# DETECTION AND CLASSIFICATION MODEL OF RADIOELECTRONIC JAMMING SIGNALS WITH ELINT SUBSYSTEM INCLUDED WITHIN THE INTEGRATED AIR ELECTRONIC WARFARE RANGE (IAEWR)

Jarosław Florczak[1], Kacper Handzel, Andrzej Kołcon, Mariusz Masiewicz
Airforce Institute of Technology, 01-494 Warsaw, Ks. Bolesława St. 6, box 96.

## ABSTRACT

The article presents a brief description of the ELINT Subsystem (PR Subsystem) included in the Integrated Air Electronic Warfare Range (IAEWR), created as part of a development project co-financed by the National Center for Research and Development. Typical ELINT class devices used in the Polish Armed Forces were implemented in the design of the PR subsystem. In particular, the authors of the paper focus on presenting the role of PR Subsystem in the process of assessing the effectiveness of registered radio-electronic jamming signals generated from an aircraft platform. This will allow for the future implementation of aviation training tasks, including the assessment of the correctness of the crew's and the aircraft's built-in defense system response to simulated electromagnetic emissions (radar threats). The article also presents the adopted criteria for the detection and classification of selected types of radio electronic interference, including narrowband noise jamming, wideband noise jamming, Range Gate Pull Off, Range False Targets and Square Swept Wave. The article describes the basic features of the above-mentioned types of interference and the general principles of detection and registration.

**Keywords**: Electronic Warfare, EW Range, Electronic countermeasures.

## 1. INTRODUCTION

In present article was introduced the ELINT Subsystem (ES) which is a part of EW Training Range (the SSPWE system), making up on basis of contract of realization of developmental project with National Centre of Research and Development (NCBR). The SSPWE system be designed to support of process of training aircraft crews in conditions of electronic warfare (EW) across creation approximate to real, microwave electromagnetic environment, and to obtain the information about reaction of crew on linked by conditions also. The SSPWE system will offer a real opportunity to be the complete system in the future, capable to ensuring approximate to real microwave threats for aircraft crews in time of flight. Further, are presented some radar jamming which are applied to electronic dazzling/disruption preliminary search and tracking radars used by missile/ the anti-aircraft artillery and airborne radars mounted on board the multi-role fighter aircraft. Moreover, the conception of jamming classification by ELINT Subsystem was introduced. This concept is based on unique recorded features, attributed to the individual kinds of radar jamming.

1 jaroslaw.florczak@itwl.pl; www.itwl.pl

Radioelectronic Systems Conference 2019, edited by Piotr Kaniewski, Jan Matuszewski, Proc. of SPIE
Vol. 11442, 114420X · © 2020 SPIE · CCC code: 0277-786X/20/$21 · doi: 10.1117/12.2565223

### 1.1. Basic description of the ELINT Subsystem

Within the SSPWE system are three basic functional items [1]:

- Management and Cooperation Unit (the JZW),
- Generation of Threats Unit (the JGZ),
- Surveillance - Measuring Unit (the JOP).

ELINT Subsystem is a part of the Surveillance - Measuring Unit.

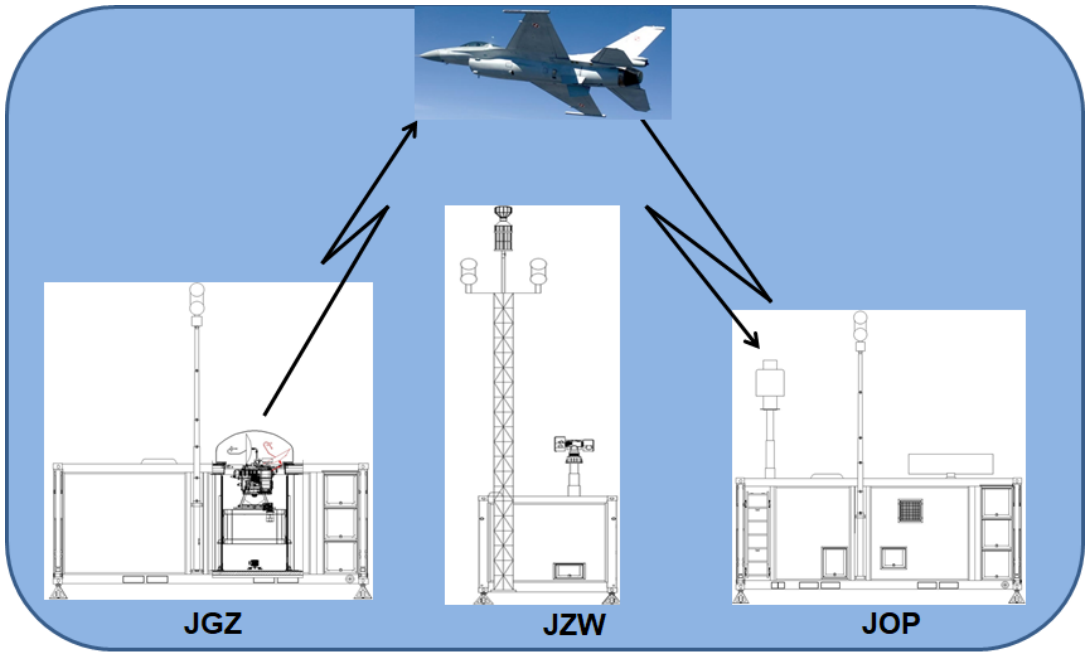


*Figure 1. EW Training Range diagram [1]*

**The Generation of Threats Unit (JGZ) will include:**

1. The Generation subsystem which will be able to generation, amplification and directed emission of threat signal.
2. The Power supply subsystem will assure e.g. power supply control for other subsystem and will contain Exchange Data unit which will perform communication tasks between other system items.

**The Surveillance - Measuring Unit (JOP) will include:**

1. The Surveillance Subsystem based on long range IFF interrogator which will be modified for the needs of the project, it will conduct location an aircraft equipped in mode 3/A and C transponder MARK X in controlled airspace.
2. The ELINT Subsystem will analyze and measure jamming bandwidth, jamming direction and also analyze jamming efficiency level by self-protection equipment of aircraft in controlled airspace.
3. Power supply subsystem (description as above).

**The Management and Cooperation Unit (JZW) will include:**

1. The Management subsystem which will conduct configuration control, as well as the steering, diagnostics control but, first of all, will be monitoring the training operation.
2. The Optoelectronic subsystem will conduct wide range *observation* of an aerial object and aiming devices with laser, night vision and thermal vision technologies in controlled area; used video tracker and laser rangefinder to determine the position of the indicated an air object.
3. The Cooperation subsystem will be receiving quick radiolocation information from co-operating sources equipped in specialized adapter and other system involving control, diagnostic and receiving data from other unit.
4. The Registration subsystem will conduct data recording referred to training additionally data time marked and will be a source of time for SSPWE system.
5. The MILNET- Z station will conduct classified data processing according to safety documentation.
6. Power supply subsystem (description as above).

It is supposed that staff of projected SSPWE system will execute all tasks during a training from Management and Cooperation positions whereas other items will be remotely controlled.

The Microwave MIZAR sets receivers which are the main part of ELINT Subsystem allows a large frequency range (e.g., 2 to 18 GHz) to be covered in bands. Their main task is to register activity of source of emission (using monitoring channel) as well as the parametric estimation and bearings (direction finding) of indicated sources of emission (using location channel). Registered data will be sent after processing to the Management and Cooperation Unit as auxiliary data for training evaluation process.

## 2. REVIEW OF SELECTED JAMMING TECHNIQUES

Active jamming used to suppress/dazzling the enemy's electromagnetic signals emitted from radars can divide on two principle kind:

- Cover Jamming;
- Deceptive Jamming.

### 2.1. Cover Jamming

The object of cover jamming is to reduce the quality of the signal output. There are following techniques inside cover jamming:

- wideband noise: generic jamming band cover a numerous radar receiver channels. With regard on jamming bandwidth it fulfils the following condition [2]:

$$\frac{B_j}{B_r} > 5$$

where:

*Bj – jamming noise bandwidth*

*Br – radar intermediate-frequency bandwidth, matched to radar pulse width.*

Figure 2 shows the comparison between of jamming band emission for wideband signal to target pulse band in intermediate-frequency channel. The aims of this kind of jamming are mainly to:

- Electronic dazzling against many radars simultaneously,
- Electronic dazzling against radars in respect of which is no knowledge about working band and pulses repetition period.

By reason of large energy consumption and a considerable dimensions of a transmitter unit, this type of interferences does not use in the self-protection systems at present. It is a part of the systems for a different purpose like onboard *Airborne Electronic Attack - AEA* system.

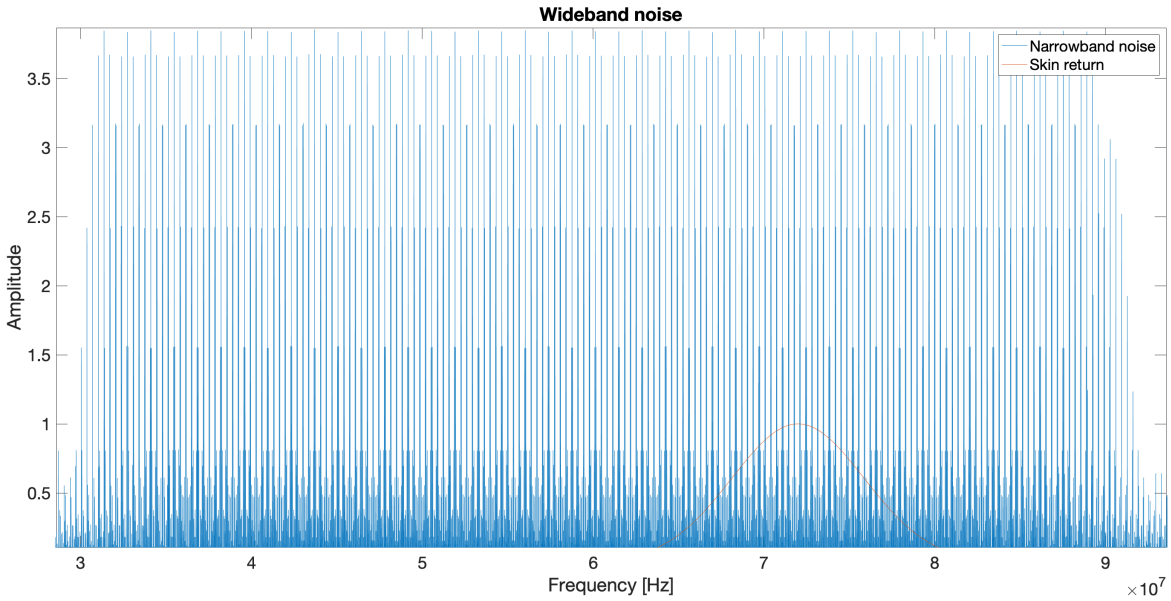


*Figure 2. Wide-band noise jamming*

- Narrow-band noise jamming: band of generated interferences is comparable with the band-pass of receiving channel IF filter.

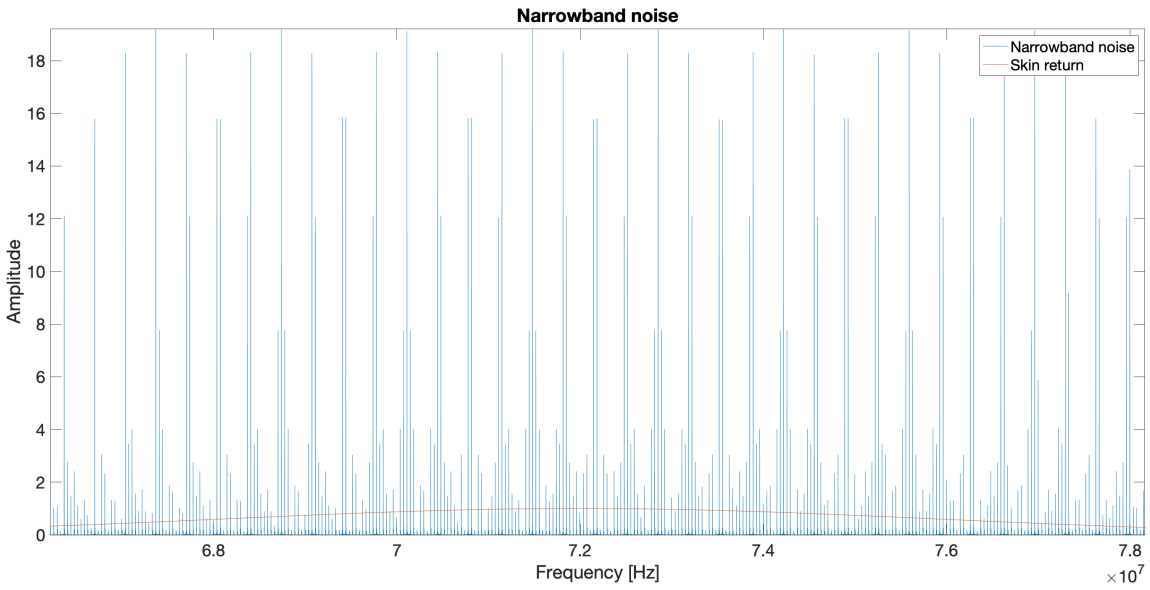


*Figure 3. Narrowband noise jamming*

Figure 3 illustrates a comparison of the narrow-band noise with an IF return pulse band. Generally this type of jamming is applied to older, non-coherent or pseudo-coherent generation of emitters without advanced moving target indication systems. It also applied in electronic attack systems equipped with large gain transmitting antennas and which are distinguished by a high power jamming signals [5].

## 2.2. Deception Jamming

Deception Jamming - (basic type of jamming used in Self-protection Systems) are intentional jamming imitating real return signals on victim radar's scope. Undoubtedly, the main advantage of using the deception jamming is the reduced capability of radar receiving systems to filter out this type of jamming signals. Matching of false waveforms in terms of carrier frequency and (in the case of using DRFM) the instantaneous phase, significantly impedes the possibility of separating the false targets from the real targets. Due to the frequency and phase matching, the requirements for the J/S ratio [5] are reduced. There are many types of deception jamming.

This article is presented selected types [8]:

1. Numerous range false targets (RFT),
2. RGPO, RGPI - Range Gate Pull-Out/In,
3. Angular deception jamming (SSW-Square-Swept-Wave).

### *2.2.1. Numerous range false targets (RFT)*

RFT technique involves the synchronous generation of series of pulses on the carrier frequency of a threat signal with a similar pulse duration.

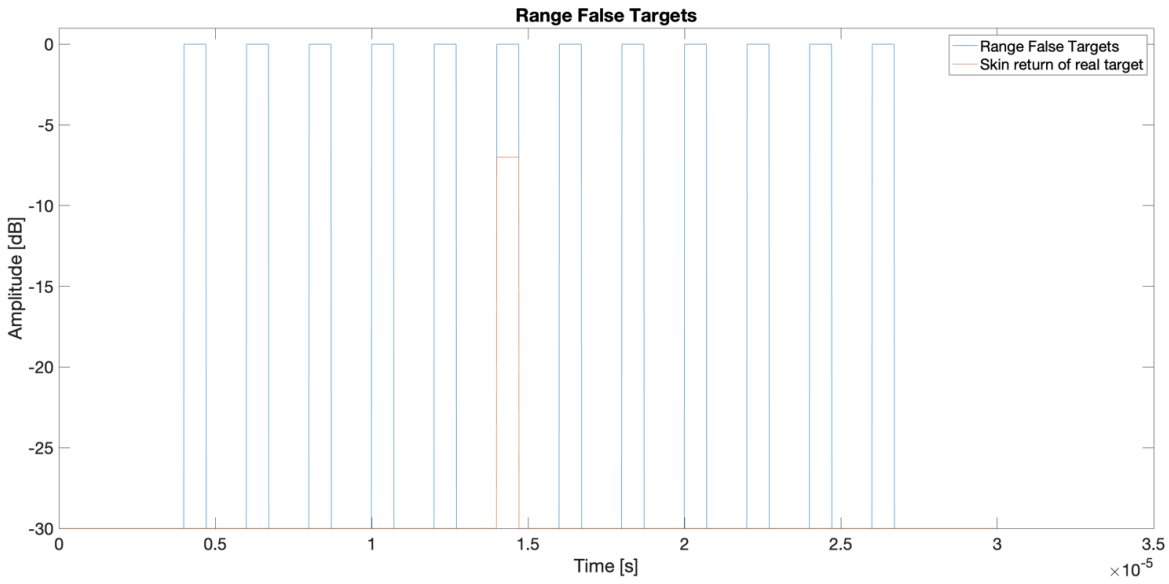


*Figure 4. RFT technique*

RFT technique is mainly used for:

- making difficulties in selecting target for tracking,
- capturing real return signal by Cover Pulse [3],
- forcing AGC systems to lower the input signal gain level, which will make in turn more difficult to receive real return from the target [5].

### *2.2.2. Range Gate Pull Off, Range Gate Pull In*

The RGPO, RGPI techniques are based on delaying (RGPO) or accelerating (RGPI) the generated pulse relative to the actual return of the tracked target.

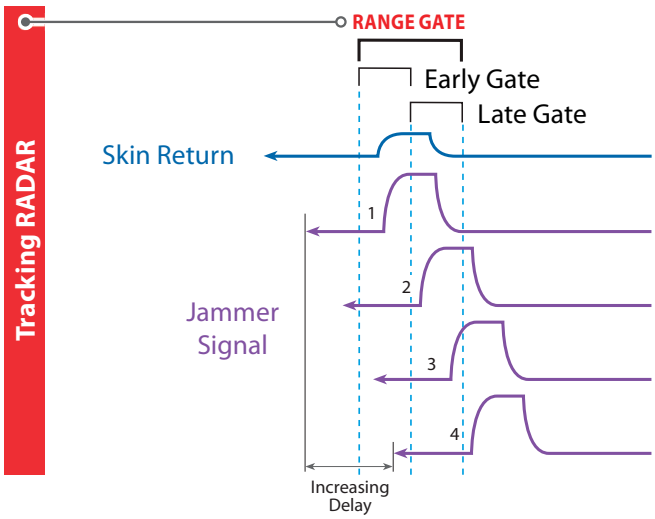


*Figure 5. Range Gate Pull Off Technique [3]*

Figure 5 shows the principle of generating the RGPO technique. False target pulse responsible for “gate stealing” is generated with increasing time delay in every pulse repetition interval. The system generating the range gate error signal compares amount of energy within “Early Gate” and in the “Late Gate”, then the system initiates a movement of the tracking gate towards the further gate to compensate the energy level [6]. This process continue until the gate leaves the range of the radar resolution cell of the target.

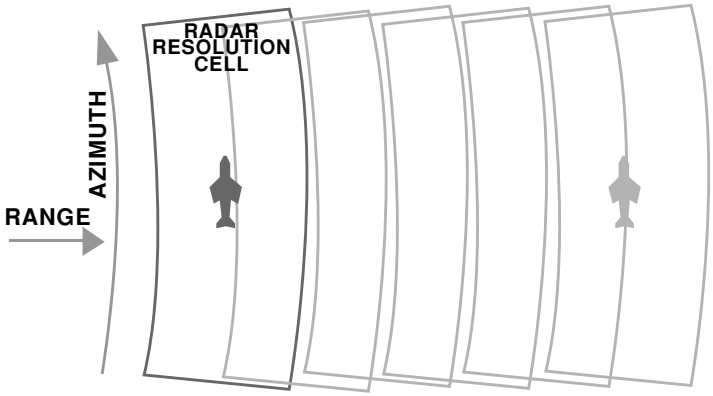


*Figure 6. RGPO technique in space [3]*

As a result of breaking the tracking process the radar is forced to change the operational mode to the target search mode. “Pushing” the range gate closer the tracking radar in a similar way mentioned above is called RGPI technique. The only difference is the opposite direction of the changes.

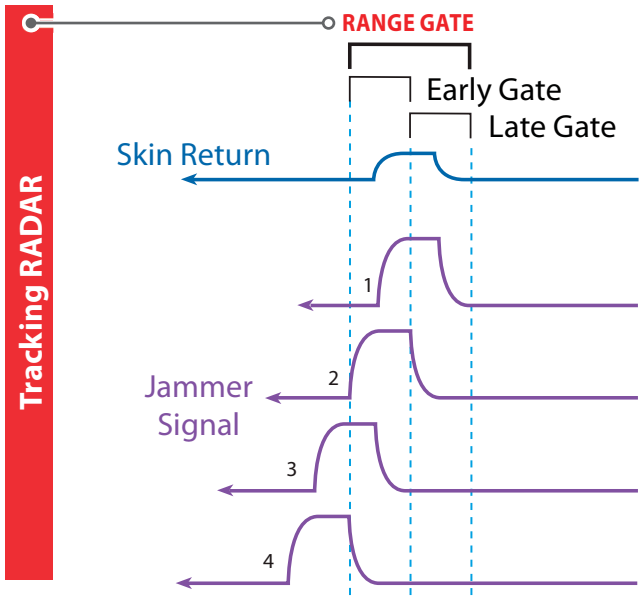


*Figure 7. Range Gate Pull In technique [3]*

The RGPI technique enforce having sufficiently large knowledge about the transmitting characteristics of the victim radar and onboard emission tracking systems (Pulse Repetition Interval Tracker) to predict the arrival time of subsequent threat pulses [5].

### *2.2.3. Angular deception jamming (Square Swept Wave)*

The angular deception jamming technique implementation (also known as ***Swept Wave Modulation***) base on rectangular wave with the constant or modulated frequency and/or duty cycle.

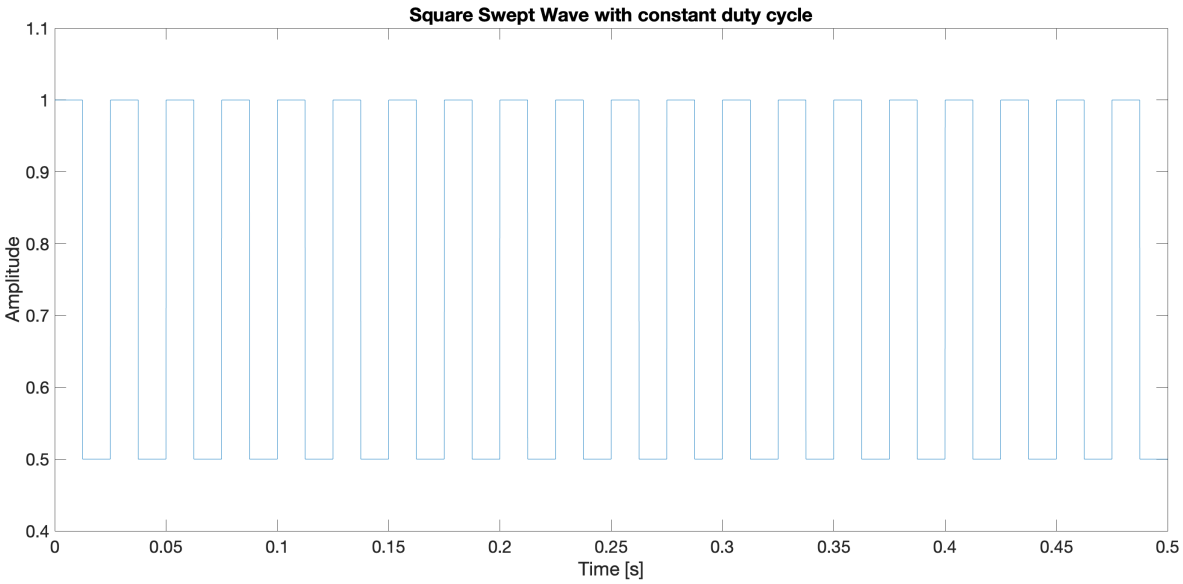


*Figure 8. Rectangular Wave with the constant frequency and duty cycle*

Figure 8 illustrates rectangular wave with the constant frequency and duty cycle equal 50 %.

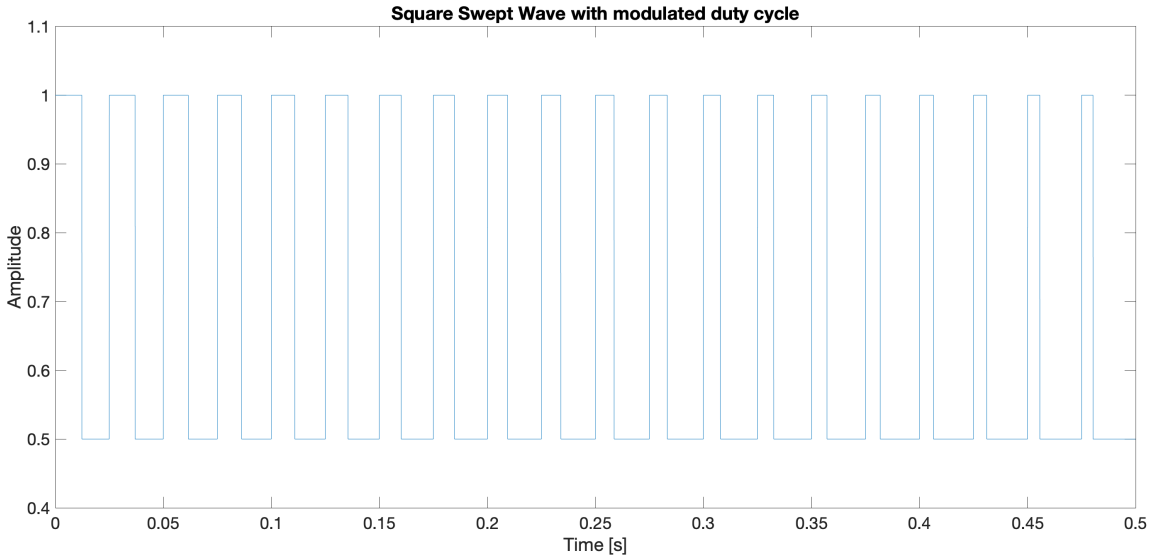


*Figure 9. Rectangular Wave with the constant frequency and modulated duty cycle*

Figure 9 illustrates Rectangular Wave with the constant frequency and modulated duty cycle. Such modulated amplitude is implement in combination with range deception jamming techniques, noise jamming techniques or continue wave noise techniques. The effectiveness of the angular deception jamming mainly

depends on side lobes level of the radar receiving antennas, presence of side lobes compensation systems or additional reference antennas.

Angular deception level are mainly used for:

- confusing the error signal generating systems responsible for controlling the angle tracking systems,
- paralysis of automatic gain control systems,
- disrupting influence on passive scanning systems (*i.e. LORO – Lobe On Receive Only*),
- decreasing the angle measurement accuracy of mono-pulse measurement direction methods.

## 3. RADAR JAMMING SIGNAL DETECTION AND CLASSIFICATION

The nature of jamming signals generated from a typical Airborne Electronic Attack or Self-Protection device is not similar to typical radar signals. Detection of such signals with a classic ELINT system is a demanding process. Proper measurement of jamming signals is possible only with particular and special care for the configuration parameters of the ELINT receivers (appropriate LIN/LOG amplifiers, fine thresholds and optimal IF bandwidths). Detection of amplitude/angle deception signals may be complicated due to high dynamic level.

Classification of detected jamming signals bases on two data streams:

- Bandwidth occupancy of signals detected in the monitoring channel,
- Time and power features of pulses estimated within the Pulse Descriptor Word from the Direction Finder (**DF**) channel.

### 3.1. *Monitoring channel data*

It is assumed that the bandwidth occupation analysis should be done first.

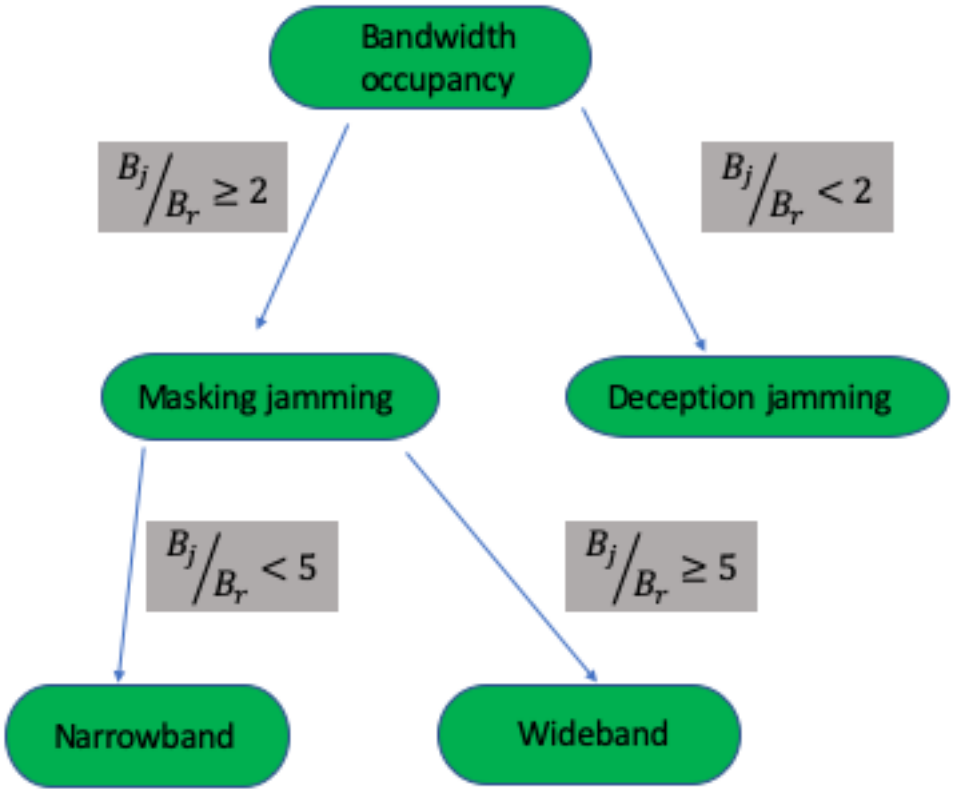


*Figure 10. Bandwidth occupancy decision tree*

According to Figure 10 it is assumed that the masking and deception jamming signals are distinguished on the basis of bandwidth occupancy coefficient. Due to ability of generating various techniques variable with time, it is necessary to define a sliding window with variable width. The bandwidth occupancy analysis will be executed again after the sliding window reached to the end of the registered sequence. Such process will allow to detect various mixed (masking and deception) jamming signals.

### 3.2. *DF channel data*

If the jamming signal within the sliding window is classified as a deception jamming, it is necessary to analyze the DF channel data stream. It is assumed that the Range Deception analysis should be done first.

### *3.2.1. Range* Deception jamming techniques

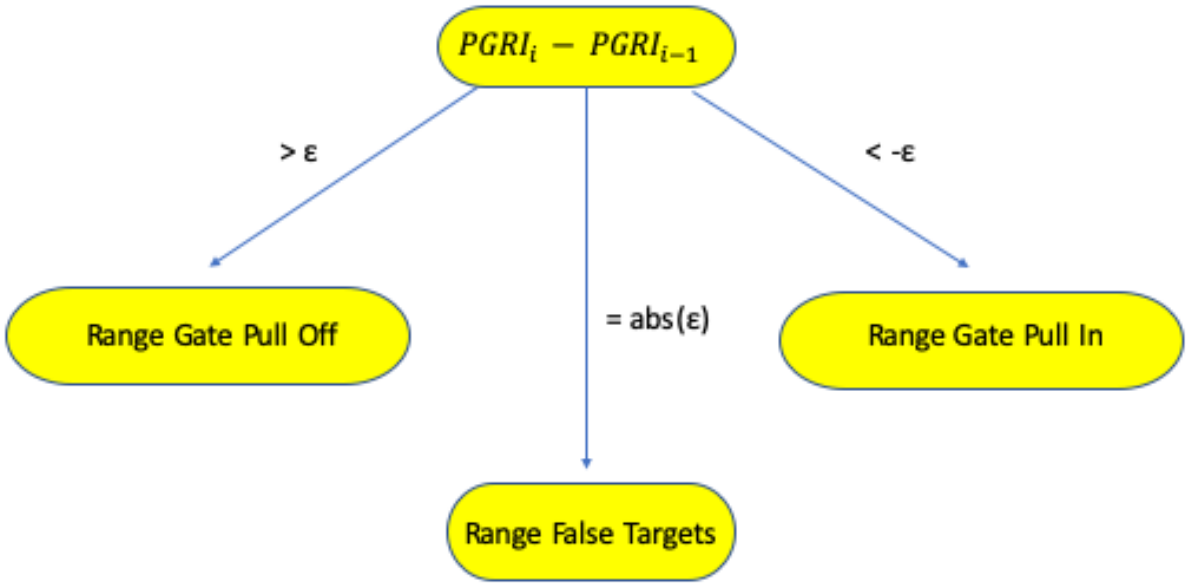


*Figure 11. Range Deception decision tree*

Classification of Range Deception jamming signals bases on the Pulse Group Repetition Interval (**PGRI**) analysis.

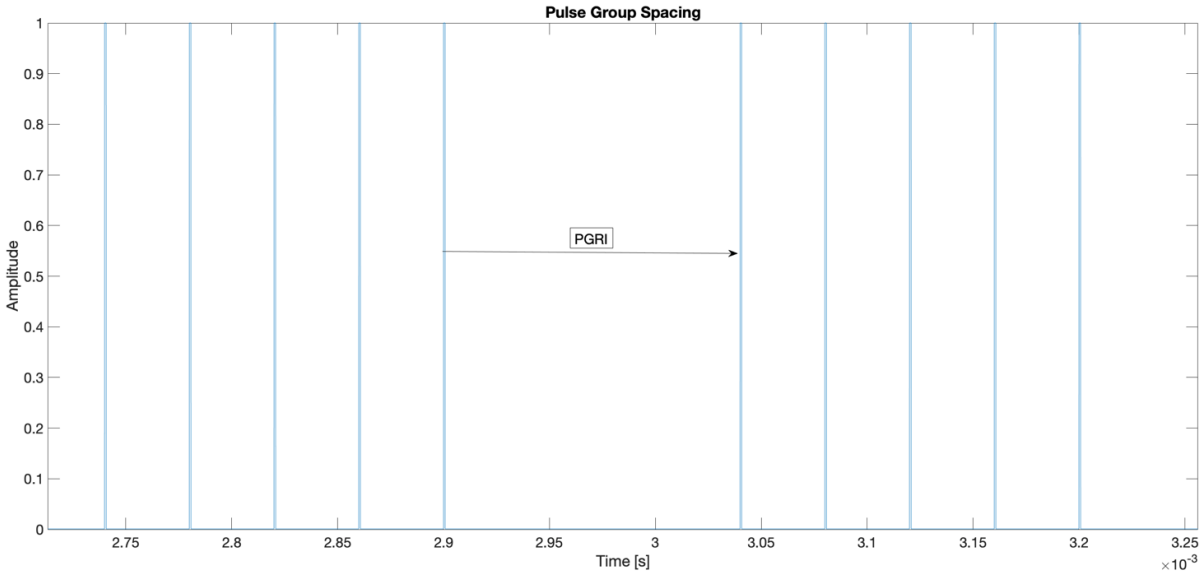


*Figure 12. Pulse Group Spacing*

Figure 12 shows the graphic interpretation of PGRI. It is defined as time between the last pulse rising edge from the preceding group and the first pulse rising edge from the succeeding group.

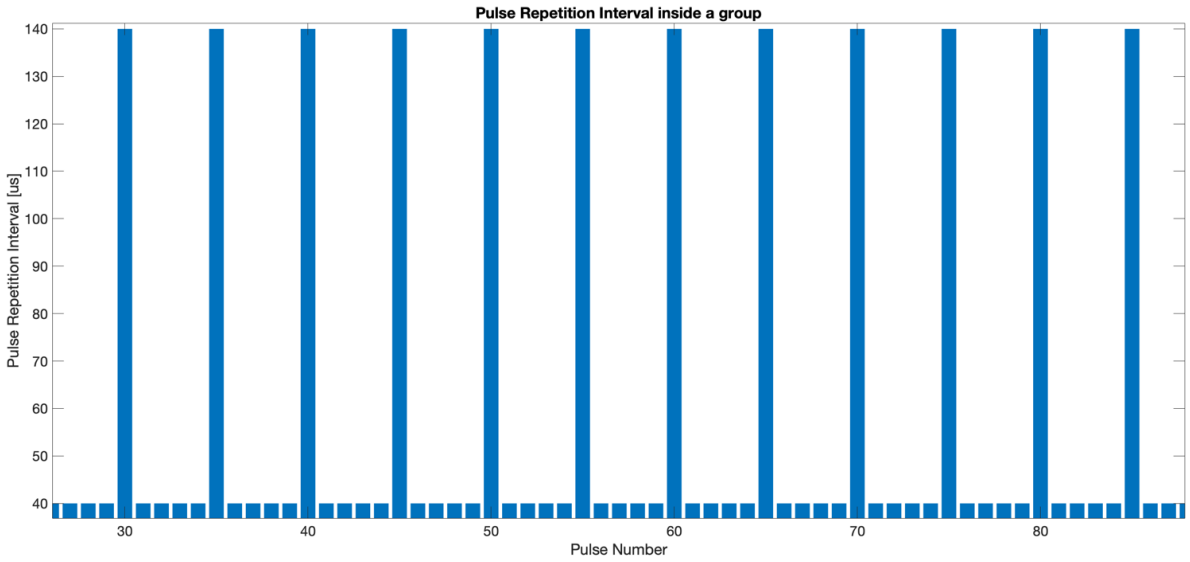


*Figure 13. Pulse Repetition Interval of registered pulses*

Higher values of the bars shown in the Figure 13 are related to the Pulse Group Repetition Interval. Lower values of the bars are related to pulses inside the pulse group. It is assumed that the pulse repetition interval of pulses inside the group is constant and equal. The pulse group repetition interval of Range False Targets (**RFT**s) may be described as [7]:

$$|PRGI_i - PGRI_{i-1}| \leq \varepsilon \tag{1}$$

where: ε means admissible time measurement error.

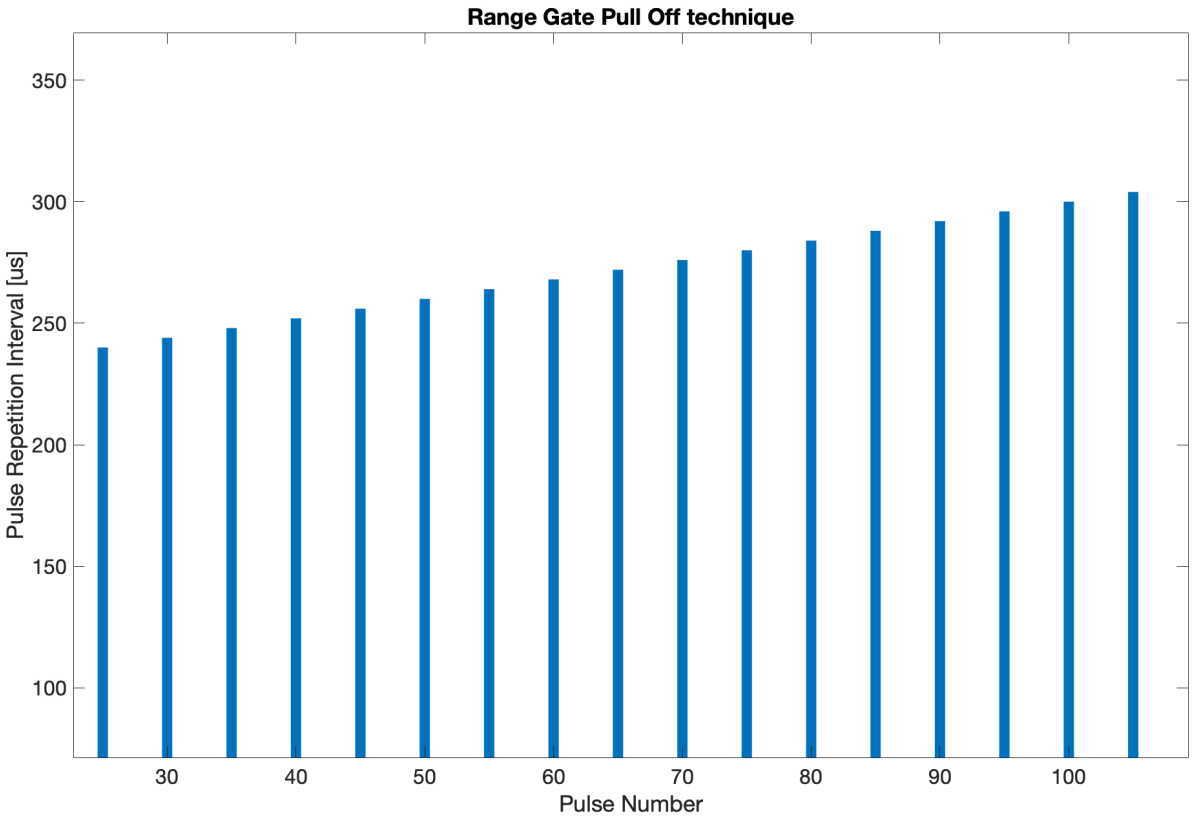


*Figure 14. PRI of the Range Gate Pull Off Technique*

Figure 14 shows the PGRI difference during the Range Gate Pull Off technique being registered. Gradient coefficient $\alpha$ defined as [4, 7]:

$$\alpha = (X^T X)^{-1} X^T Y \tag{2}$$

$$\text{where: } X = \begin{pmatrix} TOA_{PGRI1} \\ TOA_{PGRI2} \\ \vdots \\ TOA_{PGRIi} \end{pmatrix}, Y = \begin{pmatrix} PGRI_1 \\ PGRI_2 \\ \vdots \\ PGRI_i \end{pmatrix} \tag{3}$$

is positive. Value of the coefficient is dependent on the gate stealing linear rate.

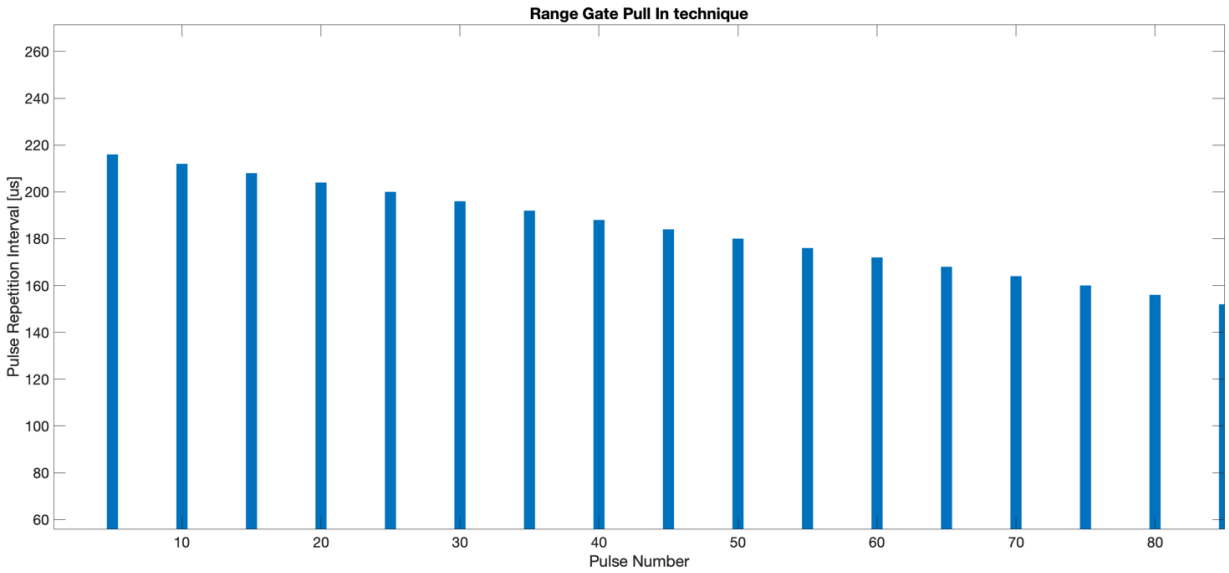


*Figure 15. PRI of the Range Gate Pull In technique*

Figure 15 shows the pulse repetition interval of the Range Gate Pull In technique. The gradient coefficient $\alpha$ is negative.

### *3.2.2. Amplitude/Angle Deception jamming techniques*

The final step of the jamming analysis is the detection and classification of Amplitude/Angular Deception jamming techniques. Such techniques appear generally with the Range Deception techniques. The frequency of the square wave used in angular deception techniques usually does not exceed the scanning frequency of the radar antenna beam. The assumed range of detected square wave frequencies is from 2 Hz to 200 Hz. The idea of angular deception technique detection bases on the Fast Fourier Transform of envelope of the pulses stored in the Pulse Descriptor Word. It is assumed that it is necessary to detect the odd harmonic frequencies of the square wave. The angular deception signal exists when:

- The strongest harmonic frequency is included within the range from 2 Hz to 200 Hz,
- The odd frequencies in the range from 6 Hz to 1000 Hz exists.

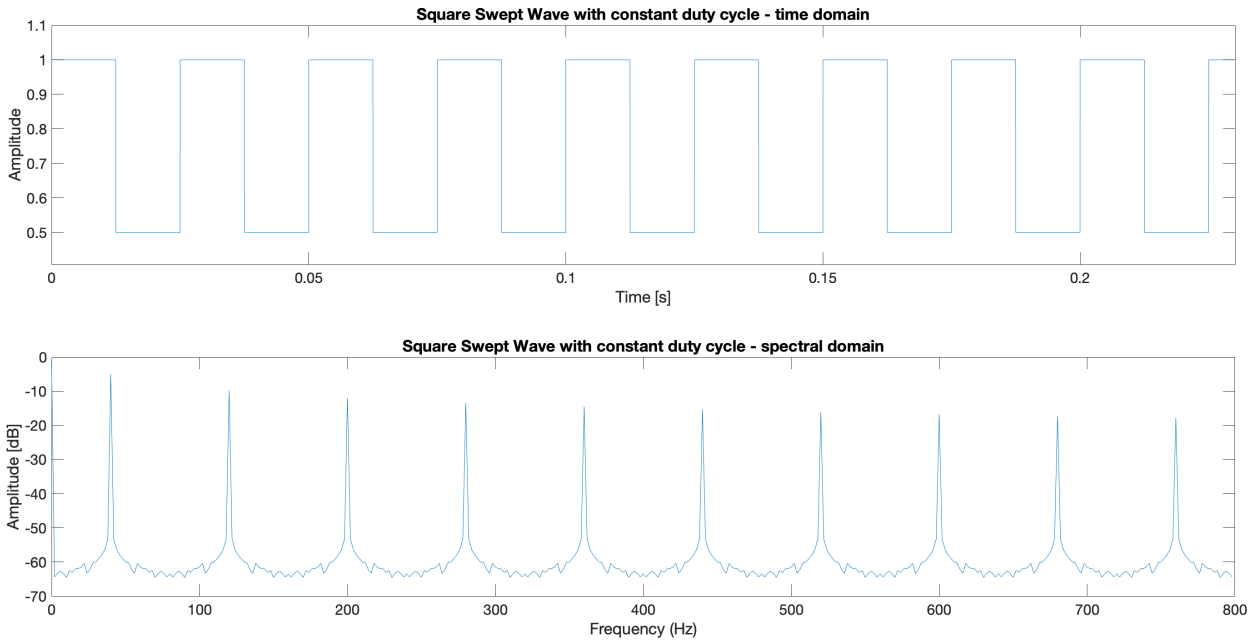


*Figure 16. Square Swept Wave with constant parameters – time and spectral domain*

Figure 16 shows a square wave in time and spectra domain. The frequency of this square wave is constant and equals to 40 Hz. The duty cycle of the wave is constant and equals to 50%. In the range of 6 Hz to 1000 Hz a lot of odd frequency exists.

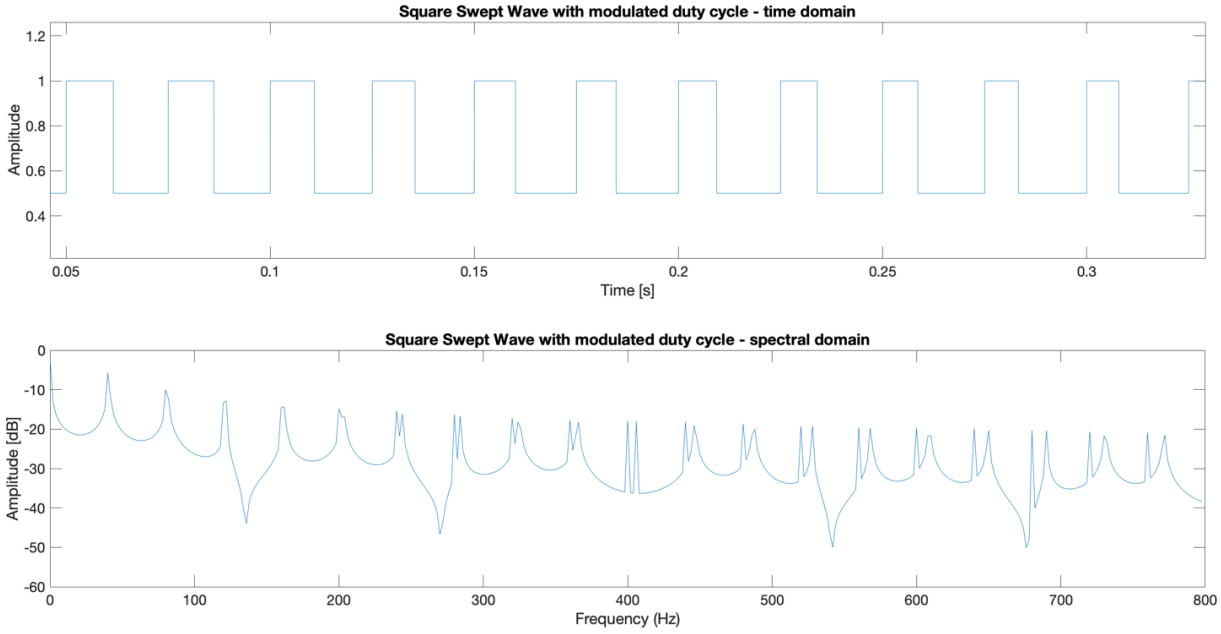


*Figure 17. Square Swept Wave with modulated duty cycle – time and spectral domain*

Figure 17 shows a modulated square wave in time and spectra domain. As in previous case, the strongest is the 40 Hz base frequency. A lot of odd harmonic frequencies exists. Due to the modulated duty cycle from 50% to 30% a lot of even harmonic frequencies exists.

## 4. SUMMARY

In the presented article the basic direction of work carried out during the development and implementation of the ELINT ESM subsystem is described. It will be one of the key elements of the system for assessing the correctness of the Aircraft Self-Protection system. At present, it will enable the validation of interference techniques generated on board the F-16 aircraft. In the future, its usefulness for the evaluation of interference generated on board the F-35 aircraft is also assumed. The presented list of interference is not complete, in the case of the F-16 aircraft it includes several possible generation techniques, for which the basic criterion of use is the detected type of threat signal.

## REFERENCES


[1] E. Jasiński, M. Masiewicz, J. Wiśniewski: „*Projekt Koncepcyjny - Poligon Walki Elektronicznej – wsparcie procesu szkolenia załóg statków powietrznych i systemów OPL Sił Powietrznych*", ITWL, Warszawa 2017

[2] F. Neri: „*Introduction to Electronic Defense Systems*", SciTech Publishing Inc.2006

[3] W. George; Griffiths, D. Hugh; J. Ch. Adamy; D. Stimsons: "*Introduction to Airborne Radar"*, SciTech Publishing 2014

[4] A. De Martino: „*Introduction to Modern EW Systems*", Artech House, 2018

[5] D. Adamy: „*EW 101 - A First Course in Electronic Warfare*", Artech House, Norwood, MA, 2001

[6] M. Skolnik: „*Radar Handbook*", McGraw-Hill, 2008

[7] A. Golden Jr.: „*Radar Electronic Warfare*", AIAA EDUCATION SERIES American Institute of Aeronautics and Astronautics, Inc. New York1987

[8] D. L. Adamy: „*Introduction to Electronic Warfare Modeling and Simulation*", Copyright 2006 by SciTech Publishing, Inc.