Transactions of the Korean Nuclear Society Spring Meeting
Gwangju, Korea, May 30-31, 2013

Segmentation Scheme for Safety Enhancement of Engineered Safety Features Component Control System

sang-seok LEE[a*], kwang-young SOHN[a], jun-ku LEE[b], geun-ok PARK[b]
[a]*Nuclear Engineering, Korea Reliability Technology and System (KoRTS)*
[b]*Research Reactor Engineering Division, Korea Atomic Energy Research Institute (KAERI)*
[*]*Corresponding author: kysohn@korts.co.kr*

1. Introduction

Segmentation scheme is required to improve Common Caused Failure (CCF), to prohibit failure propagation and to apply functional diversity. However ESF-CCS in existing reactor is designed to meet requirements of defense in depth and diversity. But it increases CCF rate, because the most implementations are using the same devices, the same functions and the same loads in redundancy systems in the same channel. CCF or undetectable failure would adversely impact safety functions of ESF-CCS in the existing nuclear power plants. We propose the segmentation scheme to solve these problems. Main function assignment to segments in the proposed segmentation scheme is based on functional dependency and critical function success path by using the dependency depth matrix. The segment has functional independence and physical isolation. The segmentation structure is that prohibit failure propagation to others from undetectable failures. Therefore, the segmentation system structure has robustness to undetectable failures. The segmentation system structure has functional diversity. The specific function in the segment defected by CCF, the specific function could be maintained by diverse control function that assigned to other segments. Device level control signals and system level control signals are separated and also control signal and status signals are separated due to signal transmission paths are allocated independently based on signal type. In this kind of design, single device failure or failures on signal path in the channel couldn't result in the loss of all segmented functions simultaneously. Thus the proposed segmentation function is the design scheme that improves availability of safety functions.

2. Methods and Results

In this section some of the techniques used to segmentation are described. The Segmentation scheme includes a Requirement, method, Segmentation structure.

2.1 Requirements

The factors for establishing segmentation design are composed of functional dependency requirements, critical functional requirements, and actuation signal path requirements. The requirements shall meet IEEE 603.[1]

2.2.1 Functional dependency requirements.

- Keeping independency between segments
- Establishing the basic group for conducting the safety function
- Preventing manual actuation control from devastating the independency between segments
- Design separate segmentation for component that is functionally independent and identical target of function
- Indentifying the degree of functional dependency through DDM (Dependency Depth Matrix)
- Keep the precedence of NSSS control function
- Critical function shall not be disturbed by any reason
- Design segmentation for the independent functions and components in consideration of success path and functional requirements

2.2.2 Critical function requirements

There are multiple signal success paths to achieve the critical functionality. Regarding this, the function that is not dependent as a result of dependency analysis shall be isolated.

Critical function	Safety Grade
Reactivity Control	Reactor trip
	Safety injection
Core heat removal	Natural Circulation
	Safety injection
Control RCS inventory	Safety injection
	Shutdown cooling inventory control
Control of RCS pressure	Safety injection
	RCS coolant gas exhaust
	Primary release
RCS Heat removal	Residual heat removal
	Shutdown cooling
	SI/SDC initiation and exhaust

2.2.3 Signal path and transmitter requirements

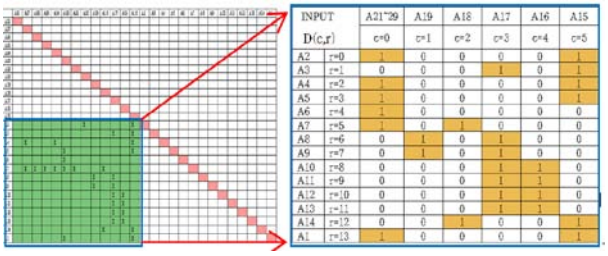
ESF-CCS function shall be maintained in spite of the loss of the single signal path and the transmitter. The requirements for this condition are as follow;

- The actuation signal of the system level and component level of ESF-CCS actuation signal shall be isolated.

- The signal path and transmitter of control signal and status feedback signal shall be isolated

2.2 Methods

1. List up the control target components that are actuated by more than one ESF-CCS actuation signal including NSSS and BOP.
2. Generate the DM (Dependency Matrix) indicated in Figure 1. DM is generated according to " Binary Matrices in System Modeling"[2]



INPUT	A21~39	A19	A18	A17	A16	A15
D(c,r)	c=0	c=1	c=2	c=3	c=4	c=5
A2	r=0	1	0	0	0	0	1
A3	r=1	0	0	0	1	0	1
A4	r=2	1	0	0	0	0	1
A5	r=3	1	0	0	0	0	1
A6	r=4	1	0	0	0	0	0
A7	r=5	1	0	1	0	0	0
A8	r=6	0	1	0	1	0	0
A9	r=7	0	1	0	1	0	0
A10	r=8	0	0	0	1	1	0
A11	r=9	0	0	0	1	1	0
A12	r=10	0	0	0	1	1	0
A13	r=11	0	0	0	1	1	0
A14	r=12	0	0	1	0	0	1
A1	r=13	1	0	0	0	0	1

Figure 1 Making Dependency Matrix

3. Generate the RDM(Raw Data Matrix) based on the formula 1 using DM, and finally DDM by multiplying MM (Masking Matrix) using formula 2.
   And draw the block diagram for identification.

$$D(c,r)\underset{c}{=}\begin{matrix}0 \text{ or } 1\\ =i \text{ or } j\end{matrix}$$
$$R(i,j)=\sum_{r=0}^{r=k} D(i,r)*D(j,r) \cdots\cdots\cdots \text{(Formula 1)}$$

where
D = Dependency Matrix for Input c = Inputs Variables(actuation signa
a= Outputs Variables (ESF) k = Total Outputs (ESF)
T = Dependency Depth Matrix i, j = Colums Variable
M = Masking Matrix R = Raw Data Matrix

$$Y(i,j)=M(i,j)*R(i,j) \ldots\ldots \text{(Formula 2)}$$

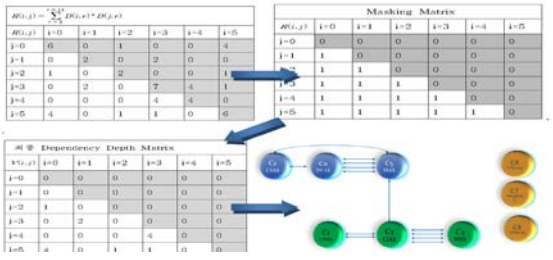


Figure 2 Dependency Block Diagram

The number of arrow in Figure 2 means the degree of dependency, arrow itself means the interface of dependent functionality. The function without arrow means independent function.

Base on this, the component signal is transmitted through isolator to component by splitting the interaction that has a low dependency unless it damages the independency between segmentation. Thus the component receives the signal from the two segments through the OR logic operation.In summary, it is possible to categorize the three groups such as independent component group, the group that has low dependency and the other

2.3 Allocate major function

Using the DDM, major function of ESF-CCS is allocated into the each segment, and the component that is actuated by major function and the safety grade functions, and the components that have a different success path and diverse signal path is allocated into different segment.

Then if the transmitter and signal path is isolated based on this methodology, the structure of ESF-CCS is modeled as in Figure 3

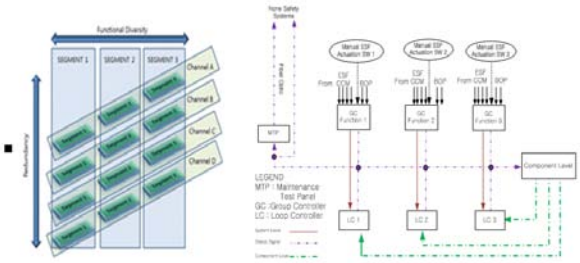


Figure 3 The segmentation structure

3. Conclusions

In conventional ESF-CCS, the single controller generates the signal to control the multiple safety functions, and the reliability is achieved by multiplication within the channel.

This design has a drawback causing the loss of multiple functions due to the CCF (Common Cause Failure) and single failure

Heterogeneous controller guarantees the diversity ensuring the execution of safety functions against the CCF and single failure, but requiring a lot of resources like manpower and cost.

The segmentation technology based on the compartmentalization and functional diversification decreases the CCF and single failure nonetheless the identical types of controllers are arranged. Also ESF-CCS in commercial legacy plant can be re-designed to acquire the safety by function re-allocation without the hardware replacement.

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No. 2012M2A8A4025979)

REFERENCES

[1] IEEE Std 603 " IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations", 2009.
[2] Warfield, John N, " Binary Matrices in System Modeling" IEEE Transactions on Systems, Man, and Cybernetics, vol. 3, pp. 441-449, 1973.