Method Research and Realization of Noise FM Jamming Based on DDS Technology

Zeng Chuyang¹, Gao Shang¹, Xiao Jianyi¹, Huang Jianwen¹, He minnuo¹, Lin Qiang¹, Huang Kaitong¹, Huang Jutao¹, Ma Ruiwen¹

¹ Information Centre, Guangdong Power Grid Corporation, Guangzhou, Guangdong, 510000, China

Abstract: Noise FM jamming which has wide jamming band and large noise power is widely used in processing backup jamming to radar, fuze and communication. The paper adopt DDS combines with characteristic of FPGA chip to generate noise FM jamming. The method has large improvement in precision, structure and speed, and has broad application and prospect.

1. Introduction
With the rapid development of information technology, electronic systems are becoming more and more complex with the continuous improvement of performance. For electronic countermeasures, the ultimate goal is to interfere with the enemy's radio communication, guidance, command, fuze and radar systems. Therefore, the construction of interference signal is of great significance. The traditional method of generating interference signal is to use VCO/DTO or D/A to realize noise frequency modulation and function sweep. In this paper, high-speed DDS chip is used to realize noise frequency modulation interference.

At the receiver side of radar, according to the relationship between the bandwidth of the noise FM signal and the bandwidth of the amplifier in the receiver, only when the frequency is within the bandwidth of the amplifier, the receiver will have output. If the transient response of the tuning loop is not considered, a series of rectangular pulses with equal amplitude and random width and interval will appear after the noise FM signal passes through the receiver. In fact, the resonant circuit has transient response, which can be measured by the time when the pulse waveform is set up. The setup time is approximately equal to the reciprocal of the bandwidth of the intermediate amplifier. When the interference bandwidth of the noise FM interference is much larger than that of the intermediate amplifier, the setup time will be much longer than the width and interval of the random pulse at the output of the intermediate amplifier. In this way, the random pulse will be broadened, and many pulses will overlap to form a continuous oscillation with random amplitude fluctuation. The pulse width of the noise FM interference at the output of the amplifier is random. The superposition of these pulses results in interference similar to the internal noise of the receiver.

Compared with the traditional method, DDS method has the characteristics of flexible control, fast speed, high precision of frequency setting, simple structure and strong anti-interference. It can be used to generate interference signals of various systems.

2. Basic principles

2.1 Characteristics of noise FM jamming
Noise FM jamming has wide jamming bandwidth and large noise power. Noise FM jamming is the most commonly used jamming form for radar, fuze and communication. The important characteristic of noise FM signal is that the power spectral density of noise FM signal has a linear relationship with the probability density of modulated noise. When the probability density of modulated noise is uniformly distributed, the power spectral density of noise FM signal is also uniformly distributed. According to this characteristic, a random number with uniform probability distribution produced by m-sequence generator is proposed as noise frequency modulation.

Firstly, zero IF orthogonal white noise is generated, then the sampling frequency controls the spectrum width, the output spectrum is square, and then the center frequency is formed by frequency shift modulation. The advantages of this method are good data universality, easy to adjust the spectral width and long enough period through pseudo-random location reading. The randomness of the output signal depends on the size of the memory and the randomness of the pseudo-random address. Because physical conditions restrict the capacity of the actual memory to some extent, it is inevitable to reuse the stored data in the process of long-term interference. Due to the regularity of the range of radar signal processing, the main performances are the processing of intra-pulse signal, signal processing in pulse repetition period, signal processing in beam irradiation time. Signal processing in beam scanning and signal processing between beam scanning. Data readout is synchronized with radar pulse repetition period, and synchronous radio frequency noise interference can also be realized. Because the read address is random, the DDS phase accumulation method cannot be used. In the simulation, m-sequence is used as read-out address of memory. In order to increase the randomness of pseudo-random address codes, the value added by the m-sequence modulus 2 of two columns of periodic reciprocity can be used as the address to read the data in memory, and the address period is the product of two columns of m-sequence periods. In this way, the period of pseudo-random address code can be very long, and the memory with small storage capacity can be used in hardware implementation, thus reducing the cost.

2.2 M sequence

M sequence is the most commonly used pseudo-random sequence. It is the abbreviation of the longest linear feedback shift register sequence. It is also a sequence generated by the shift register with linear feedback and has the longest period. When the shift register with linear feedback logic sets the initial state of all levels of shift registers, the state of all levels of shift registers will change after each shift triggered by the clock. We observe the output of the first register. As the shift rhythm moves, a sequence will be generated. This sequence is called shift register sequence. The schematic diagram of m sequence generation is shown in Figure 1.

![Figure 1. Schematic diagram of m sequence generation](image)

In fact, the maximum period of a linear shift register sequence is $2^n-1$, because a shift register entering the all-zero state will terminate in that state. M sequence is the sequence of binary shift registers with the largest period. It has been proved that m-sequence exists for any shift register with digits greater than one. M sequence has two important conclusions. Firstly, m-sequence has strong autocorrelation and weak cross-correlation. m-sequence with a period of $2^n-1$ can provide $2^n-1$ address code. Secondly, only a sequence generator whose feedback connection meets specific requirements can generate m sequences. This particular requirement can be described by characteristic polynomials as primitive polynomials. Therefore, the main task of constructing an m-sequence is to solve the characteristic polynomial problem of a primitive polynomial. The number of primitive polynomials is always even.
By finding the primitive polynomial, the \( m \) sequence can be obtained by constructing the feedback shift register.

### 3. Realization method

#### 3.1 Chip selection

In this paper, a broadband DDS chip is used to generate baseband noise FM signal. The chip is a DDS core chip. 32 frequency control bits are directly extracted by pins. There are no registers in the chip, that is, the frequency control bits appear after 0 and 1. The output frequency or phase changes after 8 clock cycles. The chip has the advantages of short frequency conversion time and wide output bandwidth. Its maximum operating time is 3.2 GHz and output frequency are up to 1.6 GHz. It has 32 bits frequency resolution. An 11-bit analog-to-digital converter is integrated in the chip. When using a 3 GHz working clock, the stray suppression can reach 45 dB in the wide band of DC~1.2 GHz, and the final frequency resolution is 0.7 Hz. Frequency control words (32bits) can be downloaded to the control port through parallel input format. The updating rate of parallel port can reach 350MHz to ensure high frequency updating speed.

In the state of confrontation, based on the sharing of resources in the space, time and frequency domains, the radar countermeasure system manages dynamically in the best way according to threat priority, and uses power resources to counter many threat sources, so as to achieve the best jamming effect. The main input information of power management system includes: electromagnetic reflection characteristics of the platform or the protected object where the jammer is located. The pulse descriptor of the emitter includes arrival time, arrival angle, carrier frequency, pulse amplitude and width, etc. The characteristic data describing the threat includes repetition frequency, carrier frequency, angle, pulse width, polarization form and engineering. State of operation, threat level, platform type, etc; Amplitude-preserving pulse signal of radiator; Output information mainly includes: various control codes or control signals of execution strategy, state control signals of execution strategy mechanism, blocking or blanking and instantaneous observation signals, interference time, interference type, interference spectrum, interference angle, interference. In addition, the state of power management equipment and self-test results are also included. In the field of electronic warfare, power management technology is widely used. Its task is to find the criteria for comprehensive decision-making, the optimal solution method of behavior strategy and the best equipment to support the implementation strategy. In today’s electronic warfare environment, power management system is indispensable in the face of a number of dense, diverse, complex and changeable threat radiation sources.

To manage resources correctly, power resources must be shared in space, time and frequency domains. The functional requirements of space power management include: high-speed directional acquisition of multiple radiation sources; sorting and identifying intercepted signals; high-speed controllable interference antenna; and time management of controllable antenna. Spatial power management generally does not cover the wide angle uniformly, but controls the maximum radiation power of electromagnetic wave to point to the threat direction, and then concentrates the power in a specific direction with a narrow beam antenna. Narrow beam means high antenna gain, and requires beam driving, sometimes focusing and defocusing. In time domain management, both suppressive jamming and deceptive jamming are emitted only within the expected time period of the threat target, which is an effective method to reduce the average power. Frequency domain requires that the intercepted signal can be separated and identified; carrier frequency can be measured at high speed; jamming frequency can be adjusted at high speed and accurately; and the ability to process fast frequency conversion radar such as frequency agility is required.

#### 3.2 Generation method of noise FM jamming

The generation of noise FM interference is mainly divided into three modules: \( m \) sequence generator, mapping module and DDS module. The structure diagram of noise FM interference generation is shown in Figure 2.
As shown in Figure 2, the uniform random sequence is generated by using m-sequence in the FPGA. We convert the random sequence into frequency control words in a certain range by mapping module. The generated frequency control words are used as frequency control words of DDS chip. Finally, the noise FM signal is output by DDS chip. The frequency control word of the DDS chip is 32 bits, so it needs to generate a 32-level m sequence at most. If a tap is drawn from the output of each shift register, then the combined output of M taps is a binary number of m-bit length, which has a total of $2^m - 1$.

Because m sequence has pseudo-randomness, the probability of occurrence of random numbers composed of these binary numbers is equal. We can think of it as white noise with uniform distribution. In this paper, a 32-Level m-sequence with a period of $2^{32} - 1$ and a characteristic polynomial of $X^{32} + X^{22} + X^2 + X + 1$ is used. The generated random number has a long period and good uniform distribution, and the whole process of generating random number only needs shift and exclusive or operation. The generating sequence is fast and suitable for implementation in FPGA.

The baseband orthogonal suppressed interference waveform stored in a memory changes simultaneously when the interference bandwidth is changed by adding clock frequency and address. If independent changes are required, separate memory and readout control circuits are required. In the simulation, separate memory and readout control circuit are used to synthesize two channels of radio frequency noise interference signal; time domain and frequency domain are used to synthesize multi-channel interference signal; control spectrum width is used in the third chapter; control center frequency is interpolated, and the frequency of each channel signal is different. The minimum common multiple of the channel signal frequency is the frequency of the synthetic adder, and the power spectral density of the signal whose frequency is lower than this value will be extended periodically at its own sampling rate. DDS method can also control the frequency of the control center, and the same frequency can be used to control the generation of each signal, and the same clock is used to synthesize, so that any signal in this frequency can be generated without continuation. Comparatively speaking, DDS method is more flexible to synthesize multi-channel interference signals, but interpolation method can save a lot of resources.

The pseudo-random number of N ($N \leq 32$) bits generated by FPGA is used as the frequency control word of DDS to generate noise FM signal. Because the selection of noise bandwidth is random, it is not chosen in the way of $2^N$, so it is necessary to map the data beyond the bandwidth. For example, when DDS chips use 3GHz clock, the frequency output range of baseband signal is set between 300 and 800 MHz, and the frequency control word is controlled by FPGA to jump randomly between 19999999 and 44444444, so the frequency control beyond the bandwidth needs to be mapped between 19999999 and 44444444. The flow chart of the mapping generation frequency control word is shown in Figure 3.

The 32-bit frequency control word generated by the FPGA is m, the frequency control word corresponding to the starting frequency of the bandwidth signal is $K_1$, the frequency control word corresponding to the cut-off frequency is $K_2$, and the 32-bit maximum frequency control word is $N_1$. We
normalize the random number $m$ generated by the FPGA by dividing it by $N_1$ and multiplying it by the control range $K_2-K_1$. Here we can use $(K_2-K_1)/N_1$ as a mapping factor. Since the range of data obtained by this method is $[0, (K_2-K_1)]$, an offset is added to the data obtained. This offset is the frequency control word $K_1$ corresponding to the starting frequency. In this way, the output results can ensure that the generated pseudo-random number is within the required bandwidth without changing the statistical characteristics of the random number.

Under the condition of simple rectangular pulse, the range resolution is directly determined by the pulse width. In order to guarantee the range resolution, the increase of pulse width is bound to be limited. It is difficult to solve the contradiction between ensuring the necessary range resolution and improving the detection range of radar when using simple pulse signals, which requires people to find and adopt more complex signal forms. Linear frequency modulation signal can obtain large time-bandwidth product by linear frequency modulation or non-linear phase modulation. It is the earliest and most widely used pulse compression signal. The radar with this kind of signal can obtain both long target detection range and high range resolution. Compared with other pulse compression signals, it also has the following advantages: matched filter is insensitive to Doppler shift of echo signal, so signals with different Doppler shift can be processed by a matched filter, which greatly simplifies the signal processing system; in addition, it can be widely used, because of the fact that the matched filter is insensitive to shift of echo signal. The generation and processing of such signals are relatively easy, and the technology is relatively mature.

Suppose when the clock of DDS chip is 3 GHz, in order to generate noise FM interference signal with starting frequency of 300 MHz and cut-off frequency of 800 MHz, the pseudo-random number of 32 bits output from the FPGA is multiplied by the mapping factor of 0.2, and the frequency control word 199999 corresponding to 300 MHz is added as the frequency control. Word, you can get 500MHz bandwidth noise FM dry number. The simulation figure before and after mapping is shown in Figure 4.

![Figure 4. Simulation diagram before (left) and after (right) mapping](image)

As can be seen from the figure above, the frequency control words generated by the m-sequence before mapping are beyond the range between 19999999 and 44444444. After mapping, all the data are within the range between 19999999 and 44444444.

In the process of implementing the whole mapping module in FPGA, only multiplier and divider are needed to obtain the frequency control word of the required control range. The algorithm is simple and easy to implement.

**4. Test result**

The output end of the noise FM signal is connected to the spectrum analyzer, and the spectrum of the noise FM signal with three different bandwidths is measured. The observed frequency modulation signal spectrum waveform is shown in Figure 5.
Figure 5. Frequency modulated signal spectrum of 10 MHz bandwidth (left), 300 MHz bandwidth (middle) and 500 MHz bandwidth (right)

Generally speaking, radio frequency noise jamming can produce jamming effect for any radar system in its frequency band range, and there are many kinds of radar jamming, so it is also the current cause. The most used interference mode. But RF noise jamming requires continuous transmission of interference, and cannot obtain signal processing gain. The jammer consumes more energy and has larger suppression coefficient. The noise FM interference bandwidth is Figure 5 (left) 10MHz, the center frequency is 505MHz, which can be used to simulate aiming noise interference signal. Figure 5 (middle and right) noise interference bandwidths are 300MHz and 500MHz respectively, which can be used to implement blocking noise interference signal. From the spectrum analyzer, it can be seen that the noise FM signal generated by DDS has high frequency setting accuracy and good frequency stability, which can meet the needs of system design.

5. Conclusions
In this paper, a method of generating noise FM jamming signal based on DDS is proposed, which can compensate for the disadvantage of the traditional jamming signal that the VCO/DTO temperature drift greatly affects the frequency setting accuracy. Moreover, it is simpler than D/A algorithm, flexible noise bandwidth setting and easy to implement in engineering. The method has been successfully applied to a noise jamming generator. The test results verify the correctness and availability of the system design. The system design scheme has good practical application value.

Acknowledgement
This paper is one of the research results of “The project of key protection technology of sensitive information leakage and theft in non-network environment in 2015”.

References
[1] Kumari R, Mukhopadhyay M. Design of GPS antijamming algorithm using adaptive array antenna to mitigate the noise and interference[J]. Journal of Ambient Intelligence and Humanized Computing, 2019(6):1-11.
[2] Ingg’s M, Tong C, O’Hagan D, et al. Noise jamming of a FM band commensal sensor[J]. Iet Radar Sonar & Navigation, 2017, 11(6):946-952.
[3] Ze L I, Yan X P, Ping L I, et al. Jamming Mechanism of Frequency Sweep Jamming to FM Doppler Fuze[J]. Acta Armamentarii, 2017, 38(9):1716-1722.
[4] Kong Z J, Hao X H, Ping L I, et al. Research on Anti-frequency Sweeping Jamming Method for Frequency Modulation Fuze Based on Timing Sequence and Correlation Detection[J]. Acta Armamentarii, 2017, 38(8):1483-1489.
[5] Hwang Y M, Jung J H, Kim K Y, et al. Energy-Efficient Resource Allocation Strategy for Low Probability of Intercept and Anti-Jamming Systems[J]. Ieice Transactions on Fundamentals of Electronics Communications & Computer Sciences, 2017, 100(11):2498-2502.
[6] Kawamura A, Yamashita T, Iguni Y. Beat Noise Suppression Using Adaptive Line Enhancers for FM Radio in Motor Vehicles[J]. Ieie Transactions on Electronics Information & Systems, 2018, 138(5):593-602.
[7] Chang X, Dong C. A Barrage Noise Jamming Method Based on Double Jammers Against Three Channel SAR GMTI[J]. IEEE Access, 2019, 7(99):18755-18763.
[8] Zheng F, Li H, Qian Y. Cognitive anti-jamming receiver under phase noise in high frequency bands[J]. Journal of Systems Engineering and Electronics, 2018, 29(1):31-38.

[9] Mao W L. Robust Set-membership Filtering Techniques on GPS Sensor Jamming Mitigation[J]. IEEE Sensors Journal, 2017, 17(6):1810-1818.

[10] Shi C, Wang F, Sellathurai M, et al. Low probability of intercept based multicarrier radar jamming power allocation for joint radar and wireless communications systems[J]. Iet Radar Sonar & Navigation, 2017, 11(5):802-811.

[11] Zheng L, Liu S, Ju L, et al. Maximising the degrees of freedom of the physical-layer secured relay networks with artificial jamming[J]. Iet Communications, 2018, 12(6):665-671.

[12] Zhu X T, Liu Y L, Tie-Zhuang L I. Anti-jamming Method by Blindly Extracting of Direct Sequence Spread Spectrum Signal Based on Cyclostationary Difference[J]. Acta Electronica Sinica, 2017, 45(6):1506-1512.

[13] Tang X, Ren P, Zhu H. Jamming Mitigation via Hierarchical Security Game for IoT Communications[J]. IEEE Access, 2018, 6(99):5766-5779.

[14] Wang L, Wang L, Zeng Y, et al. Jamming power allocation strategy for MIMO radar based on MMSE and mutual information[J]. Iet Radar Sonar & Navigation, 2017, 11(7):1081-1089.

[15] Hu L, Wen H, Wu B, et al. Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things[J]. IEEE Internet of Things Journal, 2018, 5(1):219-228.