EPJ AP

Applied Physics

EPJ.org
your physics journal

Eur. Phys. J. Appl. Phys. (2015) 69: 11002 DOI: 10.1051/epjap/2014140230

Radiated EMC immunity investigation of common recognition identification platform for medical applications

Jorge Miranda, Jorge Cabral, Blaise Ravelo, Stefan Wagner, Christian F. Pedersen, Mukhtiar Memon, and Morten Mathiesen

edp sciences

The title "The European Physical Journal" is a joint property
of EDP Sciences, Società Italiana di Fisica (SIF) and Springer

Eur. Phys. J. Appl. Phys. (2015) 69: 11002
DOI: 10.1051/epjap/2014140230

THE EUROPEAN
PHYSICAL JOURNAL
APPLIED PHYSICS

Regular Article

Radiated EMC immunity investigation of common recognition identification platform for medical applications

Jorge Miranda[1], Jorge Cabral[1], Blaise Ravelo[2,a], Stefan Wagner[3], Christian F. Pedersen[3], Mukhtiar Memon[3], and Morten Mathiesen[4]

[1] Centro Algoritmi, University of Minho, Campus de Azurém, 4800-058 Guimarães, Portugal
[2] IRSEEM, EA 4353 – ESIGELEC, 76801 St. Etienne du Rouvray, France
[3] Dept. of Engineering, Aarhus University, 8000 Aarhus C, Denmark
[4] Sekoia, 8000 Aarhus C, Denmark

Received: 29 May 2014 / Received in final form: 31 October 2014 / Accepted: 4 December 2014
Published online: 7 January 2015 – © EDP Sciences 2015

Abstract. An innovative e-healthcare platform named common recognition and identification platform (CRIP) was developed and tested as part of the CareStore project. CareStore and CRIP aims at delivering accurate and safe disease management by minimising human operator errors in hospitals and care facilities. To support this, the CRIP platform features fingerprint biometrics and near field communication (NFC) for user identification; and Bluetooth communication support for a range of telemedicine medical devices adhering to the IEEE 11073 standard. The aim of this study was to evaluate the electromagnetic compatibility (EMC) immunity of the CRIP platform in order to validate it for medical application use. The first prototype of CRIP was demonstrated to operate as expected by showing the user identification function feasibility, both via NFC and biometric, and by detection of Bluetooth devices via radio frequency (RF) scanning. The NFC module works in the 13.56 MHz band and the Bluetooth module work in the 2.4 GHz band, according to the IEEE 802.15.1 standard. The standard test qualification of the CRIP was performed based on the radiated EMC immunity with respect to the EN 61000-4-3 standard. The immunity tests were conducted under industrial EMC compliance with electric field aggression, with levels up to 10 V/m in both horizontal and vertical polarisations when the test antenna and the CRIP were placed at a distance of 3 m. It was found that the CRIP device complies with the European electromagnetic (EM) radiation immunity requirements.

1 Introduction

After the invention of semiconductors and increasing public demands on information and communication technologies, human daily life is constantly changing. Nowadays, communication technology serves to improve the efficiency of not only industrial systems, but also various services including those in the medical area [1–3]. The RF wireless technology constitutes one of the main building blocks behind the spectacular progress that has been made in medical engineering [4,5]. In 2010 researchers from the California Cancer Centre reported that RFID readers had helped enhance patient experiences [6]. From several studies, it was concluded that innovative RFID solutions allow hospitals to reduce stress and improve facility efficiencies [6].

Moreover, every year medication errors and incorrect treatments cost the health system several million dollars [1]. In the internal medicine departments of German hospitals, 29 000 patients die each year as a result of being given the wrong medication, according to a study made by the Medical University of Hanover [1]. According to the World Health Organisation, the number of patients suffering from diabetes has doubled since 1980 [7]. Patient treatment has considerably improved, with the correct transfusion in exactly the prescribed quantity facilitated by the use of RFID readers [7]. Modern information and communication technology is also making its mark in New York's biggest public hospital, where patients carry their medical history with them in a radio-tagged armband [1]. When they are admitted to the Jacobi Medical Centre as in-patients, they are issued with a paper armband with an integrated RFID chip in which are stored their name and patient number. All patient data is kept in an electronic file on the central database server [1]. Using mobile devices, the doctors can easily access all of the relevant medical data, such as case history, diagnoses, lab reports and allergy results, via the patient number

[a] e-mail: blaise.ravelo@yahoo.fr

and the wireless local area network (WLAN) at any time [1,8–10]. Recently, standardisation of new telemedicine communication systems has been initiated [11]. Facing up to the emergence of wireless mobile devices, this initiative was also extended to radiated EMC engineering.

As for all wireless electronic systems, the capacity of wireless medical devices to meet the standard requirements for operating in harsh electromagnetic (EM) environments, as can be found in hospitals and residential homes, needs to be validated according to the relevant standards. The most critical effect is the immunity of the devices under radiated EMC aggression. Recently, two investigations on RF communication systems for simple sensor devices adopted in hospitals were introduced [12,13]. Furthermore, the reliability of those systems' physical layer [14,15] needs further analysis as a function of the electromagnetic interferences (EMIs) in the real environment. So, certain challenges are still needed to achieve the implementation of highly robust e-healthcare systems [16]. For this reason, we are developing an innovative e-healthcare platform [17–19]. The technological platform will be connected to cloud networks offering market place access and all interfaces for user services [19]. The implementation of such a wide-ranging technological device requires various skills, most notably in medical informatics, numerical and analogue electronic circuits design, and RF test engineering. Furthermore, computational EM modelling approaches were proposed taking into account undesirable EM effects on wireless communication based on EM propagation environmental effects such as path loss, multipath fading, shadowing and EMIs with neighbouring systems [20–23]. The RF coverage of the CRIP RF function in a basic scenario of a corridor with medical rooms was analytically investigated in [24] by considering the ITU RF EM propagation model. However, due to the inherent complexity of the scenario this computational modelling is insufficient, and the radiated EMC immunity of the CRIP must be determined experimentally.

To be valid in the European market, EMC immunity conformity tests of the CareStore hardware product were carried out. The metrology of the radiated EMC immunity tests of the CRIP prototype RF modules is investigated in this paper. Thus, the aim of this study was to evaluate the EMC immunity of the CRIP in order to validate it for medical application use.

To do this, we introduce the experimental setup for the radiated immunity characterisation of the hardware terminal constituting the CRIP platform. First, we will introduce the EMC standard used herein according to the R&TTE directive 1999/05/EC [25]. After a brief description of the functioning principle of the CRIP box under test, we will describe the experimental setup considered to carry out the radiated EMC immunity test, including the specifications of the measurement equipment employed. In addition, we will interpret the behaviour of the device under test (DUT) during and after the immunity test. Further discussions on future work are addressed in the conclusion.

2 Description of the CareStore platform

CareStore is a candidate to become a common European standard and technical solution for automatically and seamlessly identifying care devices and people in a secure manner using RFID and biometric technology [18]. CareStore is an integrated platform intended to be user friendly with easy deployment of devices and applications. It offers healthcare applications that involve the citizens and their caregivers in personal health monitoring using an ambient-assisted living (AAL) platform. It also aims to reduce costs, improve living standards and independent life of the elderly population [26], and provide a higher degree of flexibility to users. The functioning principle of CareStore is explained in [17–19]. It consists of an open source platform and user interface connector to a cloud network for the home setting named common ambient assisted living home platform (CAALHP), a cloud platform from which applications and users' health data can be accessed by authorised persons such as doctors, nurses or caregivers, and an identification platform and health devices interface named CRIP.

2.1 CRIP platform

The Carestore platform offers the flexibility of coupling identities with devices, systems and users as well as uploading and storing drivers and applications. The CRIP platform is the component responsible for identifying users and recognising wireless medical devices. It allows designing, implementing and evaluating, in a unique and secure combined device, staff and inhabitant identification technology based on a combination of NFC and biometry. It offers the capacity to interface with the most recent standards for medical devices with extra interface hardware such as NFC and biometric fingerprint support, Bluetooth, as well as a remote application programming interface (API) for client access via representational state transfer (REST) requests.

The first prototype of CRIP consists of electronic circuit boards for NFC and fingerprint biometric user identification and Bluetooth communication. Figure 1 depicts the first prototype of the CRIP box.

2.2 CRIP hardware architecture

The CRIP base station that monitors and collects data about the patients is equipped with standardised antennae that communicate with the wireless devices using a biometric secured connection. It acts as a physical layer and sub-system of the CareStore platform. It was implemented based on a combination of several technologies including an RFID reader/writer, fingerprint biometrics sensor and a Bluetooth module. The collective functions are organised in the block diagram of Figure 2. The NFC/biometric module was implemented in conformity with the standard ISO/IEC 18092.

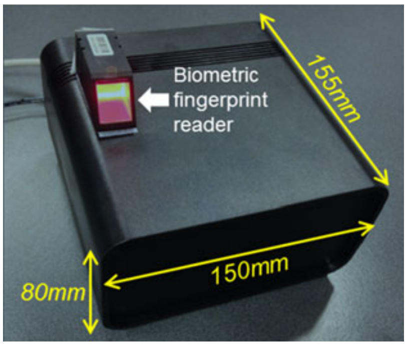

Fig. 1. First prototype CRIP box under analysis.

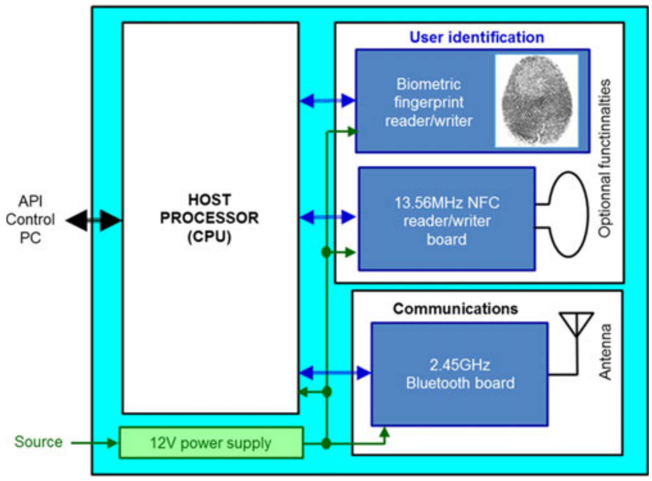

Fig. 2. Block diagram of CRIP.

The RF/analogue module of the CRIP under consideration operates under the regulation of the 2.4 GHz band IEEE 802.15.1 standard and is limited to the configuration of indoor communication in the medical room with about less than 100 m dimensions. So, similar to all RF electronic products, the EM wave transmission quality with the CareStore platform user mobility can be preserved.

One of the options proposed to identify the nurse and/or the patient for the CareStore platform is based on the use of 13.56 MHz NFC technology. Thanks to its flexibility, PN532 NFC was chosen to test its applicability. During full operation, the CRIP listens continuously for NFC clients/tags. When a NFC tag is placed over the reader, the recognition process will be performed.

The wireless transmission of the measured patient data to the CRIP box is required to operate in a medical room with a range of some meters. In order to support multiple Bluetooth stacks (versions 2.x and BLE) and optimise energy consumption in the nurse room coverage range, BLE112 module was chosen for the CareStore platform. This module works under the IEEE standard 802.15.1. The manufacturer technical specifications of this Bluetooth communication module describe the transmitter (Tx) and receiver (Rx) signal power sensitivities.

2.3 CRIP operating modes

The behaviour of CRIP can be described using a simple state machine diagram, as depicted in Figure 3. When CRIP starts it is waiting (Wait state) to receive an HTTP request or hardware interrupt. When an HTTP request is received, CRIP attends to it (AttendRequest state) and then goes back to state Wait. A hardware interrupt can occur either when a finger is placed on the biometric reader, or when a smartcard is placed over the NFC reader. If the former occurs, the user's biometric template is read (ReadTemplate state), validated against previously stored templates on the hardware (ValidateTemplate state) and, if the user is valid, its ID is sent to CAALHP (SendUserIdCaalhp state); otherwise the template reading is ignored. When a smartcard is detected, it is read (ReadSmartcard state) and, if the smartcard is successfully read, the user's ID is sent to CAALHP (SendUserIdCaalhp state), otherwise it is ignored.

Beside this process, another process is executed in parallel that sends a Bluetooth ping to the PIN Test PC (described later in Fig. 4). This process ensures that the Bluetooth radio module is always active, so that its EMC immunity can be correctly evaluated. For test purposes it provides a simple application that resembles CAALHP and communicates with CRIP via the exposed RESTful API. At any moment, a user can perform an authentication either by placing their finger on the biometric reader, or by placing a smartcard on the NFC reader. When a smartcard is valid or a biometric credential is recognised, a request is sent to the application's server (running in the background) and it is presented on screen in JSON format.

3 Operation verification of the CRIP prototype

The operation verification of the CRIP during the radiated EMC immunity tests was carried out with both the NFC RFID and Bluetooth functions. To do this, the CRIP box was connected via ethernet cable to the API control PC. The overall system is placed in close proximity (some meters) to another PC equipped with Bluetooth. The illustrative diagram showing the global configuration of the CRIP box with its associated accessories in normal functioning is depicted in Figure 4. During the test, we use a notebook as a Bluetooth test device. The control PC enables us to configure the CRIP according to the login of the users predefined by the NFC or biometric function, and also to visualise the application test for occasional interaction with CRIP.

The operation verification of the CRIP is performed via the API control PC with the monitoring of the application test:

1. Read biometric templates
2. Store templates
3. Scan for Bluetooth devices
4. Check CRIP status
0. Exit

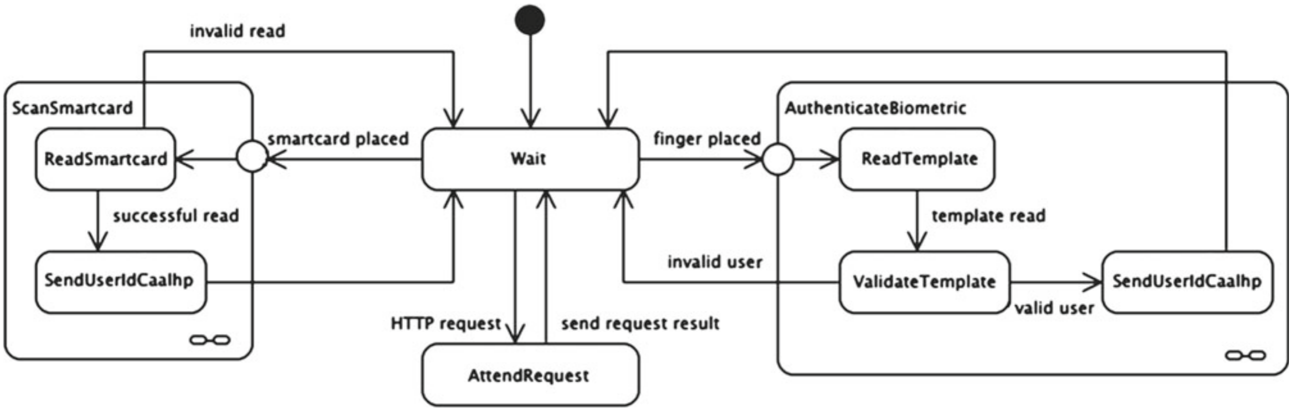

Fig. 3. The state machine describing CRIP's firmware.

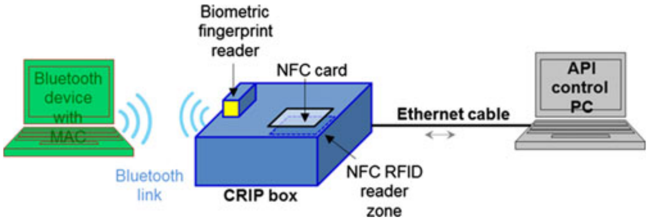

Fig. 4. Illustrative diagram of the CRIP test installation.

First, the CRIP status can be checked regularly by choosing option "4. Check CRIP status". The validity of the NFC function was checked with automatic and cyclic tests by placing the NFC card on the CRIP box. After some seconds of Bluetooth scan, the CRIP delivers the IP and the MAC address of the Bluetooth devices placed in its proximity. The test API monitoring confirms the CRIP box status before, during and after the tests. After backup of the users' identification process, we can observe that it can confirm the recognition by indicating:

□ their reference as the identifier number for the case of the NFC card which is identified here as "smartcard" option, and

□ the user identifier was also detected with "biometric" option.

After this preliminary verification, the CRIP box was placed in the semi-anechoic chamber for the radiated EMC tests.

4 Radiated immunity EMC qualification experimentation of the CRIP prototype

The present EMC qualification test was performed with respect to the requirement under R&TTE directive 1999/05/EC. We recall that the DUT investigated was developed in the frame of the project FP7-SME-2012-315158-CareStore [18,19]. As already described in the previous section, the prototype under study is classified as a medical residential device. Therefore, it should respect the standard regulation of radiated EMC certification test appropriate to ITE medical and residential devices. The EMC tests were performed at the IRSEEM laboratory for the conformity defined in the European standard EN61000-4-3, or more precisely the EM field immunity test EMC with testing and measurement techniques for radiating RF devices [25]. During and after the present immunity test, the DUT status was assessed regularly with the test application.

4.1 E-field calibration analytical approach

During the measurement tests, the Tx antenna serves as the aggressor. The electric field (E-field) aggression level (in V/m) was measured with a sensor placed in the vicinity of the DUT. The calibration formula allowing us to compare the expected E-field level from the theoretical approach and the measurement is given by [27]:

$$E(f) = \frac{7.02 \times k \times \sqrt{P_{\mathrm{ERP}}(f)}}{d}, \tag{1}$$

with the equivalent radiated power $P_{\mathrm{ERP}}(f)$ in watts, the measurement factors from the used test equipment (cable loss, connector mismatching effects, amplifier gain...) k, and the distance d in metres between the test antenna and the DUT at the operating frequency f. During the aggression test, the equivalent radiated power density from the signal generator can be extracted and monitored using the expression:

$$P_{\mathrm{ERP}}(f) = 0.61 \times G(f) \times P_{\mathrm{Tx}}(f), \tag{2}$$

where G is the antenna gain and P_{Tx} in watts is the input available power. The calibration relation is integrated into the ACCSYS-EMC$^{\mathrm{TM}}$ measurement control tool provided by HAMERA RF [28,29], which is preinstalled on the measurement control PC.

4.2 CRIP EMC qualification test procedures

The specifications on the technical references are addressed in Table 1. It corresponds to the industrial

Table 1. References of the radiated EMC test under consideration [27].

Type of test	Standard reference	Specifications
Radiated RF immunity with respect to industrial compliance	NF EN 61000-4-3	80 MHz to 1 GHz: 10 V/m, AM 80% 1.4 GHz to 2 GHz: 3 V/m, AM 80% 2 GHz to 2.7 GHz: 1 V/m, AM 80% 1 sides, Criterion A

(including residential cases) EMC qualifications known under the standard EN 61000-4-3 for the immunity tests. Accordingly, the level of the aggression electric field was adjusted to 10 V/m from 80 MHz to 1 GHz. As measurement scenario, the CRIP box was placed on the turntable in order to determine the orientation corresponding to the E-field maximal irradiation. In order to validate the EMC immunity test, the qualification criterion is that the DUT must exhibit correct operating characteristics during and after testing.

4.3 Radiated EMC immunity metrology

The EMC measurement test chamber has dimensions (9.7 m × 6.7 m × 5.4 m). The illustrative diagram of this radiated immunity test experimental setup is displayed in Figure 5. As we can see, the measurement configuration is set with the Tx antenna playing the role of aggressor device. Moreover, an ultra wide band signal generator was used to provide the test signals to feed the aggressor antenna from the frequency band 80 MHz to 2.7 GHz.

According to the standard EN 61000-4-3 definition, the CRIP box needs to be placed in the semi-anechoic chamber at the standard distance $d = 3$ m from the test Tx antenna and positioned at the height $h = 0.8$ m above the ground plane. The aggressor antenna is positioned at height h_a, which is varied from 1 m to 4 m for detecting the critical values of the operated E-fields. This DUT was set on a 4.20 m diameter turntable rotating from 0° to 360° in order to detect the received maximum signal power. All of the measurement parameters required to meet the standards, including the calibration of the obtained data, were acquired in the control office outside the semi-anechoic chamber. A control PC equipped with the ACCSYS-EMC$^{\mathrm{TM}}$ was used to calibrate and extract the measured E-field, to control the overall electrical and mechanical installations and to monitor simultaneously the power of the emission signal. The calibration procedure is based on the measurement chain comprising a signal generator, power amplifier (PA), measurement cables and the Tx antenna. Based on the references of those measurement elements, the software tool ACCSYS-EMC$^{\mathrm{TM}}$ integrates the electrical characteristics and performs the overall link budget of the measurement chain simultaneously with the mechanical control.

The control test equipment allows us:

- to set the levels of the transmitted aggression signal,
- to calibrate and store the E-field measured by the sensor,

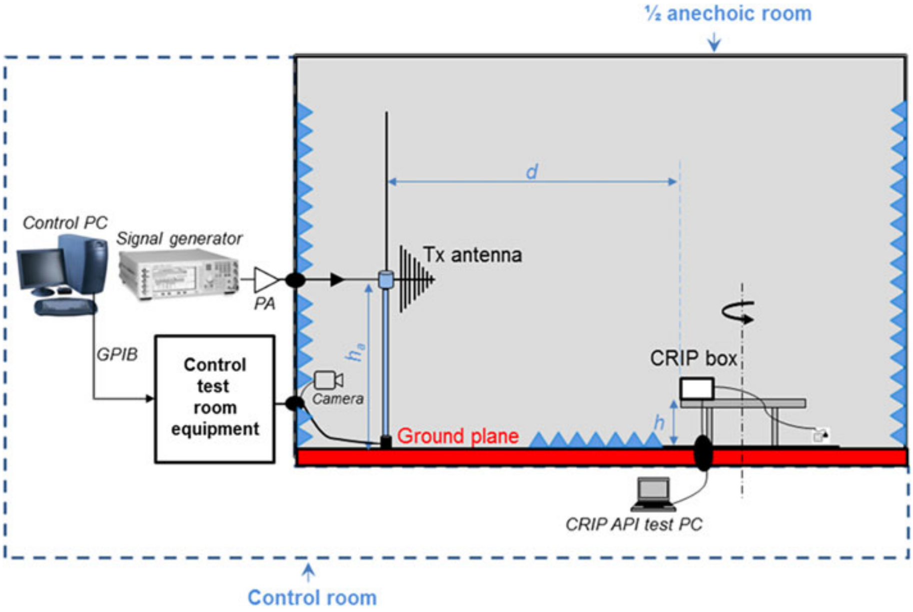

Fig. 5. Illustrative diagram of the experimental setup for the EMC immunity test.

Table 2. References of the antennae used for the EMC immunity tests.

	Manufacturer	Reference		Frequency band
Log-periodic antenna	Amplifier research	AT 5080	324752	80 MHz to 5 GHz
Dipole antenna	Schwarzbeck	STLP 9149	9149-207	700 MHz to 10.5 GHz
E-field sensor	Dare development RadiSense	CTR 1001B	10I00037SNO-14	10 kHz to 6 GHz

– to control the automatic translation of the antenna in the different vertical positions from 1 m to 4 m, and
– to control the turntable rotation.

The ACCSYS-EMC routine algorithm records the values of the transmitted power at each frequency. Then, the maximal value of the E-field provided by the sensor is selected for the different positions of the antenna and the turntable. It is noteworthy that the various positions of the antenna and the turntable allow us to consider the immunity of the CRIP on the E-field aggression from all directions. As the CRIP and the medical device's mobility during the data transmission are not significant enough, the Doppler Effect on the RF link can be neglected.

We emphasise that the radiated EMC immunity test was carried out in two sub-bands successively due to the test antennae's limited bandwidth. The log-periodic and dipole antennae, whose characteristics are addressed in Table 2, were employed for generating the EM irradiation required during the immunity test. Two different antennae were used in order to cover the standardised whole frequency bandwidth, which cannot be achieved with one antenna. The level of the E-field in the vicinity of the DUT, was checked with the E-field sensor whose reference is in the last row of Table 2.

4.4 EMC immunity experimentation results

In the semi-anechoic room, we ensure that the CRIP box, E-field sensor and the API test PC are placed on the table and exposed in the radiation coverage of the aggressor antenna. To ensure the CRIP status, an NFC card was placed on the NFC zone of the box as illustrated in Figure 5. Outside the test chamber, the measurement installation was monitored in video cast using the camera installed in the test room. Then, the CRIP status can be visualised continuously with the API test PC placed in the control corridor and linked with the DUT via the ethernet cable.

To check the CRIP immunity for any EM residential irradiation, we have considered different aspects of E-field polarisations. According to the Tx antenna's orientation, both horizontal- (H-) and vertical- (V-) polarisations were performed. According to the standard EN 61000-4-3, we fixed the levels of the E-field aggression in the expected frequency band as summarised in Table 3.

We point out that to achieve broadband emission, the signal generator was configured in AM modulation. The EMC immunity aggressions were three times higher than expected for the communication residential electronic devices. During the test campaign, the temperature and humidity values were regularly recorded in order to verify that the measurements were under normal conditions. The EMC immunity test results of the CRIP in normal operation modes presented herein were carried out within the ranges of temperature from +15 °C to +35 °C and relative humidity from 20% to 75%, as required in [26].

4.4.1 EMC immunity tests with E-field aggression in H-polarisation

During this EMC test, the DUT position was kept fixed. However, the aggressor antenna (assumed to be the Tx antenna) should be oriented in H-polarisation. The victim was the DUT and its accessories. During this test, we used the control PC to adjust and visualise the input signal power to achieve the standard values of E-field strength. Figure 6a displays the variation of the available aggression signal power versus frequency from 80 MHz to 2.7 GHz.

As can be observed here, the emission signal power to reach the expected standard level of the E-field is more than 40 dBm. The level of the EM wave aggressor in the vicinity of the CRIP was permanently verified with the E-field sensor. The plot of the average value of the E-field strength extracted, corresponding to the Tx signal power, is visualised in Figure 6b. We can see that in the frequency bands of interest, the E-field levels perfectly fit the expected standard values shown in Table 3 of the previous paragraph. As previously noted, we emphasise that this level is above the classical standard for the residential device EMC qualification, which is fixed at 3 V/m. During the operation verification, the overall experimental installation was monitored with the camera live viewing.

The CRIP function status was checked regularly during the test with the test application. According to this application, the CRIP successfully detects, using scan

Table 3. Expected E-field aggression characteristics during the EMC immunity test.

$F_{\min}$ (MHz)	$F_{\max}$ (MHz)	E-field level (V/m)	Time (ms)	Modulation
80	1000	10	1.0	AM 1 kHz 80%
1400	2000	3		
2000	2700	1		

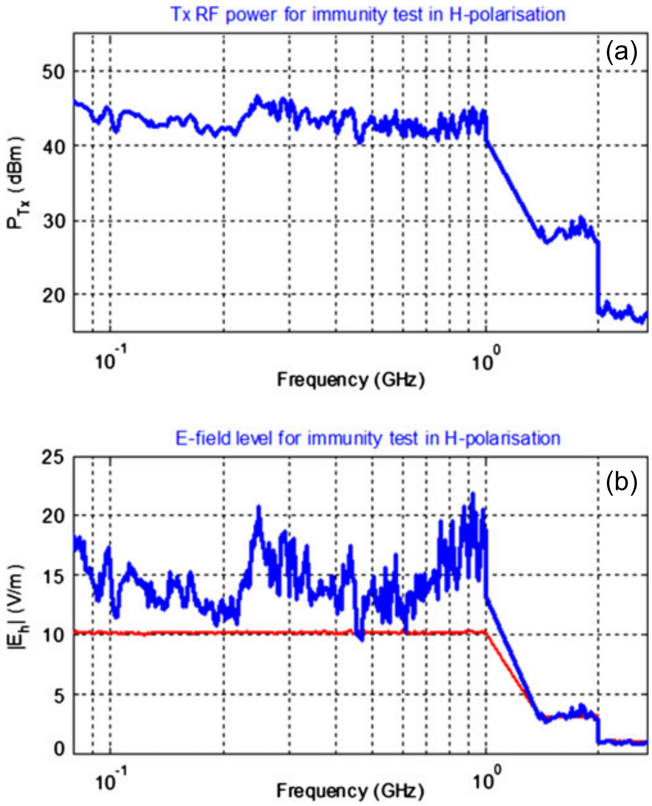

Fig. 6. Emission signal power and the E-field aggression average level during the immunity test in H-polarisation.

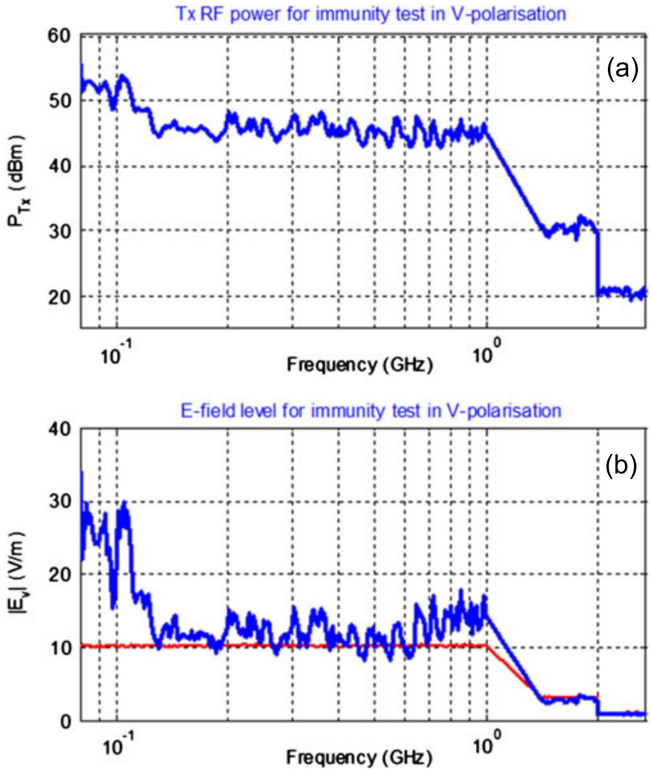

Fig. 7. Emission signal power and E-field aggression average level during the immunity test in V-polarisation.

functionality, the Bluetooth address of the PIN test PC. We emphasise that there is no observed defect during and after this radiated EMC immunity test in H-polarisation.

4.4.2 EMC immunity tests with radiation in V-polarisation

The only difference here, relative to the previous case, is the orientation of the aggressor antenna. The experimental setup is depicted in Figure 5, and a log-periodic antenna was used for the radiated immunity test performed in V-polarisation. In this case, the corresponding Tx signal power generating the aggression field is plotted in Figure 7a. Thus, the plot of the average value of the E-field amplitude from 80 MHz to 2.7 GHz for the E-field aggression in V-polarisation is displayed in Figure 7b. Once again, the noisy E-field level fits perfectly the standard addressed in Table 3. We find that the real E-field average value is above the expected level of 10 V/m in the test frequency band 80 MHz to 1 GHz. It remains higher than 3 V/m up to 2.7 GHz.

As for the previous case, the status of the CRIP platform under study was remotely monitored during the test. No defect was observed during or after this V-polarisation radiated EMC immunity test. No significant dysfunction was observed during the test. This first version of the CRIP box is in conformity with the European standard.

5 Conclusion

The radiated EMC immunity tests of the innovative e-healthcare hardware platform CRIP were performed and reported. The radiated EMC immunity tests were carried out with respect to the European standard EN 61000-4-3 [25]. The experimental setup in the semi-anechoic chamber and the control room for the proposed radiated EMC immunity standard was discussed in detail.

The Tx antenna vertical displacement, ranging from 1 m to 4 m, and the turntable rotation were under the control of equipment driven by the ACCSYS-EMC$^{\mathrm{TM}}$ software. Then, the operating frequency was swept from 80 MHz to 2.7 GHz. At each frequency, the Tx signal power and the E-field at 3 m from the source were recorded and calibrated. During the experiment, the level of the E-field aggression (10 V/m from 80 MHz to 1 GHz) were kept three times higher than expected for residential RF communication devices. The E-field aggression, up to the 10 V/m level, confirms that in the future, industrial applications of the CRIP function [25] can be envisaged. The levels of the electrical and EM signals required during the radiated EMC immunity tests in both H- and V-polarisations were presented. Then, the status of the CRIP was verified regularly with the monitoring PC connected via ethernet cable, as illustrated in Figure 4. The detection of the Bluetooth devices and the CRIP status were checked before, during and after the tests. During and after the EM aggression, it is worth noting that the NFC-RFID and Bluetooth functions of the CRIP were still intact. It was concluded that the CRIP product conforms with standard EN 61000-4-3 under the R&TTE directive 1999/05/EC, which is an essential regulation for all residential RF communication electronic equipment.

The next step of this research work will be the EMC tests of the second version of the CRIP, including the overall cloud network of the CareStore platform. Following this, CRIP will be field tested at a senior citizens care facility [26].

This research work was supported by European Framework Program FP7 Research for the Benefit of Small and Medium Enterprises (SMEs), project FP7-SME-2012-315158-CareStore.

References

1. `http://www.asianhhm.com/information_technology/medical_errors_rfid.htm`, accessed 2015
2. Intertek. *Home Healthcare Equipment* [Online]. Available: `http://www.intertek.com/medical/electrical-testing/home-healthcare/`, accessed May 2014
3. SkyeTek. *Consignment Inventory and VMI for Medical Implant Manufacturers* [Online]. Available: `http://www.skyetek.com/sites/default/files/consigned_and_vmi_medical_implant_manufacturers.pdf`
4. B. Michaels, Qmed, MPMN **28**, 28 (2012)
5. T. Hillstrom (2012, Nov. 1). *Tracking Medical Equipment & Patients with Passive RFID* [Online]. Available: `http://www.impinj.com/blog/tracking-medical-equipment-patients-with-passive-rfid/`
6. ThingMagic (2010, Feb. 24). *ThingMagic RFID Readers Help Enhance Patient Experience at California Cancer Center* [Online]. Available: `http://www.thingmagic.com/press-room/27-press-releases/285-thingmagic-rfid-readers-help-enhance-patient-experience-at-california-cancer-center`
7. D. Moncoqut (2012, Sept.). *Amélioration d'Efficacité Energétique des Systèmes RFID Médicaux* (in French) [Online]. Available: `http://www.electronique-mag.com`
8. `http://www.schreiner-logidata.com/3/industries/health-care`, accessed 2014
9. `http://www.rfidarena.com/2011/12/15/rfid-the-medical-miracle.aspx`, accessed 2011
10. `http://www.vizinexrfid.com/medical-uses-for-rfid-products/581/`, accessed 2014
11. *Medical Devices* [Online]. Available: `http://ec.europa.eu/enterprise/policies/european-standards/documents/harmonised-standards-legislation/list-references/medical-devices/index_en.htm`
12. H. Kostinger, M. Gobber, T. Grechenig, B. Tappeiner, Developing a NFC based patient identification and ward round system for mobile devices using the android platform, in *2013 IEEE Point-of-Care Healthcare Technologies (PHT), Bangalore, India, 2013*, pp. 176–179
13. K. Jeonggil, L. Chenyang, M.B. Srivastava, J.A. Stankovic, Proc. IEEE **98**, 1947 (2010)
14. J. Morrissey, Wireless communication and medical device EMI in the hospital, Activity report, Motorola Labs, 2002
15. Z. Alavikia, P. Khadivi, M.R. Hashemi, J. Med. Signals Sens. **2**, 1 (2012)
16. P. Kaeding (2005, Oct.). *RFID Medical Devices – Opportunities and Challenges* [Online]. Available: `http://wtnnews.com/articles/2384/`
17. CareStore Project [Online]. Available: `http://www.carestore.eu/`, accessed 2014
18. `http://cordis.europa.eu/project/rcn/105930_en.html`, accessed 2014
19. M. Memon, S.R. Wagner, C.F. Pedersen, F.H.A. Beevi, F.O. Hansen, Sensors **14**, 4312 (2014)
20. M.C. Jeruchim, P. Balaban, K.S. Shanmungan, *Simulation of Communication Systems*, 2nd edn. (Kluwer Academic, Plenum Publishing, New York, 2000)
21. T. Chrysikos, G. Georgopoulos, S. Kotsopoulos, Site-specific validation of ITU indoor path loss model at 2.4GHz, in *Proc. IEEE Int. Symp. World of Wireless, Mobile and Multimedia Networks & Workshops, 2009 (WoWMoM 2009), Kos, Greece, 2009*, pp. 1–6
22. J. Zhong, L. Bin-Hong, W. Hao-Xing, C. Hsing-Yi, T.K. Sarkar, IEEE Ant. Prop. Mag. **43**, 41 (2001)
23. T.K. Sarkar, J. Zhong, K. Kyungjung, A. Medouri, M. Salazar-Palma, IEEE Ant. Prop. Mag. **45**, 51 (2003)
24. B. Ravelo, J. Cabral, S. Wagner, C. Pedersen, M. Morten, EMI and BER/PER analysis of WiFi and Bluetooth communication for CRIP platform, in *Proc. of 17ème Colloque international sur la compatibilité électromagnétique (CEM 2014), Clermont-Ferrand, France, 2014*, pp. 1–6
25. Electromagnetic compatibility (EMC) Immunity tests – Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test, standard EN 61000-4-3, 2007
26. Ehpad. Établissement d'Hébergement pour Personnes Agées Dépendantes (in French), `http://www.maisons-de-retraite.fr/Ehpad/La-sante-des-seniors`, accessed 2014
27. F.H. Sanders, Derivations of relationships among field strength, power in transmitter-receiver circuits and radiation hazard limits, Technical Memorandum TM-10-469, National Telecommunications and Information Administration (NTIA), June 2010
28. `http://www.hemera-rf.com/logiciel_mesure_CEM.html`, accessed 2012
29. `http://www.accsys-fr.fr/Home/Index_en`, accessed 2014