Kudelski Group

INTERNSHIPS 2026

TABLE OF CONTENTS

© 2025 Nagravision Sàrl / All Rights Reserved

HOW TO APPLY

- Open positions are advertised on our website careers.nagra.com
- All applications must be done through our careers page
    - Trainee – Ref 15582
    - Mention the internship number(s) in motivation letter e.g. [AST-AR-01]

[AST-AR-01] **Anti jamming adaptative system**

Topics: **RADIO – SDR – AI** Master Thesis Possible: **YES**

Development of an intelligent, software-defined radio (SDR)-based system capable of detecting and mitigating jamming attacks by dynamically adapting its operating frequencies and communication parameters.

Details

This project aims to enhance the resilience of wireless communication systems against intentional interference (jamming). Leveraging SDR platforms, the system will continuously monitor the radio spectrum, identify jamming patterns, and autonomously switch to cleaner frequencies or modulation schemes to maintain reliable communication.

Key Objectives

- Design and implement a real-time spectrum sensing module.
- Develop adaptive algorithms for frequency hopping and modulation switching.
- Ensure compatibility with existing communication protocols and hardware.
- Validate system performance in simulated and real-world environments.
- Optionally, integrate machine learning techniques to predict and respond to jamming strategies.

Technical Stack:

- Hardware: SDR platforms (e.g., USRP, HackRF, LimeSDR)
- Software: GNU Radio, Python, C++, MATLAB (for prototyping)
- Algorithms: Signal classification, anomaly detection, reinforcement learning
- Protocols: Custom and standard wireless protocols (e.g., IEEE 802.15.4, LoRa, etc.)

Expected Outcomes:

- A robust prototype capable of maintaining communication under various jamming scenarios.

Team & Collaboration:

- Onboarded within the Advanced Research team, collaborating with cybersecurity, RF, and AI specialists.
- Potential for cross-functional integration with other secure communication initiatives.

[AST-AR-02] **Jamming Adaptive System**

Topics: **RADIO – SDR – AI** Master Thesis Possible: **YES**

Design and implementation of a flexible, software-defined radio (SDR)-based system capable of simulating adaptive jamming attacks against wireless communication protocols, to support research in countermeasure development and resilience testing.

Details

This internship focuses on building a modular and intelligent jamming platform that can dynamically adapt its interference strategies based on the target system's behavior. The goal is to simulate realistic and evolving jamming scenarios to test the robustness of anti-jamming mechanisms and improve the security of wireless communication systems.

Key Objectives

- Develop a real-time spectrum monitoring and analysis module to identify active communication channels.
- Implement various jamming techniques (e.g., barrage, sweep, reactive, deceptive).
- Integrate adaptive logic to modify jamming parameters based on observed countermeasures.
- Create a control interface to configure attack profiles and monitor effectiveness.
- Evaluate the impact of jamming on different protocols and environments.
- Optionally, integrate machine learning techniques to predict jamming parameters based on observed countermeasures.

Technical Stack:

- Hardware: SDR platforms (e.g., USRP, HackRF, BladeRF)
- Software: GNU Radio, Python, C++
- Algorithms: Signal detection, adaptive control, protocol analysis
- Protocols: Custom and standard wireless protocols (e.g., IEEE 802.15.4, LoRa, etc.)

Expected Outcomes:

- A working prototype capable of executing adaptive jamming attacks.
- Insights and recommendations for improving anti-jamming systems.

Team & Collaboration:

- Onboarded within the Advanced Research team, collaborating with cybersecurity, RF, and AI specialists.
- Insights and recommendations for improving anti-jamming systems.

© 2025 Nagravision Sàrl / All Rights Reserved

[AST-AR-03] **Quantum hardware Evaluation**

Topics: **Quantum security – Side Channel- Fault Attacks** Master Thesis Possible: **YES**

This subject aims to provide a state of the art of the performance, scalability and security robustness of various quantum hardware platforms, such as superconducting qubits, trapped ions, and photonic systems, in executing quantum algorithms.

Details

The study will consider the standard quantum algorithms like Grover's search, Shor's factoring, and quantum machine learning algorithms. The evaluation will focus on metrics such as gate fidelity, coherence time, error rates, and scalability. The feasibility of performing side channel and fault attacks on such kind of technology will also be investigated.

Key Objectives

- Survey the State of the Art
  - Review current quantum hardware technologies and their architectural characteristics.
  - Analyze standard quantum algorithms
- Performance Evaluation
  - Compare platforms based on metrics like:
    - Gate fidelity, Coherence time, Error rates, Scalability
  - Use available benchmarks and simulation tools to assess algorithm execution.
- Security Analysis
  - Investigate the feasibility of side channel attacks (e.g., power analysis, timing attacks) on quantum hardware.
  - Explore fault injection techniques and their impact on quantum computation.
  - Propose potential countermeasures or mitigation strategies.
- Experimental or Simulated Validation
  - Depending on access, perform hands-on experiments or simulations using platforms like IBM Qiskit, Amazon Bracket, IonQ, or photonic simulators.

Technical Stack:

- Hardware: Quantum Hardware Access (Qiskit (IBM), Cirq (Google), PennyLane, QuTiP)
- Software: Python, C,C++, MATLAB
- Algorithms: Grover's Search, Shor's Factoring, Quantum, Quantum Key Distribution

Expected Outcomes:

- A detailed comparative report on quantum hardware performance and scalability.
- A security assessment highlighting potential vulnerabilities to side channel and fault attacks.

© 2025 Nagravision Sàrl / All Rights Reserved

- Recommendations for secure quantum hardware design and future research directions.

Team & Collaboration:

- Onboarded within the Advanced Research team, collaborating with cybersecurity, Lab attacks specialists.
- Potential for cross-functional integration with other secure communication initiatives.

© 2025 Nagravision Sàrl / All Rights Reserved

[AST-AR-04] **Side Channel and Fault Attack Investigations on Hamming Quasi-Cyclic (HQC) Post-Quantum Cryptography**

Topics: **Quantum security – Side Channel- Fault Attacks** Master Thesis Possible: **YES**

This subject aims to evaluate the physical security of HQC implementations against side channel attacks (SCA) and fault injection attacks (FIA). The goal is to identify potential vulnerabilities in embedded or hardware-based deployments and propose effective countermeasures.

Details

HQC is a code-based post-quantum cryptographic scheme relying on the hardness of decoding problems in Hamming metric and quasi-cyclic codes. While mathematically secure against quantum adversaries, its real-world implementations may leak sensitive information through physical channels or be disrupted by induced faults. Side channel and fault attacks have proven effective against many key encapsulation cryptographic schemes, including other post-quantum candidates like ML-KEM and BIKE. This thesis will explore how HQC stands up to such threats and how to harden its implementations.

Key Objectives

- Identify what are the main side channel leakage vectors in HQC implementations
- Identify how vulnerable is HQC to fault injection attacks
- Define which countermeasures can be applied to protect HQC implementations
- Compare HQC to other PQ schemes in terms of physical security and its securitisation.

Technical Stack:

- HQC Reference Implementation (e.g., PQClean)
- Python / C for simulation and scripting
- ChipWhisperer (optional) for SCA and FIA
- Python libraries: NumPy, SciPy, Matplotlib

Expected Outcomes:

- A security assessment of HQC implementations under physical attack scenarios
- Simulated or experimental attack results
- Comparative analysis with other PQC schemes
- Recommendations for secure HQC deployment.

Team & Collaboration:

- Onboarded within the Advanced Research team, collaborating with cybersecurity, Lab attacks specialists.
- Potential for cross-functional integration with other secure communication initiatives.

[AST-AR-05] **Quantum Programming Exploration**

Topics: **Quantum – Implementation** Master Thesis Possible: **Possible**

This subject aims to explore the principles, tools, and techniques of quantum programming. The goal is to understand how quantum algorithms are implemented on various platforms, evaluate their performance, and identify best practices for developing quantum software.

Details

Quantum programming is a rapidly evolving field that enables the development of algorithms for quantum computers. Unlike classical programming, quantum programming involves manipulating qubits and quantum gates, often using specialized frameworks such as Qiskit, Cirq, and PennyLane. As quantum hardware becomes more accessible, understanding how to effectively program quantum systems is essential for researchers and developers

Key Objectives

- Identify what are the key differences between classical and quantum programming paradigms
- Provide an overview of how the various quantum programming frameworks compare in terms of usability and performance
- Identify what are the challenges in implementing quantum algorithms on real quantum hardware

Technical Stack:

- Qiskit (IBM Quantum), Cirq (Google), PennyLane (Xanadu) …
- QuTiP for simulation
- Python libraries: NumPy, Matplotlib

Expected Outcomes:

- Comprehensive understanding of quantum programming tools
- Performance comparison of quantum frameworks
- Implementation of key quantum algorithms
- Recommendations for best practices in quantum software development

Team & Collaboration:

- Onboarded within the Advanced Research team, collaborating with cybersecurity, Lab attacks specialists.
- Potential for cross-functional integration with other secure communication initiatives.

© 2025 Nagravision Sàrl / All Rights Reserved

[AST-AR-06] **Quantum Key Distribution**

Topics: **Quantum security – Secure communication** Master Thesis Possible: **YES**

This subject aims to explore the principles, protocols, and practical implementations of Quantum Key Distribution (QKD). The goal is to understand how quantum mechanics enables secure key exchange, evaluate the performance and security of existing QKD protocols, and investigate their integration into classical communication systems.

Details

Quantum Key Distribution is a cryptographic technique that uses quantum mechanics to securely distribute encryption keys between parties. Unlike classical key exchange methods, QKD is theoretically immune to computational attacks due to the laws of quantum physics, such as the no-cloning theorem and measurement disturbance. Protocols like BB84 and E91 have demonstrated secure key exchange, and real-world implementations are emerging in fiber-optic and satellite-based systems. However, it is important to understand that to authentication of parties is not addressed by such technique.

Key Objectives

- Identify what are the fundamental principles that make QKD secure
- Compare the different QKD protocols (e.g., BB84, E91, B92) in terms of security and efficiency
- Define what are the practical challenges in implementing QKD over long distances and ensure secure communication
- Explore how can QKD be integrated with classical cryptographic systems and if they can be complementary

Technical Stack:

- Python for simulation
- QKD simulation libraries (e.g., SimulaQron, Qiskit QKD modules)

Expected Outcomes:

- Detailed understanding of QKD principles and protocols
- Simulated performance data for the different protocols
- Comparative analysis of QKD protocols
- Recommendations for integrating QKD into classical systems and secure communication protocols

Team & Collaboration:

- Onboarded within the Advanced Research team, collaborating with cybersecurity, Lab attacks specialists.
- Potential for cross-functional integration with other secure communication initiatives.

[AST-AR-07] **High-Speed IPv6 Internet Scanner**

Topics: **Network security – AI – Distributed Systems** Master Thesis Possible: **YES**

Develop a high-performance IPv6 active space scanner capable of discovering and analysing reachable IPv6 hosts across the global internet.

Details

This project aims to develop a high-performance IPv6 active space scanner capable of discovering and analysing reachable IPv6 hosts across the global internet. Given the vastness of the IPv6 address space, the scanner will leverage intelligent heuristics, distributed computing, and machine learning to optimize scanning efficiency and coverage.

Key Objectives

- Analyse current IPv6 usage patterns and address allocation strategies (BGP, RIR data).
- Design and implement a scalable IPv6 scanning engine.
- Explore distributed scanning techniques using cloud infrastructure.
- Integrate machine learning models to prioritize likely active address ranges.
- Validate scanning performance and accuracy across diverse network environments.

Technical Stack:

- Languages: Python, Rust, C++
- Infrastructure: Linux, Docker, distributed cloud platforms (e.g., AWS, GCP)
- AI: Heuristic modelling, supervised learning, anomaly detection
- Protocols: IPv6, ICMPv6, TCP/UDP scanning

Expected Outcomes:

- A prototype IPv6 scanner capable of scanning large portions of the IPv6 space efficiently.
- Insights into IPv6 activity distribution and scanning optimization strategies.

Team & Collaboration:

- Onboarded within the Advanced Research team, collaborating with networking, cloud, and AI specialists.
- Potential for integration with broader internet measurement and security initiatives.

[AST-AR-08] **Distributed AI-Augmented DDoS Simulation Framework**

Topics: **Network security – AI** Master Thesis Possible: **YES**

Develop a distributed framework for simulating large-scale DDoS attacks using intelligent agents.

Details

This project aims to develop a distributed framework for simulating large-scale DDoS attacks using intelligent agents. Each agent will generate traffic based on AI-driven behavior models, enabling realistic and adaptive attack scenarios. The system will be used to benchmark and stress-test DDoS mitigation solutions in controlled environments.

Key Objectives

- Design a distributed architecture for traffic generation using containerized agents.
- Implement AI models (e.g., reinforcement learning or GANs) to simulate attacker strategies.
- Develop orchestration logic to coordinate multi-agent attacks.
- Benchmark mitigation systems under various attack profiles.
- Optionally, integrate telemetry and analytics dashboards for real-time monitoring.

Technical Stack:

- Infrastructure: Docker, Kubernetes, Linux networking
- Software: Python, Rust, Go
- AI: PyTorch, TensorFlow, RLlib
- Protocols: TCP/UDP, HTTP/2, custom packet formats

Expected Outcomes:

- A scalable and intelligent DDoS simulation platform.
- Comparative performance data of mitigation systems under realistic attack conditions.

Team & Collaboration:

- Onboarded within the IoT Advanced Research team.
- Collaboration with cybersecurity, AI, and infrastructure specialists.

[AST-AR-09] AI-Driven Adaptive Packet Generator for Security Testing

Topics: **Network security – AI** Master Thesis Possible: **YES**

Building a high-performance packet generator that uses AI to adapt traffic patterns based on feedback from the target system.

Details

This project focuses on building a high-performance packet generator that uses AI to adapt traffic patterns based on feedback from the target system. The goal is to simulate evolving attack scenarios and test the robustness of network defenses.

Key Objectives

- Develop a custom packet generation engine in Rust or C++.
- Integrate AI models to adapt traffic based on system responses.
- Compare performance and realism against existing tools (e.g., Scapy, Ostinato).
- Validate effectiveness in testing IDS/IPS and DDoS mitigation systems.

Technical Stack:

- **Languages**: Rust, C++, Python
- **AI**: Reinforcement learning, anomaly detection
- **Tools**: libpcap, DPDK, Scapy
- **Protocols**: TCP/IP stack, DNS, HTTP, custom payloads

Expected Outcomes:

- A prototype capable of ultra-fast, intelligent packet generation.
- Insights into how adaptive traffic affects security system performance.

Team & Collaboration:

- Embedded in the IoT Advanced Research team.
- Collaboration with network security and AI experts.

© 2025 Nagravision Sàrl / All Rights Reserved

[AST-AR-10] **IoT Botnet Emulation and Mitigation Benchmarking**

Topics: **Network security – AI** Master Thesis Possible: **YES**

Emulate IoT-based botnets (e.g., Mirai-like) and evaluate the effectiveness of mitigation strategies.

Details

This project aims to emulate IoT-based botnets (e.g., Mirai-like) and evaluate the effectiveness of mitigation strategies. The system will simulate compromised IoT devices generating coordinated traffic, allowing for realistic testing of defence mechanisms.

Key Objectives

- Model IoT device behaviour and attack vectors.
- Develop lightweight traffic generators mimicking IoT communication.
- Simulate botnet coordination and attack scenarios.
- Benchmark mitigation tools in constrained environments.

Technical Stack:

- **Languages**: C, Python, Rust
- **IoT Protocols**: MQTT, CoAP, UPnP
- **Infrastructure**: Docker, Linux namespaces
- **Security Tools**: IDS/IPS, honeypots

Expected Outcomes:

- A realistic IoT botnet emulation platform.
- Performance data on mitigation strategies in IoT contexts.

Team & Collaboration:

- Integrated within the IoT Advanced Research team.
- Collaboration with embedded systems and security specialists.

© 2025 Nagravision Sàrl / All Rights Reserved
Public

[AST-AR-11] **Adaptive Lightweight Crypto Protocol for Two-Way IoT Com**

Topics: **Embedded Security – IoT – Cryptography** Master Thesis Possible: **YES**

Building on a successful internship project that produced a lightweight cryptographic protocol for constrained IoT devices, this thesis aims to extend the protocol into a fully adaptive, two-way secure communication solution.

Details

The protocol will be designed to operate efficiently under varying network conditions, including low bandwidth, intermittent connectivity, and asymmetric transmission quality.

The student will focus on optimizing the protocol for **minimal power consumption**, **low memory footprint**, and **robustness against degraded link quality**, while maintaining strong security guarantees. The solution will be validated on real-world embedded platforms and benchmarked against existing lightweight cryptographic frameworks.

Key Objectives

- Analyze and evaluate the existing lightweight crypto protocol developed in the previous internship and validate as a candidate for this project.
- Design and implement a two-way adaptive extension of the protocol, which implies mutual authentication
- Ensure compatibility with constrained IoT devices and low-power wireless networks.
- Integrate mechanisms for dynamic adaptation to link quality and device capabilities.
- Validate the protocol on embedded platforms under various network conditions.
- Compare performance and security with existing lightweight crypto solutions (e.g., TinyDTLS, EDHOC).

Technical Stack:

- **Hardware**: STM32WL, Nordic nRF9160, other low-power MCUs
- **Software**: Embedded C/C++, STM32CubeIDE, nRF Connect SDK
- **Crypto Algorithms**: ECC, lightweight symmetric ciphers (e.g., ASCON, SPECK, AES-CTR), hash functions (e.g., SHA-256, BLAKE2s)
- **Protocols**: CoAP, UDP, custom secure messaging layer
- **Tools**: RF simulators, power profiling tools, packet sniffers

Expected Outcomes:

- A secure, adaptive, and lightweight two-way cryptographic protocol.
- Performance benchmarks under constrained and variable network conditions.
- A documented implementation suitable for integration into secure IoT stacks.

Team & Collaboration:

- Onboarded within the Kudelski IoT Advanced Research team.
- Collaboration with embedded security, cryptography, and RF specialists.
- Potential integration with secure provisioning and lifecycle management initiatives.

[AST-AR-12] **Federated Learning for Edge AI Systems**

Topics: **Software Development - AI** Master Thesis Possible: **YES**

Details

Join our cutting-edge research team to explore federated learning applications in edge AI environments. This internship focuses on developing and implementing distributed machine learning solutions that enable AI models to learn from decentralized data while preserving privacy and reducing network overhead.

Key Objectives

- **Literature Review & Research**
  - Study current federated learning frameworks and edge AI architectures
  - Analyze existing solutions for distributed model training
  - Identify key challenges in edge computing environments
- **System Design & Architecture**
  - Design a federated learning system optimized for edge devices
  - Define communication protocols between edge nodes and central server
  - Plan resource allocation strategies for constrained devices
- **Implementation & Development**
  - Implement federated averaging algorithms
  - Develop client-side training modules for edge devices
  - Create aggregation mechanisms for model updates
- **Optimization & Testing**
  - Optimize model compression and quantization techniques
  - Test system performance across different network conditions
  - Evaluate privacy preservation mechanisms
- **Evaluation & Documentation**
  - Benchmark against centralized learning approaches
  - Analyze communication costs and convergence rates
  - Document findings and prepare technical reports

Skills and Profile

- Currently pursuing a degree in Computer Science, AI, or related field
- Programming: Python, PyTorch/TensorFlow, distributed computing
- Machine Learning: Deep learning fundamentals, model optimization
- Edge Computing: Understanding of resource-constrained environments
- Networking: Knowledge of communication protocols and distributed systems

[AST-AR-13] **AI Model Watermarking and Integrity Verification**

Topics: **Software Development - AI** Master Thesis Possible: **YES**

Details

Join our innovative research team to develop advanced techniques for AI model watermarking and integrity verification. This internship focuses on creating robust solutions to protect intellectual property rights of machine learning models and ensure their authenticity in deployment environments, addressing critical security concerns in AI model distribution and usage.

Key Objectives

- **Literature Review & Research**
  - Study current model watermarking techniques and integrity verification methods
  - Analyze existing solutions for AI model protection and authentication
  - Identify key vulnerabilities in model distribution pipelines
- **Watermarking Algorithm Design**
  - Design robust watermarking schemes for neural networks
  - Develop embedding techniques that preserve model performance
  - Create extraction methods for watermark verification
- **Implementation & Development**
  - Implement watermark embedding algorithms for different model architectures
  - Develop integrity verification systems using cryptographic techniques
  - Create detection mechanisms for model tampering and unauthorized modifications
- **Security Analysis & Testing**
  - Evaluate robustness against model extraction and fine-tuning attacks
  - Test watermark persistence across model compression and quantization
  - Assess impact on model accuracy and inference performance
- **Evaluation & Documentation**
  - Benchmark watermarking effectiveness across various attack scenarios
  - Analyze trade-offs between security, performance, and detectability
  - Document findings and prepare technical reports on model protection strategies

Skills and profile

- Programming: Python, PyTorch/TensorFlow, cryptographic libraries
- Machine Learning: Deep learning architecture, model optimization, adversarial attacks
- Security: Cryptography fundamentals, digital watermarking, authentication protocols
- Research Skills: Strong analytical abilities, experimental design, technical writing

[AST-LABS-01] **Combining Side Channel attack and Laser attack**

Topics: **Electrical Engineering - Security - FPGA** Master Thesis Possible: **YES**

Explore the interest to combine at the same time Side channel measurements and Laser impulsions.

Details:

Today, some secure devices implement more countermeasures against side channel attacks. It becomes difficult to carry out attacks against this type of device.

In the context of our physical attack activities (attacks through side channels, fault attacks) for external or internal customers, we need to explore all the new attack possibilities, and this one is a serious candidate to improve our success rate.

The purpose of the internship is to test and measure the effects of combining side channel measurement with Laser illumination on an FPGA device. Previous publications have shown that such approach can improve information leakage.

Key Objectives:

- Select the best approach (algorithm, setup) for a combining attack based on a bibliographic review
- Test and measure on a dedicated bench the combining approach (Side Channel/Laser)
- Improve the current bench according to the results previously observed and published
- Publish if research work is successful

Technical Stack:

- Python/VHDL language
- Good knowledge on electronic bench instrumentation (Oscilloscope, Amplifiers, optical devices, FPGA…)
- Understanding Side channel/Laser domain is a plus

Expected Outcomes:

- Bringing expertise to the Lab in the field of combining attacks

Team & Collaboration:

- Onboarded within the Kudelski Security Labs

[AST-LABS-02] **Create a model of 'AI' for Side Channel attack**

Topics: **AI – MATLAB – Python – Side Channel** Master Thesis Possible: **YES**

Development of a solution capable of grouping all deep learning models to attack cryptographic devices inside channel.

Details

Today, the recent development of AI domain leads to an explosion of models and frameworks to support them (TensorFlow, Keras, Pytorch, Matlab), all accompanied by an exponential growth in the number of hyperparameters.

In the context of our physical attack activities (attacks through side channels, fault attacks), it becomes impossible to select the best solution and find adequate parameters.

The purpose of the internship is divided into two tasks. The first one is to develop a unique and global entry point (likely under Matlab) for all the frameworks/models. The second task is to find a method that can find the right models and corresponding hyperparameters suited to our attacks.

Key Objectives

- Develop a single global point access for Deep ML Tool/Template for attacks
- Advance in the development of a method to find the best model/hyperparameters suitable for our side channel attacks.
- Test and Validate efficiency on concrete attacks dataset
- Provide a clear documentation support for the use of tools

Technical Stack:

- Python/Matlab
- Good understanding of deep learning algorithms (CNN, Transformer...)
- Good knowledge of popular Deep Machine Learning frameworks (TensorFlow, Pythorch, Keras)
- Good mastery of software environment (Linux,Windows,WSL,JupyterHub..)
- Interest to GPU hardware
- Understanding Side channel domain is a plus

Expected Outcomes:

- A robust and easy to implement solution for our daily attack work

Team & Collaboration:

- Onboarded within the Kudelski security Lab
- Potential extension for other domains of application.

© 2025 Nagravision Sàrl / All Rights Reserved
Public

[AST-LABS-03] **Trusted Execution Environment Penetration Testing**

Topics: **Reverse Engineering – IoT – Hacking** Master Thesis Possible: **YES**

Development of methodologies for analysing, reverse-engineering, and penetration testing Trusted Execution Environments (TEE) and TEE-based applications on Android and other IoT platforms. Collaboration with EPFL HexHive lab.

Details

This project aims to explore the security properties of TEE platforms (e.g., ARM TrustZone) and applications leveraging secure enclaves. The work will involve reverse engineering TEE components, identify potential vulnerabilities, and develop penetration testing techniques to assess their robustness.

Key Objectives

- Study the architecture and security guarantees of common TEEs (TrustZone, OP-TEE, GlobalPlatform TEE APIs, etc.).
- Perform reverse engineering of TEE firmware, drivers, and TEE-based applications.
- Develop penetration testing methodologies tailored for TEEs and secure apps.
- Evaluate known attack vectors (privilege escalation, side-channel, API misuse) and discover new ones.
- Provide recommendations for securing TEE-based applications in real-world deployments.

Technical Stack:

- Hardware: ARM-based development boards, Android devices, IoT platforms
- Software/Tools: Android reverse engineering (Frida, Ghidra, IDA), fuzzing frameworks, QEMU/ARM emulation, OP-TEE
- Programming Languages: C, C++, Python, Assembly (ARM)
- Protocols & APIs: GlobalPlatform TEE APIs, secure storage, key management

Expected Outcomes:

- Deep understanding of TEE attack surface and threat models.
- Prototypes of analysis/penetration testing tools targeting TEEs.
- Identification of vulnerabilities and proposed mitigations.

Team & Collaboration:

- Onboarded within the Security Labs team, collaborating with experts in embedded security, reverse engineering, and system hardening.
- Supervision and collaboration with EPFL HexHive laboratory

[IOT-COE-01] **AI Workflow & Integration – RecovR Assistant**

Topics: **Software Development - AI** Master Thesis Possible: **NO**

Help bring the RecovR Assistant, a Retrieval-Augmented Generation (RAG) based chat agent, to production readiness. This assistant is designed to support dealership staff, vendors, and internal users by providing intelligent, contextual access to operational documentation, troubleshooting procedures, and product guidance.

Details

The intern will contribute to the industrialization and integration of the RecovR Assistant into live customer support workflows powered by Intercom. This role sits at the intersection of AI, software engineering, and customer operations, offering hands-on experience in deploying intelligent systems in production environments.

Key Objectives

- PoC Industrialization for Cloud & DevOpsRefactor and modularize existing PoC components (ingestion, retrieval, UI/UX).
    - Optimize for cloud-native deployment with CI/CD, monitoring, and scalability.
    - Collaborate with DevOps to ensure secure and maintainable architecture.
- Workflow Analysis & Design
    - Analyze current support workflows and identify integration points.
    - Map escalation paths, ticketing flows, and user roles for AI augmentation.
- RAG System Enhancement
    - Improve retrieval and generation logic for domain-specific accuracy.
    - Implement role-based access control and multimodal content handling.
- Production Readiness
    - Integrate monitoring, logging, and failover mechanisms.
    - Validate performance, scalability, and security with QA and DevOps teams.
- Intercom Integration
    - Develop APIs and workflows for embedding RecovR Assistant.
    - Enable automated ticket creation, resolution suggestions, and escalation triggers.
- Documentation & Reporting
    - Maintain clear technical and user documentation.
    - Present findings and progress to cross-functional stakeholders.

Technical Stack:

- Languages: Python, Node.js (preferred for backend)

© 2025 Nagravision Sàrl / All Rights Reserved
Public

- AI/ML: RAG architectures, LLM-based systems
- Integration: RESTful APIs, Webhooks
- Platforms: Intercom, AWS, Microsoft Azure
- Monitoring Tools: Grafana, Opsgenie (or similar)
- DevOps: CI/CD pipelines, automated testing, cloud infrastructure

Expected Outcomes:

- A fully functional and integrated RecovR Assistant application.
- Comprehensive documentation (technical and user-facing).
- A final report detailing development, challenges, and solutions.
- Training materials or sessions for internal users.

Team & Collaboration:

- Mentorship: Direct guidance from Principal Security Engineer and collaboration with AI/ML experts.
- Cross-functional Exposure: Work closely with Product, Engineering, and Support teams.
- Communication: Regular updates and presentations to stakeholders.
- Culture: Supportive, innovative-driven, and focused on real-world impact.

[IOT-AGR-01] **Autonomous Field Inspection Robot with Edge Computing**

Topics: **Hardware/Software Development - AI** Master Thesis Possible: **NO**

Details

Join our team to develop an intelligent robotic system for automated field inspection using computer vision and edge computing technologies. This internship offers hands-on experience in robotics, AI, and IoT applications for precision agriculture.

Key Objectives

- **System Architecture Design**
  - Design the overall robot architecture and communication protocols
  - Define sensor integration requirements and data flow
- **Computer Vision Development**
  - Implement real-time image processing algorithms for crop monitoring
  - Develop object detection models for identifying pests, diseases, or growth anomalies
  - Optimize models for edge deployment with reduced computational requirements
- **Edge Computing Implementation**
  - Deploy AI models on edge devices (NVIDIA Jetson, Orange Pi, or similar)
  - Implement efficient data preprocessing and analysis pipelines
  - Develop local decision-making algorithms for autonomous navigation
- **Robot Control System**
  - Program robot movement and navigation systems
  - Integrate sensors (cameras, LIDAR, GPS) for field mapping
  - Implement safety protocols and obstacle avoidance
- **Data Management & Analytics**
  - Design data collection and storage mechanisms
  - Create reporting dashboards for inspection results
  - Implement wireless data transmission to central monitoring systems
- **Testing & Validation**
  - Conduct field trials and performance evaluations
  - Optimize system reliability and accuracy
  - Document findings and prepare technical reports

Skills and Profile

- Currently pursuing degree in Computer Science, Robotics, Electrical Engineering, or related field
- Programming Languages: Python, C++, or ROS (Robot Operating System)

- Machine Learning: Experience with TensorFlow, PyTorch, and OpenCV
- Edge Computing: Familiarity with embedded systems and IoT devices
- Robotics: Basic understanding of robotic systems and sensors

[IOT-AGR-02] **RAG-Based LLM for Agricultural Field Management**

Topics: **Software Development - AI** Master Thesis Possible: **YES**

Details

Join our team to develop an intelligent agricultural assistant that leverages Retrieval-Augmented Generation (RAG) and Large Language Models to provide disease diagnosis, field state summaries, and expert agricultural guidance. This internship builds upon our existing irrigation recommendation system to create a comprehensive AI-powered agricultural advisor.

Key Objectives

- **RAG System Architecture**
  - Design and implement RAG pipeline for agricultural knowledge retrieval
  - Integrate vector databases with agricultural literature, research papers, and field data
  - Develop efficient document indexing and similarity search mechanisms
- **Disease Detection & Diagnosis**
  - Create multimodal LLM integration for analyzing crop images and sensor data
  - Build comprehensive disease knowledge base with symptoms, treatments, and prevention
  - Implement real-time disease identification from visual and environmental inputs
  - Develop confidence scoring and uncertainty handling for diagnostic recommendations
- **Field State Summarization**
  - Integrate with existing moisture sensor infrastructure and irrigation recommendation system
  - Develop automated field condition reports combining sensor data, weather, and visual observations
  - Create natural language summaries of crop health, growth stages, and environmental conditions
  - Implement trend analysis and predictive insights for field management
- **Agricultural Chatbot Development**
  - Build conversational AI interface for farmer queries and agricultural guidance
  - Implement context-aware responses using field-specific data and historical patterns
  - Develop multilingual support for diverse agricultural communities
- **Knowledge Management & Updates**
  - Design continuous learning pipeline for incorporating new agricultural research
  - Implement feedback mechanisms to improve diagnostic accuracy
  - Create system for validating and updating agricultural knowledge base
  - Develop version control for knowledge updates and model improvements

© 2025 Nagravision Sàrl / All Rights Reserved

• **Testing & Validation**

- Conduct accuracy testing with agricultural experts and field data
- Validate disease detection against known cases and expert diagnoses
- Optimize response quality and system performance
- Document system capabilities and limitations

Skills and Profile

- Currently pursuing degree in Computer Science, AI/ML, Agricultural Engineering, or related field
- Programming Languages: Python, JavaScript, or similar for LLM integration
- Machine Learning: Experience with transformers, RAG systems, LangChain, or similar frameworks
- Large Language Models: Familiarity with OpenAI, Anthropic, or open-source LLMs (Llama, Mistral)
- Vector Databases: Experience with ChromaDB, Pinecone, Weaviate, or similar • Agriculture Knowledge is a plus: Understanding of crop management, plant pathology, or precision agriculture
- API Development: REST/GraphQL APIs for chatbot and system integration

[IOT-AGR-03] **Crop Yield Forecasting using Satellite Imagery and Machine Learning**

Topics: **Software Development - AI** Master Thesis Possible: **YES**

Details

Join our team to develop advanced yield prediction systems that leverage satellite imagery, remote sensing data, and machine learning to provide accurate crop yield forecasts. This internship offers the opportunity to work at the intersection of space technology, agriculture, and AI to support farmers and agricultural decision-making.

Key Objectives

- **Satellite Image Processing & Analysis**
  - Develop automated pipelines for satellite imagery acquisition and preprocessing
  - Implement vegetation index calculations (NDVI, EVI, SAVI) for crop health assessment
  - Create image segmentation and field boundary detection algorithms
  - Build temporal analysis systems to track crop development throughout growing seasons
  - Continue and enhance developments from the previous internship phase.
- **Machine Learning Model Development**
  - Design deep learning models for yield prediction using convolutional neural networks
  - Implement time-series analysis combining satellite data with weather patterns
  - Develop ensemble methods integrating multiple remote sensing indicators
  - Create transfer learning approaches for different crop types and geographic regions
- **Multi-Modal Data Integration**
  - Combine satellite imagery with weather data, soil information, and historical yields
  - Develop data fusion techniques for optical and radar satellite observations
  - Implement feature extraction from multiple spectral bands and indices
  - Create systems to handle missing data and cloud coverage challenges
- **Crop Growth Modeling**
  - Build phenological stage detection algorithms using satellite time-series
  - Develop stress detection models for drought, disease, and nutrient deficiency identification
  - Implement crop biomass estimation using remote sensing data
  - Create growth curve modeling and yield potential assessment tools
- **Forecasting System Architecture**
  - Design scalable prediction pipelines for large-scale agricultural monitoring
  - Implement real-time processing systems for continuous yield updates
  - Develop uncertainty quantification and confidence intervals for predictions

© 2025 Nagravision Sàrl / All Rights Reserved

- Create automated model retraining and validation frameworks

• **Validation & Performance Assessment**

- Build ground-truth data collection and validation systems
- Develop accuracy metrics and performance benchmarking tools
- Implement cross-validation strategies across different seasons and locations
- Create comparative analysis with traditional yield estimation methods

Skills and profile

• Currently pursuing degree in Computer Science, AI/ML, Agricultural Engineering, or related field

• Programming Languages: Python, R, JavaScript, experience with geospatial libraries (GDAL, rasterio)

• Machine Learning: Proficiency in computer vision, deep learning frameworks (TensorFlow, PyTorch)

• Remote Sensing: Understanding of satellite systems, spectral analysis, and image processing
• Agricultural Knowledge: Basic understanding of crop physiology, farming practices, and yield factors

• Data Science: Statistical analysis, time-series forecasting, and data visualization skills

• Cloud Computing: Familiarity with cloud platforms for large-scale data processing is a plus.

[IOT-AGR-04] **Irrigation Algorithm Enhancement and Machine Learning Integration**

Topics: **Software Development - AI** Master Thesis Possible: **YES**

Details

Join our team to analyze, optimize, and enhance our existing irrigation scheduling algorithm through data-driven insights and advanced machine learning techniques. This internship offers the opportunity to work with real-world agricultural data and improve precision irrigation systems that are already deployed in the field.

Key Objectives

- **Algorithm Performance Analysis**
  - Conduct comprehensive analysis of current irrigation algorithm performance across different field conditions
  - Develop metrics and KPIs to evaluate irrigation efficiency, water usage, and crop response
  - Identify optimization opportunities through statistical analysis of historical irrigation data
  - Create comparative studies between algorithm recommendations and actual field outcomes
- **Data Mining and Pattern Recognition**
  - Analyze large datasets from deployed irrigation systems to identify usage patterns
  - Develop insights from sensor data, weather correlations, and crop performance metrics
  - Implement clustering analysis to identify different irrigation behaviour profiles
  - Create visualization tools for algorithm performance monitoring and debugging
- **Algorithm Optimization and Enhancement**
  - Refine existing irrigation timing and duration calculation methods
  - Optimize threshold parameters and decision logic based on performance analysis
  - Develop adaptive mechanisms that adjust to varying field and crop conditions
  - Implement feedback loops to continuously improve algorithm accuracy
- **Machine Learning Integration**
  - Design ML models to enhance existing rule-based irrigation decisions
  - Develop predictive models for soil moisture dynamics and crop water stress
  - Create automated parameter tuning systems using machine learning techniques
- **Real-time Optimization System**
  - Build dynamic adjustment mechanisms that respond to changing field conditions
  - Develop online learning capabilities for continuous algorithm improvement
  - Create automated model selection and hyperparameter optimization pipelines
- **Validation and Field Testing**

- Design validation protocols for algorithm improvements using field trial data
- Develop simulation environments for testing algorithm modifications
- Create performance benchmarking systems comparing old vs. enhanced algorithms
- Implement rollback mechanisms and safety checks for algorithm updates

Skills and profile

• Currently pursuing degree in Computer Science, Data Science, Agricultural Engineering, or related field

• Programming Languages: Python, R, SQL, experience with data analysis and scientific computing libraries

• Machine Learning: Proficiency in supervised learning, time-series analysis, and optimization techniques

• Data Analysis: Strong skills in statistical analysis, data visualization, and exploratory data analysis

• Algorithm Development: Understanding of optimization algorithms, control systems, and decision logic

• Agricultural Systems: Basic knowledge of irrigation principles, crop water requirements, and soil science is a plus

[IOT-AT-01] **Evaluate Reliable Positioning Logic Using GPS, Cell-Tower, and WiFi AP Data**

Topics: **Positioning Algorithms, IoT, Asset Tracking** Master Thesis Possible: **YES**

This internship focuses on designing and evaluating a reliable positioning algorithm that leverages GPS, WiFi access point data, and cell tower signals. The goal is to enhance the accuracy and consistency of location reporting for IoT asset tracking devices in diverse environments.

Detailed Description

IoT asset trackers often face challenges in environments with poor GPS signal (e.g., indoors or urban areas). To improve positioning accuracy, they also use data from nearby WiFi access points and cell towers.

The intern will:

- Analyze real-world data from deployed devices.
- Evaluate the accuracy of each positioning source.
- Design a context-aware fusion algorithm to combine or select data sources.
- Assess how different configurations (e.g., GNSS retry logic, signal thresholds) affect positioning performance and battery life.

This work aims to enhance the **RecovR platform's** ability to locate assets reliably in difficult environments like car dealerships or consumer settings.

Key Objectives

- Analyze positioning data from GPS, WiFi, and cell tower sources.
- Design and implement a positioning logic that adapts to signal availability and quality.
- Evaluate the accuracy and reliability of the proposed solution using field data.
- Optimize the algorithm for power efficiency and responsiveness.
- Document the methodology, results, and recommendations for deployment.

Technical Skills

- Programming: Python (data analysis, algorithm development), C (embedded systems)
- Positioning Technologies: GPS, WiFi scanning, LTE cell tower triangulation
- Data Analytics: Signal quality analysis, error modeling, performance benchmarking
- Machine Learning (optional): Sensor fusion, probabilistic modelling
- Tools: Jupyter, Git, RF analysis tools
- Soft Skills: Analytical thinking, problem-solving, teamwork, technical documentation

© 2025 Nagravision Sàrl / All Rights Reserved

[IOT-AT-02] **Explore Non-terrestrial Network Communication**

Topics: **Non-Terrestrial Networks, IoT, Asset Tracking** Master Thesis Possible: **YES**

This internship focuses on designing and implementing a prototype for non-terrestrial (satellite-based) communication using the Nordic nrf9151 platform. The goal is to evaluate the feasibility and performance of IoT devices communicating beyond terrestrial cellular networks.

Detailed Description of the Internship Topic

With the rapid expansion of IoT deployments, reliable connectivity in remote or underserved areas is a growing challenge**. Non-terrestrial networks (NTN)**, such as satellite-based communication, offer a promising solution to extend coverage where traditional cellular networks are unavailable.

The intern will investigate the capabilities of the **Nordic 9151 platform** for NTN applications, including hardware configuration, firmware adaptation, and protocol selection. The project involves designing and implementing **a working prototype** that can establish and maintain communication via satellite or other non-terrestrial means. The intern will also benchmark the prototype's performance, analyze **connectivity reliability**, and document the integration process.

Collaboration with hardware, firmware, and network experts will be essential to ensure the prototype meets technical and operational requirements.

Key Objectives

- Research non-terrestrial network technologies and their applicability to IoT.
- Configure and adapt the Nordic 9151 platform for NTN communication.
- Design and implement a prototype demonstrating non-terrestrial connectivity.
- Evaluate the prototype's performance in various scenarios.
- Document the development process, challenges, and results.
- Present findings and recommendations for future NTN-enabled IoT solutions.

Technical Skills

- Programming: C/C++ (embedded systems), Python (prototyping, data analysis)
- Wireless Communication: Satellite protocols, LTE-M/NB-IoT
- Embedded Systems: Nordic platforms, hardware integration, firmware development
- Networking: TCP/IP, UDP, cellular and satellite communication stacks
- Tools: Nordic SDK, RF test equipment, Git
- Soft Skills: Research, problem-solving, teamwork, technical documentation

[IOT-AT-03] **Preventive and Predictive Maintenance of IoT Devices in the Field**

Topics: **Preventive/Predictive Maintenance, IoT** Master Thesis Possible: **YES**

This internship focuses on developing machine learning capabilities to profile the standard behavior of IoT devices and detect anomalies that may indicate potential failures. The goal is to enable preventive and predictive maintenance strategies that improve device reliability and operational efficiency.

Detailed Description

IoT asset tracking devices operate under varied field conditions and rely on internal batteries while transmitting data via **LTE Cat-M1 networks**. Over time, changes in behavior—like increased power usage or poor connectivity—can indicate potential device failures.

The intern will:

- Analyze **device logs and telemetry data**.
- Build **behavioral profiles** and detect anomalies using **machine learning**.
- Design models to identify early signs of malfunction for **proactive maintenance**.
- Evaluate the models' impact on **operational efficiency**.
- Propose **optimizations or corrective actions**.

This project involves working with data from over **500,000 deployed devices**, contributing to the advancement of asset tracking reliability and performance.

Key Objectives

- Analyze device logs to identify patterns and standard behavior.
- Design and implement ML models for anomaly detection and predictive maintenance.
- Evaluate model performance and its impact on device reliability.
- Propose optimizations or corrective actions based on detected anomalies.
- Document the methodology, results, and recommendations for deployment.

Technical Skills

- Programming: Python (data analysis, ML)
- Machine Learning: Anomaly detection, time-series modeling, supervised/unsupervised learning
- Data Analytics: Feature engineering, log analysis, performance evaluation
- IoT Systems: Understanding of LTE Cat-M1, battery-powered devices, telemetry
- Tools: Jupyter, Git, ML libraries (scikit-learn, TensorFlow, PyTorch)
- Soft Skills: Analytical thinking, problem-solving, teamwork, technical documentation

[IOT-AT-04] **Theft Detection Using Machine Learning**

Topics: **Anomaly Detection, AI, IoT, Asset Tracking** Master Thesis Possible: **YES**

This internship focuses on developing and implementing machine learning techniques to profile consumer behavior and detect anomalies that may indicate theft. The goal is to enhance the security and intelligence of asset tracking solutions by enabling proactive theft detection based on behavioral analysis.

Detailed Description

Asset tracking devices generate large volumes of behavioral data as they monitor consumer usage patterns. Traditional theft detection methods often rely on fixed rules or manual alerts, which can result in delayed or missed incidents. This internship will explore the use of machine learning to automatically learn a consumer's default behavior profile and identify deviations that could signal suspicious activity or theft.

The intern will work with real-world IoT data to design, train, and validate models for anomaly detection. This includes feature engineering, model selection, and evaluation of detection accuracy. The project will also involve implementing a prototype that integrates with existing asset tracking infrastructure and may include visualization of detected anomalies for operational teams.

Collaboration with data scientists, engineers, and product managers will be essential to ensure the solution is robust, scalable, and aligned with business needs.

Key Objectives

- Analyze consumer behavioral data from asset tracking devices.
- Design and implement machine learning models for profiling and anomaly detection.
- Develop a prototype to generate consumer profiles and flag unusual behavior.
- Evaluate the effectiveness of the detection system using real-world data.
- Document the methodology, results, and recommendations for deployment.

Technical Skills

- Programming: Python (data analysis, ML), SQL (data extraction)
- Machine Learning: Supervised and unsupervised learning, anomaly detection, clustering
- Data Analytics: Feature engineering, time-series analysis, model evaluation
- IoT Systems: Understanding of asset tracking devices and data flows
- Tools: Jupyter, Git, ML libraries (scikit-learn, TensorFlow, PyTorch)
- Soft Skills: Analytical thinking, problem-solving, teamwork, technical documentation

[IOT-AT-05] **Troubleshooting Application for Wireless Devices (BLE Interface)**

Topics: **AI, IoT, Asset Tracking** Master Thesis Possible: **YES**

The internship focuses on designing and implementing a solution to exchange diagnostic information between wireless devices and troubleshooting applications using the BLE interface. The goal is to improve the efficiency and effectiveness of diagnosing and resolving issues in connected devices.

Detailed Description

Wireless IoT devices are increasingly deployed in diverse environments, making remote diagnostics and troubleshooting essential for operational reliability. This internship will involve the development of a troubleshooting application capable of communicating with devices via Bluetooth Low Energy (BLE). The intern will analyze current diagnostic needs, define the communication protocol, and implement both device-side and application-side solutions to enable seamless exchange of diagnostic data.

The project will require close collaboration with firmware and software teams to ensure compatibility and security. The intern will also document the solution and may contribute to the development of user interfaces or automation scripts for common troubleshooting scenarios.

Key Objectives

- Analyze diagnostic requirements for wireless devices in the field.
- Design a BLE-based protocol for exchanging diagnostic information.
- Implement firmware modifications to support diagnostic data exchange.
- Develop a troubleshooting application (mobile or desktop) to interface with devices.
- Test and validate the solution in real-world scenarios.
- Document the protocol, implementation, and usage guidelines.

Technical Skills

- Programming: C/C++ (embedded), Python or Java/Kotlin/Swift (application development)
- Wireless Communication: BLE protocol, device pairing, data exchange
- Embedded Systems: Firmware development and debugging
- Software Development: Mobile or desktop application development
- Tools: BLE sniffers, debuggers, Git
- Soft Skills: Analytical thinking, problem-solving, teamwork, technical documentation

© 2025 Nagravision Sàrl / All Rights Reserved

[IOT-AT-06] **WebApp Analytic Tool for Field Device Metrics Visualization**

Topics: **Analytics Dashboard, Locator Metrics, IoT** Master Thesis Possible: **YES**

This internship focuses on designing and implementing a WebApp interface to visualize key metrics reported by IoT locators deployed in the field. The goal is to improve operational visibility and decision-making through intuitive and actionable dashboards.

Detailed Description of the Internship Topic

IoT locators deployed across various environments generate a wide range of telemetry data, including heartbeat intervals, connectivity status, and location updates. However, this data is often underutilized due to the lack of a dedicated visualization interface.

The intern will be responsible for developing a WebApp analytics tool that aggregates and displays this data in a user-friendly format. The project includes defining the UI/UX design, implementing frontend components, and integrating backend APIs to retrieve real-time metrics. The tool will support use cases such as monitoring device health, identifying anomalies, and supporting deployment planning.

The intern will collaborate with engineers, product managers, and operations teams to ensure the tool meets practical needs and aligns with existing platforms. This internship may also involve prototyping mobile extensions or exploring integration with platforms like Grafana.

Key Objectives

- Design a responsive and intuitive Web UI for displaying locator metrics.
- Implement frontend components using modern web technologies.
- Integrate with backend services to fetch and display real-time data.
- Support filtering, sorting, and visualization of key metrics (e.g., heartbeat reliability, connectivity by country).
- Conduct user testing and iterate based on feedback.
- Document the architecture, usage, and deployment process.

Technical Skills

- Frontend Development: HTML, CSS, JavaScript, React or Angular
- UI/UX Design: Figma, Adobe XD, or similar tools
- Data Visuaization: Chart.js, D3.js, or similar libraries
- Backend Integration: REST APIs, JSON, WebSockets
- Tools: Git, JIRA, VS Code
- Soft Skills: Creativity, collaboration, user-centric thinking, documentation

[IOT-HW-01] **Battery Characterization and Testbench Automation for IoT Devices**

Topics: **Battery Testing, Testbench Automation, IoT** Master Thesis Possible: **YES**

This internship focuses on designing and enhancing a battery testbench for IoT devices, automating test procedures, and analyzing battery behavior under various conditions. The goal is to improve battery reliability and validate datasheet claims through real-world testing.

Detailed Description

IoT devices rely heavily on battery performance, especially in field deployments. This internship offers the opportunity to work on a comprehensive battery testbench that supports automated testing and long-term aging cycles. The intern will study the impact of temperature on battery behavior, validate datasheet specifications, and evaluate battery quality through controlled experiments.

A key part of the project involves investigating passivation and depassivation phenomena, which affect battery readiness and longevity. The intern is expected to document all procedures and findings thoroughly to support future development and quality assurance efforts.

Key Objectives

- Design and implement a battery testbench with automation capabilities.
- Perform aging cycles and temperature-based stress tests.
- Validate datasheet accuracy and assess battery quality.
- Analyze passivation/depassivation effects.
- Deliver well-documented procedures and results.

Technical Skills

- Experience with LabVIEW for test automation.
- Programming in C and Python for data handling and control logic.
- Understanding of battery chemistry and embedded systems is a plus.

© 2025 Nagravision Sàrl / All Rights Reserved

[IOT-HW-02] **Antenna Design for BLE/LTE Applications**

Topics: **PCB Antenna Design, Antenna Modeling** Master Thesis Possible: **YES**

This internship focuses on designing and modeling PCB antennas for RF applications (BLE/LTE). The intern will evaluate antenna performance and validate designs using simulation and measurement tools.

Detailed Description

Bluetooth Low Energy (BLE), Long-Term Evolution CAT-M1 (LTE) or GPS applications require compact and efficient antenna designs integrated into PCBs. This internship offers the opportunity to work on antenna design and modeling using tools such as Matlab and Spice. The intern will simulate antenna behavior, evaluate performance metrics, and validate designs through measurements. The project aims to optimize antenna characteristics for reliable BLE/LTE/GPS communications and ensure compliance with design specifications.

Key Objectives

- Design PCB antennas for BLE/LTE/GPS applications.
- Model antenna behavior using simulation tools (Matlab, Spice).
- Evaluate antenna performance through simulations and measurements.
- Validate antenna designs against performance criteria.
- Document design processes and results thoroughly.

Technical Skills

- Experience with antenna design and RF principles.
- Proficiency in Matlab and Spice for modeling and simulation.
- Familiarity with PCB design tools and BLE/LTE/GPS communication protocols.
- Strong documentation and analytical skills.