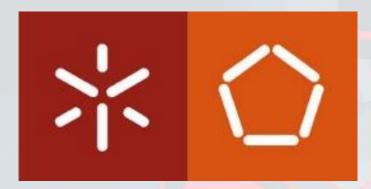
Formalizing ROS2 security configuration with Alloy

Master Dissertation in Informatics Engineering

Luís Mário Macedo Ribeiro



Universidade do Minho
Escola de Engenharia
Departamento de Informática

Introduction

☐ Automation into the industrial world ☐ Software development in Robotics □ Complexity and Middleware as solution ☐ The Robot Operating System ☐ Lack of support for safety-critical and real-time systems ☐ The creation of ROS2 and the integration with DDS ☐ Software Verification ☐ Formal Methods ☐ Model Checking and property verification ☐ The purpose of this dissertation

The Alloy Framework

- ☐ Quality Assurance on Robotic Systems
 - ☐ Usage of formal methods and verification techniques
 - ☐ Automate analysis to avoid security-critical faults
- Model Checking
 - Software verification approach
 - ☐ Behaviour specification through temporal logic
- ☐ The Alloy Framework
 - Structural and Behavioural Modelling
 - ☐ Analysis Commands and Alloy Analyzer

Software Development in ROS2

- ☐ Former Architecture Approach
- □ ROS2 with DDS as communication middleware
 - □ DDS Architecture
 - ☐ ROS2 Architecture
- ☐ Security Analysis
 - ☐ Former problems and analysis
 - □ DDS-Security specification and its security Plugin Infrastructure
 - ☐ SROS2 Enclaves and Access Control

Related Work

- ☐ Security in ROS
 - Exploiting techniques
 - ☐ Solutions regarding security deployment in ROS
 - □ DDS integration and ROS2
 - ROS2 security evaluation works
- ☐ Verification of Robotic Systems
 - ☐ Static Analysis
 - ☐ HAROS
 - Model Checking in ROS
 - Model Checking in other robotics software

Future Work

- ☐ Study of SROS2-related Security Properties
- ☐ Core Techniques Definition
- Evaluation
- ☐ Implementation
- □ Writing

TASKS	February	March	April	Мау	June	July
SROS Security Discussion						
Core Techniques Definition						
Evaluation						
Implementation						
Writing						