TECHNICAL FOUNDATIONS FOR QUALITY ASSURANCE OF SYSTEMS ENGINEERING ACTIVITIES FOR SAFETY ASSESSMENT

Tuncer I. Ören
Computer Science Department
University of Ottawa
Ottowa, Ontario
KIN 984, Canada

Maurice S. Elzas
Computer Science Department
Wageningen Agricultural University
Hollandseweg 1, 6706 KN Wageningen
The Netherlands

ABSTRACT

Basic system design axioms and a framework for design and test derivation based on structural design are presented. Over thirty quality assurance issues are elaborated on. New dimensions to quality assurance issues in the artificial intelligence era are discussed. The last part of the article is a sequel of another one titled: "Model reliability and software quality assurance in simulation of nuclear fuel waste management systems" which was published in the Proceedings of the 1985 Waste Management Conference (1).

INTRODUCTION

Safe disposal of nuclear fuel waste is one of the most challenging engineering tasks and necessitates as well as deserves application of advanced concepts of system design, modelling, simulation, and software engineering in different aspects of the safety assessment.

In a previous article, we presented a systematic view of model reliability and software quality assurance in simulation of nuclear fuel waste management systems (1). In this article, focus is on quality assurance of systems engineering activities for safety assessment and on a systemization of the relevant and desirable advanced quality assurance issues.

SYSTEM DESIGN AND ITS AXIOMS

From a systems engineering or systems approach viewpoint, a rational designer is seen as a "pessimist" who has to be able to reason quantitatively about his goals, his means, the intentions of the users, etc. in order to function properly. In other words, he has to be able to plan everything in detail long before he can trust his ideas to paper.

The impact of the systems approach on design, rests on three eminently important issues:

- It allows one to create complex objects, composed of a myriad of known components, in response to any formalized requirement.
- It can, by and large, be learned in a curriculum.
- The inherent presence of exhaustive documentation in this approach to design, allows it to be teamwork and thus facilitates objectivity and multidisciplinary cooperation (2, 3).

If the type of design discipline that was briefly described above, is used in appropriately structured way, even if not all steps can be strictly rationalized, the design team will be able to verify the adherence of their system to specifications at every step of the design process, by testing and evaluating intermediate results.

Four basic axioms govern this "appropriately structured" design process. They have been outlined in their theoretical form by Elzas in 1986 (4). Reworded in terms of daily engineering practice these axioms are:

1) Goal and requirements of the system to be designed have to be describable a priori, preferably in some quantitative way.
2) The number and type of components to be used and their interrelations have to be known sufficiently, in order to be able to guarantee a priori that the number of components and relations is finite and processing rules exist.
3) Documentation should be consistent and should be intelligible to other designers, users, and preferably to others responsible for peer review. This axiom is a central requirement to the feasibility of multidisciplinary design.
4) The time-horizon of applicability of the design should be known to such an extent that changes in the exogenous context can be foreseen. This implies that designs stay valid within a restricted time frame.

For most cases, where new objects are to be designed with known components for well defined environments, it is clear that these axioms do not form an impediment to the design activity. On the other hand the need for a priori insight in the feasibility, adequateness and verifiability of the design for e.g. waste management systems require as close adherence as possible to a systems design track in order to be able to monitor the size and precise nature of the risks incurred, and to establish as many milestones for success to avoid failure as much as possible.

One can also use elements of information theory to evaluate the nature and efficiency of the design process itself. The basic idea for this is that designing is a process by which the information-content of a requirement is manipulated/transformed into the information-content of the requirement and the information-content of the final object, in order to calculate the information loss of the design process.

From this basic notion one can derive that the more uncertainty there is before design starts, because of the vagueness of the requirement, the more manipulation leeway the designer has at his disposal. Uncertainty is reflected by a high information-content figure in information theory. Certainty, that is present in a definite object, always carries a low information value.

Styles and methods are "information filters." They reduce the diversity of choice. Precise requirements yield designs with negligible information content, in other words, they imply a design.

Some designed systems, e.g. a house, allow huge tolerances for inadequacies in the final product. Complex and/or highly interconnected systems, such as VLSI-chips or nuclear systems, allow little or no tolerance in the final product. The first class is "easy" to design in almost any creative way. The latter class leaves very few choices. The information-reduction that the former class has to achieve is almost negligible with respect to the latter class.

Therefore the last class of systems must be designed in the sequential, structured way that is typical for the systems approach, in order to be able to judge at every step which risks are incurred and which items to pay specific attention to.

A FRAMEWORK FOR DESIGN AND TEST DERIVATION

As has been shown by Wymore (5) and Elzas (6) that the systemic approach to design can be mapped into structured top-down process that naturally sequences all activities in a well defined hierarchy. Figure 1 shows the steps of the design process which are easily amenable to the stepwise generation of test procedures that fit the refinement steps in the design process and reflect the essential elements of the original requirements. A few terms that are used in Fig. 1 are explained in the sequel.

The requirements base is a more or less abstract notion that is used to reflect the fact that any requirement for a system to be designed originates with a group of potential users who have certain wishes and preconceptions of the future system in their minds, although they often are not able to put all of these in quantitative form or even, possibly into words. A round of interviewing and meetings is needed to collect this information and analyze it in order to be able to formulate these requirements in generally understandable terms so that it can be transferred and used as a primary reference document. This phase is called requirement analysis in Fig. 1.

What is often left out at this stage, but is essential for later verification, is the collection of information that adequately describes the way in which the participants will verify if their wishes have been achieved in the final design. The set of potential tests describe the ways in which the achievement of these wishes will be evaluated.

The document reporting the results of the analysis of requirements is called the information requirement specification. Informal because it might well contain a number of elements which are either not qualifiable, not realizable or amenable to elimination for other reasons.

Most complex systems consist of subsystems of quite different nature, that will be realized with different means by different teams. Therefore when the moment arrives that the system can be specified in a more formal way, the differences will have to be taken into account by making specialized specifications for every subsystem that has different nature (e.g. technical, social, economic, ecological, etc.). This is the ideal moment to also consult the set of potential tests collected before and derive specialized (and formalized) tests from them in accordance with the specializations chosen in the (formal) system specification.

The union of all formal and specialized specifications and test descriptions will then give rise to a comprehensive and formal description of the system requirements and the tests that will be used to verify their achievement, i.e., the comprehensive test protocol.

Once that this stage is reached, the feasibility of the system and the applicability of (available) technology will have to be studied in order to limit the scope of the design to systems that can actually be realized.

In principle one now has a more limited set of possible systems that are left as potential candidates for the actual design task, i.e., the set of feasible designs which can be verified, either entirely or in part, by a set of feasible tests.

Out of these sets one or more candidates will be chosen, e.g. on the basis of exogenous considerations such as policy, cost, etc., and will have to be specified as precisely as possible in the form of a global system design specification and its accompanying system test protocol. These could form for example, the basis for a request for bids.

The track that follows is entirely in the realm of the "designer" himself who will in first instance endeavor to construct a system outline specification that reflects the general characteristics of the future system with an accuracy adequate enough so that, if realized, it may pass all necessary functional tests that have been conceived to check if the system is able to perform its main intended functions.

In the next step the system that is being designed is decomposed into its components, their interfaces and couplings. The document that is created for this level is the component system design specification that gives rise to a set of tests described in the component test protocol.

Finally, one will realize a prototype system implementation for which the prototype test protocol that in the mean time has been created from the previously mentioned test protocols, will be used to verify all basic functions and short term requirements. If the system passes these tests, it can be allowed to operate for some length of time during which its behavior will be monitored in the course of the overall system performance evaluation.

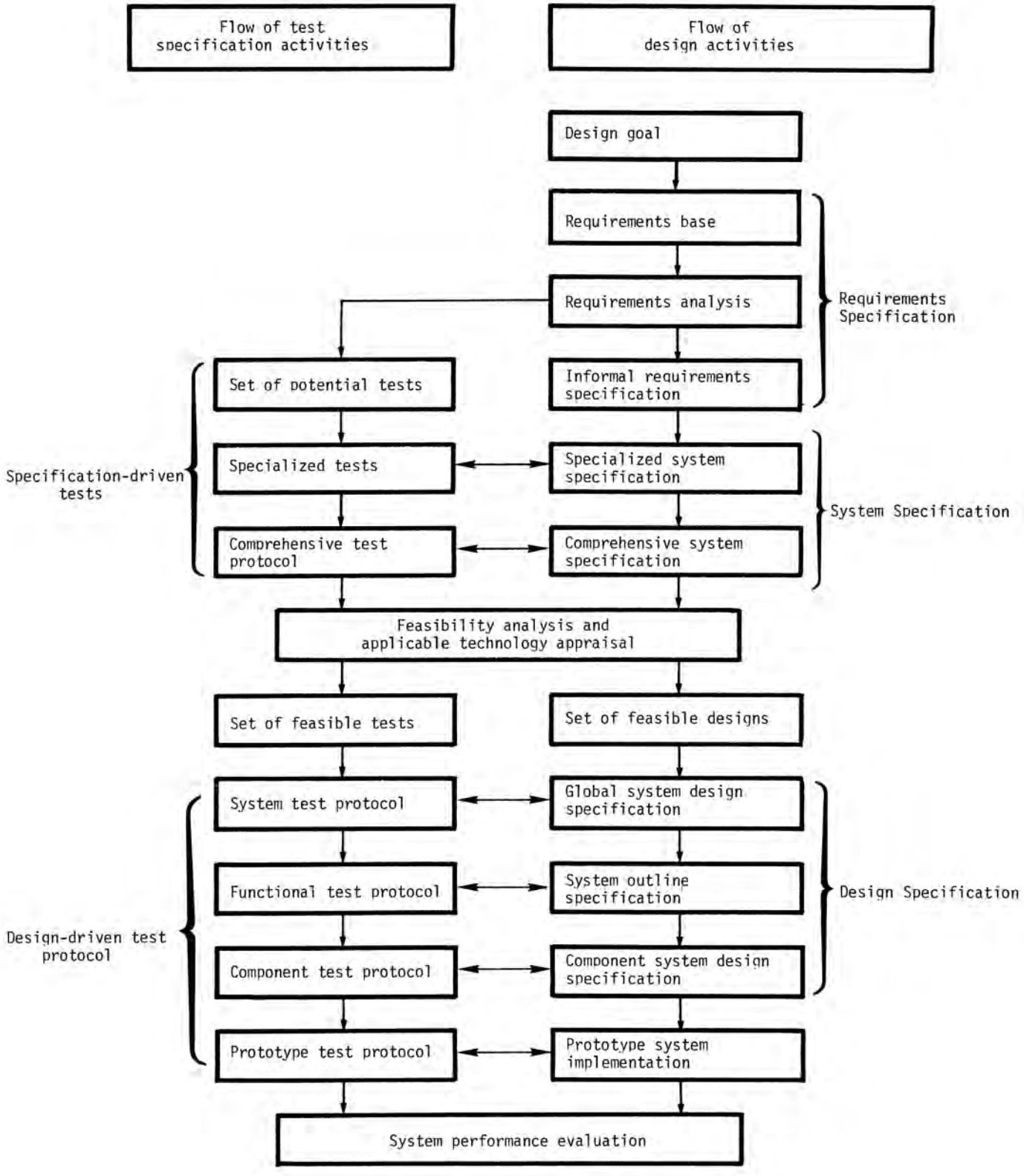

Fig. 1. Test Derivation Based on Structural Design.

QUALITY ASSURANCE POSSIBILITIES

In the previous section, the design procedure for a complex system has been described as if it would take place under ideal circumstances, i.e. under the assumption that all "actors" in the game play their respective roles with utmost honesty and full adherence to the "rules." It is evident that such a situation will (almost?) never be reached. Therefore measured are needed that assure that the right things are done at every point in the design track.

Table I can be used as an illustration of the bonds that exist between different aspects and phases of the system design process that has been described in the previous section, as well as a checklist for evaluation of an ongoing design process.

The table has been restricted to the actual design process (from global system to prototype) in order to be able to fit it on one page. It can easily be expanded to cover the full realm of all phases that were indicated in Fig. 1. It indicates all meaningful evaluations during the three most important design activities, i.e. the design of the global system, the design of the decomposed system (components, interfaces, and couplings) and the realization of the prototype. Note the similarities with Figs. 2a and 2b on pages 384 and 385 of Vol. I of the Proceedings of Waste Management '85 which are part of a previous article by the same authors (7). The present table is a far more general approach to the much more complex problem of systemic design in general. The evaluations shown in Table I are with respect to design goal, requirement base, system specification, standard components, norms (including engineering ones), and potential tests.

Evaluation of global system design specifications necessitates compliance, adequacy of design specification, relevance of feasible designs, quality of conceptual design, appropriateness of technology, and compliance with norms.

Evaluation of global system test specifications necessitates compatibility of test, test feasibility, adequacy and completeness of test.

Evaluation of decomposed system design specifications necessitates functionality, completeness, compatibility, adequacy of composition, and optimal utilization, and compliance with norms.

Evaluation of decomposed system test specifications necessitates compatibility of tests, appropriateness, adequacy, and completeness of tests.

Evaluation of prototype system implementation necessitates compliance, degree of satisfaction, completeness, evaluation of the realization, proper utilization of technology, and compliance with norms.

Evaluation of prototype system test protocol necessitates relevance, applicability, feasibility, and adequacy of test as well as completeness of test protocols.

NEW DIMENSIONS IN QUALITY ASSURANCE PROBLEMS

Due to the utmost importance as well as the interdisciplinary and multifaceted characteristics of the nuclear fuel waste management projects, powerful and systematic design and test concepts of systems engineering are required. In addition to these, modelling and simulation methodology can be very useful to provide solid and powerful bases to assure model reliability and other model-based quality assurance issues (8).

Since computerized models are used at some important phases of the assessment studies, assurance of software quality has a primordial importance. Several relevant references as well as some guidelines have been provided in the literature (9).

The fact that nuclear industry started to follow closely the advances in artificial intelligence and other innovative computer applications is very important. A topical meeting with the title "Artificial Intelligence and other innovative computer applications in the nuclear industry" will take place during August 31 through September 2, 1987 in Snowbird, Utah (10). It is organized by the Idaho Section of the American Nuclear Society and sponsored by the Human Factors Division and Remote Systems Technology Division of the ANS and the European Nuclear Society.

This topical meeting has the emphasis on how artificial intelligence and other innovative computer systems can contribute to improvements in operation, control, safety, reliability, and efficiency in the nuclear power industry. We hope that advanced software engineering concepts as well as artificial intelligence concepts will also be used to enhance nuclear fuel waste management operations.

Some advanced quality assurance concepts one has to consider in modelling and simulation are already covered in the literature (11, 12, 13). In this section, some important quality assurance concepts one has to consider in the artificial intelligence era are highlighted. It is hoped that responsibles who would commission development or tailoring of knowledge-based systems, or expert systems for nuclear industry will consider them 1) to avoid additional sources of errors to their already complex systems and 2) to take advantage of some artificial intelligence techniques to eliminate some types of errors. Table II is a systemization of the quality assurance problems pertaining to modelling and simulation. Before elaborating on the systematization, clarification of some basic terminology is in order.

As a type of system with artificial intelligence, a cognizant system is a computer or a computer-embedded system which, through its software, has cognitive abilities such as: 1) Knowledge processing abilities; 2) asking and answering questions (in a computer language or in a natural language, including a spoken language); and 3) monitoring itself, its environment, and its user.

Knowledge processing abilities of a cognizant system include:

1) Knowledge acquisition (including building knowledge bases and learning);

2) Knowledge analysis (including detection, location, interpretation, comparison, and evaluation of knowledge);

3) Knowledge transformation (including reordering, rescoping, and synthesis of knowledge);

4) Knowledge generation (through experimental and non-experimental techniques);

5) Knowledge dissemination (to users which might be humans or other knowledge processing systems with

TABLE I

Design, Implementation, and Test Evaluation Matrix

Evaluation of → / with respect to ↓	Global system		Decomposed system		Prototype system	
	Design specification	Test specification	Design specification	Test specification	Implementation	Test Protocol
Design goal	Compliance				Compliance	Relevance of tests
Requirement base	Adequacy of design specification				Degree of Satisfaction	
System Specification	Relevance of feasible designs		Functionality		Completeness	Applicability of tests
(alternative) Design Specification of Global System	Quality of conceptual design	Compatibility of tests	Completeness	Compatibility of tests	Evaluation of the realization	
Technology	Appropriateness of technology	Test feasibility	Compatibility	Appropriateness of test	Proper utilization of technology	Test feasibility
Standard components			- Adequate composition - Optimal utilization	Adequacy of test		
Norms	Compliance with norms	Adequacy of tests	Compliance with norms	Adequacy of tests	Compliance with norms	Adequacy of tests
Potential Tests		Completeness of tests		Completeness of tests		Completeness of test protocol

or without explanation (including self-explanation and meta-explanation) (14, 15).

In cognizant simulation modelling and simulation environment and/or simulation system have cognitive abilities.

As shown in Table II, Type I quality assurance problems require application of traditional quality assurance techniques in modelling and simulation Several techniques and references exist (1) and are not elaborated here due to page limitation.

Type 2 quality assurance problems require application of traditional quality assurance techniques in advanced (i.e. cognizant) modelling and simulation. Some important concepts which are not yet fully elaborated in the artificial intelligence literature are presented in modelling and simulation literature (12, 13). These concepts include adequacy. completeness, consistency, and integrity of both statis and dynamic knowledge-bases which may include model bases and rule bases.

Both Type 3 and Type 4 of quality assurance problems require advanced (i.e. cognizant) techniques embedded in quality assurance operations. These techniques are called cognizant quality assurance techniques.

Type 3 quality assurance problems require application of cognizant quality assurance techniques to traditional modelling and simulation problems. Some possibilities are: Using knowledge-based modelling and simulation advisors which provide built-in cognizant quality assurance. Built-in cognizant quality assurance is use of cognizant techniques to guide the user in the specification phase of the activities or elements for the purpose of eliminating some types of errors. This important possibility is in contrast of having additional techniques including cognizant ones to detect and eliminate errors which exist in a specification.

Type 4 quality assurance problems require application of cognizant quality assurance techniques to cognizant modelling and simulation problems. Some techniques include cognizant quality assurance of cognizant simulation environment and cognizant quality assurance of cognizant simulative design environment (12, 13).

CONCLUSION

Nuclear industry, due to its own nature, is based on an already advanced technology. It is comforting to observe that it is also open to other relevant and advanced knowledge processing technologies such as advanced systems engineering, modelling, simulation, as well as innovative computer applications and artificial intelligence. In the article, technical foundations for systems engineering design and test activities for safety assessments are discussed, a categorization of quality assurance issues is given and some important quality assurance issues that one has to take into consideration is using expert system technology are highlighted.

REFERENCES

1. T.I. ÖREN, M.S. ELZAS, G. SHENG, "Model Reliability and Software Quality Assurance in Simulation of Nuclear Fuel Waste Systems," Proc. Waste Management '85, Tucson, Arizona, March 24-28, 1985, Vol. 1, pp. 381-396 (1985).

2. C.W. CHURCHMAN, The Systems Approach, 243 p., Dell Publishing Company, New York (1968).

3. A.W. WYMORE, Systems Engineering Methodology for Interdisciplinary Teams, 431 p., Wiley, New York (1976).

4. M.S. ELZAS, "System Paradigms and Design Methodology," R. Trappl (Ed.), Cybernetics and Systems '86, pp. 625-632, D. Reidel Publishing Company (1986).

5. A.W. WYMORE, "The Tricotyledon Theory of System Design," T.I. Ören, B.P. Zeigler, M.S. Elzas (Eds.), Simulation and Model-Based Methodologies: An Integrative View, pp. 119-132. Springer-Verlag, Heidelberg, W. Germany (1984).

6. M.S. ELZAS, "System Paradigms as Reality Mappings, T.I. Ören, B.P. Zeigler, M.S. Elzas (Eds.), Simulation and Model-Based Methodologies: An Integrative View, pp. 41-67. Springer-Verlag, Heidelberg, W. Germany (1984).

7. Same as 1.

8. T.I. Ören, B.P. Zeigler, M.S. Elzas (Eds.), Simulation and Model-Based Methodologies: An Integrative View, 651 p. Springer-Verlag, Heidelberg, W. Germany (1984).

9. Same as 1.

10 "Call for Papers: Topical Meeting on AI and Other Innovative Computer Applications in the Nuclear Industry." The AI Magazine, 7:5, 112 (1986).

11. T.I. Ören, "Artificial Intelligence in Quality Assurance of Simulation Studies," M.S. Elzas, T.I. Ören, B.P. Zeigler (Eds.), Modelling and Simulation Methodology in the Artificial Intelligence Era, pp. 267-278, North-Holland, Amsterdam (1986).

12. T.I. Ören, "Quality Assurance in Cognizant Simulative Design," Proc. 1986 Winter Simulation Conference, Washington, D.C., Dec. 8-10, 1986, pp. 850-852 (1986).

13. T.I. ÖREN, "Artificial Intelligence and Quality Assurance Methodology," Lecture Notes for the Professional Development Seminar: Knowledge-Based Simulation and Modelling, Tucson, Arizona, January 19-20, The University of Arizona (1987).

14. T.I. ÖREN, "Cognizant Simulation Systems," Lecture Notes for the Professional Development Seminar: Knowledge-Based Simulation and Modelling, Tucson, Arizona, January 19-20, 1987, The University of Arizona (1987).

15. T.I. ÖREN, "Artificial Intelligence and Simulation," Proc. Artificial Intelligence Applied to Simulation, E.J.H. Kerkhoffs et al. (Eds.), Ghent, Belgium, February 25-27, 1985, Society for Computer Simulation, La Jolla, California, pp. 3-8 (1986).

TABLE II

Types of Quality Assurance Problems

Nature of quality assurance techniques		Quality assurance in two categories of modelling and simulation	
		quality assurance in traditional modelling and simulation	quality assurance in advanced (cognizant) modelling and simulation
	traditional quality assurance techniques	Type 1 Problems quality assurance in modelling and simulation	Type 2 Problems quality assurance in cognizant modelling and simulation Examples: - knowledge-base adequacy - knowledge-base completeness - knowledge-base consistency - knowledge-base integrity References: 12, 13
	advanced (cognizant) quality assurance techniques	Type 3 Problems advanced (cognizant) quality assurance in modelling and simulation Examples: - cognizant quality assurance - built-in cognizant quality assurance Reference: 11	Type 4 Problems advanced (cognizant) quality assurance in cognizant modelling and simulation Examples: - cognizant quality assurance of cognizant simulation environment - cognizant quality assurance of cognizant simulative design environment References: 12, 13