Transactions of the Korean Nuclear Society Spring Meeting
Chuncheon, Korea, May 25-26 2006

SDL-Based Protocol Validation for the Integrated Safety Communication Network in Nuclear Power Plants

Jung-hun Kim*, Dong-hoon Kim*, Dong-young Lee*, and Sung-woo Park**
**Korea Atomic Energy Research Institute, ** Hannam University*

1. Introduction

The communication protocol in nuclear power plants needs to be validated systematically to avoid the critical situation that may be caused by its own faults. We establish the methodology to validate the protocol designed for the Integrated Safety Communication Networks (ISCN) of Korea Nuclear Instrumentation and Control System (KNICS). The ISCN protocol is specified using the formal description technique called the SDL. The validation of ISCN protocol is done via the Simulator and Validator, both of which are main functions provided by the SDL.

2. Validation Methodology

The protocol validation is defined by a series of actions to examine the consistency between system requirements and protocol specification. Throughout the validation, we should be able to find out the potential errors that may happen during the process of protocol design. The design errors include deadlock, livelock and state ambiguity etc. We can also check whether the protocol performs its endowed functions precisely and satisfies the performance criteria [1].

2.1 Protocol Specification

The protocol validation must be preceded by the protocol specification based on the designed protocol. There are two alternatives to describe the protocol: informal description and formal description. While the former uses the natural language, the latter describes the protocol mathematically. Compared to the informal description, the formal description can be understood more precisely and implemented more easily. We use the Telelogic's Tau SDL suite to specify the protocol formally [2]. The advantages of SDL are as follow:

- The protocol can be specified by the set of well-defined concepts
- The specification is unambiguous, precise, and concise
- The verification can be done with respect to completeness and correctness

2.2 Validation Items

The protocol validation inspects correctness, safety, consistency and the liveness of protocol specifications. To be more concrete, the ISCN protocol has been validated for the following items.

- Deadlock: check if there exists no next state to which the current state transit
- Livelock: check if transitions occur repeatedly and infinitely among some particular set of states.
- Reachability: check if, according to the predefined transition sequence, a part or all states can be reached from the initial global state

2.3 Validation Procedure

As shown in Fig. 1, the validation of the ISCN protocol is performed via four steps: formal description, error check, simulation and validation.

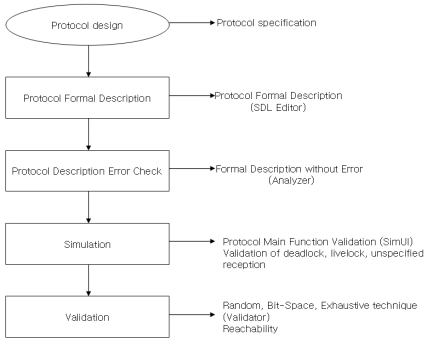

Figure 1: Validation procedure of ISCN protocol.

3. Formal Description

The ISCN protocol is applied for internal/external data exchanges among RPS, CPC and ESF-CCS systems. The basic characteristics of the ISCN protocol are as follow:

- The network topology takes the form of hierarchical star consisting of switches
- IEEE 802.15.4 [3] is adopted with the optional GTS changed to be mandatory to provide the TDMA-like data transmission
- The PHY layer is replaced by that of the IEEE 802.3 (Fast Ethernet)

For the SDL description, the ISCN protocol is configured with 10-function blocks as shown in Fig. 2.

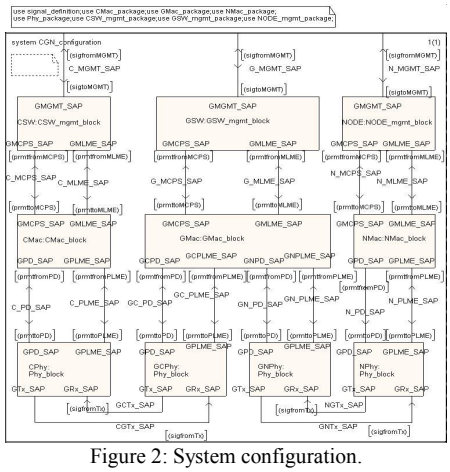

Figure 2: System configuration.

The whole system consists of CSW, GSW, and Node. Each device is designed to have PHY, MAC and management blocks. Some blocks in the CSW are appeared in Fig. 3.

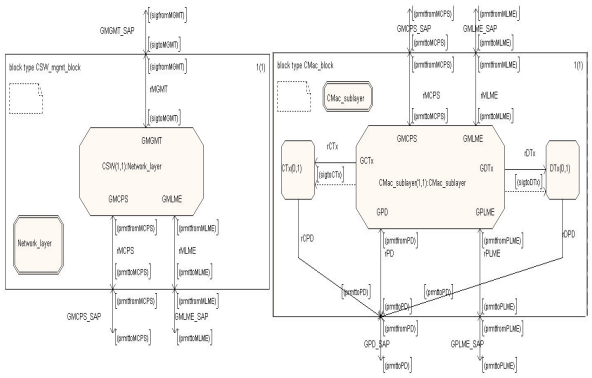

Figure 3: CSW's management and MAC blocks.

The signals are received through the channel SAP and delivered to process through the signal route. The Fig. 4 exhibits an example of process.

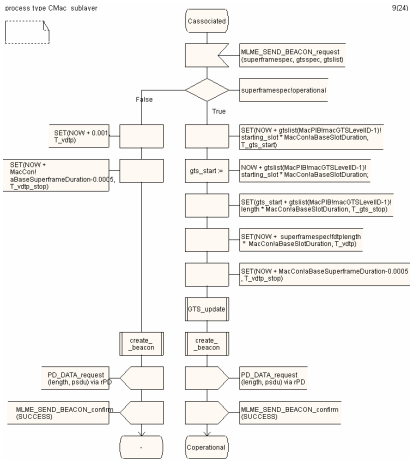

Figure 4: Process examination.

4. Protocol Validation

The SDL specification of the ISCN protocol is checked against the syntactic/semantic error, deadlock, and livelock using the SDL Analyzer and Simulator. The reachability analysis is performed through the SDL Validator [4].

4.1 Analysis

Using the Analyzer, we check and correct the syntax and semantic errors such as undefined characters, symbols and signals. The I/O assignment error of the system and the block is also validated using the Analyzer

4.2 Simulation

The deadlock, livelock and ambiguous states were validated using the Simulator. With the Simulator, the main functions of the ISCN protocol were modeled, and validated with the comparison of expectations and Message Sequence Chart (MSC) results. The Fig. 5 shows an example of MSC results for the function of data transmission.

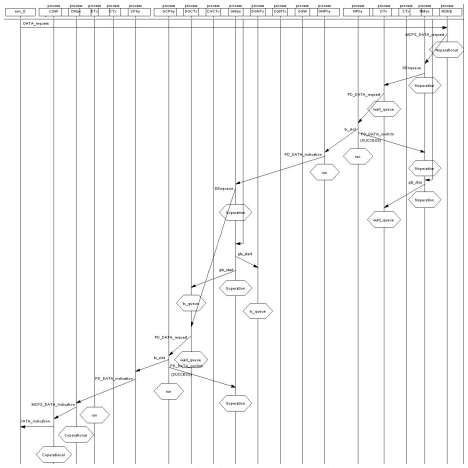

Figure 5: Data transmission from Node to CSW.

4.3 Validation

As a preliminary step, we perform the validation with the Navigator and Random Walk functions. Then, the reachability analysis is done with the Bit-State function which is based on state-space exploration method. The Fig. 6 shows an example of bit-state validation.

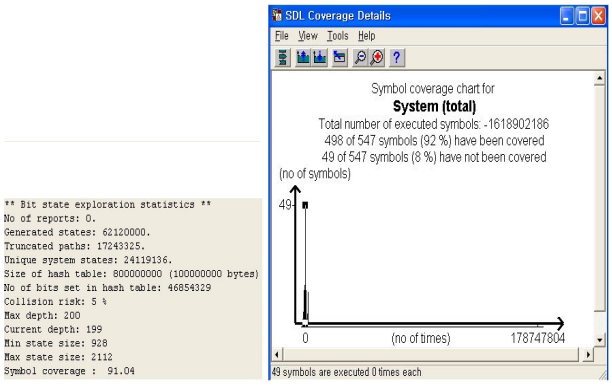

Figure 6: Validation results.

5. Conclusion

According to the generic methodology we established, the ISCN protocol has been specified using the SDL. Then the SDL specification of the ISCN protocol has been successfully validated using the SDL's analyzer, simulator, and validator. During the validation process, we could correct the 7 errors – 6 implicit signal consumptions and one decision error.

REFERENCES

[1] Marko Hannikainen, "Using SDL for Implementing a Wireless Medium Access Control Protocol," IEEE, 2000

[2] The user manual for Telelogic SDL TAU Suite 4.6, Telelogic AB

[3] IEEE Std. 802.15.4-2003, "Wireless Medium Access Control and Physical Layer Specifications for Low-Rate Wireless Personal Area Networks," 2003.

[4] Laurent Doldi, Validation of Communications Systems with SDL: The Art of SDL Simulation and Reachability Analysis, John Wiley & Sons, Ltd., 2003.