Contract-based design, model checking, and model-based safety assessment
An integrated view

Marco Bozzano, Alessandro Cimatti, Stefano Tonetta
Fondazione Bruno Kessler, Trento, Italy
Take away message

• Beyond model checking: new generation of verification techniques
• Tools integrated into structured flow
• May provide integrated backend support for assurance by producing relevant artifacts from unique model

• From model checking to ...
  • Contract-based design
    • architectural decomposition + refinement of requirements
  • Safety analysis
    • Extend nominal model to include faulty behaviours
    • Fault Tree construction: detect all fault combinations causing loss of desirable property
From architectural decomposition to contract-based design

• Hierarchical decomposition
  • Component to subcomponents
  • Implementation of leaf components

• Component associated with contracts
  • Assumptions / guarantees
  • Temporal logic

• Contracts refinement
  • Contract ensured by contract of subcomponents

• Correct implementations ensure correctness of composition
Model-based safety assessment

• Safety assessment
  – Analyze behaviour of system under faults
  – Artifacts: Fault Trees, FMEA tables
  – Qualitative and quantitative arguments

• Model-based Safety Assessment
  – Extend nominal model with faults
    • Symbolic fault injection
    • Valve stuck open, stuck closed, ...
  – Analyze extended model
    • Automated production of FT
Formal Verification, Validation, and Safety Assessment

Model Checking

\[ \mathcal{M} \models \varphi \]

Verification & Validation

Safety Assessment
Formal Verification, Validation, and Safety Assessment

\[ M \models \varphi\]

\[ M \rightarrow M[F] \]

Verification & Validation

Safety Assessment
Formal Verification, Validation, and Safety Assessment

Model Checking:
\[ M \models \varphi \]

Fault Injection:
\[ M \rightarrow M[\mathcal{F}] \]

Model-Based Safety Assessment:
\[ \delta(\mathcal{F}) : M[\mathcal{F}] \not\models \varphi \]

Verification & Validation

Safety Assessment
Formal Verification, Validation, and Safety Assessment

Model Checking: $\mathcal{M} \models \varphi$

Fault Injection: $\mathcal{M} \rightarrow \mathcal{M}[F]$

Model-Based Safety Assessment: $\delta(F) : \mathcal{M}[F] \not\models \varphi$
Formal Verification, Validation, and Safety Assessment

Contract-Based Design

Model Checking

\[ M \models \varphi \]

Fault Injection

\[ M \Rightarrow M[F] \]

Model-Based Safety Assessment

\[ \delta(F) : M[F] \not\models \varphi \]

Verification & Validation

Safety Assessment

July 18, 2015

VeriSure Workshop @ CAV’2015
Formal Verification, Validation, and Safety Assessment

Contract-Based Design

Compositional

Model Checking

\[ M \models \phi \]

Fault Injection

\[ M \rightarrow M[F] \]

Model-Based Safety Assessment

\[ \delta(F) : M[F] \not\models \phi \]

Verification & Validation

Safety Assessment

July 18, 2015

VeriSure Workshop @ CAV’2015
Formal Verification, Validation, and Safety Assessment

Contract-Based Design

Model Checking

\[ \mathcal{M} \models \varphi \]

Verification & Validation

Fault Injection

\[ \mathcal{M} \Rightarrow \mathcal{M}[\mathcal{F}] \]

Safety Assessment

Fault Injection

\[ \delta(\mathcal{F}) : \mathcal{M}[\mathcal{F}] \not\models \varphi \]

Model-Based Safety Assessment

Contract-Based Safety Assessment

July 18, 2015

VeriSure Workshop @ CAV'2015
Tool chain

• Infinite-state transition systems
  • The **OCRA** tool for contract-based design
    • http://ocra.fbk.eu/
  • The **nuXmv** model checker
    • http://nuxmv.fbk.eu/
  • The **xSAP** platform for safety analysis
    • [http://nuxmv.fbk.eu/](http://nuxmv.fbk.eu/)

• Hybrid systems
  • **HyCOMP** as a model checker
    • http://hycomp.fbk.eu/
Applications

• Joint project with Boeing on MBSA
  • Formal Design and Safety Analysis of AIR6110 Wheel Brake System [CAV’15]

• Adopted in NASA project on analysis of NextGen
  • Comparing Different Functional Allocations in Automated Air Traffic Control Design [FMCAD’15]

• The COMPASS tool chain
  • AADL modeling language
  • Several projects funded by the European Space Agency
Conclusions and Perspective

• Conclusions
  • New generation of verification techniques
  • Tools integrated into comprehensive process
  • Production of interesting artifacts from unique model

• Integration with assurance? Relevant issues:
  • Tool qualification non trivial
    • One tool vs multiple tools? Tool-to-tool transitions?
  • High level proof production
  • Support to reuse