Systems Engineering & Design Space Exploration based on the Correctness by Construction Methodology

Dr. Robert Hilbrich
German Aerospace Center (DLR)
German Aerospace Center
Research Institution, Space Agency and Project Management Agency

- Aeronautics
- Space Research and Technology
- Transport
- Energy
- Defense and Security
- Space Administration
- Project Management Agency
Current Research Project: aramis II

DEVELOPMENT PROCESSES | TOOLS | PLATFORMS
FOR SAFETY-CRITICAL MULTICORE SYSTEMS

STRUCTURED MULTICORE DEVELOPMENT
MULTICORE METHODS AND TOOLS
INDUSTRIAL PLATFORMS FOR MULTICORE SYSTEMS
Correctness by Construction

an engineering paradigm for complex safety-critical systems
Trends and Challenges in Safety-Critical Systems

• More (safety-related) functions in software
  • The average (embedded) device now has one million lines of code, and that number is doubling every two years.
  • A modern passenger jet, such as a Boeing 777, depends on 4 million lines of code. Older planes such as a Boeing 747 had only 400,000 lines of code.

• Demand for less power consumption, less weight, less space
• Shorter development cycles

• Solution:
  • Powerful hardware components: multicore processors
  • “Active” migration necessary
  • Increasing “function density”
  • Increased probability for errors and fault propagation
Are our engineering foundations adequate to handle the increasing complexity AND increasing safety requirements?
Engineering Tasks and Responsibilities

V-Model for Systems Engineering
FHWA-JPO-05-072, Federal Highway Administration (FHWA), 2005
Limits of Automated Analysis Tools

- Validation requirements are increasing
- Multicore and Parallelism increase complexity
- Space of possible system states is huge(!)

- Current analysis tools are not powerful enough to reach sufficient state coverage

- Idea:
  Argue the correctness of a system based on its **construction process** and not (primarily) on an analysis of its behavior!
Engineering Tasks and Responsibilities

V-Model for Systems Engineering
FHWA-JPO-05-072, Federal Highway Administration (FHWA), 2005
Correctness by Construction (CbyC)

Where does it come from?

Correctness by Construction: A Manifesto for High-Integrity Software

Martin Croxford and Dr. Roderick Chapman
Praxis High Integrity Systems

High-integrity software systems are often so large that conventional development processes cannot get anywhere near achieving tolerable defect rates. This article presents an approach that has delivered software with very low defect rates cost-effectively. We describe the technical details of the approach and the results achieved, and discuss how to overcome barriers to adopting such best practice approaches. We conclude by observing that where such approaches are compatible and can be deployed in combination, we have the opportunity to realize the extremely low defect rates needed for high integrity software composed of many million lines of code.

The National Institute of Standards and Technology (NIST) reported in 2002 that low quality software costs the U.S. economy $60 billion per year [1]. According to the aptly named “Chaos Maturity of Approach” section, the CbyC approach has two primary origins from Praxis High Integrity Systems.

Why did I not hear about CbyC before?

Martin Croxford and Dr. Roderick Chapman, 2005 (see: http://dl.acm.org/citation.cfm?id=1151820)
Our Research Goal

1. Apply CbyC to Systems Engineering & Design Space Exploration
2. Bridge the gap between formal methods & engineering practice

Starting Point:
- Automation of a complex and error prone synthesis task with safety requirements to satisfy
- Deployment of Software Components to Processing Cores (“Mapping”)

- Software Tool
- Specify Mapping Problem in Domain Specific Language
- Automatic Solution Search & Optimization

• How?
  • **Automatic** transformation of the specification into a “Constraint Satisfaction Problem (CSP)”
  • Uses CHOCO Solver (Open Source!)
  • Solutions can be formally proven to be correct(!)
  • Very efficient modeling!
  • Quickly modified for special requirements

• Technical Requirements of ASSIST:
  • Runs on Linux, Windows, OSX
  • Works on regular Laptop
  • Open Source License (soon: Eclipse Foundation)
  • Url: [http://assist.hilbri.ch](http://assist.hilbri.ch)

- Experiences in practice
  - Textual input was very welcome! (precise, efficient, Excel export, …)
  - Significant reduction of engineering effort (3 – 12 person months → 10 mins with ASSIST)
  - Very valuable for Systems Engineer to have several solutions and quickly explore alternatives
Summary

- Correctness by Construction – an engineering paradigm to help you when analysis tools reach the limit of their capability

- Complex synthesis tasks can be automated


- Successful application in real-world use-cases
Any Questions