Security and DevOps – reducing risks and surprises with formal code verification

As the adoption of DevOps practices in space applications continues to grow, organizations face the challenge of maintaining good code quality while keeping up with the rapid pace of development. One popular technique to monitor code quality is Static Code Analysis, a technique that analyses the source code and automatically identifies defects and bad patterns without requiring execution or test cases. However, this is not enough to ensure good code quality. In this talk we discuss how developers can thoroughly control and eliminate the risk of software failure and security issues. We present state-of-the-art code analysis tools based on formal methods, which can mathematically prove the absence of defects and vulnerabilities, instead of just finding patterns. We explore the benefits and challenges of formal code verification in a DevOps environment, specifically focusing on how it can be used efficiently, and help to reduce needless efforts and design iterations.