Proceedings of the Korean Nuclear Society Autumn Meeting
Taejon, Korea, October 2000

Segmentation Methodology Analysis for Effective Digital Control System Implementation

Jin Woong Lee, Jeong Heung Bang and Moon Jae Choi
Korea Power Engineering Company Inc.
360-9 Mabuk-ri, Kusong-myon, Yongin-shi, Kyunggi-do, Korea

Abstract

The digital control system is one of the advanced design features adopted for improving the technical and economical advantages for Korean Next Generation Reactor (KNGR). Due to the safety constraints of nuclear power plant, the advanced I&C and MMI systems have been required to be designed to protect the system against failures of I&C and MMI equipment which may degrade the performance of more than one major control or monitoring function. The functional and physical designs of these systems are segmented or explicitly incorporate other functional defensive measures to inhibit the propagation of failures across major functions. The functional and component grouping methodology, which is called 'segmentation', has been analyzed and the optimal segmentation methodology is suggested in this paper.

1. Introduction

Availability and reliability of the I&C and MMI systems is of paramount importance in the advanced nuclear power plant. Since it is expected that newer technologies will be applied in the I&C and MMI systems, including use of computers and multiplexed data transmission for which it is easy and cost-efficient to perform many functions in a single piece of equipment, the requirements need to ensure that the design is as "forgiving" as possible in terms of the probability and consequences of failures of this potentially shared equipment. Therefore segmentation methodology has focused on the defense-in-depth: to provide a greater degree of assurance that failures will be limited in their effects such that, if they occur, they cannot propagate across more than one major control function.

This paper addresses the necessity and design consideration for segmentation in advanced nuclear power plants by identifying segmentation configuration and its procedure for assignment to support meeting plant availability and reliability goals.

2. Review of Functional Group Configuration

Plant components which are controlled through the dedicated control system have been controlled using dedicated circuits for each component. However, a review of the plant components and the process system in which they reside shows that a majority of the components do not possess a unique functional identity in that they are not individually important to the plant but are collectively important as a part of a subsystem or group.

Looking at a system very simplistically, the valves in a fluid flow path are of little importance without the pump that drives the fluid. Conversely, the pump is of no value if the valves in a fluid flow path cannot be opened. This fundamental observation is the basis for the system configuration of the multi-loop control system.

2.1 Configuration of Multi-loop Control System

In the multi-loop control system, functionally dependent components are controlled by a microprocessor. The multi-loop control system consists of numerous subsystems to allow the independence that exists within the mechanical systems to be duplicated in the microprocessor based system. Therefore where flow path independence exists in a process system, that same independence is achieved through separate subsystems in the multi-loop control system. Where component redundancy exists in the mechanical system, that redundancy is maintained through separate subsystems in the multi-loop control system. Each subsystem of the multi-loop control system is electrically independent of every other subsystem such that failures do not propagate among subsystems and such that maintenance and testing can be conducted on a subsystem basis, without interfering with other plant functions.

2.2 Comparison to Dedicated Control System

Comparing the functional group control of multi-loop control system to dedicated control system designs which use dedicated logic circuits for each plant component, it can be seen that although the multi-loop control system does not achieve the same degree of independence for each component, that individual independence is of no value in a process system where the components are dependent upon each other. The important fact is that the multi-loop control system achieves the same level of independence as in the process system itself.

In fact, additional independence within the dedicated control system beyond that which exists in the process system is a detriment to system reliability. For example, a process system with ten

inter-dependent components is controlled in the multi-loop control system by one microprocessor. In the dedicated control system designs this same process system would be equivalent to being controlled by 10 microprocessors. In the multi-loop control system, a failure of the one microprocessor would render this system inoperable. In the dedicated control system design, a failure of any one of the 10 processors would render the system inoperable since all components are needed for system operation. Therefore the multi-loop control system would demonstrate to provide a 10 to 1 reliability improvement over the dedicated control system.

Another benefit of the functional group configuration can be seen in failure mode and effects analysis. Since components are assigned to functional groups of the multi-loop control system in a manner consistent with their process relationship, the effects of failures are predictable and manageable. Dedicated control system designs utilize dedicated processors for each component but that component independence is compromised through sharing of power supplies, auxiliary logic modules and auxiliary I/O cards. Failures in shared devices can effect large number of unrelated plant components, requiring difficult failure modes analysis often with unacceptable results. The functional group design of the multi-loop control system, however, achieves the functional circuit independence.

2.3 Comparison to Centralized Control with Redundancy

Another traditional control system configuration approach used commonly in process control industries is to group very large numbers of plant components into control systems that employ microprocessor in a redundant pair configuration. This type of system reduces the number of electronic components even further than achieved in the functional group configuration, therefore, long MTBF can be achieved.

However, when failures occur that cannot be accommodated by the built-in redundancy the effects can be catastrophic. Depending on the number of components and their dispersement in the process, the effects are usually worse than complete cabinet failures in a traditional control system design.

2.4 The Right Compromise

The dedicated control system usually achieves low MTBF and poor cost in spite of higher degree of individual independence and licensability advantage. While improving in MTBF and economy due to reduction the number of electronic components, the centralized control system could have deficiency of licensability.

KNGR has adopted the functional group configuration design as the right compromise between the centralized-redundant design and the single processor to component configuration of the traditional control system. The functional group configuration offers appropriate improvement of MTBF and cost-efficient factor over the traditional control system while maintaining manageable failure modes.

3. System Segmentation

A segmentation is performed on the KNGR design based on observing two levels of functional based segmentation. This task is performed using the following methodology and definitions.

Functional grouping (LEVEL 1) – The first level of groupings establish a set of groupings that are consistent with functional boundaries of the physical systems, system definitions, and based on an overview of a grouping of systems and functions (e.g. primary systems, secondary systems, and support systems).

Component groupings (LEVEL 2) - The second level of groupings follow a very simplistic perspective to further group components defined by LEVEL 1 consistent with functional plant processes.

3.1 LEVEL 1 Segmentation

This segmentation establishes the first level of functional groupings (LEVEL 1) to set groupings based on requirements for safety related and non-safety related functionality and then significant functional boundaries, secondary systems and support systems are established for maintaining the high level functional objectives of the design. For each safety function there are multiple, diverse success paths. A success path is a set of components and resource commodities that, if operable, is sufficient to satisfy a particular safety function. Diverse success paths provide multiple means to accomplish a single safety function. Within individual success paths there may be replication of capacity as well. To meet the functional objectives, specific critical safety functions that focus on operations based functional processes are required during emergencies. There are also operations based functional processes for normal plant operations. Typically these are based on non-safety related functional processes. Therefore for achieving the plant critical safety functions, diverse success paths shall be maintained. Also all component grouping assignments should be made to optimize the available success paths to satisfy an

operational objective.

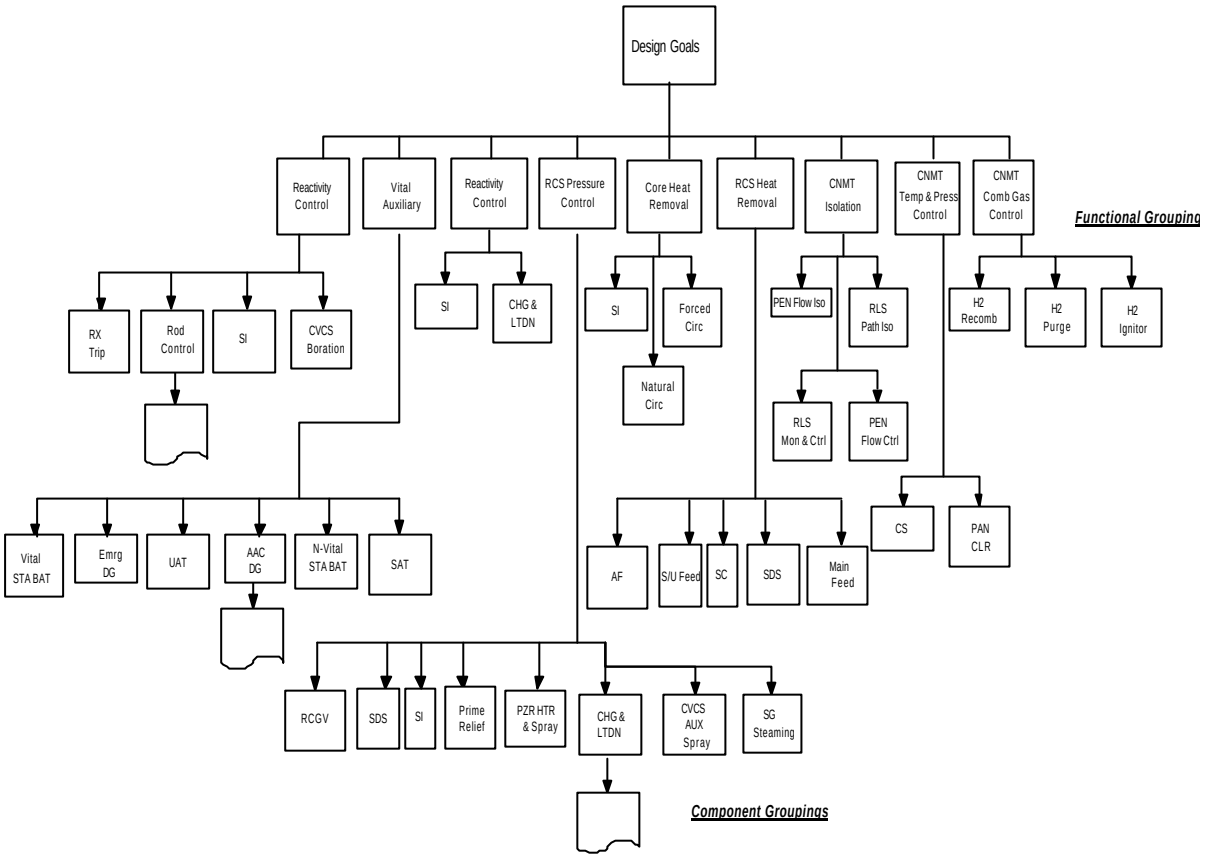

Figure 1. Critical Functions and Success Paths

3.2 LEVEL 2 Segmentation:

Component grouping is provided to accomplish the plant functions defined to meet the high level objective. These functions are expressed in terms of the functional division of physical systems as sets of components and piping configurations which define a plant process that supports operations for the high level function. The plant processes to accomplish this are then defined as sets of component groupings (LEVEL 2).

Component grouping level of segmentation emphasizes the functional divisions of the plant and not the traditional divisions based on physical systems. The following is a method for assignment of plant components to control system subgroup segments.

1) Assign functional independent components to each loop controller based on their

own power train

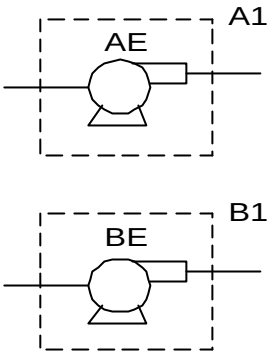

Figure 2. Functional Independent Configuration

2) Assign components of serial configuration to the same loop controller except for isolation function

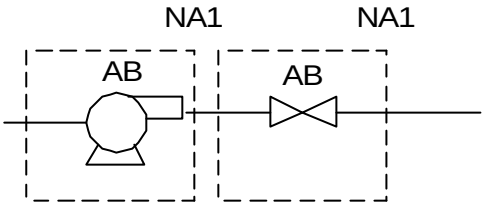

Figure 3. Serial Configuration

3) Assign components of parallel configuration to another loop controller even though they have the same power train

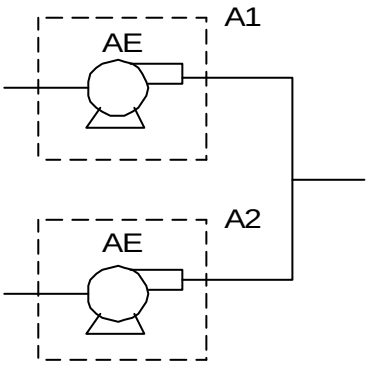

Figure 4. Parallel Configuration

4. Implementation and Analysis of Segmentation

Plant components and the interfacing instrument loops are divided into the following seven divisions in accordance with the KNGR System Diagram:

	Train Designation
• Safety Related ‘A’ SR-A	AE
• Safety Related ‘B’ SR-B	BE
• Safety Related ‘C’ SR-C	CE
• Safety Related ‘D’ SR-D	DE
• Non-Safety Related ‘A’ NSR-A	AB
• Non-Safety Related ‘B’ NSR-B	BB
• Non-Safety Related ‘E’ NSR-E	EB

Each division AE, BE, CE, DE, AB, BB and EB will have the required number of groups depending upon its ability to satisfy the design philosophy based on Level 1 Segmentation. The component assignment to groups is based on instrument channel redundancy and the flow path redundancy provided by the piping configuration with Level 2 Segmentation. Components within each group are grouped and assigned to unique microprocessor. Separate group assignment are also dictated by the presence of vital redundant equipment such as pumps. The microprocessor based control system design maximizes system availability and reliability through coordination of mechanical flow paths and instruments and components segmentation. The aim of the final grouping is to tolerate a single group failure without the loss of vital operation within the constraints of the piping and component configuration and ensure that mechanically redundant components remains functional.

4.1 Functional Groups

As previously explained, the plant components are divided among the seven (7) divisions. The P&ID has already assigned power train designations of all components. Within the constraints of the division assignments, various functional groupings are created to accommodate the design philosophy. In summary, the functional groupings, which are broken down into group control segment and loop controller component assignments, will support the followings:

1) Take advantage of redundancy of flow paths.
2) Take advantage of redundancy of components.
3) Maintain independence of flow paths.
4) Limit the size of the group to achieve higher level of failure tolerance.
5) Maximize failure tolerance, including considerations from hazard analysis.

and are consistent with:

6) The plant piping and instrumentation diagram (P&IDs).
7) Fluid system design instrumentation and component control design requirements.
8) Component design requirements.
9) Fluid system design operational requirements.
10) Instrumentation and control requirements for control system.
11) Interface requirements for component controls and process instrumentation.
12) System operational requirements.
13) Component technical manuals/system descriptions/specifications.
14) General arrangement drawings.

After initial assignments are made, components are rearranged as necessary to form more compact and cohesive groups as other systems and components are grouped. Final group assignments are made based on a review of the design as evaluated with respect to a system failure mode and effects analysis.

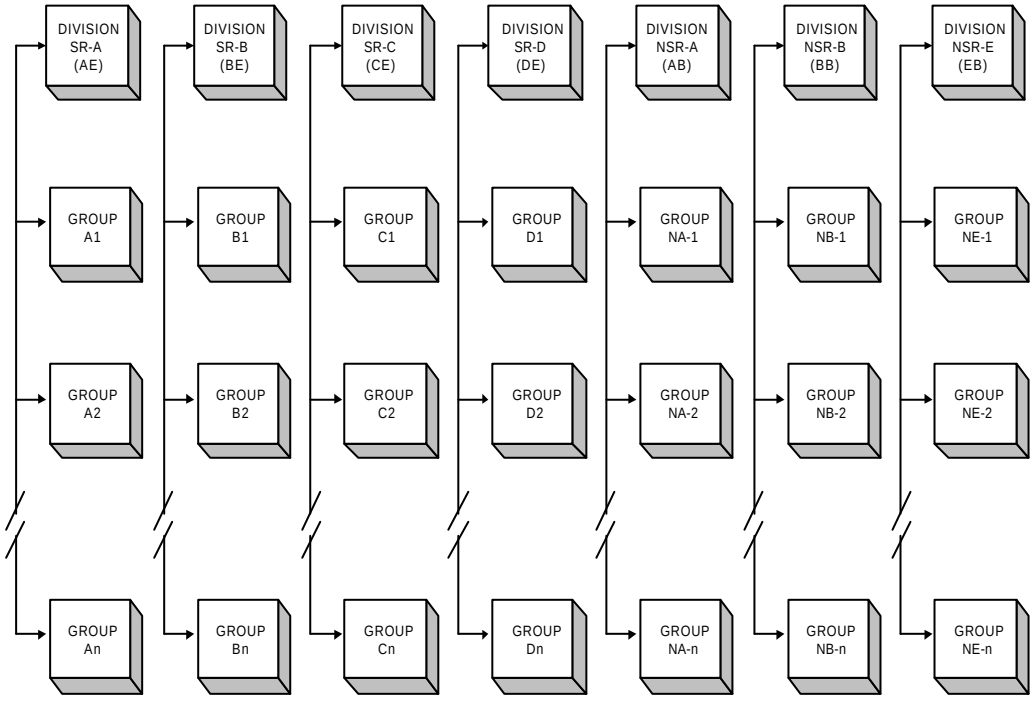

Figure 5. Control System Group Configuration

The control system group configuration is shown in Figure 5. Each block represents a group. The divisions are shown to have multiple groups in Figure 5. Each group will have the required number of components depending upon its ability to satisfy the design philosophy.

Assuming that each digital input and output per component is assigned with 6 and 2 points respectively, functional loop is composed of the simplest design structure with only a microprocessor, D/I, D/O and rack using the PLC based control system, especially Modicon PLC 984-685 series. After analyzing the MTBF of functional loop based on calculations in accordance with MIL-STD-217 to reflect actual field experience, each loop MTBF based on 1000 components per plant is as follows; 743.99(1 comp/loop), 1487.98(2 comp/loop), 2568.66(4 comp/loop), 3897.04(8 comp/loop), 5198.99(16 comp/loop) and 6143.42(32 comp/loop). Based on the MTBF calculation results, the MTBF of 4 comp/loop design is about 3.5 times better and the MTBF of 16 comp/loop design is approximately 7 times better than that of 1 comp/loop design.

However, as can be seen on the above data, there are little differences between 16 comp/loop and 32 comp/loop on the MTBF. Assuming that the failure of a loop assigned lots of components would render them inoperable at one time, it is optimal segmentation to assign less than 16 components per loop with the right compromise on reliability and safety.

4.2 Failure Mode and Effect Analysis

FMEA is performed to assess the extent to which the system complies with the criteria. From the worksheets, listings can be made with information about failure modes that cause various system effects, the existence of components or portions of the system for operational if a single failure occurs, and the means by which failures can be detected or annunciated. The assignment number of components to a group based on Level 2 Segmentation could be variable as the result of the FMEA. Also if the result of the analysis for the system segmentation does not meet the design requirements, the segmentation shall be performed again appropriately.

The segmented control system achieves high reliability and manageable failure modes by grouping mechanically dependent control functions together into common control equipment and separating independent control functions into different segments of the control system. This technique minimizes the number of electronic circuit modules in the control system, thereby maximizing MTBF. At the same time it achieves manageable failure modes since all components in a process loop are controlled by a common control equipment that has a predictable failure mode.

5. Conclusion

The Multi-loop controller configuration of the control system design provides a unique combination of advantages when compared to either a centralized-redundant design or the single processor to a component configuration of the traditional control system. These include a significant increase in MTBF which can support improved plant capacity factor while simultaneously reducing plant capital and O&M (Operational and Maintenance) cost by minimizing hardware. Further, appropriate attention to the multi-loop functional design during preparation of plant maintenance procedures can also lead to improvements in safety. The multi-loop design approach provides the opportunity for highly leveraged application of engineering resources.

Acknowledgement

This work has been carried out under the nuclear research and development program by Korea Electric Power Company and Ministry of Science and Technology in Korea.

References

[1] ANSI/IEEE, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations", ANSI/IEEE Std. 7-4.3.2-1993, Feb., 1994.
[2] Combustion Engineering, 'Nuplex 80+ Advanced Control Complex-Volume III Reference Design Documentation", Rev. 00, Apr., 1990.
[3] EPRI, "Advanced Light Water Reactor Utility Requirements Document-Volume II ALWR Evolutionary Plant", Rev. 7, Dec., 1995.
[4] IEEE, "IEEE Application Guide for Distributed Digital Control and Monitoring for Power Plants", IEEE Std. 1046-1991, Oct., 1991.
[5] I.N. Choe, M.J. Choi and J.W. Lee, 'Segmentation Methodology Analysis for Effective Digital Control System Implementation", Power Engineering, Volume 8, Jul., 1997.