Analysis of Spread-Spectrum Algorithms to Prevent Jamming Attacks in Safety-Critical Applications

Ayşegül Ağlargöz

Institute of Flight Systems, German Aerospace Center (DLR),

Braunschweig, Germany.

Wireless Innovation Forum Conference on Wireless Communication Technologies and Software-defined Radio, 15 - 17 March 2016, Reston, Virginia.

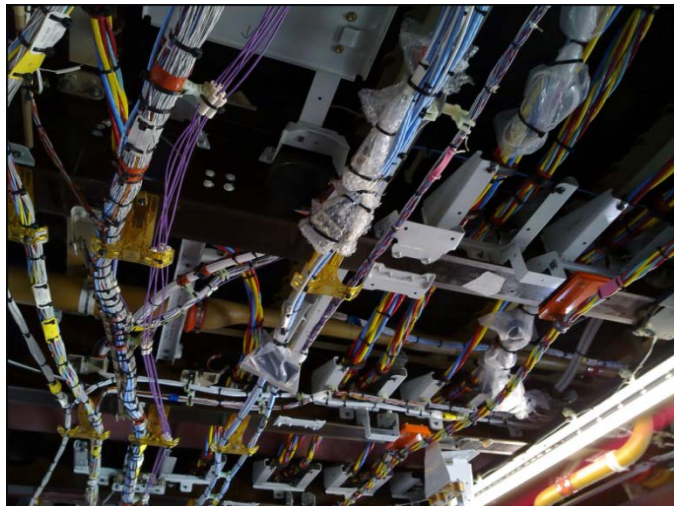
DLR

Outline

- Introduction
- Spread-Spectrum Techniques
- Simulation
  - System Parameters
  - Modelling of Jammers
  - Evaluation of Intermediate Results
- Hardware Development
  - Specifications of Development Platform
  - FHSS Transceiver Implementation
- Results & Conclusion

Introduction (I)
Drawbacks of Cables and Wiring in Aircraft

- Weight
- High cost
- Reduction of safety & reliability
- Limited functionality
- Limited expansion capabilities
- Physical limitations



Main deck ceiling of a passenger aircraft[1]

10 AWG left emergency bus feed[2]

Damage to galley feeder cables[3]

Damaged loom and hose[4]

[1] https://www.flickr.com/photos/a380spotter/4832163708, [2] TSB, In-Flight Fire Leading to Collision with Water, A98H0003
[3] AAIB Field Investigation, 2003, B737-300, G-LGTI, EW/C2003/07/07, [4]AAIB Field Investigation, 2002, B737-436, EW/C2002/11/02

Introduction (II)
Substitution of Wires with Wireless Technologies

Benefits

- Reduction of weight and cost
- Increased system flexibility
- Ease of adding new functions
- Enables monitoring of physically-refined areas

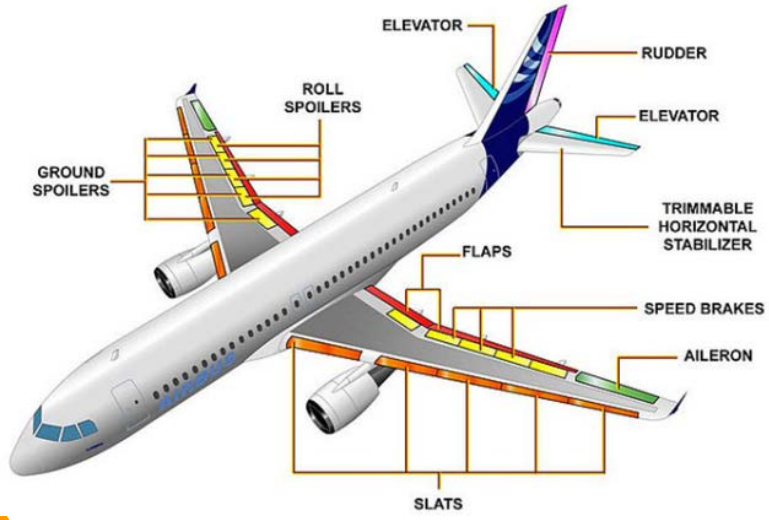
Disadvantages & Challenges

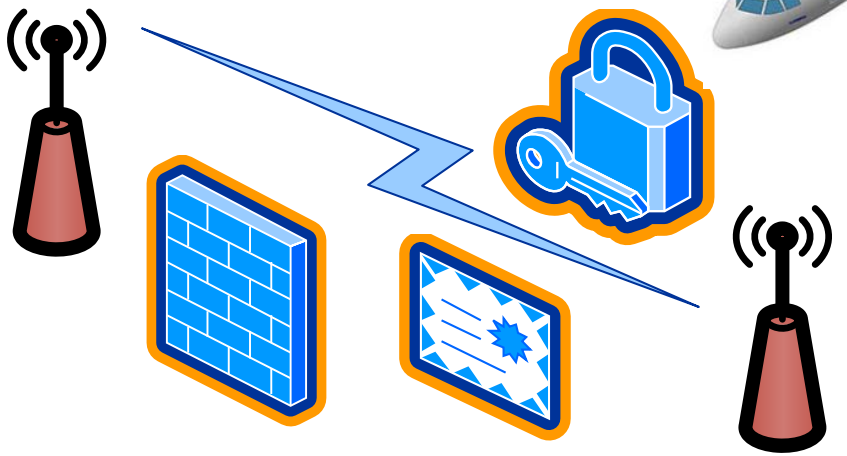
- Prone to outer disturbances
- Deteriorate safety & reliability

Introduction (III)
Wireless Concept for Safety-Critical Applications

Design Assurance Level (DAL)

- Safety-critical systems → DAL - A
- Catastrophic failure conditions
- Crucial to evaluate the safety and reliability aspects of wireless systems in aircraft





Introduction (IV)
Methods to Enhance Security & Reliability

Focus on preventing jamming attacks

- Definition of jammer by North Atlantic Treaty Organization (NATO) [1]

  " The deliberate radiation, re-radiation or reflection of electromagnetic energy with the object of impairing the effectiveness of hostile electronic devices, equipment or systems."

- **Assessment of possible countermeasures**
  - ✓ Spread-spectrum algorithms
  - ✓ Jammer localization and detection
  - ✓ Channel surfing
  - ✓ Defeating energy efficient jamming

Handheld UHF Signal Jammer[2]

[1] NATO, „NATO Glossary of terms and definitions", APP-6-2008.
[2] http://www.jammerall.com/

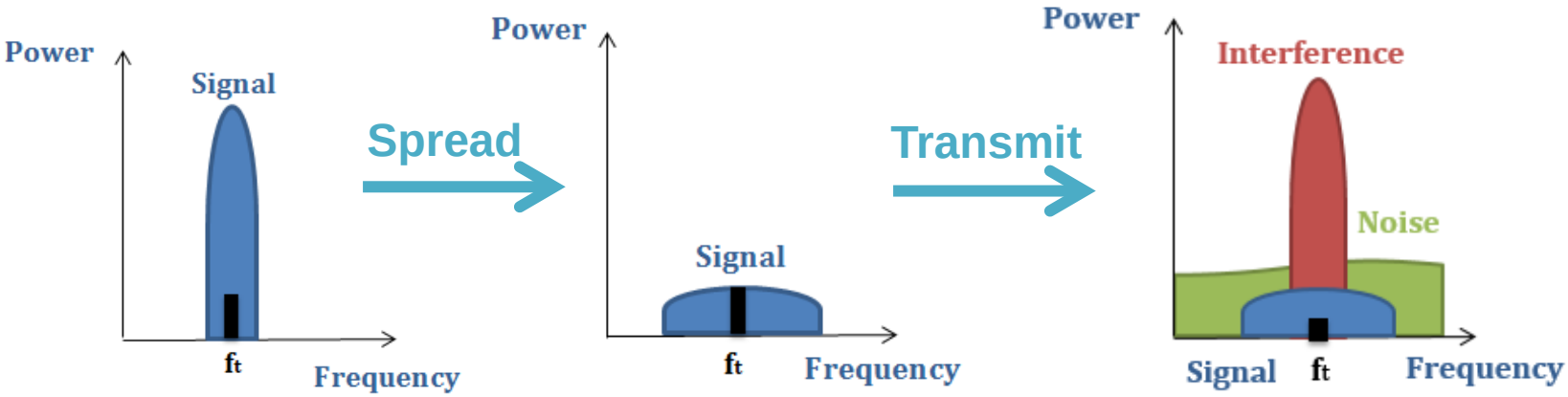
Outline

- Introduction
- Spread-Spectrum Techniques
  - **Direct - Sequence Spread Spectrum (DSSS)**
  - **Frequency - Hopping Spread Spectrum (FHSS)**
- Simulation
- Hardware Development
- Results & Conclusion

Spread-Spectrum Techniques
Direct-Sequence Spread Spectrum (I)

Method

Modulation of data signal with a higher data rate Pseudo Noise (PN) binary sequence → spreading data spectrum



Data Signal

DSSS Signal

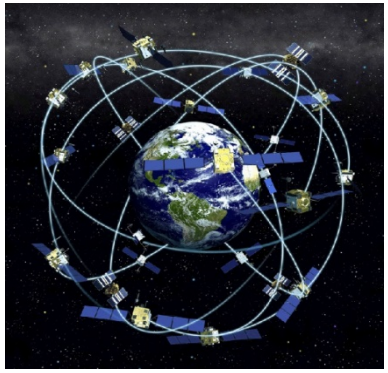
DSSS Signal in a Transmission Channel

f_t: Transmission frequency

Spread-Spectrum Techniques
Direct-Sequence Spread Spectrum (II)

Advantages

- Hard to detect by adversary
- Immune against fading
- Robust against interferences



Global Positioning System (GPS)[1]

Current Applications

GALILEO

WirelessHART

Wi Fi

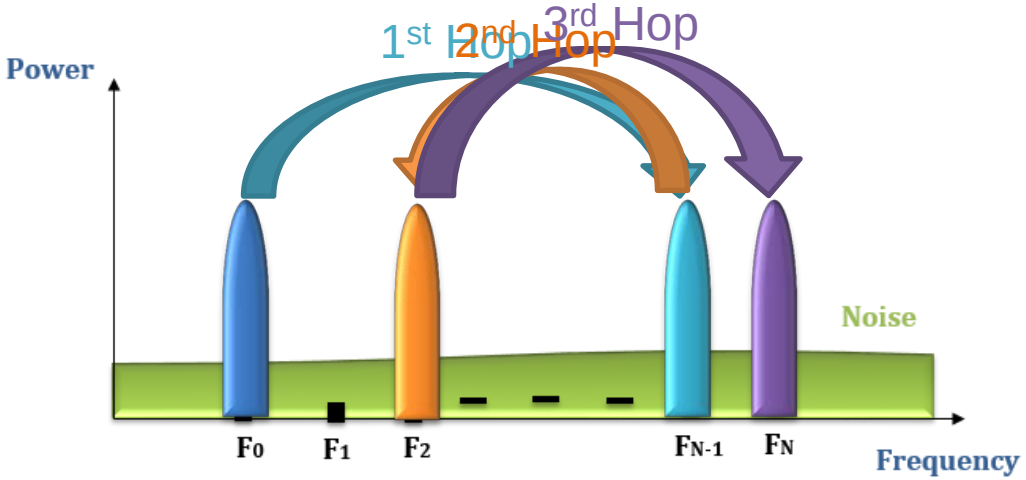
ZigBee

[1] http://www.nist.gov/pml/div688/grp40/gpsarchive.cfm

Spread-Spectrum Techniques
Frequency Hopping Spread Spectrum (I)

Method

Changes transmission frequency swiftly and pseudo-randomly



$F_0, F_1 \ldots F_N$ = Sub-channels

- Channel assignment
- Look-up table, shared PN codes
- Crucial parameters: hopping rate and pattern

Spread-Spectrum Techniques
Frequency Hopping Spread Spectrum (II)

Advantages

- Reduces eavesdropping probability
- Requires intelligent jammer development
- Better transmission quality with
  - ✓ Dynamic frequency hopping
  - ✓ Frequency selective fading

Military UHF Radio[1]

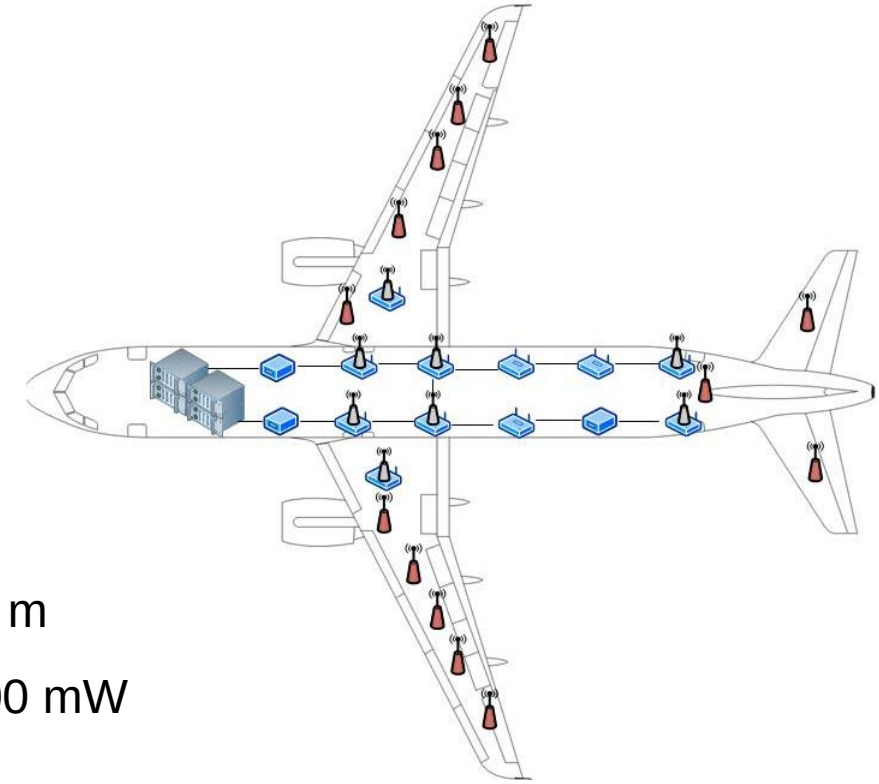
Current Applications

Bluetooth® FC Part.15 Military Use

[1]dpdproductions.com

Simulation
System Parameters

Wireless Flight Control Network Concept



Components of the Network

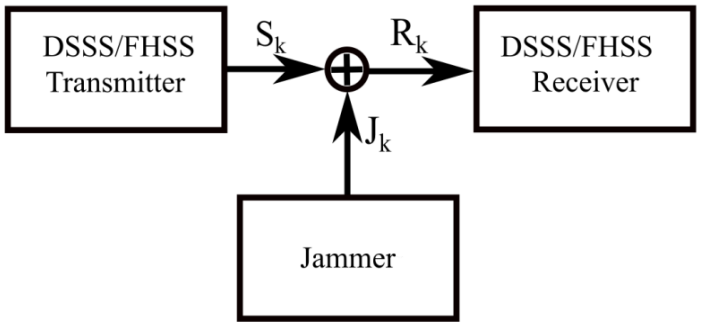
- Flight control computers
- Flight control nodes
  - ✓ Actuators and sensors

Network Specifications

- Star, hybrid star topology
- Maximum transmission range 50 m
- Maximum transmission power 100 mW
- Data-rate up to 2 Mbit/s

Simulation
Modelling of Jammers

- **Worst-case Jammers**
  - ✓ Multi-tone Jammers
  - ✓ Partial-band Jammers



S_k: Transmitted data signal

J_k: Jammer Signal, R_k: Received Signal

- **Assumptions**
  - ✓ Jammed Bandwidth

$\rho = \frac{W_j}{W_{ss}}$, $\rho = 0.4$

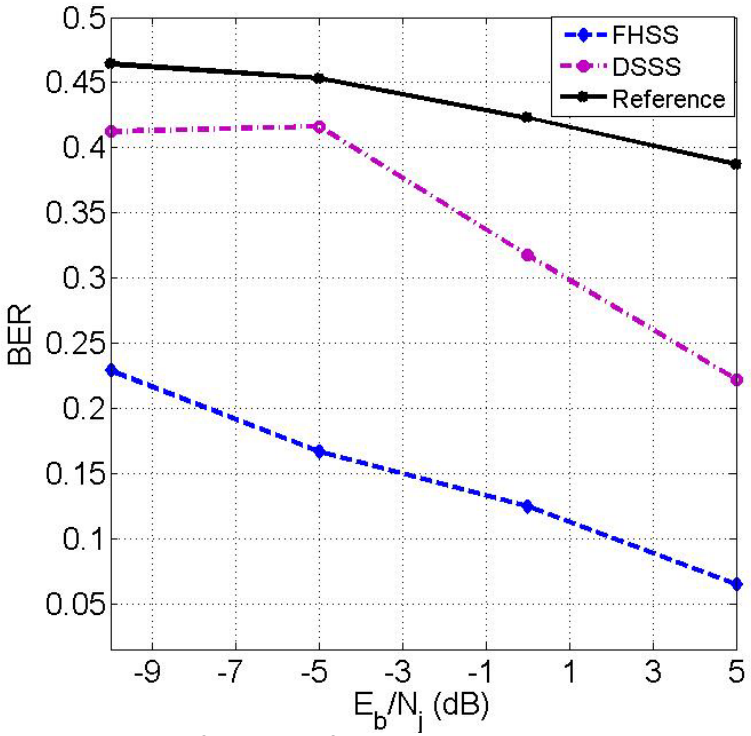
W_j : jammed bandwidth, W_{ss}: data signal bandwidth

  - ✓ Signal Power (E_b) = 10 dBm
  - ✓ Jammer Power (N_j) = 5, 10, 15, 20 dBm

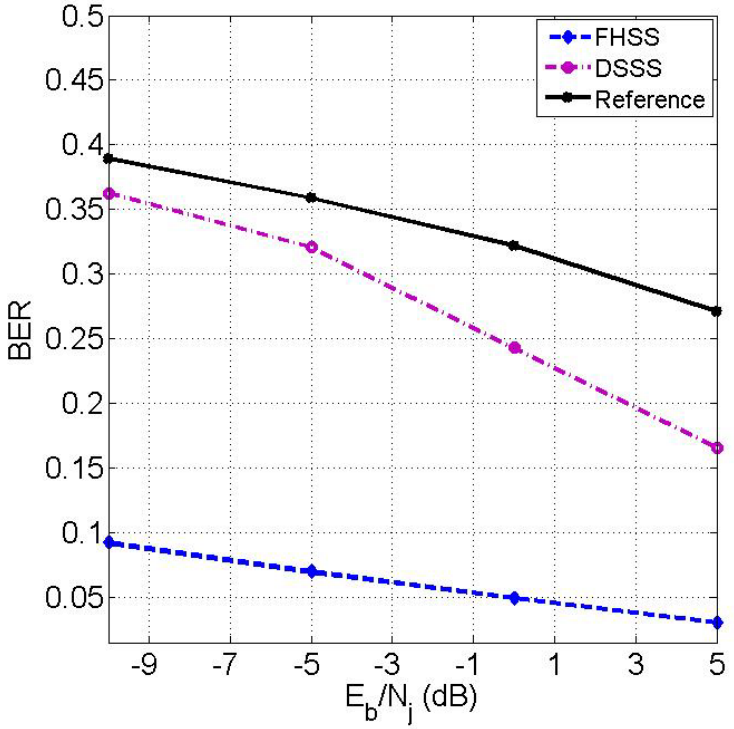
Simulation
Evaluation of Intermediate Results

Bit Error Rate (BER) Analysis

- Reference: single-carrier transmitter



Under Multi-tone Jamming

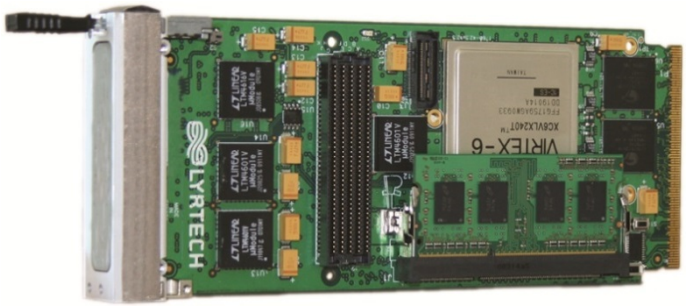


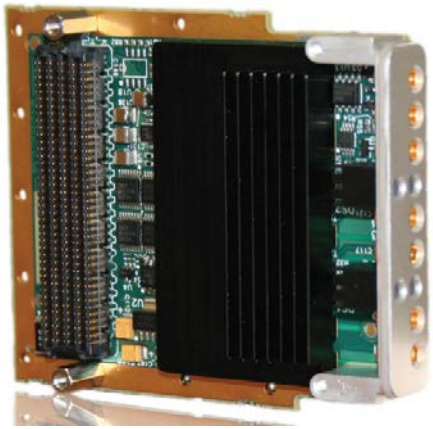
Under Partial-Band Jamming

Hardware Implementation (I)
Specifications of Development Platform

SDR Specifications

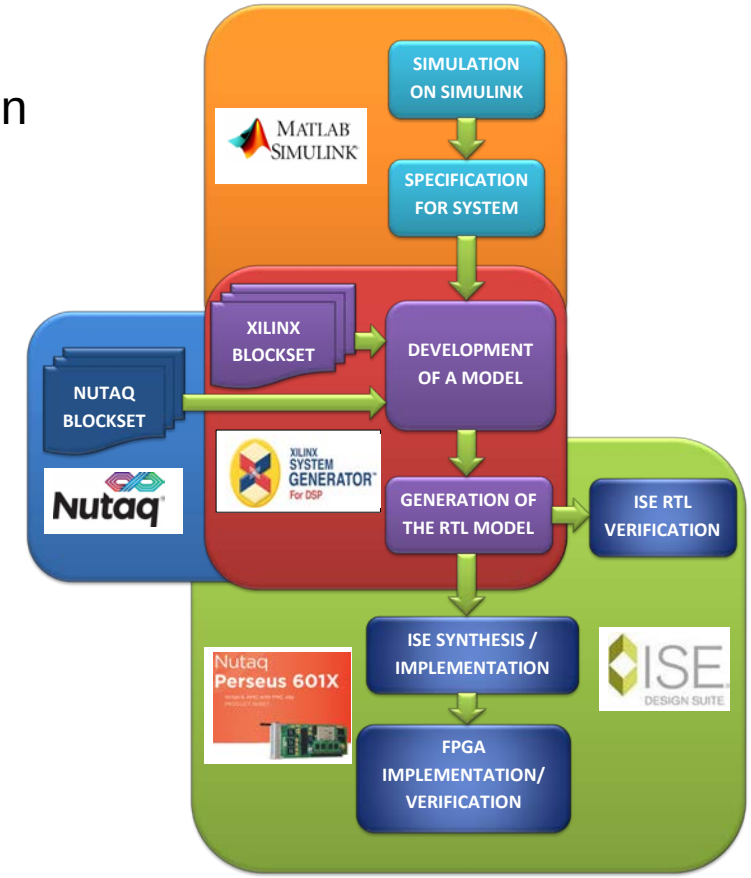
- Perseus 601X AMC
  - ✓ Xilinx Virtex 6 LXT FPGA
  - ✓ Support for Plug-in FMC
  - ✓ Up to 4 GB, 64-bit DDR3 SDRAM
  - ✓ 2 GigE ports
  - ✓ Mestor interface: FPGA JTAG, mini-B USB serial port
- Analog-to-Digital-to-Analog Converter (ADAC) 250
  - ✓ 2 14-bit 250 MSPS (ADC)
  - ✓ 2 16-bit 1 GSPS (DAC)





Hardware Implementation (II) Development Method and Tools

- Xilinx System Generator
  - ✓ Specific IP blocks for telecommunication
  - ✓ Basic algorithmic blocks
  - ✓ Digital design elements
- Nutaq Blocks
  - ✓ Custom Register (CR) Control
  - ✓ Real-time signal monitoring
  - ✓ ADAC parameters
  - ✓ GigE configuration

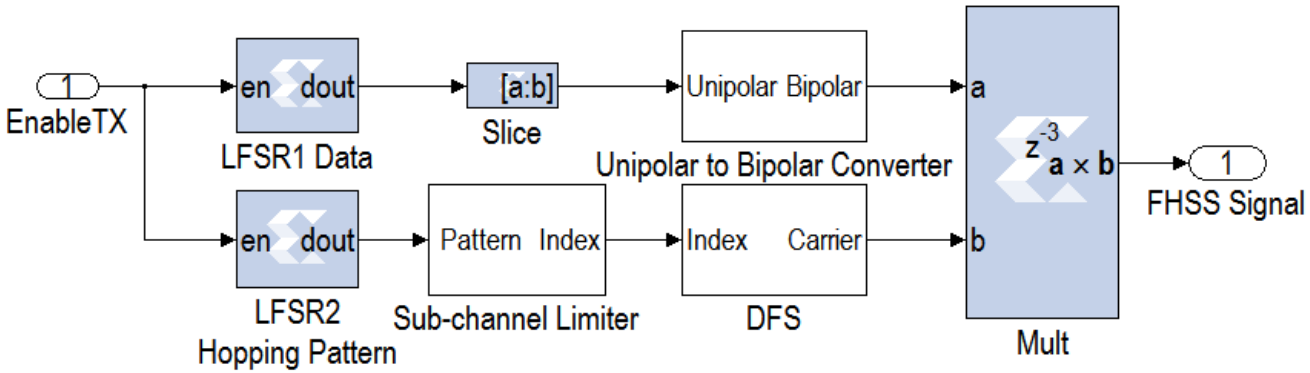


Hardware Development (III)
FHSS Algorithm Implementation

FHSS Transmitter Components

- Linear-Feedback Shift Register (LFSR)
  - ✓ Information data
  - ✓ Hopping pattern
- Direct- Frequency Synthesizer (DFS)
- Multiplier

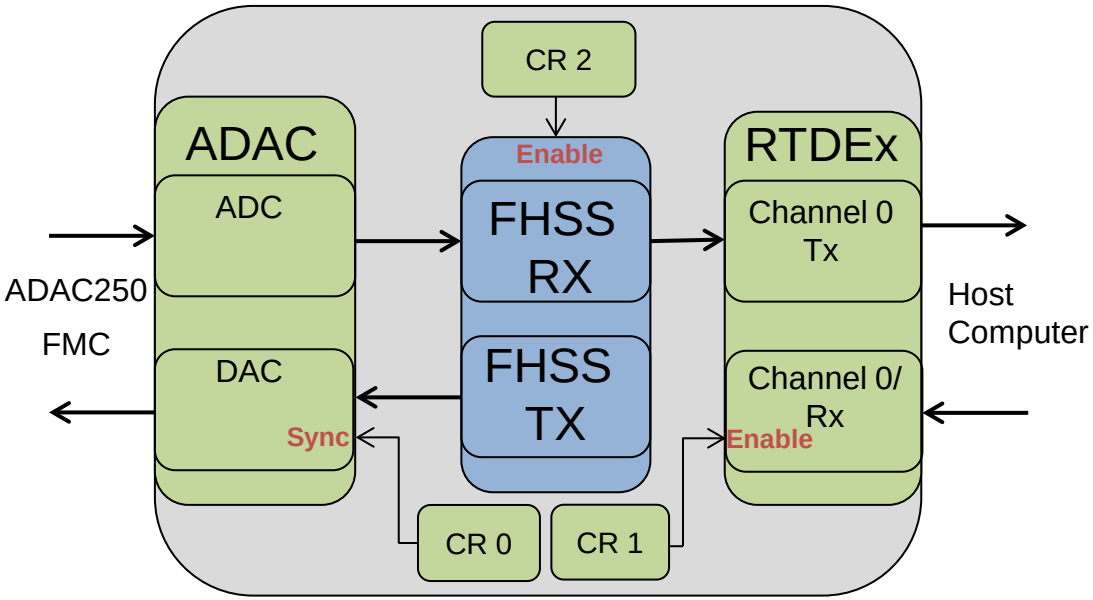
FHSS Parameter	Value
PN Generator Type	LFSR
LFSR Length	7
Sub-channel Spacing	5 kHz
Dwell Time	100 µs
Number of Sub-channels	39
ADAC Rate	200 MHz

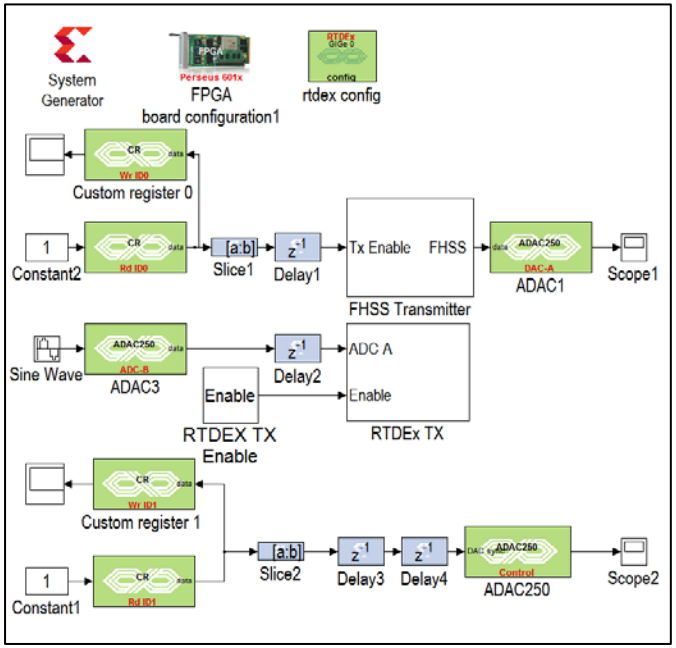


FHSS Transmitter Blocks

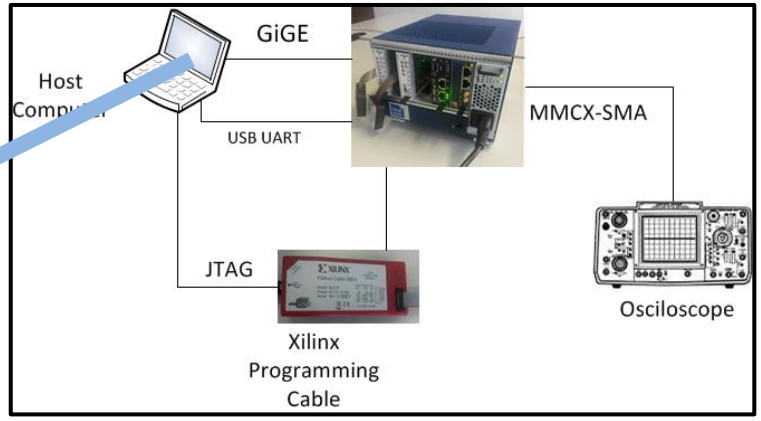
Hardware Development (III)
FHSS Algorithm Implementation

- Control signals
  - ✓ ADAC synchronize
  - ✓ Transmitter enable
  - ✓ RTDEx enable

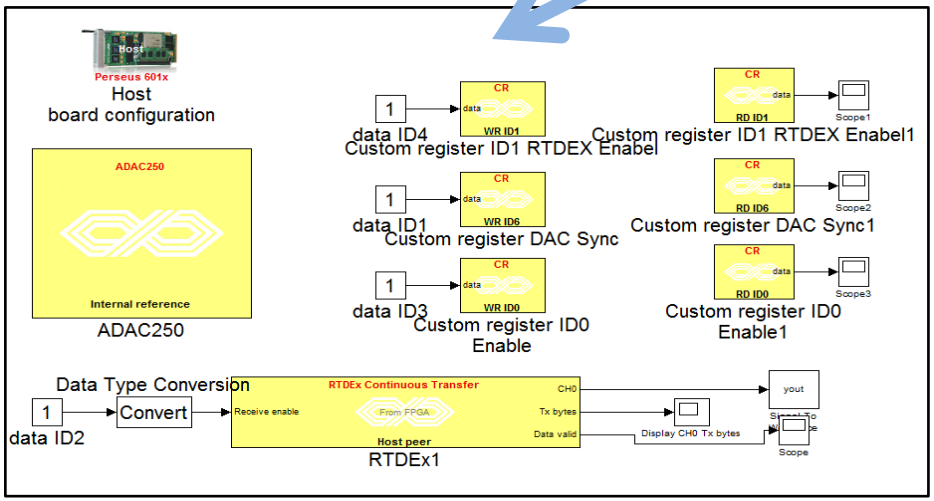




Hardware Development (IV)
Testbed Development and Testing



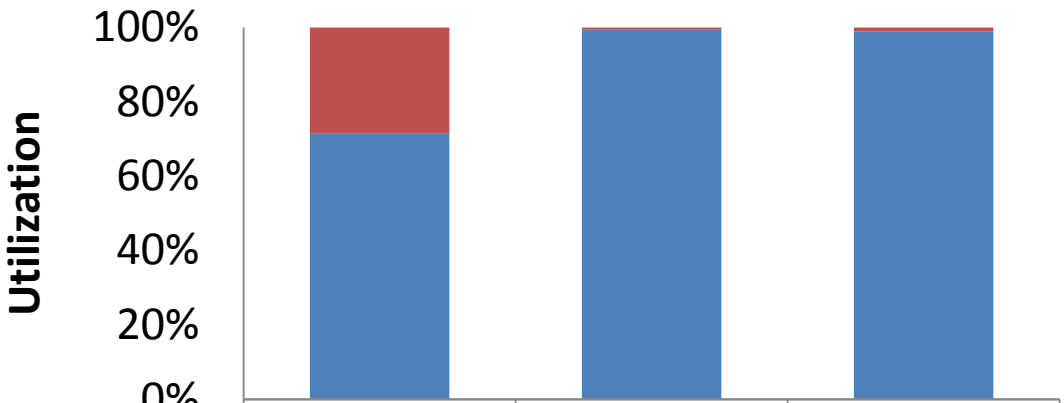
Test Environment



Host Application

Results (I)
Synthesis & Implementation Reports

- **Design Synthesis**
  - ✓ RTL schematic
- **Design Implementation**
  - ✓ Translate
  - ✓ Map
  - ✓ Place & Route
- Timing Constraints met
- Device Utilization Summary

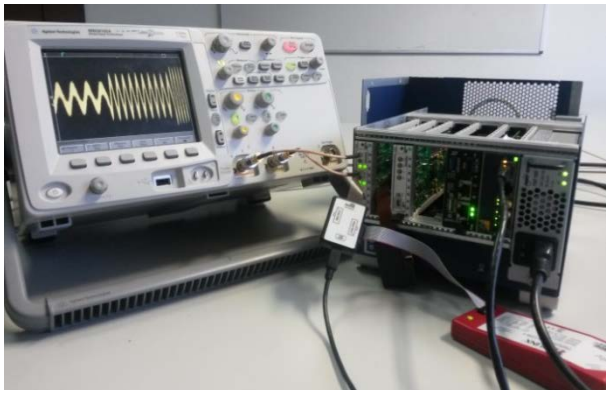


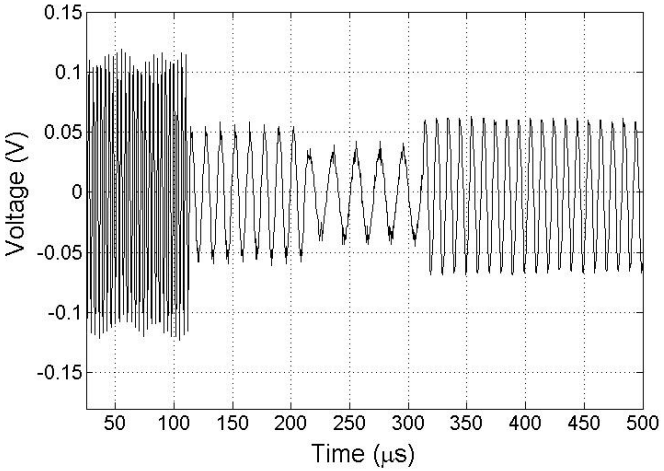
	Bonded IOs	Slice Registers	Slice LUTs
Used	285	1204	1522
Avaliable	720	301440	150720

Results (II)
Test & Validation

- Observing TX signal by oscilloscope
  - ✓ Dwell time of 100 μs
  - ✓ Hopping Pattern

    all sub-channels used
- Irregularities in the amplitude due to behavior of ADAC in the low and high frequencies
- Obtaining Rx signal in the host computer by the RTDEx and the BER Analysis

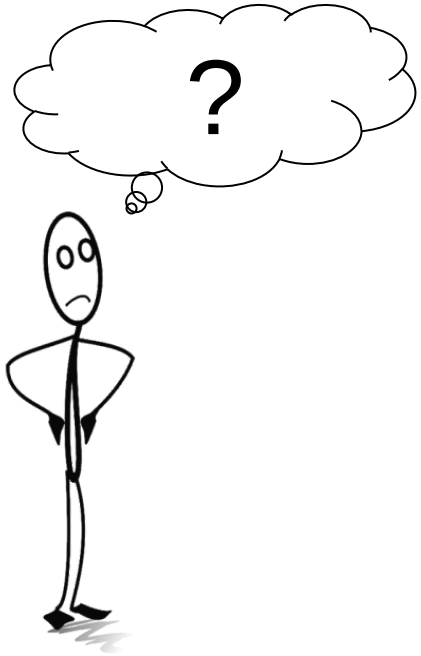




Conclusion & Future Work

- FHSS more resistant than DSSS against jamming
- Designed FHSS transceiver with Xilinx System Generator, implemented on a Virtex-6 FPGA-based SDR platform
- Design parameters of case-study fulfilled
- Enhancement in the security and reliability, especially wireless avionics intra-communications
- Necessary to assess the overall safety and reliability
  - ✓ With modulation, channel coding and the encryption methods
- Future work: Implementation of hybrid-frequency hopping transceiver

Thank you for your attention!



Aysegul Aglargoz
German Aerospace Center (DLR)
Institute of Flight Systems
Safety Critical Systems
& System Engineering
Ayseguel.Aglargoez@dlr.de

Valentin Bartkowiak
German Aerospace Center (DLR)
Institute of Flight Systems
Safety Critical Systems
& System Engineering
Valentin.Bartkowiak@dlr.de

Holger Spangenberg
German Aerospace Center (DLR)
Institute of Flight Systems
Safety Critical Systems &
System Engineering
Holger.Spangenberg@dlr.de