Course #1

Intro & the why

automotive crunch

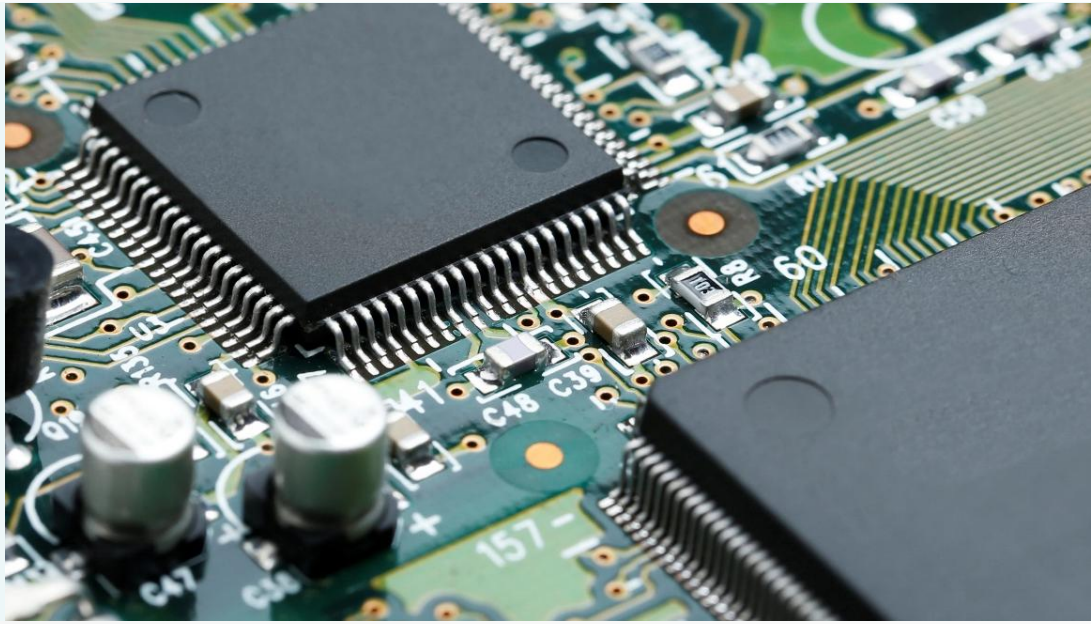
3/14/2026

Content

- Intro
- Grading system
- What will we cover
- Rules and regulations
- Next time

Intro

Intro - SS

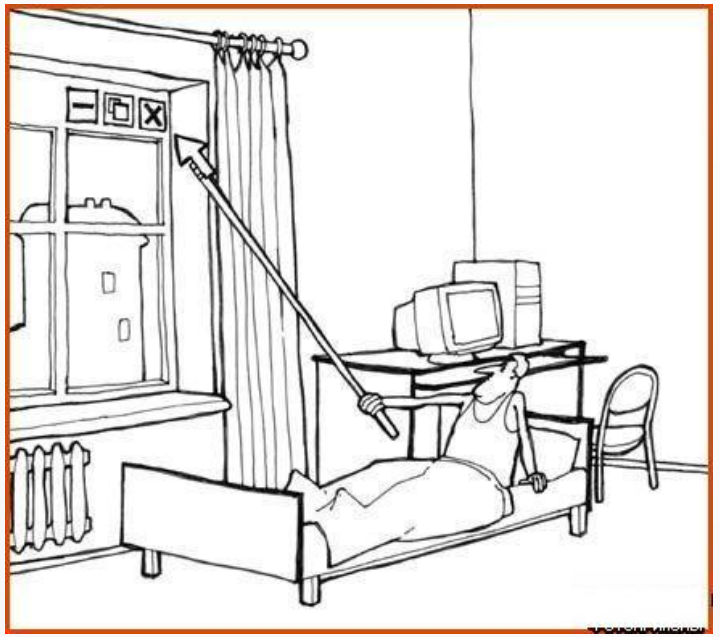


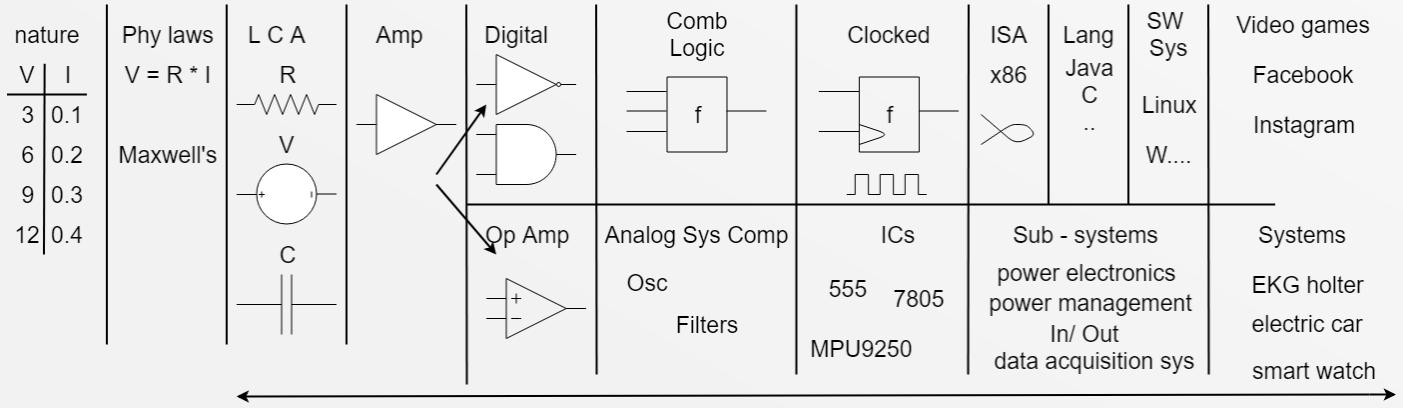
Engineering

- Scientific understanding of the natural world
- Abstract thinking

>> used to invent, design, and build things

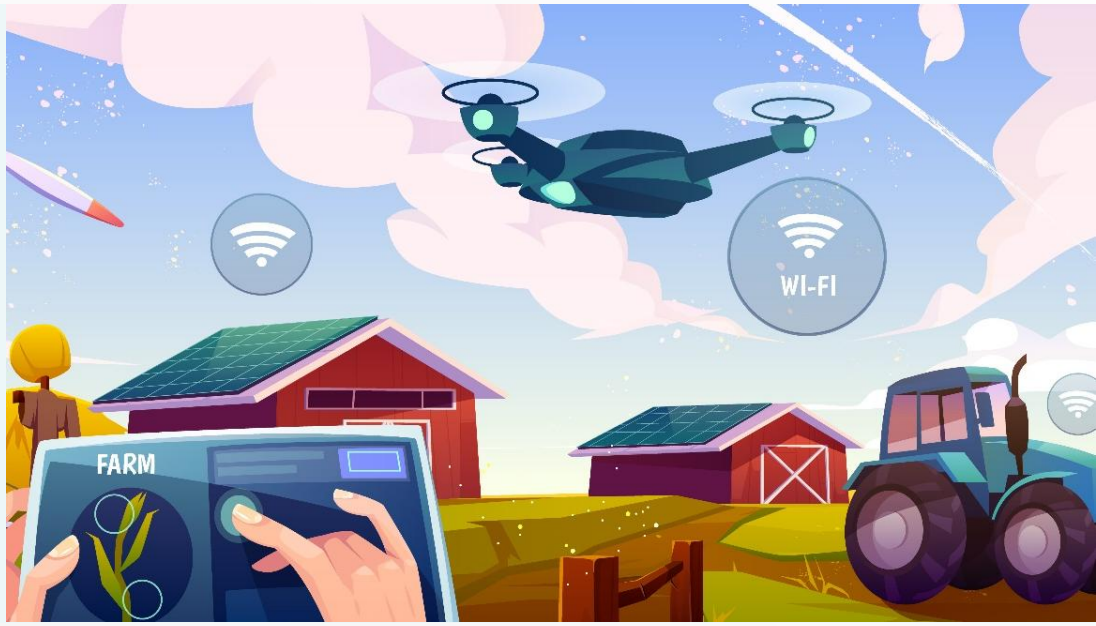
>> to solve problems and achieve practical goals





SS
automotive crunch

IoT



IoT uses & applications

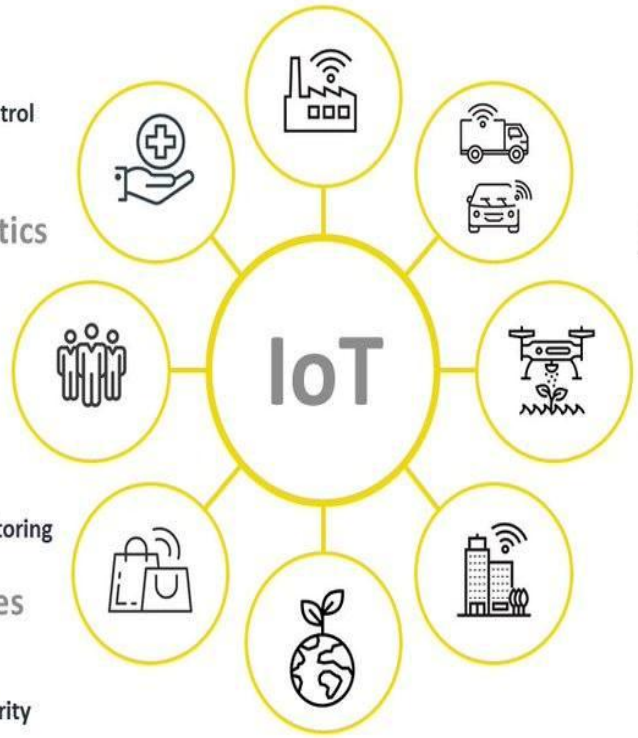
empiric

Industrial
- Machine-to-Machine communication
- Process monitoring & control
- Maintenance monitoring

Automotive & Logistics
- Autonomous vehicles
- Vehicle auto-diagnostics
- Fleet management

Smart Farms
- Soil analysis
- Crop management
- Climate/agriculture monitoring

Smart Cities & Homes
- Parking sensors
- Waste management
- Home automation & security
- Optimized energy use

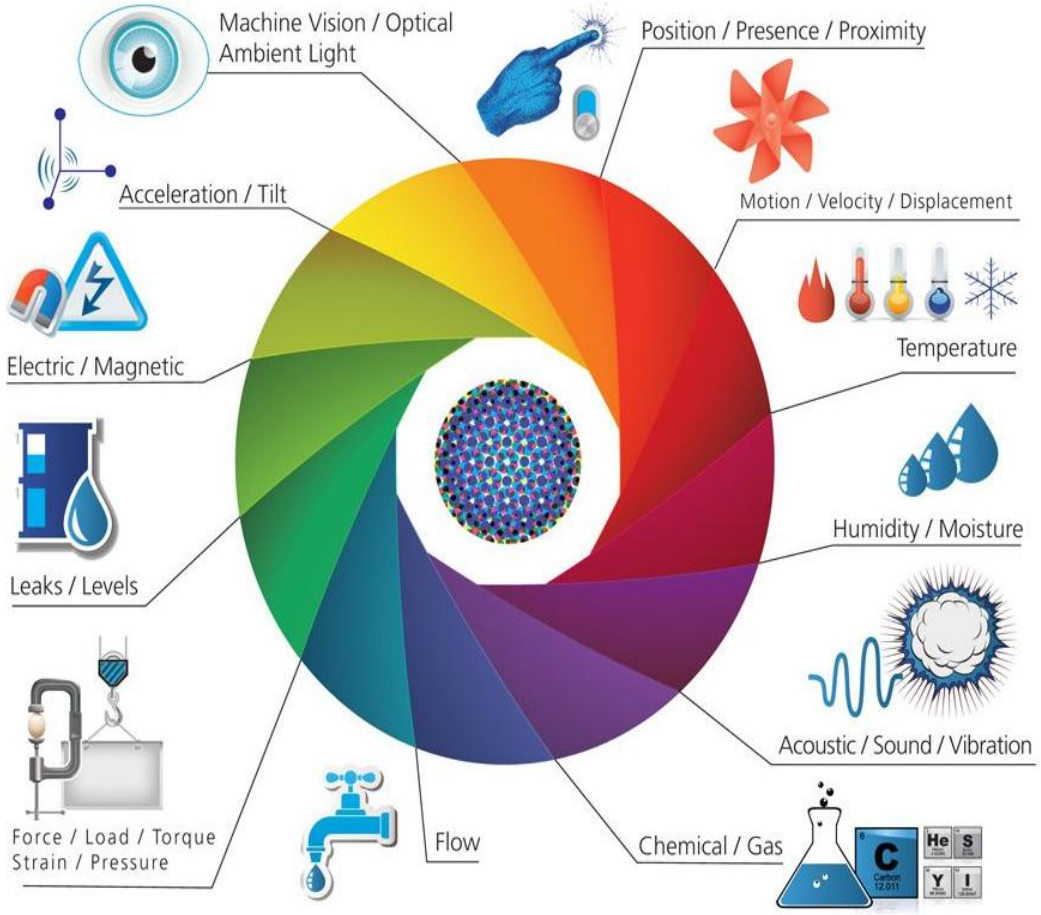


Environment
- Forest Fire Detection
- Environmental monitoring
- Species Tracking

Retail
- Inventory control
- Theft protection
- Monitoring in-store wait times

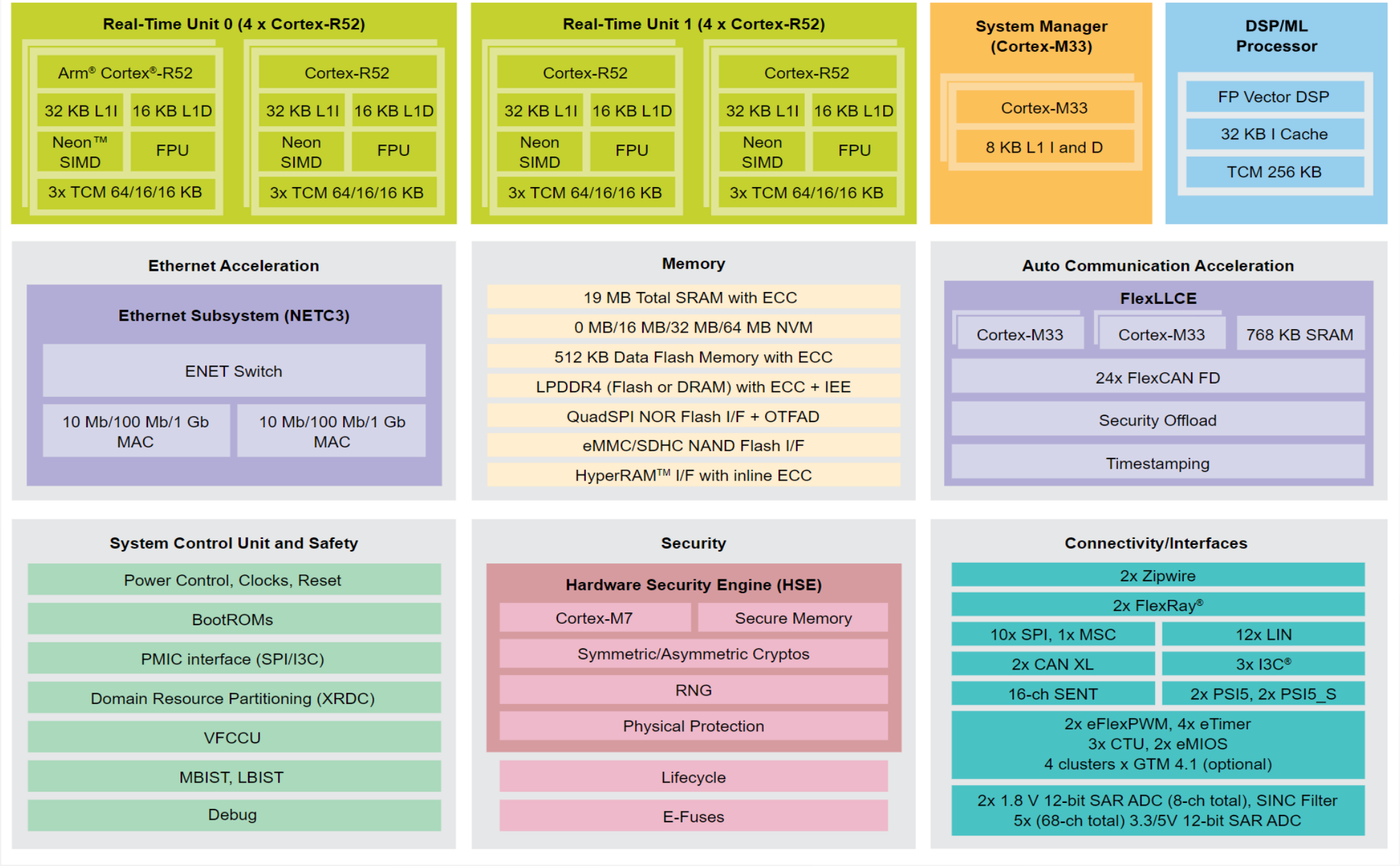
Consumers
- Smart watches & wearables
- Children/senior tracker

Healthcare
- Optimized patient care
- Fitness devices
- Ingestible sensors
- Connected inhales



Embedded systems

- **Dedicated Function**: Embedded systems are designed for a specific purpose.
- **Integration**: They are integrated into a larger system.
- **Real-Time**: Many embedded systems must respond to events in real time.
- **Resource Constraints**: They often operate with limited memory and processing power.
- **Ubiquity**: Embedded systems are everywhere in modern technology.



© https://www.nxp.com/products/processors-and-microcontrollers/s32-automotive-platform/s32z-and-s32e-real-time-processors/s32e2-safe-and-secure-high-performance-real-time-processors-with-actuation-support:S32E2

Why the “Securing Systems” name

- Security engineering;
- Security analysis;
- Security monitoring;
- Security response;
- Security forensics;

  <=
- Security architecture: integrate into “computer” systems the security features and control that will provide the protection expected of the system
  - Breadth of knowledge
  - Depth of understanding
  - Apply security technology and processes
  - Protect the system, interconnections and data

Structure

Lecture

- Embedded and automotive cybersecurity
- Basic concepts and fundamental principles
- Threat Identification and classification
- Threat taxonomies and prioritization
- Risk assessment and impact analysis
- Security use cases
- DevSecOps in embedded and automotive
- Secure development lifecycle (SDLC)
- Security standards compliance

Labs

- One project proposal, solved by all
  - Embedded device, web connected
  - Automated testing and 100% code coverage
  - Static code analysis & vulnerability identification
  - Fuzzing for security testing
  - Software bill of materials
  - Hardening and protection of the solution
- One midterm evaluation
- One assignment with a rebuttal argumentation, simulation for a real client feature negotiation

Scoring structure

Scoring structure

- 4p – final exam
- 1p – feature & rebuttal
- 3p – project security
- 1p – midterm
- 1p – labs
- 1p – bonuses

Rules for passing

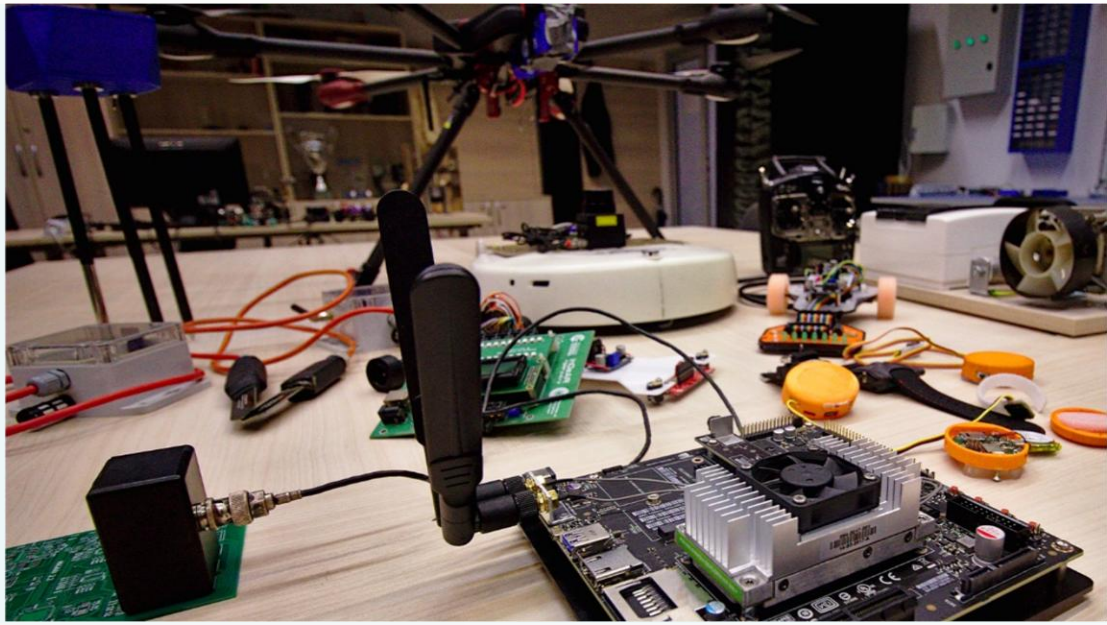
- 50% labs attendance
- 50% final grade

Extra

- **Final Exam (4p)**
  - Written evaluation with questions from the taught material.
- **Feature & Counter-argumentation (1p)**
  - **0.7p** – Argumentation and technical justification of a feature.
  - **0.3p** – Voting for the most relevant feature.
  - **Bonus**: The most appreciated counterargument receives **+0.2p** (without exceeding the total of 1p for this component).
- **Project (3p)**
  - **2.25p** – Functionality, documentation, execution.
  - **0.75p** – Security (Threat Modeling, Mitigations, Testing, Code Coverage, Hardening).
  - You have to convince the client to buy the feature or features developed by you.
- **Midterm (1p)**
  - Evaluation on course and labs topics.
- **Laboratory (1p)**
  - Active participation and completion of laboratory exercises.
- **Bonuses (maximum 1p)**
  - **+0.5p** – Voluntary presentation on a relevant topic (must be voted by colleagues or validated by the professor).
  - **+0.5p** – Consistent attendance at the course (you receive a **bonus topic** in the exam).

SS
automotive crunch

Project topic



Project details

- **Security & Compliance Encouragement**
- **Teams must aim for high security & reliability** while developing their project.
- **Security findings must be well-documented** (reports, test logs, compliance summaries).
- **Objective metrics ensure fairness** (no subjective "effort-based" scoring).

Category	Max Points	Evaluation Criteria
Functionality, Documentation, Execution	2.25p	✅ Working features, ✅ Clear documentation, ✅ Proper execution
Security & Compliance (Total: 0.75p)		
🔹 Threat Modeling & Mitigations	0.15p	📌 Identifying attack surfaces, 📌 Addressing potential threats
🔹 MISRA, CERT Findings & Compliance	0.15p	📌 Fewer violations, 📌 Proper standard alignment
🔹 Code Coverage & Testing Reports	0.15p	📌 High % test coverage, 📌 Functional + fuzz testing
🔹 Software Bill of Materials (SBOM) & Dependencies	0.10p	📌 Open-source security audit, 📌 No vulnerable dependencies
🔹 Fixing Own Vulnerabilities	0.10p	📌 Number & severity of issues fixed
🔹 Finding & Reporting Others' Vulnerabilities	0.10p	📌 Valid security issues found in peer projects
⚠ Penalty for Ignoring Critical Vulnerabilities	-0.10p	📌 Failure to fix valid reported security issues

Q&A