Proceedings of the Korean Nuclear Society Autumn Meeting
Yongpyong, Korea, 2003

A Study on a Systematic Approach of Verification and Validation of a Computerized Procedure System: ImPRO

Wei Qin and Poong Hyun Seong

Korea Advanced Institute of Science and Technology
Department of Nuclear and Quantum Engineering
373-1 Guseong-dong, Yuseong-gu,
Daejeon 305-701, Republic of Korea
philipqinwei@kaist.ac.kr

Abstract

Paper Based Procedure (PBP) and Computerized Procedure System (CPS) are studied to demonstrate that it is necessary to develop CPS in NPP I&C system. Computerized procedure system is actually a software system. All the desired and undesired properties of a software system can be described and evaluated as software qualities. Generally, software qualities can be categorized into product quality and process quality. In order to achieve product quality, the process quality of a software system should also be considered and achieved. Characteristics of CPS will be described to analyse the product and process of an example CPS: ImPRO. At the same time, several main product and process issues will be analysed from Verification and Validation (V&V) point of view. It is concluded and suggested that V&V activities can also be regarded as software development process, this point of view then is applied to the V&V activities of ImPRO as a systematic approach of V&V of ImPRO. To support and realize this approach, suitable testing technologies and testing strategies are suggested.

1 Introduction

There have been many efforts to develop CPS worldwide since recently decades. ImPRO is one of CPS developed by Jung et al based on Java platform. Besides it, there are also several CPS systems as COMPRO and SSCI developed by Westinghouse, N4 Procedure System by

EDF, and COPMA by Halden Reactor Project (HRP) which are world widely known. These systems have their own languages to describe procedures. In addition a lot of experimental CBPs have been developed without well defined instruction sets. In spite of above differences between different CPS, the overall concerns are common among them. This paper will be about a study of a systematic approach of V&V of ImPRO system.

2 Procedure systems in NPP I&C system

Procedures are typically written documents (including both text and graphic formats) that present a series of decision and action steps to be performed by plant personnel (e.g., operators and technicians) in order to accomplish a goal safely and efficiently. Nuclear Power Plants (NPPs) use procedures for a wide variety of tasks from administration to testing, and plant operation. Plant procedures provide instructions to guide operators in monitoring, decision making, and controlling the plant. [1]

Procedure functions can be organized into four cognitive categories: Monitoring and Detection, Situation Assessment, Response Planning, and Response Implementation. In terms of monitoring and detection, operators must monitor process parameters referenced by procedures. Operators must also monitor their own procedure-related actions. [2]

Historically, plant procedures have been paper-based. Following the accident at Three Mile Island, the nuclear power industry recognized the importance of having technologically sound and easy-to-use procedures to handle major plant disturbances. For emergency operations, symptom-based procedures were established that enabled operating crews to restore and maintain the plant's safety functions without having to diagnose events or the specific causes of process disturbances.

Paper-based procedures (PBPs) have characteristics that limit how information can be presented to the operators. These limitations include presenting information in sequential form, requiring numerous iterations through steps, and cautions or warnings that may be applicable for all system states. PBPs also impose tasks on the operator that are not directly related to controlling the plant. To make transitions between procedure steps and documents, and maintain awareness of the status of procedures that are in progress, operators must handle, arrange, scan, and read PBPs in parallel with monitoring and control tasks.

Computer-based procedure (CBP) systems were developed to assist personnel by computerizing paper-based procedures (PBPs). Their purpose is to guide operators' actions in performing their tasks in order to increase the likelihood that the goals of the tasks would be safely achieved. CBP

s define decisions to be made and actions to be taken where the goals are unambiguous and the correct or desired course of action is generally known. [1]

A significant difference between PBPs and CBPs is in the type of functions offered by CBP systems for viewing and using the procedures. CBPs are being developed to support procedures management. CBPs have a range of capabilities that may support operators in controlling the plant and reduce the demands associated with PBPs. In their simplest form CBPs show the same information via computer-driven video display units (VDUs). More advanced CBPs may include features to support managing procedures (making transitions between steps and documents, and maintaining awareness of procedures in progress), detecting and monitoring the plant's state and parameters, interpreting its status, and selecting actions and executing them.

The following are aspects to be considered when developing and operating V&V of CBPs: [1]

- how procedures are entered into the computer system;
- how their quality is verified (e.g., no typos or omissions);
- how errors are identified, tracked and corrected;
- how changes are incorporated;
- how configuration control (i.e., control over revisions and modification) is provided.

These problems are among the key factors which will determine the quality of the target system. They should be emphasized during the development and V&V activities of CPS to assure that all the requirements to the target system will be realized in a systematic and rigor way. These issues will be considered in the following sections.

Computerized procedure system is actually a software system from a relatively small scale of view. All the desired and undesired properties of a software system can be described and evaluated as software qualities. Generally, software qualities can be categorized into product quality and process quality. In order to achieve product quality, the process quality of a software system should also be considered and achieved. In the following sections, studies of CPS will be operated to analyse the product and process of an example CPS: ImPRO. And then, several main product and process quality issues will be analysed from Verification and Validation (V&V) point of view.

3 An example of CPS: ImPRO

3.1 Introduction of ImPRO

ImPRO is a computerized procedure system which is developed by Jung et al from KHNP

(Korea Hydro Nuclear Power). ImPRO supports operator to execute procedures rapidly and correctly. Compared to paper based procedure, ImPRO shows not only procedure rules but also relavant plant information. Moreover ImPRO can evaluate procedure statements whether they are satisfied or not in the context of plant state.

3.2 Architecture of ImPRO

3.2.1 Distribution system point of view:

As shown in fig.1. ImPRO consists of Server and several Clients. They are distributed in order to share the procedure resources freely, keep consistency. Because ImPRO shows not only procedures but also related information, ImPRO are usually integrated with process computers.

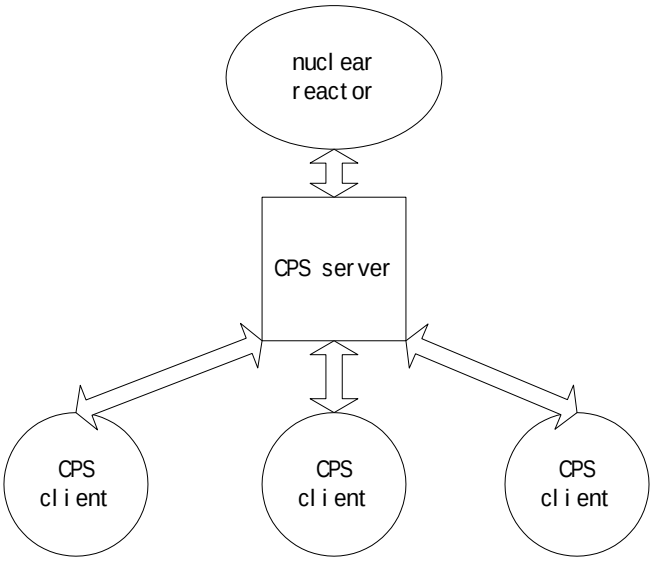

Fig.1. ImPRO from distribution system point of view

The server manages all procedure files that are not accessible from clients directly. This central management enhances consistency of procedures. The clients cannot have different version of procedure files. This architectural design basis applies to plant process information too. Whenever the clients need these resources, server delivers them to the clients on demand.

3.2.2 Information and control system point of view

In modern NPPs, I&C systems are getting more and more powerful then ever. According to this trend, CPS becomes more and more functionally powerful. This trend can described from information and control system point of view. In fig. 2., CPS communicate with operator I&O module and reactor monitoring and control system I&O module. After gathering sufficient information from I&O modules, the information processing and control module makes information processing and then gives out suitable output to achieve the desired states of the

NPP.

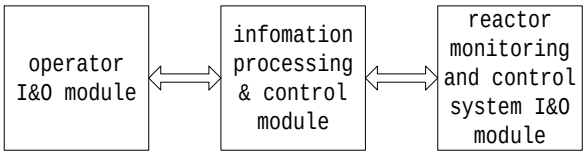

Fig.2. ImPRO from information and control system point of view

In fig. 3., a detailed information processing and control system is illustrated. In fig. 3., the information processing and control module is expanded into procedure execution module, procedure files, process information database and reactor monitoring system I&O module. Among them, procedure execution module is the core module of the whole system which is mainly in charge of information processing and control. Procedure files are written according to PML(Procedure Markup Language), which is an instance of general XML1.0 specification. Plant Database is also built in XML1.0. The data can be retrieved with XQL. One advantage of PML is inherent verification of procedures due to formalism. A device symbol is graghical presentation for a node in the plant database. Each device embodies an instrumentation in the I&C system which measures process information of the NPP or acts as an actuator. The process database of ImPRO is dynamically updated. [3]

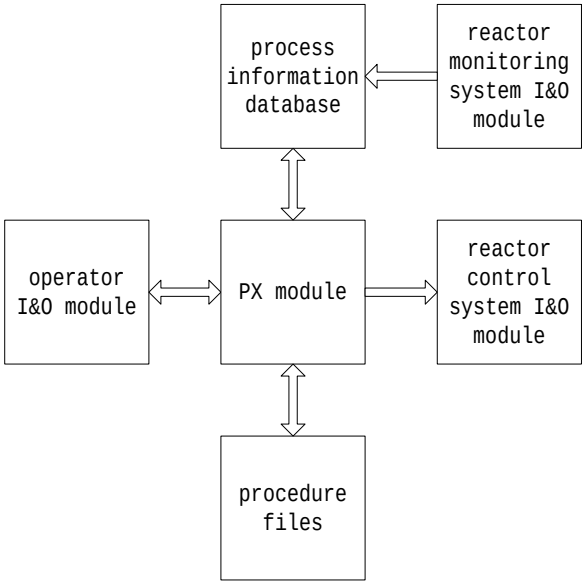

Fig.3. Detailed information and control system point of view

3.3 Procedure execution structure of ImPRO

Procedure execution structure of ImPRO is determined by the structure of the procedure itself. In order to analyse the structure of procedure execution, it is reasonable to study the structure of procedures first. Each procedure is comprised of a sequence of steps, there are

many types of steps as listed in table.1.:

Type	**Description**
Begin Step	The begin step of a procedure
End Step	The last step of a procedure. The step terminates the procedure.
Branch Step	The steps have several branches that link to several next steps.
Sequential Step	The steps which should be performed sequentially.
Non Sequential Step (NSS)	The steps which can be performed regardless of other step completion
Continuously Applied Step (CAS)	The steps which are continuously monitored after step completion

Table.1. Step types

At the same time, within each step, there are several actions or checking actions to be executed.

3.3.1 Flowchart structure of steps

As shown in fig.4. a flowchart shows overall workflow in two dimensions. The flowchart is segmented by steps. If a step is expanded, Action/Checks within the step are illustrated. Action has one output arrow, whereas Check has two output arrows. The next destination of check is determined by the current result. Action and checks in the flowchart are executed one by one.

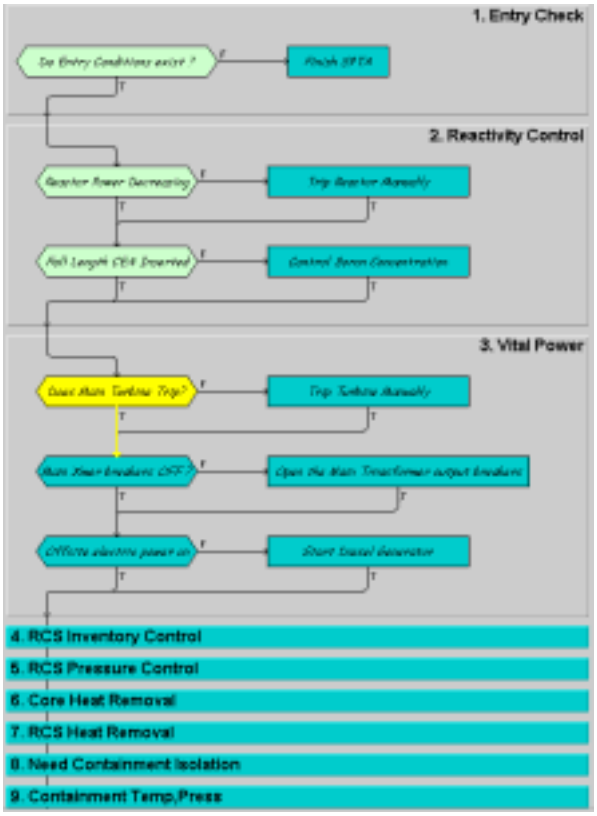

Fig.4. flowchart structure of steps

3.3.2 Success logic tree structure of actions or checks

Action/Check is described in the format of success logic tree to show the intra-relations within an Action/Check. An example is shown in fig.5. A success logic tree consists of leaf nodes, lines, and trunks with a number operator. A node has one of three states: True, False, and Unknown. Leaf nodes of a tree are related by n-out-of-m logic operator. If the number of True nodes is more than n, the logic operator becomes True. This logic tree can be nested, but not cyclic.

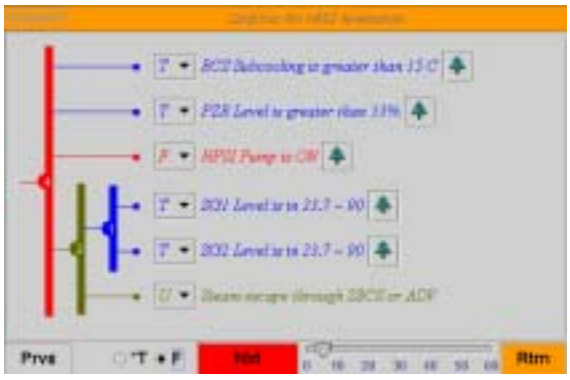

Fig.5. Success logic tree structure of actions or checks

To understand the architecture and structure of CPS fully and clearly is very important to operate V&V activities in a suitable and efficient way. By doing this, the mechanism of CPS execution can be specified and then testing case design and testing cases execution strategy based on it is available to achieve a satisfactory testability.

4 Life cycle of CPS development process and V&V activities of ImPRO

Software development can be regarded as a life cycle process of activities. By realization of life cycle process model, characteristics of the process can be identified and important process qualities can be applied and evaluated during the development process. And in this paper, a idea is initiated that V&V activities of the software itself is also a life cycle process of activities which is operated parallely with the development process.

4.1 Descriptions of the life cycle of ImPRO development process and V&V activities of ImPRO

4.1.1 A waterfall model

A waterfall model initiated by Jung et al is shown in fig.6. [4]

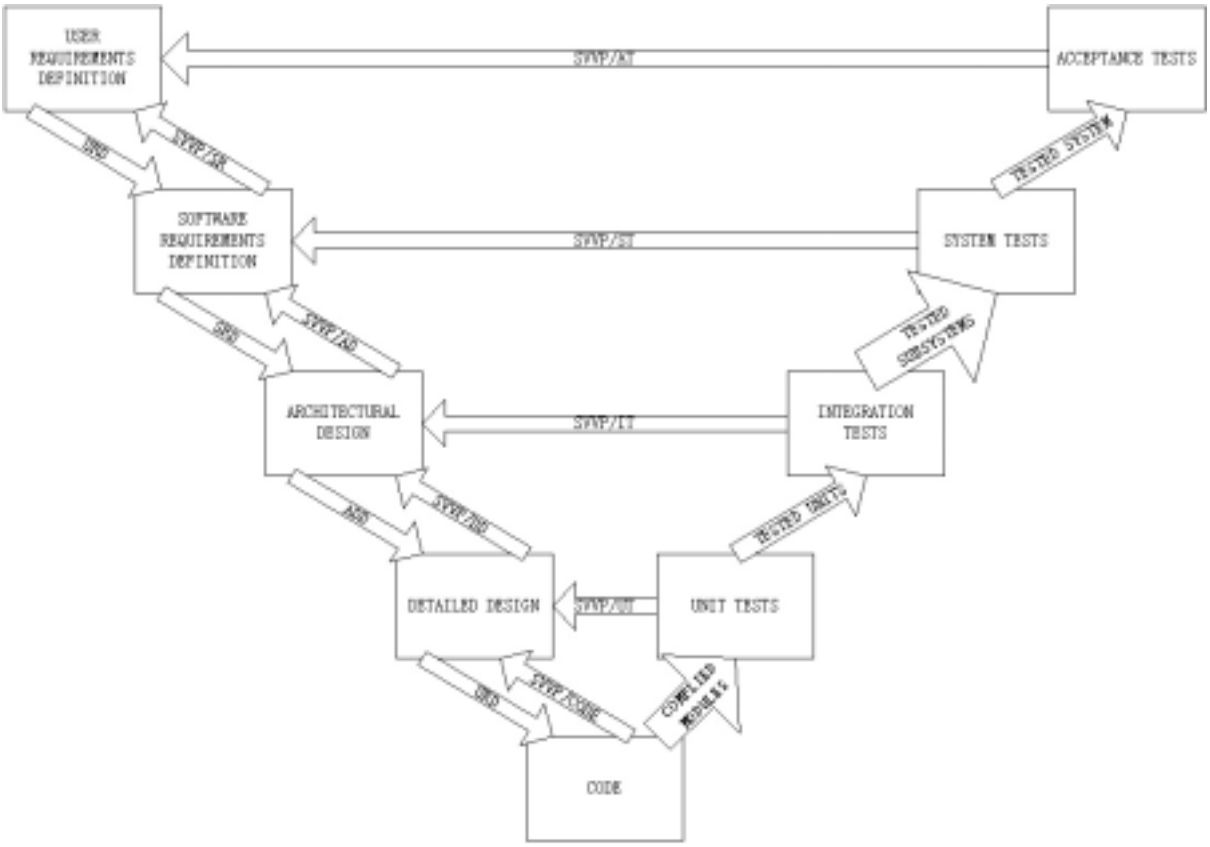

Fig.6. A waterfall model of ImPRO

The software development process can be regarded as a typical waterfall model. At the same time V&V activities are being operated simultaneously. The life cycle process of V&V activities of CPS begins together with the development activities from user's requirements analysis. The input of each stage of V&V is the output of corresponding development activities and Software Verification and Validation Plan (SVVP), and the output will be feedback to the development activities as well as feed forward to testing stage. [4]

4.2 The relationship between life cycle of ImPRO development process and life cycle of V&V activities of ImPRO as a development process

Software V&V activities process can significantly influence the software development process and farther influence the process qualities of software development process and farther more the software product qualities. From this point of view, by enhancing the process qualities of V&V process, the software development process qualities will be enhanced and then so are the ImPRO software qualities.

4.3 Characteristics of life cycle of ImPRO development process

As a CPS, ImPRO will be maintained and updated continuously during development and after being released. Any software is supposed to change during its life cycle from development, operation till abandoned. During development phase, the courses of changes can come from the customers or from V&V activities. Customers' requirements of the desired software may not be very complete or exact at the beginning, the requirements will be modified or enriched continuously until the end of software life cycle. Also, another significant source of change is V&V activities. V&V activities are designed to discover faults and deficiencies in software being developed. [5]

As a system which is important to safety, ImPRO should be possibly completely verified and tested before being released. ImPRO is a relatively large software system. According to the testing principles and technologies, it is almost impossible to operated exhausted testing because of the explosion effect of the growth number of testing cases as the size of the target system increases. So to execute the testing cases within practically limited number using an efficient testing strategy is very important.

4.4 Characteristics of life cycle of V&V activities of ImPRO as a development process

V&V activities such as testing should be able to be repeated easily in conformance with the characteristic that the ImPRO is supposed to be modified and updated continuously during development and after being released. Testing in this way is called regression testing. Testing technology should be designed to support regression testing for ImPRO.

4.5 An iterative model for life cycle of ImPRO development process and its V&V activities.

Thus, according to the descriptions in previous paragraphs about the characteristics about ImPRO development and V&V activities process, a farther iterative model is suggested to be applied for ImPRO. A initial version of ImPRO may first be developed to be applied in NPP or simulating environment to assess the effect and validity of the system. This is very possible and feasible because there are many different operating procedures for NPP. These procedures maybe implemented incrementally. After one of the procedures has been development and V&V activities has been operated simultaneously, this new procedure can be add into the initial system to update the functionalilty of the system. By this kind of iterations, ImPRO is eventually enriched and maintained.

5 Testing technologies for ImPRO V&V process

Now the focus of V&V activities of ImPRO is put onto the testing phase. As illustrated in

the process model, during every iteration of the life cycle of ImPRO, testing is operated in an incremental way. And then, as development is going on in a iteration way, testing will be operated as regression testing.

5.1 Incremental testing

Initially, testing focuses on each component individually, ensuring that it functions properly as a unit. This is called unit testing. Next, components must be assembled or integrated to form a complete software package. Integration testing addresses the issues associated with the problems of verification and program construction. After the software has been integrated, a set of high-order tests are conducted. Validation criteria (established during requirements analysis) must be tested. Acceptance testing provides final assurance that software meets all functional, behavioral, and performance requirements. This is a typical bottom-up approach.

5.2 Regression testing

Testing activities should be organized with the purpose of verifying possible regressions of software during its life, i.e., degradations of correctness or other qualities due to later modifications. Properly designing and documenting test cases with the purpose of making tests repeatable, and using suitable testing tools, will help regression testing.

Test cases should be treated in the same way as software. It is clear that such qualities as evolvability, reusability, and verifiability are just as important in test cases as they are in software. We must apply formality and rigor, incrementality and other principles in the development and management of test cases.

6 Testing strategy for ImPRO V&V process

Ideally, every testing case should be run once when any change is made. Practically, the number of testing cases will grow too large to run all the time. There is a possible way to create special set of testing cases that contain all the test cases that might possibly be affected by the current development.

In previous sections, it is mentioned that within each step of procedures, Action/Check is described in the format of success logic tree to show the intra-relations within an Action/Check. From this characteristic, it is suggested to apply fault tree analysis. [7]

An example of success logic tree is show in fig.7. It is an n out of m success logic tree. Eac h node of the tree has its own logical value as True, False or Unknown. Each node can be reg

arded as a goal to be achieved during the execution of the Action/Check. Because False and Unknown have the same effect to the result of the tree, so they can be treated equally when an alyzing the tree. The logic value of each node will be considered during the analyses, a node f ail to achieve its goal as to become True is considered to be a fault. First of all, the success lo gic tree should be transformed into fault logic tree to proceed with the analyses. An n out m s uccess logic tree becomes m-n+1 out m fault logic tree. This means if m-n+1 of the nodes fail to achieve their goals, the Action/Check will fail. [6]

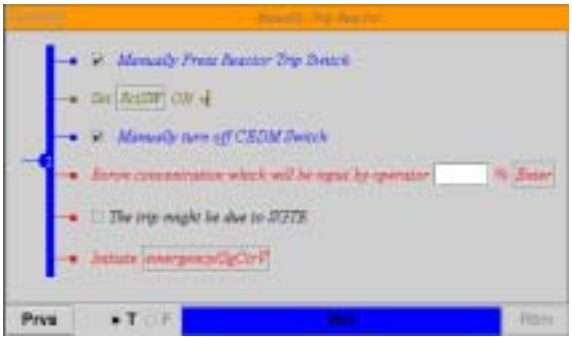

Fig.7. An example of success logic tree

Fault tress provides a graphical and logical framework for analyzing the failure modes of systems. There use helps the analyst to assess the impact of software failures on an overall system, or to prove that certain failure modes cannot occur (or occur with negligible probability).

The logic structure of the fault tree helps to determine a better testing strategy. If the probability of failing to achieve the goal of an Action/Check is relatively high, all the nodes of the fault logic tree must be covered by exhaustive testing in order to prevent the failure.

7 Conclusion

ImPRO is a typical CPS example developed on Java Standard Edition (JSE) platform. Its source code is available for the authors to make a thorough study so as to achieve a systematic approach of V&V activities. Based on software quality metrics, characteristics of CPS are described to analyse the product and process of ImPRO. At the same time, several main product and process issues will be analysed from Verification and Validation (V&V) point of view. It is concluded and suggested that V&V activities can also be regarded as a software development process, this point of view then is applied to the V&V activities of ImPRO as a systematic approach of V&V of ImPRO. This approach will operated under the aid of several software testing tools available. Further more, to improve and optimize this approach, suitable testing technologies and testing strategies are suggested.

8 References

[1] American Nuclear Society. NUREG/CR-6634 computer-based procedure systems: technical basis and human factors review guidance

[2] American Nuclear Society. NUREG -700 human-system interface design review guideline

[3] Yeonsub Jung, PoongHyun Seong, ManCheol Kim. A model for computerizd procedure based on a flowchart and success logic tree

[4] C. Ghezzi, M. Jazayeri, and D. Mandrioli. Fundamentals of Software Engineering, Prentice Hall, 2nd Edition, 2002

[5] Pressman, Roger S. Software engineering: a practitioner’s approach, McGraw-Hill, 5th ed, 2001

[6] Yeonsub Jung, Yeongcheol Shin, Iksoo Park. An incremental objective achievement model in computerized procedure execution, Reliability engineering & system safety, 2000 185-195

[7] Michael R. Lyu. Handbook of software reliability engineering, IEEE computer society press, 1995