A Method to Obtain Accident Sequences of Complex Systems

TAKEHISA KOHDA\(^1\) and KOICHI INOUE\(^2\)

\(^1\)Dept. of Aeronautics and Astronautics
Graduate School of Engineering, Kyoto University
Yoshida-Honnachi, Sakyo-ku, Kyoto 606-8501, Japan

\(^2\)Dept. of Entrepreneur Engineering
Graduate School of Engineering, Osaka Sangyo University
3-1-1 Nakagaichi, Daito, Osaka 574-8530, Japan

(Received on Sept. 29, 2004)

Abstract: Based on a system accident model where an accident occurs due to the loss of safety control actions, this paper proposes a simple method to obtain accident conditions of a complex system with interactions among human, software and hardware. For the accident to occur, two fundamental conditions are necessary: (1) a disturbance path can cause a deviation leading to the system accident, and (2) safety control actions related to the disturbance path fail to prevent or mitigate it. To obtain these failure conditions objectively, the proposed method utilizes a global system model, which clearly shows the relations between the physical behavior and safety control actions. While a formal approach using bond graphs is applied to the analysis of physical behaviour, information flow analysis is applied to safety control actions including operator actions such as monitoring and diagnosis. As long as the design assumptions and the evaluation of the safety control actions are correct, the consistency of accident conditions is guaranteed.

Key Words - system failure occurrence, system accident model, physical behaviour, safety control actions, information flow model

1. Introduction

To prevent and mitigate a system failure or system accident, various safety control actions are installed in complex technological systems such as chemical plants and nuclear plants [1]. Safety control actions in this paper mean a wide range of actions such as the system design modification, the addition of protective/shutdown systems, and inspection/maintenance operations by human operators. They can be also considered as a kind of control action composed of monitoring, decision making, and performing actions. From this viewpoint, the system failure or accident can be considered as a result of loss of safety control actions [2]. Further from the viewpoint of socio-technical systems, the organizational effect affecting the operational level (or the blunt end) of the subject system must be considered for the prevention of system accidents [3]. This paper focuses on the operational level (the sharp end), where the system accident occurs as an

* Corresponding author Email: kohda@kuaero.kyoto-u.ac.jp
observable deviation of the system physical behavior, where human, software and hardware interact one another to perform the system function.

Conventional probabilistic risk assessment (PRA) [4] identifies all possible hazards firstly and filters them, obtains event sequences to end-states from the initiation of each selected hazard using event tree analysis (ETA), and finally evaluates their probability/frequency and consequences based on the quantitative information given from fault tree analysis (FTA) [5]. To analyze system failure conditions, a fault tree (FT), a static logical relation between the system failure and component failure, is usually constructed based on the judgment and experience of system analysts. Some FT may yield an erroneous result or omit serious failure conditions. Further, in advanced systems such as autonomous robots, the sequence of component failures has a great effect on system failure. For the evaluation of system failure occurrence probability and the design of safety control actions, event sequence conditions leading to system failure (or accident sequence conditions) must be given. Thus, to obtain accident sequence conditions objectively, this paper proposes the use of a global system model.

The global system model is composed of two types of system behaviors. One is the physical behavior, which must satisfy the natural constraints, or obey physical laws such as Newton’s law for the dynamical behaviors. The other is a control action behavior, which can be constructed logically as expected. For modeling the physical behavior, bond graphs [6] are applied, because 1) they can model various systems such as mechanical, electrical, and hydraulic systems in a unified way from the viewpoint of energy flow, 2) the intuitive correspondence between bond graph elements (BGE’s) and physical behaviors/components makes it easy to construct a system physical behavior model based on the design assumptions, 3) their stepwise refinement allows easy model modifications and 4) the model itself can satisfy the physical constraints such as energy conservation. The bond graph is not only a well-established method, but also very useful and popular for control system applications such as model-based observer control [7], hybrid system control [8], and intelligent supervisory control [9].

For the control action behavior, the functional modeling approach [10] can be applied. For example, Multilevel Flow Modeling (MFM) [11] shows all goals and functions of complex industrial systems on a multiple interconnected level by using levels of means-ends and part-whole abstraction. One of MFM application areas is the diagnosis problem; MFM can be applied to three kinds of diagnosis: measurement validation, alarm analysis, and fault diagnosis [12]. Thus, the functional modeling approach can model any control action by identifying the designer-defined overall goal it must achieve and the designer/user-defined function it must perform. In this paper, the safety control actions are divided into three parts: monitoring, diagnosis (or decision making), and action parts. To obtain causal relations among these parts, this paper simplifies the functional model into the information flow model among these three parts by using a set of if-(condition)-then-(action) rules. To obtain accident conditions using the global system model, causal relations among physical behavior and safety control actions must be specified. This information is represented as the effect of a safety control action on deviations of process variables.

For the application of process system models to accident sequence analysis, the extensive studies have been done in the field of “dynamic reliability analysis” such as [13-15]. They simulate the detailed model of system dynamics, which corresponds to a
physical behaviour model in the proposed method, and also utilize Markov modelling approach to represent stochastic behaviours such as component failure. By adjusting the parameters in the system model, various accident conditions can be simulated. More informative analysis results are obtained than the conventional ETA/FTA approach. The dynamic reliability analysis is regarded as a kind of simulation-based analysis, while the proposed method is an analytical method based on the qualitative knowledge of component failure mechanism and applied at the early design stage. When the detailed quantitative information is given, the analysis result obtained by the proposed method can be confirmed using dynamic simulations.

Firstly, a system accident model is given to explain the overall analysis procedure. Then, the global system model is introduced, and how to obtain the accident sequence conditions using it is given. A simple illustrative example shows the overall process of the proposed method briefly.

2. Accident Sequence Analysis

2.1 System Accident Model

The technological system has various control systems to maintain the system state within the acceptable range. Under its normal condition, the system state is maintained within the desirable range by the ordinary control system. If the system is out of the acceptable range due to an external disturbance or malfunction of control systems, protective actions or emergency actions are taken to mitigate its effect. So, the fundamental scenario of a system accident is that an initiating event leads to a system accident through holes (or faults) of control actions and protective actions as shown by Reason’s Swiss Cheese Model [16].

According to this basic mechanism, the first step is the identification of a possible initiating event (or disturbance path) causing a specific system fault or accident state. For each disturbance path, its related safety control actions are examined to see whether they can prevent/mitigate it. Then, the logical AND combination of a disturbance path condition with failure conditions of effective safety control actions gives accident conditions. Examining the sequence dependency between disturbance path and safety control action failure, the accident sequence conditions can be obtained.

2.2 Analysis Procedure

An analysis procedure proposed in this paper is summarized as:

(0) Develop a global system model based on the design assumptions.

(1) Obtain all potential disturbance paths leading to a specific accident state using the causal tree obtained from the global system model.

(2) For each potential disturbance path, take the following steps to derive the accident sequence condition.

(2-0) Evaluate its occurrence probability.

(a) If its probability is acceptable (or very low), consider another potential disturbance path.
(b) Otherwise, evaluate the effectiveness of its related safety actions at step (2-1)

(2-1) Identify safety control actions related to the potential disturbance path and evaluate their effectiveness to obtain system failure condition.

(a) If some safety actions can prevent/mitigate the disturbance path, the accident condition is the disturbance path condition combined with their failure condition.

(b) Otherwise, the accident condition is the disturbance path condition.

(2-2) Obtain accident sequences by considering event dependency and latency.

Compared with a standard design procedure of safety related systems such as IEC61508 [17], and LOPA [1], steps (1) & (2-0) correspond to the risk evaluation without protective systems, while steps (2-1 & 2) correspond to the part of evaluation of the residual risk with protective systems. As a specific system failure is specified at step (1), the risk can be evaluated in terms of the occurrence probability of a potential disturbance path (or accident condition) in the proposed method. Steps (1) & (2-1) correspond to the derivation of system failure conditions in FTA. Since 1) the effectiveness of safety control actions depends on their environmental conditions and 2) the consideration of all possible environmental conditions is too complex to analyze beforehand, it is difficult to derive their failure condition automatically. To solve these problems, the proposed method utilizes the system analysts’ judgments in evaluating the effectiveness of safety control actions. This interactive process can also help the system analysts confirm the function of safety control actions.

2.3 Global System Model

In the safety/reliability design, design assumptions can be divided into two types: normal and failure conditions. The global system model is composed of three types of system behaviours: 1) normal physical one, which must satisfy the natural constraints, or physical laws such as Newton’s law for the dynamical behavior, 2) safety control actions such as control and protective actions, and 3) failure assumptions which represent the effect of component failure or external disturbances to be considered in the design.

2.3.1 Physical Behaviour Model

For modelling the physical behaviour, bond graphs are applied. Table 1 shows the correspondence between bond graph elements (BGE’s) and physical behaviours/components. Note that 0 (zero-junction) and 1 (one-junction) satisfy the energy conservation, corresponding to series and parallel circuits, respectively. General variables “effort” (e) and “flow” (f) are commonly used whose product is power, common concept connecting these systems. The following assumption is made on the system bond graph (SBG):

A-1: The SBG is composed of basic BGE’s: source of effort (SE), source of flow (SF), resistor (R), capacitor (C), inertia (I), transformer (TF), gyrator (GY), zero-junction (0), and one-junction (1). The characteristic function for each BGE is shown in Table 2.
A Method to Obtain Accident Sequences of Complex Systems

Table 1: Correspondence between BG and Physical Systems

<table>
<thead>
<tr>
<th>BG</th>
<th>Electrical system</th>
<th>Hydraulic system</th>
<th>Mechanical system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bond</td>
<td>Electric wire</td>
<td>Pressure pipe</td>
<td>Shaft, Rod</td>
</tr>
<tr>
<td>Effort</td>
<td>Electric voltage</td>
<td>Pressure</td>
<td>Force, Torque</td>
</tr>
<tr>
<td>Flow</td>
<td>Electric current</td>
<td>Volume flow</td>
<td>Velocity</td>
</tr>
<tr>
<td>SE</td>
<td>Voltage source</td>
<td>Pump with pressure regulator</td>
<td>Diesel engine</td>
</tr>
<tr>
<td>SF</td>
<td>Current source</td>
<td>Hydrostatic pump</td>
<td>Driving shaft</td>
</tr>
<tr>
<td>R</td>
<td>Resistor</td>
<td>Restriction</td>
<td>Friction, Damper</td>
</tr>
<tr>
<td>C</td>
<td>Condenser accumulator</td>
<td>Hydraulic compliance</td>
<td>Spring</td>
</tr>
<tr>
<td>I</td>
<td>Inductor</td>
<td>Mass action, Fluid inertia</td>
<td>Mass, Inertia</td>
</tr>
<tr>
<td>TF</td>
<td>Electric transformer</td>
<td>Hydrostatic pump, Cylinder</td>
<td>Gear reducer</td>
</tr>
<tr>
<td>GY</td>
<td>Electric DC machine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Parallel circuit</td>
<td>Parallel circuit</td>
<td>Planetary gear</td>
</tr>
<tr>
<td>1</td>
<td>Serial circuit, Fixed reducer</td>
<td>Serial circuit</td>
<td>Lever type joint</td>
</tr>
</tbody>
</table>

Table 2: BGE and Characteristic Function

<table>
<thead>
<tr>
<th>BGE Symbol</th>
<th>Function</th>
<th>BGE Symbol</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SE → e_i</td>
<td>e_i = E(t)</td>
<td>TF → j f_j</td>
<td>e_j = e_i / n</td>
</tr>
<tr>
<td>SF → f_i</td>
<td>i f_i = i F(t)</td>
<td></td>
<td>f_j = n f_i</td>
</tr>
<tr>
<td>R → e_i</td>
<td>i e_i = i R(f_i)</td>
<td>GY → j f_j</td>
<td>f_j = e_i / m</td>
</tr>
<tr>
<td>R → f_i</td>
<td>i f_i = i R(e_i)</td>
<td></td>
<td>e_j = m f_i</td>
</tr>
<tr>
<td>C → e_i</td>
<td>e_i = C( ∫ e_i dt )</td>
<td>0 → 1</td>
<td>e_i = e_a for any jj, ik</td>
</tr>
<tr>
<td>I → f_i</td>
<td>i f_i = i L( ∫ e_i dt )</td>
<td>1 → 0</td>
<td>f_a = f_k for any jj, ik</td>
</tr>
</tbody>
</table>

For the SBG under assumption A-1, state variables are displacement (integral of flow with respect to time) of a bond connecting to a C-element and momentum (integral of effort with respect to time) of a bond connecting to an I-element, while input variables are effort of a bond connecting to an SE-element and flow of a bond connecting to an SF-element [6]. Based on the causality of the SBG, all efforts and flows can be expressed in functional form of state variables and input variables [18]. Here, a functional form is defined in such a way that y is represented as f(x) if variable y is given as variable x operated by function f. The functional form shows the causal relation between physical phenomena. From the definitions of displacement and momentum, the system state equations are obtained as:
where \( b(i) \) denotes bond corresponding to state variable \( X_i \).

The system state equations can give causal relations between component behaviours and system state variables clearly, which helps the system analyst understand the effect of component failure on the physical behaviour. The system equation can also give the dynamic system behaviour.

### 2.3.2 Safety Control Actions

For the evaluation of system end-states caused by a disturbance path, the effect of safety control actions must be considered. To perform its function, a safety control action must have the following functions: (1) the detection of a deviation due to a disturbance path, (2) the selection of an appropriate protective action, and (3) the performance of the specified protective action. Corresponding to these functions, the safety control system is generally divided into 3 parts: (1) monitoring one (or sensor), (2) diagnosis one (or controller), and (3) action one (or actuator). For example, in a computerized safety action, the computer corresponds to a controller. In some safety control action, some parts can be played by one component. A pressure relief valve can perform these three functions by itself. Its behaviour is represented as:

If the monitored pressure is larger than the preset pressure, then the relief valve is to be opened. Otherwise, the relief valve is to remain closed.

Similarly, well-trained human operator actions can be represented as a concatenation of monitoring and action parts. The operational manual and the emergency procedure are represented similarly in terms of If-(condition)-then-(action) rules. In an operator recovery action issued by an alarm system, the alarm corresponds to the monitoring part and human operators play the diagnosis and actions parts.

Thus, for representing a safety control action, the following information must be specified: (1) what kind of data from the controlled object the monitoring part collects, or what kind of data initiate the safety control action, (2) how the diagnosis part makes its decision, (3) what action the actuator performs to the controlled object. Thus, the behaviour of a safety control action can be represented as a kind of input-output sequence of information, i.e., information flow model.

### 2.3.3 Failure Assumptions

In the proposed method, component failures/disturbances are assumed as:

A-2: The effect of a failure is represented as either a deviation of process variable (external disturbance) or a deviation of component function (component failure).

Consider a hardware failure. The deviation of its normal characteristic function can appear as an increase/decrease of its output compared with its normal output. This assumption can be also applied to human errors, which can be represented as a deviation from the normal or standard action. The proposed method focuses on the observable result of human errors (the phenotypes), not the cause of human errors (the genotypes). For the detailed analysis and the prevention of human errors, the investigation of the genotypes is indispensable. However, since an accident sequence is a sequence of
observable events, the proposed method thinks more of the phenotype. After a severe phenotype or human error mode is identified, its genotypes or background factors can be investigated using cognitive engineering approach such as SHERPA (Systematic Human Error Reduction and Prediction Approach) [19] or CREAM (Cognitive Reliability and Error Analysis Method) [20].

For the derivation of accident conditions, all possible component failure, human errors and external disturbances must be defined in the global system model. Especially, a failure that cannot be expressed as a deviation of its characteristic function must be added to the SBG and information flow model appropriately. Consider a tank leakage. Since the tank can be represented as a C-element, the storage of flow in Table 1, the leakage failure may be considered as a deviation of its characteristic function. But, this representation requires that the tank capacity must be infinite, which is not appropriate because the corresponding physical condition is impractical. Instead, an R-element representing the loss of flow must be added to the SBG. Thus, the global system behaviour model must include not only normal behaviours, but also some possible failure behaviours.

2.3.4 Causal Tree
Based on the SBG with safety control actions and failure assumptions, the system state equations can be obtained. Since they do not show the causal relation between process variables clearly, a causal tree representing cause-effect (or input-output) relations in the entire system is given as follows [21]:
1. Based on the system state equations obtained from the SBG, the relation between system process variables such as pressure and flow can be represented as a tree graph, whose nodes and branches represent process variables in the SBG and cause-effect relations, respectively.
2. The input-output sequence of a safety control action on the controlled variables must be added to the above tree graph.

2.4 Derivation of Disturbance Path
The global system model can give a preliminary accident condition. Firstly, the system accident must be defined as a deviation of a process variable in the causal tree. For example, a tank explosion is represented as an overpressure (or a positive deviation of the pressure) in the tank. From the specified deviation in the causal tree, the backward search can obtain possible sequences of process variables leading to it, or disturbance paths. Disturbance paths can be classified into two types:
1. a deviation caused by an external disturbance such as a deviation of input energy,
2. a deviation caused by a component failure such as a malfunction of a negative feedback control system and spurious shutdown of a valve.

The backward search of a disturbance path stops when either of these conditions is satisfied. All possible sequences of nodes are searched over the causal tree to guarantee the completeness of disturbance paths.

2.5 Derivation of Accident Conditions
Generally speaking, the system has several kinds of protective systems and control systems [1], which can prevent some abnormal events or maintain the system state as desired. If a disturbance path occurs, some safety control actions can prevent it.
Depending on the effectiveness of safety control actions related to the disturbance path, the accident condition can be obtained as follows:

If one or more safety control actions can prevent the disturbance path, their failure conditions are necessary for the disturbance path to occur.

Otherwise, the disturbance path must be an accident by itself.

Firstly, safety control actions related to a disturbance path must be identified by examining whether their monitoring part can detect it. Secondly, for the evaluation of the effect of the related safety control actions, a kind of ETA must be performed by the system analysts with consideration of the functional dependency between the safety control actions. Then, the system accident condition is obtained as logical AND combination of a disturbance path condition and failure conditions of its effective safety control actions. In obtaining the failure condition of a safety control action, the decomposition of a safety action into monitoring part, diagnosis part and action part is useful. This decomposition can analyze the failure conditions of hardware protective/control system behaviours and operator actions in the same manner [22].

2.6 Derivation of Accident Sequence Conditions

The accident conditions obtained at the previous section does not consider the sequence of failure events. Further, the event sequence leading to the accident is not always equal to the corresponding event sequence represented by the corresponding ET. For example, if a system failure condition accompanies a protective system failure, the protective system failure must occur before the disturbance path occurs. Otherwise, the protective system can prevent the disturbance path. Thus, accident sequence conditions can be obtained by considering the event sequence constraint on safety control actions. The event sequence dependency between basic events can be considered for a minimal cut set for an accident scenario of ETA [23]. To obtain minimal cut sets with event sequence dependency effectively, a novel method using BDD [24] can be applied.

Further, it must be examined whether failure of each safety control action can be detected. If it can be detected, some maintenance action, or the overall system maintenance can be taken to nullify its effect. The detection of a safety control action failure implies that the system accident condition requiring its failure cannot occur. Thus, if a safety control action failure must occur before the disturbance path, its latency or failure of its detection must be considered [25].

3. Illustrative Example

Obtain accident sequence conditions of a separator as shown in Figure 1 below:

Figure 1: Separator
3.1 Development of Global System Model

3.1.1 System Description

Gas from the wellhead manifold is led into the first stage separator. The explosion of the separator due to the overpressure is the most severe accident to be considered. To prevent the separator explosion, three independent safety actions are installed in the system. On the inlet pipeline, a process shutdown (PSD) valve, PSD1, is installed. The valve is usually held open by hydraulic pressure. When the hydraulic pressure is bled off, the valve will close by the force of a pre-charged actuator. Another PSD valve of the same type, PSD2, is installed at the gas outlet to stop the gas flow. Due to the fail-safe design of PSD valves, these valves may close spuriously, i.e., without the presence of a hazardous situation. A pressure safety valve (PSV) is installed to relieve the pressure in the separator in case the pressure increases beyond a specified high pressure (p). The PSV is equipped with a spring-loaded actuator, which may be adjusted to p. The most critical failure mode for the PSV is “fail to open” (FTO); the valve does not open when the pressure in the separator increases beyond p. Three pressure sensors, PS1, PS2, & PS3 are installed in the separator. The PS1, PS2, and PS3 are preset to be activated at pressure p1, p2, and p3 (p1 < p2 < p), respectively. If PS1 is activated, then alarm PA1 is issued so that operators can notice it and do the recovery action. Further, if the pressure increases beyond p2, PS2 provides signal via the programmable logic controller PLC1 to close PSD1 and PS3 closes PSD2, similarly. This control loop constitutes an interlock system. Even if these two safety control actions unfortunately fail and the pressure increases, the PSV finally operates to prevent the separator explosion. Thus, any of these three safety control actions can prevent the separator explosion.

3.1.2 Physical Behaviour

Firstly, construct the physical behavior model based on the system description using bond graphs. According to correspondence between BGE’s and physical phenomena, the SBG can be obtained as shown in Figure 2. The SBG shows the basic relation between flow and pressure. Other behaviors such as thermal effect are neglected for simplicity. The gas inlet is represented as the pressure source SE1, the shutdown valve is simply modeled as an R-element R1 whose characteristic is determined by set-points p2 and pressure in the separator. Since the separator can be simplified as a kind of gas storage, it is represented as a C-element C1. The PSV is represented as an R-element R3 whose characteristic is also determined by set-point p and pressure in the separator. R2 denotes the shutdown valve of gas outlet.

![Figure 2: System Bond Graph for Separator](image-url)
According to the definition of system and input variables in the SBG, let $X_1$, $U_1$, and $U_2$ denote state variable for C1, input variables for SE1 and SE2, respectively. Using a simple symbolic manipulation method [18], all efforts and flows can be obtained as functional forms of $X_1$, $U_1$, and $U_2$ as shown in Table 3, where $R_1$, $R_2$, $R_3$, and $C_1$ represent characteristic functions for R1, R2, R3, and C1, respectively. The global system state equation is obtained as:

$$
\frac{dX}{dt} = R_1(U_1 - C_1(X_1)) - R_3(C_1(X_1)) - R_2(C_1(X_1) - U_2)
$$

(2)

<table>
<thead>
<tr>
<th>Effort i</th>
<th>Flow i</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 $U_1$</td>
<td>$R_1(U_1 - C_1(X_1))$</td>
</tr>
<tr>
<td>2 $U_1 - C_1(X_1)$</td>
<td>$R_1(U_1 - C_1(X_1))$</td>
</tr>
<tr>
<td>3 $C_1(X_1)$</td>
<td>$R_1(U_1 - C_1(X_1))$</td>
</tr>
<tr>
<td>4 $C_1(X_1)$</td>
<td>$R_1(U_1 - C_1(X_1)) - R_3(C_1(X_1) - R_2(C_1(X_1) - U_2)$</td>
</tr>
<tr>
<td>5 $C_1(X_1)$</td>
<td>$R_3(C_1(X_1) - U_2)$</td>
</tr>
<tr>
<td>6 $C_1(X_1)$</td>
<td>$R_2(C_1(X_1) - U_2)$</td>
</tr>
<tr>
<td>7 $C_1(X_1) - U_2$</td>
<td>$R_2(C_1(X_1) - U_2)$</td>
</tr>
<tr>
<td>8 $U_2$</td>
<td>$R_2(C_1(X_1) - U_2)$</td>
</tr>
</tbody>
</table>

Table 3: Functional Expression of Efforts and Flows

Based on the system description, characteristic functions of the SBG under normal condition are defined as:

(C1) Since PSD$_1$ closes when the pressure in the separator (effort of bond 4) is greater than set-point $p_2$, $R_1$ is represented as:

If $e_4 \leq p_2$, $R_1(*) > 0$. Otherwise, $R_1(*) = 0$

(C2) Similarly to PSD$_1$, $R_2$ is expressed as:

If $e_4 \leq p_2$, $R_2(*) > 0$. Otherwise, $R_2(*) = 0$.

(C3) Since PSV opens when the monitored pressure in the separator is greater than set-point $p$, $R_2$ is represented as:

If $e_4 \leq p$, $R_3(*) > 0$. Otherwise, $R_3(*) = 0$.

(C4) Since the pressure in the separator is simplified as an increasing function of gas volume, $C_1$ is represented as:

If $x_1 \leq x_2$, $C_1(x_1) \leq C_1(x_2)$.

(C5) Since the manifold determines the input pressure, $U_1$ is fixed based on its property.

(C6) Since the outlet pressure is determined by the downstream process, $U_2$ is fixed.

### 3.1.3 Safety Control Actions

Four safety control actions are identified as follows:

(S1) (Operator recovery action) The monitoring part is PS$_1$ which monitors the pressure in the separator ($e_2$), and the relay circuit issues the alarm PA$_1$. Then the operator action corresponds to the diagnosis and action parts.
(S2) (Interlock system) The monitoring part is PS\textsubscript{2} which monitors the pressure in the separator (e\textsubscript{4}), the diagnosis part is PLC\textsubscript{1}, and the action part is PSD\textsubscript{1} corresponding to R\textsubscript{1} in the SBG.

(S3) The safety valve PSV fills all the roles of monitoring, diagnosis, and action parts by itself.

(S4) The monitoring part is PS\textsubscript{3} which monitors the pressure in the separator (e\textsubscript{4}), the diagnosis part is PLC\textsubscript{2}, the action part is PSD\textsubscript{2} corresponding to R\textsubscript{2} in the SBG.

3.1.4 Failure Assumptions

For simplicity, assume the following failures:

(F1) PSD\textsubscript{1}, PSD\textsubscript{2}: Spurious shutdown (SC): If e\textsubscript{4} ≤ p\textsubscript{2}, R\textsubscript{1}(*)=0, R\textsubscript{2}(*)=0.

Failure to close (FTC): If e\textsubscript{4} > p\textsubscript{2}, R\textsubscript{1}(*) >0, R\textsubscript{2}(*) >0.

(F2) PSV: Failure to open (FTO): If e\textsubscript{4} > p, R\textsubscript{3}(*)=0.

(F3) PA\textsubscript{1}: Failure to issue alarm (FIA): If e\textsubscript{4} > p\textsubscript{1}, the alarm is not issued.

These component failures are all represented as a deviation of their normal characteristic function. Additional bond graph elements to the SBG are not necessary in this case. Further, to make the following discussion easier, no human errors are assumed for the operator recovery actions.

3.2 Derivation of Disturbance Paths

The separator explosion corresponds to “overpressure in the separator”. In the SBG, the pressure in the separator corresponds to effort of bond 4 (e\textsubscript{4}). Obtain potential disturbance paths causing a positive deviation of e\textsubscript{4} using the causal tree obtained as shown in Figure 3, where broken lines show safety control actions.

Since e\textsubscript{4} is represented as C\textsubscript{1}(X\textsubscript{1}) as shown in Table 2, C\textsubscript{1}(*) or X\textsubscript{1} must increase for its positive deviation. According to the design assumption, C\textsubscript{1}(*), the capacity of the separator, does not change, and so state variable X\textsubscript{1} must increase. In other words, at the initiation of a disturbance path, dX\textsubscript{1}/dt>0 must hold. Since node “+” in the causal tree shows dX\textsubscript{1}/dt=R\textsubscript{1}(U\textsubscript{1}-C\textsubscript{1}(X\textsubscript{1}))-R\textsubscript{2}(C\textsubscript{1}(X\textsubscript{1}))-R\textsubscript{3}(C\textsubscript{1}(X\textsubscript{1}))-U\textsubscript{2}, three cases are possible:
1) output of $R_1$ increases, 2) output of $R_3$ decreases, and 3) output of $R_2$ decreases. Since $C_1(X_1)$ increases and input variable $U_1$ does not change, characteristic function $R_1$ must increase for case 1). Assumptions on $R_1$ do not satisfy this requirement. Thus, the case 1) is impossible. Similarly, the case 2) is not consistent with assumptions on PSV. Consider case 3). If the input $C_1(X_1)-U_2$ increases, the output of $R_2$ increases under its normal condition. But, if the SC of PSD$_2$ occurs, $R_2(*)=0$ implies the decrease of $R_2$. This sequence can become a disturbance path. Thus, SC of PSD$_2$ is obtained as the only possible disturbance path. This kind of backward search is done over the causal tree shown in Figure 3 using the design assumptions on normal and failure behaviors.

3.3 Derivation of System Accident Conditions

In this system, the fail-safe design of PSD$_2$ cannot prevent the occurrence of its spurious shutdown. In other words, the occurrence probability of SC of PSD$_2$ cannot be neglected. Thus, the effectiveness of safety control actions must be evaluated.

Consider which safety control action can detect the disturbance path. The design assumptions on safety control actions ((S1)-(S4)) show that the operator recovery, the interlock system, and the PSV can respond to the pressure increase in the separator, sequentially. Since these safety control actions are independent, the effect of spurious shutdown can be prevented by any of safety control actions (S1), (S2) and (S3). Thus, the system accident condition is obtained as logical AND combination of [Spurious shutdown of PSD$_2$], [Recovery action failure], [Interlock system failure], and [Safety valve failure]. Based on failure assumptions (F1), (F2), and (F3), the recovery action failure occurs due to FIA of PA$_1$, the interlock system failure occurs due to FTC of PSD$_1$, and the safety valve failure occurs due to FTO of PSV. Thus, the accident condition is obtained as:

$$\{\text{SC of PSD}_2, \text{FIA of PA}_1, \text{FTC of PSD}_1, \text{FTO of PSV}\}$$

3.4 Derivation of Accident Sequence Conditions

If at least one of safety control actions (S1), (S2) and (S3) is normal, the explosion due to SC of PSD$_2$ can be prevented. Thus, the corresponding failure to each safety control action failure must occur before SC of PSD$_2$. Further, PA$_1$, PSD$_1$ and PSV remain in the same state as their normal one when their corresponding failures occur, and thus these failures are latent. The recovery action is not possible for each safety control action. Thus, the accident sequence condition is obtained as:

$$\{\text{SC of PSD}_2 \text{ occurs after FIA of PA}_1, \text{FTC of PSD}_1 \text{ and FTO of PSV occur}\}.$$  

The effectiveness of these safety control actions can be evaluated based on the accident sequence probability of this scenario compared with the accident probability without safety control actions. If the reduced accident sequence probability cannot be accepted, some further improvement must be considered at step (2-2).

4. Conclusions

Based on the system accident model, this paper proposes a framework for the derivation of accident sequence conditions using the global system model composed of physical behavior, safety control actions, and failure assumptions. The accident conditions are obtained as logical AND combination of 1) a disturbance path condition and 2) failure
conditions of the effective safety control actions. A disturbance path can be obtained using the causal tree based on the global system model. The effective safety control actions are checked by the system analysts for each disturbance path. This interactive process can confirm the completeness of the overall safety control actions. Failure conditions of each safety control action can be obtained using its decomposition into monitoring, diagnosis, and action parts. Due to this composition, the role of human operators can be recognized clearly in safety control actions. A specific human error analysis can be also performed depending on the role of operators.

To obtain accident sequence conditions, the proposed method utilizes the sequence dependency between disturbance path and safety control action failure. For the detailed analysis of sequence dependency, the inspection and maintenance of safety control actions must be considered, which are related to the boundary conditions of the entire analysis. Since one of our research objects is the development of an interactive safety design support system, the proposed procedure must be consistent with the conventional procedure of risk-based design: identification of hazard, identification of effective safety measures, derivation of accident scenarios and their risk evaluation. Since this paper is the first step toward our object, the details of each process must be improved further for the practical application.

Acknowledgement

The authors deeply appreciate the valuable comments and suggestions made by the editor-in-chief and anonymous reviewers.

References


Takehisa Kohda is now an Associate Professor of Kyoto University, Japan. His interests lie in the systems safety and reliability, risk analysis, systems analysis, and so on.

Koichi Inoue is now a Professor Emeritus of Kyoto University and a Guest Professor at Osaka Sangyo University, Japan. His fields of interest include systems reliability and safety, system optimization, risk analysis, human interface, neural networks, and UAV control.