Heterogeneous Modelling Applied in System Security

Petr Hanáček *
hrubym@fit.vutbr.cz

Martin Hrubý*
peringer@fit.vutbr.cz

Zdena Rábová*
rabova@fit.vutbr.cz

Abstract This paper deals with methods and approaches of heterogeneous modelling and its application in risk analysis and modelling. Risk analysis is one of many tools for security improvement. The main idea of that is based on analysis of gathered information about observed company and following searching for some group of countermeasures which can reduce a risk. We start this paper by describing modern aspects of heterogeneity in computer modelling and we continue with an overview of risk analysis in heterogeneous manner.

Keywords: heterogeneous modelling, risk analysis, decision-engineering

1 Introduction

Our paper is oriented to problems of modelling of heterogeneous systems [3]. Model design of these systems is associated with selecting sufficient methods and tools supporting design and realization of models in various application environments. For this reason, it is very advisable to split the modelled heterogeneous system into a set of relatively small subsystems where each of them is going to be described separately; and in followings, the individual subsystems is being solved in its most convenient manner. This approach leads to a set of sub-models which will be then linked all together – into a heterogeneous model. Linking (interconnecting) the sub-models is not a trivial problem. A possible way of doing that has been described in Ph.D. thesis [2], where the sub-models are connected into a special communication net. This net represents a standardised view of each sub-system included in the heterogeneous system. Corresponding sub-models are then mergable to a working aggregate. Certain re-usability of sub-models is one of the greatest benefits of this method.

2 Heterogeneous modelling

As we mentioned above – the heterogeneous model is a model compounded of certain sub-models. Each sub-model may be based on different formalism, method or tool which is best in current context. There are more terms frequently used in the english literature – we may find expressions like a multi-model, a multi-paradigm model or a multi-formalism model.

Prof. Tuncer Ören in his paper [5] introduces a plenty of new terms in theory of computer modelling which defines various specific approaches in modelling:

* Brno University of Technology, Faculty of Information Technology, Božetěchova 2, 612 66, Brno, Czech Republic

– *Multi-models* – group of very close models connected into a one complex model. When such a model is being simulated, only on of sub-models is currently active.
– *Multi-aspect model* – a special case of multi-model, when more sub-models may work simultaneously.
– *Multi-resolution model* – an approach, when for a given problem, more models with a different level of abstraction are created. An user chooses his best level regarding to his particular requirements.
– *Variable structure models* – based on investigating the best structure of a model corresponding to its behaviour.
– *Mixed formalism simulation* – the simulation is followed by another way of knowledge processing (for example – an expert system which supplies the simulation with particular parameters).
– *Multi-simulation* – doing concurrent experiments with more aspects of real system.
– *Concurrent simulation* – the simulation runs concurrently with processes of reality. This approach is oftenly used in systems of predicting an controlling in on-line simulations (for example in systems of control of electricity transport or in public transportation).
– *Goal processing* in modelling and simulation.
– *Automation of design of experiments*.
– *Agent-directed simulation* – modelling based on communicating (heterogeneous) agents.
– *Holonic Agent simulation* (for cooperative systems) – a special type of agent simulation, where the agents (called holons) dynamically change their strategies if there arises a requirement to solve a high priority task.
– *Specification languages* and environments for interoperability.

As we can see, there is a huge range of specific approaches using modularity, integrating a knowledge base, concurrent and interactive simulations, inter-operability and specification (interconnecting) languages of high abstraction. The scientific literature also mentions a multi-formalism term which is probably closest to our view of the heterogeneity. The article refers the HLA platform as a suitable tool for implementation of communicating modules.

2.1 The HLA and CORBA platforms

There are some interconnection platforms for programming distributed computings. Those system architectures (HLA, CORBA) [1] are usually also heterogeneous in meaning of interconnecting the various systems (at level of programming languages, for example).

These platforms physically transport some information from a system to another system. An A application is going to send a message to B application through a special interface: the interface converts the message to some universal format (including the binary level compatibility) and sends that to the opposite interface on the other side. The opposite interface adapts the message to a form acceptable for the B application. But the HLA and CORBA platforms (compared with a general heterogeneity):

– do not bring a general methodology of making a heterogeneous model.
– limit the set of pluggable sub-systems to a relatively small group of supported languages and development environments.

HLA and CORBA can serve as a stabilised and well developed communication layer for some higher heterogeneous technology. Unifying the binary data level, message formats and net protocols are necessary requirements of such a physical communication. The XML language is another possible way of sharing information among the sub-systems.

2.2 The computer system compatibility

Let us extend the application of heterogeneity to wide range of computer systems and especially to:

- *Operating systems*, where the compatibility among the different systems is a really important requirement.
- *Applications* in some operating system where the interconnection is still not satisfactory. The inter-application data transfer is very limited – in fact, it is only a text copy-paste facility. Data can be transmitted for example with the XML standard, but mostly if the both sides and prepared for this communication (similar function is supported by OLE and COM technology).

Implementing all systems in one language or paradigm would be the final solution. The Smalltalk and Self programming environments leads to this situations as they attempt to be an operating system. The world of unified programming language is illusory and probably even not acceptable. Making the applications with a built-in heterogeneous interface would be a good compromise.

2.3 Multi-paradigm languages

In the current time, so-called multi-paradigm languages are just being developed. These languages support more programming paradigms (logic, functional, constraint-bases, object oriented, procedural, parallel). Ole Madsen (the Beta language co-author) wrote in his article [7]: "Our goal in the programming languages research and development should be in integrating of the best concepts and construction of various programming paradigms".

In most of cases, a multi-paradigm language integrates some object oriented procedural language with a logical or functional programming language. The similar connection is also presented in this thesis, but at more general level.

The Oz[6] programming language is very popular, for example. The Oz advantage is in implementing the inference mechanism into the computing, so the programs can be made in combination of deterministic and nondeterministic manner. The OLI language (Objects and Logic Integration) is another representative of this branch (OLI was derived from Smalltalk).

2.4 Design of heterogeneous models

Motivation for the heterogeneous modelling arises from the previous text. Let us comment two approaches to achieve the heterogeneity:

1. **Uniform platform for sub-system interconnection** – that is being solved in [2] and also in this paper. Unified principle of inter-system communication is a big advantage of this approach as well as a formal base of architecture of the resulting system.
2. **Spontaneous approach** – every interconnection of two sub-systems is different. There is no unified communication platform. The communication is limited to sub-systems having their created interfaces. Fragmented and incompatible communication is a certain disadvantage of this solution.

3 System security and process of the risk analysis

We are concentrated on modelling of the risk analysis process of information systems, especially for computerised information systems [4]. In this article, we focus at building suitable risk analysis models, that can be used for security countermeasure choosing.

We would like to present some practical example of computerised risk analysis but it is not very possible. Let us explain why: In the area of risk analyzation, it is rather well known that computerised risk analysis contain some uncertainty and error – but this error is *constant* for all levels of problem complexity. Obviously, in simple cases, a human expert will always design better countermeasure solution than the machine. As the complexity grows, the expert becames less and less precise and efficient, but the machine's error remains constant.

For this reason, we do not bring a case study which would take many pages of text but a general description of all aspects necessary to succeed in particular risk analysing.

3.1 Creating a risk analysis model

In our grant project "Information system security - research of attacks on tamper-resistant cryptographic hardware" which is intended to explore new results in security of information systems we have met a plenty of security laws and specifications for using various sources of information. Their applying to a particular organisation makes a security program which we verify with a suitable model. Such a model has to cover whole activity of the information system including protection and safe distribution of secret data. The vulnerable points have to be identified as well as all possible ways of attack, losses caused by these attacks, available countermeasures and so on. We use these models to verify various security mechanisms – for example verification of some secrete sensitive knowledge (password, personal identification number), verification of ownership of some equipment (key, magnetic or chip card) or verification of physical characteristics (finger-print, eye pattern). This list of all various problems necessary to solve points us to heterogeneous approach.

Because the risk analysis procedure is such a creative, intuitive and systematic process, the tools that are used to model this process must likewise be flexible, to be able to reflect the real-world scenario as true and effectively as possible. Risk analysis often relies in producing numbers and relies insufficiently on human analysis and common sense to interpret the results. The model must place a minimal hindrance on the intuitive, common sense and creative spirit necessary for the risk analysis process.

Because it is not possible to establish the correctness of a risk analysis procedure, it is necessary to ensure that the model is understandable and comprehensible as much as possible. Risk analysis should not be a black box system which "magically" provides answers that need to be trusted. It is necessary for the user to be able to intuitively follow the modelling and reasoning the process of the risk analysis, and in this manner verify the correct functioning of the model.

Generally, the risk analysis model is made of two different parts (Figure 1). This fact also brought us to use our experience in heterogeneous modelling techniques. Let us explain them:

1. System model – defines dependencies between different types of asset, and allows suitable countermeasures to be identified for data assets, physical assets, application assets and locations.
2. Knowledge based behaviour model – describes the relations among asset types, impact/threats, vulnerabilities and countermeasures.

These two sub-models reprezent different views to the same problem and each is described in a specialized way. Our target is to automatically interconnect them and then to compute the risk state by using a prolog-style inference machine.

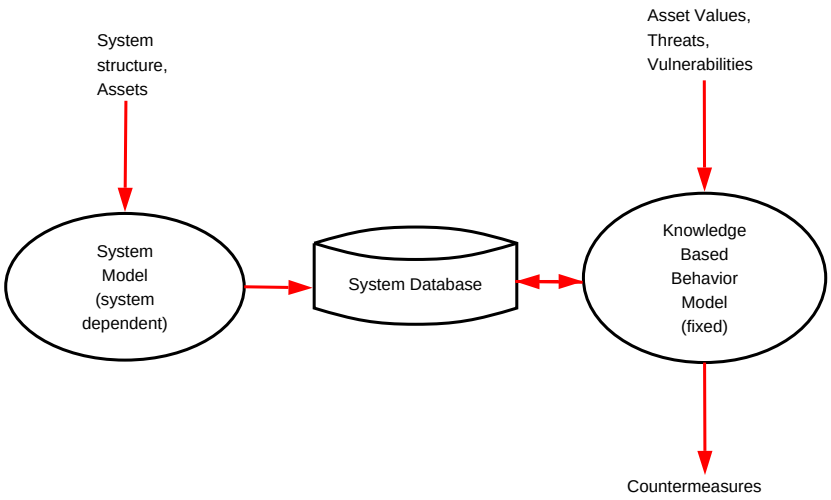

Figure 1: Structure of a risk analysis system

3.2 Risk analysis in industry

Besides the security applications in computer based information systems, we also may describe various risk analysis in the domestic industry. Let us present some aspects of risks in power engineering.

There is a big discussion being held in Czech Republic about security and safety standards in czech energy manufacturing and distributing system. The energy system must be stable in every moment of its functioning. Stability of the energy system depends on many factors. We are going to mention just some of them. In this complex application we recognise two levels of problems:

- Safety – technical stability and efficiency.
- Security – countermeasures against all possible human wanted/accident attacks to the system. Nowadays we also have to include possible terroristic attacks to power plants (especially to nuclear ones), transmition lines and exchange points.

Technical stability means that the energy system creates exactly the amount of energy which is currently being consumed. Less or more production would cause a system failure. Obviously, the consumption is not constant and varies during the day. For this reason, the controling institution has to dispose some reserve (backup) power supplies which are able to fluently and dynamically react to consumption changes. This reserves has to be bought from the energy suppliers (they are ready for instant reaction). The amount of bought reserves determines quolity and stability of the energy system. Keeping a backup reserve of electricity in production cost several billions CZK each year. There is a big effort to optimise necessary amount of reserve in dependence to some coefficient of global safety.

This technical and security analysis should give us:

– Amount of backup power (electricity, services), backup capacity of internal transmition lines and backup capacity of international transmition lines (to Germany, Poland, Slovakia, Austria).
– Cost of keeping the backups – must be optimized with a respect to safety and possible production of electrocity. There are about seven independent markets with backup services solving prices of services.
– Coefficient of global security and safety of the whole system – some unified number coeficient is required to describe current state of the system.
– Level of impact of non-stable power sources like wind generators.

Many government and private institutions cooperate in modelling of the Czech electric power system. Each developed model covers a certain aspect of the solved problem (domestic energy production balance, energy transportation, energy export and import, prices on energy market, long time perspective and others). As we can see, this system is very heterogenous and therefor, the heterogenous interconnections have to be implemented to cover the whole.

4 Summary

In this article, we brought a brief introduction to large area of heterogeneous modelling methods and methods of investigating safety and security of systems. Risk analysis, which is a main part of that, is very important in many types of every-day human activities, computer networks and industry. Analysis of all application goes through the similar process which has been mentioned in this article. Some prototype of general purpose risk analysis engine is going to be one of the results of our project.

This work is supported by the Grant Agency of Czech Republic, grant No. GACR 102/04/0871: "Information system security - research of attacks on tamper-resistant cryptographic hardware" and also by the research project CEZ:J22/98:262200012 “Research in Information and Control Systems”.

Bibliography

1. Buss, A., Jackson, L.: Distributed Simulation Modeling: A Comparison of HLA, CORBA, and RMI, In: Proceedings of 1998 Winter Simulation Conference, 1998
2. Hrubý Martin: Prostředí pro modelování heterogenních systémů, Brno, CZ, FIT VUT, 2004, s. 93, in czech
3. Hrubý Martin, Kočí Radek, Peringer Petr, Rábová Zdenka: Tools for Creating of Multimodels, In: Kybernetes: The International Journal of Systems & Cybernetics, roc. 2002, c. 9, GB, p. 1391-1400, ISSN 0368-492X
4. Hrubý Martin, Peringer Petr, Rábová Zdenka: Modelling of Tamper-Proof Devices, In: Proceedings of 38th International Conference MOSIS’04, Ostrava, CZ, MARQ, 2004, s. 6, ISBN 80-85988-98-4
5. Ören, T.: Future of Modelling and Simulation: Some Development Areas, Proceedings of the 2002 Summer Computer Simulation Conference
6. Muller, M., Muller, T., Roy, P. V.: Multiparadigm Programming in Oz, Tech. report RR 95-16, In: "Workshop Visions for the Future of Logic Programming: Laying the Foundations for a Modern Succesor to Prolog", Portland, Oregon, 1995
7. Madsen, O. L.: Towards a Unified Programming Language, ECOOP 2000, LNCS 1850, pp.1-26, Springer-Verlag Berlin Heidelberg 2000