Innovation projects 5A EIS – PX505 – 2022-2023

Responsible: Ionela PRODAN

August 2022

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.

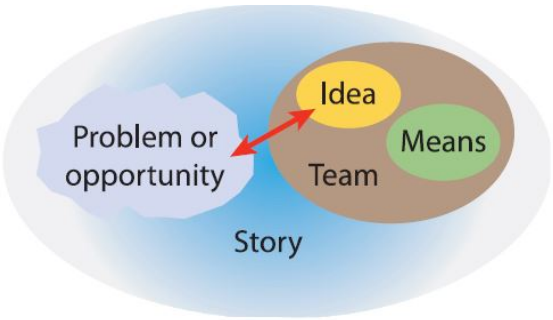
Hence, the students are not asked for something entirely new, but improvement or expansion of something that is already in use. That is:

- 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:

- 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 ($\approx$ 1 page)
- a detailed project development plan ($\approx$ 2 pages);
- a project schedule or Gantt diagram (1 page);
- a distribution of individual tasks (1 page);
- milestones and risk analysis ("plan B") ($\approx$ 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 ($\approx$ 1 page)
- Related work ($\approx$ 2 pages)
- Demonstrator architecture ($\approx$ 3 pages)
- Validation environment and results ($\approx$ 7 pages)
- Societal challenges of their innovation ($\approx$ 1 page)
- Conclusions ($\approx$ 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 2022**

  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 2022**
- **Starting of the project: 20 September 2022**
- **Mid-report submission: 21 October 2022**

  The students must upload the report on Chamilo:

  ESISAR PX504 Innovation Project 5A EIS/Travaux d'étudiants/MidReport PX505 (2022/2023)
- **Final report submission: 3 January 2023**

  The students must upload the report on Chamilo:

  ESISAR PX504 Innovation Project 5A EIS/Travaux d'étudiants/FinalReport PX505 (2022/2023)
- **Project defense: 10 January 2023**
- **Video preparation of the selected projects: until end of December 2022**

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 3 January 2023.

Part II
External proposals

1 FishID: Low Frequency RFID Reader for Fish Monitoring

Contact details nicolas.barbot@lcis.grenoble-inp.fr,
alexandre.richard@scimabio-interface.fr

Project keywords RFID, Wireless Power Transfer
Skills Electronics, RF, Antenna

1.1 Project context and goals

The study and monitoring of animal populations (fish, mammals, amphibians,...) is an essential issue for understanding ecosystems functioning and their transformations. Many human activities modify the natural behavior of animals. It is therefore essential to monitor animal populations in their environment to detect possible changes, understand the impact of human activity and assess the benefit of restoration programs.

The management of aquatic environments is the major activity of SCIMABO Interface [0], which specializes in monitoring fish populations in natural environment. (river, ponds, etc.) For this, LF RFID tags are implanted under the skin of fish. These tags are passive devices the size of a grain of rice and do not modify fish behavior. The tags can be detected by a reader when the fish passes near the loop type antenna. The exploitation of the results makes it possible to evaluate which fish were detected, their number, as well as other important informations for fish population management, like fish pass efficiency.

The current architecture of the RFID system used is based on the use of passive LF tags (implanted in the fish) and one (or more) active readers. The reader, produced by Stream-Innov, is based on the RI-RFM-008B30 and RI-CTL-MB2B modules sold by Texas Instrument. The reader uses an inductive loop to generate a magnetic field capable of transferring power to the tags. This power is also used by the tags to transmit information from the tag to the reader. This information uniquely identifies the tag read by the reader.

1.2 Project deliverables

The objective of this project is to build an alternative solutions which can replace the RI-RFM-008B30 and RI-CTL-MB2B modules:

- State of the art of the LF RFID technology
- Study of the RI-RFM-008B30 [0] and RI-CTL-MB2B [0] modules
- Design and implementation simple functionalities of the modules
- Integration with existing motherboard

References

[0] *RI-CTL-MB6B*. https://www.ti.com/lit/ug/scbu044/scbu044.pdf.

[0] *RI-RFM-007B*. https://www.mouser.com/datasheet/2/405/ri-rfm-007b-443793.pdf.

[0] *SCIMABO Interfaces*. https://www.scimabio-interface.fr/en/.

2 HealthDemo: Safe, Secure Connected HealthCare System Demonstrator

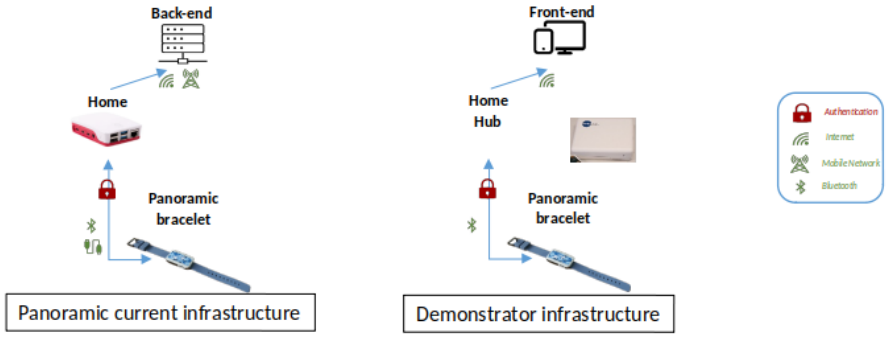
Contact details Thibault.FRANCO-RONDISSON@cea.fr, Christophe.VILLEMAZET@cea.fr

Project keywords IoT Security; embed Linux; BLE; Healthcare System
Skills Embedded System Programming, System Security

2.1 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 and the Panoramic Wearable, a medical device. The main purpose of this demonstrator is to show how the wearable medical IoT devices can be securely connected to the secure gateway which aggregate and analyze the medical data.

The gateway was developed by CEA LETI in the framework of IRT Nanoelec, it integrates STM32MP1 microprocessor based on the ARM TrustZone hardware isolation combined with STSAFE-TPM (Trusted Platform Module) certified CC EAL4+ and FIPS140-2 level 2; in order enables a safe area of execution with a secure module providing secure key storage for long term keys and a cryptographic toolbox for companies who want to secure devices communication.



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 CEA-LETI, STMicroelectronics, IRT Nanoelec and Panoramic Digital Health. Panoramic current setup uses a raspberry as aggregator connected to the device over BLE and the data are processed on a remote platform (see illustration above). The Panoramic Digital Health bracelet includes an accelerometer, gyroscope, magnetometer and pressure sensor that can quantify many relevant activities including mobility, sleeping, scratching. Data can be transmitted to the gatweway using BLE. The bracelet also includes a machine learning core which enables limited edge AI in the bracelet: the output of this MLC can be transferred to the Gateway for further edge computing.

The main tasks of the project are: 1. Replace the Raspberry with the secure gateway. 2. Define a use case to illustrate the data processing for medical data 3. Process the data from the Wearable into the gateway. 4. Create a clean User Interface to show processed data. 5. Illustrate the security enables with the new gateway After the integration of all the system components, the scenario will be deployed to showcase the security of the system.

2.2 Project deliverables

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

References

[0] *DigiFed*. https://digifed.org/generic-experiment/generic-experiment-on-cybersecurity-secure-platform-for-iot/.

3 eTex: Electrical signal conversion of a triboelectric fabrics into a sound or light signal

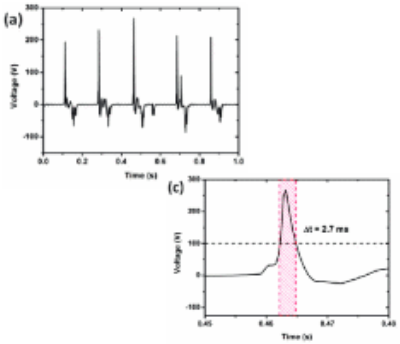
Contact details	**pascal.weber@gammao.fr**
Project keywords	**Triboelectricity, e-textile, Midi, Digital Arts, wearable electronics**
Skills	**embedded programming, signal processing, microcontroller**

3.1 Project context and goals

The field of wearable and e-textiles is booming. This discipline aims to integrate electronic functionalities in wearable devices, such as motion sensors, physiological sensors, or GPS sensors. The market of e-textile should reach a global volume of 500 million € within 3 years. GammaO is working in the field triboelectricity apply to the textile industry, thus emerged the idea of applying this technology to the event market as follow:

1. Triboelectric electrodes made by the company GammaO are placed on the surface of clothing or furnishing textiles, and the artist or user comes to activate these electrodes by contact (friction) thus generating a signal.
2. Analog signal processing to filter out stray background noise, by analog filters such as Notch filter, and/or signal rectification such as diode bridge Optional processing, which can also be carried out digitally after the acquisition of the analog signal
3. Analog signal acquisition
4. Digital interpretation of the signal(s) in terms of intensity, frequency, and duration.
5. Output of the signal processed according to the communication protocols between electronic instruments, controllers, sequencers, and music software such as: Midi Protocol, DMX Protocol (Light Effect), Midi Show Control (MSC), Midi Tuning Standard (MTS), General Midi...





3.2 Project deliverables

- Design, implement and validation of a FPGA board and its software
- Live Demonstration showcasing the potential of the solution
- Documentations to replicate the demonstrator within the partners

References

[0] K. Dong, X. Peng, and Z. L. Wang. "Fiber/fabric-based piezoelectric and triboelectric nanogenerators for flexible/stretchable and wearable electronics and artificial intelligence". *Advanced Materials* 32.5 (2020), p. 1902549.

4 Trace: Enhancing traceability of components during their Supply Chain process, through vocal assistance technologies

Contact details lina.duque@cat.com
Project keywords traceability, track and trace, voice assistance, escalation, packing list, shipment, GPS.

Skills

4.1 Project context and goals

Caterpillar France [**cat**] aims to implement a future a Track and Trace system, allowing to trace de parts' location during their Supply Chain process, starting at the supplier's location and up to the assembly line in Grenoble.

The objective of the future Components Traceability System is to achieve full components traceability.

Nevertheless, our Supply Chain processes are extremely complex today and very little automatized. We have no ERP in place. It would be required to decompose such a project into much simpler deployment steps. The first stage of deployment would only concern the connection of two main logistics data sources, which should be done prior to the shipment of the parts from the supplier's location towards Caterpillar location, and that are managed in different IT systems:

1. Part/component serial number (part ID)
2. Transport ID, which contains:
   - transport/truck identification
   - associated packing list
   - location of the truck

Today, the link between truck ID and packing list lacks robustness, contain many errors and is not reliable. Thus, the traceability of the actual location of a component is not reliable.

4.2 Project deliverables

- Assessment of available innovative technologies for components traceability in upstream logistics operations within the machines industry (with a similar structure to ours). Provide synthesis report.
- Assessment of the pertinence of using available voice assistance technologies in innovative ways, for the enhancement of the traceability of parts Supply Chain processes. Provide synthesis report.

5 QboardFM - space version of a mother board for an innovative smart CubeSat

Contact details tania.mcnamara@univ-grenoble-alpes.fr
Project keywords CubeSat, Earth Observation, Artificial Intelligence
Skills Electronics, PCB Placement, Mechanics, Thermics

5.1 Project context and goals

Started in early 2020, the QlevEr Sat project aims at bringing Artificial Intelligence (AI) onboard a demonstration CubeSat for Earth Observation (EO), which is a major innovation in the world of satellites. The overall project is led by the Centre Spatial Universitaire de Grenoble (CSUG) in collaboration with the Multidisciplinary Institute in Artificial Intelligence (MIAI UGA), Teledyne e2v and Air Liquide. QlevEr Sat will be surveying specific regions for deforestation. As the number of satellites increases, embarking AI directly on board will drastically reduce the bandwidth required for data transmission: only the post-analysis results can be downlinked, rather than images themselves.

During the preliminary phase of the project (Phase B), on the software side, the project team has developped an innovative light-weight edge AI model capable of running on the ARM microprocessor provided by Teledyne e2v (Qormino with its integrated 4GB DDR RAM) to detect forest vs non-forest and clouds vs non-clouds on high-definition images, thus reducing the average filesize by 50. Potentially it could learn to detect any texture, making it very versatile and innovative. It was developed in C++ and has already been successfully tested. On the hardware side, the team has designed and subcontracted a very first version of the Qormino mother board (Qboard) at CubeSat format (10 cm x 10 cm), based on existing reference designs, but the PCB test campaign has not yet started. The Place & Route was done in Altium Designer. Besides, it is necessary to define the future version of this first PCB engineering model for the future Flight Model (FM) of the satellite : what needs to be kept, what needs to be removed, what needs to be added, to make it fly. In other words to make it as suited as possible to a Low Earth Orbit environment, but still with the "NewSpace" approach.

The aim of the proposed student project is to study the technical risks and constraints (environmental and mechanical) for such a PCB in Space, to specify a more space-enabled (rather than fully space-qualified) version of the current engineering model prototype designed (in Altium Designer) for ground tests and demonstrations only, and to initialize a qualification plan for the future Qormino board Flight Model (QboardFM)). The tasks of the project are:

- Based on the current PCB design, identify the functions and components not needed for a space model
- Identify space qualified counterparts for some components
- Perform a preliminary place (part of place& route) of parts on the board based on mechanical and thermal constraints
- Produce a preliminary radiation tolerance analysis, including simulation of faults on power supply due to radiation events (Single Events Effects such as bit flips, etc.)

5.2 Project deliverables and supervision

- Environmental and mechanical risk analysis
- List of PCB Flight Model components and changes
- Preliminary board design (component placement only) based on mechanical constraints
- Preliminary radiation tolerance analysis at least on power supply
- Qualification plan initialization (test criteria, test equipments, test steps...)

The project will be supervised by an expert in Space electronics from the Air Liquide industrial partner in its CSUG-dedicated time, together with the CSUG QlevEr Sat Project Manager for the organisational aspects.

6 AI4RFID: Artificial Intelligence for better RFID localization

Contact details	**christophe.loussert@mojix.com**
Project keywords	**Artificial Intelligence, Data Science, Machine Learning, embedded programming, RF communication**
Skills	**Data science techniques, Embedded programming and Hands-on experimentation**

6.1 Project context and goals

RFID Technology is a mature technology that is use in many applications like logistic or stores. In this project, we want to address a well known problem that is still unsolved: the classification between "moving" tags and stationary tags. Indeed, the use case is made of a store security checkpoint (see Fig. 1) with:

1. "moving" tags physically running through the antennas (stolen items if not detected at the cashier)
2. "stationary" tags (on fixture inside the store)

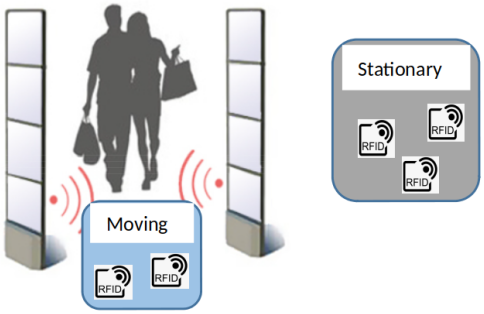


Figure 1: Use case of the project : a security checkpoint with moving and stationary tags.

RFID detects 100% of the "moving" tags passing by the antennas. RFID can also detect "stationary" tags up to 10m. Based on a traditional simplified RF model, the classification "moving" / "stationary" generates a number of errors, typically 5%. The goal is to implement Artificial Intelligence to reduce this error rate. Eventually, this AI will be implemented real time onto a low cost platform.

6.2 Project deliverables

1. Dataset in an RFID security checkpoint use case will be collected.
2. AI prediction model from the dataset
   a) tools : Python/pandas, scikitLearn, numpy, seaborn
   b) visualization, data structuring, modelling
   c) Performance comparison with simplified RF model
3. Embedded software will allow to run this AI model real time onboard the RFID reader itself and also a lost cost electronic platform (raspberry, arduino, …)

Part III
Students proposals

Part IV
Digital Arts proposals

7 VOLCA: Free the VOLCAs!

Contact details	**yann.kieffer@esisar.grenoble-inp.fr**
Project keywords	**Korg VOLCA, function extension, firmware, reverse-engineering, device modification**
Skills	**signal encoding/decoding, embedded programming, low-level code exploration, soldering/unsoldering, legal aspects**

7.1 Project context and goals

Although synthesizers have existed for more than 50 years now, a rather new tendency started during the 2010's: small but decent, affordable desktop synthesizers. The 3 big synthesizer manufacturers, which happen to be Japanese – namely Yamaha, Roland and Korg – all have started their line of "small and smart" synth lines. Korg's one is branded under the name VOLCA, and has now around 10 products available (synths and rhythm machines). Of course, the VOLCAs cannot compete in functionality with bigger and more expansive products. Still, they are great machines with nice features: for example, all of them have a sequencer, and a modulation sequencer. Although they can be used as genuine electronic musical instruments, the VOLCAs have a reputation of feeling a little unfinished – a feeling that is also an attribute of some full-size electronic instruments. Some able individuals have taken some time to try to improve the situation. Famous examples are the hardware modifications to try to improve the snare drum sound of the Korg VOLCA Beats [0], or the new custom firmwares created by Pajen for the Korg VOLCA Sample and the Korg VOLCA FM [0]. An internet survey will allow you to find out how Pajen was able to propose new firmwares for two of the VOLCAs. But Pajen did not document his work all the way through analysis and modification of firmwares. The objective of this project, "Free the VOLCAs", is twofold:

- Replicate Pajen's work, with the goal of making it widely available. This will need care as to what is legally possible or not in matters of reverse-engineering;
- Identify weak spots of the VOLCAs, and try to offer patches or improvements, whether that be software (firmware modifications, preferred) or hardware (more difficult for 3rd party to carry out).

VOLCAs will be provided to the team, but beware that, depending on the devices, there may be a delay in weeks between ordering and getting the device(s).

Figure 2: (a) Korg VOLCA Beats (b) Korg VOLCA FM (c) Korg VOLCA Sample

7.2 Project deliverables

- Code with documentation for decoding and encoding firmware from/to audiofiles in WAV format.
- Documentation (preferably as a set of web pages) explaining how to explore and modify firmwares for the VOLCAs.
- At least one example of improvement: i) full "how-to" documentation for hardware modifications; ii) documentation, source-code and firmware for software modifications.
- A short document making precise what are the currently legally accepted practices of reverse-engineering, and what are the limits one should not cross to be safe in, say, the USA and France.

References

[0] *Better Gear - Korg Volca Workstation (Pajen Firmware):* https://youtu.be/aq76Vr4Xm5I.

[0] *How to Mod Your Korg Volca Beats Snare Guide :* https://youtu.be/LLt33PDG2Wg.

Part V
LCIS/ESISAR proposals

8 Wring: Design of a Watchdog for hardware attack detection using ring oscillators

Contact details	**romain.siragusa@lcis.grenoble-inp.fr**
Project keywords	**FPGA, hardware attack, communication, Radiofrequency**
Skills	**embedded programming, VHDL, RF communication**

8.1 Project context and goals

IoT devices are present in many applications. Often low-cost and simple, they can be a gateway for software or hardware attacks. In a previous project, we showed that it was possible to use ring oscillators (Fig 1.a) to authenticate FPGA chips. Indeed, these resonators, simply designed by looped inverters, have the particularity of being very sensitive to the environment: temperature, supply voltage, threshold voltage of the transistors, etc. Fig 1.b shows that the resonant frequency a RO place on different slice of the FPGA varies a lot. It is therefore possible to use the resonant frequency of these devices to define a specific authenticator for each chip. Recently, we have also shown that it is possible to use these resonators at RF frequencies, around 800 MHz, to realize On-Off Keing modulated communications.

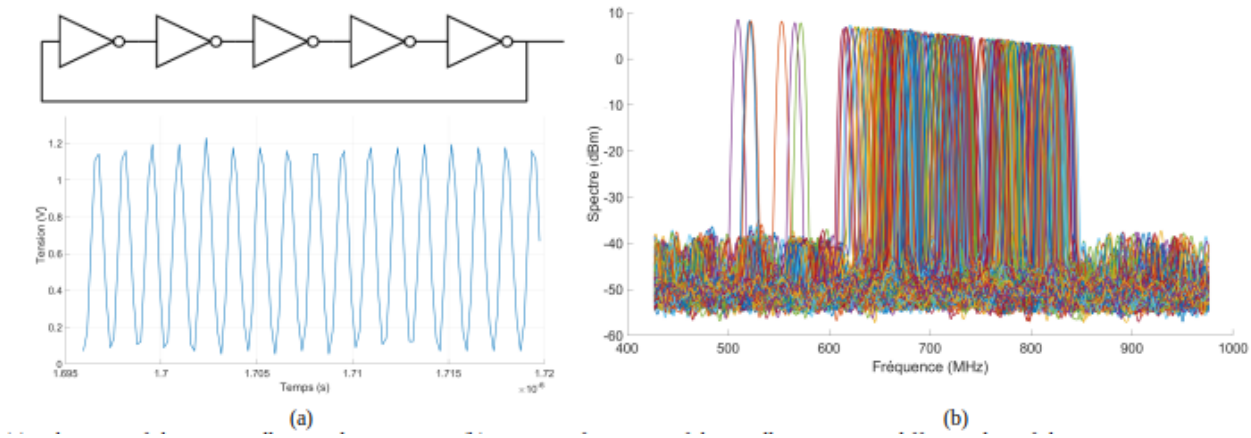


Figure 3: (a) Schematic of the ring oscillator and its response (b) Resonant frequency of the oscillator route on different slice of the FPGA. We can see the strong sensitivity of these oscillators.

The objective of this project is to exploit the sensitivity of RO to detect a hardware attack on an FPGA during an OOK communication. The device will be able to generate a threat level in real time during the communication. The attacks can be a modulation of the supply voltage or a RF pulse on the chip. The first step will be to implement several identical oscillators in the FPGA and to measure the frequency dispersion we obtain. The second step will be to develop a system to measure the frequency of the oscillators at the reception of the communication. This system will have to be done at the logic level and can be imagined with counters. The last step will be to measure the sensitivity of the RO to attacks and to detect these attacks in real time.

8.2 Project deliverables

- Design, implement and evaluation of multiple ring oscillators on the provide FPGA board.
- Design and implementation of a circuit to measure the frequency of RO.
- Evaluation of the sensitivity of RO to hardware attacks such as power supply modulation or EM pulse.

References

[0] *"Development of an RF link using FGPA with associated security tools – SeWiCom", LCIS Internship manuscript, 2022.* https://filesender.renater.fr/?s=download&token=cd030dd1-f5cb-43f1-8b36-3e741f9875ce.

9 RTdetect: Real-time object detection with passive millimeter wave imaging system

Contact details raymundo.de-amorim-junior, etienne.perret, romain.siragusa, nicolas.barbot@lcis.grenoble-inp.fr

Project keywords Real-Time Imaging, mm-Wave radar imaging, Synthetic Aperture

Skills C/C++ programming, RF communication

9.1 Project context and goals

Millimeter-wave (mmW) imaging is widely used for personnel security (e.g. screening at airports, checkpoints), medical diagnostic image (e.g. cancer diagnosis, vital signs monitoring), military area (e.g. surveillance, reconnaissance), automotive industry (e.g. car and pedestrian monitoring) and other fields [0]. Electromagnetic imaging enables the construction of images by the radiated- or scattered-field estimation of a target. In particular, mm-wave imaging provides a fair trade-off between penetration capabilities and resolution, for non-destructive evaluation. Then, mmW radars enable the higher capability to distinguish different targets (resolution), when compared to lower frequency-based devices. Consequently, this technology undergoes an expansion in the last years and became competitive in terms of cost. However, a common problem with mmW imaging is the characterization of the 3D zone, in which the object interacts with the reader. The most of time no interaction between the reader and the object is traduced by that not collaborating to the image formation.

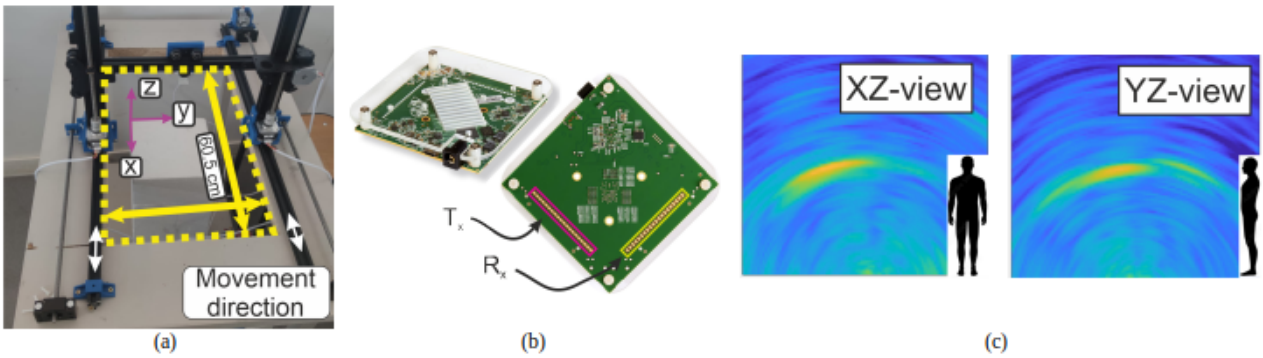


Figure 4: (a) 3D displacement table (b) mmW reader (bandwidth 62 GHz to 69 GHz) and (c) scatter field of a human body at 1m for mmW reader.

The first objective of the project is to develop a Graphic User Interface (GUI) to control a 3D displacement table and a mmW radar [0]. Then the 3D zone in which the radar is able to interact will be characterize. Finally, one and two dimensional (2D) effective apertures for resonant (chipless tags) and non-resonant (metal plate) objects will be done to validate the measurement bench. An imaging application considering a human body near to the reader can be downloaded at [0].

9.2 Project deliverables

- Development of a Python/MATLAB interface (GUI) for reader-3D table control.
- Characterization of a 3D zone considering different objects.
- Imaging formation considering its trade-offs.

References

[0] *Drive:* https://drive.google.com/file/d/1-LXQEvoNKCoWvuVOOpxefhWUx8Sw8gnf/view?usp=sharing.

[0] *VTRIG-74*. https://www.minicircuits.com/pdfs/VTRIG-74.pdf.

[0] M. E. Yanik and M. Torlak. "Near-field MIMO-SAR millimeter-wave imaging with sparsely sampled aperture data". *Ieee Access* 7 (2019), pp. 31801–31819.

10 QuadControl: Experimental validation of a nonlinear controller for a quadcopter

Contact details	**huu-thinh.do,ionela.prodan@lcis.grenoble-inp.fr**
Project keywords	**UAV, Feedback linearization, Trajectory tracking**
Skills	**Robotics, Matlab/Simulink and Python, Modeling, Control theory**

10.1 Project context and goals

For UAVs (Unmanned Aerial Vehicles), with their undeniable beneficial applications, various complex nonlinear control designs have been introduced. The quadcopter drone is well-known to be classified as a differentially flat system [0], which provides us an input transformation law to exactly linearize the system in closed-up online [0]. With this advantage, it is possible to control the nonlinear system with the basis of linear control theory (full-state feedback, loop-shaping, etc.) instead of dealing with the original nonlinear model [0].

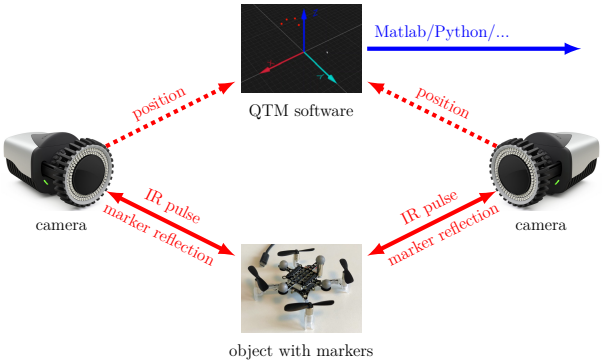
This project aims to experimentally validate a nonlinear controller for trajectory tracking and obstacle avoidance missions. With such motivation and taking advantage of the motion capture systems (Lighthouse from Bitcraze and Qualisys) available at the Esisarium platform of Esisar and LCIS, the project proposes the following missions and goals:

- First, with the mathematical model, linearization control law will be designed and tested via simulation.
- Second, with the controller achieved, validation on Crazyflie platform will be carried out using the Qualisys motion capture system.
- Then comparison between the simulation and experimental result will be constructed in order to analyze the performance and robustness of the controller.
- Finally, analysis for the advantages as well as its drawbacks will be provided to conclude the study.

10.2 Project deliverables

- Understand the Crazyflie platform;
- Python implementation with Bitcraze Crazyflie interface in Ubuntu.
- Simulation scripts of the designed controllers, done with Matlab/Simulink and Python;
- Technical report with simulations and experimental results.

Note that an internship (PFE) within the LCIS lab is available on a related topic during February-July 2023.



References

[0] H.-T. Do, I. Prodan, and F. Stoican. "Analysis of alternative flat representations of a UAV for trajectory generation and tracking". *2021 25th International Conference on System Theory, Control and Computing (ICSTCC)*. IEEE. 2021, pp. 58–63.

[0] M. Fliess, J. Lévine, P. Martin, and P. Rouchon. "Flatness and defect of non-linear systems: introductory theory and examples". *International journal of control* 61.6 (1995), pp. 1327–1361.

11 MultiDrones: Coordination of multiple drones using Qualisys Track Manager

Contact details	vincent.marguet@lcis.grenoble-inp.fr, ionela.prodan@lcis.grenoble-inp.fr
Project keywords	UAV, Coordination, Trajectory planning, Collision avoidance, Communication
Skills	Programming, Matlab, Python, Qualisys Track Manager (QTM), Control theory, networks

11.1 Project context and goals

Unmanned Aerial Vehicles (UAVs) are nowadays used in many areas: health, search and rescue, precision agriculture. To properly manage a UAVs team, equipped with multiple sensors and actuators, it is necessary to test these technologies and design reliable coordination strategies able to efficiently manage the team [0, 0]. Several constraints need to be considered depending on the scenario: keeping a certain distance among the UAVs representing the communication range, avoid collision with static and moving obstacles, pass throw some particular waypoints in order to achieve a mission, land with enough battery remaining.

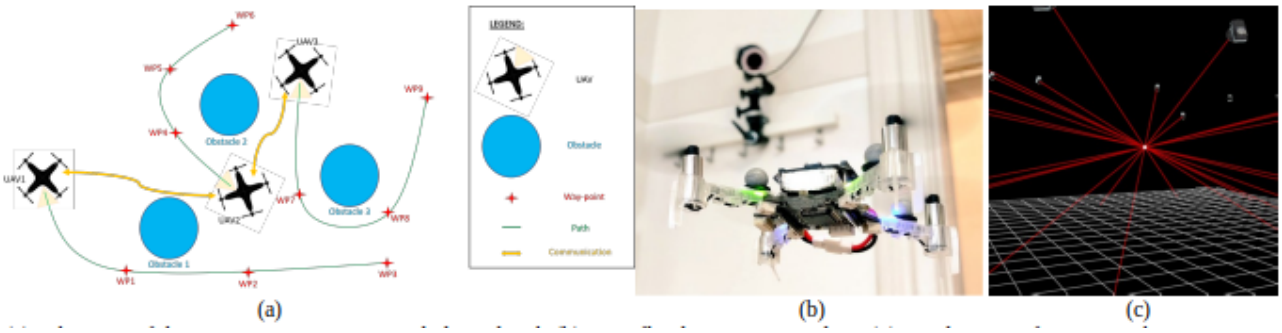


Figure 5: (a) Schematic of the UAV communication and planned path (b) Crazyflie drone using Qualisys (c) Localization of a UAV with QTM

11.2 Project deliverables

- Understand the Crazyflie platform and its various positioning systems.
- Simulation scripts of the designed controllers, done with Matlab/Python for multiple drones flying simultaneously.
- Python implementation of sense and avoidance strategies for collision avoidance.
- Technical report with simulations and experimental results.

Note that an internship (PFE) within the LCIS lab is available on a related topic during February-July 2023.

References

[0] V. Marguet, B. Gheorghe, I. Prodan, and F. Stoican. "Reliable motion planning and coordination for a team of aerial drones". *Journée des doctorants 2022*. 2022.

[0] 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.

12 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

12.1 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 [0].

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

12.2 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 micro-controller 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

[0] 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.

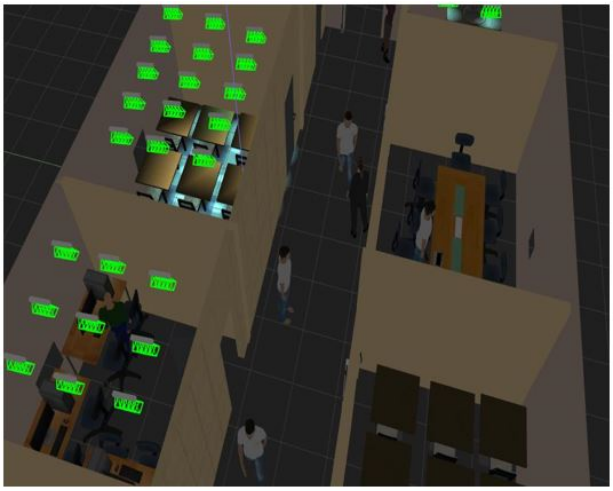
13 EMSBuild: Routing energy system for smart buildings

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

Project keywords Smart Building, ROS, Gazebo
Skills Embedded programming, Linux tools

13.1 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 (<5,000 sqft) or medium-sized (5,000-50,000 sqft). 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.

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), we use Power over Ethernet (PoE) which is a technology that passes electric power over twisted-pair Ethernet cable to power the loads.

A routing energy algorithm will be studied in order to supply power only to critical loads in case of Grid problem or in an autonomous functionning mode of the smart building. The algorithm will be implimented on a Raspberry PI which controls a PoE switch (Evaluation Board by Texas Instruments based on the Power Source Equipement (PSE) : TPS23881).

13.2 Project deliverables

- Development of an API for a linux embedded system to control the PSE.
- Energy routing algorithm..
- Documentations.

References

[0] *ROS official website*. https://www.ros.org/.

[0] 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.

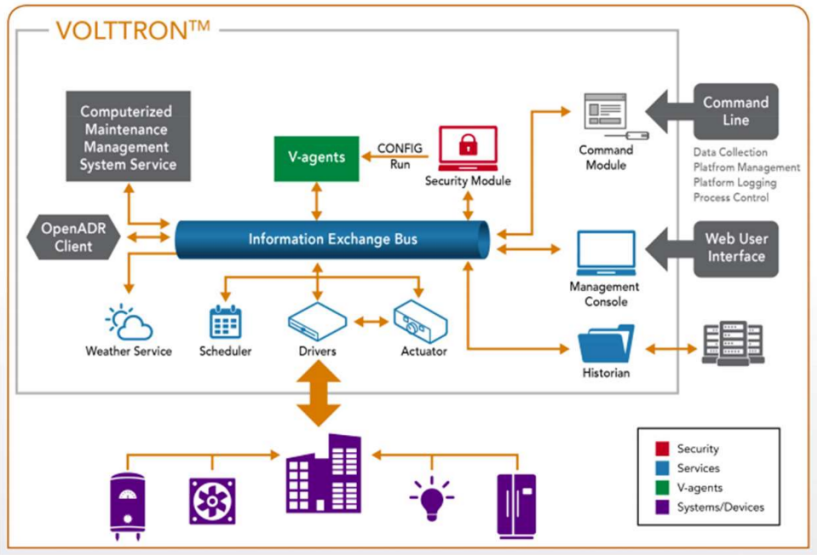
14 SmartBuildV: Smart building management platform based on VOLTTRON™ (Eclipse Foundation)

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

14.1 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™ is an open source distributed control and sensing software platform [0]. 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 [0]... and interface this platform with Gazebo interface for simulations purposes (cooperation with the other group project working on Gazebo is possible).



14.2 Project deliverables

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

References

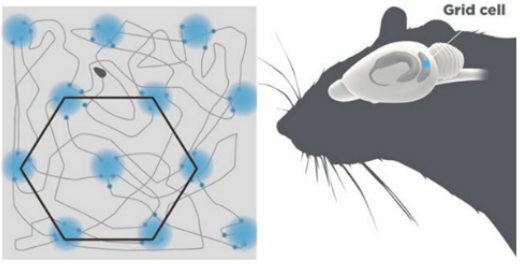
[0] *MQTT*. https://mqtt.org/.

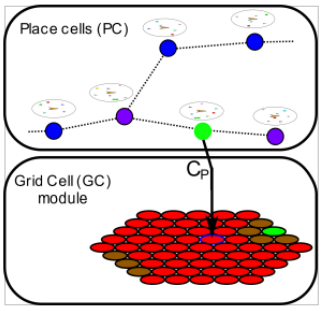
[0] *VOLTTRON*. https://volttron.org/.

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

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

15.1 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.

15.2 Project deliverables

- Defining a state of the art of visual cue extraction and detection methods (e.g. ORB, pattern matching...)
- Development of a visual system to recognize a place
- Integration of the place recognition system in the navigation model
- Implementation of the navigation model on a robotic platform and development of control models for exploration and navigation exploiting the bio-inspired navigation model.

References

[0] 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.

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

[0] 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.

16 CSAW'22: Embedded Security Challenge

Contact details mickael.seignobos@esisar.grenoble-inp.fr, vincent.beroulle@esisar.grenoble-inp.fr

Project keywords Hardware Security, Embedded Systems
Skills Embedded programming, Communicating system, Security

16.1 Project context and goals

This project aims to participate in the CSAW's Embedded Security Challenge. CSAW is the world's largest student-run cyber security event, featuring international competitions, workshops, and industry events. Competitors must exploit the weaknesses of a target system, assess the effectiveness of their hardware security techniques, identify vulnerabilities and implement effective defense mechanisms.

The Embedded Security Challenge (ESC) is an educational, research-oriented tournament aimed at hacking into the hardware of embedded systems. First, run in 2008, it is the oldest hardware security competition in the world. 2022 represents ESC's 15-year anniversary.

Past ESC competitions have focused on the security of radio frequency identification (RFID) readers, data exfiltration attacks against IoT devices, and in 2020, hacking the firmware of a wifi access point running on a RISC-V IoT platform using open-source reverse engineering tools.

Details on this year's competition will be announced on its official page at https://www.csaw.io/esc

The current competition timeline is:

- 22 August 2022: Qualification Round Start
- 9 September 2022: Registration Deadline
- 21 September 2022: Qualification Report Submission Deadline
- TBD: Finalists Notification
- TBD: First Challenge Set Released
- TBD: Final Challenge Deliverables Deadline
- 9-11 November 2022: In-Person Demos & Presentations

This project can be opened for 2 teams.

16.2 Project deliverables

- Qualify a team at the event by writing a 4 pages report [0]
- Participate to the challenge
- Win the challenge...

References

[0] *CSAW 2022*. https://github.com/TrustworthyComputing/csaw_esc_2022.

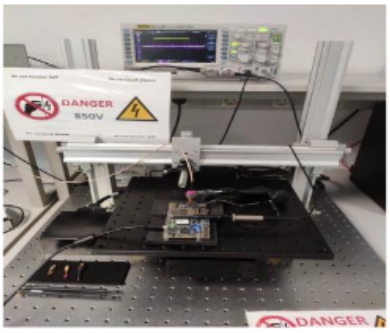
17 EMFI: ElectroMagnetic Fault Injection for attacking 32-bit microcontrollers

Contact details ihab.alshaer@lcis.grenoble-inp.fr, vincent.beroulle@esisar.grenoble-inp.fr, christophe.deleuze@lcis.grenoble-inp.fr

Project keywords Electromagnetic Fault Injection, ChipWhisperer

Skills embedded programming, hardware security, Electromagnetic fault injection, ChipWhisperer, microcontroller, scripting

17.1 Project context and goals



In the context of hardware security, fault injection can be defined as a powerful physical attack, possibly non-invasive, where the attacker has physical access to the device or its surrounding environment. The attacker will try to change the normal behavior of the device during program execution by injecting one or more faults, then observing the erroneous behavior [0]. The injection process can be done in different ways: exposing the device to radiations, laser beams, intense light, or an electromagnetic (EM) pulse, inducing variations in the power supply or in the clock signal, changing the environmental conditions such as the temperature, etc [0]. Fault injection has proved its ability in breaking real systems and applications. For example: XBOX 360 [0], PlayStation 3 [0], embedded cryptographic keys [0], etc.

The proposed project aims to perform fault injection campaigns on ChipWhisperer target boards, that embed ARM Cortex-M processors. This project is under the CLAM project, which is a collaboration project between three labs: LCIS, TIMA, and VERIMAG. CLAM aims at performing fault injection attacks using different physical techniques and conducting fault simulations at different levels of a digital system, in order to provide realistic fault models by analyzing and comparing the results of the injections and the simulations. These fault models are necessary to build and design efficient countermeasures against fault attacks.

17.2 Project deliverables

- Dealing with ChipWhisperer environment
- Perform a successful EM fault injection attack on 32-bit MCU ChipWhisperer targets
- Full automation of the injection process: delay, pulse amplitude, probe position, results monitoring

References

[0] *F. Project, "The xbox 360 reset glitch hack,":* https://free60project.github.io/wiki/ResetGlitchHack.html.

[0] *N. Lawson, "How the ps3 hypervisor was hacked,"* https://rdist.root.org/2010/01/27/how-the-ps3-hypervisor-was-hacked/.

[0] *Y. Lu, "Attacking hardware AES with DFA,"* https://yifan.lu/images/2019/02/AttackingHardwareAESwith pdf.

[0] I. Alshaer, B. Colombier, C. Deleuze, V. Beroulle, and P. Maistri. "Microarchitecture-aware Fault Models: Experimental Evidence and Cross-Layer Inference Methodology". *2021 16th International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS)*. IEEE. 2021, pp. 1–6.

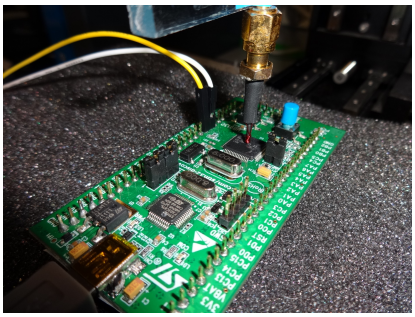
[0] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache. "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures". *Proceedings of the IEEE* 100.11 (2012), pp. 3056–3076.

18 AttackC: Electromagnetic Fault Injection Attacks on Cryptographic Algorithms

Contact details amir-pasha.mirbaha@esisar.grenoble-inp.fr, vincent.beroulle@esisar.grenoble-inp.fr

Project keywords Hardware Security, Fault Injection Attacks, Cryptography
Skills Embedded Programming, Python, MATLAB, Cryptanalysis

18.1 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) [0]; because it can be induced without chip decapsulation, even on the most performant recent SoCs [0].

As a consequence, it is possible to inject faults into the encryption process inside an unsecured microcontroller. For instance, an Advanced Encryption Standard (AES) [0] implementation as a symmetric cryptography algorithm can be targeted [0]. In this case, it may be possible to extract the secret key or other sensitive information by differential methods and basic cryptanalysis skills [0]. 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 by using existing basic control codes in Python and MATLAB
- Programming an AES in target microcontrollers
- Fabrication and 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

18.2 Project deliverables

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

References

[0] 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 (2020), pp. 680–693.

[0] 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*. IEEE. 2012, pp. 7–15.

[0] P. Maurine. "Techniques for EM fault injection: equipments and experimental results". *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*. IEEE. 2012, pp. 3–4.

[0] M. J. Dworkin, E. B. Barker, J. R. Nechvatal, J. Foti, L. E. Bassham, E. Roback, J. F. Dray Jr, et al. "Advanced encryption standard (AES)" (2001).

[0] E. Biham and A. Shamir. "Differential fault analysis of secret key cryptosystems". *Annual international cryptology conference*. Springer. 1997, pp. 513–525.

19 POSS: Power-Off Attack on Security Sensors

Contact details vincent.beroulle@esisar.grenoble-inp.fr, amir-pasha.mirbaha@esisar.grenoble-inp.fr

Project keywords cybersecurity, vulnerability analysis, fault attack, FPGA prototype, circuit self-test

Skills embedded programming, hardware security, FPGA prototyping, digital circuit design and simulation, physical fault injection

19.1 Project context and goals

Embedded systems, because they contain confidential information, are subject to fraudulent manipulation, commonly called attacks, by malicious people. Among several means of hardware attacks, one of the most effective is Laser Fault Injection. However, sensitive circuits, like chip bank cards, are equipped with security sensors (e.g., photodetectors) to bring out any circuit package's tampering. Besides, these countermeasures functioning is limited to the Power-On state of the circuit. Embedded security sensors [0, 0, 0], must be powered on to operate. Therefore, while the circuit is not powered, the sensors are also unpowered, and there is no supervision of fraudulent manipulations. Thus, the sensors can be targeted and deactivated by an attacker.

The Power-Off Attacks (POA) could disable various on-chip security sensors such as voltage, clock glitch, or laser pulse detectors while the circuit is unpowered. Hence, the possible existence of POA carried out against an unpowered circuit is an issue for the embedded systems' security and can still be undetectable after repowering the circuit.

The POSS innovation project aims at designing self-test capabilities for security sensors to address the new threats posed by the laser fault injection attacks when the target device is powered off. The goal of the project is thus to develop a systematic framework to test several security sensors online to guarantee their integrity in mission mode, making sure a POA has not disabled them. Thanks to the knowledge of the POA effects, it will be possible to identify what are the sensor properties that can be altered by the POA, and the online test should check that. The tests could be extended to the digital part processing the sensor test results. Finally, the best solutions to protect systems against POA will be evaluated using FPGA prototyping.

19.2 Project deliverables

- Select and simulate digital security sensors (from a selection of digital sensors)
- Fault modeling and sensor simulation in the presence of fault injection
- Online self-test design to test sensors and associated digital parts
- Prototyping and validation on FPGA (using physical fault injection mechanisms)

References

[0] C. Deshpande, B. Yuce, N. F. Ghalaty, D. Ganta, P. Schaumont, and L. Nazhandali. "A configurable and lightweight timing monitor for fault attack detection". *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE. 2016, pp. 461–466.

[0] W. He, J. Breier, S. Bhasin, N. Miura, and M. Nagata. "Ring oscillator under laser: potential of pll-based countermeasure against laser fault injection". *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE. 2016, pp. 102–113.

[0] L. Zussa, A. Dehbaoui, K. Tobich, J.-M. Dutertre, P. Maurine, L. Guillaume-Sage, J. Clediere, and A. Tria. "Efficiency of a glitch detector against electromagnetic fault injection". *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE. 2014, pp. 1–6.

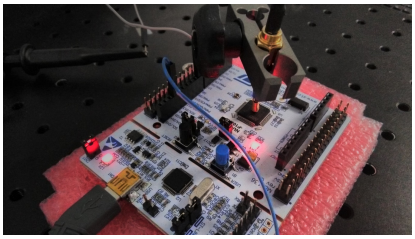
20 TrigS4FI: Smart Triggering for Electromagnetic Fault Injection Attacks

Contact details amir-pasha.mirbaha@esisar.grenoble-inp.fr, vincent.beroulle@esisar.grenoble-inp.fr

Project keywords Hardware Security, Electromagnetic Fault Injection, Synchronization, Smart Triggering

Skills embedded programming, Python or MATLAB scripting, signal processing

20.1 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 [0]. Fault Injection (FI) is an effective hardware attack that can be performed by injecting Electromagnetic [0]/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. It's an open-source and low-cost material for this aim. It allows to receive and transmit 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., a ST-Nucleo Board). Then, improving the attack's synchronization by using a HackRF One board [0].

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 IoT purpose microcontrollers by an existing code (AES-128) and, if necessary, with some modifications to have an appropriate Trigger Signal
- Realization of EM fault injection on the microcontrollers
- Improving the attack's synchronization by using a HackRF One board

20.2 Project deliverables

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

References

[0] 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.

[0] 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)*. IEEE. 2018, pp. 87–92.

[0] P. Maurine. "Techniques for EM fault injection: equipments and experimental results". *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*. IEEE. 2012, pp. 3–4.