Innovation projects 5A EIS – PX505 – 2021-2022

Responsible: Ionela PRODAN

August 2021

Contents

Part I
Organizational details of PX505

0.1 Attributes of the Innovation Project

PX505 is a multidisciplinary project[1] addressed to the 5th year students of ESISAR of the EIS (Electronique, Informatique et Systèmes) specialization, the apprentice students and the Master MISTRE attendees.

The main goal is to create a real or virtual prototype ("demonstrator") combining several disciplines taught at ESISAR (minimum two).

What is innovation?

> Innovation is using novel ideas and approaches to solve existing problems, it also means being creative.

The students are asked for innovation, not invention:

- An invention is something entirely new that has never been done or seen before.
- Innovation is a change or modification to improve something that already exists.

For example, Thomas Edison is credited for the invention of the light bulb in 1879, however, generations of light bulb innovations have created the millions of different and improved light bulbs in use today.

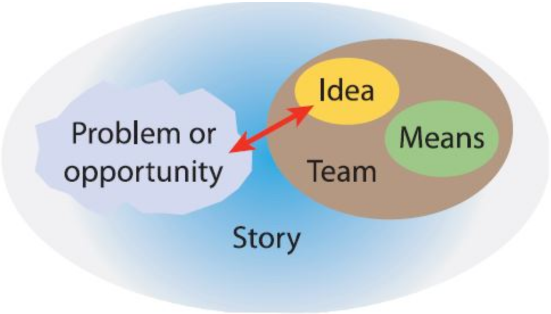
Hence, the students are not asked for something entirely new, but improvement or expansion of something that is already in use. That is:

- use of a new technology (e.g., Artificial Neural Network, ROS - Robotic Operation System) for an existing usage (motion recognition, motion planning, etc.);
- creation of a new usage (e.g., automatic plants watering, smart building monitoring, etc.) using existing technologies (automate the process).

What are the attributes of the innovation project?

We underline that *"good projects start with an idea that is rooted in a problem or opportunity"*.

- The first step for the students is to find a good problem which is to be addressed by a clear idea (i.e., choose a proposed subject or provide their own).
- The team develops the idea to act on the problem.
- The team has access to the means necessary to implement the idea for solving the problem: i) team skills and motivation; ii) tools and instrumentation; iii) funding provided by ESISAR to each team (i.e, 300 euros for all projects and 600 euros only for the digital arts projects).
- The story is a way for the team to develop and talk about their ideas among the members and to be able to explain them to other people who understand or not technology.



How the innovation project is organized?

Team composition: Depending on the year and the total number of students, the responsible of PX505 will create teams of 4 students, mixing apprentice, MISTRE and EIS students of ESISAR, with different background.

Project selection: Each student chooses and orders at least 6 subjects (see the list of subjects hereinafter). The link for selecting the projects will be provided at the end of august 2020.

If several students/teams select the same subjects then a random draw will be performed. The students are encouraged to respect the final composition of the team. No modifications will be done once the project will start.

Project evaluation: The teams have to provide 3 deliverables: a mid-report (20%), a final report (40%) and a public oral defense (40%). Even if the project outcome will be evaluated for the entire team, individual marks for each student are also possible.

[1] This work benefits from the French government IRT Nanoelec program, ANR-10-AIRT-05.

Digital Arts Specific Support: These types of projects benefit from workshops with artists and brainstorming, exhibition and/or show visits. The students involved in such projects will have specific technical support and funding. The responsible for this type of project is Yann.Kieffer@esisar.grenoble-inp.fr.

0.2 Responsible Innovation

> Responsible innovation considers the role that new products, processes or business models have in society. This means a responsible approach towards innovation involves creating change that has positive impacts on society and the environment.

It is worth noting that innovation processes, systems and investments should preferably be focused on addressing societal challenges and our urgent global problems, in climate, health, planning, energy, water and quality of life [2].

Hence, it is of the essence that the students acquire an adequate and shared conception of responsibility for their innovations and new technologies:

- Are their innovations saving lives?
- Are they producing jobs equitably?
- Are they helping to save the planet from heating up?
- Are they safe and secure?
- Do they also respect our privacy?
- Do they respect the freedom and autonomy of people?
- If not, how can we make them so?

Two courses on Responsible Innovation will be given to the students by Assoc Prof. HDR Elena BARBU (IAE Grenoble, Graduate School of Management):

- the first course (3 hours), given in September, will help the students to become acquainted with the main philosophical issues in relation to Responsible Innovation;
- the second course (3 hours), given in December, will help the students to address and discuss the societal challenges of each project.

Note that, addressing the societal challenges of each project will represent an evaluation criteria for the reports and projects defenses.

0.3 Students' role

To achieve the goals of the project, the team must understand and implement the idea. The students are encouraged to be autonomous, motivated and very well organized all along the duration of the project. These are the key elements for obtaining very good results.

The students need to take advantage of the 2 free half-days per week in the timetable to meet and work on their project.

For the final defense, when explaining how the project is innovative, it is important to also consider why the innovative solution is better than the more traditional method(s). Possible reasons include:

- saves time;
- is more cost-effective or efficient;
- increases reach and potential beneficiaries;
- reaches new beneficiaries that would not have been reached otherwise;
- targets a completely new area (very rare).

Finally, any trouble appearing throughout the project must be brought to the attention of the supervisor(s) and/or the PX505 responsible.

[2] Jakobsen, Stig-Erik and Fløysand, Arnt and Overton, John: *"Expanding the field of Responsible Research and Innovation (RRI)–from responsible research to responsible innovation"*, Taylor & Francis, 2019.

0.4 Supervisor(s)' role

As mentioned above, the students are encouraged to work autonomously and put their ides into practice. Of course, discussing the ideas with the team's supervisor(s) will speed up the progress of the project and offer a global view of the expected results. Hence, the supervisor(s) is(are) expected to:

- monitor(s) the progress of the project;
- proofread(s) and evaluate(s) the reports;
- participation in, and evaluation of the defense;
- validate(s) the instrumentation purchases;
- check(s) on the coordination of the group and the active participation of each of the members (a weekly discussion with the students is encouraged);
- co-evaluate(s) of the final oral presentation.

0.5 Reports and presentation templates

All the reports and presentations must be written and defended in English.

The intermediate report (representing 20% of the final grade) must contain (8 pages maximum):

- the project idea (≈ 1 page)
- a detailed project development plan (≈ 2 pages);
- a project schedule or Gantt diagram (1 page);
- a distribution of individual tasks (1 page);
- milestones and risk analysis ("plan B") (≈ 2 pages);
- insights on the societal challenges of their innovation;
- a complete purchase list (validated by the supervisor(s)).

The final report (representing 40% of the final grade) must contain (15 pages maximum without Annex):

- Abstract (10 lines maximum)
- Introduction (≈ 1 page)
- Related work (≈ 2 pages)
- Demonstrator architecture (≈ 3 pages)
- Validation environment and results (≈ 7 pages)
- Societal challenges of their innovation (≈ 1 page)
- Conclusions (≈ 1 page)
- Annex: project organization, specific schematics, photos, code or proofs (no page limitation)

The defense presentation timetable contains (20 minutes maximum):

- 15 minutes for presenting the topic, the approach, the results and the societal challenges of the product/system;
- 5 minutes for demonstration;
- 10 minutes for questions and answers.

The final presentation must clearly show the contribution of each participant in the project: each project member must present some of the slides with a uniform distribution (as the industrial project defense in the 4th year). The final grade is individual.

0.6 Deadlines

Hereinafter, are delineated the innovation project deadlines. The links for selecting the projects and uploading the mid and final reports on Chamilo will be provided along the Semester.

- **Project selection: 9 Sept - 16 Sept 2021**

  The students must connect to the following link and select all the projects in order of their preferences:

  https://docs.google.com/forms/d/1OJTYUNa-9AqhEROF05SdYZ5xV7E6Y4u2ENAEArREc0Q/edit

- **Project assignment and the selected teams: 17 - 20 Sept 2021**
- **Starting of the project: 21 September 2021**
- **Mid-report submission: 21 October 2021**

  The students must upload the report on Chamilo:

  ESISAR PX504 Innovation Project 5A EIS/Travaux d'étudiants/MidReport PX505 (2021/2022)

- **Final report submission: 4 January 2022**

  The students must upload the report on Chamilo:

  ESISAR PX504 Innovation Project 5A EIS/Travaux d'étudiants/FinalReport PX505 (2021/2022)

- **Project defense: 11 January 2022**
- **Video preparation of the selected projects: until end of January 2021**

Note that each team will have at their disposal a room in building C of Esisar to properly develop their work. Some important details on the rooms are the following:

- the rooms are provided in very good conditions so we required that they are maintain as they are during the whole duration of the project;
- they keys of the rooms will be given by the PX responsible in Sept. They should be returned on 4 January 2022.

Part II

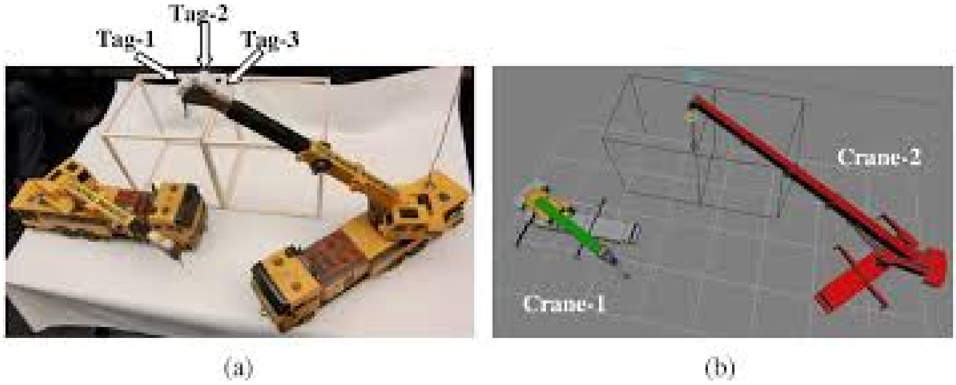
External proposals

1 Crane: Design a 3D object identification and 3D collision avoidance algorithm using LIDAR and simulation

Contact details	gregory@ascolab.fr, ionela.prodan@lcis.grenoble-inp.fr
Project keywords	**robotics, object recognition, collision avoidance, ROS, LIDAR.**
Skills	**embedded programming, computer vision, microcontroller**

1.1 Project context and goals

Massive development of LIDAR technology, open new alternative for current industrials solutions. Integrating the full "environment" in a robotic solution allow new interaction between robot and the field, and could also offer new services around the robot. Applying robot principle, 3D mapping, object recognition/classification on work site can be a new way of avoiding collision between machines themselves (cranes, wheeloaders, concrete pump), but also with their environment (ground, building, pedestrians, tools). Furthermore, 3D mapping can also offer new services: 3D mapping of building, material storage volume/position, object recognition, data analysis. By this way, it is interesting for ASCOLAB to use simulation/visualization environment to quickly validate idea, concept, algorithm, and demonstrate the feasibility. Furthermore, adding in this simulation solution some real "stuff" representing real objects and mapping (rover, LIDAR...) will help designing new algorithms and check real behavior.



Example of application:

- 3D mapping using LIDAR installed on tower cranes, and collision avoidance of tower cranes movements.
- 3D mapping using LIDAR installed on the back of wheeloader/truck to detect pedestrian or obstacle, but also to map the site and compute material storage volume (sand, gravel, rocks...) in a quarry.

The goal is to validate solution of 3D mapping and object recognition/classification, then validate the principle of object collision avoidance algorithm. There are basically 3 tasks:

- Setting up a 3D simulation environment of object/robot
- Testing collision avoidance algorithm in this 3D simulation
- Then setting up LIDAR usage and object recognition algorithm and integrate these data in the simulation environment

1.2 Project deliverables

- Full ROS environment [1] to simulate construction site (tower cranes, mobile crane, building, people...)
- Working LIDAR + objects identification algorithm, integrated in viewer/simulation tool + simple maquette
- State of the art for object identification and collision avoidance algorithms
- Simulated crane movement in ROS included collision avoidance algorithm

References

[1] Stanford Artificial Intelligence Laboratory et al. *Robotic Operating System*. Version ROS Melodic Morenia. May 23, 2018. URL: https://www.ros.org.

2 AI4Cubesat: On-board artificial intelligence for Earth observation

Contact details tania.mcnamara@univ-grenoble-alpes.fr, frederic.martin1@@univ-grenoble-alpes.fr

Project keywords CubeSat, artificial intelligence, imaging.

Skills SoC, FPGA, VHDL, C programming

2.1 Project context and goals

Started in early 2020, the QlevEr Sat project [1] aims to bring Artificial Intelligence (AI) onboard a demonstration cubesat for Earth Observation (EO). The overall project is led by the Centre Spatial Universitaire de Grenoble (CSUG) in collaboration with the Multidisciplinary Institute in Artificial Intelligence (MIAI UGA) and Teledyne e2v. QlevEr Sat will be surveying specific regions for deforestation. A 5 m resolution is necessary to observe daily changes on a given target area. As the number of satellites increases, embarking AI algorithms directly on board will drastically reduce the bandwidth required for ground data transmission: only the post-analysis results can be downlinked, rather than images themselves.

The "UFO QlevEr Demo" project is the phase B2 of the overall project, i.e. the second part of the cubesat's Preliminary Definition which is planned from June 2021 to March 2022.

QlevEr Demo aims at building a real-scale 6U ground model of the future space cubesat, partly as a functional engineering model, partly as a 3D-printed mockup. This non-flying model shall be capable of acquiring some images, running embedded AI algorithms developed by the DSE partner and transmit the results to the main On Board Computer assembled by the U-Space partner.

Within this phase, the present student project addresses the Payload's electronics subsystem, more precisely: the FPGA bridge between the CMOS imager and the AI microprocessor in charge of sensor control and image acquisition.

The objective of the project is to specify, develop and prototype the HW & SW links between the Payload (instrument part) and the platform (navigation part) of the CubeSat to implement Telemetries (TM) and Telecommands (TC) communications.

2.2 Project deliverables

The aim is to set up the interfaces between payload modules and platform On Board Computer (OBC) in order to manage TM/TC exchanges inside the QlevEr nanosatellite. The development is based on a ZynQ SoC module [2] (ARM processor, FPGA and RAM memory).

The tasks involve:

- Implement the current SoC design (VHDL, IPs & C code) of the Internal Pattern Generator, VDMA and QSPi modules on your own SoC development kit,
- Emulate the PF OBC, based on the PF provider's documentation on a similar SoC development kit,
- Specify and implement TM/TC UART and I2C links to dialogue with the image sensor.

References

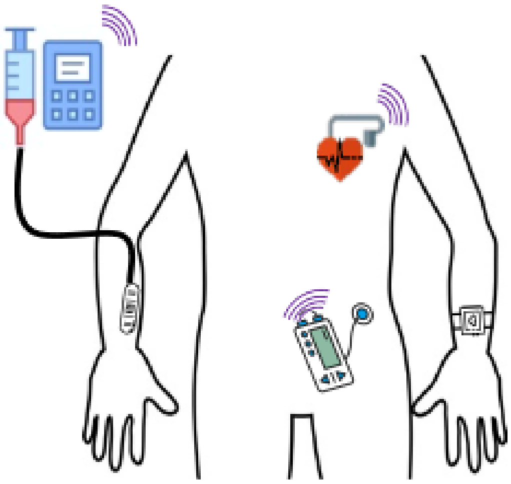
[1] *QlevEr Sat*. https://www.csug.fr/menu-principal/projets/qlever-sat/qlever-sat-751384.kjsp.

[2] *Xilinx Zynq-7000*. https://www.xilinx.com/products/silicon-devices/soc/zynq-7000.html.

3 SafeDemo: A Safe and Secure Connected Healthcare System Demonstrator

Contact details	armand.castillejo@st.com, david.hely@lcis.grenoble-inp.fr
Project keywords	IoT Security; AI; Edge-computing; Bluetooth Low Energy; Healthcare System; Medical device.
Skills	Embedded System Programming, System Security.

3.1 Project context and goals



The goal of this project is to implement a secure connected health care demonstrator. This demonstrator will be based on a secure gateway embedding edge-computing capabilities dedicated to medical applications and several medical devices connected using mainly through a secured "Medical IoT Module". The main purpose of this demonstrator is to show how several medical IoT devices can be securely and dynamically connected to a secure gateway which aggregate and analyze the medical data.

It will first be necessary to define a generic medical use case which can efficiently highlight the advantages of such a solution (in terms of usability, innovation, and security). The demonstrator should show how such an end-to-end system can guarantee that the data collection and access are safe and secure. This scenario will be set-up with the main partners of the project STMicroelectronics [1], IRT Nanoelec [2] and Maatel [3]. Once the scenario is validated, the system will then be deployed and the team will develop all the necessary software stacks to realize the demonstrator. The main technical tasks are:

- Low Power Bluetooth (BLE) connection between the devices and the gateway
- Gateway interface and data collection through ethernet connection
- Medical devices data management (considering several stakeholders categories)
- System Security management (data ciphering within the device)

After the integration of all the system components, the scenario will be deployed to showcase the security of the system.

3.2 Project deliverables

- Demonstration scenario
- Software Stacks for each system components
- Live Demonstration showcasing the benefits of the solution
- Documentations to replicate the demonstrator within the partners showrooms.

References

[1] https://www.st.com/content/st_com/en.html.

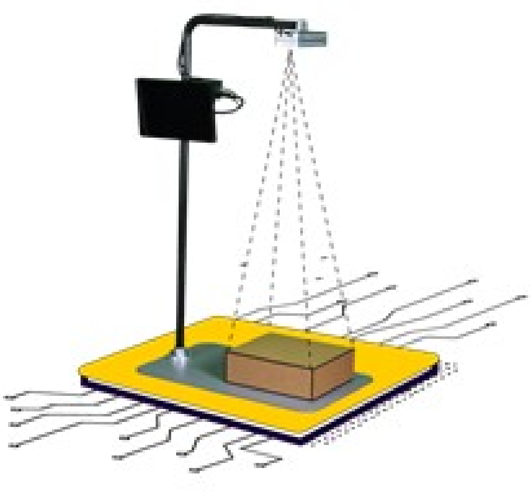
[2] https://irtnanoelec.fr/en/.

[3] https://maatel.com.

4 DWSys: Dimensioning and weighting system design for packages

Contact details	cyril.vidal@preciamolen.fr
Project keywords	computer vision, radar, programming.
Skills	embedded programming, computer vision, microcontroller

4.1 Project context and goals



To prepare for the future of the group, PRECIA MOLEN is investing in creating new weighting solutions, software and data analysis applications that will meet the customers' needs. The innovation Unit aims to develop a dimensioning and weighing system for the logistics market.

The dimensioning system consists of measures packages and objects in a wide range of sizes – from as small as a 10 cm cube to as large as a 150 cm cube and communicate the information to an indicator through a serial interface. The accuracy should be ±1 cm. The response time should be less than 1 s. It can be used in many different environments from a courier company retail store to an inbound station of a warehouse.

The work will include a varied range of challenges:

- research and explore various state of the art techniques to measure objects
- Design, develop and implement end to end solutions, from the acquisition setup to processing algorithms [2] Implementation
- Participate in the selection of components (sensors, lenses, filters, lights, ToF sensor [1]...)
- Set up quick physical proof of concepts of such solutions
- Compare performance and efficiency of different approaches (hardware and software) to improve our product
- Work with Precia Molen team to implement communication with Precia Molen products

4.2 Project deliverables

- Technologies study
- Components selection
- Mock up of a dimentioning system

References

[1] *ST Time of Flight sensors*. https://www.st.com/en/imaging-and-photonics-solutions/time-of-flight-sensors.html.

[2] G. Bradski. "The OpenCV Library". *Dr. Dobb's Journal of Software Tools* (2000).

Part III

Students proposals

Part IV
Digital Arts proposals

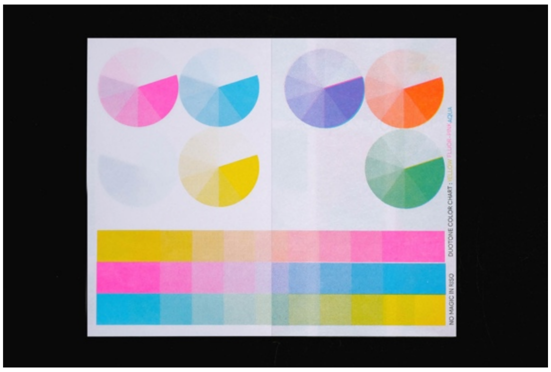
5 RISO: Hacking a printer's RIP

Contact details romain.laurent@esad-gv.fr, yann.kieffer@grenoble-inp.fr

Project keywords printing, hacking, prototyping, graphic design.

Skills reverse engineering, embedded and network programming, packet analysis.

5.1 Project context and goals



In 1980, a new kind of copier has been launched on the market. Called a Risograph, or in short, RISO, this copier can print only one color each time a sheet passes through it. This copier was designed for customers who would need copying (written) documents in the cheapest possible way – associations, schools, parishes... A special feature of this copier is its use of a so-called 'master': a sheet pierced by tiny holes letting the ink pass through them, like a stencil. For several years now, artists and graphic designers have been diverting its use, thanks to its singular aesthetic. By printing several colors on the same sheet – passing the sheet several times through the RISO – they created what is now called risography, meaning, the use of the RISO for its graphic potential.

The aim of this project is to enhance the artistic potential of the RISO by adding to it a small device, plugged between the so-called RIP (a computer sending the image to be printed to the RISO) and the RISO itself. The RIP and the RISO communicate through Ethernet, so the Ethernet link would be broken, and the device placed in between the computer and the RISO. The function of the device is to alter slightly the image being sent for printing, creating effects resembling – or not – what could happen to an aging printer or copier. Such an alteration, realized by a small piece of software, will be called in the following a graphic treatment.

Here is one way this project could be taken to a successful completion:

- analyze how information is exchanged between the RIP and RISO
- create prototype graphic treatments on the computer to validate that the main aim can be reached
- select a cheap and portable device as the target device
- integrate one or more graphic treatments into the device

5.2 Project deliverables

- A fully autonomous device that can be plugged between a RIP and a RISO copier, altering the images as they pass through the device
- A complete documentation explaining how to clone such a device
- An archive (or online deposit) of all the code that has been written to create this device
- A documentation explaining how to create a new graphic treatment for the device
- (bonus) A nice interface for selecting one graphic treatment in a set from the device; or better, a nice graphic interface showing the effect the device currently has on the image being altered.

References

[1] http://maisonriso.fr/la-risographie/.

[2] https://odotoo.com/risograph/.

[3] https://www.quintalatelier.com/collections/livres.

[4] https://spectorbooks.com/exploriso.

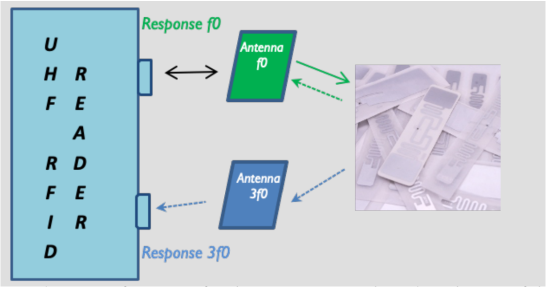
[5] https://www.behance.net/gallery/80887921/NO-MAGIC-IN-RISO.

Part V
LCIS/ESISAR proposals

6 ARTag: Authentication of RFID Tags

Contact details **smail.tedjini@grenoble-inp.fr**
Project keywords **RFID, Authentication, Harmonic reader, Digital signature.**
Skills **RFID, ΔRCS, Signal processing, QRcode generation.**

6.1 Project context and goals



UHF RFID tags are among the most used devices for identification purposes and more recently for sensing. Given the advantages of RFID technology, its use is already widespread and is now experiencing new developments, in particular thanks to the RAIN alliance[3]. RAIN RFID is a global alliance promoting the universal adoption of UHF RFID technology that connects billions of everyday items to the internet, enabling businesses and consumers to identify, locate, authenticate, and engage each item. Among the relevant and very enabling information that each tag can provide to the RFID reader, in addition to the identification, a specific signature for tag authentication purposes is fundamental when securing is required to determine if an item is genuine. Authentication is very important in numerous applications where we need not only to identify a tag but also to ensure that this tag is the one we need. Although several software authentication methods are possible, they are very CPU memory and time-consuming. Authentication methods requiring less embedded resources are expected. Such methods must be compliant to all UHF standard tags without need of extra hardware or software ressources.

The objective of this project is to develop and perform an authentication method (the HRFID-authenticate[4]). Such a method is based on the exploitation of the characteristics of the signals generated by any tag when interrogated by a standard RFID reader. More precisely, when an UHF RFID tag receives an interrogation signal from reader it replies to reader by modulating its reflection between two states. From wireless communication point of view each reflection state corresponds to a specific value of tag Radar Cross Section (RCS). The difference between the two states is the Differential RCS (ΔRCS). The ΔRCS depends on the frequency of the interrogation signal and on the physical characteristics of the tag (RFID chip, antenna, substrate, impedance matching between tag antenna and RFID chip). Since two tags even with same reference have physical tiny differences, they result in ΔRCS differences in the generated tags replies. The idea is to cumulate these small differences over the frequency bands (fundamental and its harmonics) [1]. It is by cumulating this variability of the ΔRCS between two tags that the authentication function can be obtained. The procedure requires building a database that contains the ΔRCS for each tag. Finally, a digital signature (in the form of QRcode) will be associated with each tag which allows it to be authenticated. For the measurement we will use the professional RFID platform "tagformance".

6.2 Project deliverables

- Discover and run the HRFID reader
- Discover and run the Measurement Tagformance[5] platform
- Database generation of authenticated tags
- Develop and run authentication metric(s) on Matlab
- Validation on real tags
- Generate a digital authentication key

References

[1] G. Andía Vera, Y. Duroc, and S. Tedjini. "Analysis of Harmonics in UHF RFID Signals". *IEEE Transactions on Microwave Theory and Techniques* 61.6 (2013), pp. 2481–2490.

[3] https://rainrfid.org/

[4] HRFID-authenticate, patent pending. It is issued as an application of the HRFID project.

[5] Tagformance https://landing.voyantic.com/download-tagformance-pro-catalogue.

7 SenseROS: Sense-and-avoidance strategies for nanodrone collision avoidance implemented in ROS

Contact details	**ionela.prodan@lcis.grenoble-inp.fr, florin.stoican@upb.ro, nguyen@fe.up.pt**
Project keywords	**UAV, ROS, Gazebo, Collision avoidance**
Skills	**Robotics, Matlab/Simulink and Python, Modeling, Control theory**

7.1 Project context and goals

The increased use of small aircrafts in cluttered spaces such as indoor or urban environments raise the chance of "conflicts' (near collisions, unsafe maneuvering). In this context, many recent works have dealt with "potential conflict resolution" or "deconfliction", which is the prescription of maneuvers to maintain a certain minimal safety distance between aircrafts when a potential conflict is identified [2].

We will consider sense-and-avoidance strategies where obstacles are detected at runtime and collision avoidance is implemented on-the-fly. This is done through the analysis of proximity sensors (such as sonar/lidar) and subsequent control decisions. ROS (Robot Operating System) and Gazebo allow to simulate realistically the autonomous vehicles and retrieve their exact position and attitude, thus making the collision avoidance computations possible to implement.

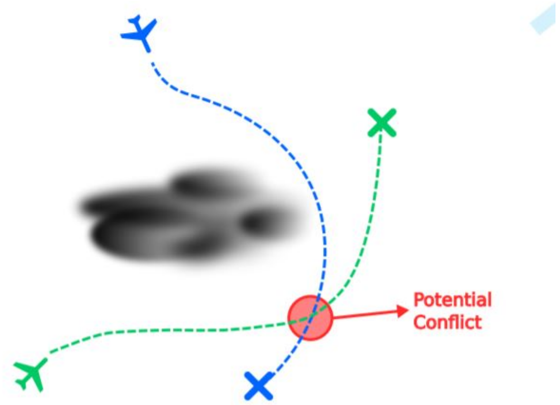


Fig. 1. A typical mission with two vehicles and their respective target sets hindered by a no-fly zone.

There are drone platforms already implemented in Gazebo (among which, popular ones such as Crazyflie, Hector, etc.) hence, the students can concentrate on the control and implementation aspects of the scheme.

The objectives of the project are the following:

- Understanding ROS and Gazebo environments [3];
- Improve an already existing motion planning algorithm by enforcing collision avoidance among two aerial vehicles [4];
- Extend the solution for multiple aerial vehicles [1].

7.2 Project deliverables

- Understand the Crazyflie platform simulated in ROS and Gazebo;
- Python implementation of sense and avoidance strategies for collision avoidance;
- Simulation scripts of the designed controllers, done with Matlab/Simulink and Python;
- Technical report with simulations and experimental results.

References

[1] N. Tran, I. Prodan, E. Grøtli, and L. Lefèvre. "Potential-field constructions in an MPC framework: application for safe navigation in a variable coastal environment". *IFAC-PapersOnLine* 51.20 (2018), pp. 307–312.

[2] R. J. M. Afonso, R. K. H. Galvao, and K. H. Kienitz. "Sense avoidance constraints for conflict resolution between autonomous vehicles". *IEEE Intelligent Transportation Systems Magazine* 9.1 (2017), pp. 110–122.

[3] F. Furrer, M. Burri, M. Achtelik, and R. Siegwart. "RotorS—A modular Gazebo MAV simulator framework". *Robot Operating System (ROS)*. Springer, 2016, pp. 595–625.

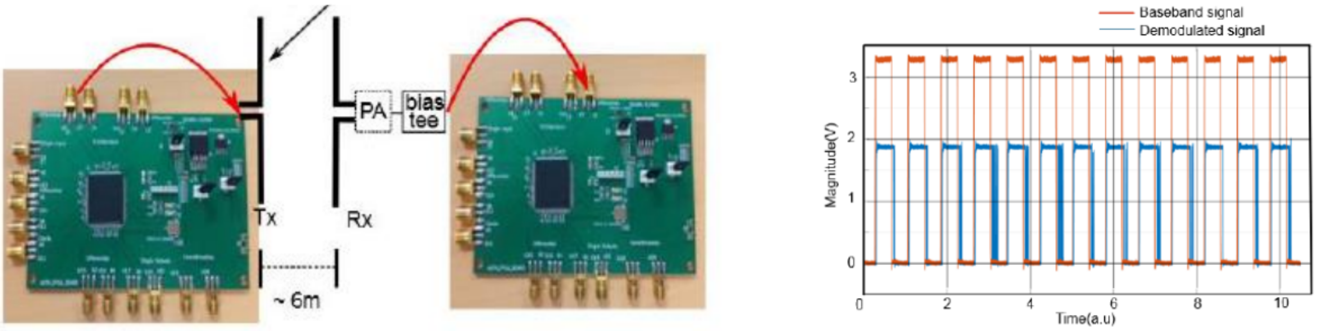
[4] I. Prodan, G. Bitsoris, S. Olaru, C. Stoica, and S.-I. Niculescu. "Constrained control design for linear systems with geometric adversary constraints". *IFAC Proceedings Volumes* 46.2 (2013), pp. 815–820.

8 WirelessFPGA: Wireless communications using FPGA

Contact details	**romain.siragusa@grenoble-inp.fr**
Project keywords	**FPGA, Wireless, Radiofrequency.**
Skills	**embedded programming, VHDL, RF communications.**

8.1 Project context and goals

FPGA were first developed to do prototyping of systems before designing a system on chip. Today, the decrease of their cost and their flexibility makes them good candidate to be used in any embedded system. However, this flexibility has a limit when it is desired to achieve wireless communication between two FPGAs. Indeed, being purely logical circuits, the design of RF transceivers is so far impossible without the addition of expensive analog circuits such as mixers, amplifiers, PLLs, etc. For example, it is possible to find commercial FPGAs that generate RF signals, but these are generated by analog blocks directly integrated into the FPGA. In a recent thesis at the LCIS laboratory, we proved that it was possible to use low-cost FPGAs to perform complex RF functions from simple power splitters to RF transceivers. A ten-meter communication using an OOK protocol was carried out around 500 MHz by simply adding a wire antenna to the FPGA [2].



(a)

(b)

Figure 1: (a) Schematic of the wireless communication using Spartan 3 FPGA (b) Baseband and demodulated signal using 6 meters communication.

The objective of the project is initially to take charge of the FPGA boards developed during the thesis and to redo the elementary RF components such as a switch, a power divider or an oscillator. Then a wireless communication in OOK modulation will be carried out and characterized. The reading range, the phase noise of the oscillator, the maximum bit rate and the bit error rate will be important elements to evaluate. A second objective will be to evaluate the use of the Lattice ECP5-5G FPGA board to perform a wireless link at 2.45 GHz [1]. Indeed, these FPGAs have analog blocks allowing the generation of signals up to 5 Gbit/s. The goal is therefore to divert the use of these blocks to perform a RF link without adding components other than an antenna.

8.2 Project deliverables

- Design, implement and validation of a basic RF functions on the provide FPGA board.
- Design, implement and validation of a RF wireless communication on the provide FPGA board. The limits of the systems need to be evaluated.
- Generate a digital authentication key

References

[1] *Lattice ECP5 Evaluation Board.* https://www.latticesemi.com/products/developmentboardsandkits/ecp5evaluationboard.

[2] M. M. Ahmed, E. Perret, R. Siragusa, D. Hely, F. Garet, N. Barbot, and M. Bernier. “Implementation of RF communication subsets on common low frequency clocked FPGA”. *2019 49th European Microwave Conference (EuMC).* 2019, pp. 742–745.

9 MicroGrid: Design and testing of a prototype small scale DC microgrid

Contact details	**ionela.prodan@lcis.grenoble-inp.fr,** **nicolas.barbot@lcis.grenoble-inp.fr**
Project keywords	**DC microgrid, Energy management**
Skills	**Embedded programming, Electronics, Instrumentation, Control theory, Matlab/Simulink and Python**

9.1 Project context and goals

Green (solar and wind in particular) energy production is supposed to increase significantly in the coming years, since the traditional energy supplies of Earth are finite and suffer from a ”diminishing returns” curse. This requires a ”smartgrid” system capable of dealing with distributed production/intermittent variations of output and optimal scheduling of demand. Microgrids are key solutions for integrating renewable and distributed energy resources, as well as distributed energy-storage systems [1].

Microgrids are composed of a monitoring systems which allows to estimate the power generated and consumed, the use and/or the state of each node of the grid. A (central) entity is responsible for gathering the information of the grid and determine the best strategy to maximize a given metric (reliability, security or efficiency) in real time.

The objective of this project is to design and test a prototype small scale DC microgrid. This electrical network can be composed of different producers (photovoltaic cells, wind turbine) and different consumers (light systems, motors, resistances and the like). Moreover, some systems could act simultaneously as producers and consumers (electric vehicles, batteries, super capacitors). The testing of the designed DC grid consists in implementing classical algorithms for power balancing.

Figure 2: Some of the microgrid components: fuel cells, wind turbine, power inverter.

9.2 Project deliverables

- Selection of the different producers/consumers for the prototype (some instrumentation devices have already been bought);
- Development of a generic monitoring interface. This system will be supervised through a microcontroller whose role will be, first, to measure the power generated or consumed by a node and, second, to distribute it throughout the grid, using the common bus. An interface will connect to a PC on which supervision software will reside.
- On the PC station, algorithms have to be developed (in Matlab or Python) with the goal of switching on and off different resources of the grid. Complex algorithms based on optimization can also be implemented to maximize a given metric (for example, minimize power loss).
- Hardware implementation of a prototype of the proposed small scale DC grid.

References

[1] I. Prodan and E. Zio. “A model predictive control framework for reliable microgrid energy management”. *International Journal of Electrical Power & Energy Systems* 61 (2014), pp. 399–409.

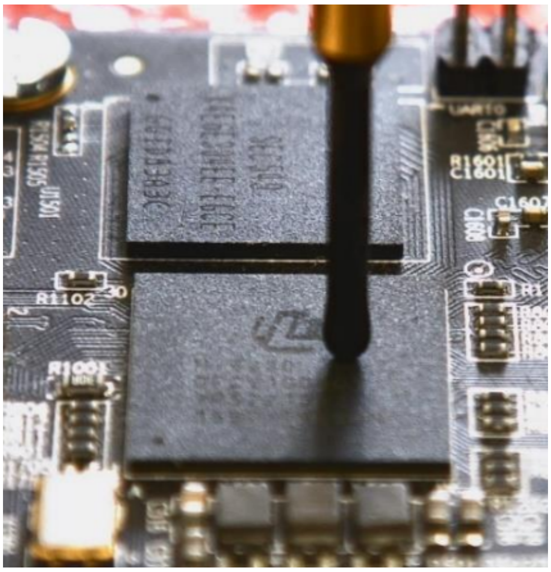
10 RISC-V: Architecture Evaluation Against Electromagnetic Fault Attack

Contact details {zahra.kazemi, amir-pasha.mirbaha, david.hely}@grenoble-inp.fr

Project keywords Embedded Systems, Hardware Security, Fault Injection Attacks.

Skills Embedded Programming, FPGA Design, Python or MATLAB.

10.1 Project context and goals



Critical embedded systems (e.g., healthcare IoTs) that are physically accessible by the adversary can be subjected to fraudulent manipulations called hardware attacks. One of the most effective hardware attacks can be conducted by the Electromagnetic Fault Injection (EMFI) [4]. In order to alter the chip, EMFI can be induced without any decapsulation, even on the most performant recent SoCs [2, 3]. The CTSYS team works on deploying tools to evaluate such threats against various processor architectures, including ARM, AVR, and RISC platforms.

The goal of this work is to evaluate a RISC-V-based system under such attacks. To this end, an electromagnetic (EM) glitch generator should be used to generate and inject flexible EM pulses into the target under evaluation, here a Rocket-Chip RISC-V system ASIC design.

The students need to characterize the effect of EM glitch attacks on the running embedded C application on the RISC-V processor. The different steps of the work will be:

- To develop a script to configure the EM glitch generator in order to inject accurate faults within the system
- To report the fault configuration that leads to successful attacks on high-level C functions
- To implement the SecPump application [1] on the RISC-V processor and assess the important parts of its code
- To report the SecPump's Control/Data flow corruptions by the EMFI

10.2 Project deliverables

- Completed EMFI configurator scripts
- Results of EMFI campaign against embedded C application running on the RISC-V based system
- Classification of EMFI effects on high-level C functions
- Evaluation report of SecPump application against EMFI

References

[1] C. Bresch, D. Hély, S. Chollet, and R. Lysecky. "SecPump: A Connected Open-Source Infusion Pump for Security Research Purposes". *IEEE Embedded Systems Letters* 13.1 (2021), pp. 21–24. DOI: 10.1109/LES.2020.2979595.

[2] M. Dumont, M. Lisart, and P. Maurine. "Modeling and Simulating Electromagnetic Fault Injection". *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 40.4 (2021), pp. 680–693. DOI: 10.1109/TCAD.2020.3003287.

[3] K. Basu, R. Elnaggar, K. Chakrabarty, and R. Karri. "PREEMPT: PReempting Malware by Examining Embedded Processor Traces". *2019 56th ACM/IEEE Design Automation Conference (DAC)*. 2019, pp. 1–6.

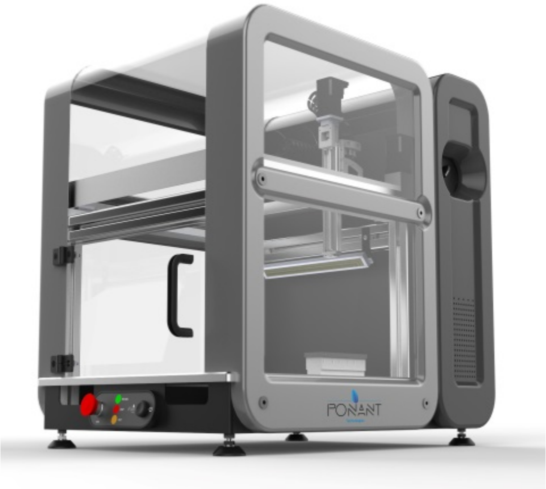
[4] P. Maurine. "Techniques for EM Fault Injection: Equipments and Experimental Results". *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*. 2012, pp. 3–4. DOI: 10.1109/FDTC.2012.21.

11 CAROB2: Cybersecurity Analysis with a ROBot

Contact details {gabriel.blanchard, vincent.beroulle, mickael.seignobos}@esisar.grenoble-inp.fr

Project keywords cybersecurity, vulnerability analysis, wireless attacks, IoT.
Skills embedded programming, hardware security, microcontroller

11.1 Project context and goals



The multiplication of the industrial Internet of Things ”IIoT” increases the attack surface of industrial sites. This increase in the density and number of access points involves significant security breaches. The cost constraints faced by manufacturers during the design and manufacturing phases can lead to the choice of weak or non-existent security mechanisms. The IoT designer has few means to assess cybersecurity during its product development cycle. The proposed project aims to develop a demonstrator showing the value of having a tool for automatically assessing the vulnerability of a connected insulin pump. A robot provided by the company PONANT Technologies will allow automating the implementation of configurations via, for example, a Bluetooth application on a smartphone (pin code, operating mode selections). The insulin pump has been developed in the LCIS laboratory. It is based on a STM32 microcontroller and a Bluetooth Low Energy extension.

Wireless attacks (such as jamming, spying, man in the middle) will be carried out for a large number of object configurations. To perform these attacks the MIRAGE framework [1] developed in Python with the BLE Ubertooth one dongle [2] will be used. The observation of the IoT device interface or its side-channels (consumption, timing, EM radiation) in real time will be used to guide the robot in performing the configuration choices.

11.2 Project deliverables

- Definition of wireless attack scenarios
- Selection of side-channel parameters to monitor the internal state of the pump
- Analysis of attack results with MIRAGE for different scenarios
- Full automation of RF vulnerability scanning with PONANT robot to automate tests

References

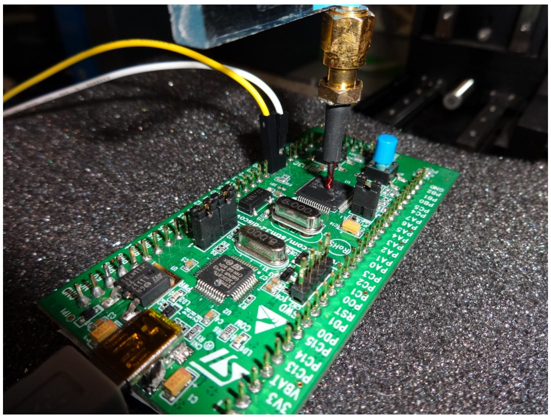
[1] R. Cayre, J. Roux, E. Alata, V. Nicomette, and G. Auriol. *Mirage : un framework offensif pour l’audit du Bluetooth Low Energy.*

[2] *Dominic Spill. Ubertooth.* `http://ubertooth.sourceforge.net/`. 2012.

12 AttackC: Electromagnetic Fault Injection Attacks on Cryptographic Algorithms

Contact details	**{zahra.kazemi, amir-pasha.mirbaha, david.hely}@grenoble-inp.fr**
Project keywords	**Hardware Security, Fault Injection Attacks, Cryptography.**
Skills	**Embedded Programming, FPGA Design, Python or MATLAB.**

12.1 Project context and goals



Embedded systems, because they contain confidential information, are subject to fraudulent manipulation, commonly called attacks, by malicious people. Between several means of hardware attacks, one of the most effective is Electromagnetic Fault Injection (EMFI) [3]. Because EMFI can be induced without chip decapsulation, even on the most performant recent SoCs [1].

As a consequence, it is possible to inject faults into the encryption process inside an unsecured microcontroller. For instance, an Advanced Encryption Standard (AES) [4] implementation as a symmetric cryptography algorithm can be targeted [2]. In this case, it may be possible to extract the secret key or other sensitive information by differential methods and basic cryptanalysis skills. The goal of this project is to inject exploitable faults into the cryptography processes inside an unsecured microcontroller. The different steps of the work will be:

- Programming the EMFI equipment for an automated characterization process, including the EM glitch injector, the XYZ table, and the circuit, from the control PC
- Programming an AES in target microcontrollers
- Evaluation of some EM pulse injection antennas
- Realization of exploitable EM fault injection on target microcontrollers
- Cryptanalysis of the faulty and correct encryption pairs to find the secret keys by Differential Fault Analysis methods

12.2 Project deliverables

- Python or MATLAB scripts for controlling the EM Fault Injection bench
- Embedded AES codes
- Characterization test results for EM pulse injection antennas
- Setup details for successful attacks and the associated results

References

[1] M. Dumont, M. Lisart, and P. Maurine. “Modeling and Simulating Electromagnetic Fault Injection”. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 40.4 (2021), pp. 680–693. DOI: 10.1109/TCAD.2020.3003287.

[2] A. Dehbaoui, J.-M. Dutertre, B. Robisson, and A. Tria. “Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES”. *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*. 2012, pp. 7–15. DOI: 10.1109/FDTC.2012.15.

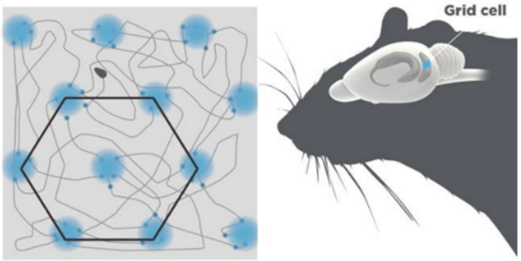
[3] P. Maurine. “Techniques for EM Fault Injection: Equipments and Experimental Results”. *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*. 2012, pp. 3–4. DOI: 10.1109/FDTC.2012.21.

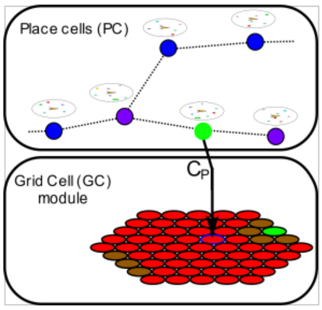
[4] M. Dworkin, E. Barker, J. Nechvatal, J. Foti, L. Bassham, E. Roback, and J. Dray. *Advanced Encryption Standard (AES)*. en. Nov. 2001. DOI: https://doi.org/10.6028/NIST.FIPS.197.

13 BioNav: Implementation of a bio-inspired navigation model on robotic platforms

Contact details	**{simon.gay, ionela.prodan}@lcis.grenoble-inp.fr**
Project keywords	**bio-inspired navigation, robotics, computer vision.**
Skills	**embedded programming, Java, computer vision, robot conception**

13.1 Project context and goals





Navigating in an unknown environment is a very complex task for mobile robots. However, many living beings can perform it with ease. This observation led to studies on mammal's navigation capabilities and the discover of specific neurons implied in navigation since the 70s (namely place cells, grid cells, head direction cells, border cells, center cells...). Since these discoveries, several artificial models were proposed in simulated environments and robotic platforms both to validate biological hypothesis and for developing robust navigation systems. Some of these models showed the capacity to map an entire city. In a collaboration between LCIS and LITIS laboratories, a new model was proposed to develop such a robust navigation system, based on several navigation neurons models (place cell, grid cell, head direction cell). This model was tested and validated in virtual environment but, although being tested with a simple stereo-camera, no robotic implementation was tested yet.

The aim of this project is thus to implement this navigation model on a robotic platform. This means developing a sensorial system that can provide spatialized information to the navigation model, optimizations for embedded applications and the development and tests of exploration and navigation strategies allowing to map an unknown environment and navigate toward a specific position of the environment.

13.2 Project deliverables

- Development of a sensory system that can provide spatialized points of interests that can be used by the navigation System. Different types of points of interests can be used in the different phases of development: AR-Tag (using their relative size on image), stereovision to detect position of salient elements, pattern detection;
- Implementation and optimization of the navigation model for embedded system (i.e. Raspberry Pi);
- Development and evaluations of exploration strategies to map an unknown environment and high level navigation algorithms to exploit the constructed environment model;
- Comparison with optimization-based control algorithms for safe navigation in cluttered environments.

References

[1] P. Santikellur, A. Bhattacharyay, and R. S. Chakraborty. "Deep Learning based Model Building Attacks on Arbiter PUF Compositions." *IACR Cryptol. ePrint Arch.* 2019 (2019), p. 566.

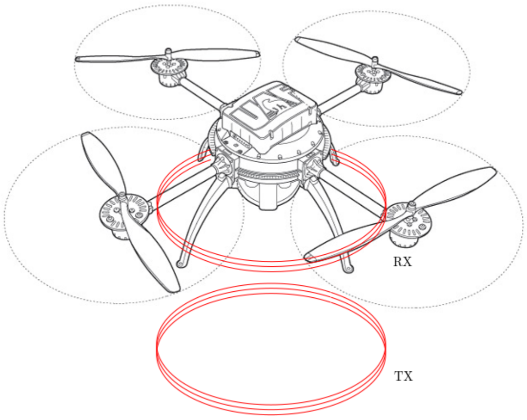
[2] T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama. "A new arbiter PUF for enhancing unpredictability on FPGA". *The Scientific World Journal* 2015 (2015).

[3] M. Soybali, B. Ors, and G. Saldamli. "Implementation of a PUF circuit on a FPGA". *2011 4th IFIP International Conference on New Technologies, Mobility and Security.* IEEE. 2011, pp. 1–5.

14 WPT4Drones: Wireless Power Transfer for Batteryless Nano Drones

Contact details	**{nicolas.barbot, ionela.prodan}@lcis.grenoble-inp.fr**
Project keywords	**Coils, Couplings, Drones, Controller.**
Skills	**Electronics, RF design, python, automation.**

14.1 Project context and goals



Wireless power transfer allows to supply any device without using wired connection. Classical examples include, NFC, RFID, phone chargers... Basic architecture is composed of two coupled coils, one used in transmission and the other used in reception. AC signal is applied on the first coil which generates a magnectic flux. This flux is collected by the second coil, then rectified and adapted to feed the load. Most of the devices operate at low frequency (below 1 MHz) and are limited to distances lower than 1 cm however, resonant coupling can be used to increase the distance while keeping an acceptable efficiency [2].

For the drone, Bitcrase Crasyflie will be investigated. This drone is a quadcopter of 27 g whose architecture can be enhenced by adding different kind of sensors. The main advantage of this drone is its opensource firmware which can be fully customized and adapted to any application.

The objective of this project is to design a wireless power transfer using resonant coupling allowing to lift a quadricopter form the ground. Both transmitting and receiving modules can be acquired and/or realized for the wireless power transfer. The receiving coil and associated electronis will be embedded on the quadcopter while transmitting coil is fixed on the ground. The quadcopter firmware has to be adapted to keep the quadcopter above the transmitting antenna at the heighest possible distance. Similar works have already succeed in real demonstrations [1].

This project will be presented at the student contest of the Wireless Power Week organized in July 2022 at Bordeaux.

www.wpw2022.org

14.2 Project deliverables

- Bibliographic study for the transmitting and receiving modules
- Characterization of the modules using laboratory instruments
- Optimization (EM simulations) of critical parts (coils...)
- Firmware modification of the Crasyflie
- Integration and test of the prototype

References

[1] J. M. Arteaga, S. Aldhaher, G. Kkelis, C. Kwan, D. C. Yates, and P. D. Mitcheson. "Dynamic Capabilities of Multi-MHz Inductive Power Transfer Systems Demonstrated With Batteryless Drones". *IEEE Transactions on Power Electronics* 34.6 (2019), pp. 5093–5104. DOI: 10.1109/TPEL.2018.2871188.

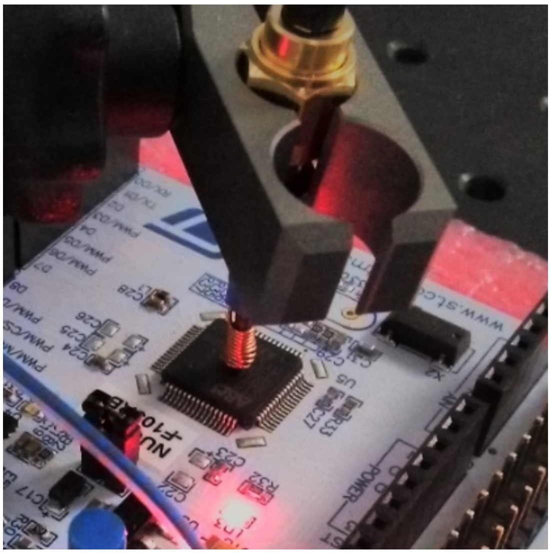
[2] A. Kurs, A. Karalis, R. Moffatt, J. D. Joannopoulos, P. Fisher, and M. Soljačić. "Wireless Power Transfer via Strongly Coupled Magnetic Resonances". *Science* 317.5834 (2007), pp. 83–86. ISSN: 0036-8075. DOI: 10.1126/science.1143254. eprint: https://science.sciencemag.org/content/317/5834/83.full.pdf. URL: https://science.sciencemag.org/content/317/5834/83.

15 TrigS4FI: Smart Triggering for Electromagnetic Fault Injection Attacks

Contact details {zahra.kazemi, amir-pasha.mirbaha, david.hely, vincent.beroule}@grenoble-inp.fr

Project keywords Hardware Security, EM Fault Injection, Synchronization.
Skills Embedded Programming, Python or MATLAB, Hardware Security

15.1 Project context and goals



With the rise of IoT systems in our daily lives, these objects deserve special attention to ensure their different security aspects, including hardware security concerns [2]. Fault Injection (FI) is an effective hardware attack that can be performed by injecting Electromagnetic [3]/Laser pulses into a target circuit or inserting glitches in its clock/voltage signal. To induce the faults, close to the points of interest (usually when the operations on the data are being performed), one can utilize GPIO (General Purpose Input-Output) pins which can be set high or low. This signal, namely Trigger Signal, gives helpful information to synchronize the targeted processor and the fault injector. A prevalent example is when an encryption algorithm is executing, and the Trigger Signal must be lifted at the start of an encryption algorithm and dropped at the end. Nevertheless, some targets do not have GPIO accessible to generate the trigger. This project aims to continuously acquire an analog physical quantity (Here EM emissions from the target) and convert it into digital data to simulate a Trigger Signal. We use a HackRF One board, an open-source and low-cost material for this aim. It allows receiving and transmiting a wide range of signals. However, only the analog/digital converter will be used. To capture emissions, there will be an antenna similar to a pen.

This project aims to use an EM fault injector to induce perturbation into an AES encryption running inside an unsecured microcontroller (e.g., an ST-Nucleo Board). Then, improving the attack's synchronization is envisaged by using a HackRF One board [1].

The different steps of the work will be:

- Programming the EMFI equipment for an automated characterization process, including the EM glitch injector and the circuit, from the control PC. The basic (MATLAB or Python) scripts will be provided.
- Programming a STM32 by an existing code (AES-128) and generating a Trigger Signal
- Realization of EM fault injection on the microcontrollers
- Improving the attack's synchronization by using a HackRF One board

15.2 Project deliverables

- Characterization results for EM fault injection campaign on target embedded code
- Modifying AES code to generate patterns that can improve the gathered signal from the HackRF One
- Comparing the accuracy of two methods of synchronization (GPIO Trigger vs. HackRF One)

References

[1] A. P. Sayakkara and N.-A. Le-Khac. "Electromagnetic Side-Channel Analysis for IoT Forensics: Challenges, Framework, and Datasets". *IEEE Access* 9 (2021), pp. 113585–113598.

[2] Z. Kazemi, A. Papadimitriou, D. Hely, M. Fazcli, and V. Beroulle. "Hardware Security Evaluation Platform for MCU-Based Connected Devices: Application to Healthcare IoT". *2018 IEEE 3rd International Verification and Security Workshop (IVSW)*. 2018, pp. 87–92. DOI: 10.1109/IVSW.2018.8494843.

[3] P. Maurine. "Techniques for EM Fault Injection: Equipments and Experimental Results". *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*. 2012, pp. 3–4. DOI: 10.1109/FDTC.2012.21.

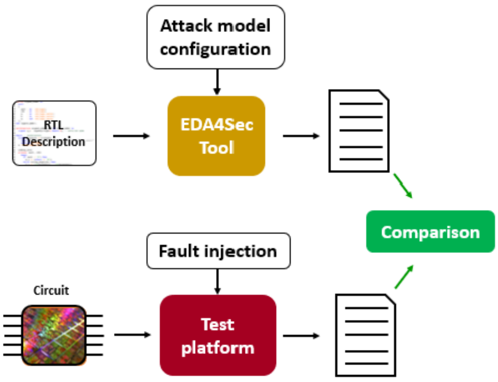
16 EDA4sec: Deployment and verification of fault injection model against hardware implementation of security primitives

Contact details {johan.marconot, david.hely, amir-pasha.mirbaha}@grenoble-inp.fr

Project keywords Hardware Security, Healthcare IoT, Clock Glitching.

Skills VHDL, hardware security, python

16.1 Project context and goals



Today adversaries exploit physical vulnerabilities to compromise integrated circuits. One of the most feared hardware threats is the fault injection: using pulse, laser or clock glitch an attacker can provoke a logic fault into the circuit, modifying the signal value or the register states. In the worst-case critical security operation such as ciphering or authentication processing can be corrupted; from smartcards to consumer devices such as PlayStation Vita'SoC for which an attacker shows how to break its secure boot ROM with voltage glitching [2].

The CTSYS team works on the deployment of tools to evaluate such threats against modern integrated circuits and embedded systems to further design efficient countermeasures (at both hardware and software levels). Lately, the team has developed CAD analysis tool which aims at evaluating an RTL design against the fault injection attack threat, in order to secure the circuit as soon as possible in its conception flow. Linksium, a technology transfer structure at Grenoble, supports and finances the development of this tool, name EDA4sec [1].

The goal of this project is to participate to the deployment and enhancement of EDA4sec by performing some fault injection attacks against the physical implementation of RTL designs such as AES or authentication module (and other circuits provided by industrial partners). These experiments will be based on EM and clock injections[3, 4, 5]. First, the team will have to identify with experiments the best set-up to break the security of the IC under study. Identify and to classify the most sensitive logic elements. Then, the experimental results will be compared with the analysis made by the tool EDA4SEC to verify the results of the software tool and investigate adequate configurations of the fault injection model in order to improve the correctness of the analysis tool.

16.2 Project deliverables

- Conduct fault injection (based on EM or clock perturbation) against RTL design (AES, FSM)
- Identify and classify the most sensitive register of the targeted circuits
- Assessing the pertinence of provided software model base security analysis tool
- Propose new model configuration to improve analysis of RTL design

References

[1] *EDA4sec*. https://www.linksium.fr/en/projects/eda4sec.

[2] Y. Lu. *Injecting Software Vulnerabilities with Voltage Glitching*. 2019. arXiv: 1903.08102 [cs.CR].

[3] A. Papadimitriou, D. Hély, V. Beroulle, P. Maistri, and R. Leveugle. "A multiple fault injection methodology based on cone partitioning towards RTL modeling of laser attacks". *2014 Design, Automation Test in Europe Conference Exhibition (DATE)*. 2014, pp. 1–4. DOI: 10.7873/DATE.2014.219.

[4] L. Zussa, J.-M. Dutertre, J. Clédière, and A. Tria. "Power supply glitch induced faults on FPGA: An in-depth analysis of the injection mechanism". *2013 IEEE 19th International On-Line Testing Symposium (IOLTS)*. 2013, pp. 110–115. DOI: 10.1109/IOLTS.2013.6604060.

[5] A. Dehbaoui, J.-M. Dutertre, B. Robisson, and A. Tria. "Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES". *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*. 2012, pp. 7–15. DOI: 10.1109/FDTC.2012.15.

17 BHFR2: Bionic Head and Facial Recognition

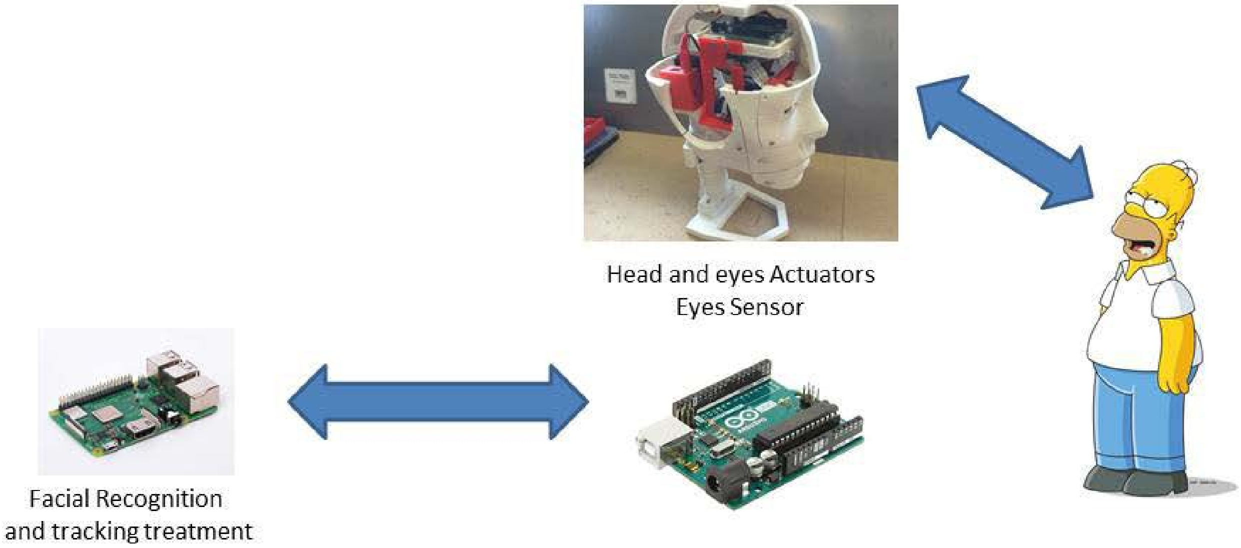
Contact details	**laurent.guilloton@esisar.grenoble-inp.fr**
Project keywords	**Camera, Facial Recognition, Jetson Nano/RPI/STM32/Arduino.**
Skills	**embedded programming, Electronics, 3D printing.**

17.1 Project context and goals

BHFR2 is the continuation of a previous project. It aim to create interaction between a robot and a human. By using developments on facial recognition like OpenCV [3] it would be interesting to develop a demonstrator recognizing shapes and faces to launch an action, a message, ...

So this project can be decomposed in different parts :

- finish printing and assembling the head and neck of the robot
- Control head and neck movement
- Study the different method for facial recognition and how implement them on an embedded computer.
- Choose and implement one of these methods on a Raspberry Pi [2] or Jetson Nano [1].



This work will eventually develop new features such as opening a door depending on the person detected or otherwise.

17.2 Project deliverables

- Head and eyes functional
- Comparative facial recognition algorithms
- Implementation and test in the final prototype

References

[1] *Jetson Nano*. https://developer.nvidia.com/embedded/jetson-nano-developer-kit.

[2] *Raspberry Pi*. https://www.raspberrypi.org/.

[3] G. Bradski. “The OpenCV Library”. *Dr. Dobb’s Journal of Software Tools* (2000).

18 SmartBuildROS: Smart Building simulation with ROS and Gazebo

Contact details {karem.hafsi, denis.genon-catalot}@lcis.grenoble-inp.fr

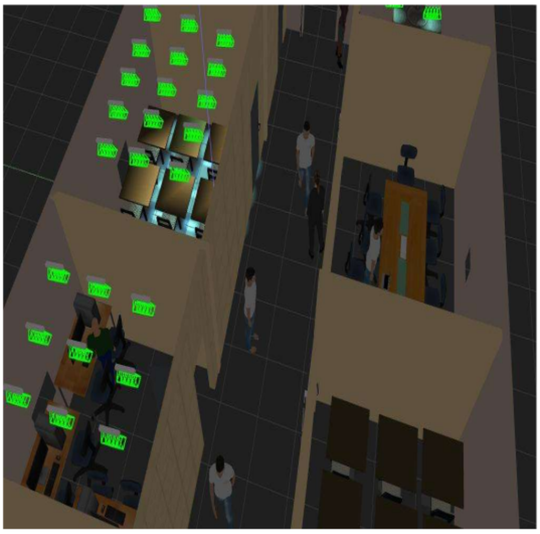
Project keywords Smart building, simulation.
Skills embedded programming, Linux tools.

18.1 Project context and goals

The World buildings consume over 30% of the worldwide total energy consumption, and 90% of these buildings are either small-sized (lower than 5,000 sqft) or medium-sized (5,000-50,000 sqft) [3]. For small- and medium-sized buildings, heating consumption is the dominant end use, followed by lighting, plug loads and cooling. Specifically, Heating, Ventilation, and Air-Conditioning (HVAC), lighting and plug loads account for almost 90% of all consumption in buildings.

In this context, reducing buildings consumption is the main goal for many projects around the world including this LCIS research lab project.

Gazebo is an open-source 3D simulator which integrates the ODE physics engine [1], it's almost used with ROS [2] (Robotic Operating System) for robots and autonomous cars simulation, but it can model sensors that "see" the simulated environment, such as laser range finders, cameras, Kinect style sensors, etc.



In this project, we will model our smart building as bunch of nodes in distributed architecture. These nodes represent all the loads in the buildings (lights, blinds, HVAC, etc) and all energy sources such as battery storage, grid source, solar panels, etc.

Differents scenarios will be studying (depend on grid energy price, availability of renewable energy, loads priority...). In each case we are going to simulate the impact of its changes on our simulated environment, its impact on the end-users comfort and at the end the final energy balance.

18.2 Project deliverables

- Development of an API between Gazebo and smart nodes.
- Gazebo plugins development.
- Simulated nodes development.
- Documentations.

References

[1] *Gazebo*. http://gazebosim.org/.

[2] Stanford Artificial Intelligence Laboratory et al. *Robotic Operating System*. Version ROS Melodic Morenia. May 23, 2018. URL: https://www.ros.org.

[3] A. Anvari-Moghaddam, H. Monsef, and A. Rahimi-Kian. "Cost-effective and comfort-aware residential energy management under different pricing schemes and weather conditions". *Energy and Buildings* 86 (2015), pp. 782–793.

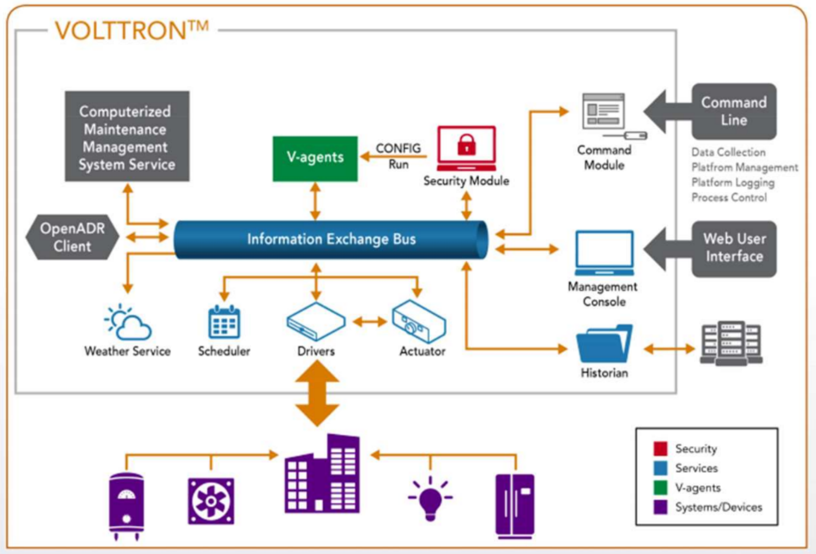
19 SmartBuildV: Smart Building management platform based on VOLTTRON^{TM} (Eclipse Foundation)

Contact details	**{karem.hafsi, denis.genon-catalot}@lcis.grenoble-inp.fr**
Project keywords	**Smart building, simulation.**
Skills	**embedded programming, Linux tools, python.**

19.1 Project context and goals

With a consumption of 458 Mtoe in 2016, buildings account for 41% of the final energy consumption and 60% of the electricity consumption in the EU-28. Two thirds of this consumption are for residential buildings. In this context, reducing buildings consumption is the main goal for many projects around the EU and the world including LCIS research lab project (ANR-C3 , Arrowhead,...).

VOLTTRON^{TM} is an open source distributed control and sensing software platform [2]. Cost effective, scalable and secure, this technology improves the control of heating, ventilation and air conditioning (HVAC) systems, electric vehicle chargers, distributed energy resources such as renewable and batteries, entire building power loads and more. The main goal of this project is to set up a multi-agents system using the Voltron platform for energy distribution between sources and loads. All agents in the system should cooperate to minimize the energy consumption and subserve the use of renewable energy. To achieve, we need to develop some drivers in order to communicate with not supported protocols such as MQTT [1]... and interface this platform with Gazebo interface for simulations purposes (cooperation with the other group project working on Gazebo is possible).



19.2 Project deliverables

- Development of a driver for MQTT communication.
- Development of the different agents.
- Interface between Voltron and Gazebo.
- Documentations.

References

[1] *MQTT*. https://mqtt.org/.

[2] *VOLTTRON*. https://volttron.org/.

20 OpenSource3d: Open source software design, testing, and assembling of a custom equipment for 3d RFID tag characterization.

Contact details	**{marco.garbati, etienne.perret}@lcis.grenoble-inp.fr**
Project keywords	**Python, G-code, instrumentation, RFID, RF characterization.**
Skills	**Python, C++, G-code, Arduino, Robotics, Electronics.**

20.1 Project context and goals

The development of the Internet of Things "IoT" brings the need of customized test equipment not available in the market [1]. This project concerns the software design, testing, and assembling of a custom equipment for 3d RFID tag characterization. It should be able to perform automatic 3-d cartography evaluation of a RFID tag response. The main control unit is a dedicated personal computer. The PC is controlling at the same time the mechanical motion of the tags (positioning of the tag), and the dedicated RFID test equipment. The mechanical and electronic design have been already carried out. It makes use of off the shelves components, such as: the 3-d printing machine Creasee CS30, and the Zonestar ZM3E4 control board for 3-d printing machine. In addition, few mechanical parts have been designed and manufactured with a Zortrax 3-d machine.

The project is based on three main points:

- The firmware for the machine needs to be designed. It has to be open source and written in G-code. Utility such as Marlin Firmware and Visual Studio can be used to simplify the process. The firmware is based on the functionality of the Zonestar ZM3E4 control board.
- To carried out the testing process, the project needs the realization of a main control software written in Python, that should be able to communicate with the machine and also with RFID test equipment such as a Vector Network Analyzer "VNA".
- A complete 3-d cartography of a chipless RFID tags response needs to be generated at the end of the project to validate the system functionality.

20.2 Project deliverables

- Source G-code of the firmware designed for the Zonestar ZM3E4 control board.
- Source python code of the main control software
- 3-d cartography result of a chipless RFID tag.

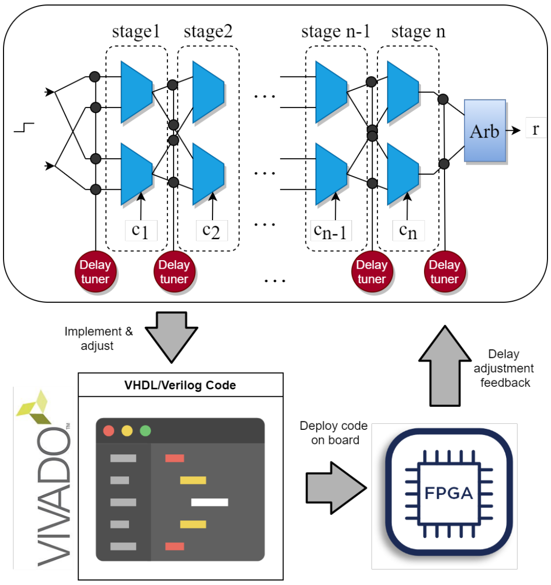
References

[1] R. T. de Alencar, N. Barbot, M. Garbati, and E. Perret. "Characterization of Chipless RFID Tag in a 3-Dimensional Reading Zone". *2019 IEEE International Symposium on Antennas and Propagation and USNC-URSI Radio Science Meeting.* 2019, pp. 639–640. DOI: 10.1109/APUSNCURSINRSM.2019.8888559.

21 SA-PUF: Implementation of Simple Arbiter PUF on FPGA

Contact details	**{amir.ali-pour, david.hely}@lcis.grenoble-inp.fr**
Project keywords	**Arbiter PUF, FPGA; Verilog, VHDL.**
Skills	**Embedded programming, VHDL, design verification**

21.1 Project context and goals



Have we wondered whether two silicon micro-chip instances with exactly the same design, would differ in their micro fabrication? Indeed, in their macro manifestation, they should be the same. However, micro-variations do exist in the bare-metal level of silicon-chips' fabrication which infers that two or more silicon chips do differ from one another in their micro-fabrication. And this is where Physically Unclonable Functions (PUFs) come to play to use this low-level differentiation and implement device-specific unique identifiers. PUF have been introduced now for more than a decade and are considered nowadays as one of the emerging security primitives for resource-constraint ecosystems in the field of IoT. PUFs are leaning to replace the conventional way of encryption key generation which are heavily depended on storing key data on non-volatile memory. Variants of PUF exist, each characterizing the functionality differently based on the micro-variations. Strong PUF is a macro variant which aims at implementing a functionality on silicon chip to make compositions of the underlying micro-variations to generate an abundance of device specific identifiers. This functionality is based on mapping a bit-vector challenge (the input) to a response (output) and generate a so-called Challenge-Response-Pair (CRP). Very large number of CRPs can be generated by a strong PUF depending on the size of the challenge (see Figure. 1). Arbiter PUF is one of the known strong PUF structures. The idea of Arbiter PUF is based on the delay difference between two racing paths which are structurally similar, but due to minor process variations, they differ in the signal propagation delay. The structural construction of Arbiter PUF is seemingly simple, which is one of the reasons why it is a common strong PUF. It provides a rich source of device specific identifiers. However, the planning and deployment of the Arbiter PUF design onto a circuit, a chip or an FPGA is a bit of a challenge. There the designer needs to make sure that the PUF's unique characteristic is manifested solely by the signal paths' propagation delay differences, and not by constructional differences. This means for instance, that when an Arbiter PUF VHDL code is deployed on two or more FPGA's, the allocated resources of the FPGAs' are exactly the same, but their CRP characteristic is different.

In this project, the students will implement a simple Arbiter PUF using Verilog or VHDL, and evaluate their implemented PUFs on several FPGAs to confirm the true functionality of their implemented PUF. The implementation work in this project is fairly simple. However, the verification process is where the students are challenged to ace their work. Throughout this project, the students will be introduced and then engaged with formal yet fairly straightforward verification methods to confirm that their PUF is correctly mapped on the device micro-variations. The end result will be to see how the micro-variations can in turn provide device-specific identifiers, which is the beginning point of how PUFs would work.

21.2 Project deliverables

- Design and implementation of a simple Arbiter PUF with low dimentiality using Verilog or VHDL.
- Design and implementation of dynamic components which allow tuning the PUF to eliminate macro-variation effects on the PUF characteristic.
- Verification and evaluation of their Arbiter PUF on few (3 to 5) FPGA boards.
- Verification records of the implemented Arbiter PUF with formal methods (given to the students by the supervisor).