Transactions of the Korean Nuclear Society Autumn Meeting
PyeongChang, Korea, October 30-31, 2008

Formal Verification of Computerized Procedure with Colored Petri Nets

Yun Goo Kim, Yeong Cheol Shin
MMIS Team, Nuclear Engineering and Technology Institute, KHNP Co.,Ltd,
25-1 Jang-dong, Yuseong-gu, Daejeon, Korea, 305-343
goodguy@khnp.co.kr, ycshin@khnp.co.kr

1. Introduction

Computerized Procedure System (CPS) supports nuclear power plant operators in performing operating procedures which are instructions to guide in monitoring, decision making and controlling nuclear power plants. Computerized Procedure (CP) should be loaded to CPS. Due to its execution characteristic, computerized procedure acts like a software in CPS. For example, procedure flows are determined by operator evaluation and computerized procedure logic which are pre-defined. So the verification of Computerized Procedure logic and execution flow is needed before computerized procedures are installed in the system. Formal verification methods are proposed and the modeling of operating procedures with Coloured Petri Nets(CP-nets) is presented.

2. Formal Verification of CP

2.1 Verification in Engineering System(ES)

Engineering System(ES) is supporting system for user to analyze, edit, verify, test and install the computerized procedure. Verification of computerized procedure can be classified into three parts, which are availability verification, suitability verification and structural verification. Procedure Writing Guideline (PWG) is used for availability verification and suitability verification. The formal verification which is covered in this paper is structural verification with CP-nets.

Computerized procedure is executed as application software in CPS, so Computerized procedure can be modeled as software for structural verification. There are many formal and semi-formal modeling language for software verification such as State Machine, Coloured Petri Nets, symbolic model checking (SMV), SPIN and so on. The characteristic of Computerized Procedure execution and its instruction can be modeled with CP-nets. So, verification process with CP-nets is developed and proposed.

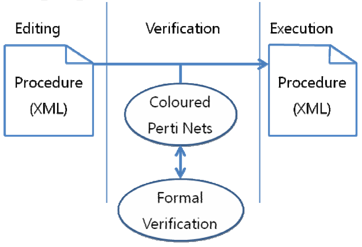

Fig. 1. Structural verification process of Computerized Procedure execution flow

2.2 Coloured Petri Nets (CP-nets)

CP-nets is a modeling language. CP-nets combines the strengths of ordinary petri nets with the strengths of a high-level programming language. CP-nets also have a formal, mathematical representation with a well-defined syntax and semantics. It is possible to formulate standard request for verification properties such as reachability, deadlock, liveness as well as user defined requests using ML language.

2.3 Modeling of Procedure Step

There are several types of instruction in computerized procedure and main instructions are unitary instruction and binary instruction. As expressed from its name, unitary instruction has one outgoing way for the execution flow and binary instruction has two. Fig 2 shows an example step of operating procedures.

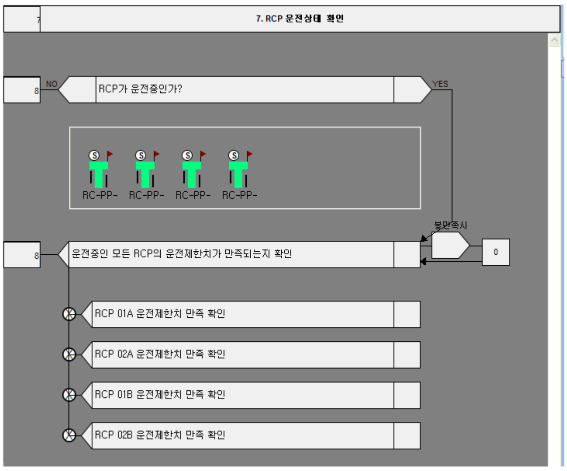
7
7. RCP 운전상태 확인
8
NO
RCP가 운전중인가?
YES
RC-PP-
RC-PP-
RC-PP-
RC-PP-
불만족시
8
운전중인 모든 RCP의 운전제한치가 만족되는지 확인
0
RCP 01A 운전제한치 만족 확인
RCP 02A 운전제한치 만족 확인
RCP 01B 운전제한치 만족 확인
RCP 02B 운전제한치 만족 확인

Fig. 2. Instruction and Step detail in Computerized Procedure

The step in Fig 2 was modeled with CP-nets. For the status of instruction, token whose name is “Status” was used and its colour sets are "Execution", “Non-Execution”, “Completable”, “Complete”. This token “Status” is delivered to the next step according to its execution result. Also between instructions, token whose name is “Evaluation” is used for system and user evaluation. Instructions were modeled as place and execution flows were modeled as transition. Transition is fired when system or user evaluate instruction according to DCS variables and logics. Current modeling is only for step and instruction level, so the DCS process variable and DCS logics are not modeled but the result of evaluation are included.

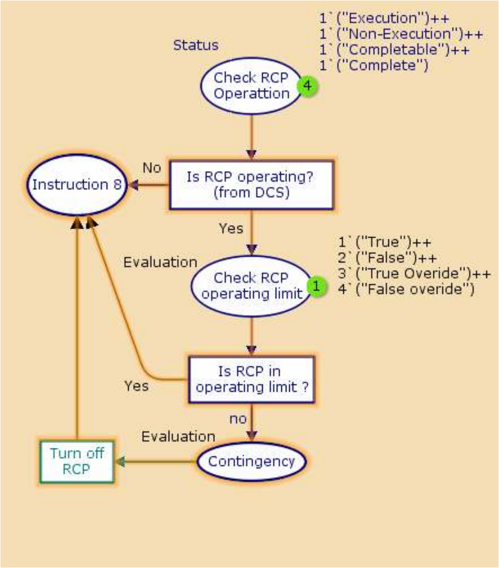

Fig. 3. Coloured petri nets modeling of procedure step

2.4 Interfaces for Automatic Translator

Current modeling was done by manually. But verification of procedure should be done frequently because writing and revision happens all the times. So automatic modeling from computerized procedure can be useful. Computerized procedures are XML format and they contain information for modeling. Converting rules between XML and CP-nets are needed for automatic translator.

3. Conclusions

Formal verification methods with CP-nets are proposed. CP-nets modeling was done and through the simulation, verification properties are verified. Formal verifications are very helpful to the analyzer and the verifier. But it is difficult to CP-nets modeling for operators and there are many procedures to be verified. So, automatic conversion is recommended.

REFERENCES

[1] K. Jensen, L.M. Kristensen, L. Wells. Coloured Petri Nets and CPN Tools for Modelling and Validation of Concurrent Systems. In International Journal on Software Tools for Technology Transfer (STTT).2007

[2] L. Wells. Performance Analysis using CPN Tools. Proceedings of the First International Conference on Performance Evaluation Methodologies and Tools 2006. ACM Press, 2006.

[3] SYSTEM SPECIFICATION for COMPUTERIZED PROCEDURE SYSTEM (DDS1) KHNP Document No. : 9-797-K-464-001