A novel approach for quantitative importance analysis of DI&C systems in NPP

Sung-Min Shin[a], Sang Hun Lee[b], and Seung Ki Shin[a]
[a] Korea Atomic Energy Research Institute, 111 Daedeok-daero 989beon-gil Yuseong-gu, Daejeon, Republic of Korea, smshin@kaeri.re.kr, skshin@kaeri.re.krt
[b] Korea Institute of Nuclear Safety, 62, Gwahak-ro, Yuseong-gu, Daejeon, Republic of Korea, lees@kins.re.kr

Abstract: The safety-related Instrumentation and Control (I&C) system of nuclear power plants (NPPs) has quite complex interactions between its components including human factors in accordance with the redundancy/diversity design concept applied to ensure their functions, and the complexity is further increased with the recent introduction of digital characteristics. Moreover, it is very difficult to secure quantified failure information of digital components required in analyzing the digital I&C system according to the PSA (Probabilistic Safety Assessment) which is the analysis framework of the existing NPP I&C system. Therefore, this study proposes a new approach to resolve these issues. The approach proposed in this study basically includes all components including humans for sensing signal generation, safety signal generation, and safety signal execution from the system modeling phase to integrate all complex interactions between system components refer to the Systems-Theoretic Accident Model and Processes (STAMP), and it assigns weights to related components in consideration of characteristics in system design and strategies in system operation, instead of failure information. Then the approach calculates the effect on a path for a safety signal generation/execution and system when a specific component is unavailable. The proposed approach was explained through a simple example. It is expected that the proposed approach can be used for deriving useful insights from the initial stage of system development to the state of system improvement as a kind of auxiliary analysis technique.

1. INTRODUCTION

The safety-related instrumentation and control (I&C) systems in nuclear power plants (NPPs) are implemented with redundancy/diversity design concepts to ensure their functional availability[1-3]. This leads to complex interactions between the components in an I&C system, which may vary depending on specific accident scenarios and subsequent mitigation strategies. Moreover, many existing analog component-based I&C systems are being digitalized due to the obsolescence of the analog components, which introduces characteristics that were not previously present such as software and networks, further increasing the complexity of the interactions between system components [4-7].
The safety of the I&C systems in NPPs is verified through probabilistic safety assessment (PSA) [8-10], and one of the aforementioned redundancy/diversity design concepts is to provide an automatic or manual initiation of the safety functions. Each failure probability of each initiation is eventually integrated into a fault tree (FT) for PSA, but the analysis process for each is quite different; for automatic functions, a failure logic using the module level of basic events is directly modeled into the FT, on the other hand, for manual functions the human error probability (HEP) is derived through human reliability analysis (HRA) that considers various performance shaping factors (PSFs) such as stress level and workload[11-12]. Then the HEP is linked to the gate of FT logic alternative to the automatic function. From the authors' point of view, at least the soundness of the I&C system additionally needs to be considered in the HRA process because it can affect the acquisition of information for decision-making and the transmission of generated manual safety signals.
For a quantitative fault tree analysis, specific values of failure information, such as failure rate(or probability), common cause failure (CCF) parameters, are required. Moreover, for the analysis of digital I&C (DI&C) system, additional failure information that was not required in the analysis of the analog

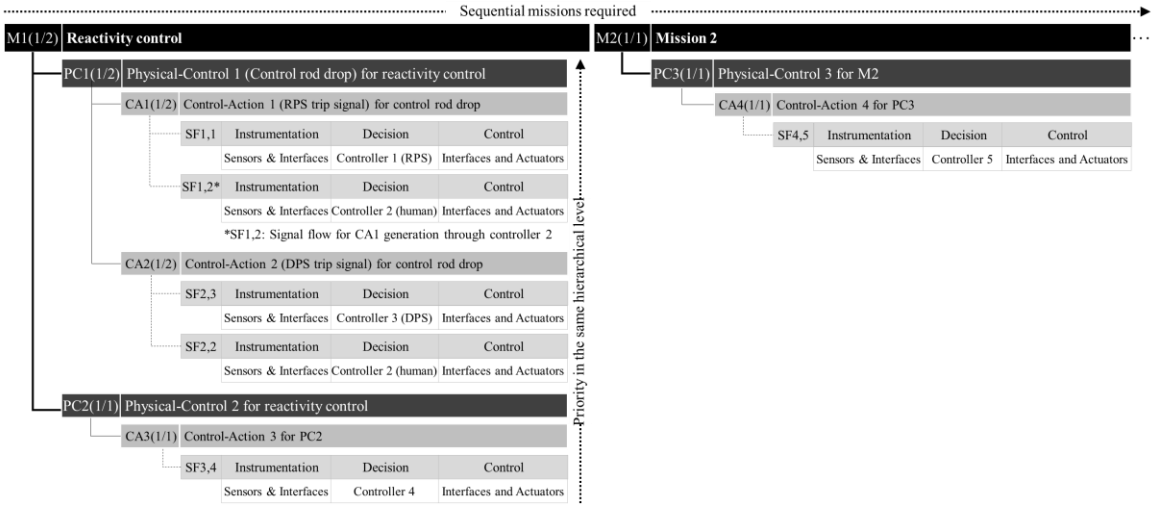
system, such as software reliability[13-14], network reliability[15]. However, definitions of the failure modes and underlying methodologies related to quantifying such failure information of DI&C system components have not been firmly established yet[16-17]. This study aims to suggest a new approach to resolve the above-mentioned issues: (1) a systematic analysis of the complex interactions between DI&C components, (2) an analysis process linking automatic/manual signal generation and execution, and (3) a quantification of the analysis results without failure information of the DI&C system.
There is an approach to viewing the analysis of I&C systems as problems in control, not failures, which is called STAMP (Systems Theoretic Accident Model and Processes) and it models the control structure of a given system based on control loops composed of a controller, controlled process, feedbacks (FBs), and control actions (CAs)[18-20]. STAMP-based analyses applied to various fields, such as aircraft [21], medical [22], railroad [23], maritime [24], and nuclear [25-26] industries, show that it can identify potential hazards that can occur in complex interactions between system components. The authors believe that this STAMP system can be useful for this study. The authors consider human operator, the subject of manual safety signal generation, as one controller. It will be possible to set a foundation for linking automatic/manual aspects and for analyzing the complex interactions of DI&C components. In the proposed methodology, weights are assigned to particular components in the control structure referring to the system design and operation strategy, instead of failure information, as the basis for the quantitative analysis results. This paper explains the concepts of the proposed methodology with a simple example.

2. METHOD

2.1. Basic Concepts of the Approach

The DI&C system, which performs safety-related functions, applies the concepts of redundancy and diversity to prevent the failure of intended functions due to a single component failure. In this paper, the redundancy/diversity design of the DI&C system is analyzed from two perspectives: the functional perspective which is the analysis of conceptual strategies for accident mitigation, and the signal flow perspective which is the analysis of signal transfer from measurement to control.

Figure 1. Example analysis of the functional redundancy/diversity of a DI&C system



First, functional redundancy/diversity of the DI&C system can be organized according to hierarchy, priority, and complementary relation between mitigation strategies, as shown in Figure 1. When the sequential roles required to the DI&C system according to the accident scenario is called the mission (M), the I&C system must perform physical control (PC) for a mission. For example, in the event of an abnormal situation, the most important mission (M1) to be taken is reactivity control. In general, reactivity control is performed by a control rod drop (PC1), and if there is an alternative means (PC2) for reactivity control, then PC1 and PC2 can be placed in the same hierarchical level (Each hierarchical level can be expressed via indentation). Then a PC can be initiated by a CA which is a kind of activation

signal, and a CA can be generated and transmitted by a specific SF. Thus, the functional redundancy/diversity of the DI&C system can be organized as follows: Mission (M)–Physical Control (PC)–Control Action (CA)–Signal Flow (SF).
If multiple mitigations mean exist at the same hierarchical level, the complementary relations and priority between them need to be specified. In the case of M1 within the given example, the success criteria of PC1 and PC2 for M1 is 1/2, which means one of the two PCs is sufficient for the success of M1. If both PCs are required, it should be specified as 2/2. Meanwhile, at the same hierarchy level, priorities can be specified according to upper/lower placement. In Figure 1, PC1 has priority over PC2. Similarly, to the above, the functional redundancy/diversity of the DI&C system for the completion of a given mission can be organized according to hierarchy, priority, and complementary relations between functional elements.
Second, the concept of redundancy/diversity is also applied to SFs. Various instrumentation signals (the same as FB in STAMP) can be generated by a number of sensors and can be transmitted along different paths to various controllers for safety signal generation (the same as CA in STAMP). A human operator can compensate for the failure of automatic CA generation, or the generated CA can be transmitted through different paths to a number of valves or pumps that are complementary to each other. To see these characteristics, it is necessary to model all SFs of the system into a control structure and examine it SF by SF. In the example in Figure 1, the RPS trip signal (CA1) can be generated automatically by the RPS trip logic or manually by a human operator. The RPS trip logic and human operator can collect different, identical, or additional FBs through different paths, and also, the generated CA through the RPS trip logic or human operator can be transmitted to the actuators in different, identical, or partially overlapped paths. In other words, the components utilized for the two SFs might be different, identical, or overlapped. Therefore, if a component is unavailable, the soundness of several SFs can be affected in different ways. For reference, A specific SF can be defined according to the combination of a CA and a controller. Thus, in SFi,j, i is the index of the CA and j is the index of the controller. For reference, in Figure 1, SF1,2 and SF2,2 utilize the same controller C2 (human).
The basic concept of the approach presented in this paper is as follows. For each SF, in the event of a problem with a particular component, the degree to which the soundness of the associated SFs is degraded is assessed, and the larger the degradation is, the more important the component is. Then by summing the importance of each component calculated for each SF over the Mission (M)–Physical Control (PC)–Control Action (CA), the final importance of each component on that mission is calculated.

2.2. Details of the Methodology

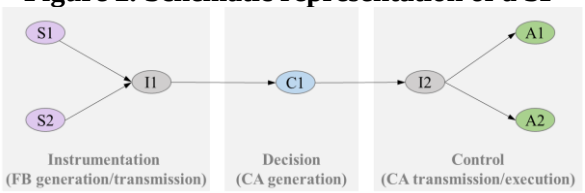
The I&C system measures and controls control targets. Looking deeper, there are generally three steps: (1) instrumentation, where the FB or FBs referred to for CA determination are generated by a sensor or sensors and transmitted to the controller through the associated interface(s); (2) decision, where a controller determines the CA generation based on the FB(s) received; and (3) control, where the generated CA is transmitted to the actuator(s) performing the related physical action through the associated interface(s). Basically, all functions of the I&C system are considered to go through these three steps, which make up the aforementioned SF. It should be noted that each step is linked in series, and a complete failure of a step is considered to cause the failure of the corresponding SF. Each of the three steps involves the operation of one or more of the following four types of components:

- Sensor (S): a component that generates FB
- Interface (I): a component that transmits FB from a sensor to a controller or a CA from a controller to an actuator
- Controller (C): a component that determines whether a CA is generated or not, and which CA should be generated
- Actuator (A): a component that receives a CA and performs corresponding physical actions.

As a simple example, a schematic of each SF using above components can be draw as given Figure 2. Each component can be represented by a node with a component type-specific ID (S for sensor, I for

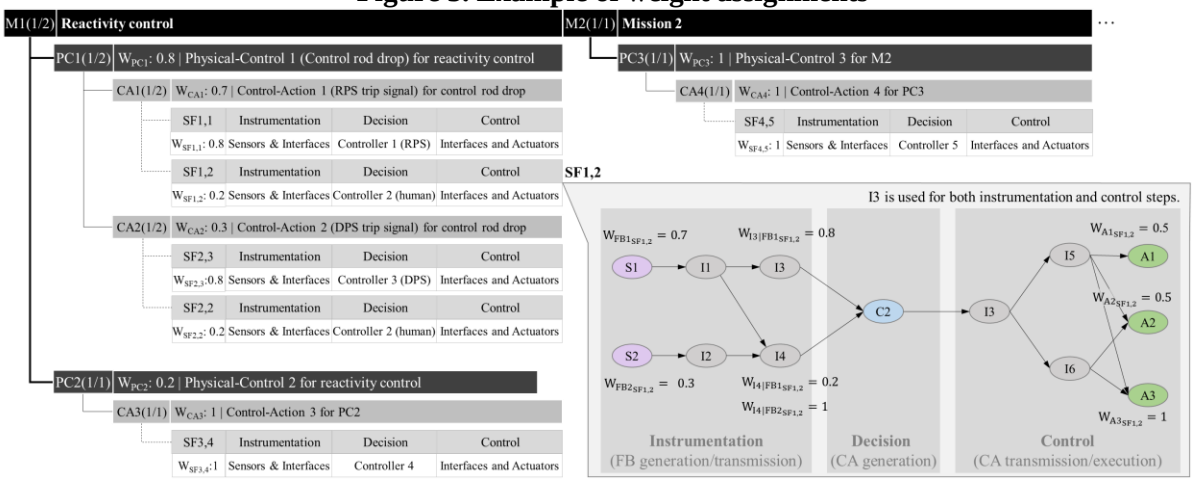
interface, C for controller, A for actuator), and the signal flow between components can be represented by an arrow. If necessary, arrows may indicate the name of the FB or CA. In this manner, by accumulating all SFs, it is possible to model the entire system similar to the control structure covered by STAMP.

Figure 2. Schematic representation of a SF



The proposed method assigns weights, instead of failure information, as the basis for deriving quantitative analysis results as follows. First, weights are assigned to the elements in the same functional hierarchy level, from PC to SF, according to the relationship and the relative importance between the elements in achieving the needs of the higher hierarchy. Second, in a single SF, weights are assigned to FBs and some components from the instrumentation and control perspective. Figure 3 indicates both types of assigned weights.

Figure 3. Example of weight assignments



At the same hierarchical level, the weight of an element is between 0 and 1, and the sum of the weights of the elements that cause the failure of the higher hierarchy needs (minimal cut set: MCS) should be equal to 1. For example, the MCS for M1 is PC1× PC2 since one of them can complete M1, so the sum of the weights of PC1 and PC2 is 1: W_{PC1}= 0.8, W_{PC2} = 0.2. If both PC1 and PC2 are needed for M1 completion, that is the MCS for M1 is PC1 + PC 2, the weights of each PC will be 1. Based on this principle, the weights of each CA and SF are assigned, for example W_{CA1}= 0.7 and W_{CA2}= 0.3, $W_{SF1,1}$= 0.8, $W_{SF1,2}$= 0.2, and so on, all with sums equal to 1. The weight assignments for PC, CA, and SF described above can be defined as below.

$$\sum_{y \in MCS_{Mx}} W_{PCy} = 1, \text{where } MCS_{Mx} \text{ is the MCS of the PCs causing Mx failure} \quad (1)$$

$$\sum_{i \in MCS_{PCy}} W_{CAi} = 1, \text{where } MCS_{PCy} \text{ is the MCS of the CAs causing PCy failure} \quad (2)$$

$$\sum_{j \in MCS_{CAi}} W_{SF\,i,j} = 1, \text{where } MCS_{CAi} \text{ is the MCS of the SFs causing CAi failure} \quad (3)$$

The assigned PC, CA, and SF weights will be utilized when updating the importance of the components derived within each SF to the overall importance from a mission's point of view. The underlying philosophy is as follows: if a component is used in a specific SF, and the SF is used to generate a CA

that is treated as important, and the CA is also used to perform an important PC, then the component is very important from a mission perspective.
Next, weights are assigned to some components within a single SF. From the perspective of instrumentation, weights are assigned between FBs generated by sensors and between the front-end interfaces where a particular FB is transmitted to the controller. The principle is that if there is a SF, which transfers a FB significant on decision-making through an effectively recognizable path to the controller, the components in that SF should be considered as important ones. An example weight assignment for SF1,2 is given in Figure 3. When a human operator (C2) generates CA1, there are two reference FBs generated by the sensors, S1 and S2, and it is assumed that the S2 signal (FB2) is used as auxiliary information of the S1 signal (FB1); for this reason, a weight of 0.7 is assigned to FB1, relatively higher compared to the weight assigned to FB2 (0.3). Regarding FB transmission, FB2 is transmitted to C2 only through the front-end interface I4, so the weight of I4 transmitting FB2 for SF1,2, $W_{I4|FB2_{SF1,2}}$, is equal to 1. Meanwhile, FB1 is transmitted to C2 through two front-end interfaces, I3 and I4, so the weights of these interfaces are assigned such that the sum of them is equal to 1. In the example, a higher weight is assigned to I3 assuming that the human operator pays more attention to the signals transmitted through this interface: $W_{I3|FB1_{SF1,2}} = 0.8$, $W_{I4|FB1_{SF1,2}} = 0.2$. The weight assignment for the FBs and front-end interfaces from the instrumentation perspective can be defined like below.

- $W_{FBk_{SF\,i,j}}$: Weight of a specific FB k in SF i, j (CA i generation through controller j)
  where $\sum_{k=1}^{\alpha} W_{FBk_{SF\,i,j}} = 1$ for a specific SF i, j ($0 \le W_{FBk_{SF\,i,j}} \le 1$, $W_{FBk_{SF\,i,j}} = 0$ if FB k is not used for SF i, j)
  where α = total number of FBs in a given system

- $W_{Ix|FBk_{SF\,i,j}}$: Weight of a specific front-end interface x transmitting FB k in SF i, j
  where $\sum_{x=1}^{\beta} W_{Ix|FBk_{SF\,i,j}} = 1$ for a specific SF i, j ($0 \le W_{Ix|FBk_{SF\,i,j}} \le 1$, $W_{Ix|FBk_{SF\,i,j}} = 0$ if component x is not the front-end interface transferring FB k for SF i,j)
  where β = total number of interfaces in a given system

Based on the weight assignments above, the importance (IM) of sensor n ($IM^{INS}_{Sn|SF\,i,j}$) or interface n ($IM^{INS}_{In|SF\,i,j}$) in SFi, j from the instrumentation perspective can be obtained. The IM of a sensor is straightforward: if there is a problem with a particular sensor, the controller cannot receive the FB generated by that sensor through any path, and so the weight assigned to the FB generated by that sensor itself becomes the importance of that sensor.

$$IM^{INS}_{Sn|SF\,i,j} = W_{FBk_{SF\,i,j}} \ (n = k) \qquad (4)$$

Generated FBs can be transmitted by complex interconnections of related interfaces before they are transmitted to the controller. Even if an interface fails, FB(s) may be still transmitted to a controller through all or some paths depending on the system's design characteristics. Therefore, the importance of a particular interface is calculated according to the following concepts: how large the negative effect is in comparison to the sum of the negative effects and the degree to which it can still function:

$$IM^{INS}_{In|SF\,i,j} = \sum_{k=1}^{\alpha}\left(W_{FBk_{SF\,i,j}} \frac{\sum_{g\in G_{In}|FBk_{SF\,i,j}} W_{g|FBk_{SF\,i,j}}}{\sum_{g\in G_{In}|FBk_{SF\,i,j}} W_{g|FBk_{SF\,i,j}} + \sum_{f\in F_{In}|FBk_{SF\,i,j}} W_{f|FBk_{SF\,i,j}}}\right) \qquad (5)$$

where $G_{In}|FBk_{SF\,i,j}$: Group of front-end interfaces transmitting FB k via interface n in SF i, j

where $F_{In}|FBk_{SF\,i,j}$: Group of front-end interfaces transmitting FB k not via interface n in SF i, j

Regarding SF1,2 given in Figure 3, the importance of the instrumentation-related components is calculated below as an example.

$$IM^{INS}_{S1|SF1,2} = W_{FB1_{SF1,2}} = 0.7$$

$$IM^{INS}_{S2|SF1,2} = W_{FB2_{SF1,2}} = 0.3$$

$$IM^{INS}_{I1|SF1,2} = \sum_{k=1}^{2}\left(W_{FBk_{SF1,2}} \frac{\sum_{g\in G_{I1}|FBk} W_{g|FBk_{SF1,2}}}{\sum_{g\in G_{I1}|FBk_{SF1,2}} W_{g|FBk_{SF1,2}} + \sum_{f\in F_{I1}|FBk_{SF1,2}} W_{f|FBk_{SF1,2}}}\right)$$

where $G_{I1}|FB1_{SF1,2} = \{I3, I4\}$, $F_{I1}|FB1_{SF1,2} = \{0\}$, $G_{I1}|FB2_{SF1,2} = \{0\}$, $F_{I1}|FB2_{SF1,2} = \{I4\}$

$$= W_{FB1_{SF1,2}} \frac{\sum_{g\in\{I3,I4\}} W_{g|FB1_{SF1,2}}}{\sum_{g\in\{I3,I4\}} W_{g|FB1_{SF1,2}} + \sum_{f\in\{0\}} W_{f|FB1_{SF1,2}}} + W_{FB2_{SF1,2}} \frac{\sum_{g\in\{0\}} W_{g|FB1_{SF1,2}}}{\sum_{g\in\{0\}} W_{g|FB1_{SF1,2}} + \sum_{f\in\{I4\}} W_{f|FB1_{SF1,2}}}$$

$$= 0.7\frac{(0.8+0.2)}{(0.8+0.2)+0} + 0.3\frac{0}{0+1} = 0.7$$

Similarly to the above,

$$IM^{INS}_{I2|SF1,2} = 0.3$$

$$IM^{INS}_{I3|SF1,2} = 0.56$$

$$IM^{INS}_{I4|SF1,2} = 0.44$$

Regarding the second step in the SF, decision, there is no specific weight assignment. Throughout the proposed methodology, it is presupposed that there is one controller per SF, and this single controller decides whether to generate a CA. Therefore, for any problem with controller j, the CA i cannot be generated, which means a complete failure of the decision step in SFi,j. In this regard, the importance of a controller ($IM^{DEC}_{Cn|SF\,i,j}$) related to SFi, j can simply be defined as below:

$$IM^{DEC}_{Cn|SF\,i,j} = 1\ (n = j) \qquad (6)$$

The ultimate purpose of the control step is the operation of the relevant actuators. To secure the control step, there may be specific system designs such as installing multiple actuators for redundancy or adopting a different type of actuator for diversity. However, the completion of the control step means the activation of the minimum relevant actuators to achieve the goal. In this regard, weights are assigned to the actuators as follows. First, all the MCSs of the actuators in SFi,j ($MCSz_{SF\,i,j}$: Possible numerous MCS of actuators,z,for SFi,j) that cause control step failure are derived, and then a weight is assigned to each actuator such that the sum of the weights of the actuators that make up each MCS is 1. In Figure 3, it is assumed that either A1 or A2, and A3 must be activated for the control rod drop; therefore, the MCS of SF1,2 can be defined as $MCS1_{SF\,1,2}$ = {A1, A2} and $MCS2_{SF\,1,2}$ = {A3}. Then depending on the number of actuators for each MCS, the weights will be assigned equally. MCS1 has two actuators, A1 and A2, so each actuator is assigned with a weight of 0.5, while the single actuator in MCS2, A3, is assigned with a weight of 1: $W_{A1_{SF1,2}} = W_{A2_{SF1,2}} = 0.5$, $W_{A3_{SF1,2}} = 1$

$$W_{Ay_{SF\,i,j}} = \frac{1}{m} \qquad (7)$$

where m is the number of actuators in the MCS including the actuator y in SFi,j

Based on the weight assignments to the actuators, the IM of an interface ($IM^{CTL}_{I_n|SF\,i,j}$) or an actuator ($IM^{CTL}_{A_n|SF\,i,j}$) in SFi, j from the control perspective can be calculated. Although it seems similar to the one of instrumentation step, it differs from that because the control step transfers a single CA to multiple actuators not transfers multiple FBs to a single controller.

Depending on the system design, there may be a number of MCSs of the actuators for each SF, and the control step may fail even by a single MCS. Therefore, after analyzing the impact of each MCS by an unavailable component, the maximum value of the impact is assumed as the importance of that

component. However, in this approach, the impacts on the MCSs other than the most impacted MCS are ignored, so the sum of the impacts on all MCSs may be presented as a reference indicator.

$$IM^{CTL}_{In|SF\,i,j} = \max\{IM_{In|SF\,i,j}(z) : z = 1..\gamma\} \quad (8)$$

where γ is the number of MCSs of the actuators in SFi,j

$$IM_{In|SF\,i,j}(z) = \frac{\sum_{g\in G_{In}|MCSz_{SF\,i,j}} W_{g_{SF\,i,j}}}{\sum_{g\in G_{In}|MCSz_{SF\,i,j}} W_{g_{SF\,i,j}} + \sum_{f\in F_{In}|MCSz_{SF\,i,j}} W_{f_{SF\,i,j}}} \quad (9)$$

where $G_{In}|MCSz_{SF\,i,j}$: Group of actuators receiving CA i via interface n in MCSz in SFi, j
where $F_{In}|MCSz_{SF\,i,j}$: Group of actuators receiving CA i not via interface n in MCSz in SFi, j

The IM of an actuator is straightforward, similar to that of a sensor. The weight assigned to an actuator corresponds to the importance of that actuator since the weight is assigned from the perspective of a successful PC.

$$IM^{CTL}_{An|SF\,i,j} = W_{Ay_{SF\,i,j}}\ (n = y) \quad (10)$$

Regarding SF1,2 given in Figure 3, the importance of the control-related components can be calculated as below.

$$MCS1_{SF\,1,2} = \{A1, A2\}, MCS2_{SF\,1,2} = \{A3\}$$

$$IM_{I3|SF\,1,2}(1) = \frac{\sum_{g\in G_{I3}|MCS1_{SF\,1,2}} W_{g_{SF\,i,j}}}{\sum_{g\in G_{I3}|MCS1_{SF\,1,2}} W_{g_{SF\,i,j}} + \sum_{f\in F_{I3}|MCS1_{SF\,1,2}} W_{f_{SF\,i,j}}}$$

where $G_{I3}|MCS1_{SF1,2} = \{A1, A2\}$, $F_{I3}|MCS1_{SF1,2} = \{0\}$

$$= \frac{\sum_{g\in\{A1,A2\}} W_{g_{SF\,i,j}}}{\sum_{g\in\{A1,A2\}} W_{g_{SF\,i,j}} + \sum_{f\in\{0\}} W_f} = \frac{(0.5+0.5)}{(0.5+0.5)+0} = 1$$

$$IM_{I3|SF\,1,2}(2) = \frac{\sum_{g\in G_{I3}|MCS2_{SF\,1,2}} W_{g_{SF\,i,j}}}{\sum_{g\in G_{I3}|MCS2_{SF\,1,2}} W_{g_{SF\,i,j}} + \sum_{f\in F_{I3}|MCS2_{SF\,1,2}} W_{f_{SF\,i,j}}}$$

where $G_{I3}|MCS2_{SF1,2} = \{A3\}$, $F_{I3}|MCS2_{SF1,2} = \{0\}$

$$= \frac{\sum_{g\in\{A3\}} W_{g_{SF\,i,j}}}{\sum_{g\in\{A3\}} W_{g_{SF\,i,j}} + \sum_{f\in\{0\}} W_f} = \frac{1}{1+0} = 1$$

$$IM^{CTL}_{I3|SF\,1,2} = \max\{M_{I3|SF\,1,2}(1), M_{I3|SF\,1,2}(2)\} = 1$$

Similarly to the above,

$$IM^{CTL}_{I5|SF\,1,2} = 0.67$$

$$IM^{CTL}_{I6|SF\,1,2} = 0.5$$

$$IM^{CTL}_{A1|SF\,1,2} = IM^{CTL}_{A2|SF\,1,2} = 0.5$$

$$IM^{CTL}_{A3|SF\,1,2} = 1$$

As described above, a method of calculating the importance of each component considering redundancy/diversity design in one SF has been presented. In addition, DI&C systems have functional redundancy/diversity design. From the functional aspect, the importance of each component for a given mission x can be calculated from Eqs. 11–14 according to its type. In the equations, a, b, and c represent the total number of PCs, CAs, and controllers, respectively.

$$IM_{Sn|Mx} = \sum_{y=1}^{a}\sum_{i=1}^{b}\sum_{j=1}^{c} W_{PCy}\left\{W_{CAi}(W_{SF_{i,j}} \cdot IM^{INS}_{Sn|SF\ i,j})\right\} \quad (11)$$

$$IM_{Cn|Mx} = \sum_{y=1}^{a}\sum_{i=1}^{b}\sum_{j=1}^{c} W_{PCy}\left\{W_{CAi}(W_{SF_{i,j}} \cdot IM^{DEC}_{Cn|SF\ i,j})\right\} \quad (12)$$

$$IM_{An|Mx} = \sum_{y=1}^{a}\sum_{i=1}^{b}\sum_{j=1}^{c} W_{PCy}\left\{W_{CAi}(W_{SF_{i,j}} \cdot IM^{CTL}_{An|SF\ i,j})\right\} \quad (13)$$

$$IM_{In|Mx} = \sum_{y=1}^{a}\sum_{i=1}^{b}\sum_{j=1}^{c} W_{PCy}\left[W_{CAi}\left\{W_{SF_{i,j}}(IM^{INS}_{In|SF\ i,j} + IM^{CTL}_{In|SF\ i,j})\right\}\right] \quad (14)$$

Lastly, it is considered that there might be multiple successive missions required of a DI&C system. By adding the subtotal importance of each component derived for each mission throughout all missions, the final importance of each component can be derived from Eqs. 15–18. The maximum importance for each component can vary depending on the system features for redundancy or diversity. In other words, if a specific component is used multiple times in several SFs according to the system design for redundancy or diversity, the importance of that component can increase, and its upper limit cannot be specified. Thus, each component importance derived by this methodology can be properly analyzed through relative comparison.

$$IM_{Sn} = \sum_{X=1}^{T} IM_{Sn|Mx} \quad (15)$$

$$IM_{Cn} = \sum_{X=1}^{T} IM_{Cn|Mx} \quad (16)$$

$$IM_{An} = \sum_{X=1}^{T} IM_{An|Mx} \quad (17)$$

$$IM_{In} = \sum_{X=1}^{T} IM_{In|Mx} \quad (18)$$

3. APPLICATIN TO AN EXAMPLE

In this section, an application of the methodology through a hypothetical I&C system is shown. A single mission, heat removal from the reactor, is required to the system by forming the flow paths from the coolant tank to the reactor, as shown in Figure 4. The configuration of the SFs in the I&C system and weight assignments to the PCs, CAs, and SFs are organized in Figure 5.

Figure 4. Configuration of actuators in the example system

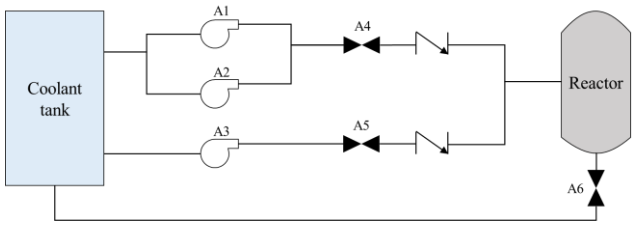


Figure 5. Functional redundancy/diversity and weight assignments in the example system

M1(1/2) **Heat removal from the reactor**

PC1(1/2) W_{PC1}: 0.8 | Formation of the primary flow path (A1, A2, A4, A6)

CA1(1/2) W_{CA1}:1 | Run A1 and A2, Open A4 and A6

SF1,1	Instrumentation	Decision	Control
$W_{SF1,1}$: 0.8	S1, I1, I4	C1 (Auto-controller)	I7, I8, I9, A1, A2, A4, A6

SF1,2	Instrumentation	Decision	Control
$W_{SF1,2}$: 0.2	S1, S2, I2, I5, I6	C2 (human)	I5, I8, I9, A1, A2, A4, A6

PC2(1/1) W_{PC2}: 0.2 | Formation of the auxiliary flow path (A3, A5, A6)

CA2(1/1) W_{CA2}: 1 | Run A3, Open A5 and A6 (Conservatively assuming that A6 has not been opened by CA1)

SF2,2	Instrumentation	Decision	Control
$W_{SF2,2}$: 1	S1, S2, S3, I2, I3, I5, I6	C2 (human)	I5, I9, A3, A5, A6

It is assumed that two types of PCs are possible from the I&C system for mission completion: primary (PC1) or auxiliary (PC2) flow path formations. The primary flow path is formed by CA1 (run A1 and A2, open A4 and A6), where CA1 can be generated/executed by SF1,1 (auto-controller related) or SF1,2 (human operator related), and A1 or A2 alone has sufficient capacity to remove heat. On the other hand,

the auxiliary flow path is formed by CA2 (Run A3, Open A5 and A6), where CA2 can be generated/executed by only one SF, SF2,2 (of which controller is a human operator, same to the SF1,2). In terms of weight assignment, it is assumed that PC1, which is expected to be accomplished primarily, is more important: W_{PC1} = 0.8 and W_{PC2} = 0.2. PC1 and PC2 are each accomplished by a single CA, CA1 and CA2, respectively: W_{CA1} 1 = 1 and W_{CA1} = 1. Regarding CA1, it is desirable to be automatically generated/executed by the auto-controller (C1) to eliminate unnecessary confusion and to response efficiently. If the automatic CA1 is not generated/executed by the auto-controller, the human operator (C2) should recognize the situation and generate a manual CA, in which case the human operator is subject to a task load and may experience mental burden: $W_{SF1,1}$ = 0.8, $W_{SF1,2}$ = 0.2. Otherwise, CA2 is generated/executed by a single SF, SF2,2, and thus the weight of SF2,2 is 1.
The three SFs of the I&C system each have 3 sensors, 9 interfaces (as a human–system interface, interface 5 is used for both instrumentation and control steps), 2 controllers, and 6 actuators. In more detail, CA1 and CA2 can be generated/executed as described below and as shown in Figure 6.

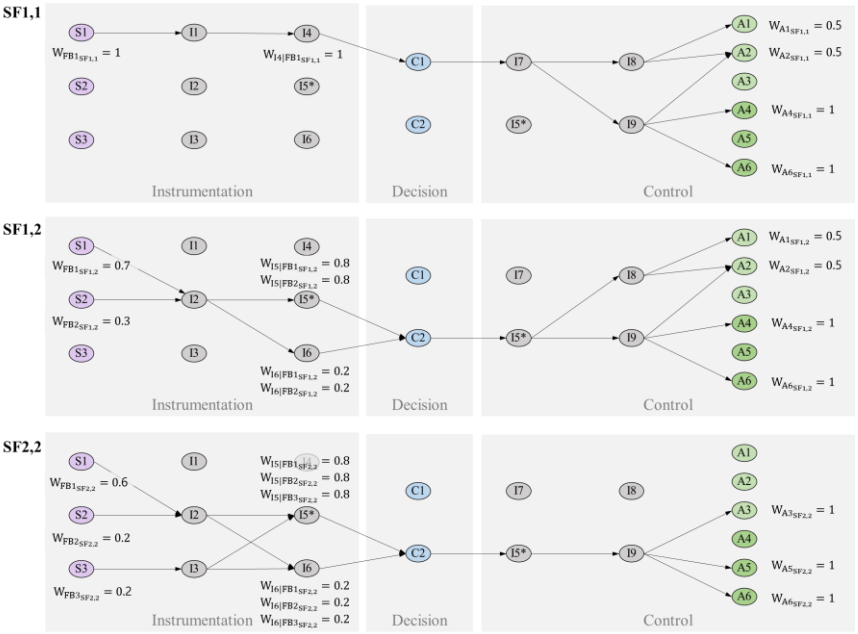
- CA1 is generated by either C1 or C2
  - SF1,1: CA1 is decided to be generated by C1 referring to FB1 received via I4, and transmitted to A1, A2, A4, and A6 via I7, I8, and I9.
  - SF1,2: CA1 is decided to be generated by C2 referring to FB1 and FB2 received via I5 and I6, and transmitted to A1, A2, A4, and A6 via I5, I8, and I9.
- CA2 is generated by C2
  - SF2,2: CA2 is decided to be generated by C2 referring to FB1, FB2, and FB3 received via I5 and I6, and transmitted to A3, A5, and A6 via I5 and I9.

The weights for the sensors, front-end interfaces, and actuators are assigned on the basis of the following assumptions:

- Auto-controller (C1) generates CA1 referring to only a single FB, FB1.
  - $W_{FB1_{SF1,1}} = 1$
- When the human operator (C2) generates CA1, it is assumed that the FB2 signal is used as auxiliary information compared to FB1.
  - $W_{FB1_{SF1,2}} = 0.7, W_{FB2_{SF1,2}} = 0.3$
- When the human operator (C2) generates CA2, it is assumed that FB2 and FB3 are used as auxiliary information compared to FB1.
  - $W_{FB1_{SF2,2}} = 0.6, W_{FB2_{SF2,2}} = W_{FB3_{SF2,2}} = 0.2$
- In the case of the auto-controller, a single FB is received over a single interface, I4, to make a decision. On the other hand, the human operator makes a decision based on a number of FBs received over multiple interfaces, I5 and I6, but is assumed to pay more attention to the FB received from I5 than that from I6.
  - $W_{I_4|FB1_{SF1,1}} = 1$ (FB1 for SF1,1 is received only though I4)
  - $W_{I_5|FB1_{SF1,2}} = W_{I_5|FB2_{SF1,2}} = 0.8$, $W_{I_6|FB1_{SF1,2}} = W_{I_6|FB2_{SF1,2}} = 0.2$ (C2 pays more attention to the FB received from I5 than I6)
  - $W_{I_5|FB1_{SF2,2}} = W_{I_5|FB2_{SF2,2}} = W_{I_5|FB3_{SF2,2}} = 0.8$, $W_{I_6|FB1_{SF2,2}} = W_{I_6|FB2_{SF2,2}} = W_{I_6|FB3_{SF2,2}} = 0.2$ (C2 pays more attention to the FB received from I5 than I6)
- The PC can be completed with only one of the two pumps, A1 and A2, which are activated by CA1. All the other valves and pumps must operate normally for PC completion.
  - $MCS1_{SF\,1,1} = \{A1, A2\}, MCS2_{SF\,1,1} = \{A4\}, MCS3_{SF\,1,1} = \{A6\}$
  - $MCS1_{SF\,1,2} = \{A1, A2\}, MCS2_{SF\,1,2} = \{A4\}, MCS3_{SF\,1,2} = \{A6\}$
  - $MCS1_{SF\,2,2} = \{A3\}, MCS2_{SF\,2,2} = \{A5\}, MCS3_{SF\,2,2} = \{A6\}$

- $W_{A1_{SF1,1}} = W_{A2_{SF1,1}} = W_{A1_{SF1,2}} = W_{A2_{SF1,2}} = 0.5$
- $W_{A4_{SF1,1}} = W_{A6_{SF1,1}} = W_{A4_{SF1,2}} = W_{A6_{SF1,2}} = W_{A3_{SF2,2}} = W_{A5_{SF2,2}} = W_{A6_{SF2,2}} = 1$

Figure 6. Components in each signal flow within the example system



Based on Eqs. 1–10 and the assigned weights, the importance of the components in each step in each SFi,j can be calculated. In this calculation, the subtotal importance and final importance are the same from the assumption that only one mission is required. In Table 1, larger and smaller values are highlighted in red and green, respectively.

Table I. Results of the component importance analysis of the example system

PC	W_{PC1}					0.8	W_{PC2}		0.2	IM_n
CA	W_{CA1}					1	W_{CA2}		1	
SF	$W_{SF1,1}$		0.8	$W_{SF1,2}$		0.2	$W_{SF2,2}$		1	
n	$IM^{INS}_{n\|SF1,1}$	$IM^{DEC}_{n\|SF1,1}$	$IM^{CTL}_{n\|SF1,1}$	$IM^{INS}_{n\|SF1,2}$	$IM^{DEC}_{n\|SF1,2}$	$IM^{CTL}_{n\|SF1,2}$	$IM^{INS}_{n\|SF2,2}$	$IM^{DEC}_{n\|SF2,2}$	$IM^{CTL}_{n\|SF2,2}$	
S1	1			0.7			0.6			0.872
S2				0.3			0.2			0.088
S3							0.2			0.040
C1		1								0.640
C2					1			1		0.360
A1			0.5			0.5				0.400
A2			0.5			0.5				0.400
A3									1	0.200
A4			1			1				0.800
A5									1	0.200
A6			1			1			1	1.000
I1	1									0.640
I2				1			0.8			0.320
I3							0.2			0.040
I4	1									0.640
I5				0.8		1	0.8		1	0.648
I6				0.2			0.8			0.192
I7			1							0.640
I8			0.67			0.67				0.536
I9			1			1			1	1.000

The rationality of the derived results can be verified as follows. All control actions (CA1 and CA2) must open A6 for mission completion, and all CA transmissions to A6 are via I9, so these two components (A6 and I9) are analyzed as the most important components. S1 is also analyzed as an important

component as it is not only used to generate CA1 through the high-weighted SF (SF1,1) for the high-weighted PC (PC1) but also used in all other SFs (SF1,2 and SF2,2). A4 is also analyzed as an important component because both control steps in the SF for the high-weighted PC (PC1) fail if A4 is unavailable. In addition, C1, I1, I4, I5, and I7 are analyzed as having some significance for mission completion. I1, I4, and C1 transmit the only FB (FB1) and generate the CA in the high-weighted SF (SF1,1), while I5 and I7 represent a bottleneck in the transmission of the CAs. On the other hand, S3 and I3 are analyzed as having very low importance because they are only used in SF2,2 for the low-weighted PC (PC2) and are also treated as reference information for FB1 and FB2.

4. CONCLUSION

In this paper, the authors proposed a methodology to comprehensively evaluate the quantitative importance of the components of digital I&C systems that may have complex interactions including automatic/manual aspects even when reasonable failure data of the components cannot be obtained. This method provides a framework to analyze the redundancy/diversity design features from a functional aspect according to the hierarchy of mission, physical control, and control action, as well as from a signal flow aspect according to the correlation between the components constituting each SF. The SFs are divided into three steps, instrumentation, decision, and control, and the impact of a particular component on each step is quantified based on an assigned weight under the principle that the entire SF fails when a step becomes disabled due to problems with the components that make it up. The subtotal importance of each component calculated for each SF is then used to derive final importance values in conjunction with the weights allocated to the PCs, CAs, and SFs.
Based on the analysis results according to the proposed methodology, increased safety of a control system might be achieved by modifying the system design to not concentrate importance on a small number of components or by driving the implementation of high reliability for certain components with high importance. Before such practical applications though, it is necessary to consider the following points in utilizing this methodology.

- This study assumed that the signals (FBs or CAs) do not deteriorate or change in the process of transmission.
- This study assumed that one CA is created by only one controller.
- The results of analysis vary depending on the assigned weights.
- The boundary and balance between components should be properly considered and defined.

In this paper, the focus was on establishing the logical concept of methodology. Currently, an application analysis is being performed on a real-world system to validate the validity of this methodology. Furthermore, in order to ensure the validity of the methodology, it is believed that a method that objectively and systematically assign related weights must be supported. In this regard, the authors plant to conduct a follow-up study.

Acknowledgements

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety(KoFONS) using the financial resource granted by the Nuclear Safety and Security Commission(NSSC) of the Republic of Korea (No. 2106005) and by the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT. (2020M2D7A1079182)

References

[1] IAEA, “Safety of Nuclear Power Plants: Design”, Specific Safety Requirements No. SSR-2/1 (Rev. 1), Vienna 2016.
[2] IAEA, “Criteria for Diverse Actuation Systems for Nuclear Power Plants”, IAEA TECDOC SERIES, IAEA-TECDOC-1848, Vienna 2018

[3] World Nuclear Association, “Defence-in-Depth and Diversity: Challenges Related to I&C Architecture” , 2018
[4] NRC, “Digital I&C Systems in Nuclear Power Plant”, NUREG/CR-6579, 1998
[5] D. Blanchard and R. Torok, “Risk Insights Associated with Digital Upgrades,” Proc. 10th International Probabilistic Safety Assessment & Management Conference, PSAM 10, Seattle, Washington, June 7–11, 2010, paper 453
[6] World nuclear association, “I&C Modernization: Current Status and Difficulties”, 2020
[7] ANS, “How the NRC modernized infrastructure and where it”, 2021
[8] T.L. Chu, G. Martinez-Guridi, M. Yue, J. Lehner and P. Samanta, “Traditional Probabilistic Risk Assessment Methods for Digital Systems”, NUREG/CR-6962, United States Nuclear Regulatory Commission, Washington D.C. 2008
[9] Recommendations on assessing digital system reliability in probabilistic risk assessments of nuclear power plants, NEA/CSNI/R(2009)18, OECD/NEA/CSNI, Paris, 2009.
[10] S. Authen, J. E. Holmberg, "Reliability analysis of digital systems in a probabilistic risk analysis for nuclear power plants”, Nuclear Engineering and Technology, Vol 44 Issue 5, P. 471-482, 2012.
[11] Kim YC, Kim JW, Park Jk, Choi CS, Kim HE. An HRA Method for Digital Main Control Rooms – Part II: Estimating the Failure Probability Due to Cognitive Error. Korea At. Energy Research Inst., Daejeon, Republic of Korea, Tech. Rep. Sep. 2020 KAERI/TR-8065/2020.
[12] Markus Porthin, Marja Liinasuo, Terhi Kling, Effects of digitalization of nuclear power plant control rooms on human reliability analysis – A review, Rel. Eng. Syst. Saf, Volume 194, 2020,
[13] Sang Hun Lee, Seung Jun Lee, Sung Min Shin, Eun-chan Lee, Hyun Gook Kang, Exhaustive testing of safety-critical software for reactor protection system, Rel. Eng. Syst. Saf, Volume 193, 2020
[14] Sejin Jung, Junbeom Yoo, Young-Jun Lee, A Software Fault Tree Analysis Technique for Formal Requirement Specifications of Nuclear Reactor Protection Systems, Rel. Eng. Syst. Saf, Volume 203, 2020,
[15] Sang Hun Lee, Hee Eun Kim, Kwang Seop Son, Sung Min Shin, Seung Jun Lee, Hyun Gook Kang, Reliability modeling of safety-critical network communication in a digitalized nuclear power plant, Rel. Eng. Syst. Saf, Volume 144, 2015
[16] Markus Porthin, Sung-Min Shin, Milan Jaros, Jiri Sedlak, Paolo Picca, Richard Quatrain, Jeanne Demgné, Hans Brinkman, Venkat Natarajan, Tero Tyrväinen, Christian Müller, Ewgenij Piljugin, "WGRISK DIGMAP: Comparison of PSA Modeling Approaches for Digital I&C", 12th NPIC&HMIT, 2021
[17] NRC “Office of Nuclear Regulatory Research FY2020-22 Planned Research Activities”, 2020
[18] N. G. Leveson, “A new accident model for engineering safety systems”, Safety Science, Volume 42, Issue 4, Pages 237-270, 2004
[19] N. G. Leveson, “Engineering a Safer World: Systems Thinking Applied to Safety”, The MIT Press, 2011
[20] N. G. Leveson, J. P. Thomas, “STPA Handbook, MIT, 2018
[21] Allison CK, Revell KM, Sears R, Stanton NA. Systems Theoretic Accident Model and Process (STAMP) safety modelling applied to an aircraft rapid decompression event. Saf. Sci. Oct. 2017;98:159–66.
[22] Faiella G, Parand A, Franklin BD, Chana P, Cesarelli M, Stanton NA, Sevdalis N. Expanding healthcare failure mode and effect analysis: A composite proactive risk analysis approach. Rel. Eng. Syst. Saf. Jan. 2018;169:117–26
[23] Read GJM, Naweed A, Salmon PM. Complexity on the rails: A systems-based approach to understanding safety management in rail transport. Rel. Eng. Syst. Saf. Aug. 2019;188:352–65
[24] Model for safety assessment of autonomous merchant vessels. Rel. Eng. Syst. Saf. Oct. 2018;178:209–24.
[25] Wheeler T, Clark A, Williams A, Muna A, Dawson L, Geddes B, Blanchard D.Hazards and Consequences Analysis for Digital Systems. EPRI technical report Dec. 2018.
[26] Shin S-M SHIN, Lee SH, Shin SK, Jang IS, Park JK. STPA-Based Hazard and Importance Analysis on NPP Safety I&C Systems Focusing on Human–System Interactions. Rel. Eng. Syst. Saf. Volume 213, 2021