Processo de Engenharia de Software Crítico

22 Novembro 2023

Nesta palestra, foi abordado o tema de processos de engenharia de software critico. Os palestrantes começaram a definir engenharia de sistemas como uma abordagem interdisciplinar para criar sistemas que envolvem: engenharia de requisitos, verificação, hardware, software, fatores humanos, *soft-systems* e gestão de projetos. É importante aplicar controlo e disciplina ao longo do ciclo de vida do desenvolvimento de sistemas. Isto pode ser alcançado usando o modelo "V" e através de abordagens com *Agile* ou abordagens híbridas como *Agile+Waterfall.*

A segurança funcional é crucial em domínios como automóvel, ferroviário, dispositivos médicos, defesa, aeroespacial e espacial. Na palestra foi destacado a necessidade de gestão de risco, identificando ameaças e impactos. E, no caso de software, o ênfase deve estar no processo de desenvolvimento mais do que no produto final.

Os palestrantes discutiram casos de uso específicos, como o controlo do barramento energia, o sistema de trem do Boeing 787-10 e projetos ferroviários, enfatizando os padrões de segurança e as abordagens de desenvolvimento.
No final da palestra, foi explorado a ligação entre segurança e cibersegurança e a importância de considerar ambas para garantir a fiabilidade dos sistemas.

Dentro do contexto da segurança funcional, acho que é importante destacar a importância da análise de riscos, como por exemplo a abordagem SIL (Safety Integrity Level). A compreensão destas abordagens e usando técnicas de análise de riscos vai, não só, permitir que o desenvolvimento tenha mais detalhe na definição de medidas de segurança, mas também que o desenvolvimento de sistemas seja mais estável.

Uma ideia inovadora, relacionado com a ligação entre segurança e cibersegurança, seria desenvolver uma ferramenta para integrar avaliações de segurança durante o processo de desenvolvimento do sistema.
Esta ferramenta iria analisar tanto a exposição a ameaças cibernéticas como a eficácia das medidas de segurança (podendo se adaptar dinamicamente) para manter a segurança do sistema.

Carlos Rijo – 1101626