Verification of Safe & Secure Systems using Formal Specification - An Introduction

Mairead Meagher

Waterford Institute of Technology,

2017

Waterford Institute *of* Technology

Overview of Safe, Secure Systems and Formal Methods

- Motivation for Safe and Secure Systems
  - Safety-critical and Mission-critical systems
  - Why systems fail
  - Why writing correct software is difficult
  - Organizational and Technical Approaches
- What are Formal Methods?
  - Languages,Tools and Methodologies
  - Application Domains and Environment Assumptions
- Stages of the Formal Process
  - Formal Specification
  - Design and Development

Overview of Safe, Secure Systems and Formal Methods

- Formal Specification
  - Specification Styles
    - Declarative vs operational specifications
    - Partial vs Total models
    - Deterministic vs non-deterministic models
    - Abstract vs concrete models
  - Types of Formal Specification Notations
    - Model-BasedSpecifications
    - Algebraic Specification Languages
    - ProcessAlgebra

Overview of Safe, Secure Systems and Formal Methods

- The Z Notation
  - What is a Z Specification?
  - Where did it come from?
  - The Mathematics of Z
- Structuring Specifications
  - Top-level structures
- Limitations of Formal Specifications
- Two short Examples

Any questions?

Irgendwelche Fragen?

Aon céisteanna?