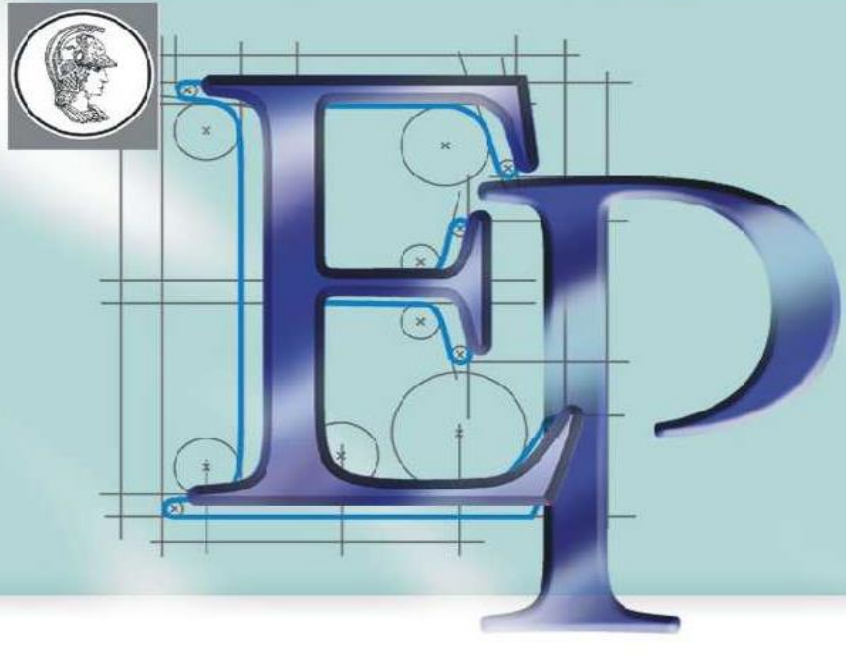


# Projeto de Formatura – 2023



## PCS - Departamento de Engenharia de Computação e Sistemas Digitais

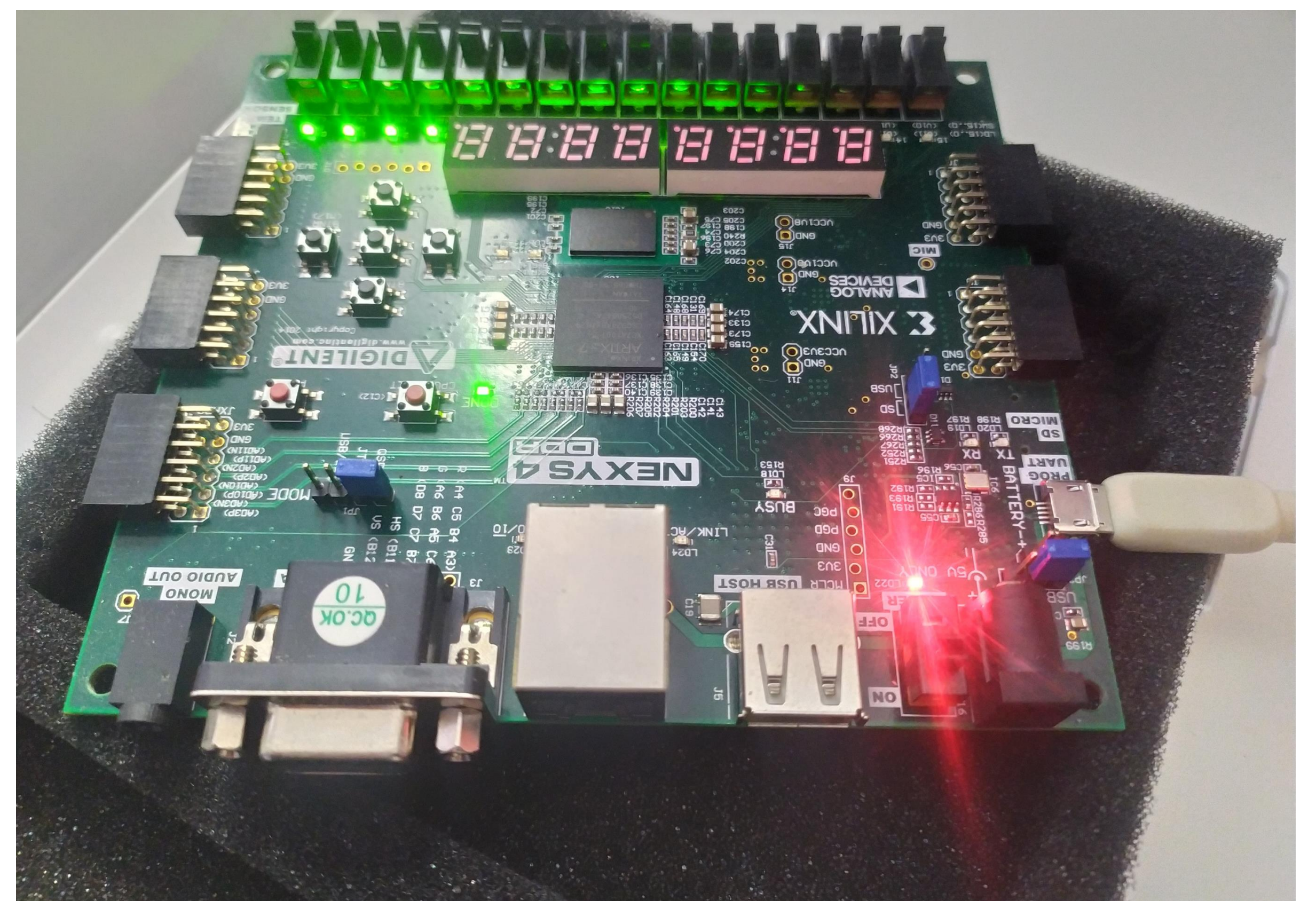
### Engenharia Elétrica – Ênfase Computação

Tema:

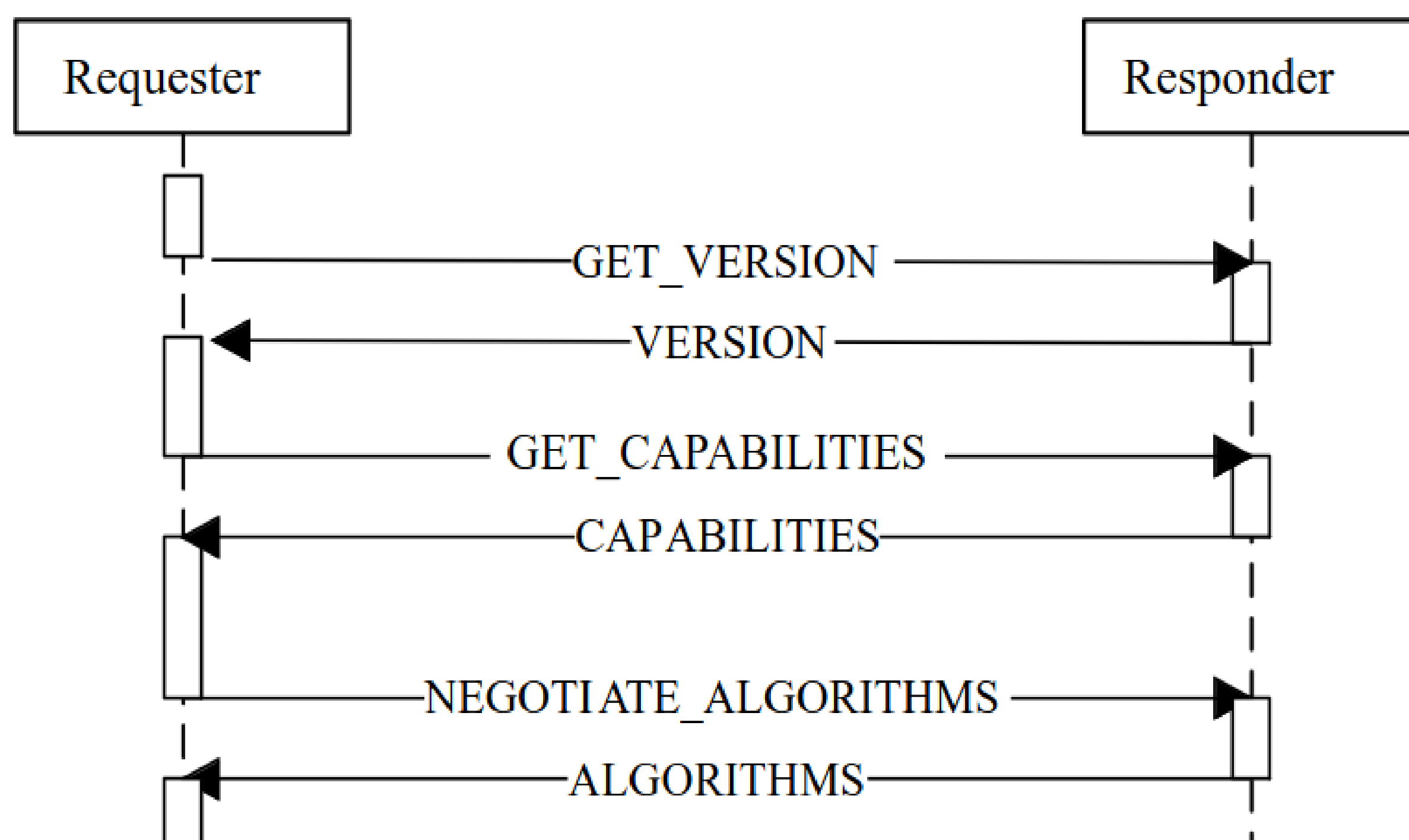
## Implementação em hardware do protocolo SPDM

Nos últimos anos, houve um aumento expressivo do uso de sistemas computacionais, com isto, novos fabricantes de hardware entraram no mercado, o que acabou por gerar preocupações sobre estes novos fabricantes abusarem de sua posição na cadeia de fabricação para realizar modificações maliciosas nestes hardwares ou em seus firmwares. Ataques realizados em nível de firmware/hardware são de difícil detecção, isso ocorre devido a este tipo de ataque ser realizado abaixo do sistema operacional, ou seja, defesas como antivírus e firewall não são eficazes, com estes ataques podem ser utilizados para instalar malwares ou backdoors.

Recentemente na indústria e academia surgiu o protocolo SPDM – Security Protocol and Data Model, este protocolo realiza a autenticação do firmware, juntamente com a criação de um canal seguro de comunicação, assim, sendo possível observar se houve algum tipo de modificação não desejada e ainda assim possuir um canal confiável para a comunicação em baixo nível, como por exemplo, um barramento.



Considerando os objetivos propostos, todo o projeto foi realizado dentro de uma FPGA da Digilent, a Nexys 4 DDR, a FPGA contém em sua programação uma implementação em Risc-V do processador Rocket Chip juntamente com uma placa de rede Ethernet e suporte a entrada serial promovidos pela biblioteca Litex, uma biblioteca em Python para construção de Hardware. O sistema operacional é um Kernel Linux cujo qual o driver da placa de rede Ethernet foi modificada para comportar o SPDM e pode assim ser autenticada. A BIOS desenvolvida pela Litex foi modificada ao adicionar funções que se utilizam da LibSPDM (versão em biblioteca aberta do SPDM) para realizar autenticação e ser autenticada por outros componentes.



## Objetivos

O objetivo do trabalho se encontra no campo de inovação ao realizar a implementação do protocolo SPDM em um hardware dedicado, assim, de modo que seja possível realizar uma avaliação do seu desempenho em alguns aspectos como, por exemplo, uso de memória. A viabilidade deste trabalho pode indicar a possibilidade de utilização do SPDM em atividades comerciais como sistemas embarcados ou utilização em servidores.

**Integrante:** Gustavo Cerqueira Bastos

**Professor(a) Orientador(a):** Prof. Dr. Marcos Antonio Simpicio Jr  
**Co-orientador(a):** Prof. Dr. Bruno de Carvalho Albertini

## Resultados

Os resultados foram compilados de modo que fosse possível observar o uso de memória extra ao se incorporar o protocolo SPDM, o resultado indica viabilidade do uso do protocolo, devido as suas alocações de memória serem suficientemente otimizadas para serem comportadas em uma FPGA (funcionando como um sistema embarcado). Usualmente se gasta pouco mais de 80KB para comportar uma autenticação do SPDM, isto incluindo tanto as funções de autenticado e autenticador.

```
----- L1ft0ff! -----
OpenSBI v0.8-703-g84c6dc1
OpenSBI
Platform Name       : freechips,rocketchip-unknown
Platform Features  : medeleg
Platform HART Count : 1
Platform IPI Device : aclint-mswi
Platform Timer Device : aclint-mtimer @ 500000Hz
Platform Console Device : litex_uart
Platform HSM Device  : ---
Platform PMU Device  : ---
Platform Reboot Device : ---
Platform Shutdown Device : ---
Platform Suspend Device : ---
Platform CPPC Device  : ---
Firmware Base       : 0x80000000
```