D-RisQ have harnessed the power of Formal Methods mathematics to develop automated development tools which ensure against unwanted systems behaviour, provide the certification evidence, and by reducing the need for test, save up to 80% of the development time and cost.

Software systems fail. Currently the standard way to mitigate some of the risk of failure is by extensive testing and verification, typically 70% of the cost of a systems development. In safety critical or business critical environments the cost of failure can be high in terms of reputation, money and potentially, lives. In parallel, regulation, insurance and corporate governance is driving ever stricter compliance regimes.

D-RisQ is bringing over 200 man years of development effort for the UK MoD to the commercial market with an integrated set of automated development tools. These tools will operate at the requirements capture level, C-Code level and Object Code level to ensure systems only behave in the way they are designed and do nothing else, and then provide the certification evidence to prove it.

The tools utilise the formal proof inherent in Formal Methods mathematics, a technique which has up until now, been in the unique domain of academia. Sitting behind standard systems and software design tools, Modelworks®, ClawZ® and Fever will provide the designer with the output showing when any unwanted behaviour of the design exists. This proof negates the need for extensive software testing and provides the evidence of correct behaviour for regulatory authorities.

The developer can then trust that the design output will be right first time. Costs and time will be saved by overcoming the need for rework necessary as a result of bugs, faults and failures which would normally be found much later in the test and verification process. The technique is equally applicable to the detection of any unwanted code attributable to Malware and metamorphic viruses.

D-RisQ is a closely knit SME in the Severn Valley Cyber cluster and has been operating for 3 years. Its current major consulting contracts in support of the development of the toolset are in automotive (JLR, Ricardo, Johnson Matthey Battery Systems), IT (resilience of critical infrastructure), Robotics and Autonomy.

Although safety critical applications have the most obvious need to be free of software failure, the consequences for all systems developers is clear with recent software failures in banking, transport and medical making news headlines and putting companies reputation at risk.

D-RisQ Ltd.
Wyche Innovation Centre
Walwyn Road, Upper Colwall
Malvern, Worcestershire, WR13 6PL
+44 (0) 1684 252452
www.drisq.com

Features
- Automated tools invisible to the developer
- Stand alone tools or integrated from top to bottom in the development cycle
- Eliminates unwanted systems behaviour
- Detects unwanted design or code
- Provides regulatory evidence
- Reduces drastically the need for software testing
- Saves up to 80% of the development cost

D-RisQ Toolset
- **Modelworks®** (Sept 15)
  - Based upon model checking IP from Oxford University
  - Front end using UML or Stateflow
  - Shows that requirements/system behaviours (e.g. HAVE to, NEVER, failure) are instantiated in the design
- **ClawZ®** (Sept 16)
  - Based upon a proprietary theorem prover
  - Front end using Simulink & Stateflow
  - Automatically shows that generated code correctly implements the design
- **Fever** (Sept 17)
  - Automatically shows that object code correctly implements the design
- **Consultancy**
  - Working with clients to harness D-RisQ tools and techniques in their own bespoke environments

www.drisq.com