# Notas SR

## Requisitos:

**Confidencialidade:**

- All communications have to use a secure communication protocol with at least a 256 bit key.

- The system shall encrypt all the input data. Passwords must be encrypted inside the database. (If the database is corrupted, an attacker should not be capable of getting account information.)

- During the development of the application, every implementation shall be tested and analyzed carefully paying attention to potential vulnerabilities.
- All data must be confidential. Only the user with the correct permissions shall be able to access their personal information. No one from outside shall be allowed to get information.

- Information exchanged shall be exchanged via a secure channel to prevent third parties from intercepting the communication.

**Availability:**

- The information received shall be stored in the system so that the system is available 99.9 % of the time even if there is no possibility of obtaining new information from the server.

- The software must be replicated in two offsite locations to provide execution redundancy, with proper server synchronization.

**Integrity:**

- Data received from the server regarding the position of the signs shall be validated first before storing it in the vehicle backup system.

- The system communication shall implement digital signatures.

- All data shall remain the same (unaltered), except if some controlled and planned action is performed on it.

- The system shall validate the user input. All the data that a user inputs must be analyzed and if something is not right, the user shall be informed and the data is rejected.

**Non-Repudiation:**

- The system should log all communications and calibrations drills details, including timestamps and location information.

- The application shall log all users actions with a timestamp.

**Authentication:**

- Only system administrators with specific elevated permissions should be able to manually configure critical internal drone calibration parameters.

- During development there shall be authentication measures in the repository that contains the system code.

**Auditability:**

- Fazer auditoria antes do sistema ir para produção.
-

**Compliance:**

- Complies with GDPR of EU.

**Trustworthiness:**

- Complies with GDPR of EU.

# Testes:

**Confidencialidade:**

- Try to access other user data. By logging into an account, try to obtain another account private information,
- Check if the content of the messages passed in the middle of the secure channel can be read, to verify its resistance to overhearing.
- Check if during the calibration drill, the user that supervises the drill is authenticated in the software. An alternative is to check the logs for this information.
- Verify if the encryption algorithm used in the communication system has a 256 bit key

**Availability:**

- By checking at a constant interval if the communication system can successfully send and receive messages correctly, the up time can be calculated.
- By checking all drone information on differently located redundant servers in an instant, the data should be the same.
- Try many times to do some action, run overnight, over weekend, for a week or doing it automatically to measure any possible downtime.

**Integrity:**

- Trying to change data in an unauthorized way and change it in a correct way. Trying to find a way to change the personal profile information, like the name, phone number, etc... apart from the correct way.
- Try to corrupt the database by changing files, replacing them by older versions
- Verify if the communication fails with the use of an invalid digital signature.

**Non-Repudiation:**

- Monitor messages between the server and the cars for a set period of time and then verify that all those messages are logged in the log file
- Record the transaction and confirm if the author is the same.
- Verify if the communication fails with the use of an invalid digital signature.

**Authentication:**

- Perform a clone operation on the repository and verify that it requires authentication to be performed

# External/Internal interfaces:

**Externo:**

- Sistema bancário
- Sistema de autenticação LDAP
- Monitorização externa
- Receção de energia que vem de uma companhia de eletricidade

**Interno:**

- interface com a base de dados do sistema
- Interface da aplicação entre o GUI e a API.
- interface do sistema físico com o posto de eletricidade

**Random:**

- Interface gráfico com outras cenas (teclado, ecrã, etc)
- Cabos de rede
- Wifi
- Portas de entrada e saída do sistema a analisar
- Interface WEB
- Backend para outras portas
- Sistema de backup
- 1 ou mais base de dados

# Tipos de vulnerabilidades:

- SQL
    - analisar/filtrar input
    - Utilizar stored procedures no acesso a base de dados
- XSS
    - filtrar input do utilizador
    - garantir que o input do utilizador não é utilizado diretamente no output
- DOS
    - firewall
    - load balance
    - servidores melhores
    - soluções inteligentes para detecção de DOS
- Unrestricted Upload of File with Dangerous Type
    - Verification of max file size
    - Verification of magic bytes and extension
    - Special characters sanitation

- Broken authentication
    - não enumerar as contas disponíveis.
    - Não utilizar hash function fracas para guardar as passwords
    - garantir que existe entropia nas passwords (não serem passwords fáceis)

- CSRF
    - usar CORS

# Tipos de atacantes:

- script kiddie (só por divertimento)
- hacktivists (são motivados por política ou religião)
- government employees/state sponsored hackers (ordens do governo)
- white hacker (engenheiros)
- black hacker (hackers)
- cyber terrorist (terroristas)

- spy hackers(espiões)

# Design principles:

1. Apply Defense in Depth
2. Use a Positive Security Model
3. Fail Securely
4. Run with Least Privilege
5. Avoid Security by Obscurity
6. Keep Security Simple
7. Detect Intrusions
    1. Log All Security-Relevant Information
    2. Ensure That the Logs Are Monitored Regularly
    3. Respond to Intrusions
8. Don't Trust Infrastructure
9. Don't Trust Services
10. Establish Secure Defaults

# Secure SW Lifecycle:

software

| Phase | Microsoft SDL | McGraw Touchpoints | SAFECode |
|---|---|---|---|
| Education and awareness | Provide training | | Planning the implementation and deployment of secure development |
| Project inception | Define metrics and compliance reporting<br>Define and use cryptography standards<br>Use approved tools | | Planning the implementation and deployment of secure development |
| Analysis and requirements | Define security requirements<br>Perform threat modelling | Abuse cases<br>Security requirements | Application security control definition |
| Architectural and detailed design | Establish design requirements | Architectural risk analysis | Design |
| Implementation and testing | Perform static analysis security testing (SAST)<br>Perform dynamic analysis security testing (DAST)<br>Perform penetration testing<br>Define and use cryptography standards<br>Manage the risk of using third-party components | Code review (tools)<br>Penetration testing<br>Risk-based security testing | Secure coding practices<br>Manage security risk inherent in the use of third-party components<br>Testing and validation |
| Release, deployment, and support | Establish a standard incident response process | Security operations | Vulnerability response and disclosure |

## Software Quality Attributes

Critic soft

**We can have a very extensive list of attributes:**

- Safety
- Security
- Reliability
- Resilience
- Robustness
- Understandability
- Testability
- Adaptability
- Modularity
- Complexity
- Portability
- Usability
- Reusability
- Efficiency
- Learnability
- And many other “ilities”

## Security Goals::Defenses

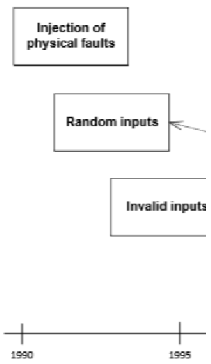
Crit

- Computer access control
- Application security
  - Antivirus software
  - Secure coding
  - Secure by default
  - Secure by design
  - Secure operating systems
- Authentication
  - Multi-factor authentication
- Authorization
- Data-centric security
- Encryption
- Firewall
- Intrusion detection system
- Mobile secure gateway
- Runtime application self-protection (RASP)

- Confidentiality ensures that computer-related assets are accessed only by authorized parties.
  - i.e. reading, viewing, printing, or even knowing their existence
  - Secrecy or privacy
- Integrity means that assets can be modified only by authorized parties or only in authorized ways.
  - i.e. writing, changing, deleting, creating
- Availability means that assets are accessible to authorized parties at appropriate times.
  - i.e. often, availability is known by its opposite, denial of service.

# Security/Robustness Testing

- Robustness Testing
- Injecting physical faults
- Using Random inputs
- Using invalid inputs
- Using type-specific tests
- Applying mutation techniques
- Model-Based/Simulation Robustness Testing
- Exploratory testing



Robustness testing

Pen testing

Fuzz testing

Static code analysis

## How to ensure safety?

- Training or proven experience
- System/Environment knowledge
- Risk/Hazards Analysis
- System and Safety Requirements
- Follow up on development (traceability)
- Verify and Validate
- Build and maintain a Safety Dossier (Safety Case)
- Support external Independent Assessors…

| STRIDE Classification | Domain | Threat Description |
|---|---|---|
| Denial of Service | Airborne, Space, Automotive, Railway | Jamming and flooding ground station, VLAN flooding attack, Flooding signals to satellite, Fake correspondent node addresses, Unauthorized Brake, Attacking Active Brake Function, Attacking E-Toll, Head Unit Attack, Flashing per OBD, WLAN Attack, Disturbing passenger Information system, GSM-R Attack (DoS - Denial of service) |
| Elevation of privileges | Airborne, Automotive, Railway | VLAN Tagging attack, Attacking E-Toll, Force Green Wave/Getting traffic lights green ahead of the attacker, Flashing per OBD, E-Call, Manipulate Speed Limits, Manipulate Traffic Flow, Database attack |
| Repudiation | Automotive | Engine DoS-Attack (Engine Refuse to Start) |
| Spoofing | Airborne, Space, Railway | Spoofing attacks on the Automatic Dependent Surveillance – Broadcast (ADS-B) system, Fake correspondent node addresses, Spoofed binding updates, Fake/Modified telecommands delivered to satellites, WLAN Attack |
| Tampering | Airborne, Automotive, Railway, Space | Interference in communications, Tampering GPS coordinates, Tampering attacks on ADS-B, Head Unit Attack, Simulate Traffic Jam, Tamper with Warning Message, Flashing per OBD, Manipulate physical components, Manipulate signalling components, GPS data falsification, Disturbing passenger Information system, Tampering satellite Software updates |

blah