Compositional Correctness by Dezyne

MDENET Symposium

Rutger van Beusekom (CTO Verum)[1]

December 1st, 2022

verum.

[1] rutger{@dezyne.org,.van.beusekom@verum.com}

Breakdown

Simon (Sinek) Says: "Start with Why"

- Why: Make Software Design an Engineering Discipline
- How: Take Formal Methods Mainstream
- What: Compositional Correctness by Dezyne

verum.

Software Spectrum

Programs as Statements

- Transform Input to Output
- Finish
- Produce a Single Result
- Sequential
- Deterministic
- Sum of its parts

verum.

Software Spectrum

Programs as Statements

- Transform Input to Output
- Finish
- Produce a Single Result
- Sequential
- Deterministic
- Sum of its parts

Software Systems

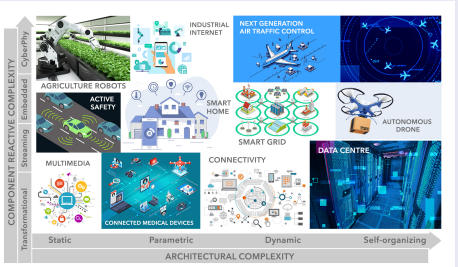
- Transform(State) Input to Output
- Continuous
- Reactive
- Concurrent
- Non-deterministic
- Emergent behaviour

verum.

Our (Collective) Challenge in Engineering the Systems of the Future

Resolving Conflicting Demands

- Productivity
- Correctness

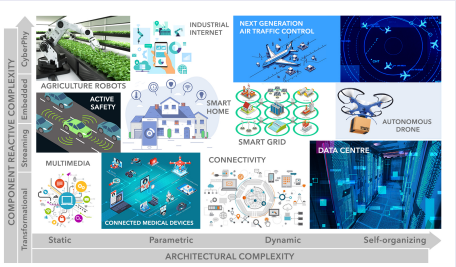


verum.

Our (Collective) Challenge in Engineering the Systems of the Future

Resolving Conflicting Demands

- Productivity
- Correctness

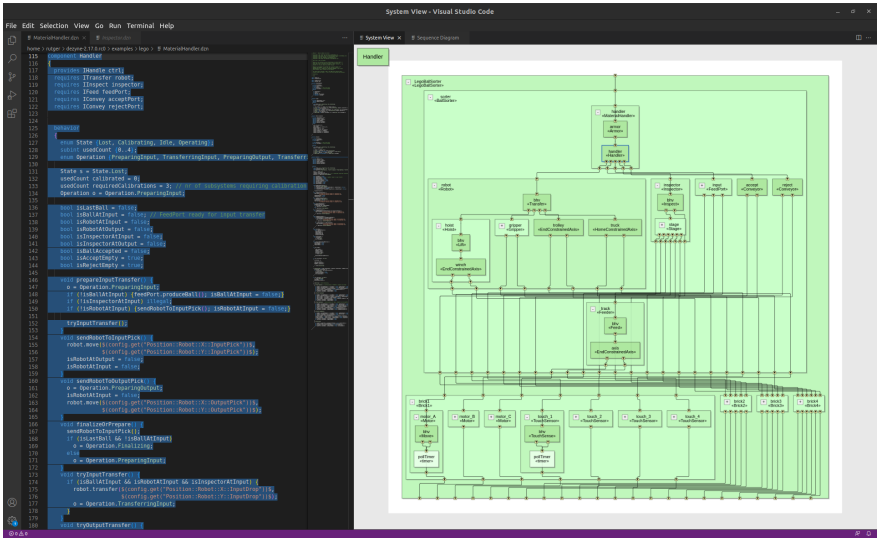


Manage Complexity through Rigorous Design

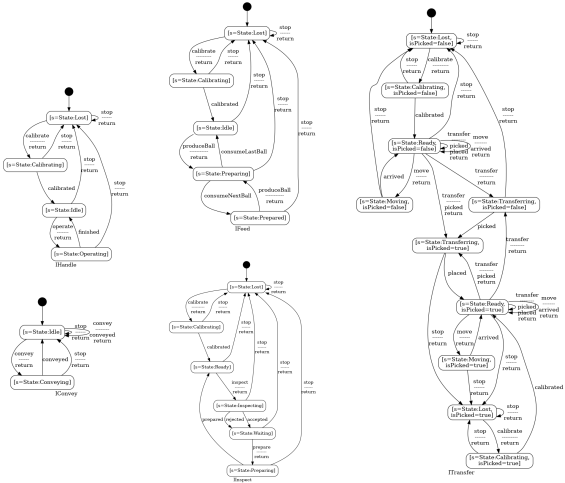
- Formalizing and Validating Requirements
- Design Top down
  - Stepwise Refinement
  - Verifiable
- Construct Bottom up
  - Composition
  - Correct by Construction

verum.

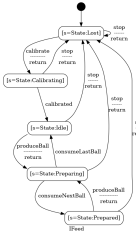
Language for Structure & Behaviour

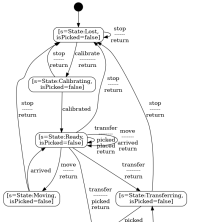


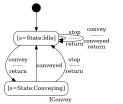
State Space

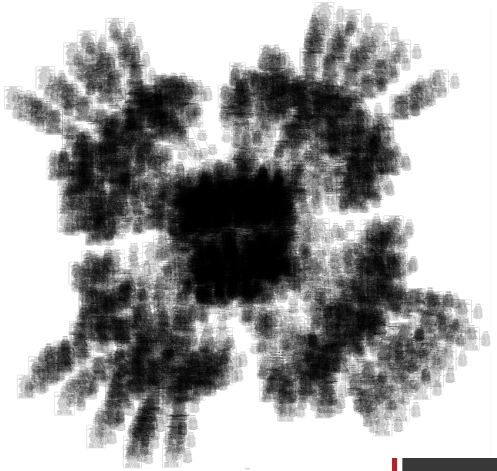

[s=State:Lost]
stop / return
calibrate / return
[s=State:Calibrating]
calibrated
[s=State:Idle]
operate / return
finished / return
[s=State:Operating]
IHandle
[s=State:Lost]
calibrate / return
[s=State:Calibrating]
calibrated
[s=State:Idle]
produceBall / return
consumeLastBall
[s=State:Preparing]
consumeNextBall
produceBall / return
[s=State:Prepared]
IFeed
[s=State:Lost, isPicked=false]
[s=State:Calibrating, isPicked=false]
[s=State:Ready, isPicked=false]
pickedUp / return
move / arrived / return
[s=State:Moving, isPicked=false]
transfer / return
[s=State:Transferring, isPicked=false]
picked / return
[s=State:Transferring, isPicked=true]
placed / transfer / picked / return
[s=State:Ready, isPicked=true]
[s=State:Moving, isPicked=true]
[s=State:Lost, isPicked=true]
[s=State:Calibrating, isPicked=true]
ITransfer
[s=State:Idle]
convey / return
conveyed / return
[s=State:Conveying]
IConvey
[s=State:Lost]
[s=State:Calibrating]
calibrated
[s=State:Ready]
inspect / return
[s=State:Inspecting]
prepared / rejected / accepted
[s=State:Waiting]
prepare / return
[s=State:Preparing]
Respect

State Space Explosion



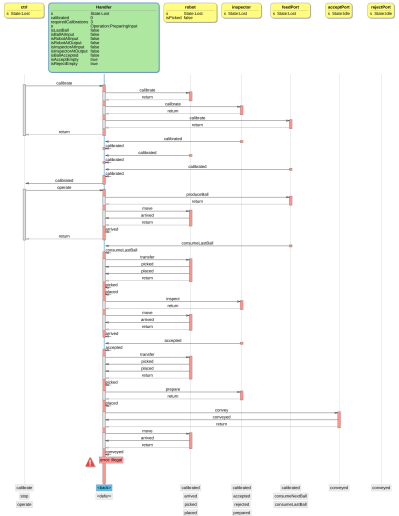






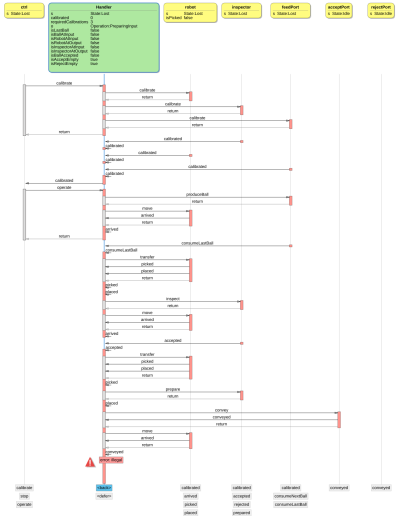
verum.

Model Checking and Divide and Conquer to the Rescue



verum.

Model Checking and Divide and Conquer to the Rescue



Compositional Correctness

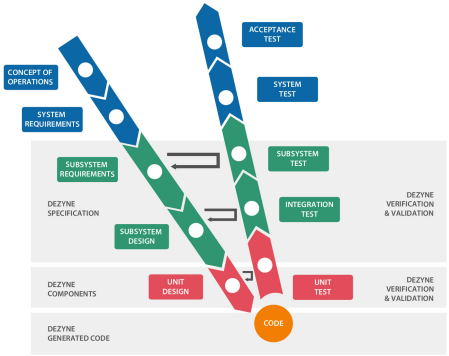
- Interfaces: Design by Contract
- Components fully encapsulated by Interfaces
- Construct Systems from Verified Components

verum.

Verum Industrial Customers

Multinationals

- Semiconductor
- Healthcare
- Automotive



verum.

Want to know more or give it a try?

Dezyne is FREE (as in freedom, not as in lunch) software

Visit

`https://dezyne.org`

`https://download.verum.com`

verum.

Want to know more or give it a try?

Dezyne is FREE (as in freedom, not as in lunch) software

Visit

`https://dezyne.org`

`https://download.verum.com`

Roadmap

- Constraining Interfaces (1st Release Candidate)
- Shared Interface State (Working prototype)
- Module Specification (Proof of concept)
- Functional Verification (Proof of concept)
- Data Contracts
- Legacy Transformation
- Model Based Refactoring

verum.

verum.

FYI (For Your Inspiration)

Some Epigrams by Alan J. Perlis

- Every program is a part of some other program and rarely fits.
- It is easier to write an incorrect program than understand a correct one.
- A programming language is low level when its programs require attention to the irrelevant.
- Programmers are not to be measured by their ingenuity and their logic but by the completeness of their case analysis.
- Fools ignore complexity. Pragmatists suffer it. Some avoid it. Geniuses remove it.
- `http://www.cs.yale.edu/homes/perlis-alan/quotes.html`

verum.