ReSIST NoE

Resilience for Survivability in IST

SIXTH FRAMEWORK PROGRAMME

Modelling and Evaluation of Largeness in Evolving Systems

Andrea Bondavalli

University of Firenze (here PISA)

Introduction

Systems **complexity** has always been a very critical issue and is becoming even worse in modern infrastructures and systems.

When modelling such systems, complexity of the resulting models depends on the
- dependability measures to be evaluated,
- the modelling level of detail, and
- the stochastic dependencies among the components.

State-space models are commonly used and require a very high number of states for the modelling and complex and costly analytical techniques, or simulation for they solution

The **large size** of models known as the **'state space explosion problem'** is one of the major difficulties in the dependability evaluation of real systems.

Information Society Technologies

How to cope with Largeness

SIXTH FRAMEWORK PROGRAMME

Much work done and progress made in addressing such problems at the model construction and model solution levels.

These are complementary and both are needed to generate and process detailed and large dependability models for the evaluation of the resilience of real life systems.

In the rest of the presentation we will illustrate

- Three main classes of structured techniques for a modular model construction.
- Model solution techniques.
- Specific methods developed to deal with such large and evolving systems taking as examples web, grid and mobile based systems

Information Society Technologies

Model construction techniques

SIXTH FRAMEWORK PROGRAMME

At model construction level, we can identify three approaches:

i) model composition; the system model is constructed in a bottom-up fashion. The models representing parts of the systems are built in isolation, thus having a limited view of the system context.

ii) system decomposition and model aggregation; it follows a top-down approach: starting from an overall view of the system context, the model for the overall system is decomposed in a set of simpler sub-models.

iii) the derivation of dependability models from high-level specifications (based on UML -Unified Modeling Language- or AADL -Architecture Analysis and Design Language- the overall model (e.g., a Markov chain or a Petri net), is built by transformation (usually semi-automatic) from such high level specification.

Composition approaches - Principles

The principle of the composition approach is
- to build complex models in a modular way through a composition of its sub-models
- then solved as a whole.

Most of the works belonging to this class define the rules to be used to construct and interconnect the sub-models
- exploiting the degree of dependency among subcomponents.

These dependencies are used to reduce the model complexity creating, smaller, equivalent representations.

Example

Stepwise refinement approach [Betous-Almeida & Kanoun 2004-a] following the system development refinement process.

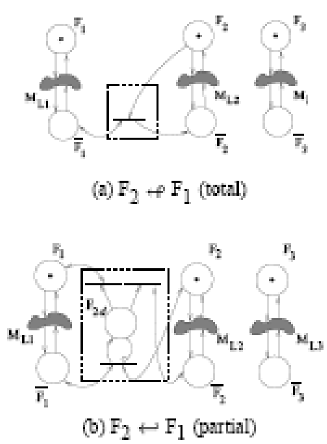


Figure 4. Functional dependencies

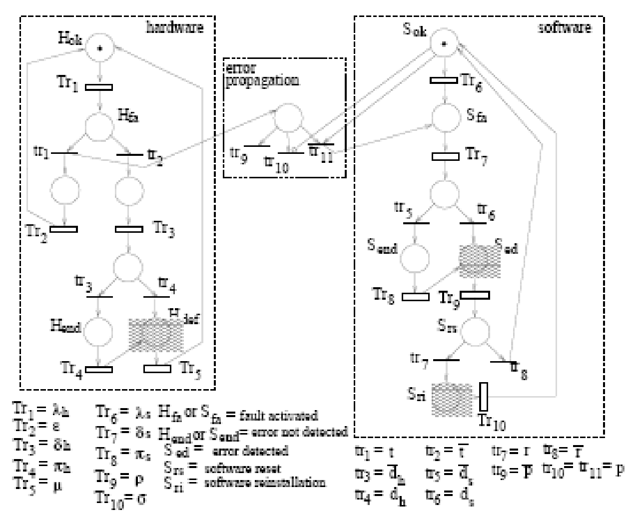


Figure 15. Structural model of a software and a hardware components

Decomposition / aggregation approaches - Principles

Most decomposition and aggregation methods are characterized by a hierarchical decomposition approach

Thus they try to avoid the generation of large models.

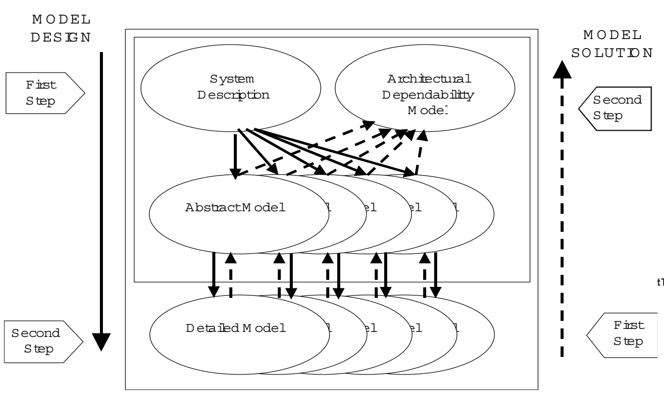
The overall model is decoupled in simpler and more tractable sub-models:

-sub-models are solved separately and

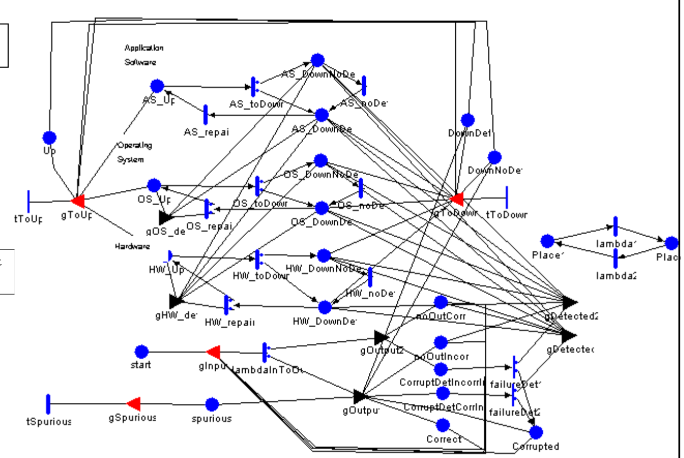
-the measures obtained from the solution of the sub-models are then aggregated to compute the overall measures.

An example:

Decomposition exploiting the hierarchy of control systems [Lollini *et al.* 2005-a], solution carried out in a bottom-up fashion (aggregation).



Detailed generic Model



Derivation from high-level specification

Model-driven engineering are more and more used in industry (in particular UML and AADL)

As system designers use integrated set of methods → approaches have been developed for allowing the (semi-automatic) generation of dependability evaluation models from such model-driven engineering.

Research based on UML:

- The European project HIDE [Majzik & Bondavalli 1998, Bondavalli *et al.* 2001a, Majzik *et al.* 2003] automatic analysis defining several model transformations from structural and behavioural UML diagrams into GSPNs, DSPNs and SRNs.
- The issue of deriving automatically models from UML behavioural specifications, has also been addressed in [Bernardi 2003].
- synthesis of dynamic fault trees (DFT) from UML system models [Pai & Dugan 2002].

AADL has more recently received some interest:

- A stepwise approach for the description of complex dependability models from AADL [Rugina et al. 2006].

Solution approaches

Two main approaches for dealing with largeness at solution time

-largeness avoidance techniques that try to reduce the size of the generated models

-largeness tolerance techniques which make use of space and time efficient algorithms to reduce the storage requirements of the state space and the generator matrix and to optimize the state space exploration, generation and analysis.

It is important to note that largeness avoidance and largeness tolerance techniques are complementary

Both are needed, at model construction and model solution levels each bringing its contribution.

Large and evolving systems

Systems are evolving and becoming more complex and large.

They are also more and more closely interconnected and show increasingly complex interactions.

All this is demanding a continuing evolution and improvement of the modelling and evaluation capabilities in order to quantify their dependability characteristics.

Among types of systems that present these challenges we considered

- Dependability modelling of Web-based systems and services
- QoS analysis of Mobile Telephone Systems
- Service Provisioning and Grid Systems

Dependability modelling of Web-based systems and services

The dependability of the **delivered services as perceived by the users** is a key issue for Internet applications and Web Services

When Internet is used for money critical applications (online banking, stock trading, reservation processing and shopping) Availability (wrt. Accidental & Malicious faults) is critical.

Many measurement-based efforts for the evaluation of the of web hosts [Oppenheimer & Patterson 2002, Kalyanakrishnam et al. 1999], less emphasis put on modelling.

A multi-level approach for modelling the user perceived availability of internet applications considering 4 abstraction levels modeled with various techniques, [Kaâniche *et al.* 2003-a].

Detailed analytical performability models to analyze the availability of web services implemented on cluster architectures. [Martinello et al. 2005]

Dependability modelling of web-based systems and services performed considering a business model workflow [Gönczy et al. 2006]:

QoS analysis of Mobile Telephone Systems

Telephone Systems are getting more and more business critical and complex showing strong interactions with an integrated Information and telecommunication Infrastructure.

Analysis of GPRS by providing a modelling approach to understand the effects of outage periods on the service provision [Porcarelli et. al. 2002, Porcarelli et. al. 2003].

Congestion analysis of GPRS infrastructures consisting of a number of partially overlapping cells [Lollini *et. al.* 2005-b], using QoS indicators as a measure of the service availability perceived by users.

A general approach [Lollini *et. al.* 2006] applicable to cellular systems, including GSM, GPRS and UMTS networks. It enhances the modularity, reusability, scalability and the maintenance of the overall model.

Service Provisioning and Grid Systems

Various novel IT business models depend on adaptive infrastructure mechanisms to share resources, create distributed and collaborative applications, and manage and maintain systems and applications.

Such platforms, (known as grid computing, service provisioning, utility computing, on demand computing) pose various new challenges on evaluation methods and techniques.

In [Jarvis et al. 2004] various new challenges with respect to the performability evaluation of such systems are addressed

In [Palmer & Mitrani 2005], theoretically optimal policies to allocate resources to customers are computed, and compared with a newly proposed heuristic validated and tuned using the experimental system described in [Fisher et al. 2004].

A methodological approach [Machiraju et al. 2002] to systematically introduce metrics for the business' operation and managers. It relies on the concept of 'Quality of Business' [van Moorsel, 2002], and is implemented based on contracts and/or service level agreements (SLAs) [Molina et al. 2005].

Conclusions

- The increasing scale and complexity of modern-day computing systems continues to demand good techniques for the construction and solution of large quantitative models.
- In addition, these large, dynamic and evolving systems pose some **new challenges** that the ReSIST partners aim to address.
- Evaluation methods must deal with metrics at an increasingly high level of abstraction, to express the impact of the computing infrastructure on an enterprise business.
- Of increased significance is also the need of quantitative evaluation methods to support the effective use of adaptation mechanisms prevalent in modern-day systems.