MATISSE - Methodologies and Tools for Industrial Strength Systems Engineering

Colin O’Halloran
Systems Assurance Group
KI Systems
QinetiQ
Malvern Technology Park
MATISSE partners

- QinetiQ (lead partner with Formal Systems as subcontractor)
- CNRS (Scientific co-ordinator)
- Gemplus (Industrial Partner)
- Siemens Transport International (Industrial Partner)
- Aabo Akademi (working with Wallac as industrial partner)
- ClearSy (B tool provider, J.R. Abrial consultant)
- Southampton University (Academic Partner)
MATISSE approach

• MATISSE project is exploiting and enhancing existing generic methodologies and associated technologies that support the correct construction of software-based systems.

• Strong emphasis is placed on
  – the B Method and its associated technology
  – as well as CSP and its associated model checker FDR.

• Other methods and tools are also being exploited such as
  – UML and Action Systems
Workpackages

- Methodology
- Tools
- A liquid handling workstation for healthcare clinicians and researchers
- A railway signalling and control system
- An embedded verifier for a smartcard
Achievements

- “Strawman” Methodology Handbook has been produced.
- Initial requirements for tools and enhancements identified
  - B0 translator to C (developed for smartcard constraints)
  - U2B tool for translating UML to B (B2UML required)
  - B2CORBA
  - Automatic verification of automatically generated code (under investigation)
- Common evaluation plan for case studies to measure effectiveness of methodology and tools.
Advertisement

Satellite Refinement Workshop organised by MATISSE at the ZB conference at Grenoble in January