Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 12-13, 2016

MC/DC and Toggle Coverage Measurement Tool for FBD Program Simulation

Eui-Sub Kim [a], Sejin Jung [a], Jaeyeob Kim [a], Junbeom Yoo [a*]
[a]*Division of Computer Science and Engineering, Konkuk University, 120, Neungdong-ro, Gwangjin-gu, Seoul, Republic of Korea*
[*]*Corresponding author: jbyoo@konkuk.ac.kr*

1. Introduction

Functional verification of function block diagram (FBD) is important when developing the software of reactor protection system (RPS) in instrumentation and control (I&C) of nuclear power plant (NPP). The RPS is typically designed with PLC programming languages such as FBD or ladder diagram (LD) [1] in the design phase. Hence, verification and validation (V&V) and rigorous quality demonstration should be considered in the FBD design level.

The functional verification of FBD program can be implemented with various techniques such as testing [2] and simulation [3]. Simulation is preferable to verify FBD program, because it replicates operation of the PLC as well. The PLC is executed repeatedly as long as the controlled system is running based on scan time. Likewise, the simulation technique operates continuously and sequentially.

Although engineers try to verify the functionality wholly, it is difficult to find residual errors in the design. Even if 100% functional coverage is accomplished, code coverage have 50%, which might indicate that the scenario is missing some key features of the design. Unfortunately, errors and bugs are often found in the missing points. To assure a high quality of functional verification, code coverage is important as well as functional coverage.

Coverage can be considered as a quantitative measure, which exhibits how thoroughly program is tested/simulated, and developers and vendors can use it to indicate their confidence in the readiness of their program [4]. As the RPS is safety critical system, the both coverages (functional and code) are sufficiently satisfied to detect and remove residual errors. However, FBD simulation and coverage measurement are not easy, since PLC software engineering tools provided by PLC vendors support for the FBD programming and simulation, working on their own tools and PLC hardware.

We developed a coverage measurement tool, ‘FBDCover’, and a fair tool, ‘FBDSim’, for FBD program simulation. It measures MC/DC and toggle coverage, and graphically shows the coverage result and the rank of each scenarios. The toggle coverage can help monitor the change of output variables and output of block, false-to-true and true-to-false. The MC/DC coverage can help confirm that all of decision cases of input in block are simulated. The coverages notify points of the design which is not simulated. Engineers can estimate quality of the scenarios. Besides, they can modify or add new scenarios for simulating unstimulated points with the result. The rank of scenarios, also, can help manage the scenarios for regression or additional simulation.

We performed a case study with an example replicating a bistable process (BP) of RPS [5] of ARP-1400 in Korean nuclear power plant in order to provide the efficiency of the proposed coverage measurement tool.

This paper is organized as follows: Section 2 provides techniques and tools used in the coverage measurement for FBD simulation. A case study with FBD examples of a Korean nuclear power plant is presented in Section 3 and Section 4 concludes the paper and provides remarks on future research extension.

2. Coverage Measurement for FBD Simulation

In this section some of the techniques used to measure the toggle and MC/DC coverage for FBD program simulation and some of developed tools are described.

2.1 Toggle Coverage for FBD Simulation

Toggle coverage, which is one of the oldest measurements of coverage in hardware design, measures the bits of logic that have toggled during simulation [6]. It focus on how a Boolean variable is changed which confirm only 1-to-0 and 0-to-1. Toggle coverage will show which signal did not change the state. A Boolean variable is said to be fully covered when it toggles back and forth at least once. If a bit is never changed, it has 0% toggle coverage. If a bit is changed from 0 to 1 and not changed from 1 to 0, the bit has 50% coverage. To achieve full coverage, a bit changed from 0 to 1 and 1 to 0 again. If a bit is never changed, engineers should doubt weather some condition is dead condition or not.

For the FBD simulation, the toggle coverage can be defined a condition set of output (1-to-0, 0-to-1) in each Boolean output variable, function block and block. The coverage measures whether each Boolean output variable, function block and block in an FBD program has been exercised and how often during validation. If an output variable has never toggled, it indicates any logic that effect a change the output variable has never been simulated.

2.2 MC/DC Coverage for FBD Simulation

The definitions of MC/DC and related terms in DO-178B [7] are as follows:

• Condition: A Boolean expression containing no Boolean operators.
• Decision: A Boolean expression composed of conditions and zero or more Boolean operators. If a condition appears more than once in a decision, each occurrence is a distinct condition.
• MC/DC: Every point of entry and exit in the program has been invoked at least once, every decision and condition in a decision has taken all possible outcomes at least once, and each condition in a decision has been shown to independently affect that decision's outcome. A condition is shown to independently affect a decision's outcome by varying just that condition while holding fixed all other possible conditions.

For the FBD simulation, the MC/DC coverage can be defined a combination of input conditions of each function block or block in FBD program. The coverage measures whether all of independent decision condition are simulated. If any condition has never simulated, it imply any condition can have errors or not.

For example, an AND block can have four input conditions - (0,0), (0,1), (1,0), (1,1), and the decisions are following combination - (0,1), (1,0), (1,1). The combination (0,1) and (1,1) indicate the independent effect of condition IN2 on the diction. Similarly the combination (1,0) and (1,1) indicate the independent effect of condition IN1. Table.1. shows some of examples of MC/DC coverage condition for function block and block.

Table I: An example of MC/DC coverage

	Inputs	MC/DC
AND	IN1, IN2	(0,1) (1,0) (1,1)
OR	IN1, IN2	(0,0) (0,1) (1,0)
GT,GE,LT,LE,EQ, NOT	IN1· IN2	(0), (1)
SR	SET, RESET, prev	(0,0,0) (0,0,1) (0,1,0) (0,1,1) (1,0,0) (1,1,0) (1,1,1)
RS	SET, RESET, prev	(0,0,0) (0,0,1) (0,1,1) (1,0,0) (1,0,1) (1,1,0) (1,1,1)
SEL	G	(0) (1)
MUX	K	(0 ~ Size of K)
TON	IN, PT<ET	(0,0) (1,0) (1,1)
TOF	IN, PT<ET	(0,1) (1,0) (1,1)

2.3 FBDSim: FBD Simulation Tool

Since PLC software engineering tools provided by PLC vendors support for the FBD programming and simulation, working on their own tools and PLC hardware, simulating FBD program and measuring coverage with the existing tools are not easy. We thus developed the 'FBDSim' for simulating FBD programs. Fig.1. shows 'FBDSim' which reads a set of FBD scenarios and writes the results into a text file. It automatically simulates FBD programs with tons of scenarios in a way of batch processing.

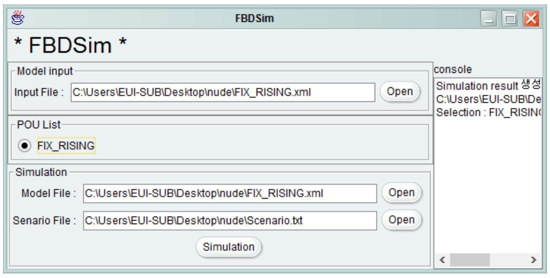

Fig. 1. A screenshot of the 'FBDSim'

2.4 FBDCover: Coverage Measurement Tool

The 'FBDCover', depicted in Fig.2, is a visual tool to show a percentage of coverage of MC/DC and toggle with graphic feature and a set of uncovered points in regard with MC/DC and toggle coverage with tree feature. One of the main goals of the coverage tool is to provide the user with informative presentation of coverage information and uncovered points information. The information can be used to increase a confidence of simulation quality. Engineers can modify and add new scenario in order to simulate the uncovered points.

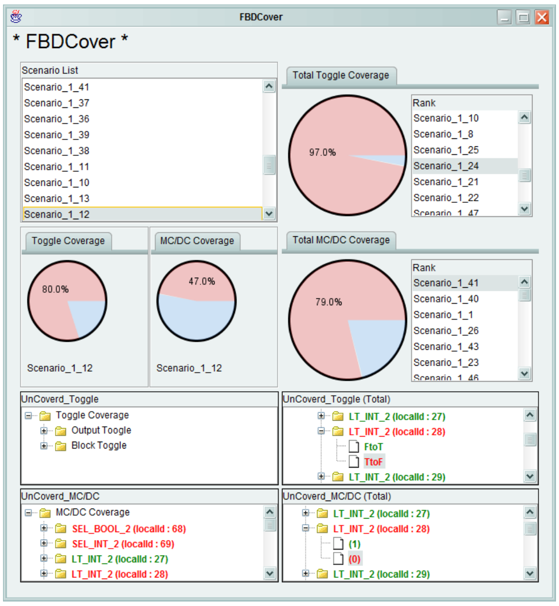

Fig. 2. A screenshot of the 'FBDCover'

The ‘FBDCover’ and ‘FBDSim’ are pair tool for FBD simulation and coverage measurement. While ‘FBDSim’ executes the FBD program, the tool identifies which points are executed, and then stores the result of coverage to the internal data structure. After the simulation by the ‘FBDSim’ is done, the ‘FBDCover’ reads the coverage and shows result with graphical and tree notation.

Another goal is to manage the scenarios used in simulation for regression testing or change of function. The ‘FBDCover’ provides ranking of scenarios based on MC/DC and toggle. Engineers can consider to withdraw scenarios, which have low coverage, for higher confidence of functional verification. Even engineers can generates more and more scenarios until 100% coverage.

3. Case Study

We performed a case study with an example replicating a bistable process (BP) of RPS in Korean. The BP reads 18 sensor values from a nuclear reactor and decides to generate trip/pre-trip signals out to shutdown the reactor immediately, if any value is out of safe range. We use the ‘FIX-RISING’ logic of RPS BP in this case study. The case study is aiming for showing the efficiency of the developed tools and the connectivity with other existing tool, we developed.

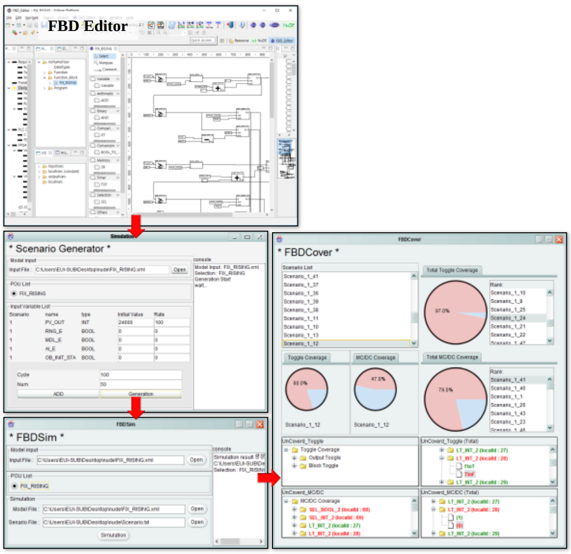

Fig. 3. A tool chain - ‘FBD Editor’, ‘Scenario Generator’, ‘FBDSim’, ‘FBDCover’

Fig.3. describes a tool chain used in case study. The tool chain consists of four tools such as ‘FBD Editor’, ‘Scenario Generator’, ‘FBDSim’ and ‘FBDCover’. We first designed a replication of RPS BP with ‘FBD Editor’. By just drag-and-drop, we designed all of functions of logic completely. Next, we generated a set of scenarios with ‘Scenario Generator’, which can generate random scenarios, while preserving predefined constraints such as rate-of changes of continuous input variables. Then, we simulated the FBD program with the scenarios by the ‘FBDSim’ and obtained both coverages and uncovered points in FBD program by the ‘FBDCover’.

4. Conclusions & Future Work

We developed a pair tool ‘FBDSim’ and ‘FBDCover’ for FBD simulation and coverage measurement. The ‘FBDSim’ automatically simulates a set of FBD simulation scenarios. While the ‘FBDSim’ simulates the FBD program, it calculates the MC/DC and Toggle coverage and identifies unstimulated points. After FBD simulation is done, the ‘FBDCover’ reads the coverage results and shows the coverage with graphical feature and uncovered points with tree feature. The coverages and uncovered points can help engineers to improve the quality of simulation. We slightly dealt with the both coverages, but the coverage is dealt with more concrete and rigorous manner. We are now planning to extend the coverage, analysis the coverage result and generates full coverage simulation scenarios.

Acknowledgements

This paper was supported by the Ministry of Science, ICT & Future Planning and the National Research Foundation of Korea (NRF-2015R1D1A1A02062154).

REFERENCES

[1] International Electrotechnical Commission, International standard for programmable controllers: Programming languages, part 3, 2003.

[2] Eunkyoung Jee, Junbeom Yoo, Sungdeok Cha and Doohwan Bae, A Data Flow-based Structural Testing Technique for FBD Programs, Information & Software Technology, Vol.51, No.7, July, pp.1131-1139, 2009.

[3] S. Richter, J. Wittig, Verification and validation process for safety I&C systems, Nuclear Plant Journal (May–June) (2003) 36–40.

[4] Yang, Qian and Li, J Jenny and Weiss, David M, A survey of coverage-based testing tools, The Computer Journal, Vol.52, No.5, pp.589-597, 2009

[5] Korea Atomic Energy Research Institute (KAERI), Software Design Specification for Reactor Protection System, KNICS-RPS-SD231 Rev.02, 2006.

[6] Jou, Jing-Yang and Liu, C, Coverage analysis techniques for hdl design validation, Proc. Asia Pacific CHip Design Languages, pp. 48-55, 1999.

[7] RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certification, December 1, 1992.