

Who's checking your products DNA?



The simple way to build
complex software
systems

DNA defines complex organisms. If DNA is defective, the results can be disastrous.

Software is the DNA of your product. How do you know it's defect free?

ASD:Suite is the solution. It ensures your product's DNA is correct.

How ASD can save the embedded software industry.

Verum has invented a new (patent pending) technology for designing and mathematically verifying the correctness and completeness of complex software systems. This technology is called Analytical Software Design (ASD).

ASD blends new methods invented by Verum co-founder Guy Broadfoot with a number of existing methods originating from the University of Oxford and IBM. The result is a technology that allows designs of complex software systems to be modelled and mathematically verified for completeness, correctness and conformance to specification before a single line of code has been written.

ASD forms a bridge between a series of useful but informal methods invented in industry – such as Sequence-Based Specification (SBS), Box Structure Development Method (BSDM) and Statistical Testing – and some extremely powerful techniques invented in academia, including the Communicating Sequential Processes (CSP) language and the Failure Divergence Refinement (FDR) model checking tool.

The industrial methods form an efficient, accessible way of rigorously specifying a complete design for a software system, easily understood by industrial stakeholders. But on their own these methods do not go far enough: they cannot, for instance, be used to determine the dynamic correctness of a software design – i.e. whether the design will behave correctly under all circumstances.

CSP is a formal modelling language – a process algebra – that allows complex behaviour to be modelled and checked for correctness under all circumstances. It is an exceedingly powerful way of modelling complex behaviour, but is also esoteric and inaccessible to the average software engineer.

Verum's unique ASD technology means that software designs can now be created using efficient, accessible SBS/BSDM to ensure their mathematical completeness, and then translated into CSP where they can be checked for mathematical correctness. The result is a method for the design of behaviourally complex software systems that it is efficient, economic and accessible, and yet mathematically rigorous.

Once the design has been shown to be defect free by model checking, a large percentage of source code can be generated directly from the SBS design models. Typically 95% of the code can be produced automatically. For the remaining code that needs to be written by hand, specifications and test cases can be generated directly from the design model.

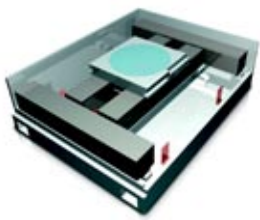
ASD is not just another technique that assists developers to create embedded software with fewer defects. It eliminates the defects and guarantees the software's correctness.

“ ASD is a formal method that is informal enough to be applied in practice”

See www.verum.com for further information or contact us at info@verum.com

ASD Advantages & Benefits

MagLev Stage Software
Design for Philips
Applied



Customer Conclusions:

The application of ASD is cost neutral over conventional design methods during the first half of the project lifecycle.

The application of ASD results in a factor 12 reduction in defects found during initial integration testing.

The application of ASD results in a predictable completion date for the project.

Applying ASD provides you with the means to:

- Verify automatically that functional specifications comply with safety cases before design and implementation;
- Verify automatically that designs meet functional specification before implementation;
- Analyze behavior between components for deadlocks, race conditions, non-determinism, divergence and correctness before implementation;
- CSP models are generated automatically from ASD specifications - Economic
 - no need to verify models against specifications;
 - CSP model traceability is not an issue;
 - queue models generated automatically;
- Stakeholders understand the specifications

Verum's ASD Software Development Suite is compatible with existing development environments - mathematical expertise less important.

Mathematically verified software results in a number of benefits:

Benefit

Risk Reduction

Effort and Time-to-Market Reduction

Increased Quality

ASD Design & Modelling

Guarantees conformance to specification.

First-time-right architecture & design.

Eliminates the majority of (complex) design defects.

Automatic Code Generation

Accelerates incremental development.

Reduces effort and duration.

Eliminates defects caused by human factors.

See www.verum.com for further information or contact us at info@verum.com