Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 10-11, 2007

Performance Analysis and Test Results of a High Reliablity-Safety Data Link (HR-SDL) for a Safety Grade PLC (POSAFE-Q)

Chang Hwoi Kim,[a] Dong Young Lee,[a] Hong Seong Park,[b]

a Korea Atomic Energy Research Institute, 150 Deokjin-dong, Yuseong-gu, Daejeon, Korea, 305-353, chkim2@kaeri.re.kr
b Kangwon National University, hspark@kangwon.ac.kr

1. Introduction

As a part of a Korea Nuclear Instrument & Control System (KNICS) Project, the HR-SDL communication module which uses Profibus FDL protocol based on SDN (Send Data with No acknowledge) has been developed. The HR-SDL will be used for transmitting a safety signal between safety channels. For this reason, the HR-SDL satisfies the independence requirements of Reg Guide 1.75 and IEEE std. 384, and it also satisfies the data communication requirements between the channels in a safety system referred to IEEE std. 7-4.3.2 Annex E-2003.

To evaluate the performance and reliability, a theoretical analysis was performed. The analysis items are a data transmission timing, and a recovery time with a token packet error, transmission fault rate, and so on.

To prove the performance of the HR-SDL, several tests such as component tests, integration tests, system tests, and equipment qualification tests were performed and successfully tested.

2. Functional Requirements

HR-SDL is the safety class communication module to transmit safety signal such as a reactor trip, and it has the following functions.

- Data flow of the HR-SDL should be in uni-direction and broadcasting method should be used. But, if it is used in the same channel, bi-directional communication is permissible.
- HR-SDL communication module should use deterministic protocol to secure the real time operation.
- Communication protocol of the HR-SDL is composed of minimum function rather than various functions, which should have self-diagnosis and security-authentication functions.
- HR-SDL should provide the cycle redundancy check function to confirm the integrity of communication data.
- The Communication data between processor module and HR-SDL shall be exchanged through shared memory without hardware and software interrupt.
- HR-SDL should provide 4 independent communication ports.
- The transmission time from one HR-SDL module to another PLC HR-SDL module should be 20ms at maximum.
- Loss of the HR-SDL module and/or the damage of communication path must not generate stall of processor module or unpredicted halt.
- HR-SDL transmission speed is from 9.6 Kbps to 12 Mbps, and user must be able to set the speed using an engineering tool.

3. Analysis of Data Transmission Property

To evaluate the performance and reliability, a theoretical analysis was performed. The analysis environment is shown in figure 1.

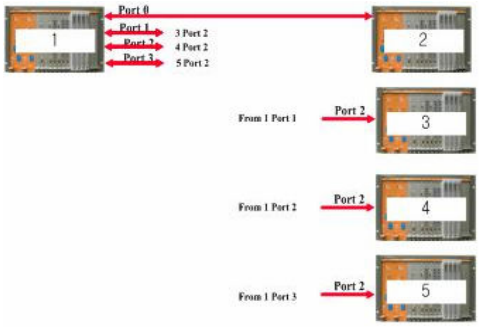

Figure 1. System configuration for theoretical analysis

3.1 Assumptions

For the analysis, we defined the following assumptions and conditions.

- Transmission speed is 12Mbit/s
- Data frame including header and data is 255 byte and maximum size of the transmission data in the frame is 244 byte.
- The synchronization time ($\mathbf{T_{SYN}}$) is 33 bit time at maximum.
- Propagation delay time does not consider because the HR-SDL uses fiber optic.
- Token data size is 64 bit at maximum.

3.2 Analysis of the transmission time

To evaluate the transmission time, we calculated the message cycle time (T_{MC}), token cycle time (T_{TC}), real rotation time (T_{RR}), target rotation time (T_{TR}), and token rotation time (T_{TRT}).

The calculated results show that the transmission time is within 10ms. At that time, a token rotation occurs 65 times. And also, the calculated delay time according to the token rotation time and HR-SDL transmission period (10ms) is as follow:

$0 \leq$ delay time ≤ 0.143942ms.

3.3 Analysis of transmission fault

To evaluate a transmission fault, we analyzed the error rate of the data frame and token frame. The calculated data frame error rate is 0.000002804999599303319 per data packet. And also, the calculated token error rate is 0.000000063999996302580 per token packet. Using these error rates, the calculated period of data packet error is 3,565,067.5(ms) and the period of a token packet error is 1,183,712(ms).

3.4 Analysis of delay time at token error

The recovery time caused by the token packet error is calculated by using the slot time (T_{SL})and idle time. According to KS Profibus specification, a time-out time (T_{TO}) is defined as follow:

$T_{TO} = 6 * T_{SL} + 2 * n * T_{SL}$ (n =0).

The calculated time-out time is 0.4498245ms. If a station does not receive a token within a time-out time, the station requires a token initialization caused by a token error. At that time, a token is re-generated from the lowest address station. And the data is re-transmitted after 10 token rotations. Thus, the recovery time is calculated as follow:

$T_{TO} + N*T_{TR} = 0.4498245\text{ms} + 10*0.143942\text{ms}$
$= 1.8892445\text{ms}.$

Where, the T_{TR} is Target Rotation Time.

From the analysis, we know that the maximum data delay time is 2.0331865ms and the delay time has no effect on a data transmission. And a data packet error occurs about once per hour. To reduce the error occurrence period, the same data should be sent several times within the scan time (10ms).

4. Performance Test and Results

To prove the performance of the HR-SDL, several tests were performed. To verify the functionality of the hardware and software component, the component test (CT) was performed.

And also, to verify the functionality and performance according to a component integration and a integration with a processor module, the integration test (IT) was performed successfully.

To prove the overall performance of the HR-SDL, the system test (ST) was performed. The test items are as follows:

- Response time test
  This test is to check the response time from a digital input to a HR-SDL output. For the response time test, the application program contains 2,000 simple logic elements within a 60% CPU load. Test results showed that the response time was within 2*scan time + HR-SDL delay time. The maximum response time was 87ms at 40ms the scan time. this result satisfies our requirements (100ms).
- Deterministic performance test
  This test is to verify the deterministic capability according to a variation of the CPU load in processor module. Test results showed that the HR-SDL transmission performance did not depend on the CPU load.
- Data transmission error characteristic test
  This test is to verify the fail safe capability when a data transmission error occurs in the communication path. Test results showed that the CPU did not halt in split of communication path error and HR-SDL module error.
- Data transfer rate test
  This test is to verify the data transmission rate at a normal, off-normal, and error operation. The rate is calculated in bps(bit per second). Test results showed that the data transfer rate did not change.

5. Conclusion

HR-SDL communication module was developed for a safety grade PLC. This module uses deterministic, uni-direction, and broadcasting methods, And the HR-SDL protocol is Profibus FDL (Fieldbus Data Link) with SDN (Send Data with No acknowledge). To evaluate the performance and reliability, a theoretical analysis was performed. The analysis items were the data transmission timing, recovery time when a token packet error occurred, and transmission fault rate. And to prove the performance of the HR-SDL, several tests such as component tests, integration tests, and system tests were performed. The test results satisfied the requirements and specifications

REFERENCES

[1] IEEE Std. 7-4.3.2-2003, Standard Criteria for Digital Computer in Safety Systems of Nuclear Power Generating Stations.
[2] NUREG/CR-6082, Data Communications, 1993.
[3] USNRC Reg. Guide 1.152, Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants, Rev. 01, Jan. 1996.
[4] SIEMENS SIMATIC NET ASPC 2 / HARDWARE User Description (Advanced PROFIBUS Controller according to EN 50 170), Ver 2.0, July 1999.