Rigorous Digital Engineering

Advancing Assurance in Critical Systems

What is Rigorous Digital Engineering (RDE)?

RDE is a modern approach that integrates formal methods, digital models, and engineering processes to build trustworthy, high-assurance systems.

- **Rigorous**: Uses formal reasoning and verification
- **Digital**: Builds and connects digital models (twins and threads)
- **Engineering**: Applies across software, hardware, systems, safety, and more

Why RDE?

- Reduces development effort and cost
- Improves quality and reduces bugs
- Supports certification and regulatory review
- Encourages early discovery of design flaws
- Increases system assurance and traceability

Core Components of RDE

- **Formal Methods**: Proofs, model checking, contracts
- **Digital Twins**: Executable models of physical systems
- **Digital Threads**: Traceable links between design, implementation, and evidence
- **Model-Based Engineering (MBE)**: Systematic use of models for design and analysis

Example Impacts of RDE

- Shifts focus “left” (earlier in lifecycle) and “up” (to abstraction)
- Enables faster prototyping and iteration
- Minimizes defects and rework
- Enhances confidence in system safety and correctness

Tools & Technologies in RDE

- **Programming**: C, C++, Rust, Haskell, Java, VHDL, SystemVerilog
- **Modeling**: SysML, AADL, UML, F*, ACSL, Alloy, Event-B
- **Formal Reasoning**: Coq, Isabelle, PVS, Frama-C, SAW, UPPAAL
- **IDEs**: Eclipse, VS Code, Rodin, OSATE, Crescendo
- **Platforms**: RTOS, seL4, RISC-V, FPGAs

RDE in Practice

- Emphasizes **design-by-contract** and **correct-by-construction**
- Bridges modeling, simulation, and physical deployment
- Applies equally to software, firmware, and hardware systems
- Generates artifacts suitable for automated analysis and verification

Future of Engineering with RDE

- Increasing automation in assurance evidence generation
- Improved tool integration and model traceability
- Education and training to mainstream RDE practices
- Wider adoption in regulatory and safety-critical contexts

Takeaways

- RDE brings **formal rigor**, **digital precision**, and **engineering discipline** together
- It's **not hype**—it's a proven method to build **trustworthy critical systems**
- Adoption leads to **better, safer, and more efficient** engineering outcomes

Questions & Discussion

Let's explore how RDE can help shape the future of your systems.