this subject are discussed later in this article.

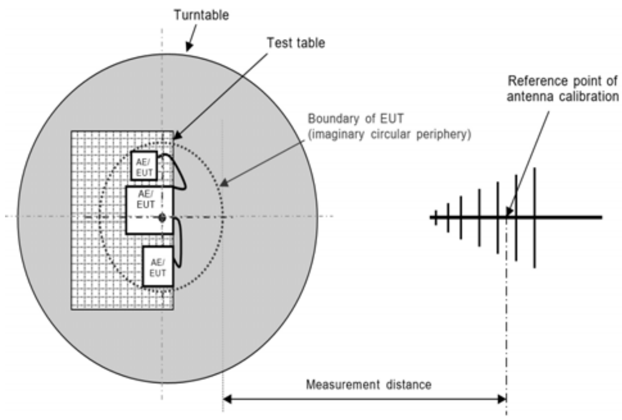

Fig.2. Typical test set-up for radiated emission tests [5]

The immunity standard for multimedia devices, which would indicate the direction of the test as EN 55032, has not yet been introduced in Europe (although CISPR 35 Publication which does just that, as it was mentioned before, is already published – it is difficult to say what slows down the introduction of it in Europe, especially when it is taken into account, that both CISPR 32 and CISR 35 were always meant as complementary publications/standards). The EN 55032 standard is significantly is far more sensitive to problems with complex equipment and their modular design when compared to EN 55022, which it replaced. Looking at the construction of EN 55032 standard and its preparation for the commonality of certain fragments with the expected EN 55035 standard for the immunity of multimedia equipment, it is to be expected that the latter one (still awaiting the unification with the European Norms requirements) will also take into account the complexity and multi-module construction of contemporary (and probably future) devices. On the other hand, it should not be expected that all the issues related to the internal compatibility of multi-modular devices (and systems) or interactions between elements of the system will be satisfactorily addressed. Meanwhile, it is clear today that these issues may be the biggest challenge in the of IoT devices world.

It must be remembered, that the EU Directives essential requirements (and consequently Directives harmonized standards) put main impact at electromagnetic spectrum protection and protection of the systems that make use of that spectrum, especially (historically) radio diffusion systems, against the interfering effects of disturbances generated by devices that are newly introduced to the market. The second essential requirement of EU Directives should theoretically ensure, that those newly introduced to the market devices are adequately secured against intentionally generated electromagnetic fields. Meanwhile in the case of IoT devices, being mostly low power devices, the main problem may be to ensure the compatibility (read: undisturbed cooperation) between the devices. It is true that meeting the two basic objectives (essential requirements) of the Directives should theoretically also ensure that the coexistence of equipment meets the essential requirements of the Directives. However, in the case of IoTs, it may be that, due to their specific location (often direct proximity), for the devices working in the proximity of other devices (in addition to constantly changing their mutual position) the current (classical) approach and the standards theoretically "safeguarded" by the appropriate allowed emission limits and required levels of immunity combined with measurement methods that measure distance distances that do not correspond to actual distances between devices in the IoT world will simply be insufficient.

The first steps to take into account the actual conditions of modern devices coexistence (including those that already can be regarded as IoT devices), as already mentioned, have been made in the IEC 61000-4-39 standard [2]. This March 2017 published international standard (just published as the EN 61000-4-39 on June 9th 2017) is intended to refer to the immunity testing of devices in the immediate proximity of other electromagnetic field generating devices and is related to the problem that has been observed by placing various types of mobile devices and RFID devices close together. Taking these issues into account, IEC 61000-4-39 and its research methods can be a good step towards addressing the challenges we face with the Internet of Things. Unfortunately, it should be taken into account that adoption of standards is quite time-consuming and even after the introduction of this standard, it may take some time before it finds its references in general standards and product standards.

Real time tests approach

The new FFT (Fast Fourier Transform) powered fast receiver solutions, recently emerging in the market for measuring equipment, enable accurate and more complete information about the measured device disturbances that sometimes switch at the nanosecond level. Devices with such short switching times produce very broad electromagnetic spectrum. The use of FFT-equipped receivers allows us to judge the distributed spectrum of signals and at the same time gives us the opportunity to indicate possible electromagnetic compatibility problems resulting from the generation of disturbances over a very wide frequency range.

It is important to note that IoTs often operate in such a way that most of the time they are in standby mode and their period of activity and communication between them occurs sporadically and takes relatively short time – those times range from several milliseconds to single seconds. The types of disturbances produced in such work cycles are very difficult to detect with conventional measurement methods, unless multiple frequency sweeps using the MaxHold function are used, which is very time consuming, but first and foremost it does not guarantee that all emissions (including unwanted or spurious emissions) from the device will be recorded. With the ability to analyse the emissions in real time and thus simultaneously measure for a relatively wide frequency range (instead of stepwise scanning), it is possible to record all events and consequently evaluate the device with a much greater degree of confidence than in the classical approach.

The FFT based EMI receivers can become an element that will significantly enhance classical, CISPR's requirements based tests with the additional capabilities of using such "fast", Real Time Analysis using receivers. All the more so, since these types of solutions are slowly being allowed to be used in some CISPR Publications - for the time being mainly only as the support for existing solutions, but in the future the importance of these measurement techniques will most probably increase significantly.

PCBs approach

The issues related to the IoT devices electromagnetic compatibility verification can also be approached in similar way as for the integrated circuits (PCBs) measurements. In most cases speaking of IoT devices we are talking about relatively small components. Most of these devices are designed as integrated circuits which are then integrated on a common plate. Thus it seems that also for such solutions, methods similar to those described in EN 61967-x [8] and EN 62132-x series [9] could be used. On the basis of such or similar solutions, the problem approach used by many R & D designers can be applied. One of the first articles that linked IoT and EMC issues from the engineer point of view [10] shows some considerations on the applicability of this type of measurement techniques to IoT systems and devices.

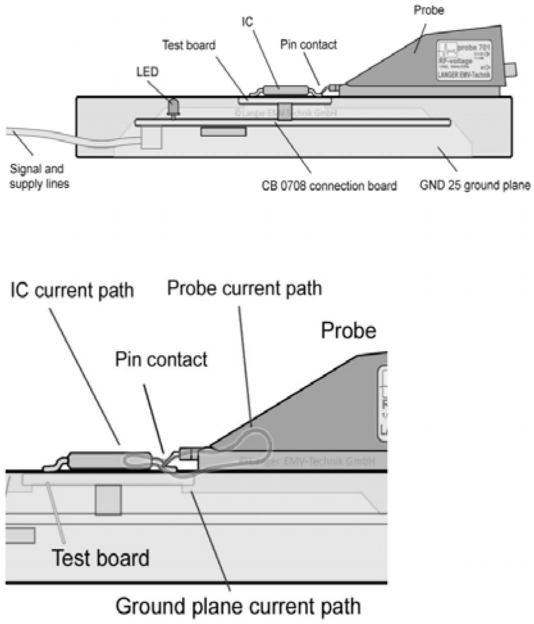

Fig.3. Measurement system for pin current and pin voltage [10]

Among the main issues that need to be mentioned here, one of the most important ones seems to be the ability to test for EMC in the very early stages of element development. It is very important since the one of the principals of a well-designed EMC layout is to think about EMC issues that have already existed from the very beginning of the product's life - from the prototype design phase right to the final product. In fact, only this approach provides the right and the best possible EMC design - in the world of IoT, it is equally, or even more, true.

It should be borne in mind, however, that such an approach, if misapplied, may also involve some risk. In most cases, the device will not meet the requirements and conditions of its typical operation. Yes, tests at this level allow for special signals or device software to approximate the worst working conditions (worst case scenario), but this will not always correspond to the final application of the device and its co-operation with other devices.

System approach

Another possible approach to the IoT devices electromagnetic compatibility is to test these devices as whole integrated systems comprising dozens or even hundreds of components (despite it is a significant departure from the approach adopted in the EU Directives [6, 7] because the Directives look at these components as separate devices – mainly because they are marketed separately, neglecting the fact that they work together). In particular, during immunity testing, such systems may exhibit significantly lower susceptibility to the disturbances than single components. This is due to the fact that IoT devices in most cases are able to transfer their functions to other devices, and thanks to that the impact made by the disturbance on a single device does not cause errors in the operation of the entire system. This system approach is therefore much closer to the “real world” IoT applications.

There are known cases of large installations with multiple devices (for example, sensors) in which due to the one component (or the small group of components) lack of immunity the whole system, due to redundancy discussed above, does not react negatively to the disturbances. Of course, this does not apply to cases in which an incorrectly functioning system component is a key element, which then causes the whole system to crash. In complex systems (and we must remember that in most applications when talking about IoT systems we will deal with complex systems), it may be that not only the vulnerabilities of the devices themselves (hardware susceptibility level), but also software susceptibility level may increase or decrease immunity to disturbances and errors caused by them.

On the other hand, it can (and must) be said that mutual interactions of equipment can also contribute to the increased emission of electromagnetic disturbances of the whole system.

It must be borne in mind that the accumulation of a large number of devices in a small space can cause that even though individual devices are able to meet the emission standards, all systems may no longer be able to maintain this capability.

Summary

Every IoT device that is to be introduced to the market must be able to boast positive results of EMC tests. Currently applied classical approach to electromagnetic tests may, due to being time consuming and costly, not be enough to keep up with the fast-growing technology.

It seems that with the further intensive development of electronics (and with that the IoT devices intensive development), it will be necessary to use complex (hybrid) EMC test methods to ensure the proper operation of systems consisting of so many components. What might be interesting as a "bonus" with such an approach - we can simultaneously get significant reduction of the research, development and test costs.

Even already today measuring devices and standards using the latest measurement techniques are being developed and used to provide real-time measuring capabilities, not just the current practice and the classical emission testing approach, performed only by frequency scanning. This approach, combined with classical (possibly modified) measurement methods and test settings, covers not only individual devices but also entire systems, allowing for better, more reliable EMC testing of IoT devices equipped mainly with ultra-fast processors.

In this paper, the authors took the attempt to gather and present the broadest possible spectrum of ideas and suggestions for how to deal with the massive increase in the number of collaborating or co-existing high-tech electronic devices due to the increased development of IoT devices.

***Authors**: mgr inż. Marek P. Michalak, Instytut Łączności – Państwowy Instytut Badawczy, Zakład Kompatybilności Elektromagnetycznej, ul. Swojczycka 38, 51-501 Wrocław, e-mail: M.Michalak@itl.waw.pl; mgr inż. Monika E. Szafrańska, Politechnika Wrocławska, Wydział Elektroniki, ul. Janiszewskiego 11/17, 50-372 Wrocław, e-mail: monika.szafranska@pwr.edu.pl*

REFERENCES

[1] http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
[2] IEC 61000-4-39 Electromagnetic compatibility (EMC) - Part 4-39: Testing and measurement techniques - Radiated fields in close proximity - Immunity test
[3] EN 55022 Information technology equipment– Radio disturbance characteristics– Limits and methods of measurement
[4] EN 55024 Information technology equipment - Immunity characteristics - Limits and methods of measurement
[5] EN 55032 Electromagnetic compatibility of multimedia equipment - Emission requirements
[6] DIRECTIVE 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC
[7] DIRECTIVE 2014/30/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility
[8] EN 61967-x Integrated circuits - Measurement of electromagnetic emissions - Part x:… (series of standards)
[9] EN 62132-x Integrated circuits - Measurement of electromagnetic immunity - Part x:… (series of standards)
[10] Langer G., Is EMC prepared to handle the challanges of the Internet of Things, Interferencetechnology 2016, ITEM 28 April 2016