

AEGIS – Mobile Device for Generating Electromagnetic Curtain for Special Applications and Countering the Threats of RCIED

Piotr Rajchowski, Krzysztof K. Cwalina, Jarosław Magiera, Alicja Olejniczak,
 Paweł T. Kosz, Agnieszka Czapiewska, Robert Burczyk, Krzysztof Kowalewski,
 Jarosław Sadowski, Sławomir J. Ambroziak

Abstract—In the article, the concept, design and realization of the technological demonstrator of a mobile device for generating an electromagnetic curtain (with a name AEGIS) were presented, both in the hardware and software areas. The device is designed to block the radio communication which allow detonating the Radio Controlled Improvised Explosive Devices (RCIEDs). The preliminary laboratory tests of the demonstrator for generating the jamming signal, that were presented in the paper, aimed at assessing the correctness of the device operation and verification of generated signal parameters. On the basis of the obtained results, the ability to jam the cellular systems as well as other radio devices operating in the frequency band from 400 MHz to 2700 MHz was assessed.

Keywords—electromagnetic curtain generator, IED, jammer, RCIED

I. INTRODUCTION

DURING the operational activities of public entities like the Police, Border Guard and Army officers carry out their actions with lost packages in urban areas. Often there is a need to analyze unidentified packages left on the airport or other public areas before their disposal. In many cases, left packages are suspected to be a radio-controlled improvised explosives devices (RCIEDs). In order to increase the security level of officers and bystanders, special equipment is used to establish a so-called electromagnetic curtain. This process can be understood as generation of a jamming signal, often with a wide spectrum, preventing the realization of radio communication services, e.g. using the cellular systems. It is worth noting that in many cases it is necessary to maintain the communication between the officers for operational purposes. For this reason, it is desirable to be able to adjust the parameters of the jamming signal, by isolating in the wideband jamming signal non-jammed frequency channels, the so-called protected bands [4-8].

In the paper, the concept and realization of a mobile device

This research work has been funded by The National Centre for Research and Development (NCBiR) within the project No. DOB-1P/02/03/2016.

Elements of the demonstrator are protected by the polish patent 220907 “Device for forming the radio signal” (in polish).

All authors are with Gdansk University of Technology, G. Narutowicza 11/12 Street, 80-233 Gdansk, Poland (e-mail: {piorajch, kkcwalina, kowal, jaroslaw.sadowski}@eti.pg.edu.pl; {jaroslaw.magiera, alicja.olejniczak, agnieszka.czapiewska, robert.burczyk, slawomir.ambroziak}@pg.edu.pl).

for generating an electromagnetic curtain are presented. The device is able to generate a wideband (up to 1 GHz of occupied bandwidth) jamming signal in the frequency range from 400 MHz to 2.7 GHz. During the developed research and development project a technological demonstrator, that meets the needs of governmental security entities, was built.

II. MOBILE DEVICE FOR GENERATING AN ELECTROMAGNETIC CURTAIN

A. Key Assumptions

The main goal of the developed device for generating electromagnetic curtain is to counter the threats caused by the RCIEDs, that can be activated e.g. by using cellular systems, cheap ISM (Industrial, Scientific, Medical) band radio modules, or in general any device operating in the frequency range 400 MHz – 2700 MHz. The assumed jammed bandwidth is achieved by using several simultaneously operating jamming channels.

Modern laboratory equipment allows to build a laboratory stand with described functionality, but its operational abilities are limited by the dimensions of the device. One of the key assumptions of the project is to build a demonstrator with the size of a handheld suitcase. To fulfil these requirements jamming channels are miniaturized and consist of specialized electronic components. Moreover, to maximize the utility of the demonstrator it is placed on a remote-controlled self-propelled platform [1, 5, 6].

B. Design of the Electromagnetic Curtain Generator

The device for generating an electromagnetic curtain can be identified as a simplified vector signal generator. The basic concept assumes using the FPGA (Field- Programmable Gate Array) matrix for generating the samples of the waveform and a DAC (Digital to Analog Converter) converter to produce an analog signal in the baseband. In the presented device, a SoC (System on a Chip) module from Xilinx Company (Zynq family) was used. In its structure, there are FPGA matrix and processor with ARM (Advanced RISC Machine) core. Such a dual structure allows to generate the samples of a jamming signal on the processing system core (PS – ARM processor) that can be controlled by a real-time operating system. Further, the samples are sent to the programmable logic core (PL – FPGA matrix) for additional transformations. To send the samples of a wideband radio signal a high throughput with low



latency connection is required. To achieve that a DMA (Direct Memory Access) mechanism is used. The samples, in a complex form, generated by the developed software, described in section III, are further sent to the DAC converter using the parallel interface compatible with the LVDS (Low-Voltage Differential Signaling) signal lines. The DAC generates a baseband jamming signal. Afterwards, the signal is sent to quadrature modulator (QM), that shifts the signal into the desired frequency range. To simplify the design of the radio frequency path and eliminate the need for high-frequency signal distribution authors selected a QM with integrated VCO (Voltage Controlled Oscillator) and PLL (Phase Locked Loop) circuits. The output signal from QM is directed to the external power amplifier. It must be noticed, that power amplifier (PA) class also influences the shape of the jamming signal. It is desired to use a PA operating in the A linear class with the maximum output power at 1 dB compression point [2, 3].

In Fig. 1 a general block diagram of the device for generating electromagnetic curtain is presented. It contains functional elements and visualize the basic assumptions of the device. The two marked independent jamming channels are communicating with each other and with manipulator (the controlling device) by using the Ethernet interface. The connection is used to send control commands (CC) to each jamming channel and vice versa. In a CC user can specify parameters such as the jammed bandwidth, protected bands (bands free of jamming signal) and control the basic functionality of the device. The design of the manipulator will be described further in the article, in section II.C [1-3, 5-6, 9-11].

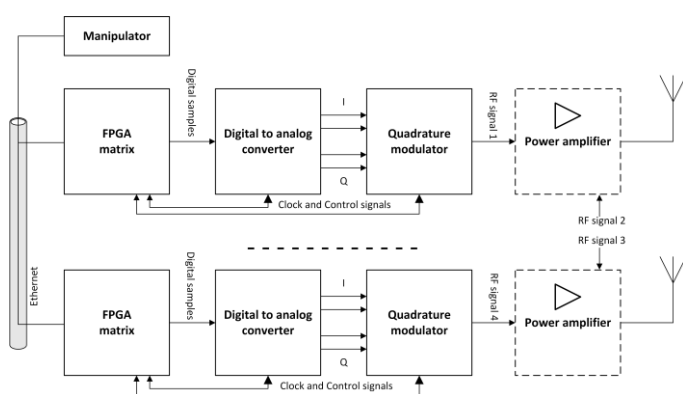


Fig. 1. Block diagram of designed electromagnetic curtain generator.

The laboratory demonstrator, based on the concept presented in Fig. 1, was constructed during the first stage of the conducted project. It was built as a set of four simultaneously working jamming channels with a similar structure (producing jamming signals *RF signal 1 - 4*) based on components available as evaluation boards from Analog Devices Company. Parameters of the jamming signal, e.g. its bandwidth, center frequency were adjustable by using software running on a PC computer. Instead of basic parameters, the user can also specify if the jamming signal is a noise-like or chirp type [1].

It is worth mentioning that developed laboratory demonstrator was used to verify the assumption that by using the proposed equipment it is possible to build a device that has the operational ability to disturb the radiocommunication systems that can be used to detonate the RCIED devices. Authors assessed that the laboratory demonstrator has assumed

abilities in the scope of generating a jamming signal but its structure and used laboratory equipment highly limit its applicability in real conditions [1].

C. A prototype of the Electromagnetic Curtain Generator

The final stage of the project was focused on building a miniaturized device, with the size of a travel suitcase, with functional capabilities suitable for public entities. After the first stage of the project, the main technical assumptions were not modified what means that the concept of using four identical and simultaneously working jamming channels was sustained but a hardware modification was done. Instead of using an evaluation boards from Analog Devices it was decided to design own RF signal board containing e.g. PLL (Phase Locked Loop) clock generator, DAC, set of low pass filters, QM, first stage amplifier and a control unit (a microcontroller). The block diagram of the jamming channel with RF signal board and mainboard is presented in Fig. 2. The block diagram is mainly based on the concept presented in Fig. 1, but it was expanded by the control unit and a set of 5th order Butterworth low pass filters.

The developed RF board software configures registers of used integrated circuits to set required parameters of the RF path and report current status to the operator. It is also worth noting that block *Adaptive gain control* is responsible for compensating the nonlinearities of the output power characteristics of the quadrature modulator, and 1st stage amplifier to ensure 0 dBm signal power at the input of the power amplifiers.

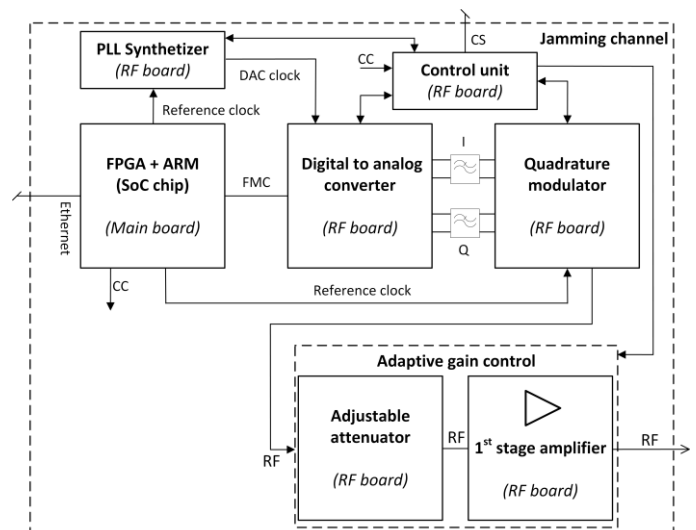


Fig. 2. Block diagram of the jamming channel with matched elements of the RF and main board.

The full block diagram of the electromagnetic curtain generator is presented in Fig. 3. The device consists of four jamming channels, two power amplifiers, a power supply section and a power control unit. Due to the technological limitations, it is obligatory to use two independent power amplifiers to cover the desired frequency band (400 MHz – 2700 MHz), and they totally deliver up to 53 dBm (200 W) of output power. To extend the functionality of the demonstrator, the signal from the jamming paths can be switched between the inputs of the power amplifiers. Switching algorithm is implemented in the *Control units* of the jamming channels. The *Control unit* is also communicating with the *Main*

controller of the demonstrator, whose role is to coordinate the operation of four jamming channels, monitor the state of the Power control unit and power amplifiers. The technological demonstrator can be powered by internal 24 V batteries, from the mains (230 VAC) or by external 24 V batteries [6].

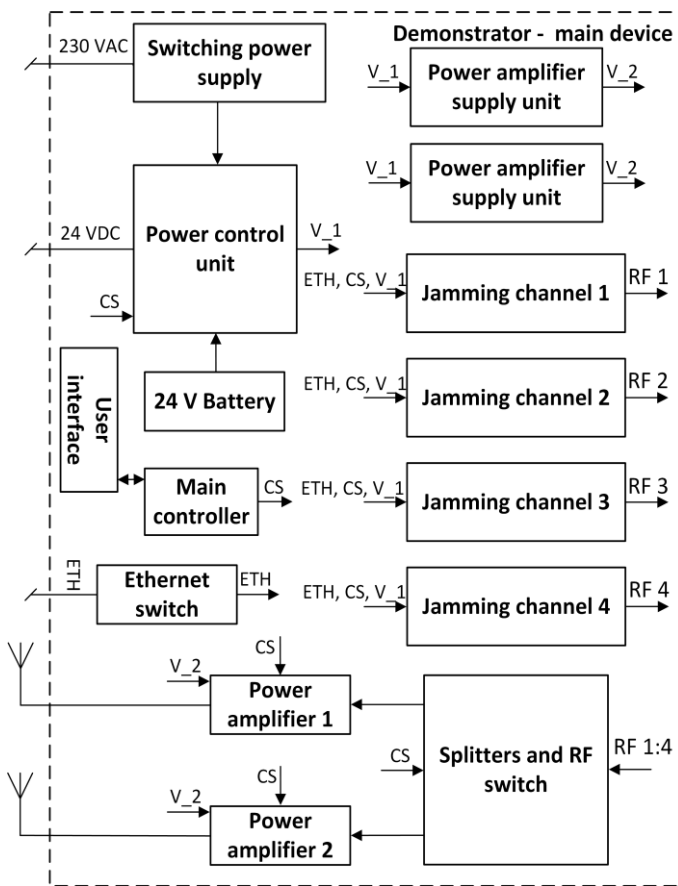


Fig. 3. The block diagram of the electromagnetic curtain generator.

In this point, two additional elements of the demonstrator presented in Fig. 4 shall be described: the manipulator and the self-propelled platform. The manipulator is designed to control the demonstrator by the end-user. One can adjust the parameters of the jamming signal, review the state of jamming channels and also control the self-propelled platform.

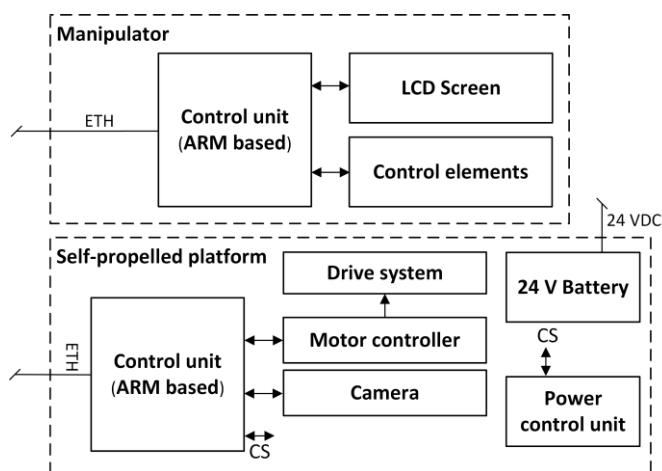


Fig. 4. The full block diagram of the manipulator and the self-propelled platform.

As *Control elements* a touch screen, software keys, keyboard and joysticks were used. The front panel of the manipulator is shown in Fig. 5. All CCs are sent via the Ethernet interface to the electromagnetic curtain generator and the platform. The principle of operation of the software was described in section III.

In the operational conditions, it may be desired to rapidly and simply turn off/on the demonstrator. Additionally to the manipulator, the demonstrator is equipped with a master power switch and jamming on/off keys (marked as a *User interface* in Fig. 3). After power-up by default, the jamming channels are set to generate a signal in a frequency bands dedicated for operation of the GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunications System), LTE (Long Term Evolution) networks. By pressing the jamming on key, the user can instantly jam mentioned bands.



Fig. 5. The front panel of the manipulator.

The platform (block diagram presented in Fig. 4) is designed to remotely carry the demonstrator in the proximity of the unidentified package without exposing the officer. The integrated camera can be used for remote recognition of the field or just used for remote steering purposes. The off-road capabilities of the platform are sufficient for driving in an urban area. The demonstrator can be easily driven over the curbstones, sidewalks or lawns.

The overall form of the prototype AEGIS in a ready for operation state is presented in Fig. 6. The main part of the demonstrator for generating the jamming signal is mounted inside the protective case. It is worth noting that the case can be handled individually without the platform, so it is capable of storing the RF and power cables, two antennas and tripods. In presented in Fig. 6 scenario, the case is securely placed on the platform. The transmitting antennas are mounted on the two detachable masts, using the RF cables connected to the demonstrator's case. To simplify the connections the RF cables are equipped with the SnapN quick-lock type connectors. Between the manipulator, platform and demonstrator some wired connections can be seen. These are the communication lines used for sending commands from the manipulator and the power connections between the platform and demonstrator.



Fig. 6. Technological demonstrator ready for operation.

In this point it is worth to sum up the technical parameters of the demonstrator. They have been listed in the Tab. I.

 TABLE I
 BASIC TECHNICAL PARAMETERS OF THE TECHNOLOGICAL DEMONSTRATOR

Parameter	Value	Unit
Lower frequency	400	MHz
Upper frequency	2700	MHz
Maximum bandwidth of jamming signal	1000	MHz
Number of antennas	2	-
RF signal total output power	200	W
Supply voltage	24 DC / 230 AC	V
Battery operational time	min. 2.5	Hours

III. JAMMING CHANNEL SOFTWARE

Each of the four jamming channels operation (the generation of jamming signal) is managed by a dedicated software running on the SoC chip. In this section of the paper, the PS part of this software is described. It is identical for each jamming channel, thus only a single channel is considered.

There are two main roles of jamming channel software. The first one is to send the CC to the *Control unit* (Fig. 2) in the jamming channel in accordance with requests obtained from the manipulator. Second is to provide feedback information to the manipulator about the current status of the jamming channel.

The software comprises three components, as shown in Fig. 7. These are TCP client, Jamming channel manager (JCM) and Jamming waveform generator (JWG).

A. TCP Client

TCP client acts as an interface with the manipulator. It connects to TCP server which is part of manipulator software. As jamming channels have different IP addresses, manipulator serves each client independently.

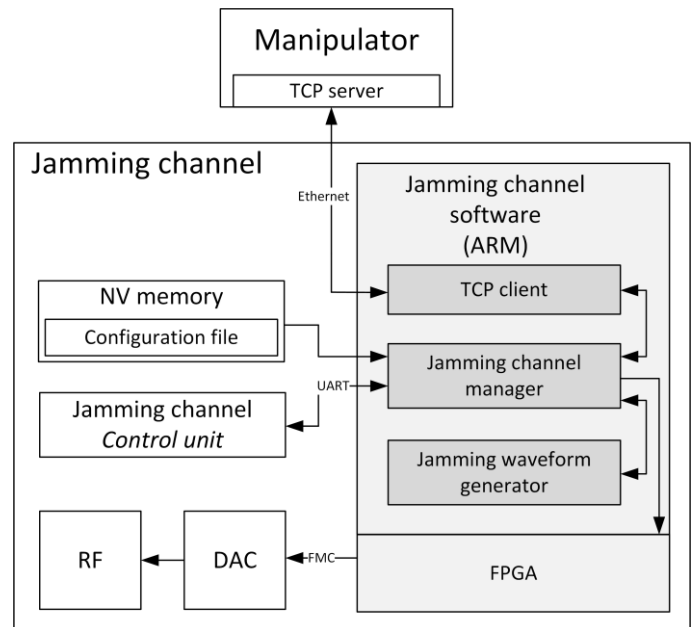


Fig. 7. Interfaces between jamming channel software and hardware.

When a request message is sent from the server, TCP client decodes this message and passes the request to JCM for further processing. Information from JCM about the request success or failure is sent back to the manipulator via TCP client. When there are no requests from the server, the client periodically sends status update messages to the manipulator, so that the user is informed about potential hardware problems. Moreover, TCP client is used to inform the manipulator about hardware capabilities of the particular jamming channel, i.e. about its operating frequency range and the maximum bandwidth of the jamming signal.

B. Jamming Channel Manager

JCM is the core component of jamming channel software. During the software initialization stage, it reads channel-specific parameters from a configuration file. These parameters include channel identifier (from 1 to 4), operating frequency range, the maximum bandwidth of the jamming signal, jamming waveform sampling frequency and IP address/TCP port of server on the manipulator.

After receiving a request from TCP client, it firstly performs a check on the current status of the channel. There are several possible status values, but in normal operation, only three of them may occur – namely: disabled, configured and jamming. The first two correspond to states when jamming is inactive. However, in the configured state the channel hardware is already set up for jamming yet the channel output is disabled. When channel status is set to jamming, the channel hardware is configured and the channel output (so is the power amplifier) is enabled providing the signal to the power amplifier.

The jamming channel state transition graph is depicted in Fig. 8. It presents the operation of JCM depending on the current channel status and type of the request received from the TCP client. Disabling or enabling jamming channel output is simply performed by sending a CC to the jamming channel *Control unit* via the UART interface (see Fig. 2 and 7). In contrast, configuring jamming channel hardware is a more complex operation.

Jamming channel configuration starts with generating a jamming waveform according to jamming scenario defined by the user. Waveform means a digital baseband representation of the jamming signal. It is a series of complex samples calculated by the JWG. The procedure of waveform generation is described in the subsection C. Once the desired waveform is ready, the samples are pushed to PL part of the SoC (using the DMA method) which interfaces with digital-to-analog converters (DACs) via the FMC (FPGA Mezzanine Card) interface. When a jamming channel is in a *configured* or *jamming* state, the waveform is transmitted in an infinite loop resulting in a periodic output signal.

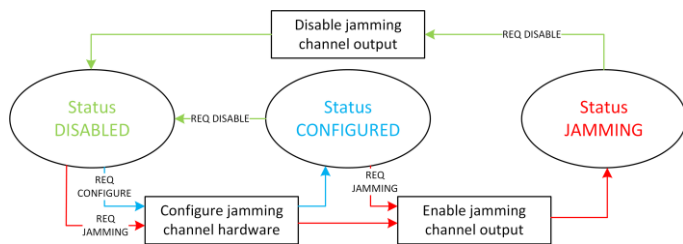


Fig. 8. Jamming channel state transition graph.

The last step of the jamming channel configuration is setting up the quadrature modulator parameters. For this purpose, the jamming channel manager sends the CC message to the jamming channel *Control unit* via the UART interface. This message contains information about the desired carrier frequency of the jamming signal. In turn, the *Control unit* sets the appropriate frequency of the integrated local oscillator which drives the quadrature modulator.

In a case of jamming request, after configuring the jamming channel, its output is enabled by sending another message to jamming channel *Control unit*. In turn, when disabling request is received similar message is sent by the JCM which switches off the jamming channel output (and so the power amplifier) and then the status is set to *disabled*.

C. Jamming Waveform Generator

During jamming channel configuration the JWG generates the desired jamming waveform based upon a set of parameters. These include jammed bandwidth and waveform duration. Their values determine jamming efficiency, thus they should be selected cautiously. The unnecessarily wide band may decrease the jamming range while too short waveform duration may lead to too large spaces in the bins of jamming signal spectrum.

The waveform is generated using one of the two methods. In the first one, a noise-like signal is generated as an inverse Fourier transform of the uniformly flat power spectrum. In the second method, linear frequency modulation is used which results in narrowband jamming signal sweeping the desired frequency range. Information about the selected method of waveform generation is included in the jamming request or configuration request.

Within the jammed frequency band one or more, free from jamming sub-bands may be defined, to provide for example a critical communication channel. If such protected bands are required, the JWG receives information about their number and baseband frequency ranges. Respective frequency bins located inside these bands are zeroed before waveform is

obtained through the IFFT calculation. Protected bands containing zero (center) frequency should be avoided due to DC interference caused by hardware impairments introduced in DACs and modulator branches [3]. For this reason, if protected band contains zero frequency, JWG introduces additional frequency offset to cause positioning of the zero frequency outside the protected band. This frequency offset is further compensated by JCM in the local oscillator frequency setting.

IV. LABORATORY TESTS OF THE DEMONSTRATOR

A. Preliminary Tests of the Demonstrator

The main goal of the preliminary measurement studies of the laboratory demonstrator was to investigate the shape of a jamming signal and check the correctness of operation of the device.

During the first test scenario, a jamming signal (wideband noise-like and a chirp signal) with an exemplary bandwidth of 80 MHz was generated. To investigate the imbalance of the quadrature and in-phase channel of the DAC and QM four 5 MHz protected bands were notched asymmetrically with respect to the 1 GHz center frequency. As it is presented in Fig. 9 noise level in the protected band is about 1 dB higher with respect to the sideband frequency range. Parameters of the signals were analyzed using the broadband power meter Keysight E4416A with a Keysight E9304A probe, by using the spectrum analyzer Anritsu MS2690A, Agilent DSO9404A oscilloscope and R&S NRT power meter [1, 3].

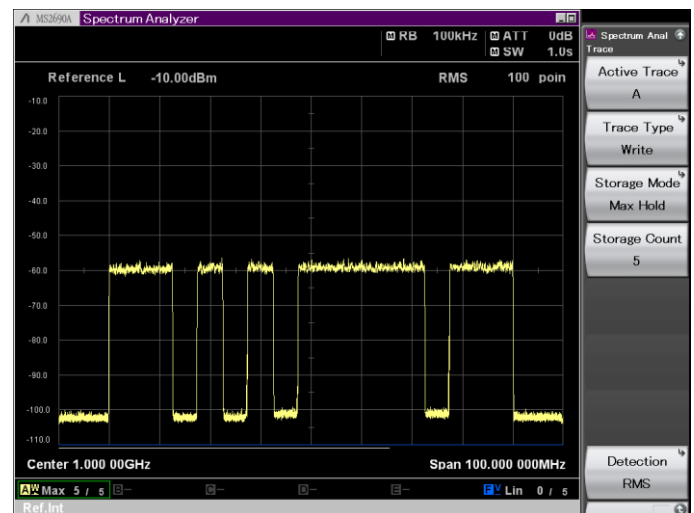


Fig. 9. The spectrum of the 80 MHz width noise-like jamming signal with notched protected bands.

In further laboratory tests, the shape of the jamming signal was investigated in a different frequency ranges, which tested additional configuration parameters of the QM. It occurred, that there is no significant noticeable difference in the shape of the jamming signal when the different center frequency was selected.

B. Final Laboratory Tests of the Technological Demonstrator

The goal of the final laboratory tests was to verify the usability of the developed demonstrator and check the end parameters of the jamming signals. During the first phase, the operation of the adaptive gain control section was investigated.

In Fig. 10 the output power (with and without compensation) of the jamming channel as a function of frequency is presented. It can be seen that there is a need for attenuating or amplifying the jamming signal to adjust its power to a constant level.

The curve was approximated by a nonlinear function and the formula with additional conditions was implemented in the software of the Control unit (Fig. 2). The additional conditions can be understood as selected switches and splitters (different attenuation) and used an algorithm for generating the jamming signal (different Peak to Average Power Ratio - PAPR value) [2-3]. Using the compensation algorithm, it is possible to keep the power of the jamming signal at a level just under the 0 dBm to avoid pushing the amplifier to work in the nonlinear region.

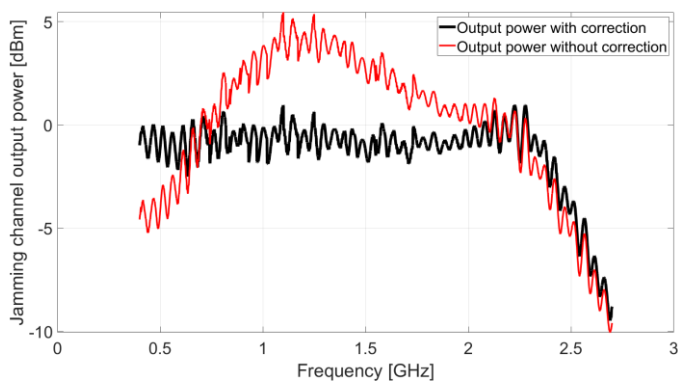


Fig. 10. Output power as a function of the frequency of a single jamming channel in the operational frequency range.

During the second phase of the laboratory tests, the usability of the demonstrator was verified. The device was controlled by using the developed manipulator and its interactive software. User configured sample jamming bands in a way that each jamming channel generated the RF signal. The summed RF signal from four jamming channels (after amplification) was observed by using the spectrum analyzer and a wideband power meter. During these tests also the self-propelled platform was tested, especially its bearing capacity and ability of cooperation with the demonstrator.

CONCLUSION

In this article, a technological demonstrator designed to emit a wideband jamming signal, which was developed during the research and development project with the name AEGIS, is presented. The device can be used to prevent the remote

detonation of radio-controlled improvised explosive devices by generating a wideband jamming signal. As an additional functionality of the demonstrator, the possibility of creating a so-called protected band in the jamming signal has been implemented to maintain own radio communication.

During the final construction stage and laboratory tests, the demonstrator was investigated in the scope of parameters of the jamming signal and usability for the end-user. The generated signals were analyzed using laboratory measuring instruments, and the obtained results met the assumptions regarding the output power of the jamming signal, its spectrum shape and the ability to jam cellular systems or other unlicensed radio systems in the frequency range 400 MHz – 2700 MHz with a maximum bandwidth 1 GHz. In order to verify a possible range of jamming, further field tests are necessary after obtaining a license for the emission of the EM fields in licensed frequency bands.

REFERENCES

- [1] S. Ambroziak, R. Katulski, J. Sadowski, J. Stefański, "Device for forming the radio signal (in polish)", Patent Office of the Republic of Poland, exclusive right number: 220907.
- [2] J. Magiera, "Simulation of wideband jamming signal generator for protection against the RCIED (in polish)", *Telecommunication Review and Telecommunication News*, vol. 6, pp. 521-524, July 2017, DOI: 10.15199/59.2017.6.85.
- [3] J. Magiera, "Wideband Signal Generation for Jamming Radio-Controlled Improvised Explosive Devices", 41st International Conference on Telecommunications and Signal Processing (TSP), 2018, pp. 607-610. DOI: 10.1109/tsp.2018.8441327
- [4] E. V. McDonald, T. Bullard, "Military Geosciences and Desert Warfare", Springer, 2017.
- [5] P. Rajchowski, K. K. Cwalina, P. Kosz, S. Ambroziak. *Mobile Device for Generating Electromagnetic Curtain for Special Applications*, Conference materials, CBRNe Convergence, Indianapolis, 2017, USA.
- [6] P. Rajchowski, K. K. Cwalina, J. Magiera, P. T. Kosz, A. Czapiewska, R. Burczyk, J. Sadowski, S. J. Ambroziak, "AEGIS – Mobile Device for Generating an Electromagnetic Curtain for Special Applications and Protection Against the RCIED (in polish)", *Telecommunication Review and Telecommunication News*, vol. 6, pp. 366-369, July 2019, DOI: 10.15199/59.2019.6.52.
- [7] H. Schubert, A. Rimski-Korsakov, "Stand-Off Detection of Suicide Bombers and Mobile Subjects", Springer, 2005.
- [8] K. Wilgucki, R. Urban, G. Baranowski, P. Grądzki, P. Skarżyński, "Automated Protection System Against RCIED", Military Communication Institute, 2011.
- [9] Xilinx, "Technical datasheet, AXI DMA v7.1, LogiCORE IP Product Guide". Xilinx Vivado Design Suite, 2018.
- [10] Xilinx, "Processing System 7 v5.5, LogiCORE IP Product Guide". Xilinx Vivado Design Suite, 2017.
- [11] Xilinx, "AXI Interconnect v2.1, LogiCORE IP Product Guide". Xilinx Vivado Design Suite, 2017.