This article is part of the IEEE Reliability Society 2008 Annual Technology Report.

Risk Analysis of Phased-Mission Systems with Multiple Failure Modes

Takehisa Kohda
Kyoto University
Email: kohda@kuaero.kyoto-u.ac.jp

Summary and Conclusions
General systems such as production plants and aircrafts can be regarded as a phased-mission system, which perform several different functions depending on their operation stage. This paper proposes a novel, simple and practical risk analysis method of phased mission systems with multiple failure modes. Firstly, based on the physical definition of a system accident, system accident occurrence conditions at each phase are obtained in terms of component state conditions at start/end of a phase. Evaluating component state conditions, the system accident occurrence probability can be easily evaluated. An illustrative example of a batch process in the chemical reactor shows the merits and details of the proposed method.

Introduction
In the batch operation of chemical plants, one processing unit such as a reactor performs several tasks sequentially according to the unit processing requirements. Similarly, general systems perform different functions depending on their operation stage. From the viewpoint of reliability, the system must be regarded as a phased mission system [1], whose functional relation among components changes depending on the operation stage. Further, definition of failure for a component also changes depending on its operation stage. The conventional binary state representation such as failure/success states [2] cannot be effective. Due to this property, the occurrence of a hazard in the system depends on the operation stage as well as the total operation time. This kind of operation characteristics is not limited to chemical plants, but also applicable to the general system including production plants and transportation systems such as airplanes. Thus, the phased-mission analysis approach must be applied with consideration of multiple failure modes for a component as well as the system.

Problem Statement
In applying logical approaches such as basic event transformation [3] or sophisticated methods such as Markov chains [4] and Petri-Nets [5] to the evaluation of mission reliability of a phased-mission system, the system success/failure conditions at each phase must be given for each phase. However, the system accident conditions or minimal cut sets for the phased mission system cannot be obtained easily, because normal component condition changes depending on the processing stage and so multiple failure modes must be considered. The first step in the risk analysis of a batch processes is the identification of system accident conditions at each phase. This corresponds to a kind of fault tree construction [6].

This paper proposes a step-by-step procedure from the definition of system accidents to the derivation of accident occurrence conditions. A simple component state representation and its probability evaluation are also introduced to evaluate the system accident occurrence probability. The proposed method is explained using a simple batch system described in next chapter.

A Simple Batch System
Consider a simple batch process in Figure 1. A chemical reaction of materials A and B occurs in the reactor vessel to produce material C. Since the chemical reaction is exothermic and a runaway reaction can occurs at a high temperature, the temperature must be controlled to maintain the reaction process safe. The batch process consists of the following 6 phases:

Phase 1. Standby: The system waits for the start of operation.
Phase 2. Feed of material A: Through valve V1, material A comes into the reactor vessel.
Phase 3. Feed of material B: Through valve V2, material B comes into the reactor vessel mixed with material A.
Phase 4. Heat-up: To initiate the chemical reaction, the temperature of reactor vessel is increased by the external steam flow.
Phase 5. Chemical reaction: To maintain the appropriate temperature for the reaction, the reactor vessel is cooled by the external cooling water flow.
Phase 6. Purge: After the completion of the reaction, the product of material C is delivered to the down-ward processes.

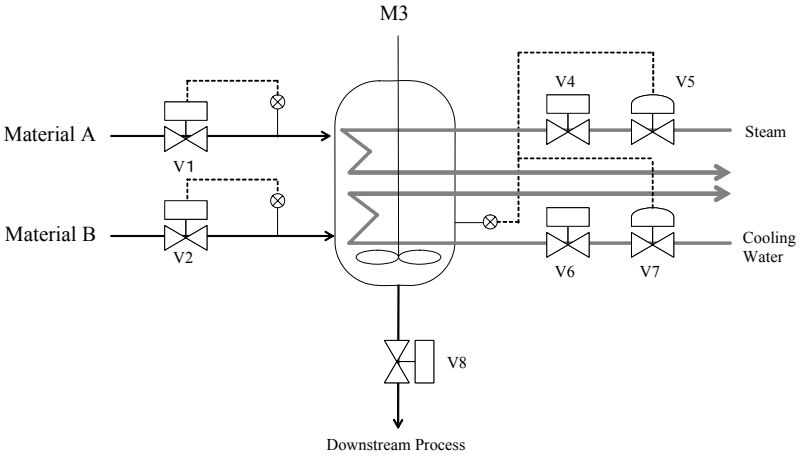

Figure 1. A Simple Batch System

Table 1 Operation conditions of valves and mixer

Phase	V1	V2	M3	V4	V5	V6	V7	V8
1	C	C	S	C	C	C	C	C
2	O	C	R	C	C	C	C	C
3	C	O	R	C	C	C	C	C
4	C	C	R	O	A	C	C	C
5	C	C	R	C	C	O	A	C
6	C	C	S	C	C	O	C	O

Notes: For valve (V), C: closed state, O: open state A: state adjusted by controller
For mixer (M), S: stopping state R: running state

The batch process repeats this sequence several times to produce a desired amount of material C. The operation conditions of valves and mechanical mixer for each phase are shown in Table 1.

Consider the effect of a component failure on the batch process. For example, closure failure of valve V1 does not cause any damage to the system at the first phase (standby), because the required state for V1 is the same as the state caused by its failure. But it causes a serious damage at the second phase (feed of material A), because the mixer runs without material A, breaking the reactor vessel, which is a kind of system accidents to be considered. Thus, in the phased-mission system, the effect of a component failure depends on its operation mode. In this example, the following failure modes are assumed for each component, as shown in Table 2.

Table 2. Failure Modes for Components

Component	Failure Modes	
V1	Failed-Close (FC)	Failed-Open (FO)
V2	Failed-Close (FC)	Failed-Open (FO)
M3	Inadvertent Run(IR)	Inadvertent Stop(IS)
V4	Failed-Close (FC)	Failed-Open (FO)
V5	Failed-Close (FC)	Failed-Open (FO)
V6	Failed-Close (FC)	Failed-Open (FO)
V7	Failed-Close (FC)	Failed-Open (FO)
V8	Failed-Close (FC)	Failed-Open (FO)

System Accident Condition at Phase k

The first stage in the risk analysis of a phased mission system is the derivation of system accident conditions at each phase. This corresponds to a kind of fault tree construction [6]. A step-by-step procedure from the definition of system accidents to the derivation of minimal cut sets is applied [7], as shown below.

Step 1: General definition of system accident conditions:

The first thing to do is to express a general definition of system accidents to be prevented. This definition can be derived from the general information on chemical reactions, chemical properties of materials, and chemical plant operations.

In this example, two types of system accidents are assumed: (S1) a runaway or undesired reaction and (S2) a serious damage to reactor vessel. For each system accident, its occurrence conditions are given as follows:

(S1): A runaway or undesired reaction will occur,
- (A1) if the ratio of material B to material A exceeds the specified value,
- (A2) if the reaction temperature increases,
- (A3) if the mixer stops during the reaction,
- (A4) if material A reacts with residual of material C.
- (A5) if material A or B is supplied at high temperature.

(S2) The reactor vessel will be seriously damaged,
- (A6) if the mixer runs without any material in the vessel.

Step 2: Derivation of system accident conditions using plant-specific conditions

The general definition at step 1 explains how a system accident occurs physically in the batch system. For the risk analysis, more explicit expressions of conditions in terms of operation conditions must be specified at each phase.

1) The first modification is to express conditions in terms of plant operation conditions.

For example, the ratio of material B to material A in (A1) is related to the input operation of materials A and B. The ratio exceeds the specified value if {the input volume of material B is surplus} OR {the input volume of material A is insufficient}.

Thus, general definition of accident conditions can be transformed into operation conditions. This procedure corresponds to a kind of top down approach in the fault tree construction [6].

As a characteristic of the phased-mission system, the operation condition changes depending on its processing stage. Thus, the same type of system accident can occur under distinct failure conditions associated with different operation phases.

Consider a severe damage caused by the mixer running without any material. At the standby phase, this accident can happen due to an inadvertent run of mixer. At the feed phase of material A, the accident can happen due to {the closure failure of valve V1} OR {the inadvertent opening of purge valve V8}. Thus, a system accident condition must be checked at each operation phase by considering component failure effects and their normal conditions.

2) Derive minimal deviation from the normal condition that satisfies a system accident occurrence condition

Firstly, accident occurrence conditions can be obtained by comparing normal component states as shown in Table 1 with system accident conditions (A1)-(A6). Minimal deviation from the normal condition that satisfies a system accident condition corresponds to a system accident occurrence condition at the phase. Generally speaking, more deviations are necessary for an accident to occur, rarer the probability becomes that the corresponding accident will occur is. From a practical viewpoint, accidents with more conditions than the minimal number of conditions can be omitted. How many abnormal conditions are allowable depends on the analyst's judgment or the object of the risk analysis. In this paper, meaningless or impractical accident conditions are omitted in the analysis.

Considering the occurrence of a failure event, it must occur during the operation at a specific phase or during specific phases. For example, accident condition (A4), {the purge operation of V8 is insufficient} AND {the feed of material A}, can occur at phases 1 and 2. For phase 1, {the insufficient purge} is the effect of an operation failure occurring only at phase 6 in the previous batch cycle, while {the feed of material A} is a failure event occurring at phase 1. The occurrence of {the insufficient purge} at phase 6 does not cause any loss immediately, but its effect can seriously appear at phase 1 combined with the occurrence of another failure. Further, the effect of {the insufficient purge} at phase 6 is a single point failure (minimal cut set composed of one basic event) at phase 2. Thus, in obtaining the accident occurrence conditions at each phase, the effect of a component failure occurring at the previous phase must be considered.

Further, the effect of a component failure can be affected by its detection possibility. For example, assume that the normal state of a valve is "closed" at phase 1. The effect of a FO failure occurring at phase 1 can be immediately detected, while the effect of a FC failure cannot be detected at phase 1 because the failed-state is the same as its normal condition at phase 1. Thus, depending on its normal operation condition, the detection possibility of a component failure can be determined. The conventional phased mission analysis [3] does not consider this point when expanding component condition into basic event conditions. This paper applies conservative assumptions that the system will be stopped to repair or restore immediately when the effect of a component failure is apparently different from its normal one, in other words, it can be detected. Thus, only the latent or hidden failure condition can remain whose effect is the same as its normal state. This assumption can make it easier to fix the occurrence time of a failure event.

In this manner, for example, accident occurrence conditions at phase 1 can be obtained as:

(A4): {purge operation of V8 is insufficient} **AND** {failed-open failure of V1}

(A5): **{**{failed-open failure of V4} **AND** {failed-open failure of V5}**}** **AND** **{**{failed-open failure of V1}**OR** {failed-open failure of V2 }**}**
(A6): {inadvertent run of M3}

Thus, component conditions must be represented with information on when they should occur as well as failure modes. To express these conditions explicitly, a triplet expression of {component, operation or failure event, time requirement} is introduced as in [7], where "time requirement" expresses specific phases during which "operation or failure event" must occur. Thus, component conditions are represented in such a form as:

$$\{ C_i, F_j, m\text{-}n \} \qquad (1)$$

where C_i denotes component i, F_j denotes failure event j, and m-n denotes phases from m to n when failure event j can occurs ($m \leq n$).

Thus, accident conditions occurring at each phase with nimal combination of component failure can be obtained as follows:

Phase 1:
(A4): {(V8, FC, 6-6), (V1, FO, 1-1)}
(A5): {(V4, FO,1-1), (V5, FO,1-1), (V1, FO,1-1)},
{(V4, FO, 1-1), (V5, FO, 1-1), (V2, FO, 1-1)}
(A6): {(M3. IR, 1-1)}

Phase 2:
(A4): {(V8, FC, 6-6)}
(A5): {(V4, FO, 2-2), (V5, FO, 2-2)}
(A6): {(V1, FC, 1-2)}, {(V8, FO, 2-2)}

Phase 3:
(A5): {(V4, FO, 3-3), (V5, FO, 3-3)}
(A6): {(V8, FO, 3-3)}

Phase 4:
(A2): {(V5, FO, 4-4)}
(A3): {(M3, IS, 4-4)}
(A6): {(V8, FO, 4-4)}

Phase 5:
(A1): {(V2, FO, 5-5)}
(A2): {(V7, FC, 1-5)}, {(V6, FC, 1-5)}, {(V4, FO, 4-5), (V5, FO, 4-5)}
(A3): {(M3, IS, 5-5)}
(A6): {(V8, FO, 5-5)}

Phase 6:
(A6): {(M3, IR, 6-6)}

variables for component conditions and their probability evaluation. Since multiple failure modes for a component are mutually exclusive, they cannot be represented by the

conventional binary expression with success/failure states. In the following section, we introduce multi-state

System Accident Probability

State variable expressions for components and system are introduced to evaluate their occurrence probabilities.

Assumptions

The following assumptions are made for the system and components.

(a1) A system accident occurs if any system accident condition represented in terms of component conditions is satisfied at any phase.

(a2) The system state is as good as new at the start of a mission, i.e., all the components are as good as new.

(a3) The system state is represented in terms of states of N components. Components can include human operators.

(a4) Components failures are statistically independent

(a5) Component i has Mi +1 failure modes, which are mutually exclusive. Failure mode 0 for each component denotes its normal state.

(a6) Without stop of the plant operation, no component can be repaired or replaced. After component i comes into failure mode j, it remains until the end of mission, a shutdown, or a system accident.

(a7) Transition rate of component i from its normal state to failure mode j at time t is represented as $\lambda_i^j(t)$, where t is the elapsed time from the initiation of the mission.

Component State Variables

The state of component *i* at time *t* is represented by binary variable $X_i^j(t)$ as follows.

$$X_i^j(t) \equiv \begin{cases} 1, & \text{if component } i \text{ is in failure mode } j \text{ at time } t, \\ 0, & \text{otherwise.} \end{cases} \quad (2)$$

where j=0,1,...,M_i., Since component *i* must be in a state: it can be a failure mode or the normal operating state, the following equation must hold from assumptions (a5) & (a6):

$$\sum_{j=0}^{M_i} X_i^j(t) = 1 \quad (3)$$

Assumption (a2) implies that

$$X_i^0(0) = 1 \text{ and } X_i^j(0) = 0 \text{ for } j \neq 0. \quad (4)$$

Assumptions (a6) & (a7) implies that

$$X_i^0(t_1) \geq X_i^0(t_2) \text{ and } X_i^j(t_1) \leq X_i^j(t_2) \text{ for } t_1 \leq t_2 \ \& \ j \neq 0. \quad (5)$$

Using this monotonic property of $X_i^j(t)$, the following simplification rules hold.

$$X_i^0(t_1)X_i^0(t_2) = X_i^0(t_2), \quad \text{for } t_1 \leq t_2. \quad (6)$$

$$X_i^j(t_1)X_i^j(t_2) = X_i^j(t_1) \quad \text{for } t_1 \leq t_2 \ \& \ j \neq 0. \quad (7)$$

$$X_i^0(t_1) \vee X_i^0(t_2) = X_i^0(t_1), \quad \text{for } t_1 \leq t_2. \quad (8)$$

$$X_i^j(t_1) \vee X_i^j(t_2) = X_i^j(t_2), \quad \text{for } t_1 \leq t_2 \ \& \ j \neq 0. \quad (9)$$

Further, using the mutually exclusiveness of failure modes, the following simplification rules hold:

$$X_i^{j_1}(t_1)X_i^{j_2}(t_2) = 0, \quad \text{for } j_1 \neq j_2 > 0 \ \& \text{ any } t_1, t_2 \geq 0. \quad (10)$$

$$X_i^j(t_1)X_i^0(t_2) = 0, \quad \text{for } j \neq 0,\ t_1 < t_2. \tag{11}$$

$$\overline{X_i^{j_1}(t_1)}X_i^{j_2}(t_2) = X_i^0(t_1)X_i^{j_2}(t_2), \quad \text{for } j_1 \neq 0,\ \text{any } j_2,\ t_1 < t_2. \tag{12}$$

where $\overline{X}$ denotes the negation of X.

Since event $B(C_i, F_j, t_1, t_2)$ that component i experiences failure mode j between t_1 and t_2 can be represented as {component i is not in failure mode j at t_1} AND {component i is in failure mode j at t_2}. Thus, the following equation holds.

$$B(C_i, F_j, t_1, t_2) = \{X_i^j(t_1) = 0\}\text{AND}\{X_i^j(t_2) = 1\} \tag{13}$$

Using equation (12), this expression can be represented as:

$$B(C_i, F_j, t_1, t_2) = \{X_i^0(t_1)X_i^j(t_2) = 1\} \tag{14}$$

System State Variable

Similarly to component state variable $X_i^j(t)$, the system state during time t at phase k, $Y_k(t)$, can be defined as follows:

$$Y_k(t) \equiv \begin{cases} 1, & \text{if the system is in an accidental stateat time } t \text{ during phase } k, \\ 0, & \text{otherwise.} \end{cases} \tag{15}$$

Using the system accident condition at phase k, which can be represented in terms of $B(C_i, F_j, t_1, t_2)$, the system state can be represented in terms of state variables $X_i^j(t)$. For example, system accident condition at phase 3, $Y_3(t)$, can be expressed as:

$$Y_3(t) = \left\{X_{V4}^0(t_3^S)X_{V4}^{FO}(t)X_{V5}^0(t_3^S)X_{V5}^{FO}(t)\right\} \vee \left\{X_{V8}^0(t_3^S)X_{V8}^{FO}(t)\right\} \tag{16}$$

where t_k^S and t_k^E denote the start and end times of phase k.

System Accident Occurrence Condition at Phase l

Now obtain the system accident occurrence condition at phase l. The above condition, equation (16), shows a condition whether the system is suffering from the system accident at phase 3, which does not always implies that the system accident occurs at phase 3 because another system accident might occur at the previous phase. One of the most important characteristic is that the system accident condition at the later phase does not always lead to an immediate system accident when it is satisfied. System accident occurs at phase l requires that {no accident occurs before the phase l} AND {accident firstly occurs at phase l}.

Thus, system occurrence conditions at time t during phase l, denoted by binary variable $\phi_l(t)$, can be represented in terms of $Y_k(t)$, as:

$$\phi_l(t) = \left(\bigwedge_{k=1}^{l-1} \overline{Y_k}(t_k^E)\right) Y_l(t) \tag{17}$$

where each $Y_k(t)$ can be represented in the similar way as equation (16).

System Accident Probability at Phase L

Component State Probability

Define state probability of component *i* at time *t*, $Q_i^j(t)$, as:

$$Q_i^j(t) \equiv \Pr\{X_i^j(t) = 1\} = \mathrm{E}\{X_i^j(t)\} \qquad (18)$$

where $\mathrm{E}\{\}$ denote the expectation operation.

From assumptions (a5), (a6) & (a7), $Q_i^j(t)$ can be represented as:

$$Q_i^0(t) = \exp\left(-\int_0^t \lambda_i^f(s)ds\right) \qquad (19)$$

$$Q_i^j(t) = \int_0^t \lambda_i^j(\tau)\exp\left(-\int_0^\tau \lambda_i^f(s)ds\right)d\tau \quad \text{for } j \neq 0 \qquad (20)$$

where $\lambda_i^f(t) \equiv \sum_{j=1}^{M_i} \lambda_i^j(t)$.

Note that the value of $\lambda_i^j(t)$ mainly depend its operation condition at each phase. For constant transition rate, $\lambda_i^j(t) = \lambda c_i^j$, equations (19) and (20) can be simplified into:

$$Q_i^0(t) = \exp\left(-\lambda c_i^f t\right) \qquad (21)$$

$$Q_i^j(t) = \frac{\lambda c_i^j}{\lambda c_i^f}\left\{1 - \exp\left(-\lambda c_i^f t\right)\right\}, \text{ for } j \neq 0 \qquad (22)$$

where $\lambda c_i^f \equiv \sum_{j=1}^{M_i} \lambda c_i^j$.

Using these equations, the probability that event $B(C_i, F_j, t_1, t_2)$ occurs can be evaluated as:

$$\Pr\{B(C_i, F_j, t_1, t_2)\} = Q_i^j(t_2) - Q_i^j(t_1) \qquad (23)$$

System Accident Occurrence Probability

The system accident occurrence probability at phase *l* for the phased-mission system, $Q_S^l(t)$, can be obtained as:

$$Q_S^l(t) = \Pr\{\phi_l(t) = 1\} = \mathrm{E}\left\{\left(\bigwedge_{k=1}^{l-1} \overline{Y_k}(t_k^e)\right) Y_l(t)\right\} \qquad (24)$$

As shown in equation (16), $Y_k(t)$ are represented as logical OR of {logical AND combination of $X_i^j(t)$ at different time *t*}, and so $\overline{Y_k}(t)$ are represented as logical AND of {logical OR combination of $\overline{X_i^j}(t)$ at different time *t*}. Expanding the logical expression of the right term in equation (24) by applying the simplification rules of $\overline{X_i^j}(t)$, the reduced form can be expressed as logical OR of logical AND combination of { $X_i^j(t)$, $X_i^0(t_1)X_i^j(t_2)$, or $\overline{X_i^j}(t)$ }. Using the statistical independence of component failures, the system occurrence probability can be

evaluated from component failure probabilities.

Illustrative Example

Obtain the system accident probability occurring at phase 3 in the first mission cycle. In the first mission, because previous cycle does not exist, event (V8, FC, 6-6) cannot occur. Further, at phase 1, the occurrence conditions of (A4) requires 2 more component failure events than (A6), accident occurrence (A4) can be neglected for the simplicity. Under these simplification assumptions, the system accident conditions at phases 1, 2, and 3 can be modified as:

Phase 1: {(M3. IR, 1-1)}
Phase 2: {(V4, FO, 2-2), (V5, FO, 2-2)} OR {(V1, FC, 1-2)}, {(V8, FO, 2-2)}
Phase 3: {(V4, FO, 3-3), (V5, FO, 3-3)} OR {(V8, FO, 3-3)}

Using state variable $Y_k(t)$, the occurrence of system accident at phase 3 can be expressed as:

$$\phi_3(t) = \overline{Y}_1(t_1^E)\overline{Y}_2(t_2^E)Y_3(t) \tag{25}$$

where

$$\overline{Y}_1(t_1^E) = \overline{X_{M3}^{IR}}(t_1^E) \tag{26}$$

$$\overline{Y}_2(t_2^E) = \left\{\overline{X_{V4}^0}(t_2^S) \vee \overline{X_{V4}^{FO}}(t_2^E) \vee \overline{X_{V5}^0}(t_2^S) \vee \overline{X_{V5}^{FO}}(t_2^E)\right\} \wedge \left\{\overline{X_{V1}^{FC}}(t_2^E) \vee \overline{X_{V8}^0}(t_2^S) \vee \overline{X_{V8}^{FO}}(t_2^E)\right\} \tag{27}$$

$$Y_3(t) = \left\{X_{V4}^0(t_3^S)X_{V4}^{FO}(t)X_{V5}^0(t_3^S)X_{V5}^{FO}(t)\right\} \vee \left\{X_{V8}^0(t_3^S)X_{V8}^{FO}(t)\right\} \tag{28}$$

After logical expansion of equation (25) using component-wise simplification rules of $X_i^j(t)$, $\phi_3(t)$ can be obtained as:

$$\begin{aligned}\phi_3(t) = {} & \left\{\overline{X_{M3}^{IR}}(t_1^E)\right\} \\ & \wedge \left(\overline{X_{V1}^{FC}(t_2^E)X_{V8}^0(t_2^S)X_{V8}^{FO}(t_2^E)}\, X_{V4}^0(t_3^S)X_{V4}^{FO}(t)X_{V5}^0(t_3^S)X_{V5}^{FO}(t)\right. \\ & \left. \vee \overline{X_{V4}^0(t_2^S)X_{V4}^{FO}(t_2^E)X_{V5}^0(t_2^S)X_{V5}^{FO}(t_2^E)}\, X_{V8}^0(t_3^S)X_{V8}^{FO}(t)\right)\end{aligned} \tag{29}$$

Note that state variable expressions for each component in equation (29) can be evaluated quantitatively based on the statistical independence of component failures. System accident probability at time *t* in phase 3, $Q_S^3(t)$, can be obtained as follows:

$$\begin{aligned}Q_S^3(t) = {} & \left\{1 - Q_{M3}^{IR}(t_1^E)\right\}\left(\left[1 - \left\{Q_{V1}^{FC}(t_2^E)\right\}\left\{Q_{V8}^{FO}(t_2^E) - Q_{V8}^{FO}(t_2^S)\right\}\right]\right. \\ & \times \left\{Q_{V4}^{FO}(t) - Q_{V4}^{FO}(t_3^S)\right\}\left\{Q_{V5}^{FO}(t) - Q_{V5}^{FO}(t_3^S)\right\} \\ & + \left[1 - \left\{Q_{V4}^{FO}(t_2^E) - Q_{V4}^{FO}(t_2^S)\right\}\left\{Q_{V5}^{FO}(t_2^E) - Q_{V5}^{FO}(t_2^S)\right\}\right]\left\{Q_{V8}^{FO}(t) - Q_{V8}^{FO}(t_3^S)\right\} \\ & \left. - \left\{Q_{V4}^{FO}(t) - Q_{V4}^{FO}(t_3^S)\right\}\left\{Q_{V5}^{FO}(t) - Q_{V5}^{FO}(t_3^S)\right\}\left\{Q_{V8}^{FO}(t) - Q_{V8}^{FO}(t_3^S)\right\}\right)\end{aligned} \tag{30}$$

Thus, the system accident occurrence probability can be easily evaluated based on component state probabilities. The effect of a common cause failure can be analyzed by collecting components affected by it into a subsystem, whose state probabilities can be analyzed independently.

Conclusions

This paper proposes a systematic procedure to obtain system accident occurrence conditions and probabilities of the batch process in a chemical plant. Since the functional relation among components changes depending on the processing stage, a phased mission analysis approach is applied. A step-by-step procedure is developed to obtain accident occurrence conditions at each phase based on the general definition of system accidents in the batch process. To deal with the time dependency among phases and multiple failure modes, a component state variable is introduced to represent {component, failure event, and occurring time}. This representation can simplify not only the logical operations of component conditions, but also the probability evaluation of system accident occurring at a specific phase. Practical consideration of maintenance operation in the phased-mission system is our next step.

References

[1] G. R. Burdick, J. B. Fussell, D. M. Rasmuson, J. R. Wilson, "Phased Mission Analysis: A Review of New Developments and An Application," *IEEE Trans. Reliability*, vol. 26, no. 1, 1977, pp 43-49

[2] A. Hoyland, M. Rausand, *System Reliability Theory, Models and Statistical Methods*, John Wiley & Sons, INC., 1994

[3] J. D. Esary, H. Ziehms, "Reliability Analysis of Phased Missions," *Reliability and Fault Tree Analysis*, SIAM, Philadelphia, 1975, pp 213-236

[4] J. B. Dugan, "Automated Analysis of Phased-Mission Reliability," *IEEE Trans. Reliability*, 1991, vol. 40, no. 1, pp 45-51

[5] I. Mura, A. Bondavalli, "Hierarchical Modeling & Evaluation of Phased-Mission Systems," *IEEE Trans. Reliability*, 1999, vol. 48, no. 4, pp 45-51

[6] W. E. Vesely, F. F. Goldberg, N. H. Roverts, D. F. Haasl, *Fault Tree Handbook*, USNRC, NUREG-0492, 1981

[7] T. Kohda, M. Nakagawa, "Risk Evaluation of Batch Processes in Chemical Plants Using Phased-Mission Analysis," Proc. ESREL2006, 2006, pp 151-156