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

Guidelines for Defense-in-Depth and Diversity Activities in Digital Instrumentation and Control Systems

S. W. Cheon, J. Y. Kim, J. S. Lee, K. Y. Lee, and J. K. Park

Korea Atomic Energy Research Institute
150 Dukjin, Yusong, Taejon 305-351, Korea

Abstract

Digital Instrumentation and Control (I&C) systems are becoming an ever-increasing part in I&C systems of nuclear power plants due to such features such as versatility, flexibility, and reduced sizes. The digital technology introduces a possibility that common-cause or common-mode failures (CCF or CMF) may cause redundant safety systems to fail in such a way that there is loss of safety function. A special form of CMF analysis called "defense-in-depth and diversity" (D-in-D&D) analysis has been developed to identify possible common-mode failure vulnerabilities and to support a specific licensing action in digital systems. There are two main stages in D-in-D&D activities: both plan and analysis. How to plan and analyze D-in-D&D in digital I&C systems is important to minimize the possibility of CMFs and thus increase the plant reliability. This paper describes the guidelines for D-in-D&D activities in digital I&C systems.

1. Introduction

Instrumentation and control (I&C) systems in nuclear power plants help ensure that the plant operates safely and reliably by monitoring, controlling, and protecting critical plant equipment and processes. The potential for common-cause or common-mode failures (CCF or CMF) has become an important issue as the software content of digital I&C systems has increased. CCFs are multiple component failures having the same cause. CMFs denote the failure of multiple components in the same way, such as stuck open or fail as-is [1].

The potential for CMFs was not present in earlier analog I&C systems used in operating nuclear power plants because it could usually be assumed that CMF, if it did occur, was due to slow processes such as corrosion or premature wear-out. This assumption is no longer true for systems containing digital software, which are used in advanced light water reactors (ALWR). Specifically, digital I&C systems share more data transmission functions and share more process equipment than their analog counterparts. Redundant trains of digital I&C systems may share databases (software) and process equipment (hardware). With the advent of software operated devices—where multiple redundant units would all be executing the same program with essentially the same inputs and outputs and more-or-less synchronous—the possibility of simultaneous failure in redundant units becomes all too real.

A special form of CMF analysis called "defense-in-depth and diversity" (D-in-D&D) analysis has been developed to identify possible common-mode failure vulnerabilities in digital systems. *Defense-in-depth* is the concept of multiple lines of defense against a perceived threat so that if one line of defense is penetrated, another line is invoked to limit the damage caused by the penetration. This can be carried through several levels, i.e., "echelons of defense." According to NUREG/CR-6303 [2], digital I&C systems should provide four echelons of defense: i.e., control system, reactor trip system (RTS), engineered safety features actuation system (ESFAS), and a monitoring and indicator system. *Diversity* is the notion that if redundant systems are different in some substantial way from each other, a failure in one will not necessarily imply a failure in the other. NUREG/CR-6303 [2] describes six

important types of diversity: human diversity, design diversity, software diversity, functional diversity, signal diversity, and equipment diversity.

NUREG-0493 [3] was an assessment of a single reactor protection system (RESAR-414 IPS) that addressed common-mode failure concerns and introduced a method of analysis. In SECY 91-292 [4], the staff included discussion of its concerns about common-mode failures in digital systems used in nuclear power plants. As a result of the reviews of ALWR design certification applications that used digital protection systems, the staff documented an initial statement of a four-point D-in-D&D requirement. This position was documented as Item II.Q in SECY 93-087 [5] and was subsequently modified in the associated Staff Requirements Memorandum (SRM) [6]. Based on experience in the detailed reviews, the US NRC has established the modified four point position on D-in-D&D for the advanced reactors as a branch technical position, BTP-19 [7]. NUREG-0493 has been rewritten and extended as NUREG/CR-6303 [2]. NUREG/CR-6303 is advisory for the assessment of the ALWR designs and the method described is not mandatory. IEC 60880 [8] summarized possible diverse features against software-induced CMFs. Issues of common-mode software failure potential were discussed in [1].

There are two main stages in D-in-D&D activities: both *plan* and *analysis*. How to plan and analyze D-in-D&D in digital I&C systems is important to minimize the possibility of CMFs and thus increase the plant reliability. This paper describes the guidelines for D-in-D&D activities in digital I&C systems. Figure 1 shows overall classifications of D-in-D&D planning and analysis activities.

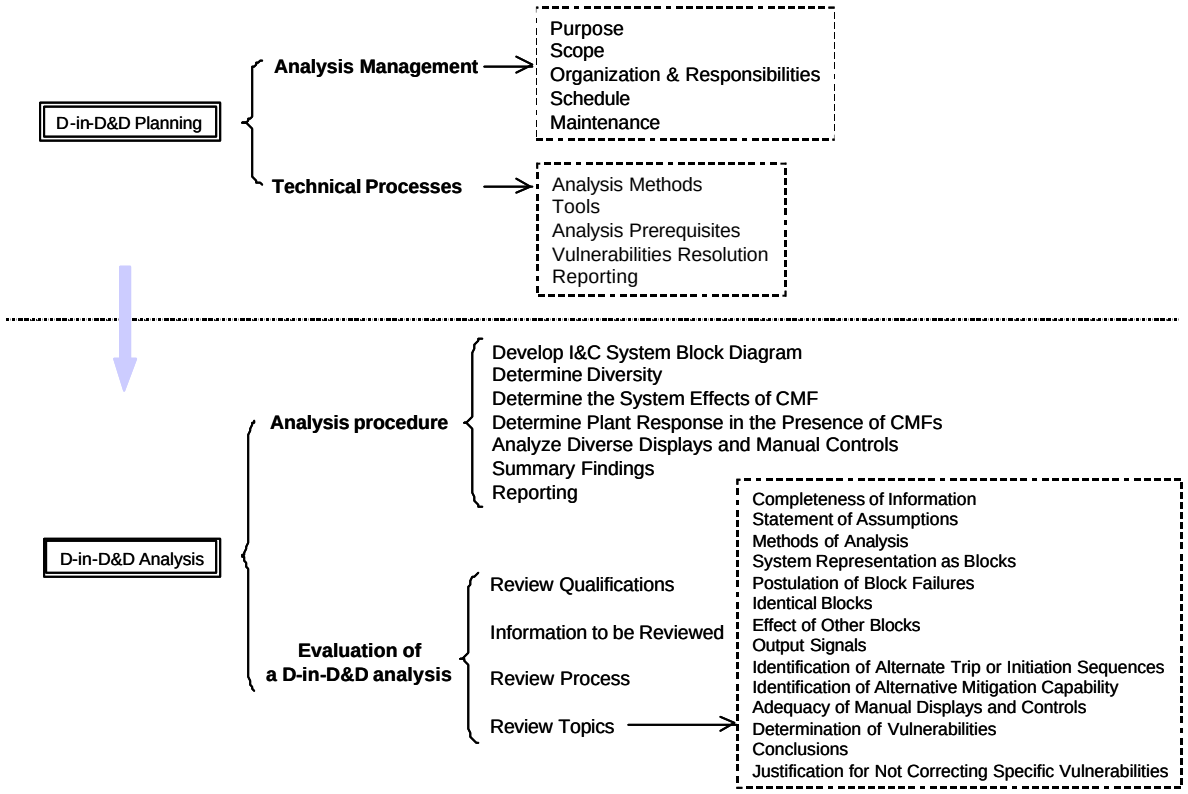

Fig. 1 Overall classification of D-in-D&D planning and analysis

2. Planning of D-in-D&D

Regulatory authorities may wish to review a D-in-D&D plan to ensure that an appropriate analysis will be produced and to minimize the need for re-work after the evaluation is complete. This section describes issues that should be considered in planning to perform a D-in-D&D analysis, presuming that analyses of plant response to design basis events are a separate effort.

D-in-D&D plans are expected to be relatively shorter and more concise than D-in-D&D analyses. Therefore, peer review of the plans is an appropriate technique for plan review. Following up the review with a walkthrough meeting between the reviewer and the vendor is a recommend method for resolving comments on the plan.

Topics to be considered in reviewing D-in-D&D plans should consider the planning characteristics described in NUREG-0800, BTP-14 [9], the D-in-D&D review guidance of BTP HICB-19 [7], and the planned application of the D-in-D&D analysis guidelines in NUREG/CR-6303 [2].

2.1 Analysis Management

2.1.1 Purpose

The purpose of the D-in-D&D analyses should be identified. Typically, the purpose should be to analyze the computer-based nuclear reactor protection system in order to discover and identify design vulnerabilities to CMFs and to support a specific licensing action.

The D-in-D&D analysis involves three major activities.

1. Construction of a system model that describes what portions of the design have a potential for common mode failure. Typically, this system model is in the form of a block diagram with supporting information on describing the dependencies between blocks.
2. Analysis of the I&C system response to design basis events (i.e., design basis accidents and anticipated operational occurrences) in combination with assumed common mode failures.
3. Analysis of the plant and offsite consequences of the combination of design basis events and common mode failures.

2.1.2 Scope

The bounds of the analysis should be identified. This should include i) identification of the systems and equipment to be considered in the CMF analysis, ii) the systems to be considered as candidate diverse back-up systems, and iii) the set of anticipated operational occurrences (AOOs) and accidents to be considered. Typically the CMF analysis will be limited to the plant protection system, all other I&C systems will be considered as potentially providing diverse mitigation functions, and all AOOs and accidents that form the plant design basis accident set will be considered.

A complete identification of the scope will require identifying any exclusions from the analysis. Exclusions might involve:

- Function, systems, and components not to be considered in the CMF analysis (e.g., exclusion of functions provided only for economic protection),
- Systems and components excluded from consideration as potentially providing diverse mitigation functions (e.g., exclusion of systems which will not be built to the quality level appropriate for diverse mitigation functions), and
- Failures that are defined out-of-scope for the analysis (e.g., failure modes that were determined not credible by previous analyses or licensing commitments).

It may not be necessary to describe the bases for these exclusions in a written plan, but ultimately they must be justified in the final D-in-D&D analysis report.

2.1.3 Organization and Responsibilities

Organization requires a description of the D-in-D&D team. Responsibilities requires a definition of the responsibilities and authority of the software safety organization.

The D-in-D&D team should be identified and their relationship to each other should be described. The team must include I&C analysis skills, detailed knowledge of the I&C system design, and detailed knowledge of the plant response to design basis events. Occasionally, one person may have the skill and knowledge to fill two or all three of these roles. It is more likely, however, that the team will be

composed of at least three people: *an I&C analyst*, one or more *I&C designers*, and one or more *design basis event analysts.* These team members respectively represent each of the key knowledge and skills outlined above. In addition to the analysis team, one or more *reviewers* independent of the team must be available. Figure 2 illustrates the typical relationships between D-in-D&D participants and the input and output information.

(a) Role of I&C analyst

The I&C analyst is the key member of this team. The I&C analyst should be an experienced I&C engineer with extensive background in I&C systems, I&C software, failure analysis and historical I&C component and software failures. Typically, the I&C analyst should lead the analysis with the support of one or more members of the I&C design and accident analysis organizations.

(b) Role of I&C designers

The role of the supporting I&C design team members is to assist the analyst in understanding the characteristics of the I&C systems, and components (including both hardware and software). The I&C analyst may have a single point of contact on the design team, but the overall knowledge of the design (including hardware and software) should be available to support the analysis as needed. These people will typically assist in:

- choosing blocks,
- determining diversity,
- identifying the specific failures to be considered,
- postulating common-mode failures, and
- confirming diversity among echelons of defense.

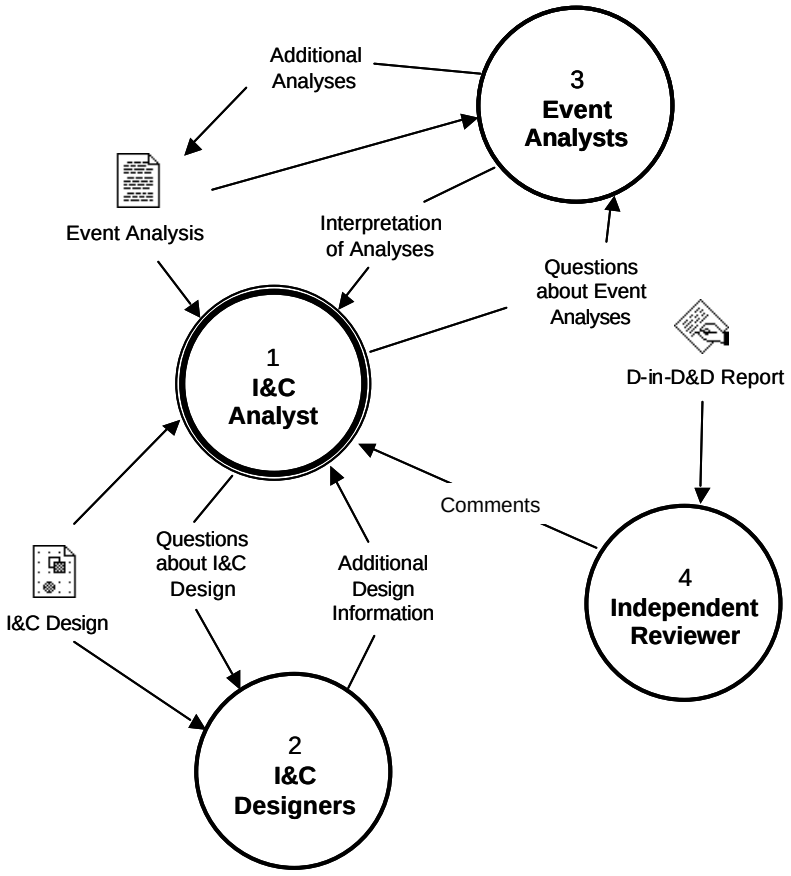

Fig. 2 D-in-D&D information flow

(c) Role of event analysts

The event analyst team member will be involved in confirming that the diverse features maintain plant and offsite consequences within the acceptance criteria of the four point position [7]. Often, the I&C analyst may be able to make this determination based upon examination of existing design basis event analysis documents. However, the assistance of an event analyst may often be needed to interpret the analytical results. The event analyst may also need to run additional calculations modeling the plants response to design basis events assuming mitigation is provided by the diverse functions credited in the analysis.

(d) Role of the independent reviewer

The provisions for independent verification of the analysis should be identified. Typically, the project's quality assurance (QA) procedures covering design verification should be adequate to control independent verification of the D-in-D&D analysis. The independent verifier should have at least the same level of skill and experience as the I&C analyst assigned to conduct the analysis.

2.1.4 Schedule

Scheduling requires that the time order of events necessary to achieve the purpose of the planning document is given as either absolute dates or relative to other project events. The schedule should discuss both the timing of D-in-D&D analysis relative to other design events and the timing of events within the analysis itself. D-in-D&D analyses may be performed at any point after sufficient information is available about the I&C system design and the plant response to design basis events.

Typically, analysis may begin after initial design basis event analyses are complete and the I&C system conceptual design and architecture are mature: ideally D-in-D&D analysis should be conducted as soon as an initial protection system block diagram is available. At this stage, the results of the analysis may be used to influence the design so as to reduce vulnerabilities and to minimize the need for a separate diverse protection system. Figure 3 shows recommended timing of the D-in-D&D analysis.

Correction of CMF vulnerabilities identified by a D-in-D&D analysis may require changes to the system concept, architecture, or software development environment. Such changes may be made for lower cost early in the design process.

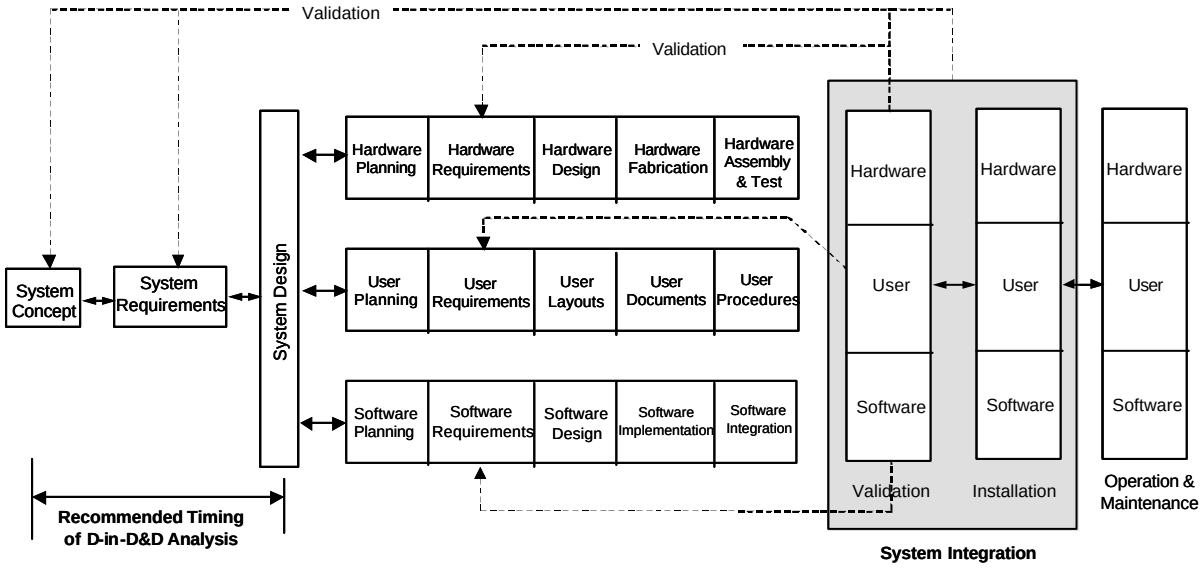

Fig. 3 Recommended timing of the D-in-D&D analysis

2.1.5 Maintenance

Planning should consider the need to maintain the analysis current as the plant design evolves during the design phase and plant operation. A strategy for evaluating the impact of design changes on the analysis conclusions should be developed. One possible strategy would be to update the analysis whenever the design changes in a way that affects the block analysis or plant response analysis.

Another strategy would be to evaluate the effects of changes on the analytical conclusions and to modify the analysis itself only when there is a change that affects the conclusions. In the later case, provisions for documenting the impact analysis should be made and the impact analyses must consider the cumulative impact of all changes made since the last revision of the D-in-D&D analysis. Whatever strategy is adopted it must meet the fundamental project QA requirements for design control and document control applicable to analyses.

2.2 Technical Processes

2.2.1 Analysis Methods

The methods used to carry out the analysis should be considered during planning. The typical method is for the I&C system analyst to work with the design team to develop an I&C system block diagram, as suggested in NUREG/CR-6303 [2] (see Fig. 4 for the overall structure of Guidelines). Common mode failures of the blocks are assumed and plant response is evaluated for each design basis event, assuming the postulated common mode failure.

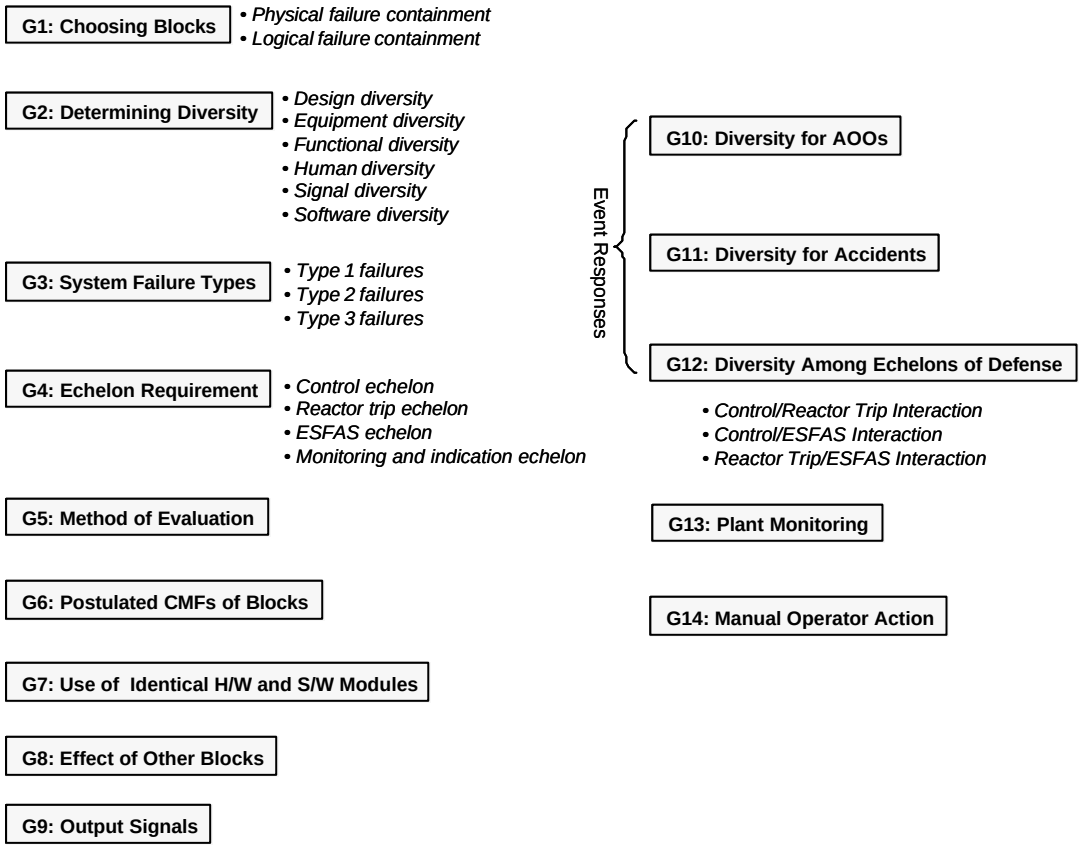

Fig. 4 The overall structure of guidelines as suggested in NUREG/CR-6303 [2]

Once blocks are defined, the common mode failure of each set of blocks is postulated and the consequences of these events on the protection system functionality identified. NUREG/CR-6303, Guideline 3 discusses the types of failures that should be considered and Guidelines 5, 6 and 7 describe considerations in postulating the common mode failures. Guidelines 8 and 9 describe

considerations in determining the effect of the postulated failure on the system. The result of this analysis is an identification of the diverse functions available to respond to plant conditions given each credible common mode failure.

For each combination of common mode failure and design basis accident, the diverse mitigation functions are identified, the plant response is determined, and the results are compared against the acceptance criteria given in Guidelines 10, 11, and 12 of NUREG/CR-6303.

2.2.2 Tools

The tools to be used for performing and documenting the analysis should be identified. Tools needed for conducting D-in-D&D analyses include tools for constructing block diagrams, tools for recording failure effects on individual plant events, and tools for summarizing CMF vulnerabilities.

Common drawing programs are typically sufficient for constructing block diagrams. CASE (Computer Aided Software Engineering) tools for developing deployment diagrams or class diagrams may also be useful for block diagramming tools and may automate the collection of some block diagrams.

The effects of assumed CMFs may be documented in simple tables that show the assumed block failures and remaining diverse functions credited as providing event mitigation.

2.2.3 Analysis Prerequisites

Planning should recognize the prerequisite conditions for starting an analysis. Generally, the following conditions should be met before the analysis begins.

- The I&C system conceptual design should be sufficiently mature so that the information needed for the block analysis is available, and sufficiently stable so that extensive changes to the block diagrams will not be needed to maintain consistency with the actual design.
- The accident analyses that will provide the basis for the plant safety analysis report should be substantially complete, stable, and should identify primary and secondary mitigation functions. Ideally, the secondary mitigation functions analyzed should cover the diverse mitigation functions assumed in the D-in-D&D analysis. Since these will not be known until the analysis is complete, the need to conduct additional analyses of plant responses assuming the specific mitigation functions identified in the D-in-D&D analysis should be anticipated.

2.2.4 Vulnerability Resolution

Planning should consider the method for resolving identified vulnerabilities. Often vulnerabilities will be addressed by changes to I&C system design. In some circumstances, however, it may be possible to accept identified vulnerabilities based upon, for example, the existence of diverse features outside of the analysis scope (e.g., mechanical systems features that provide defense-in-depth), or additional analysis to show that assumed failure modes are not credible. Such alternatives should be used very sparingly and carefully. The authority for accepting identified vulnerabilities should be well understood.

2.2.5 Reporting

The general outline of the report should be prepared during the analysis planning.

3. Analysis Procedure of D-in-D&D

This section describes the typical sequence of activities by the vendor for developing a D-in-D&D analysis. Figure 5 shows a brief D-in-D&D analysis procedure which is based on NUREG/CR-6303 [2]. Other analysis sequences are acceptable. In practice, the analyses may be iterative in nature with the analysis being refined as information is gained and as issues are identified.

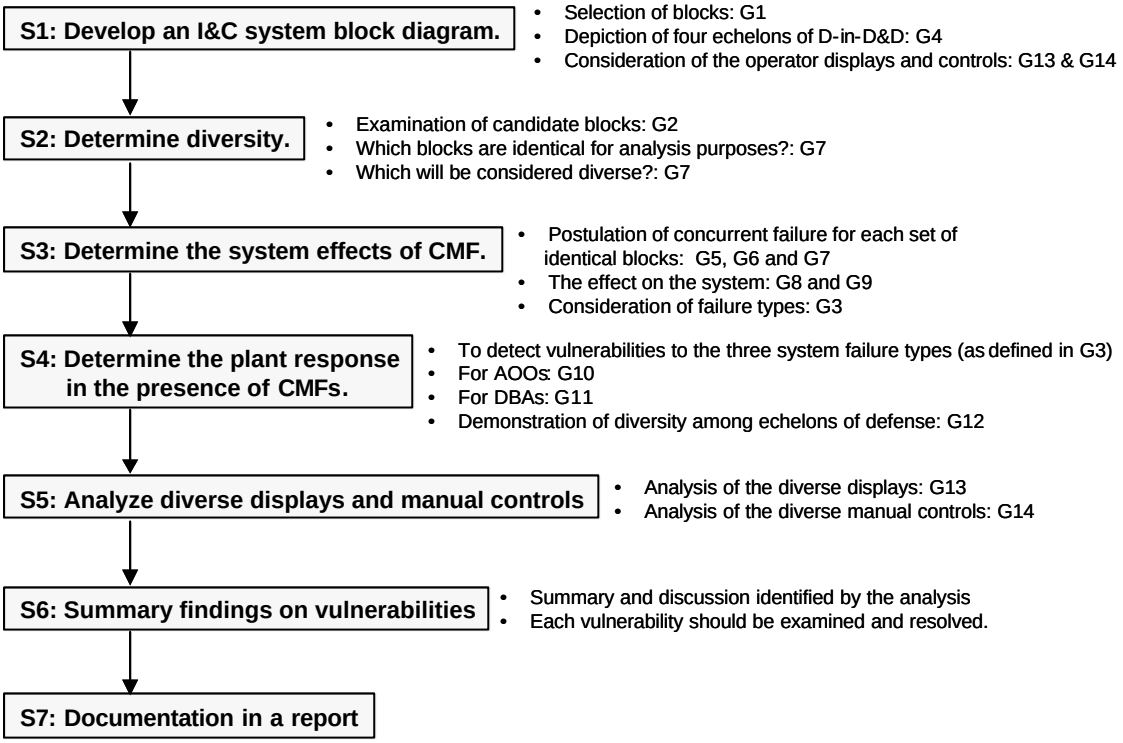

Fig. 5 A brief D-in-D&D analysis procedure

3.1.1 Develop an I&C system block diagram

Typically a D-in-D&D analysis begins with the development of an overall I&C system block diagram that shows the protection systems and the other systems that may be credited as diverse mitigation systems. The block diagram should depict the four echelons (i.e., RTS, ESFAS, control system, and monitoring and indicator system) of defense in depth as described in Guideline 4 of NUREG/CR-6303. The block diagrams should include the operator displays and controls credited to meet the criteria in Guidelines 13 and 14 of NUREG/CR-6303.

Blocks within a system should be selected consistent with Guideline 1 of NUREG/CR-6303 such that it may be credibly assumed that failures internal to each block will not propagate (either physically or via common design errors) to other blocks. Blocks may be selected as the smallest portion of the system that meet this criterion, but the selection of larger blocks is acceptable. For example, some analyses have made the simplifying assumption that the entire protection system fails and have demonstrated that plant consequences are acceptably mitigated by diverse systems. More often, however, a more detailed block diagram of the I&C system is needed to support the analysis.

The block diagrams should show all communication connections between blocks. The communication connections may be depicted very simply, but the analyst must understand what kinds of information can propagate along each connection.

3.1.2 Determine diversity

Each system, subsystem, or block should be assessed to determine if it can be credited as diverse from other elements in the block diagram. Guideline 2 of NUREG/CR-6303 should be followed in determining diversity and a summary should be prepared describing which groups of blocks are considered vulnerable to common mode failure, groups of elements are not subject to common mode failure, and the reasons behind these judgments. One way of performing this analysis is to describe each block and discuss the reasons why there is or is not a potential for common mode failure affecting both the selected block and other blocks in the diagram. This analysis may sometimes be

done at a higher level than a block.

3.1.3 Determine the system effects of common mode failure

For each set of identical blocks in the protection system, concurrent failure should be postulated in accordance with Guidelines 5, 6, and 7 of NUREG/CR-6303. The effect on the protection system should be determined using the criteria of Guidelines 8 and 9. This analysis should consider each type of failure described by Guideline 3.

Once the effect of common mode failure on system elements is understood, the effect on the protection system response to design basis events is examined. Each event analyzed in the plant safety analysis is examined and each set of common mode failures that can affect the assumed response to the event is considered. For every event/common mode failure pair, the remaining operable functions are examined to determine if at least one diverse protection mechanism is available.

3.1.4 Determine the plant response in the presence of common mode failures

The diverse protection mechanisms identified by the analysis of system effects must be shown to limit consequences within the criteria provided in Guidelines 10, 11, and 12 of NUREG/CR-6303. Furthermore, diversity among echelons of defense must be demonstrated in accordance with Guideline 12.

For *anticipated operational occurrences* as described in Guideline 10 (in combination with primary protection system failure), the goal of defense-in-depth analysis using best-estimate (realistic assumptions) methodology is to show that no more than a small fraction (10%) of the 10 CFR 100 dose limit is exceeded, and that the integrity of the primary coolant pressure boundary is not violated.

For *design basis accidents* as described in Guideline 11 (in combination with primary protection system failure), the goal of defense-in-depth analysis using best-estimate methodology is to show that any credible failure does not result in exceeding the 10 CFR 100 dose limits, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment.

3.1.5 Analyze diverse displays and manual controls

The diverse displays and manual controls provided as a backup to the automatic systems are analyzed for conformance with Guidelines 13 and 14 of NUREG/CR-6303. This should be possible by simple examination of the block diagram.

3.1.6 Summary findings on vulnerabilities

The vulnerabilities identified by the analysis should be summarized and discussed. Each vulnerability should be examined and dispositioned. Disposition may involve making system modifications to remove the vulnerability or developing a technical justification for accepting the vulnerability.

3.1.7 Documentation in a report

The D-in-D&D analysis should be documented in a report. Figure 6 describes a recommended report structure. Ideally, much of the required information should be developed during the analysis and preparation of the final report should only involve assembling the information into the final form.

4. Evaluation of a D-in-D&D Analysis

The purpose of an evaluator's review of a D-in-D&D analysis is to confirm that the D-in-D&D requirements for the I&C systems incorporating digital computer-based RTS or ESFAS are followed. Such a review has three objectives:

- to verify that adequate diversity has been provided in a design,
- to verify that adequate defense-in-depth has been provided in a design, and
- to verify that the displays and manual controls for critical safety functions initiated by

operator action are diverse from computer systems used in the automatic portion of the reactor protection system and ESFAS.

Fig. 6 An example of the table of contents for a D-in-D&D analysis document

The evaluation should include a review of the applicant's accident analysis section of the safety analysis report to determine the adequacy of diversity within the protection system to protect against common mode failure for each analyzed event. If a postulated common mode failure could disable a safety function, then a diverse means of accomplishing the function should be provided.

The regulatory review of the D-in-D&D analysis should be conducted soon after the analysis is completed. Resolution of any analysis deficiencies found could involve fundamental changes to I&C system architecture or design approaches. Therefore, it is important to have agreement early in the design process so that the cost of any necessary changes may be minimized.

4.1 Reviewer Qualifications

The evaluation of D-in-D&D analyses should be performed by staff with I&C analysis skills, general knowledge of the I&C system design, and general knowledge of the overall plant design including the design basis accident analysis. This reviewer will need the support of personnel with detailed knowledge in the area of design basis accident analyses.

The event analyst should be involved in reviewing the analysis of plant response assuming the functioning of diverse functions in place of primary protection functions.

4.2 Information to be Reviewed

The following specific information should be available for review:

(a) Safety Analysis Report (SAR)

The applicant's safety analysis report, including design addenda that further describe the reactor protection system, the reactor control system, the reactivity control system, and the engineered safety features (ESF). SAR Chapters 7, 15 and 18 are particularly pertinent.

(b) Defense-in-depth and diversity assessment

The required main parts for review include system representation as blocks, statement of assumptions,

secondary trip sequences, alternative mitigations, detailed analysis, consolidated results, and conclusions.

4.3 Review Process

Figure 7 shows an overall D-in-D&D review process [10]. In digital-based RTS, at least two diverse systems should be provided to mitigate any potential initiating event. Additionally, diverse displays and controls should be provided.

The review of D-in-D&D analyses should typically consist of determining that sufficient information is supplied in the assessment, that the applicant states assumptions, that the detailed analysis follows the applicant's interpretation of the guidelines, and that the conclusions are supported by all of the foregoing.

The review may consider some or all of the review topics described in Sec.4.4 below, depending upon what the reviewer feels is necessary to achieve the desired level of confidence in the analysis. Typically, a review should consider at least the reasonableness of assumptions, system representation of blocks, postulation of block failures, identification of alternative trip or initiation sequences, identification of alternative mitigation capability, and the justification for any cases in which vulnerabilities are not corrected.

For any limited scope review, if problems are found, the depth and breadth of the review should be expanded in order that the consequences of the identified problems may be characterized.

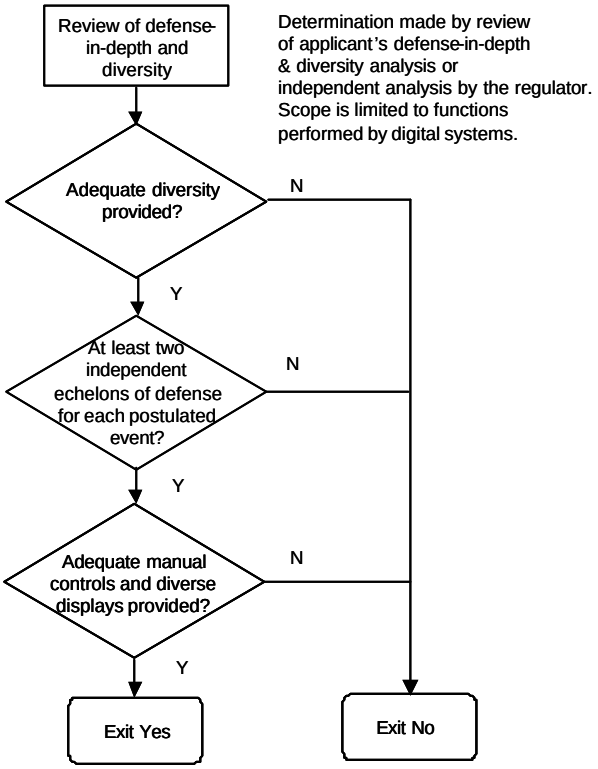

Fig. 7 Defense-in-depth and diversity review process [10]

4.4 Evaluation Topics on D-in-D&D

Topics that would be considered in a complete review include the following.

(a) Completeness of information

The analysis is examined to confirm that it is complete as outlined in Sec. 4.2 above.

(b) Statement of assumptions

The assumptions should be evaluated to assure that they match the applicant's design basis, and that the general guidelines of NUREG/CR-6303 [2] are applied to the design being assessed. As a part of the overall review, the reviewer should be alert for assumptions that have not been recognized or documented by the analysts. The applicant/licensee should also have in place a process to confirm the validity of assumptions as the design uncertainties covered by the assumptions are resolved.

(c) Method of analysis

The reviewer should confirm that the method of analysis follows the procedures described in NUREG/CR-6303. In some instances, modifications will be necessary to adapt the analysis method to the design under review. In these cases, the reviewer should confirm that the modifications to the method are reasonable and technically defended.

(d) System representation as blocks

The system being assessed should be represented as a block diagram; the inner workings of the blocks are not necessarily shown. This block diagram provides the fundamental system model to which postulated common mode failures are applied. The choice of blocks should conform with Guideline 1 of NUREG/CR-6303.

(e) Postulation of block failures

The failures postulated for the chosen blocks should be examined for credibility and adherence to guidelines. Each of the failure types identified in Guideline 3 of NUREG/CR-6303 should have been postulated and the failures should be applied to the system model as described in Guidelines 5 and 6. In conducting this review, the reviewer should be alert for possible failures that are omitted.

(f) Identical blocks

The bases for deciding which blocks are considered identical, and for judging diversity of blocks, should be reviewed for credibility and adherence to Guidelines 1, 2, and 7 of NUREG/CR-6303.

(g) Effect of other blocks

The analyses should be reviewed to determine if the effects of postulated failures are carried through other non-failed blocks as described in Guideline 8 of NUREG/CR-6303.

(h) Output signals

The one-way assumption on output signals should be verified for the design as discussed in Guideline 9 of NUREG/CR-6303. Both electrical isolation and communication independence are required. Communication independence means that data transmission failure, corrupted data, or failure of coordination signals (handshake signals) cannot cause a good block to fail because one of its outputs is connected to a bad block.

(i) Identification of alternate trip or initiation sequences

The review should confirm that appropriate thermal-hydraulic analyses have been performed for the sequence of events that would occur if the primary trip channel were to fail to trip the reactor or actuate engineered safety features. The analytical tools and models used should be consistent with those used for other plant safety analyses, however, the analyses to support the D-in-D&D analysis may use best-estimate (realistic assumptions) methods, rather than conservative methods and assumptions. In default of specific thermal-hydraulic analyses, reasoning, supported by thermal-hydraulic analyses in SAR Chapter 15, may be used to identify sequences of events that would occur if the primary trip channel were to fail to trip the reactor or actuate engineered safety features. In some instances, because possible common-mode failures may simultaneously disable both a primary and a secondary trip channel, it may be necessary to identify relevant tertiary trip sequences. The review

should confirm that the best estimate methods and assumptions used are acceptable.

(j) Identification of alternative mitigation capability

The review should confirm that the analysis has considered the alternative mitigation functions for each design basis event.

Where a common-mode failure is compensated by an automatic function that is different from the primary function that has been assumed to fail, a basis should be provided to explain why the different function constitutes adequate mitigation for the conditions of the event.

Where operator action is cited as the diverse means for response to an event, the applicant/licensee should demonstrate that adequate information (indication) and sufficient time are available for operator action.

(k) Adequacy of manual displays and controls

The availability of manual controls and displays in conformance with the four point position [7] should be demonstrated by the licensee/applicant. This may be done as part of the D-in-D&D analysis or it may be contained in a separate analysis. Manual displays and controls should be sufficient to both monitor the plant states and to actuate systems required by the control room operators to place the nuclear plant in a hot-shutdown condition. In addition, the displays and controls should monitor and control the following critical safety functions: i.e., reactivity level, core heat removal, reactor coolant inventory, containment isolation, and containment integrity. The manual capability should consist of hardwired, system-level controls and displays in order to provide plant operators with information and control capabilities that are not subject to common-mode failures caused by software errors in the plant's automatic digital I&C safety system [7].

The point at which the manual controls are connected to safety equipment should be downstream of the plant's digital I&C safety system outputs, but should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment. To achieve system-level actuation at the lowest possible level in the safety system architecture, the controls may be hardwired either to analog components or to simple (e.g., the component function can be completely demonstrated by test), dedicated, and diverse, software-based digital equipment that performs the coordinated actuation logic.

Human factors engineering principles and criteria should be applied to the selection and design of the displays and controls. The human performance requirements should be described and related to the plant safety criteria. Recognized human factors standards and design techniques should be employed to support the described human performance requirements.

(l) Determination of vulnerabilities

The detailed analyses should be examined to determine that guidelines are followed in recording failures-to-trip or -actuate under postulated common-mode failures. A vulnerability exists when the analysis fails to show the acceptance criteria given in Guidelines 10, 11, and 12 of NUREG/CR-6303 are met. Consolidated results should be examined to determine that vulnerabilities discovered in detailed analyses are reflected in consolidated results.

(m) Conclusions

Conclusions should be examined to determine if the requirements of the Commission's regulations are met without or with modification of the design.

(n) Justification for not correcting specific vulnerabilities

If any identified vulnerabilities are not addressed by provision of alternate trip, initiation, or mitigation capability, justification should be provided. Justification may be based upon the availability of systems outside of the scope of the analysis that act to prevent or mitigate the event of concern. For example, I&C system vulnerability to common-mode failure affecting the response to large-break loss-of-

coolant accidents and main steam line breaks has been accepted in the past. This acceptance was based upon the provision of primary and secondary coolant system leak detection, and pre-defined operating procedures that together enable operators to detect small leaks and take corrective actions before a large break occurs.

5. Conclusions

This paper has provided comprehensive D-in-D&D guidelines that can help the vendor/evaluator to prepare/review D-in-D&D planning and/or analysis documents. Most of the guidelines described in this paper were based on NUREG-0800, BTP-19 and NUREG/CR-6303.

How to plan and analyze D-in-D&D in digital I&C systems is important to minimize the possibility of CMFs and thus increase the plant reliability. If the D-in-D&D plan was wrong or insufficient, the subsequent stage such as D-in-D&D analysis may be misdirected.

Software cannot be proven to be error-free, and therefore is considered susceptible to common-mode failures because identical copies of the software are present in redundant channels of safety-related systems. To defend against potential common-mode failures, high quality, defense-in-depth, and diversity are considered to be key elements in digital I&C system design. Implementation of software diversity should use independent systems with functional diversity. The use of system diversity, diverse software features and diverse design approaches should be considered.

References

[1] Digital Instrumentation and Control Systems in Nuclear Power Plants – Safety and Reliability Issues, Section 5: Common-Mode Software Failure Potential, Final Report, Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, Board on Energy and Environmental Systems, Commission on Engineering and Technical Systems, National Research Council, National Academy Press, Washington, D.C., 1997.

[2] NUREG/CR-6303. "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," U.S. Nuclear Regulatory Commission, December 1994.

[3] NUREG-0493. "A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System." U.S. Nuclear Regulatory Commission, March 1979.

[4] SECY-91-292, "Digital Computer Systems for Advanced Light Water Reactors," U.S. Nuclear Regulatory Commission, Sept. 16, 1991.

[5] SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," U.S. Nuclear Regulatory Commission, April 2, 1993.

[6] Staff Requirements Memorandum. "SECY-93-087, Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," U.S. Nuclear Regulatory Commission, July 21, 1993.

[7] NUREG-0800, BTP HICB-19. "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," Rev. 4, U.S. Nuclear Regulatory Commission, June 1997.

[8] Draft Amendment 1 to IEC 60880. "Software for Computers Important to Safety For Nuclear Power Plants – First Supplement to IEC Publication 880," Ed. 1, International Electrotechnical Commission, April 1999.

[9] NUREG-0800, BTP HICB-14. "Guidance on Software Review for Digital Computer-Based Instrumentation and Control Systems," Rev. 4, U.S. Nuclear Regulatory Commission, June 1997.

[10] NUREG-0800, Appendix 7.0-A. "Review Process for Digital Instrumentation and Control Systems," June 1997.

[11] KINS/AR-541. "Development of the Technology for D-I-D and Diversity Regulations of Computer-based Reactor Protection Systems," Korea Institute of Nuclear Safety, April 1998.

[12] KAERI/TR-1628/2000. "Guidelines on the Defense-in-Depth and Diversity Planning and Analysis in Digital Instrumentation and Control Systems," Korea Atomic Energy Research Institute, August 2000.