Anexo A. Electronic Support, electronic protect and radar jamming

In this appendix the topics under electronic warfare are further developed, especially electronic support and electronic protect, in electronic attack only radar jammings are commented.

A.1 Electronic support

Electronic support (ES) is defined as the measures to gather information from enemy's radio frequency (RF) emissions to allow an understanding of the enemy electronic system's characteristics.

There are two ways of using the information extracted from enemy's signals, if the signals are long processed and the procedure of extraction and analysis takes long time, then intelligence information is created but if instead, the signals are rapidly processed and the information is almost immediately used, then that is called combat information. ES creates combat information and it accomplishes its function fulfilling 3 objectives: intercept, identify and locate intentional and unintentional radiation.

ES determines what it is called the enemy's Electronic order of battle (EOB), this means, that ES's function is to reveal which kind of emitters is the enemy using, which frequency, from where is it emitting and all the possible related information. In order to achieve these aims, the ES systems have 2 principal roles: interception and geolocation.

A.1.1 Interception

The first of all the functions is to intercept the signal, this means, that the enemy emission has to arrive to a friendly receiver. This may seem trivial, but it is not. It is important to remark that usually these signals do not want to be detected, nor decoded.

The intercepted emitter has some countermeasures to fight against ES measures, these techniques belong to the EP systems and they are explained in the next section more deeply. It is possible to say that interception can be divided into 3 different actions that should be taken in sequence: detection, interception and

exploitation. Each one represents one phase within the ES process. Detection refers to actions taken in order to find where and when enemy signals are being transmitted in the electromagnetic spectrum. Once the signal is found, interception systems come to scene, these receivers have to be able to recognize which modulation is the enemy using in order to demodulate the signal to the baseband. When the signal has been demodulated then exploitation methods will extract the information from the signal. The level of protection a signal has against these actions is measured by three parameters, probability of detection (POD), probability of interception (POI) and probability of exploitation (POE).

The attacker has two ways to proceed if despite of all the difficulties (EP measures) he achieves interception. Once a signal is intercepted there are two approaches to extract information from it depending on the attack that should follow. If the attack only needs to know the frequency and the modulation, then the externals of the signal must be studied (i.e. frequency, bandwidth, baud rate, etc.). But if the attacker wants to know what information is being transported, then the internals of the signal must be studied, which is much more difficult because the attacker has to be able not only to detect and intercept the enemy signal, but also to decode it. This latter action is usually really complicated (if not impossible) because of encryption.

Detection systems are typically complex receivers capable of searching for weak signals in a wide section of the spectrum; those receivers use a waterfall display (figure A.1) in order to represent all the information with the highest accuracy. This display represents the signal's bandwidth on the X-axis and the duration on the Y-axis, while the signal's strength is represented with the boldness of the line. With this display the operator avoids skipping signals that are not continuous in time (such as push-to-talk PTT).

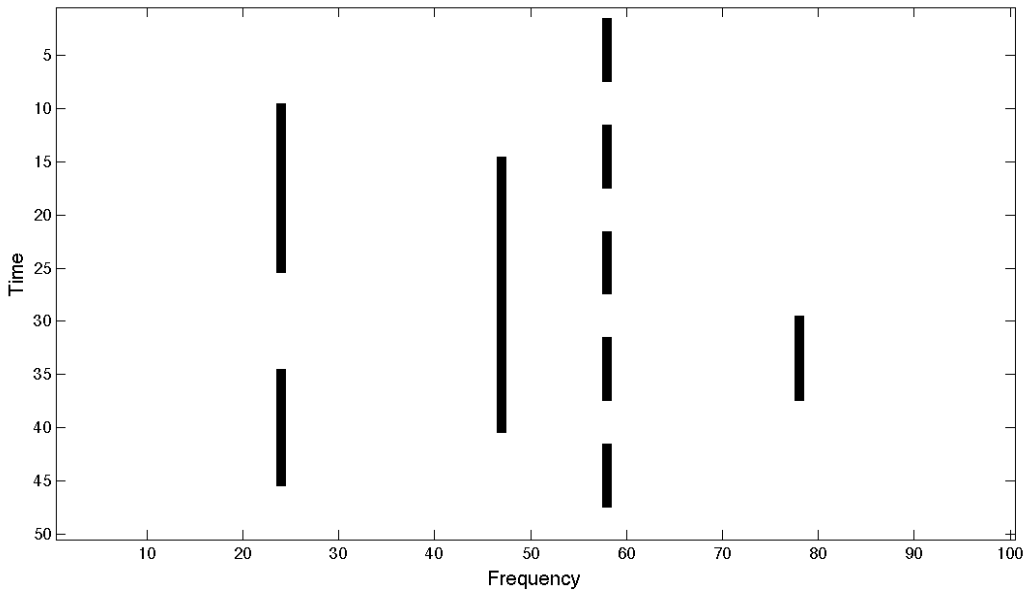


Figure A.1: Example of a waterfall display

A.1.2 Geolocation

The second interception's function is to place the emitters in the battlefield. Case ES used against radar systems, locating the main source (i.e. the radar emitter) would be a great advantage for the friendly forces. But if the friendly forces able to locate emitters in the battlefield they would be able to locate also the enemy forces. Mobile armies are usually (if not always) communicated by RF links, locating where those links start and end would represent a huge advantage in the war. Direction finding (DF) is the most common technique to achieve geolocation.

A.2 Electronic protect

Electronic protect (EP) concerns all the measures taken with the purpose of preventing the adversaries from using ES and EA systems on allied communications. In essence, EP provides protection against manipulation by an adversary, as well as unavailability of the friendly information to the enemies.

From the point of view of the intercepted emitter there are three countermeasures to fight against undesirable listeners. The emitter can endow the signals with low probability of detection (LPD), low probability of interception (LPI) and low probability of exploitation (LPE).

First step to secure allied signals is to prevent the observer from knowing that the transmissions are out there. Low probability of detection tries to hide our signals from enemy's receivers. There are some digital techniques that allow us to do that, but the most important are direct sequence spread spectrum techniques (DSSS). DSSS expands the spectrum used by the signal without increasing its energy; in essence, it expands our signal so much that in the end it is placed below the noise level. This makes it really difficult for a casual observer to figure out if a signal is being or is not being transmitted (figure A.2).

If the target cannot avoid the observer from noticing its transmission, he should prevent him from gathering useful information. Low probability of interception pursues that although the observer knows there is a signal there, he should not be able to trace or intercept it; this is achieved mainly through frequency hopping spread spectrum techniques (FHSS).

FHSS does not expand the spectrum used by the signal at a certain moment, but the signal's carrier jumps within a range of frequencies after a time called hop time (T_{hop}) and since the jumps follow a pseudorandom sequence the observer is not able to follow the data transmission.

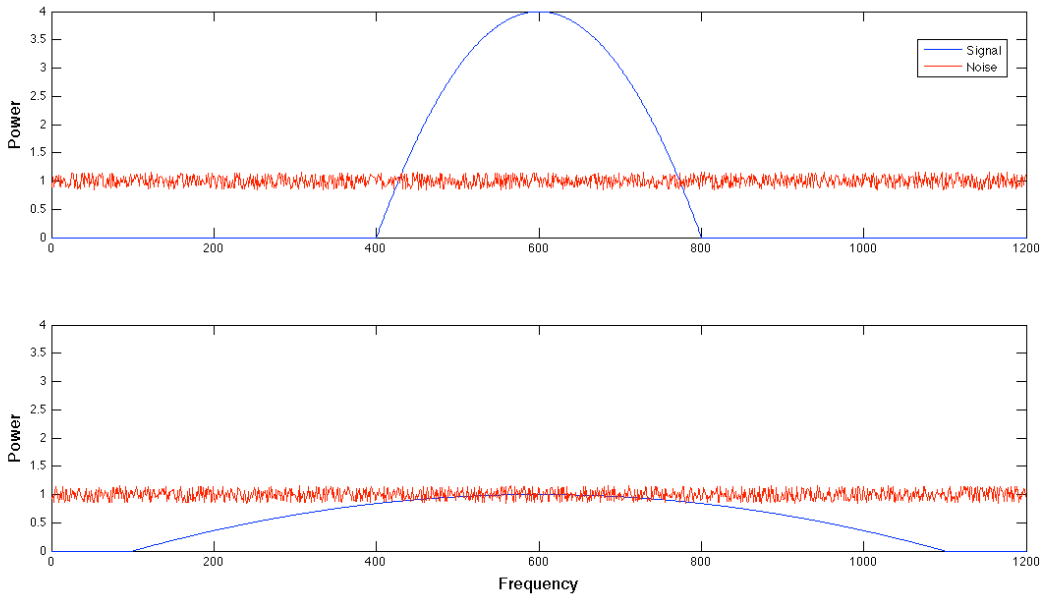


Figure A.2: Effects of spread spectrum techniques in a signal's spectrum

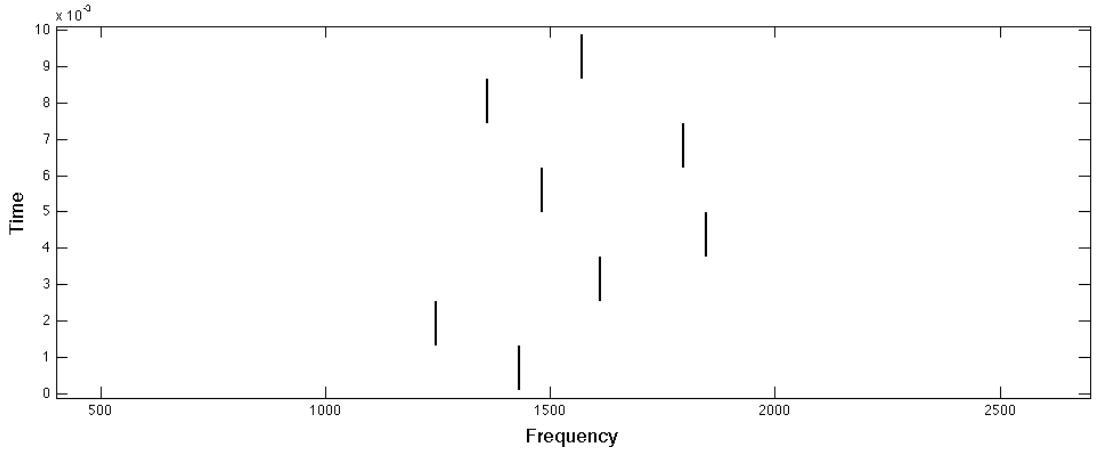


Figure A.3: Example of a frequency hop signal.

The jumps are so fast (for example more than 1600 times per second in case of Bluetooth) that makes really difficult to follow the transmission for someone who does not know in advance the next hopping frequency. The last protection that is here commented is low probability of exploitation. LPE focuses on encrypting the information transported, so it gets really difficult to extract for someone who is not allowed.

In addition to these measures there are three other important actions to inhibit adversaries from using friendly information to their good.

Emission control (EMCOM) is the most basic measure in EP. EMCOM regulates the emission parameters (power, frequency, antenna's height, etc.), so that the friendly signal does not arrive to the enemy. If the enemy is physically unable to see friendly signals because no electromagnetic waves arrive to his antennas, then communications are totally secure.

Other method within EMCOM is push-to-talk (PTT); the emitter has to activate the emitter in order to talk. This way, the only possible moment where the enemy could find friendly communication is when it is taking place, otherwise he is not aware of the system's specifications. This is useful because if nothing is being transmitted a casual listener would not be able to locate our signal and then he would continue searching in another part of the spectrum.

Other protection method is the screen jamming; this is basically placing a jammer between the friendly networks and the enemy ES systems. It is like deploying an electromagnetic curtain between the friendly emitter and the ES systems.

A.3 Radar jamming

Attacks against radar systems are now commented; this section's objective is to give a background on radar jamming, so that the differences between communication and radar jamming can be seen.

- **Range-gate Pull-Off (RGPO):** This technique is used against pulsed radars, basically consists on copying the reflected pulse and sending it back to the radar emitter with more energy than the real one. This way the receiver thinks that the target is not in its real position (since the position obtained by the receiver depends on the time it takes the pulse to come back).
  There is a version of this technique called Range-gate pull-in (RGPI) that instead of answering to the radar with a fake pulse, the jammer sends the fake pulse in advance so the receiver thinks the target is closer than it really is. In order for the jammer to be able to use RGPI it is mandatory to know the radar's pulse repetition interval (RPI), information that should be supplied by the ES systems.

- **Velocity-gate Pull-Off (VGPO):** Only useful against continuous wave (CW) and doppler radars, this technique is used to hide the target's real speed by changing frequency or phase on the fake reflected signal.
- **Inverse gain:** This technique is used to deny the radar's localization function. This technique consists of generating a contra-pulse with the opposite gain as the radar's pulse, so that for the radar the received signal is approximately a constant level (figure A.4).

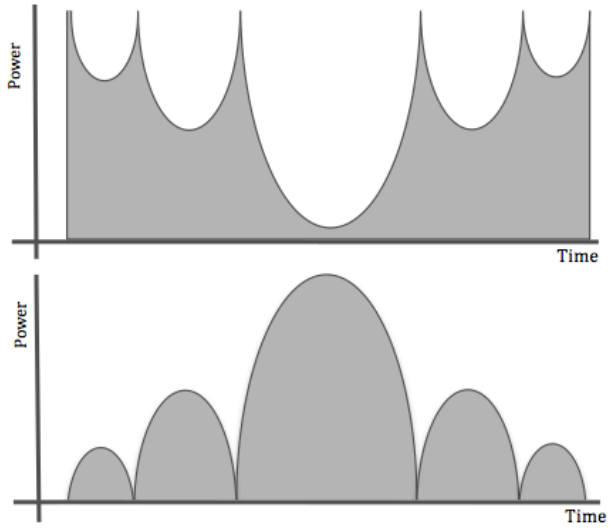


Figure A.4: Inverse gain Jamming. Figure above represents the pulse created by the jammer, while bottom figure is the radar pulse. Both pulse added return a constant power level.

- **Cover jamming:** This term refers to the same concept as it was in communication jamming, emitting high power signals in order to increase noise at the receiver so the SNR decreases as much as possible so the returned pulse cannot be detected.

- **Absolute gain control:** Radar systems are prepared to receive low energy and high energy signals, in order to achieve that properly they have an automatic gain control (AGC) system. The concept behind this attack is to surpass the dynamic range of the AGC system sending signals to the receiver with a much higher energy than the reflected pulses.
  This way the radar's receiver will change its gain to receive the high power signal but it will miss low powered signals (i.e. reflected pulses).

- **Terrain bounce:** Only against missile guided systems. It consists of sending a high-energy pulse with such an angle that after reflecting it hits directly the missile's receiver. Therefore, the missile would think its objective it is in the ground's direction.

Anexo B. Flight control systems

Flight control systems (FCS) are a very challenging part within the development of airplanes. The main objective of this system is to provide a structure so that the pilot is able to control the mobile parts of the plane in order to control the flight.

In the origins of aviation the pilot controlled the plane using a system of cables and pulleys, this generation of FCS were completely mechanical and the limits were the physical conditions of the pilot. Soon, the rapid evolution of aircrafts reached a point where no pilot was strong enough to move the direct mechanical FCS and hydraulic boosters became necessary.

Although hydraulic boosters opened the door to faster and bigger aircrafts, they also prevented the pilot from the feeling of what was happening outside the cabin (with direct mechanical connections the pilot could feel the speed, the pressure and other parameters). Then a new function for FCS appeared, now it had to procure the pilot external feeling, this is made through two different approaches: 'spring feel' and 'Q' feel.

The next step was removing all mechanical connections between the pilot and the FCS and create a fully electrically wired FCS, where the flight parameters would be measured by sensors strategically placed and their values would be displayed in the cabin's panel.

But as it happens now with the wireless technology, the wired FCS was also subject of many studies and it was not fully implemented until all the advantages were clear, all the problems were solved and the technology was safe enough.

The advantages of fly-by-wire (FBW) over the previous FCS generation (hydraulic boosted FCS) are many; this technology allows the pilot to control directly the attitude of the plane rather than the mechanical surfaces that control it. This way, heavy and big aircrafts became way easier to control.

Figure B.1: FCS evolution

In FBW, actuators control plane's attitude, this is achieved by changing the mobile parts of the plane. These mobile pieces control the different plane's movements, which includes: yaw, roll and pitch (figure B.2). All actuators that make those movements possible comprise what is called the primary flight control system. There exists as well, a group of actuators that form the secondary flight control system. This latter system's function is to allow flap and slat control, as well as speed brakes (figure B.3 shows the mobile parts of a plane).

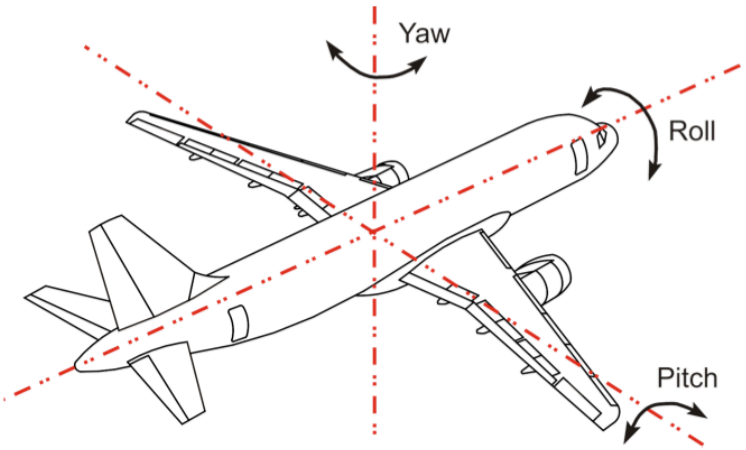


Figure B.2: Description of the movements controlled by the primary FCS

The pilot is able to control all those mobile parts thanks to a set of actuators placed along the aircraft; figure B.4 shows the basic compontents that comform a FBW flight control system. Those actuators are connected to a computer by wires, and it is this computer's job to translate pilot's orders into physical movements through actuators and mobile parts.

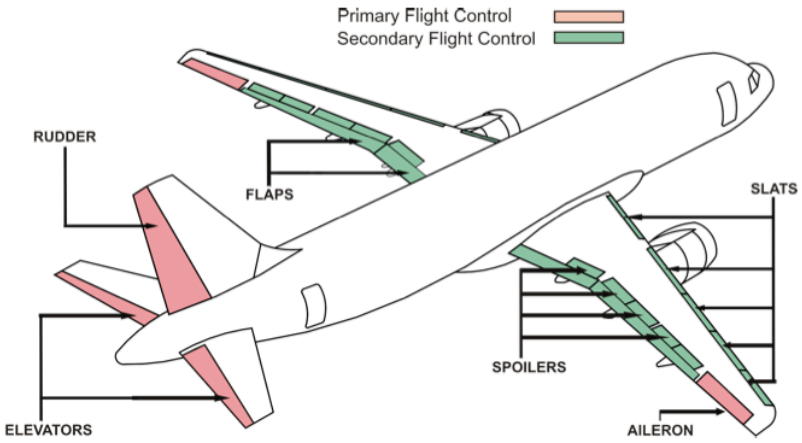


Figure B.3: Airbus A320 control surfaces

As FBW meant a great improvement in the aerospace industry, wireless FCS does not represent a deep change from fly-by-wire. Indeed the only thing wireless FCS change is the physical layer, but the function remains the same. It could seem that the wireless technology implementation in avionics has been too long delayed, but as said above, in a critical system (as FCS) new technologies have to be mature enough in order to be implemented as the main system.

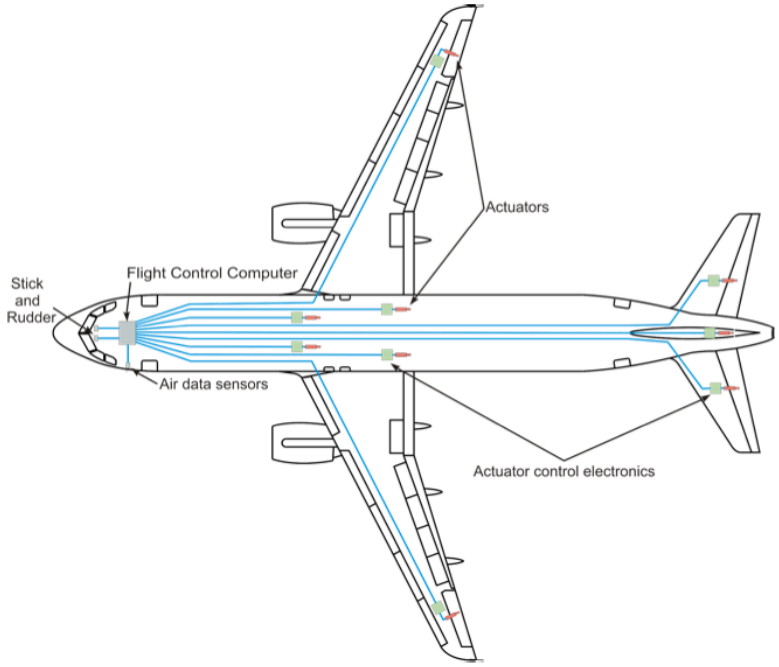


Figure B.4: Basic elements of a FBW flight control system

Anexo C. Attack scenarios and defenses

Within this appendix, the possible attacking devices and the possible scenarios during a plane's flight are analyzed. Then some other considerations about possible attacks and defenses are presented in order to give a global view of the possible threats.

C.1 Jammers

In this section some commercial and military communication jammers are introduced, so an overview of jamming devices can be built. In order to adapt the different kinds of jammers to the purpose of this diploma thesis devices are divided in three different types, according to its size.

Since jammers are mostly a military device, the information about them is regulated, some facts like the kind of jamming they use, their weight, size, antenna gain, etc. are not available. Even the catalogues of commercial jammers do not offer much information about their products.

First *pocket jammers* are presented. This group includes all the jammers (including the power source) that could fit in a standard hand luggage or could be carried by a passenger in a pocket. Hand luggage or cabin luggage is the luggage a passenger is allowed to carry in the passenger compartment. It is delimited by size (and usually by weight too), the maximum size is defined by the International air transport association (IATA) and it is 56cm wide, 45cm long and 25cm deep. Also jammers that fit in these measures but cannot be disguised will not be considered; it is assumed that these devices would not pass through the security control and the passenger would not be allowed to fly with it.

This category also includes most of the civilian jammers made for conference rooms or personal purposes. They are around 110x60x30mm big and have an output power of 2W. 2W is not two high; hence they are only useful in closed rooms and for short distances (maximum 15-20m). In its majority the jammed spectrum is between 850-2500 MHz. Those jammers are specially designed for Bluetooth, Wi-Fi, GSM, 3G, GPRS and some models may also include GPS. Although most of the models can work connected to a DC source, they also can work with a Li-ion battery and its autonomy is around 1 hour at full work.

The next group is *suitcase jammers*. Those are the jammer devices that have more or less the size of a suitcase and must be carried in the cargo compartment. These jammers are much more powerful that pocket jammers, in exchange they are much heavier, much bigger and much more difficult to disguise. The jamming frequencies really depend on each model; they go from a few MHz to a few GHz. Jamming frequencies are also focused on the usual communication channels (GSM, Wi-Fi, GPS, etc.), though some of them are also prepared to jam frequencies up to 10GHz. As said before, suitcase jammers are more powerful than pocket jammers; typical values for output power go from 30W until 300W, depending on the jammer, the frequency and the bandwidth jammed at the moment. Although all the jammers within this group allow direct current (DC) supply, for the purpose of this project we assume that they are working with the battery since they are supposed to be in the plane's cargo department.

The last group of jamming devices encloses all the jammers that cannot be carried by a single person; therefore they must be mounted on one or more vehicles. Within this group can be included jammers for convoys, carried by one of the vehicles and also dedicated trucks for war operations. One jamming system can be composed of more than one vehicle; it is possible for one vehicle to be the power source while other is the jammer itself, this way huge radiating power can be achieved.

The parameters these jammers work with are radiated power from 300W until 1100W, all these jammers must have a dedicated power supply according to their power requirements. These systems usually offer a wide range of choices for the clients; so they can choose the product that fits better with their desires. Due to this it is difficult to set a standard range of working frequencies, as well as other parameters for these jammers.

C.2 Flight phases

A flight's phase concerns any period during a flight that can be differentiated from the others by any reason. According to Common Taxonomy Team created by The International Civil Aviation Organization (ICAO) and the Commercial Aviation Safety Team (CAST) there are 13 possible phases within a flight. This analysis considers just the normal phases within a flight, herein are quoted the 8 phases belonging to a normal flight according to the Common Taxonomy Team.

- Standing (STD): Aircraft is stationary at the gate ramp.
- Pushback/Towing (PBT): Aircraft is moving in the gate, ramp or parking area assisted by a vehicle.
- Taxi (TXI): The aircraft is moving under its own power before the take off.

- Take off (TOF): From the application of take off power to an altitude of 35 feet above runaway elevation.
- Initial climb (ICL): From take off to the first prescribed power reduction or until reaching 1000 feet above runaway elevation.
- En route (ENR): From initial climb until approach time is reached.
- Approach (APR): Decent from cruise elevation (1000 feet above runaway elevation) until landing flare.
- Landing (LDG): From the beginning of landing flare until the aircraft leaves landing zone.

Another phase that should be mentioned is Maneuvering (MNV), this phase is usually not found in a normal flight but it must be taken into account. To this phase belongs all kind of low altitude/aerobatic flight operations.

Now that flight's phases are kwon, in the next part of this document the possible jamming scenarios are presented taking into account flight's phases and jamming devices.

Any of the phases above is suitable for an attack, although phases STD, PBT and TXI would not represent a major threat since the plane is still landed.

C.3 Scenarios

First of all, it is important to define what can and what cannot constitute a real threat. In order to consider the possible attack as a real threat, the jamming to signal ratio (JSR) is measured. This parameter measures the relation between the jamming signal and the desired signal at the receiver. The required JSR for a successful attack can vary but picking 10 dB as a threshold is acceptable because it is a value applied in many situations.

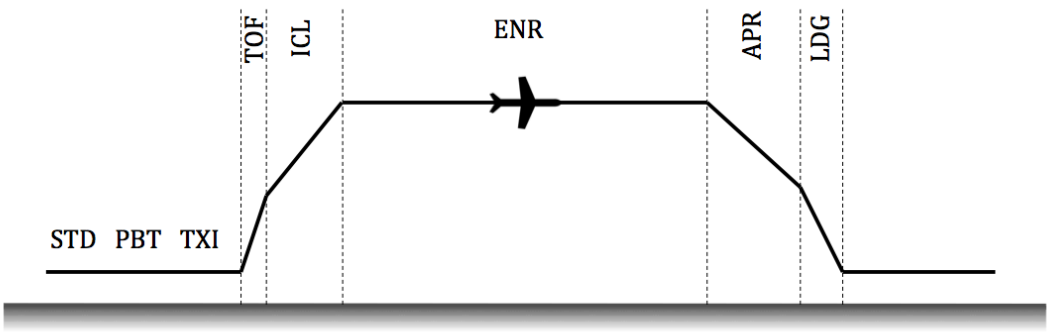


Figura C.1: Flight phases during an normal flight.

In order to calculate the JSR value it is necessary to know how to calculate the jamming power received J and the signal power received S, those steps are done with the following equations:

$$S = P_T + G_T - 32 - 20\log(F) - 20\log(D_s) + G_R \quad \text{(C.1)}$$

P_T = signal transmit power (dBm)
G_T = transmitter antenna gain (dB)
F = frequency (MHz)
D_S = distance from transmitter to receiver (km)
G_R = receiver antenna gain (dB)

$$J = P_J + G_J - 32 - 20\log(F) - 20\log(D_J) + G_{RJ} \quad \text{(C.2)}$$

P_J = jammer transmit power (dBm)
G_J = jammer antenna gain (dB)
F = frequency (MHz)
D_J = distance from jammer to receiver (km)
G_{RJ} = receiver antenna gain in the jammer's direction (dB)

Remark that these equations have into account just losses caused by free space propagation, in order to create a real model also absorption due to the plane's fuselage, seats, people, etc. should be considered. As it can be seen from the pair of equation (C.1) and (C.2), both received powers (S and J) answer to the same parameters but there are some differences that must be mentioned.

C.3.1 Distances

Except for mounted jammers, it is assumable that the longest distance between nodes will be larger than the shortest distance between the jammer and its closest node. In mounted jammers (except for the case when the jammer is carried on another plane) the distance no the nodes would be much bigger that distance between nodes. ENR flight phase is realized around 12000 meters above the ground. In the table C.1, average distances calculated for all jammers in a middle-sized aircraft (Airbus A320) can be seen.

C.3.2 Antennas

For this diploma thesis omnidirectional antennas are supposed in both systems (communication and jammer, except for mounted jammers), but the reality is, that the final communication system will have directive antennas. This way all the

interferences coming from undesired directions would be filtered. Moreover the efficiency of the communication system would be much higher since all the energy is radiated towards the receiver.

The reason why omnidirectional antennas are assumed in pocket and suitcase jammers, is because the person carrying the device cannot be sure about the position the jammer is going to be during the flight (specially in suitcase jammers). Mounted jammers are a special case. Since the distance between the jammer and the plane is in relation much bigger than the plane itself it is necessary to have a directive antenna, so that most of the power can be directed to the plane's position.

C.3.3 Power

According to the research that has been carried out during this diploma thesis, the maximum radiated power available for the jammers is around the values shown in table C.1:

Jammer	Distance (m)	Power (W)
Pocket jammer	0.3-3	0.2-2
Suitcase jammer	3-20	<300
Mounted jammer	500-12000	<1100

Table C.1: Relation of distance ranges between jammers and the closest node and max. radiated power for each jammer.

C.4 Jammer assumptions

In capitel 2 it was described that a jammeing's efficiency is highly dependant on the information the attacker has about the victim. In this project the worst case sceneario want to be simulated, therefore it will be assumed that the jammer is aware of almost all the transmission's parameters. In order to simulate the attacks the next assumptions are taken:

- The jammer always searches the most destructive jammer during the longest time possible.
- The attacker will try to place the jammer device the closest to the main node, case that is not possible the closest to the biggest node concetration.
- The attacker could have an adaptative device, which is able to change its jamming parameters (such as type of attack, bandwidth, power...)
- The jammer has a limited power source. Except for mounted jammers.
- The jammer uses omnidirectional antennas. Except for mounted jammers.

- The jammer knows OFDM's parameters
    - Bandwidth
    - Central frequency
    - Symbol period
    - Channel estimation technique
    - Channel coding
- The jammer is aware of TDMA's parameters
    - Slot length
    - Frame size
- The jammer knows all the anti-jamming defenses.

This assumptions mean that the jammer is capable of focusing all its energy exaclty on the OFDM's transmission band. At the same time, it is also assumed that the jammer knows the system's weaknesses and would use them to its profit.

C.5 Defenses

In capitel 3, it was settled that one of the requirements was designing a system with low power consumption. It is assumable then, that the maximum radiated power available in the communication system would be much lower than the power in a suitcase jammer or in a mounted jammer. In case the communication system had to face a jammer with such a high-radiated power in the same conditions there is no way the communication system would be able to perform its function in acceptable conditions.

Although this could sound quite discouraging, there are different defense levels that the jammer must surpass in order to perform a successful attack.

- **Human defense:** The first defense against jamming in case of on board jammers would be the airport security checks. The personal in charge of carrying these inspections must be capable of recognizing hazardous devices before they go into the plane.

- **Physical defense:** The next level of defense would be the physical isolations in the plane. For example, in order to prevent an attack from a suitcase jammer the cargo bay could have an isolated space where all the suitcases containing electronic devices could be stored.

- **Antennas:** Another protection against interference and jammers is the antenna's directivity. If the antennas used to build the flight control system are highly directional with low side lobes, only the jammers placed in the same

direction as the main lobe would be of interest. This would reduce for example the efficiency of mounted jammers placed on the ground, since the interferences would have a completely different arrival angle as the inside-plane links.

- **Electronic defenses:** To this group belong all the defenses implemented in the communication system and based on electronic devices and systems.

An actuation protocol has been designed in case a jammer is able to perform an attack successful enough to trigger the electronic defenses. This protocol settles in which order the different electronic protections must be applied in a hostile environment (not only under an attack, but also in a high interference situation).
This protocol differentiates between two different cases: small BER increment and big BER increment. Small BER increments are those cases where the BER increase but the system can still perform its function and the plane is still under control. On the other hand, big BER increments are those situations where the BER increases until the system is unable to realize its function (plane is no longer controllable), those situations are unacceptable and must be resolved immediately.

Small BER variations:

1. Increase transmission power
2. Select second transmission frequency
3. Change channel codification (digital modulation and error correction codes)
4. Change transmission frequency
5. Eliminate non critical nodes from the network
6. Change to back-up system

Big BER variations:

1. Select second transmission frequency
2. Change transmission frequency (if the BER does not improve until small BER levels jump to point 6)
3. Increase transmission power
4. Change channel codification
5. Eliminate non critical nodes from the network
6. Change to back-up system

Anexo D. Frequency allocation

When a new system able to emit radiation is introduced, it is the designer's work to conceive the system so that it does not interfere with the already allocated bands. Figure D.1 shows the current frequency allocation plan used in aeronautical communications.

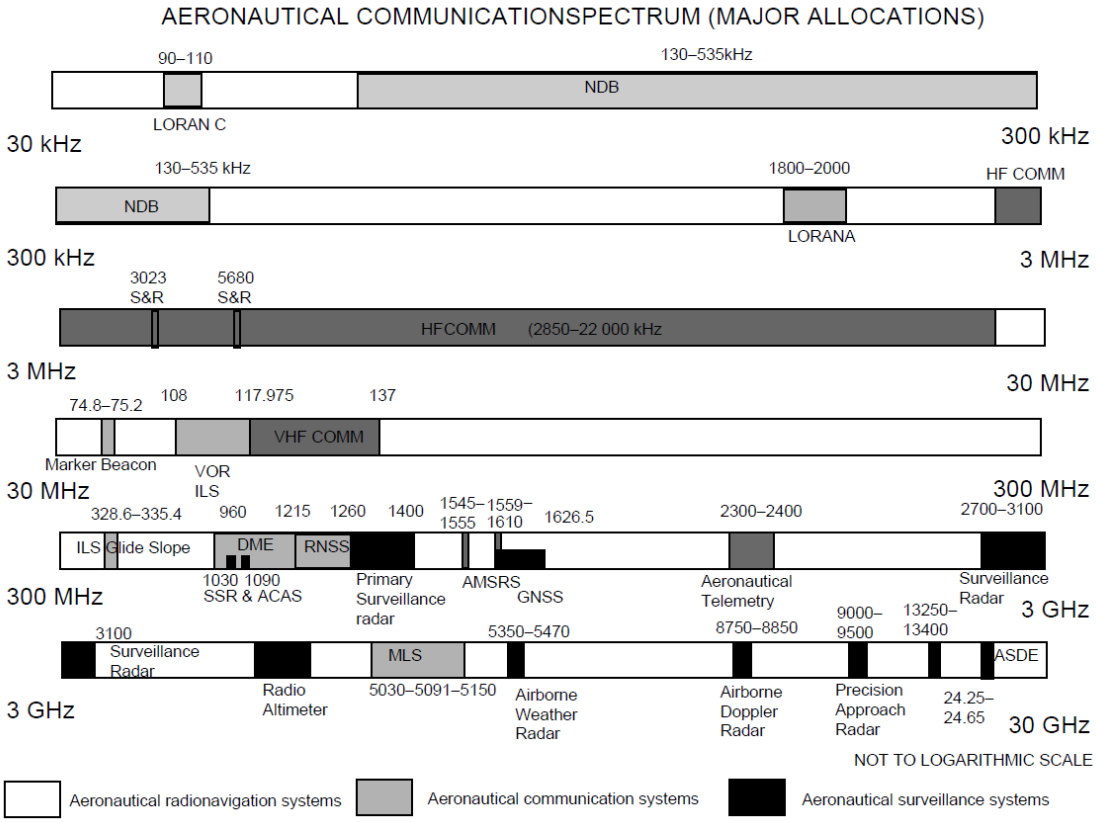


Figure D.1: Frecuency allocation for aeronautical communcations

This project must be design so it fulfills the plan above showed, as well as the necessities inherit to the project itself.
According to the project's nature it is necessary to place its allocation frequency high in the spectrum (i.e. above 3 GHz.). The main reasons are:

- A high frequency is more suitable due to the antenna's size.
- Lower frequencies are all allocated in the civil spectrum. Using the same frequencies would result into interferences while flying near cities and populated areas.

- Using an OFDM signal with a big bandwidth (around 60 MHz), which must be able to move dynamically its central frequency.

- High data transmission rates are required.

All the reasons above exposed suggest an allocation above 3 GHz.

According with what it has been exposed in section 4.9, the system needs two different frequencies due to redundancy. One of the requirements was that those frequencies have to be separated enough so channel effects could be considered independent. This requirement could be fulfill selecting between a range of frequencies around the 4 GHz and the other around the 20 GHz band. But as it has been said, in order to use those frequencies in the final project they must be first reserved by the competent authorities.

Anexo E. Simulink models

First level blocks as well as some features were described in section 5, this appendix offers complementary information to that section, so that all the models are in the end explained in detail. This appendix is organized as it follows: first the single frequency model is explained, in this section the blocks necessary to create an OFDM link are included (transmitter, channel and receiver), next, extra blocks to the OFDM link are described, that includes jamming, SNR estimation, difference mean and drawing blocks. To finish, the model with frequency redundancy is explained.

E.1 Single frequency model

First the single frequency model will be described. Most of the blocks are the same as in the two-frequency model; therefore they will be only here explained.

As explained in section 5.1, the single frequency model is formed by a transmitter, a channel and a receiver. Each of them composed by many subsystems. Figure E.2 shows the first level model.

E.1.1 Info generator

This sub block generates de information bits and separates them in frames. Bernoulli Binary Generator block generates the information bits with the appropriate data rate and structure: it generates messages (frames) of 480 bits, sending 1 bit every 4.843×10^{-8}. The subsystem can be seen in figure E.1.

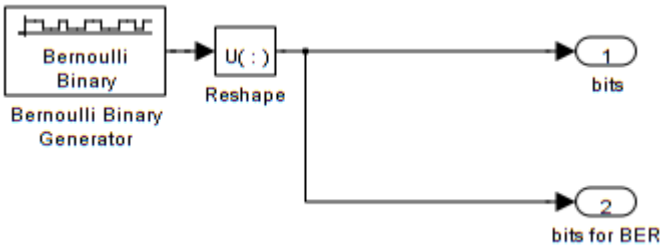


Figura E.1: Blocks in info generator block

E.1.2 Encoder

Encoder block applies error correction techniques to the link. Here the convolutional code, the repetition code and the interleaving are found (figure E.3).

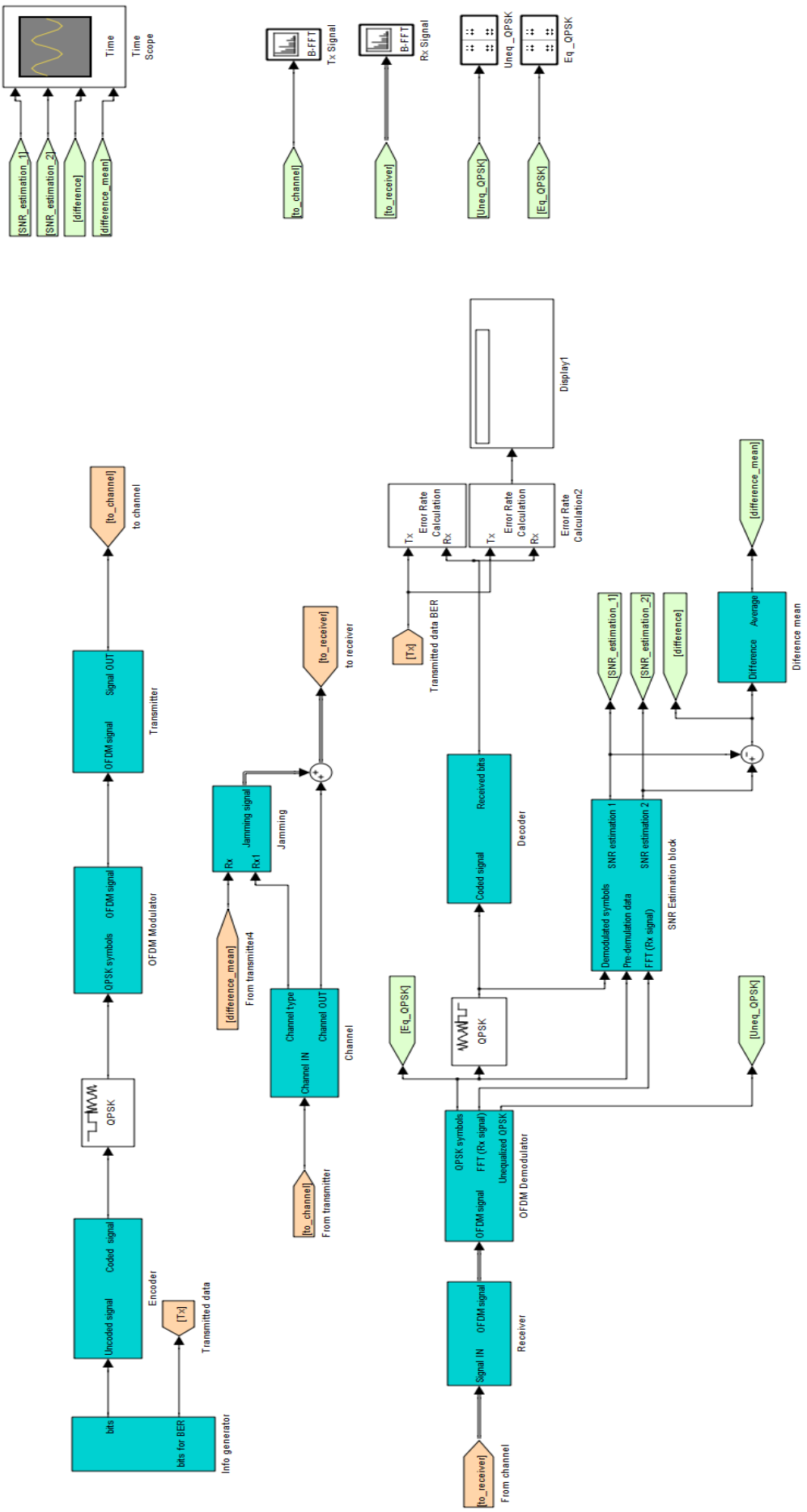


Figure E.2: Global view of the single frequency model

Convolutional code block applies the punctured convolutional encoding with a ratio ¾ and a Matlab expression poly2trellis(7, [133 171]) , the punctured code can be described under Matlab expressions as [1 1 1 0 0 1]. As well, the convolutional code resets every frame, so that the fact that each frame is sent by a different emitter can be simulated. After the convolutional code the repetition code is implemented.

In order to simulate more randomness two interleavers are simulated. The first interleaver is a matrix interliever block, which interleaves the input vector by a matrix of 48x40. The second is a random interleaver of 1920 elements with a random seed.

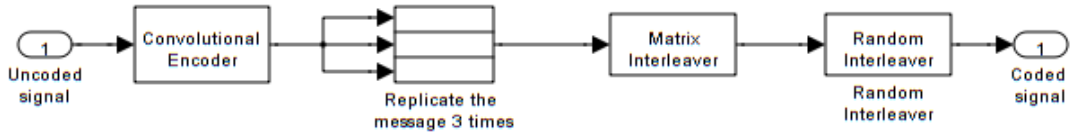


Figure E.3: Encoder subsystem

E.1.3 QPSK Modulator

Modulates binary data into a QPSK modulation according to the constellation showed in section 4.

E.1.4 OFDM Modulator

This block transforms the QPSK signal into a valid OFDM signal (figure E.4).

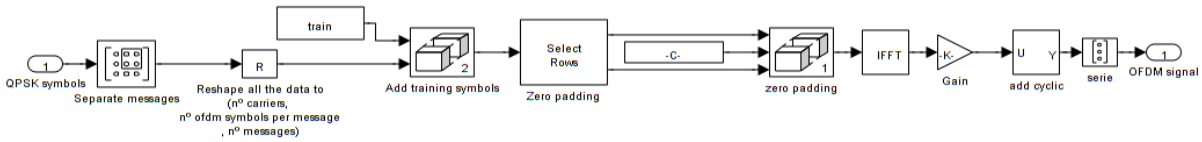


Figure E.4: OFDM modulator subsystem

Separate messages block is used to separate frames into a third dimension while reshape block is the equivalent to the serial-parallel block in an OFDM modulator. It transforms the serial data stream into a stream with the shape needed to conform the OFDM message (240 subcarriers x 4 symbols).

Next blocks add the training symbols to the message. Training symbols are 2 symbols stored in memory, which are added before the information symbols,

conforming a message to a shape of 240 subcarriers x 6 symbols. Zero padding blocks add the number of zeros needed to compute a 512 IFFT (i.e 512-240=272).

IFFT block computes the IFFT of input matrix along the 1st dimension with a length of 512, and gain block its used to maintain a normalized signal's energy after the IFFT.

Add cyclic bock is used to attack the cyclic prefix to the OFDM symbol; its length is of 102 samples.

The last block, called serie is used to transform the matrix shape of the message into a lineal data stream so it can be sent through the transmitter. It is equivalent to the parallel-serie block in the OFDM block diagram.

E.1.5 Transmitter

Transmitter block is a squareroot raised cosine filter that applies an oversampling of 10 samples. Filter gain is set to sqrt(10) so the signal in the output has a total energy of 1. The transmission power is settled through the trx_pwr variable, which is modified through the transmitter block's mask. The subsystem blocks can be seen in figure E.5.

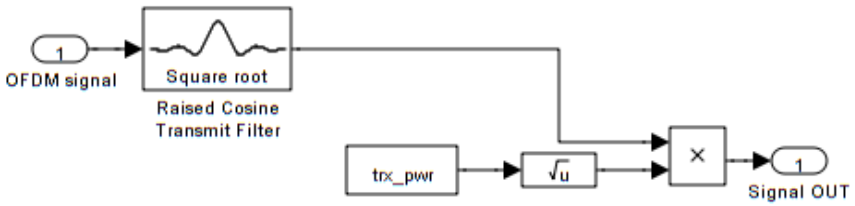


Figure E.5: Transmitter susbsystem

E.1.6 Channel

Channel block selects the type of channel to be simulated. Through the mask, the user can modify the variable "channel_select", which chooses the output of a multiport switch.

This subsystem contains the 3 different channel simulators: AWGN, multipath Rayleigh and flat fading Rayleigh. Both Rayleigh channels are enclosed inside an enable block, because this way the block does not execute unless it is needed, improving simulation speed. Figure E.6 shows the inside of the channel block.

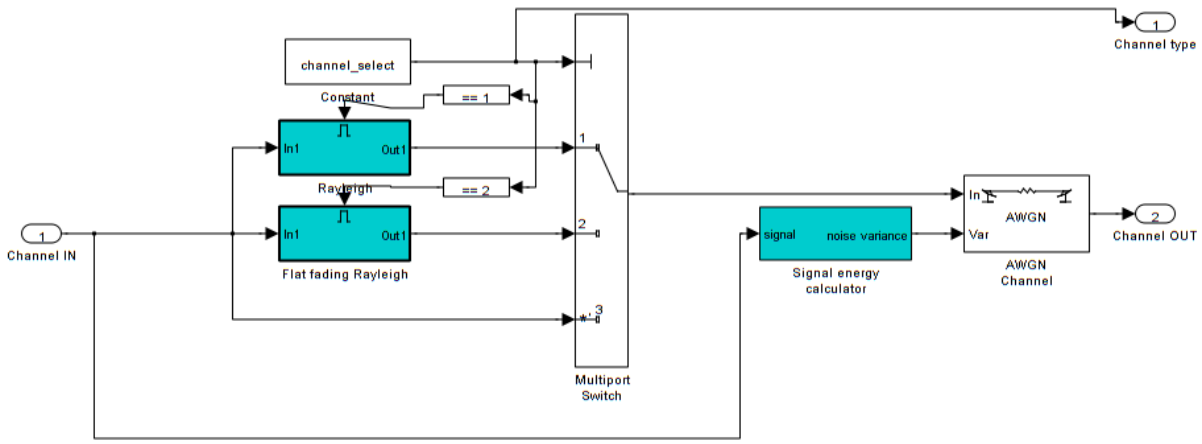
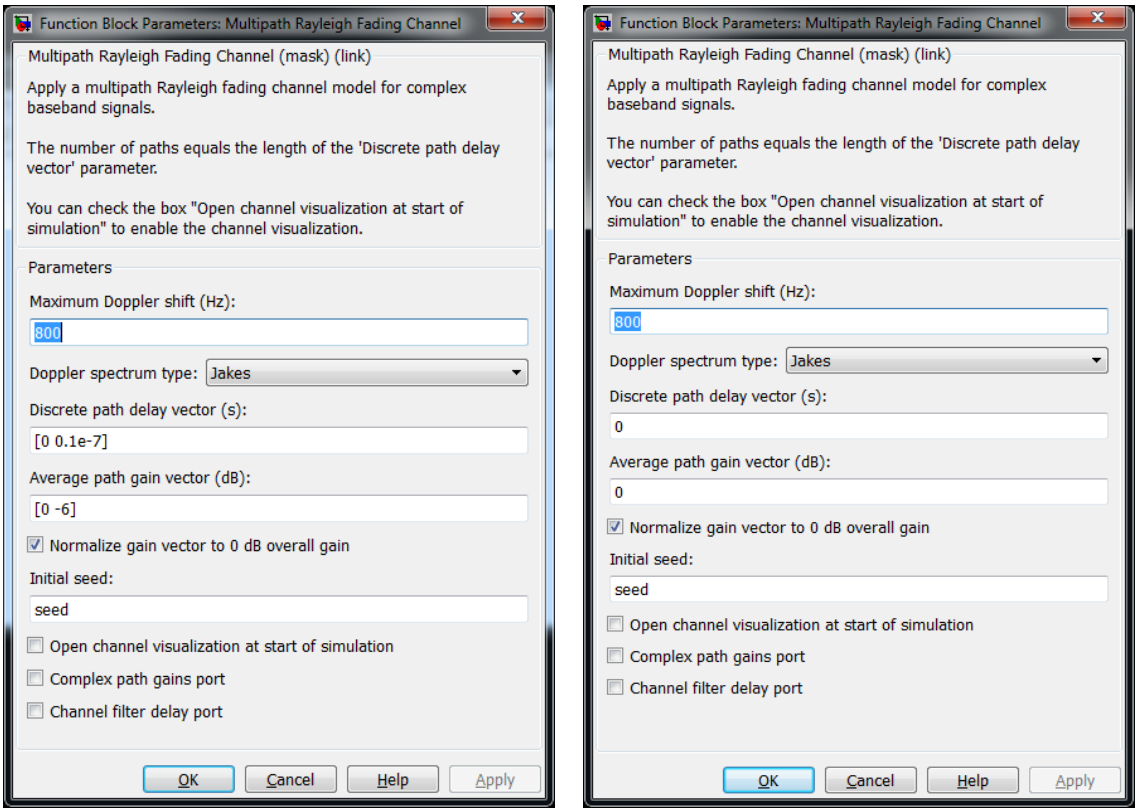


Figure E.6: Channel subsystem

Figures E.7 show the configuration parameters used in the Rayleigh channels.



a) Multipath Rayleigh b) Flat fading Rayleigh

Figure E.7: Rayleigh channels configuration

One of the model's objectives is to be able to calculate the BER with a certain E_b/N_0, selecting the E_b/N_0 for the simulation is done through external parameters and it is the AWGN channel's job to introduce the selected E_b/N_0 into the model.

In MATLAB's help documents can be seen that the equation that govern this block is:

$$NoiseVariance = \frac{SignalPower \cdot SymbolPeriod}{SampleTime \cdot 10^{\left(\frac{E_S}{10 \cdot N_0}\right)}} \qquad \text{(E.1)}$$

In order to calculate this variance blocks in figure E.8 are used. It is observable that the variance noise is multiplied by a factor of 512/240. This is necessary because the AWGN block adds the noise in time domain, regardless of the signal's spectrum. This way the noise energy is distributed along the signals spectrum uniformly. In the receiver, the subcarriers that belong to the zero-padding range are filtered, therefore the noise is also filtered. In order to generate the desired noise power in the OFDM transmission band it is necessary then to increase the power.

In relation to the other parameters in this equation, the transmitter oversampling sets the relation between the SymbolPeriod and the SampleTime to 10.

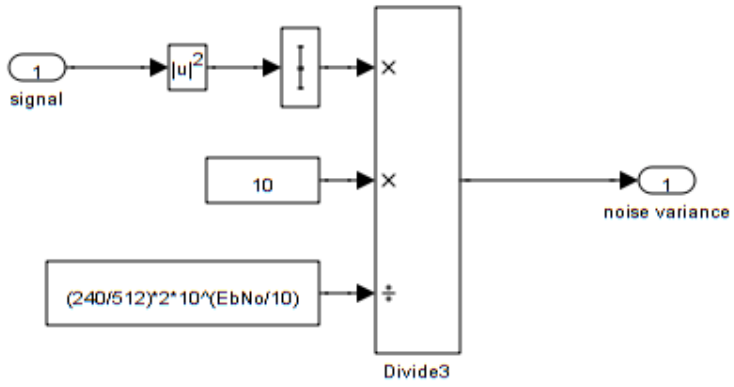


Figure E.8: Noise variance calculation blocks

E.1.7 Receiver

The receiver is, as shown in figure E.9, the square root raised cosine receive filter, (which is the pair of the transmitter filter) and a remove delay block. The receiving filter basically undoes what the transmitter filter does. And the deleting delay block is there to eliminate the delay that both filters introduce.

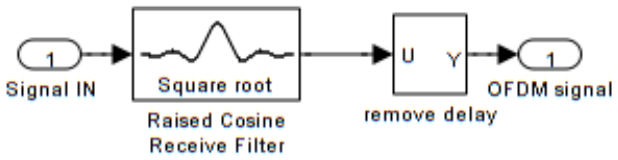


Figure E.9: Receiver subsystem

E.1.8 OFDM Demodulator

This block performs the opposite operations as the modulator. The difference resides in the LS equalizer, which will be more deeply explained. Figure E.10 shows the blocks forming this subsystem.

First blocks are the serie-to-parallel block and the remove cyclic block. Then a 512 size FFT is realized in order to obtain the QPSK symbols. The gain block is there to maintain the signal's energy at 1.

Remove zero padding block deletes the subcarriers that do not carry information. That is 272 out of the 512.

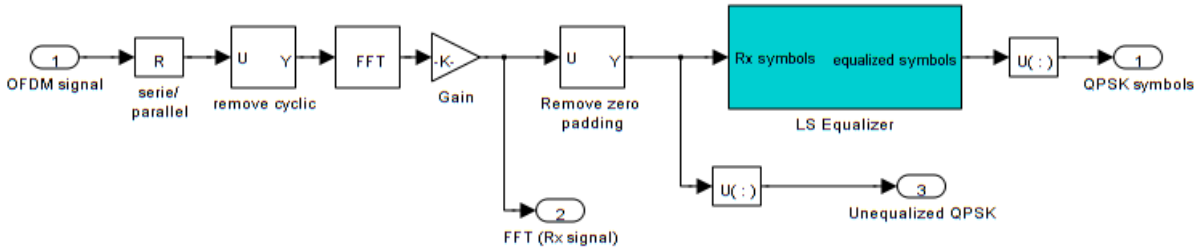


Figure E.10: OFDM demodulator subsystem

Next block is the equalizer. Bibliography about LS equalizers is extensive and will not be here reproduced, only the necessary equations to understand the blocks displayed in figure E.11.

Assuming a transmission equation as in (E.2), where in frequency domain:

X: Transmitted signal
H: Channel response
N: AWGN noise
Y: Received signal

$$Y = XH + N \tag{E.2}$$

Channel estimation obtained by an LS estimator answers relation (E.3).

$$H_{LS} = X^{-1}Y \tag{E.3}$$

Then, in order to apply this channel estimation on Y we can use equation (E.4).

$$X = YH_{LS}^{-1} \tag{E.4}$$

Which is the equation implemented in Simulink.

Then just the average between the two training symbols is done. Afterwards the estimated channel is replicated four times, one for each information symbol that has to be equalized. This process can be seen in figure E.11.

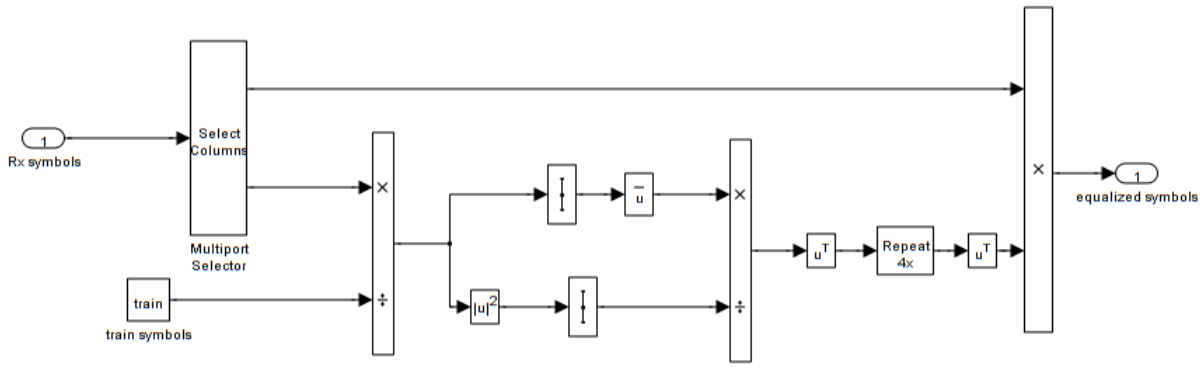


Figure E.11: LS channel equalizer subsystem

The last block in the OFDM demodulator is the parallel-to-serie converter.

E.1.9 Decoder

After QPSK demodulator, where the QPSK symbols are demodulated into bits, comes the decoder.

This block's function is undoing the interleaving, the convolutional code and the repetition code. The blocks configuration is the same as it was in the encoder.

The repetition code is demodulated through a voter. In order to implement this in an efficient way the message is divided in its three repetitions and then a logical circuit is implemented following the truth table shown in table E.1. The output bits are the bits received; those are compared to sent bits in BER calculators to obtain the BER results.

b_1	b_2	b_3	Output
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Table E.1: Voter's truth table

E.2 Extra blocks

The previous section explains all the blocks that conform the simple single frequency model. In this section the extra block that do not directly take part in the link are commented. Those are the jamming block, the SNR estimation block and the difference mean block.

E.2.1 Jamming block

This blocks implements the creation of all jamming types as well as part of the cognitive radio features' simulation. Figure E.12 shows all the blocks that conform the jamming subsystem.

The jamming block possesses a tunable mask, where some of the jamming parameters are introduced. Those are:

- Jamming enable: enables jamming
- Jamming type: selects the type of attack
- Jammer available power (W): introduces the power of the jammer in Watts
- Jamming attack delay after frequency hop: this parameter regulates the time the jammer needs to find the new system's transmitting frequency after a hop due to a jamming detection.

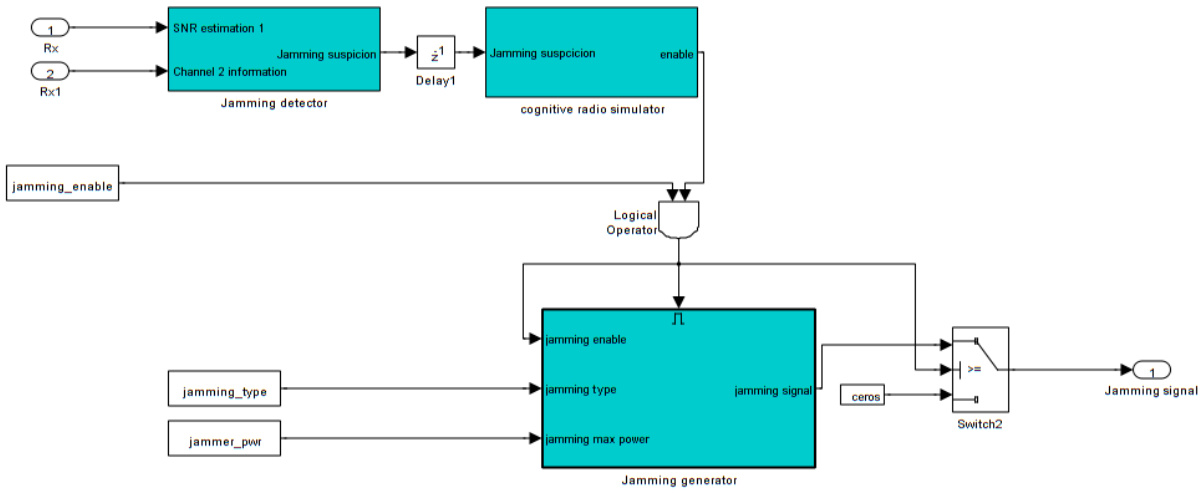


Figure E.12: Jamming subsystem

First mention that the jamming is only active when both enables are at '1'. Otherwise the block does not execute, saving some execution time. The switch before the out port is necessary in order to introduce ceros in case the jamming was

active and suddenly turned inactive, if not the jamming generator block would maintain the output it had when it changed from enabled state to disabled.

Inside jamming generator subsystem, the blocks shown in figure E.13 can be found. The blocks are placed simulating a typical case structure. In case jamming type is “Partial band jamming” then only the corresponding block is executed. The switches after the jamming blocks are there for the same reason explained above.

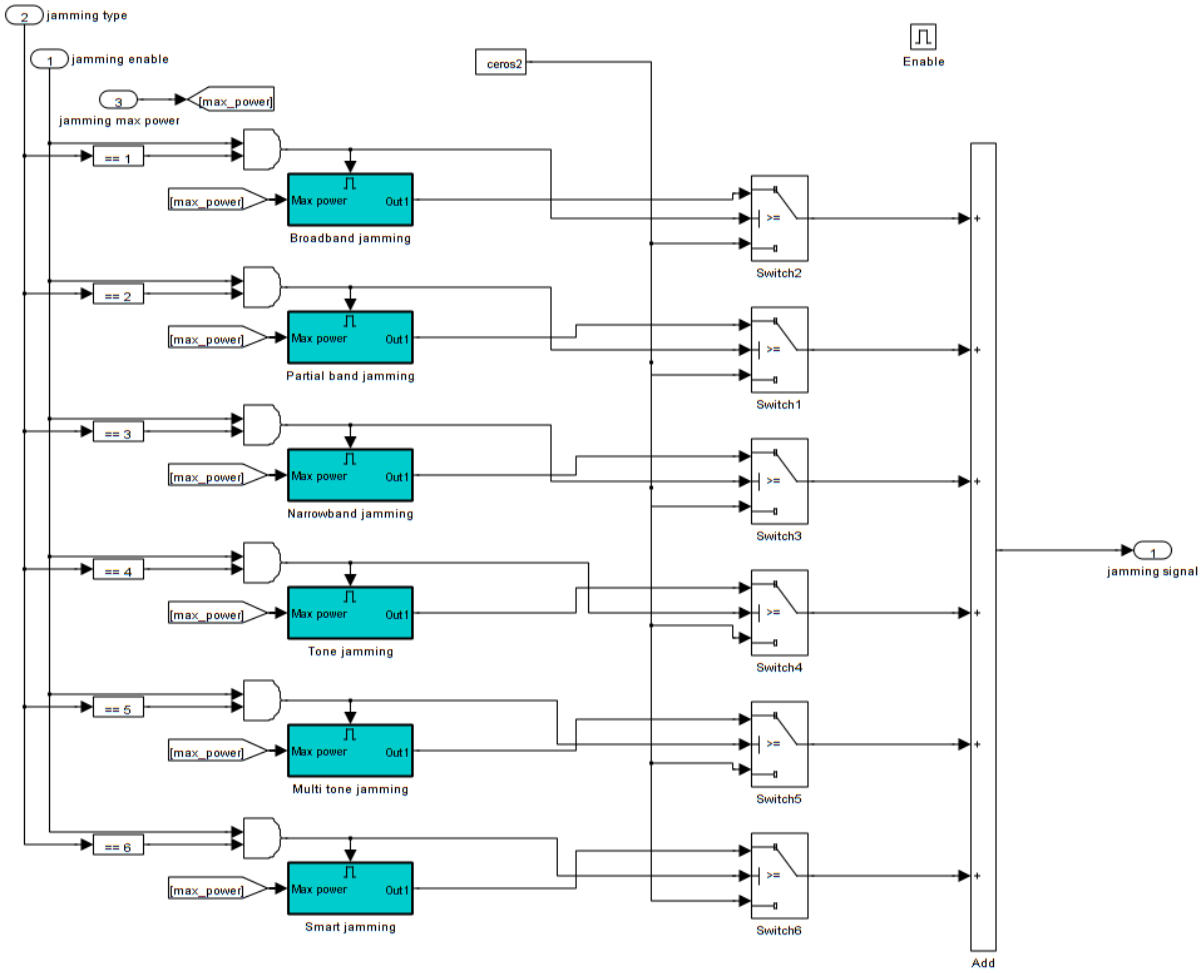


Figure E.13: Jamming generator subsystem

The three jammings that belong to noise-jamming group have the same block structure (figure E.14). Random noise is generated with such a variance, that afterwards the noise signal is filtered to the desired bandwidth, its power is 1. Then the jamming signal’s power is scaled by a factor in order to generate a signal with the power specified in the jamming block’s mask. The variable Max power, regulates the final jamming signal’s power. This variable is control through jamming block’s mask.

Tone jammings are modeled just creating tones with a random phase, one tone in case of tone jamming or multiple tones in case of multitone jamming. Their amplitudes are as well calculated in order to create a jamming signal with energy 1.

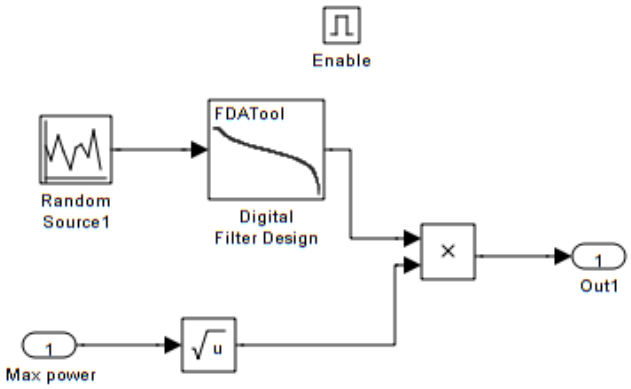


Figure E.14: Noise jammings generators

Smart jamming is created in a similar way as noise jammings; the main different is that all the power is placed in the first amount samples (the equivalent to the number of samples that belong to the training symbols).

After the jamming generator, the jamming detector is commented. This block's function is to decide if the system is being attacked, the inputs to this block are the average difference between the SNR estimators for the last K frames and the type of channel the system is simulating. In case an attack is detected the block's output would be '0', otherwise it output remains at '1'.

The detection is done comparing the average mean with a value that depends on the channel that is being used and the E_b/N_0 that the system is simulating. In case the channel is AWGN then the average difference is compared to 3. Otherwise the value is obtained from a lookup table that is filled with empirical values calculated for each E_b/N_0. The description of this process has been deeply developed in chapter 5, therefore it will not be here repeated.

After detector block a delay is introduced to break the loop created by the mean difference value.

Cognitive radio simulator block simulates the automatic frequency hop after jamming detection is positive. This is simulated by turning off the jamming during a certain time, then the jamming is turned on again simulating that the jammer is working in the new frequency. This block implements the following high level code:

```
while system_is_running do
  if espera=0
                then
                    if jamming_suspicion=0
                       then out=0; espera=defense_level;
                       else out=1;
                  end
                else
                     espera=espera-1;
                     out=0;
            end
end
```

This code transformed into Simulink blocks can be seen in figures E.15 and E.16.

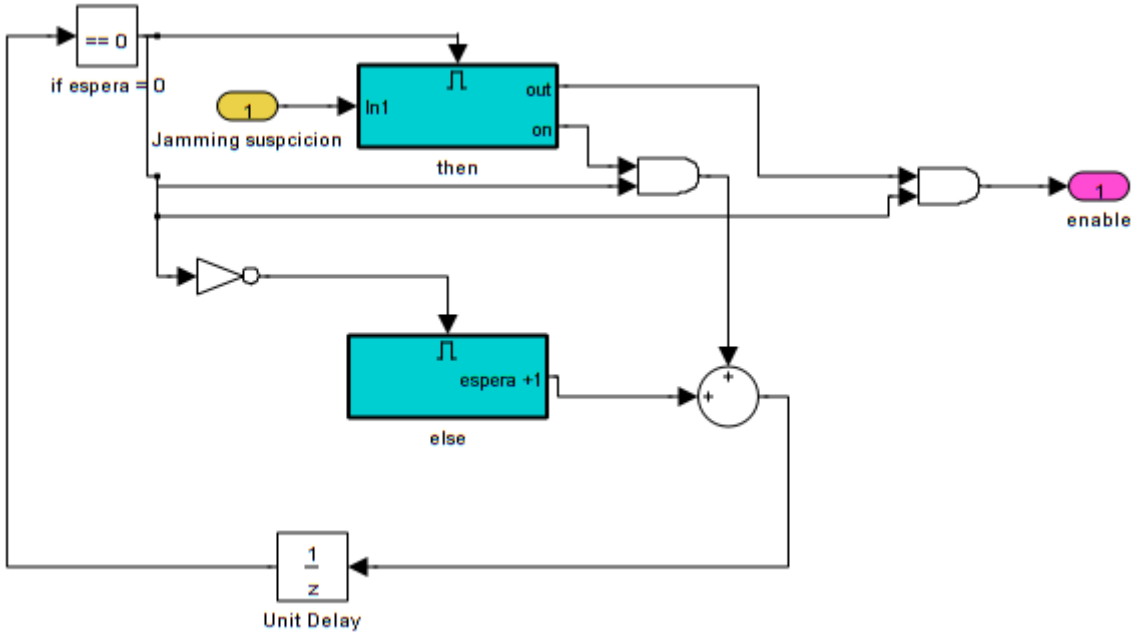


Figure E.15: Cognitive radio simulator subsystem

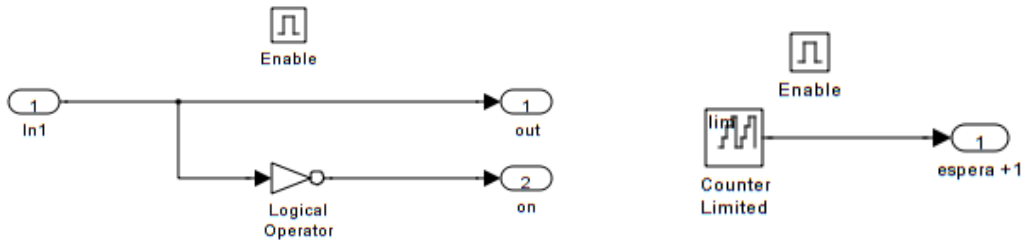


Figure E.16: Left shows the “then” block inside cognitive radio simulator subsystem, right shows “else” block.

E.2.2 SNR estimation

As explained in section 5.3, this block performs both SNR estimations needed in the system. Global view of the block can be seen in figure E.17.

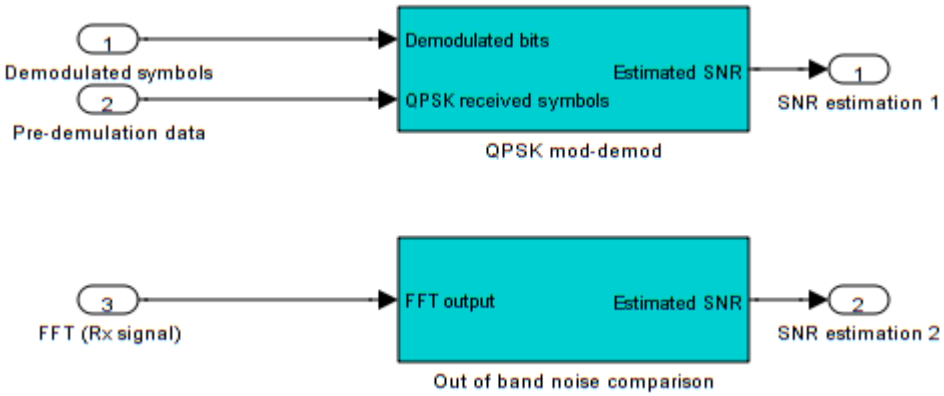


Figure E.17: SNR estimation subsystem

Estimator 1 accomplishes the estimation through the method described in section 5. Blocks can be seen in figure E.18. After calculating the noise power the SNR is calculated calculating the inverse of the noise's power (QPSK signal is normalized to energy 1).

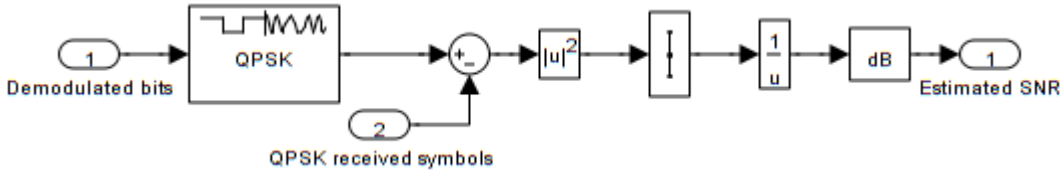


Figure E.18: QPSK mod-demod based estimator subsystem

Estimator 2 implements the method explained in section 5. Blocks can be seen in figure E.19.

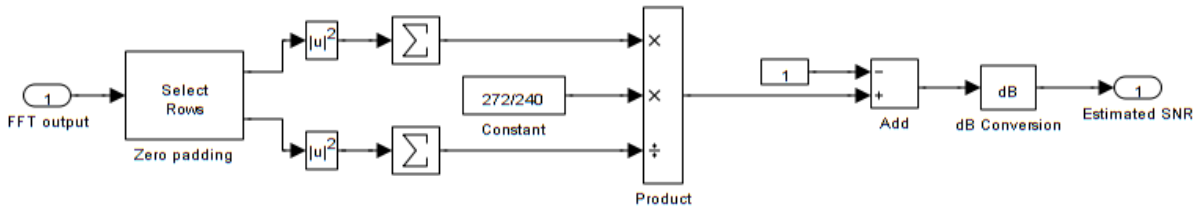


Figure E.19: Out of band noise estimator subsystem

E.2.2 Difference mean

The difference mean block calculates the average of the last X frames' SNR estimation difference. Figure E.20 shows the blocks that build this subsystem.
First buffer controls the number of frames used to calculate one average, through its size. The higher this value is, the lesser false alarms appear and the slower the system answer is. Unbuffer block is necessary to transport the output to the jamming block.

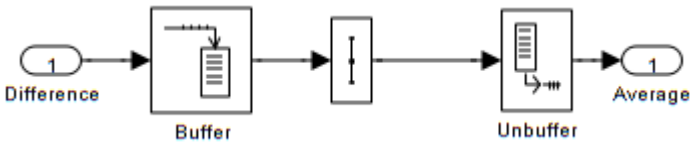


Figure E.20: Difference mean subsystem

E.2.3 Drawing blocks

In the single frequency models there are 5 different blocks able to display data. They are all placed in the right side of the model.

One of the blocks is a time scope, able to display the information about the SNR estimation values, as well as the difference and the average difference values. This way can be seen how the system behaves once the jamming is activated.

Spectrum scopes are also present; with them, the power density spectrum of the transmitted and the received signal can be displayed. The other two displays show the QPSK constellation formed by the received data before and after the LS equalizer.

E.3 Two frequency model

The two-frequency model has almost the same blocks (except voter block) as the single frequency model but duplicated. The blocks are as well reordered in new subsystems so the model is easier to follow (figure H.21).

E.3.1 Transmitter

Transmitter block has basically the same blocks as in the single frequency model. The only difference resides in the two transmitters (one for each frequency).

In this model, all the input parameters are introduced through the mask in the transmitter block. The parameters are grouped into buses that go to the block where the values are needed. Both, transmitter's mask and block diagram can be seen in figures E.22 and E.23.

E.3.2 Channel, jamming and receiver

The channel, jamming and receiver blocks have no differences compared to the blocks used in the single frequency model.

E.3.3 Other interferences

This block performs no function, it is a dumb block prepared to save space in order to simulate other interferences such as natural and unintended in future versions of this model.

E.3.4 Voter

This block is in charge of selecting which frequency should be listened each moment. The logical circuit is calculated through the truth table described in section 4.6. Depending on the output value bits from frequency 1 or frequency 2 are selected. Add and gain blocks are only for displaying purposes.

E.3.5 Display

In the two-frequency model it is possible to display how the system answers to an active jamming, as well as the response speed. Figure H.25 shows a screenshot taken during a simulation.

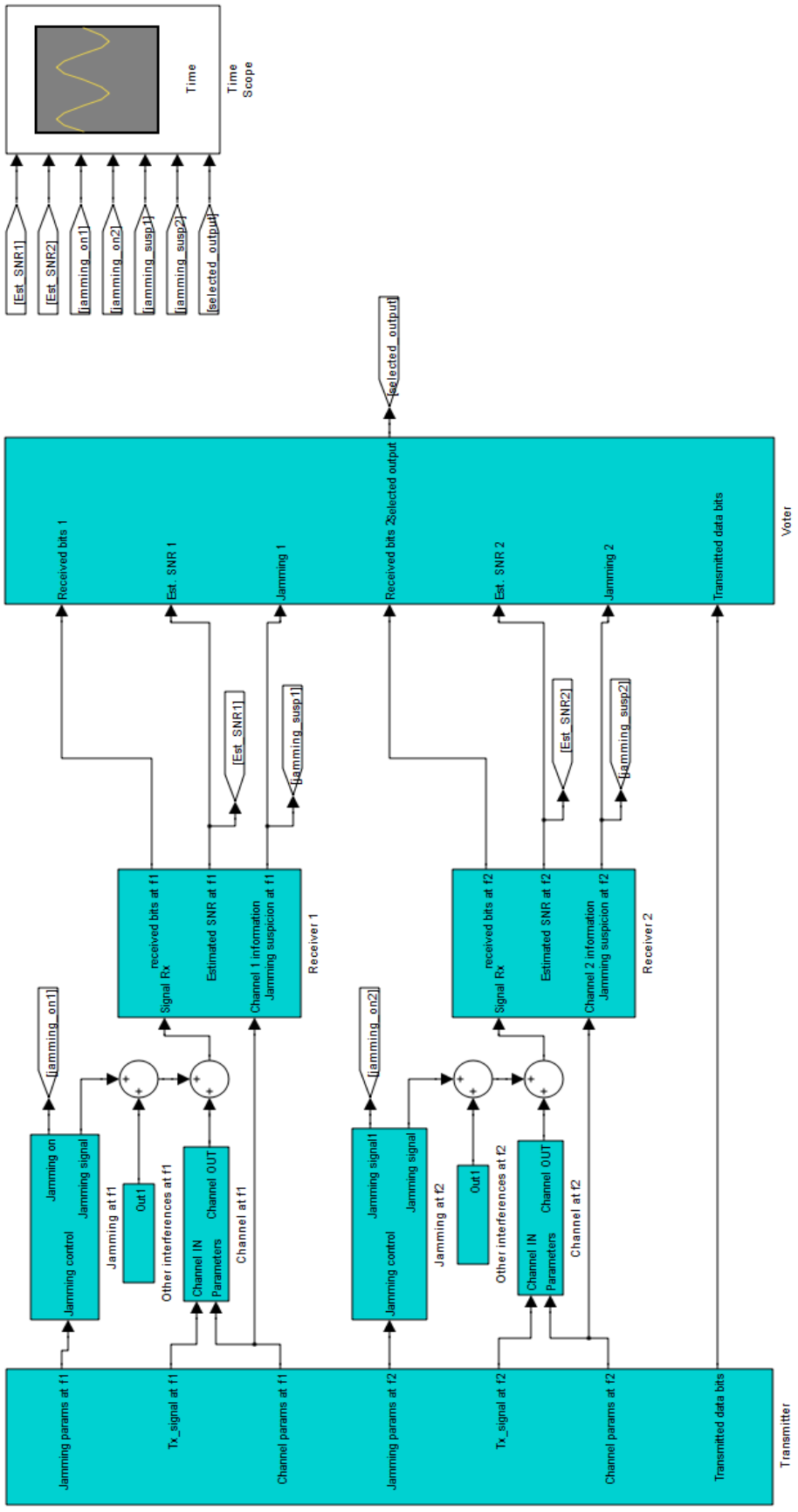


Figure E.21: two-frequency system model

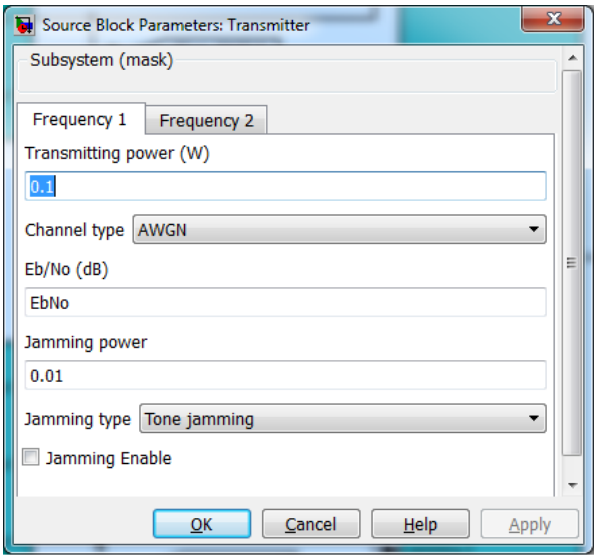


Figure E.22: Transmitter's block mask. Show all tunable parameters in the system

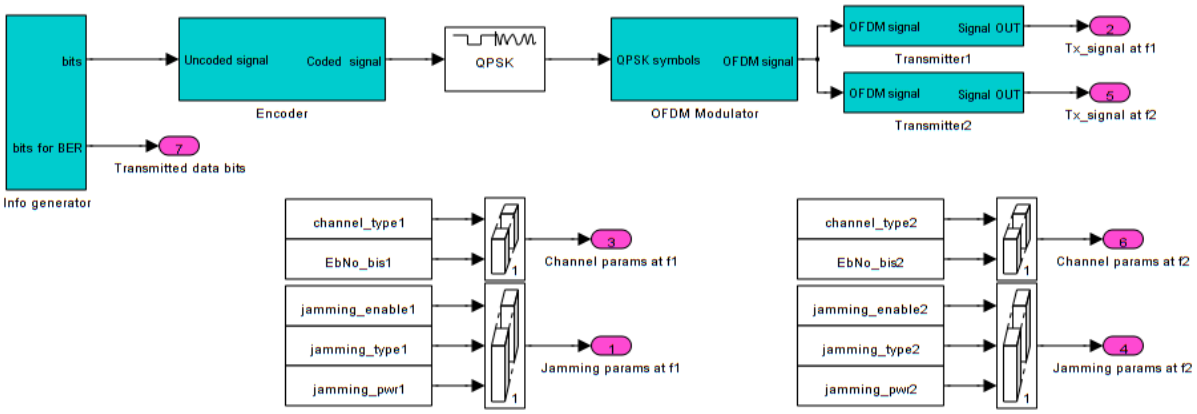


Figure E.23: Transmitter subsystem

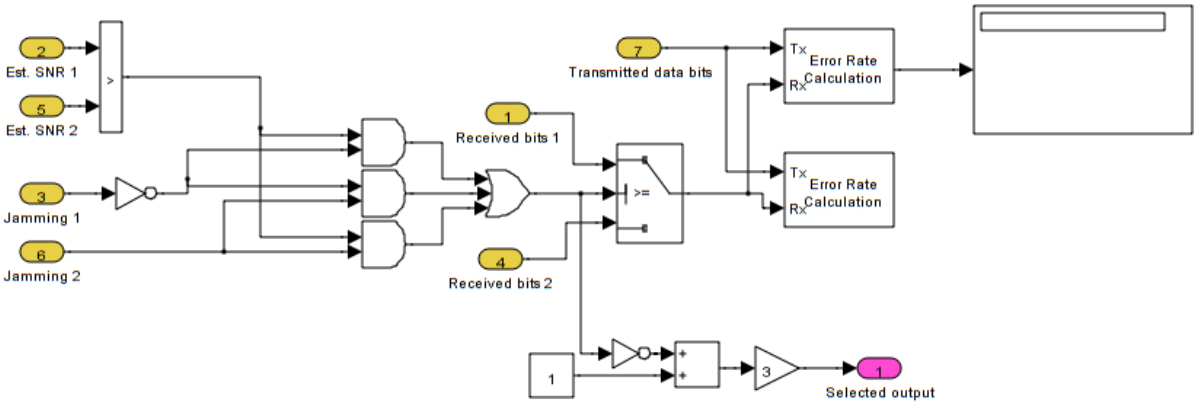


Figure E.24: Voter subsystem

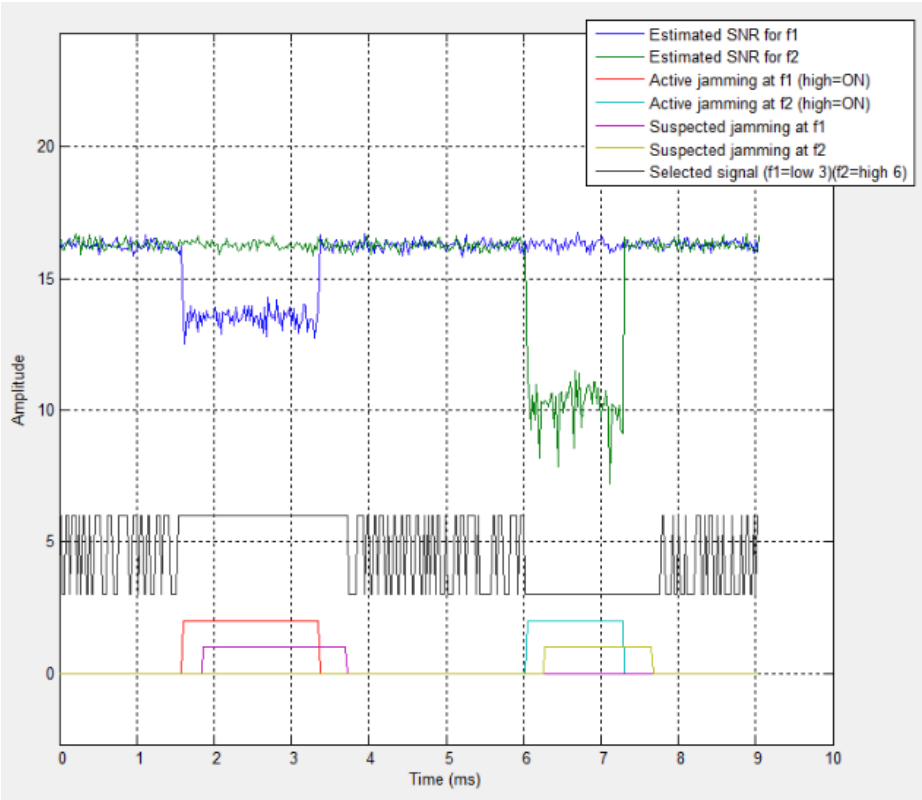


Figure E.25: Example of a working scope in the 2 frequency system

Anexo F. Evolución temporal

F.1 Hitos del proyecto

1. Fase de documentación
   1.1. Guerra electrónica
   1.2. Sistemas de Control de vuelo
   1.3. Sistemas de comunicaciones

2. Fase de diseño
   2.1. Diseño del sistema de comunicaciones

3. Modelado
   3.1. Familiarizarse con Simulink
   3.2. Creación del modelo del enlace monofrecuencia
   3.3. Primeros tests, comprobación del sistema monofrecuencia
   3.4. Simulación de los jammings
      3.4.1. Documentación acerca de la simulación de jammings
      3.4.2. Creación y simulación de los jammings
   3.5. Diseño e implemenatción de las medidas de mejora
      3.5.1. Redundancia en frecuencia
      3.5.2. Simulación de radios cognitivas
      3.5.3. Redundancia en tiempo y datos

4. Simulación
   4.1. Llevar a cabo las simulaciones necesarias

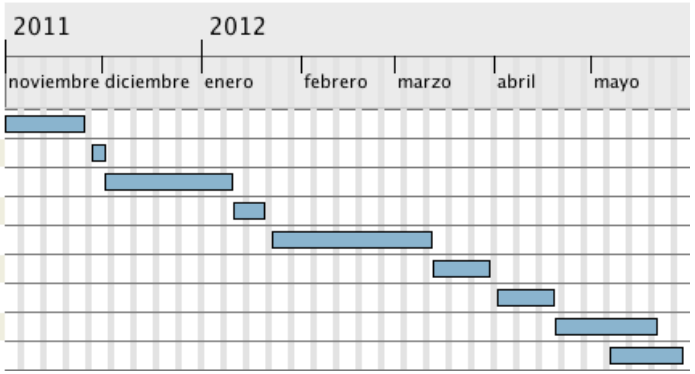
5. Resultados y conclusiones
   5.1. Estudio de los resultados obtenidos en las simulaciones
   5.2. Detectar puntos débiles del sistema
   5.3. Plantear mejoras
   5.4. Proponer lineas de futuro

6. Documentación en la memoria

F.2 Diagrama de Gantt

A continuación se expone el diagrama de Gantt correspondiente al proyecto realizado.

Nombre	Fecha de inicio	Fecha de fin
Estudio y documentación: Guerra electrónica	1/11/11	25/11/11
Estudio y documentación: Sistemas de control de vuelo	28/11/11	1/12/11
Estudio y documentación: Opciones para el sistema de comunicaiones	2/12/11	10/01/12
Diseño del sistema	11/01/12	20/01/12
Modelado del enlace básico y el jamming	23/01/12	12/03/12
Diseño de sistemas de mejora	13/03/12	30/03/12
Modelado de los sistemas de mejora	2/04/12	19/04/12
Simulaciones	20/04/12	21/05/12
Documentación en la memoria	7/05/12	29/05/12



Figrua F.1: Diagrama de Gantt