A New Approach to Quantitative Importance Analysis of I&C System Components

Sung-Min Shin [a*], Sang Hun Lee [a], Seung Ki Shin [a]
[a]*Korea Atomic Energy Research Institute, 111 Daedeok-daero, 989beon-gil, Yuseong-gu, Daejeon, Republic of Korea 34057*
[*]*Corresponding author: smshin@kaeri.re.kr*

1. Introduction

The quantitative methods for reliability or risk analysis of instrumentation and control (I&C) systems are usually based on probabilistic failure information of each system component. This approach is well suited to the analysis of systems with sufficient operation experience. However, it is difficult to apply to a system which has not enough operation experience since the appropriate failure information of the components cannot be assured. It is, therefore, necessary to explore a new approach for quantitative analysis that does not rely on the failure information of components.

There are approaches to viewing accidents in the control system as problems in control, not failures. The approach to safety engineering, called STAMP (system-theoretic accident model and processes), models a control structure of a control system based on control loops which is composed of a controller, controlled process, feedbacks (FBs), and control actions (CA) [1-8]. The methodology the authors would like to present in this paper is basically based on the similar scheme. In addition to that, as a basis for quantitative analysis results, relative weights for some elements that make up the system are assigned. In this paper, basic concepts and details of methodology with a simple example are described.

2. Methods and Results

2.1 Basic Concept

The I&C system literally measures and controls control targets. In deeper look, there are three steps: (1) Instrumentation, the feedback (FB) being referred to control action (CA) determination is generated by the sensors and transmitted to the controller through the associated interfaces, (2) Decision, a controller determines the CA generation based on the FBs received, and (3) Control, the generated CA is transmitted to the actuators performing the physical action through the associated interfaces. Basically, all functions of the I&C system are considered to go through the three steps, instrumentation – decision – control, so this general association is named as signal flow (SF) in this paper. A specific SF is formed according to the CA and controller, and each of the three steps consists of some of the following four types of components:

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

According to the given conditions of control target and the functional design of the I&C system, several SFs within the I&C system can be organized by hierarchy,

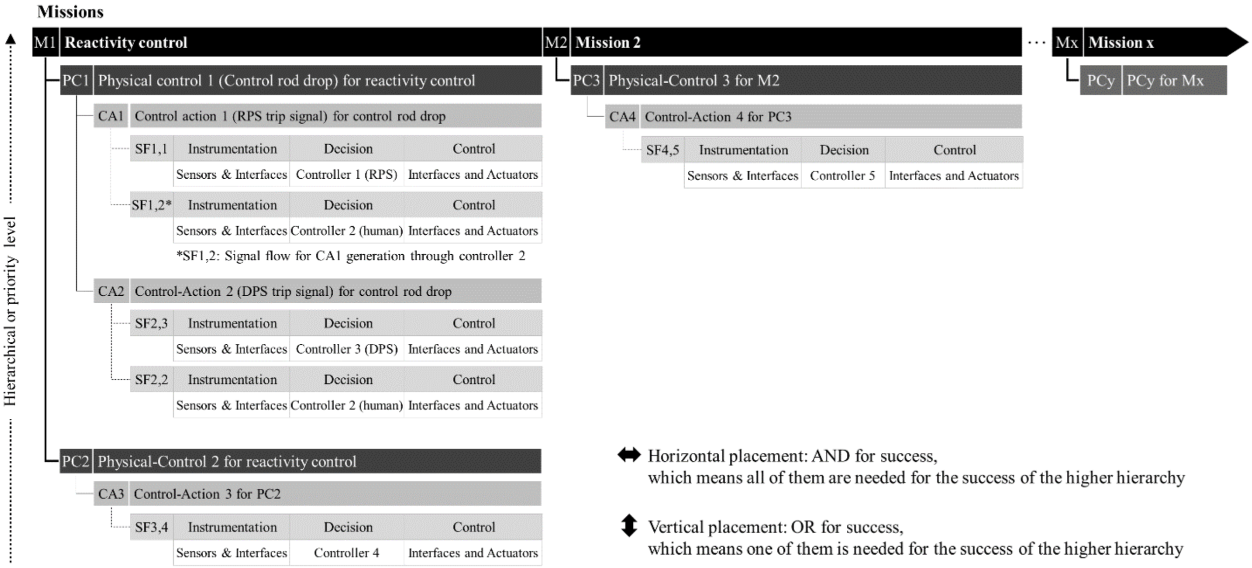
Missions
M1 Reactivity control
M2 Mission 2
Mx Mission x
PC1 Physical control 1 (Control rod drop) for reactivity control
PC3 Physical-Control 3 for M2
PCy PCy for Mx
CA1 Control action 1 (RPS trip signal) for control rod drop
CA4 Control-Action 4 for PC3
SF1,1 Instrumentation Decision Control
Sensors & Interfaces Controller 1 (RPS) Interfaces and Actuators
SF4,5 Instrumentation Decision Control
Sensors & Interfaces Controller 5 Interfaces and Actuators
SF1,2* Instrumentation Decision Control
Sensors & Interfaces Controller 2 (human) Interfaces and Actuators
*SF1,2: Signal flow for CA1 generation through controller 2
CA2 Control-Action 2 (DPS trip signal) for control rod drop
SF2,3 Instrumentation Decision Control
Sensors & Interfaces Controller 3 (DPS) Interfaces and Actuators
SF2,2 Instrumentation Decision Control
Sensors & Interfaces Controller 2 (human) Interfaces and Actuators
PC2 Physical-Control 2 for reactivity control
CA3 Control-Action 3 for PC2
SF3,4 Instrumentation Decision Control
Sensors & Interfaces Controller 4 Interfaces and Actuators
Hierarchical or priority level
Horizontal placement: AND for success,
which means all of them are needed for the success of the higher hierarchy
Vertical placement: OR for success,
which means one of them is needed for the success of the higher hierarchy

Fig. 1. Example configuration of signal flows in an I&C system

priority, and relation between them, as shown in the Fig. 1. In certain conditions of control target, when the sequential roles required by the I&C system are called missions, for a mission (M), physical control(s) should be completed. The physical control (PC) can be activated by the CAs, and the CAs can be generated and executed by the SF. Therefore, the I&C system can be hierarchically organized according to mission (M) – physical control (PC) – control action (CA) – signal flow (SF): Implementation/Decision/Control – Component.

Most safety I&C systems apply the concepts of diversity and redundancy to secure the reliability of their functions. The implementation process of those concepts results in various combinations of SFs. For description, an example is given in part of the Fig. 1. In the event of an abnormal situation at a nuclear power plant, the most mission to be taken is reactivity control. Generally, the reactivity control is achieved through control rod drop (PC1), and if there is an alternative means (PC2), the PC1 and 2 can be vertically placed. Here the vertical placement means one of the elements is enough for the functioning required from higher hierarchy. If both PC1 and 2 are needed for the mission completion, they should be placed horizontally. Upper side placement, another principle, at the same hierarchy means priority, so PC1 is a priority over PC2. At any hierarchy, if there are multiple elements in the same hierarchy, the horizontal/vertical and upper/lower side placement can be applied from the same perspective. In a deeper hierarchy, control rod drop, the PC1, can be made through either CA1 (RPS trip signal) or CA2 (DPS trip signal); It is assumed that either CA1 and 2 can drop the control rod, and the CA1 takes priority over CA2.

In the deepest hierarchy, SF, the RPS trip signal can be generated automatically by the RPS machine or manually by the human; Either SFs can generate and execute CA1, and the SF through RPS machine takes priority over the SF through human. RPS machine and human can collect different, identical, or additional FBs through different paths, and the generated CA through RPS machine or human can be transmitted to the actuators in different, identical, or partially overlapped paths. In other words, the components utilized for the two SFs might different, identical, or overlapped.

In summing up the above, the SFs within the I&C system under a given mission can be schematized as shown in Fig. 1. by hierarchy, priority, and relation between them. Considering that each SF is formed by the components, it should be noted that certain components utilized in each SF can also be used in other SFs. Therefore, if a component is unavailable, the soundness of several SFs can be affected. The basic concept of the method 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 three steps, instrumentation, decision, and control is degraded is assessed, and the larger the degradation is, the more important component is. Then, by summing the importance of each component calculated for each SF all over the missions, the final importance of each component for that missions is calculated.

2.2 Details of Methodology

The design information for the I&C system can be utilized to schematic the SF as given Fig. 2. The SF can be expressed by placing sensors and interfaces related to FB generation/transmission at the front, centering on the controller, and interfaces and actuators related to CA transmission/execution at the back. Each component can be represented by a node with component type-specific ID (S for sensor, C for controller, A for actuator, I for interface), and the signal flow between components can be represented by an arrow. If necessary, an arrow may indicate the name of the FB or CA.

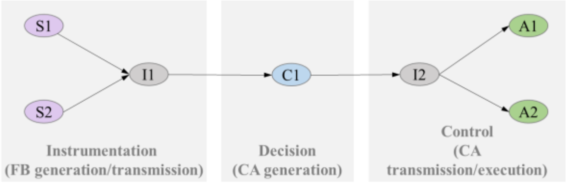

Fig. 2 . Schematic representation of signal flow

This method assigns weights, instead of failure information, as the basis for quantitative analysis results: (1) the weights assigned to the elements in the same 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, and (2) in a single SF, the weights are assigned to some FBs and components from the instrumentation and control perspective (Fig. 3.).

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, MCS for M1 is PC1× PC2 since one of them can complete M1, so sum of weights for 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 MCS for M1 is PC1 + PC 2, the weights for each PC will be 1, respectively. Based on this principle, example weights for each CA and SF are assigned: W_{CA1}= 0.7, W_{CA1}= 0.3, and sum of them equal to 1, $W_{SF1,1}$= 0.8, $W_{SF1,2}$= 0.2, and sum of them equal to 1, and so on. The weight assignment for PC, CA, and SF described above can be defined like below.

$\sum_{y\in MCS_{Mx}} W_{PCy} = 1$

where MCS_{Mx} is MCS of PCs causing Mx failure

$\sum_{i\in MCS_{PCy}} W_{CAi} = 1$

where MCS_{PCy} is MCS of CAs causing PCy failure

$\sum_{j\in MCS_{CAi}} W_{SF\,i,j} = 1$

where MCS_{CAi} is MCS of SFs causing CAi failure

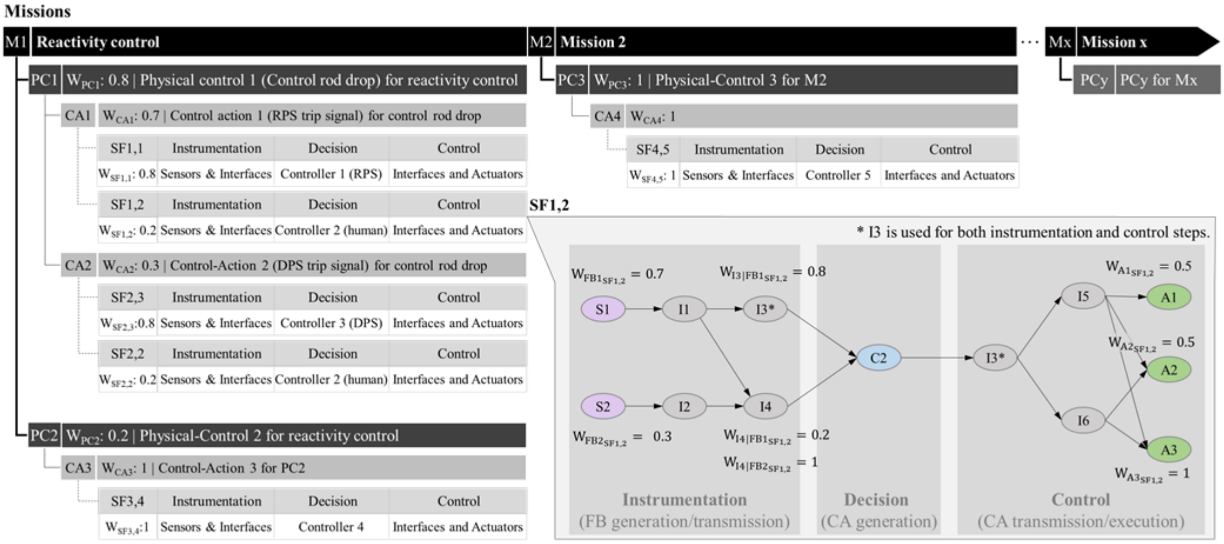
Missions
M1 Reactivity control
PC1 W_{PC1}: 0.8 | Physical control 1 (Control rod drop) for reactivity control
CA1 W_{CA1}: 0.7 | Control action 1 (RPS trip signal) for control rod drop
SF1,1 Instrumentation Decision Control
$W_{SF1,1}$: 0.8 Sensors & Interfaces Controller 1 (RPS) Interfaces and Actuators
SF1,2 Instrumentation Decision Control
$W_{SF1,2}$: 0.2 Sensors & Interfaces Controller 2 (human) Interfaces and Actuators
CA2 W_{CA2}: 0.3 | Control-Action 2 (DPS trip signal) for control rod drop
SF2,3 Instrumentation Decision Control
$W_{SF2,3}$:0.8 Sensors & Interfaces Controller 3 (DPS) Interfaces and Actuators
SF2,2 Instrumentation Decision Control
$W_{SF2,2}$: 0.2 Sensors & Interfaces Controller 2 (human) Interfaces and Actuators
PC2 W_{PC2}: 0.2 | Physical-Control 2 for reactivity control
CA3 W_{CA3}: 1 | Control-Action 3 for PC2
SF3,4 Instrumentation Decision Control
$W_{SF3,4}$:1 Sensors & Interfaces Controller 4 Interfaces and Actuators
M2 Mission 2
PC3 W_{PC3}: 1 | Physical-Control 3 for M2
CA4 W_{CA4}: 1
SF4,5 Instrumentation Decision Control
$W_{SF4,5}$: 1 Sensors & Interfaces Controller 5 Interfaces and Actuators
Mx Mission x
PCy PCy for Mx
SF1,2
* I3 is used for both instrumentation and control steps.
$W_{FB1_{SF1,2}} = 0.7$
$W_{I3|FB1_{SF1,2}} = 0.8$
S1
I1
I3*
S2
I2
I4
$W_{FB2_{SF1,2}} = 0.3$
$W_{I4|FB1_{SF1,2}} = 0.2$
$W_{I4|FB2_{SF1,2}} = 1$
C2
I3*
I5
I6
A1
A2
A3
$W_{A1_{SF1,2}} = 0.5$
$W_{A2_{SF1,2}} = 0.5$
$W_{A3_{SF1,2}} = 1$
Instrumentation
(FB generation/transmission)
Decision
(CA generation)
Control
(CA transmission/execution)

Figure 3 Example of weights assignment

The assigned weights to PC, CA, and SF will be utilized when updating the importance of components derived within each SF to the importance from a mission perspective. The underlying philosophy is like follow; If a component is used in a specific SF, and the SF is used to generate a CA that is treated as important, and CA is also used to perform an important PC, the component is very important from a mission perspective. For example, let's say different sensors are used in SF1,1 and SF2,2. Comparing $W_{SF1,1}$ (0.8) and W_{CA1} (0.7) with $W_{SF2,2}$ (0.2) and W_{CA2} (0.3), from a mission perspective, the sensor used in SF1,1 would be more important than the sensor used in SF2,2.

Next, within a single SF, weights are assigned from the instrumentation, and control perspective. Based on the assigned weights, the importance of each component is calculated by evaluating the extent to which a particular component impairs the soundness of each step when that component unavailable.

From the instrumentation perspective, weights are assigned between FBs generated by sensors, and between the front-end components through where a particular FB is transmitted to the controller. The principle is that it would be important that the FB, which has a significant impact on the decision, be transmitted as a path effectively recognizable to the controller. An example of weight assignment for SF1,2 is given in Fig. 3. When 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 an auxiliary information of S1 signal (FB1); For this reason, weight of 0.7 is assigned to FB1 which is relatively high compare to the weight for FB2 (0.3). Regarding the FB transmission, the FB2 is transmitted to C2 through the only front-end component I4, so the weight of front-end component I4 transmitting FB2 for SF1,2, $W_{I4|FB2_{SF1,2}}$, equal to 1. Meanwhile, the FB1 is transmitted to C2 through the two front-end components I3 and I4, so the weights for 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 human 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 components 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/execution through controller j)

where $\sum_{k=1}^{\alpha} W_{FBk_{SF\,i,j}} = 1$ for a specific SF i, j $(0 \leq W_{FBk_{SF\,i,j}} \leq 1$, $W_{FBk_{SF\,i,j}} = 0$ if FB k is not used for SF i, j)

where α = total number of FBs in a given system

$W_{Cx|FBk_{SF\,i,j}}$: Weight of a specific front-end component x transmitting FB k in SF i, j

where $\sum_{x=1}^{\beta} W_{Cx|FBk_{SF\,i,j}} = 1$ for a specific SF i, j $(0 \leq W_{Cx|FBk_{SF\,i,j}} \leq 1$, $W_{Cx|FBk_{SF\,i,j}} = 0$) if component x is not the front-end component 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 a sensor n ($IM^{INS}_{S_n|SF\,i,j}$) or an interface n ($IM^{INS}_{I_n|SF\,i,j}$) in SF i, j from the instrumentation perspective can be calculated. The underlying principle is that the importance of a sensor or interface corresponds with the degree to which the soundness of instrumentation (FB_k generation/transmission) is degraded due to that unavailable component. The closer the calculated value to 1, the more likely the failure of that component will result in a complete loss of instrumentation step. In case of IM for a sensor, it is simple. If there is a problem with a particular sensor, the controller cannot receive the FB generated by that sensor through any path, so the weight assigned to the FB generated by that sensor itself becomes the importance of that sensor.

$$\mathrm{IM}^{\mathrm{INS}}_{\mathrm{Sn|SF\,i,j}} = W_{\mathrm{FBk}_{\mathrm{SF\,i,j}}}\ (n = k) \qquad \text{(Eq. 1)}$$

Generated FB signals 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 for diversity. However, that doesn't mean the transmission is not degraded at all. Therefore, the importance of a particular importance is calculated according to the following concepts: how large the negative effect is in compare to the sum of the negative effects and the degree to which it can still function.

$$\mathrm{IM}^{\mathrm{INS}}_{\mathrm{In|SF\,i,j}} = \sum_{k=1}^{\alpha}\left(W_{\mathrm{FBk}_{\mathrm{SF\,i,j}}}\frac{\sum_{g\in G_{\mathrm{In}}|\mathrm{FBk}} W_{g|\mathrm{FBk}_{\mathrm{SF\,i,j}}}}{\sum_{g\in G_{\mathrm{In}}|\mathrm{FBk}_{\mathrm{SF\,i,j}}} W_{g|\mathrm{FBk}_{\mathrm{SF\,i,j}}}+\sum_{f\in F_{\mathrm{In}}|\mathrm{FBk}_{\mathrm{SF\,i,j}}} W_{f|\mathrm{FBk}_{\mathrm{SF\,i,j}}}}\right) \qquad \text{(Eq. 2)}$$

where $G_{\mathrm{In}}|\mathrm{FBk}_{\mathrm{SF\,i,j}}$: A group of front-end components transmitting FB k via the interface n in SF i, j

where $F_{\mathrm{In}}|\mathrm{FBk}_{\mathrm{SF\,i,j}}$: A group of front-end components transmitting FB k other than the interface n in SF i, j

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

$$\mathrm{IM}^{\mathrm{INS}}_{\mathrm{S1|SF1,2}} = W_{\mathrm{FB1}_{\mathrm{SF1,2}}} = 0.7$$

$$\mathrm{IM}^{\mathrm{INS}}_{\mathrm{S2|SF1,2}} = W_{\mathrm{FB2}_{\mathrm{SF1,2}}} = 0.3$$

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

(where $G_{\mathrm{I1}}|\mathrm{FB1}_{\mathrm{SF1,2}} = \{\mathrm{I3},\mathrm{I4}\}$, $F_{\mathrm{I1}}|\mathrm{FB1}_{\mathrm{SF1,2}} = \{0\}$, $G_{\mathrm{I1}}|\mathrm{FB2}_{\mathrm{SF1,2}} = \{0\}$, $F_{\mathrm{I1}}|\mathrm{FB2}_{\mathrm{SF1,2}} = \{\mathrm{I4}\}$)

$$= W_{\mathrm{FB1}_{\mathrm{SF1,2}}}\frac{\sum_{g\in\{\mathrm{I3,I4}\}} W_{g|\mathrm{FB1}_{\mathrm{SF1,2}}}}{\sum_{g\in\{\mathrm{I3,I4}\}} W_{g|\mathrm{FB1}_{\mathrm{SF1,2}}}+\sum_{f\in\{0\}} W_{f|\mathrm{FB1}_{\mathrm{SF1,2}}}} + W_{\mathrm{FB2}_{\mathrm{SF1,2}}}\frac{\sum_{g\in\{0\}} W_{g|\mathrm{FB1}_{\mathrm{SF1,2}}}}{\sum_{g\in\{0\}} W_{g|\mathrm{FB1}_{\mathrm{SF1,2}}}+\sum_{f\in\{\mathrm{I4}\}} W_{f|\mathrm{FB1}_{\mathrm{SF1,2}}}}$$

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

$$\mathrm{IM}^{\mathrm{INS}}_{\mathrm{I2|SF1,2}} = \sum_{k=1}^{2}\left(W_{\mathrm{FBk}_{\mathrm{SF1,2}}}\frac{\sum_{g\in G_{\mathrm{I2}}|\mathrm{FBk}} W_{g|\mathrm{FBk}_{\mathrm{SF1,2}}}}{\sum_{g\in G_{\mathrm{I2}}|\mathrm{FBk}_{\mathrm{SF1,2}}} W_{g|\mathrm{FBk}_{\mathrm{SF1,2}}}+\sum_{f\in F_{\mathrm{I2}}|\mathrm{FBk}_{\mathrm{SF1,2}}} W_{f|\mathrm{FBk}_{\mathrm{SF1,2}}}}\right)$$

(where $G_{\mathrm{I2}}|\mathrm{FB1}_{\mathrm{SF1,2}} = \{0\}$, $F_{\mathrm{I2}}|\mathrm{FB1}_{\mathrm{SF1,2}} = \{\mathrm{I3},\mathrm{I4}\}$, $G_{\mathrm{I2}}|\mathrm{FB2}_{\mathrm{SF1,2}} = \{\mathrm{I4}\}$, $F_{\mathrm{I2}}|\mathrm{FB2}_{\mathrm{SF1,2}} = \{0\}$)

$$= W_{\mathrm{FB1}_{\mathrm{SF1,2}}}\frac{\sum_{g\in\{0\}} W_{g|\mathrm{FB1}_{\mathrm{SF1,2}}}}{\sum_{g\in\{0\}} W_{g|\mathrm{FB1}_{\mathrm{SF1,2}}}+\sum_{f\in\{\mathrm{I3,I4}\}} W_{f|\mathrm{FB1}_{\mathrm{SF1,2}}}} + W_{\mathrm{FB2}_{\mathrm{SF1,2}}}\frac{\sum_{g\in\{\mathrm{I4}\}} W_{g|\mathrm{FB1}_{\mathrm{SF1,2}}}}{\sum_{g\in\{\mathrm{I4}\}} W_{g|\mathrm{FB1}_{\mathrm{SF1,2}}}+\sum_{f\in\{0\}} W_{f|\mathrm{FB1}_{\mathrm{SF1,2}}}}$$

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

$$\mathrm{IM}^{\mathrm{INS}}_{\mathrm{I3|SF1,2}} = \sum_{k=1}^{2}\left(W_{\mathrm{FBk}_{\mathrm{SF1,2}}}\frac{\sum_{g\in G_{\mathrm{I3}}|\mathrm{FBk}} W_{g|\mathrm{FBk}_{\mathrm{SF1,2}}}}{\sum_{g\in G_{\mathrm{I3}}|\mathrm{FBk}_{\mathrm{SF1,2}}} W_{g|\mathrm{FBk}_{\mathrm{SF1,2}}}+\sum_{f\in F_{\mathrm{I3}}|\mathrm{FBk}_{\mathrm{SF1,2}}} W_{f|\mathrm{FBk}_{\mathrm{SF1,2}}}}\right)$$

(where $G_{\mathrm{I3}}|\mathrm{FB1}_{\mathrm{SF1,2}} = \{\mathrm{I3}\}$, $F_{\mathrm{I3}}|\mathrm{FB1}_{\mathrm{SF1,2}} = \{\mathrm{I4}\}$, $G_{\mathrm{I3}}|\mathrm{FB2}_{\mathrm{SF1,2}} = \{0\}$, $F_{\mathrm{I3}}|\mathrm{FB2}_{\mathrm{SF1,2}} = \{\mathrm{I4}\}$)

$$= W_{\mathrm{FB1}_{\mathrm{SF1,2}}}\frac{\sum_{g\in\{\mathrm{I3}\}} W_{g|\mathrm{FB1}_{\mathrm{SF1,2}}}}{\sum_{g\in\{\mathrm{I3}\}} W_{g|\mathrm{FB1}_{\mathrm{SF1,2}}}+\sum_{f\in\{\mathrm{I4}\}} W_{f|\mathrm{FB1}_{\mathrm{SF1,2}}}} + W_{\mathrm{FB2}_{\mathrm{SF1,2}}}\frac{\sum_{g\in\{0\}} W_{g|\mathrm{FB1}_{\mathrm{SF1,2}}}}{\sum_{g\in\{0\}} W_{g|\mathrm{FB1}_{\mathrm{SF1,2}}}+\sum_{f\in\{\mathrm{I4}\}} W_{f|\mathrm{FB1}_{\mathrm{SF1,2}}}}$$

$$= 0.7\frac{0.8}{0.8+0.2} + 0.3\frac{0}{0+1} = 0.56$$

$$\mathrm{IM}^{\mathrm{INS}}_{\mathrm{I4|SF1,2}} = \sum_{k=1}^{2}\left(W_{\mathrm{FBk}_{\mathrm{SF1,2}}}\frac{\sum_{g\in G_{\mathrm{I4}}|\mathrm{FBk}} W_{g|\mathrm{FBk}_{\mathrm{SF1,2}}}}{\sum_{g\in G_{\mathrm{I4}}|\mathrm{FBk}_{\mathrm{SF1,2}}} W_{g|\mathrm{FBk}_{\mathrm{SF1,2}}}+\sum_{f\in F_{\mathrm{I4}}|\mathrm{FBk}_{\mathrm{SF1,2}}} W_{f|\mathrm{FBk}_{\mathrm{SF1,2}}}}\right)$$

(where $G_{\mathrm{I4}}|\mathrm{FB1}_{\mathrm{SF1,2}} = \{\mathrm{I4}\}$, $F_{\mathrm{I4}}|\mathrm{FB1}_{\mathrm{SF1,2}} = \{\mathrm{I3}\}$, $G_{\mathrm{I4}}|\mathrm{FB2}_{\mathrm{SF1,2}} = \{\mathrm{I4}\}$, $F_{\mathrm{I4}}|\mathrm{FB2}_{\mathrm{SF1,2}} = \{0\}$)

$$= W_{\mathrm{FB1}_{\mathrm{SF1,2}}}\frac{\sum_{g\in\{\mathrm{I4}\}} W_{g|\mathrm{FB1}_{\mathrm{SF1,2}}}}{\sum_{g\in\{\mathrm{I4}\}} W_{g|\mathrm{FB1}_{\mathrm{SF1,2}}}+\sum_{f\in\{\mathrm{I3}\}} W_{f|\mathrm{FB1}_{\mathrm{SF1,2}}}} + W_{\mathrm{FB2}_{\mathrm{SF1,2}}}\frac{\sum_{g\in\{\mathrm{I4}\}} W_{g|\mathrm{FB1}_{\mathrm{SF1,2}}}}{\sum_{g\in\{\mathrm{I4}\}} W_{g|\mathrm{FB1}_{\mathrm{SF1,2}}}+\sum_{f\in\{0\}} W_{f|\mathrm{FB1}_{\mathrm{SF1,2}}}}$$

$$= 0.7\frac{0.2}{0.2+0.8} + 0.3\frac{1}{1+0} = 0.44$$

Regarding the second step of SF, decision, there is no specific weight assignment, and the importance of a controller ($\mathrm{IM}^{\mathrm{DEC}}_{\mathrm{Cn|SF\,i,j}}$) related to a SF i, j can simply be defined as below.

$$\mathrm{IM}^{\mathrm{DEC}}_{\mathrm{Cn|SF\,i,j}} = 1\ (n = j) \qquad \text{(Eq. 3)}$$

Throughout the methodology, a conservative assumption that when a problem occurs within a particular component, the component cannot perform any of the required functions is applied. Throughout the methodology, it is presupposed that there is only one controller in one SF, and the only controller decides whether to generate a CA. In addition, a conservative assumption that when a problem occurs within a particular component, the component cannot perform any of the required functions is applied. Therefore, if there is a problem with the controller j the CA i cannot be generated, which means complete failure of decision in a SF.

Even if instrumentation and decision have been performed well, a PC may not be accomplished if some problems occur in control step. The ultimate purpose of control step is the operation of the relevant actuators. There may be specific system designs to secure the control step such as placing multiple actuators from the redundancy concept or adopting a different type of actuator from the diversity concept. In other words, an I&C system may be equipped with more than the minimum necessary actuators for control step. Therefore, the completion of the control step means the activation of the minimum relevant actuators to achieve the goal from a PC perspective. In this regard, the weights are assigned to the actuators; First, all MCS of actuators in SF i,j ($\text{MCSz}_{\text{SF i,j}}$) that cause control step failure is derived, and then a weight is assigned to each actuator to be the sum of the weights of the actuators that make up each MCS is 1. In Fig. 3, although details are not specified, it is assumed that either A1 or A2 and A3 must be activated for control rod drop; Therefore, the MCS of SF1,2 can be defined as $\text{MCS1}_{\text{SF 1,2}}$ = {A1, A2} and $\text{MCS2}_{\text{SF 1,2}}$ = {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, and the single actuator, A3, in MCS2 is assigned with a weight of 1: $W_{\text{A1}_{\text{SF1,2}}} = W_{\text{A2}_{\text{SF1,2}}} = 0.5, W_{\text{A3}_{\text{SF1,2}}} = 1$

$$W_{\text{Ay}_{\text{SF i,j}}} = \frac{1}{m}$$

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

Based on the weight assignments to the actuators, the IM of an interface ($\text{IM}^{\text{CTL}}_{\text{In|SF i,j}}$) or an actuator ($\text{IM}^{\text{CTL}}_{\text{An|SF i,j}}$) in SF i, j from the control perspective can be calculated. The underlying principle is similar to the one for importance calculation of sensor and interfaces from the instrumentation perspective. The importance of an interface or actuator corresponds with the degree to which the soundness of control step (CA i transmission/execution) is degraded due to that unavailable component. The closer the value to 1, the more likely the failure of that component will result in a complete loss of control step. However, the calculation process is very different from the instrumentation step because there is a disparate between the instrumentation step that transfers multiple FBs to a single controller and the control step that transfers a single CA to multiple actuators.

Depending on the system design, there may be a number of MCS of 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 MCS other than the most impacted MCS are ignored, so the sum of the impacts on all MCSs may be presented as a reference indicator.

$$\text{IM}^{\text{CTL}}_{\text{In|SF i,j}} = \max\{M_{\text{ln|SF i,j}}(z) : z = 1..\gamma\}$$

where γ is the number of MCS in SF i,j

$$M_{\text{ln|SF i,j}}(z) = \frac{\sum_{g\in G_{\text{In}}|\text{MCSz}_{\text{SF i,j}}} W_{g_{\text{SF i,j}}}}{\sum_{g\in G_{\text{In}}|\text{MCSz}_{\text{SF i,j}}} W_{g_{\text{SF i,j}}} + \sum_{f\in F_{\text{In}}|\text{MCSz}_{\text{SF i,j}}} W_{f_{\text{SF i,j}}}} \quad \text{(Eq. 4)}$$

where $G_{\text{In}}|\text{MCSz}_{\text{SF i,j}}$: A group of actuators receiving CA i via the interface n in the MCSz in SF i, j

where $F_{\text{In}}|\text{MCSz}_{\text{SF i,j}}$: A group of actuators receiving CA i other than the interface n in the MCSz in SF i, j

The IM for an actuator is straightforward like the one for sensors. The importance of each component in the control step is how much of a negative impact it has on PC accomplishment when the component is unavailable. The weight assigned to an actuator corresponds to the importance of that actuator since the weight is assigned from the perspective of PC accomplishment.

$$\text{IM}^{\text{CTL}}_{\text{An|SF i,j}} = W_{\text{Ay}_{\text{SF i,j}}} \ (n = y) \qquad \text{(Eq. 5)}$$

Regarding the SF1,2 given in Fig. 3, the importance of control related components can be calculated like below.

$$\text{MCS1}_{\text{SF 1,2}} = \{\text{A1}, \text{A2}\}, \text{MCS2}_{\text{SF 1,2}} = \{\text{A3}\}$$

$$M_{\text{l3|SF 1,2}}(1) = \frac{\sum_{g\in G_{\text{I3}}|\text{MCS1}_{\text{SF 1,2}}} W_{g_{\text{SF i,j}}}}{\sum_{g\in G_{\text{I3}}|\text{MCS1}_{\text{SF 1,2}}} W_{g_{\text{SF i,j}}} + \sum_{f\in F_{\text{I3}}|\text{MCS1}_{\text{SF 1,2}}} W_{f_{\text{SF i,j}}}}$$

(where $G_{\text{I3}}|\text{MCS1}_{\text{SF1,2}} = \{\text{A1}, \text{A2}\}$, $F_{\text{I3}}|\text{MCS1}_{\text{SF1,2}} = \{0\}$)

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

$$M_{\text{l3|SF 1,2}}(2) = \frac{\sum_{g\in G_{\text{I3}}|\text{MCS2}_{\text{SF 1,2}}} W_{g_{\text{SF i,j}}}}{\sum_{g\in G_{\text{I3}}|\text{MCS2}_{\text{SF 1,2}}} W_{g_{\text{SF i,j}}} + \sum_{f\in F_{\text{I3}}|\text{MCS2}_{\text{SF 1,2}}} W_{f_{\text{SF i,j}}}}$$

(where $G_{\text{I3}}|\text{MCS2}_{\text{SF1,2}} = \{\text{A3}\}$, $F_{\text{I3}}|\text{MCS2}_{\text{SF1,2}} = \{0\}$)

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

$$\text{IM}^{\text{CTL}}_{\text{I3|SF 1,2}} = \max\{M_{\text{l3|SF 1,2}}(1), M_{\text{l3|SF 1,2}}(2)\} = 1$$

$$M_{\text{l5|SF 1,2}}(1) = \frac{\sum_{g\in G_{\text{I5}}|\text{MCS1}_{\text{SF 1,2}}} W_{g_{\text{SF i,j}}}}{\sum_{g\in G_{\text{I5}}|\text{MCS1}_{\text{SF 1,2}}} W_{g_{\text{SF i,j}}} + \sum_{f\in F_{\text{I5}}|\text{MCS1}_{\text{SF 1,2}}} W_{f_{\text{SF i,j}}}}$$

(where $G_{\text{I5}}|\text{MCS1}_{\text{SF1,2}} = \{\text{A1}, \text{A2}\}$, $F_{\text{I5}}|\text{MCS1}_{\text{SF1,2}} = \{\text{A2}\}$)

$$= \frac{\sum_{g\in\{\text{A1,A2}\}} W_{g_{\text{SF i,j}}}}{\sum_{g\in\{\text{A1,A2}\}} W_{g_{\text{SF i,j}}} + \sum_{f\in\{\text{A2}\}} W_{f_{\text{SF i,j}}}} = \frac{(0.5+0.5)}{(0.5+0.5)+0.5} = 0.67$$

$$M_{\text{l5|SF 1,2}}(2) = \frac{\sum_{g\in G_{\text{I5}}|\text{MCS2}_{\text{SF 1,2}}} W_{g_{\text{SF i,j}}}}{\sum_{g\in G_{\text{I5}}|\text{MCS2}_{\text{SF 1,2}}} W_{g_{\text{SF i,j}}} + \sum_{f\in F_{\text{I5}}|\text{MCS2}_{\text{SF 1,2}}} W_{f_{\text{SF i,j}}}}$$

(where $G_{\text{I5}}|\text{MCS2}_{\text{SF1,2}} = \{\text{A3}\}$, $F_{\text{I5}}|\text{MCS2}_{\text{SF1,2}} = \{\text{A3}\}$)

$$= \frac{\sum_{g\in\{\text{A3}\}} W_{g_{\text{SF i,j}}}}{\sum_{g\in\{\text{A3}\}} W_{g_{\text{SF i,j}}} + \sum_{f\in\{\text{A3}\}} W_{f_{\text{SF i,j}}}} = \frac{1}{1+1} = 0.5$$

$$\text{IM}^{\text{CTL}}_{\text{I5|SF 1,2}} = \max\{M_{\text{l5|SF 1,2}}(1), M_{\text{l5|SF 1,2}}(2)\} = 0.67$$

$$M_{\text{l6|SF 1,2}}(1) = \frac{\sum_{g\in G_{\text{I6}}|\text{MCS1}_{\text{SF 1,2}}} W_{g_{\text{SF i,j}}}}{\sum_{g\in G_{\text{I6}}|\text{MCS1}_{\text{SF 1,2}}} W_{g_{\text{SF i,j}}} + \sum_{f\in F_{\text{I6}}|\text{MCS1}_{\text{SF 1,2}}} W_{f_{\text{SF i,j}}}}$$

(where $G_{\text{I6}}|\text{MCS1}_{\text{SF1,2}} = \{\text{A2}\}$, $F_{\text{I6}}|\text{MCS1}_{\text{SF1,2}} = \{\text{A1}, \text{A2}\}$)

$$= \frac{\sum_{g\in\{\text{A2}\}} W_{g_{\text{SF i,j}}}}{\sum_{g\in\{\text{A2}\}} W_{g_{\text{SF i,j}}} + \sum_{f\in\{\text{A1,A2}\}} W_{f_{\text{SF i,j}}}} = \frac{0.5}{0.5+(0.5+0.5)} = 0.33$$

$$M_{\text{l6|SF 1,2}}(2) = \frac{\sum_{g\in G_{\text{I6}}|\text{MCS2}_{\text{SF 1,2}}} W_{g_{\text{SF i,j}}}}{\sum_{g\in G_{\text{I6}}|\text{MCS2}_{\text{SF 1,2}}} W_{g_{\text{SF i,j}}} + \sum_{f\in F_{\text{I6}}|\text{MCS2}_{\text{SF 1,2}}} W_{f_{\text{SF i,j}}}}$$

(where $G_{\text{I6}}|\text{MCS2}_{\text{SF1,2}} = \{\text{A3}\}$, $F_{\text{I6}}|\text{MCS2}_{\text{SF1,2}} = \{\text{A3}\}$)

$$= \frac{\sum_{g\in\{\text{A3}\}} W_{g_{\text{SF i,j}}}}{\sum_{g\in\{\text{A3}\}} W_{g_{\text{SF i,j}}} + \sum_{f\in\{\text{A3}\}} W_{f_{\text{SF i,j}}}} = \frac{1}{1+1} = 0.5$$

$$\text{IM}^{\text{CTL}}_{\text{I3|SF 1,2}} = \max\{M_{\text{l5|SF 1,2}}(1), M_{\text{l5|SF 1,2}}(2)\} = 0.5$$

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

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

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

After deriving the importance of each component for each instrumentation, decision, control step for every SF i,j, the subtotal importance for each component for a given mission x can be calculated like equations 6 - 9, according to its type. In the equations, a, b, and c represent the total number of PCs, CAs, and controllers, respectively.

$$\mathrm{IM}_{\mathrm{Sn|Mx}} = \sum_{y=1}^{a}\sum_{i=1}^{b}\sum_{j=1}^{c} \mathrm{W}_{\mathrm{PCy}}\left\{\mathrm{W}_{\mathrm{CAi}}(\mathrm{W}_{\mathrm{SF}_{\mathrm{i,j}}} \cdot \mathrm{IM}^{\mathrm{INS}}_{\mathrm{Sn|SF\,i,j}})\right\} \quad \text{(Eq. 6)}$$

$$\mathrm{IM}_{\mathrm{Cn|Mx}} = \sum_{y=1}^{a}\sum_{i=1}^{b}\sum_{j=1}^{c} \mathrm{W}_{\mathrm{PCy}}\left\{\mathrm{W}_{\mathrm{CAi}}(\mathrm{W}_{\mathrm{SF}_{\mathrm{i,j}}} \cdot \mathrm{IM}^{\mathrm{DEC}}_{\mathrm{Cn|SF\,i,j}})\right\} \quad \text{(Eq. 7)}$$

$$\mathrm{IM}_{\mathrm{An|Mx}} = \sum_{y=1}^{a}\sum_{i=1}^{b}\sum_{j=1}^{c} \mathrm{W}_{\mathrm{PCy}}\left\{\mathrm{W}_{\mathrm{CAi}}(\mathrm{W}_{\mathrm{SF}_{\mathrm{i,j}}} \cdot \mathrm{IM}^{\mathrm{CTL}}_{\mathrm{An|SF\,i,j}})\right\} \quad \text{(Eq. 8)}$$

$$\mathrm{IM}_{\mathrm{In|Mx}} = \sum_{y=1}^{a}\sum_{i=1}^{b}\sum_{j=1}^{c} \mathrm{W}_{\mathrm{PCy}}\left[\mathrm{W}_{\mathrm{CAi}}\left\{\mathrm{W}_{\mathrm{SF}_{\mathrm{i,j}}}(\mathrm{IM}^{\mathrm{INS}}_{\mathrm{In|SF\,i,j}} + \mathrm{IM}^{\mathrm{CTL}}_{\mathrm{In|SF\,i,j}})\right\}\right] \quad \text{(Eq. 9)}$$

By adding the subtotal importance of each component derived for each mission throughout the entire missions, the final importance of each component can be derived like equations 10 - 13. The maximum value of each component can vary depending on the system design characteristics and cannot specify its upper bound. Therefore, the relative importance of each component can be analyzed for now, which will be re-considered in near future.

$$\mathrm{IM}_{\mathrm{Sn}} = \sum_{\mathrm{X}=1}^{\mathrm{T}} \mathrm{IM}_{\mathrm{Sn|Mx}} \quad \text{(Eq. 10)}$$

$$\mathrm{IM}_{\mathrm{Cn}} = \sum_{\mathrm{X}=1}^{\mathrm{T}} \mathrm{IM}_{\mathrm{Cn|Mx}} \quad \text{(Eq. 11)}$$

$$\mathrm{IM}_{\mathrm{An}} = \sum_{\mathrm{X}=1}^{\mathrm{T}} \mathrm{IM}_{\mathrm{An|Mx}} \quad \text{(Eq. 12)}$$

$$\mathrm{IM}_{\mathrm{In}} = \sum_{\mathrm{X}=1}^{\mathrm{T}} \mathrm{IM}_{\mathrm{In|Mx}} \quad \text{(Eq. 13)}$$

3. Discussion and Conclusions

In this paper, the authors propose a methodology to evaluate the quantitative importance of components for control systems where reasonable failure data of components is difficult to obtain. Based on the analysis results according to the proposed methodology, the safety of the control system might be achieved by modifying the system design to do not concentrate the importance on a small number of components, or by forcing the implementation of high reliability for certain components with high importance. However, it is necessary to consider the following prerequisites and precautions in utilizing this methodology

- It is assumed that signals (FBs or CAs) do not deteriorate or changed in the process of transmission.
- It is assumed that one CA is created by only one controller.
- The results of this analysis may vary dependingon the assigned weights. Therefore, a method for objective and systematic weighting needs to be further considered.
- The appropriateness of the level of detail of the component and the balance of the components in it should be considered.
- 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.

REFERENCES

[1] N.G. Leveson, “Engineering a safer world: systems thinking applied to safety” MIT Press, Cambridge, MA, USA, 2011

[2] N.G. Leveson, “A new accident model for engineering safer systems” Safety Science., Vol, 42 (4), p. 237-270, 2004

[3] .G. Leveson and J. Thomas, “STPA Handbook”, 2018

[4] A. Abdulkhaleq, S. Wagner, and N. Leveson “A comprehensive safety engineering approach for software-intensive systems based on STPA” Procedia Engineering, Vol. 128, p. 2-11, 2015

[5] Y. Lu, S.G. Zhang, P. Tang, and L. Gong, “STAMP-based safety control approach for flight testing of a low-cost unmanned subscale blended-wing-body demonstrator” Safety Science, Vol. 74, p. 102-113, 2015

[6] C.K. Allison, K.M. Revell, R. Sears, and N.A. Stanton, “Systems Theoretic Accident Model and Process (STAMP) safety modelling applied to an aircraft rapid decompression event” Safety Science, Vol. 98, pp. 159-166, 2017

[7]Faiella, A. Parand, B.D. Franklin, P. Chana, M. Cesarelli, N.A. Stanton, and N. Sevdalis, “Expanding healthcare failure mode and effect analysis: A composite proactive risk analysis approach” Reliability Engineering and System Safety, Vol. 169, p. 117-126, 2018

[8] G.J.M. Read, A. Naweed, and P.M. Salmon, “Complexity on the rails: A systems-based approach to understanding safety management in rail transport” Reliability Engineering and System Safety, Vol. 188, p. 352-365, 2019