Title: A Design Method of a Plant Alarm System for First Alarm Alternative Signals using a Modularized CE Model

Author names and affiliations:

Kazuhiro Takeda,[a], Takashi Hamaguchi,[b], Naoki Kimura,[c], and Masaru Noda,[d]

[a] Faculty of Engineering, Shizuoka University, 3-5-1 Johoku Hamamatsu, 432-8561, Japan

[b] Graduate School of Engineering, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya, 466-8555, Japan

[c] Faculty of Engineering, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka, 819-0395, Japan

[d] Department of Chemical Engineering, Fukuoka University, 8-19-1 Nanakuma, Jonan-ku, Fukuoka, 814-0180, Japan

Corresponding author:

Name: Kazuhiro Takeda

Affiliation: Faculty of Engineering, Shizuoka University,

Phone: +81-53-478-1176

E-mail: tktaked@ipc.shizuoka.ac.jp

Postal address: 3-5-1 Johoku Hamamatsu, 432-8561, Japan

Abstract

Management of a plant alarm system has been identified as one of the key safety issues because of disasters caused by alarm floods. When a chemical plant is at abnormal state, an alarm system must provide useful information to operators as the third layer of an independent protection layer (IPL). Therefore, a method of designing a plant alarm system is important for plant safety. Because the plant is maintained in the plant lifecycle, the alarm system for the plant should be properly managed through the plant lifecycle. To manage changes, the design rationales of the alarm system should be explained explicitly. This paper investigates a logical and systematic alarm system design method that explicitly explains the design rationales from know-why information for proper management of changes through the plant lifecycle. In the method, the module structure proposed by Hamaguchi et al. (2011) to assign a fault origin to be distinguished is extended. Using modules to investigate the sets of alarm sensors and the alarm limits setting for first alarm alternative signals to distinguish the fault origin, an alarm system design method is proposed. Also, the completeness of fault propagation for a branch of the Cause-Effect model as the plant model is explained. Using the modules and the set of fault origins to be distinguished by the alarm system, we try to explicitly explain the design rationales of the alarm system.

Keywords: First Alarm; Plant Alarm System Design; Cause-Effect Model;

Alarm Management; Plant Alarm Malfunction.

1. Introduction

A plant alarm system is one of the important elements as the third layer of the independent protection layers (CCPS, 2001). Management of the plant alarm system has been identified as one of the key issues because of disasters caused by alarm floods. When the plant is at abnormal state, an alarm system must provide useful information to operators as the third layer of the IPL. Because the modification of the plant is happening throughout the plant lifecycle, the alarm system for the plant should be properly managed through the lifecycle. A framework to manage the alarm system lifecycle has been proposed (ISA, 2009). If the alarm system was designed without sufficient assessment using design rationales, the alarm system may not properly function as a part of the IPL when the plant is at abnormal state. Thus, the alarm system cannot protect the plant from accidents or disasters.

Although some methods of alarm limits setting or nuisance alarms reduction obtained through plant improvement activities have been proposed, there is no systematic design method to explicitly provide whole design rationales. Hence, a useful design method is required for this problem.

2. Alarm System Design Problem

To support safe operation, an alarm system is required to provide early detection of an abnormal state of a plant and to alert the operators. An objective alarm system should distinguish significant fault origins at early abnormal state. For example, the operators assume that the fault origins of the abnormal state may be leakage from a pipe or a decrease in source pressure. If the real fault origin is leakage from a pipe, opening a valve as the countermeasure for a decrease in source pressure will lead to a disaster. To implement a suitable countermeasure, these fault origins should be distinguished by the alarm system. In this paper, a set of fault origins to be distinguished by the alarm system is called set C. The alarm system design problem consists of the following sub problems.

Sub problem 1: Selection of the set C.

Sub problem 2: Selection of the set of alarm sensors to distinguish the set C.

Sub problem 3: Setting of the limits of the alarm sensors to alert operators.

Takeda et al. (2010) assume that the limits of the alarm sensors are properly set and

that the status (normal or abnormal) of the process variables can be observed. They have proposed a design method to search the sets of alarm sensors to logically distinguish the set C using abnormal status patterns of the sets of alarm sensors, a CE (cause-effect) model and the rule of propagation of a fault in the model. An abnormal status pattern contains an abnormal status of one or more alarm sensors. The CE model represents cause-effect relationships between process variables. In the paper, it is assumed that the order of detection time of an abnormal status of the alarm sensors is unreliable. Therefore, the method may reject the set of alarm sensors which is able to distinguish the set C using the order of detection time of an abnormal status of the alarm sensors.

Kato et al. (2011) have proposed a design method to reject the set of alarm sensors which cannot distinguish the set C even if the detection order is available. However, it is difficult to use the limits setting to satisfy the detection order of all alarm sensors as correct fault propagation paths.

In the alarm system design, if a set of alarm sensors cannot distinguish the set C, then decision making will be needed to either add sensors or use another method to distinguish the set C. The proposed methods cannot provide the design rationales for decision making in the alarm system design, although the methods present the results

of distinguishability of the set C.

To provide the design rationales, Hamaguchi et al. (2011) have proposed a module using the CE model and allocation of sensors to assign at most one fault origin of the set C. They also assume that the detection order of the alarm sensors is unreliable. Therefore, a loop of the CE model becomes one module, even if the loop contains one or more alarm sensors.

This paper investigates a logical and systematic alarm system design method that explicitly explains the design rationales from know-why information for proper management of change through the plant lifecycle. The approaches of modules using the CE model and allocation of sensors proposed by Hamaguchi et al. (2011) are useful to explicitly explain the design rationales. In this paper, the modules proposed by Hamaguchi et al. (2011) to assign the fault origin to be distinguished are extended. Using modules to investigate the sets of alarm sensors and the alarm limits setting, an alarm system design method is proposed. Using the two types of modules and a set of fault origins to be distinguished by the alarm system, we try to explicitly explain the design rationales of the alarm system. This paper assumes the following conditions for alarm system design.

(1) Plant model: The operation states of an objective plant can be estimated. Cause-effect relationships between process variables in the operation states can be represented as a CE model, which is constructed by nodes and directed arcs. The CE model has been used for alarm management and fault diagnosis (I. S. Kim, 1994; H. Vedam and V. Venkatasubramanian, 1997; F. Yang et al., 2010). Synthesis of the CE model of an industrial chemical plant has been widely discussed by many researchers (S. Tateno et al., 1994; C. Palmer et al., 2000; D. C. Montgomery, 2001). It is assumed that the CE model is given for alarm system design by using the proposed methods.

(2) Fault origins: Only one of the fault origins to be distinguished by the alarm system can occur simultaneously. A set of fault origins to be distinguished is obtained by use of a process hazard analysis such as a HAZOP (Hazard and operability) study. The process hazard analysis roughly considers detection time, diagnosing time, reaction time, operating conditions and so on. Those exact values are not necessarily required for the analysis.

Formatted: Font color: Red

Formatted: Font color: Red

Formatted: Font color: Red

(3) Mapping of fault origins: The fault origins to be distinguished can be assigned one by one to pairs of nodes and their signs of the CE model. The nodes represent process variables. One fault origin can be assigned to one pair at most, because the fault origins cannot be distinguished when two or more fault origins are assigned to a pair.

(4) Abnormality propagation: The abnormality of an upper node can propagate to lower nodes only by the path of the CE model. However, the propagation between the nodes does not always happen under abnormal situations. Only the propagated nodes are abnormal status. The other nodes, that are not propagated, are normal status. On the branches of the CE model, it is uncertain which branches or how many branches can have an abnormality propagating from the upper node to the lower nodes. This topic is explained in section 3.4.

(5) Available sensors: In alarm system design, known existing sensors are initially available for the set of alarm sensors. When the set C cannot be distinguished by any sets of existing sensors, an approach to add new sensors is conceivable. However, this approach is out of the scope of this paper.

(6) Alarm limits setting: After determination of the sensors, the alarm limits should be set. The process parameters in a plant would change. It is assumed that the parameters are adequately measured by above mentioned sensors, the alarm limits are evaluated and coordinated by using a proposed method (e.g., Kimura et al., 2013). This paper mentions requirements of the alarm limits settings by using a CE model, which is a simple model and does not represent rigorous dynamics of the objective plant, although sensitivity of the sensors should be analyzed to set the alarm limits.

3. Explicit Design Rationales Using Modules to Assign Fault Origins of the set C

3.1. CE model

An example plant and a CE model corresponding to the example plant are shown in Figure 1(a) and Figure 1(b). This plant has two raw material flow rates, F1 and F2, two product flow rates, F4 and F5, one intermediate flow rate, F3, and two liquid levels, L1 and L2. The nodes of the CE model represent process variables, and the arcs represent cause and effect relationships between the nodes. The arcs are solid for positive influences and broken for negative influences. Sensor nodes available for the set of alarm sensors are the double circles in this paper. The nodes assigned with the fault origins to be distinguished are filled circles in this paper. For example, a blockage of an intermediate pipe is assigned to the node F3 and the sign (-).

A general CE model can be constructed from combinations of four basic components (straight, combined, branch and strongly connected) as shown in Figure 2. For example, the CE model in Figure 1 contains all the components. In the following figures, the nodes are numbered for general expression. This paper investigates the design method of modules to assign fault origin of the set C using the basic components. The modules

consist of measured primitive group units and unmeasured primitive group units.

Figure 1. Example plant and CE model.

Figure 2. Basic components.

3.2. Basic Design Method of Modules to Assign Fault Origins of the set C

In this paper, a measured primitive group unit means upstream nodes from a sensor node before another sensor node or to an uppermost node. In the case of a sensor node and an uppermost node, the node is a measured primitive group unit. An unmeasured primitive group unit means upstream nodes from a lowermost unmeasured node before a sensor node or to an uppermost node. In each measured primitive group unit, fault propagation can be detected, but in which node the fault occurs cannot be distinguished. Thus, one fault origin at most to be distinguished should be assigned to the measured primitive group unit. In an unmeasured primitive group unit, fault propagation cannot be detected, because the unmeasured primitive group unit is lowermost and has no sensor node. Thus, no fault origin to be distinguished should be assigned to the unmeasured primitive group unit. This information is the design rationales for the

above-mentioned sub problems 1 and 2.

A design example of the modules to assign a fault origin of the set C for a straight component is demonstrated in Figure 3. It is assumed that the CE model represent a pipeline system and the nodes 1, 2, …, 6 are an upper pressure, an upper flow rate, a middle pressure, a middle flow rate, a lower pressure, and a lower flow rate, respectively. To illustrate the modules, some arcs are eliminated. Sensor nodes are the middle pressure 3 and the lower pressure 5. The measured primitive group units are {1,2,3} and {4,5}. The unmeasured primitive group unit is {6}. For the measured primitive group unit {1,2,3}, when the sensor node 3 detects an abnormal status (abnormal lower pressure), it is thought that each node in the measured primitive group unit {1, 2, 3} can be respectively assigned the fault origins (leakage from the upper section, blockage at the upper section, and leakage from the middle section) to be distinguished. However, which node is the fault origin cannot be distinguished. Thus, either node 1, 2 or 3 can be assigned the fault origin to be distinguished. For the measured primitive group unit {4,5}, it is thought that each node in the measured primitive group unit {4, 5} can be respectively assigned the fault origins (blockage at the middle section and leakage from the lower section) to be distinguished when the sensor node 3 represents a normal state and the sensor node 5 detects an abnormal status (abnormal lower pressure). However,

which node is the fault origin cannot be distinguished. Thus, either node 4 or 5 can be assigned the fault origin to be distinguished. A fault occurring in unmeasured primitive group unit {6} cannot be detected. Thus, the node in the unmeasured primitive group unit should not be assigned any fault origins to be distinguished.

Figure 3. Module to assign fault origins to be distinguished.

The design method for the straight components can be easily extended for the combined component or the branch component with a measured junction node. For the branch component with an unmeasured junction node, the extension of the measured and unmeasured primitive group units is explained in the following section.

3.3. Extension for the Branch Component with an Unmeasured Junction Node

An example of a branch component with an unmeasured junction node and measured primitive group units is shown in Figure 4(a). It is assumed that the CE model represent a branched pipeline system and the nodes 1, 2, …, 7 are a source pressure, a junction pressure, a left branch pressure, a middle branch flow rate, a right branch flow rate, a middle branch pressure, and a right branch flow rate, respectively. The junction

node 2 has three output branches. The branches are a part of the respective measured primitive group unit. The nodes in the branches are the unshared nodes. The upper nodes from the junction node 2 are shared with the measured primitive group units and the shared nodes as shown in Figure 4(b). One fault origin at most to be distinguished can be assigned to the unshared nodes of the measured primitive group unit.

Assigning a fault origin to the shared node means the assignment of the fault origin to all measured primitive group units sharing the node. Thus, one fault origin at most to be distinguished can be assigned to the entire measured primitive group units with the shared nodes. The unmeasured primitive group unit should be redefined for the structure. Redefinition of the unmeasured primitive group unit is that the unit means upstream nodes from a lowermost unmeasured node before a sensor node, to an uppermost node or before an unmeasured junction node.

When two or more measured and unmeasured primitive group units share the nodes as shown in Figure 5, the nodes in the units are divided into shared nodes and unshared nodes. The left branch is the unmeasured primitive group unit. The other branches are a part of the respective measured primitive group unit. The upper nodes from the junction node 2 are shared with two measured primitive group units and the shared nodes. As mentioned above, one fault origin at most to be distinguished can be assigned

to the entire measured primitive group units with the shared nodes.

Figure 4. Extension for the branch component with unmeasured junction node and measured primitive group units.

Figure 5. Extension for the branch component with unmeasured junction node and measured and unmeasured primitive group units.

3.4. Completeness for Branch Component

The topic mentioned in section 2 (4) is explained. When a fault occurs at the node 1 or 2 in Figure 5, it is uncertain in which branches or in how many branches the abnormality can propagate from the upper node to the lower nodes. Therefore, all measured primitive group units sharing the unmeasured junction node are merged into a measured group unit as shown in Figure 6. If the effects are propagated only along the branches with the unmeasured primitive group unit, the effects aren't measured. Thus, the branch component with the unmeasured primitive group units (Figure 6(a)) is a less desirable component than the branch component without unmeasured primitive group units (Figure 6(b)) for completeness of the detecting capability.

Figure 6. Completeness for the branch component as a measured group unit.

3.5. Modularizing of a Strongly Connected Component

A measured primitive group unit assigned (unassigned) with the fault origins to be distinguished is called an assigned (unassigned) measured primitive group unit. A CE model with straight and strongly connected components is shown in Figure 7(a). It is assumed that the CE model represents recycled pipeline system and the nodes 1, 2, …, 5 are an upper pressure, an upper flow rate, a middle pressure, a middle flow rate, and a lower pressure, respectively. The nodes 2, 4 and 5 are sensor nodes. The CE model is divided into three measured primitive group units {1,2}, {3,4}, and {5}. The unit {1, 2} connects to the unit {3,4}, the unit {3,4} connects to the unit {5}, and the unit {5} connects to the unit {1,2}. The connections are based on the arcs. An alarm system design procedure involves the CE model to be converted to the modules to assign the fault origin of the set C and also the assignment of fault origins to be distinguished.

If there are unassigned measured primitive group units in a lower stream from an assigned unit, the unassigned measured primitive group units are merged into a measured group unit. The merging procedure continues until there is no unassigned

measured primitive group unit. As shown in Figure 7(b), there are 5 patterns of the measured group units for various assignment of fault origins to be distinguished. As shown in Figure 7(c), it is assumed that the fault origins (leakage from the upper section and the lower section) to be distinguished are assigned to the nodes 1 and 5. The unit {3,4} isn't assigned the fault origins. The unit {1,2} and the unit {3,4} are merged into a measured group unit {1,2,3,4}. The unit {5} is a measured group unit {5}.

It is assumed that the first detected alarm sensor is identified after fault propagation is widely spread. The alarm sensors in each measured group unit are the first alarm alternative signals to distinguish the fault origin in the unit. The limits of any first alarm alternative signals of the unit are set to detect an abnormal state earlier than the alarm sensors of the other units.

The measured primitive group unit is a module for explicitly describing the condition in which a fault origin to be distinguished in the unit can be distinguished. On the other hand, the measured group unit is a module for investigating the sets of alarm sensors and the alarm limits setting after assignment of the fault origins to be distinguished. Using the measured group units, the strongly connected components are modularized (Figure 7(b)).

In the first pattern of Figure 7(b), the node 2 (abnormal lower flow rate at the upper

section) or 4 (abnormal lower flow rate at the middle section) is sufficient for detection earlier than node 5 (abnormal lower pressure at the lower section) when the fault 1 (leakage from the upper section) occurs. The node 5 is sufficient for detection earlier than nodes 2 and 4 when the fault 5 occurs. The limits setting for the detection is easier than the order of detection time of all alarm sensors and follows the order of fault propagation in the CE model. The progress and result information are the design rationales for the above-mentioned sub problem 3.

Figure 7. Measured group units for strongly connected component.

4. Conclusion

This paper investigated a logical and systematic alarm system design method that explicitly explains design rationales from know-why information for proper management of change through the plant lifecycle. In the method, the module structure proposed by Hamaguchi et al. (2011) to assign the fault origin to be distinguished was extended to modularize the branch and strongly connected components. The modules are constructed using the nodes connections and allocation of sensors of the CE model.

Also, the completeness of fault propagation for a branch of the CE model as the plant model is explained. Using the modules and the set of fault origins to be distinguished by the alarm system, we tried to explicitly explain the design rationales of the alarm system.

References

CCPS, 2001, Layer of Protection Analysis, New York; American Institute of Chemical Engineers, Center for Chemical Process Safety

ISA, 2009, Management of Alarm Systems for the Process Industries, North Carolina

K. Takeda, T. Hamaguchi and M. Noda, 2010, Plant Alarm System Design based on Cause-Effect Model, Kagaku Kogaku Ronbunshu, 36, 2, 136—142

M. Kato, K. Takeda, M. Noda, Y. Kikuchi and M. Hirao, 2011, Design Method of Alarm System for Identifying Possible Malfunctions in a Plant Based on Cause-Effect Model, 11th Int. Sympo. PSE

I. S. Kim, 1994, Computerized systems for on-line management of failures: a state-of-the-art discussion of alarm systems and diagnostic systems applied in the nuclear industry, Rel. Eng. Sys. Safety, 44, 3, 279—295

T. Hamaguchi, K. Takeda, M. Noda and N. Kimura, 2011, A Method of Designing Plant

Alarm Systems with Hierarchical Cause-Effect Model, 11th Int. Sympo. PSE

D. C. Montgomery, 2001, Introduction to Statistical Quality Control, John Wiley, New York

C. Palmer and P. W. H. Chung, 2000, Creating Signed Directed Graph Models for Process Plants, Ind. Eng. Chem. Res., 39, 7, 2548—2558

S. Tateno, B. Shibata, Y. Tsuge and H. Matsuyama, 1994, Automated Synthesis of a Signed Directed Graph for Chemical Plants, Trans. Soc. Inst. Cont. Eng., 30, 11, 1385—1394

N. Kimura, T. Hamaguchi, K. Takeda, M. Noda, 2013, Determination of Alarm Setpoint for Alarm System Rationalization using Performance Evaluation, HCI Int. 2013

H. Vedam, V. Venkatasubramanian, 1997, Signed digraph based multiple fault diagnosis, Comp. & Chem. Eng., Vol. 21, Suppl., pp.S655—S660

F. Yang, S. L. Shah, D. Xiao, 2010, Correlation analysis of alarm data and alarm limit design for industrial processes, American Cont. Conf., 5850—5855

Figure captions:

Figure 1. Example plant and CE model.

(a) Example Plant

(b) CE model

Figure 2. Basic components.

(a)Straight

(b) Combined

(c) Branch

(d) Strongly connected

Figure 3. Module to assign fault origins to be distinguished.

Figure 4. Extension for the branch component with unmeasured junction node and measured primitive group units.

(a) Branch component

(b) Measured primitive group units

Figure 5. Extension for the branch component with unmeasured junction node and measured and unmeasured primitive group units.

(a) Branch component

(b) Measured primitive group units

Figure 6. Completeness for the branch component as a measured group unit.

(a) Measured primitive group units

(b) Measured group units

Figure 7. Measured group units for strongly connected component.

(a) Measured primitive group units

(b) Various patterns of measured group units

(c) Measured group units assigned with fault origins to the node 1 and 5

Figure

Fig.1 (a)

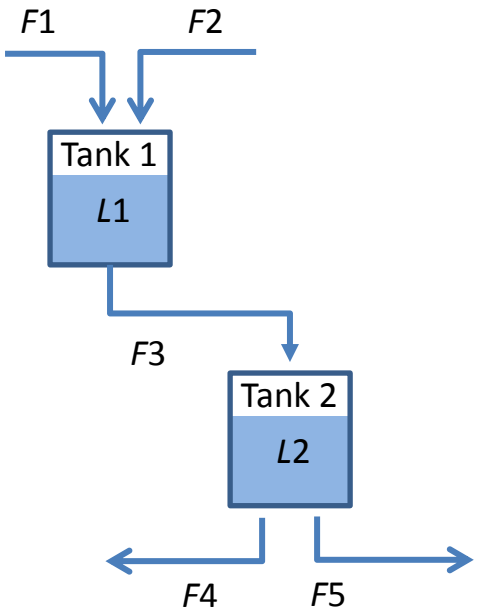

Fig.1 (b)

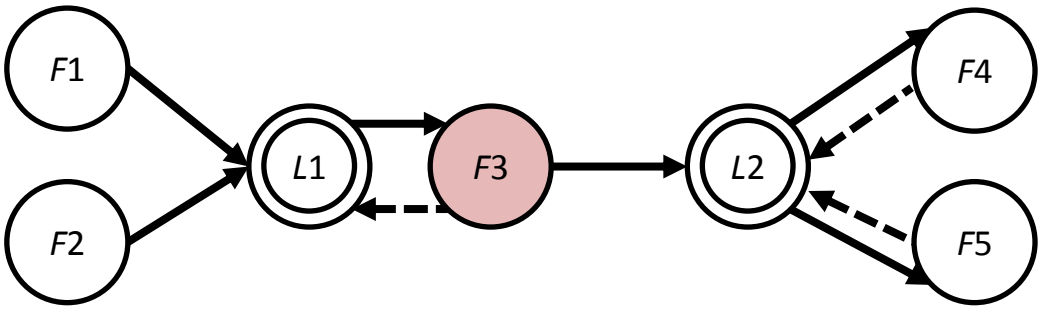

Fig.2 (a)

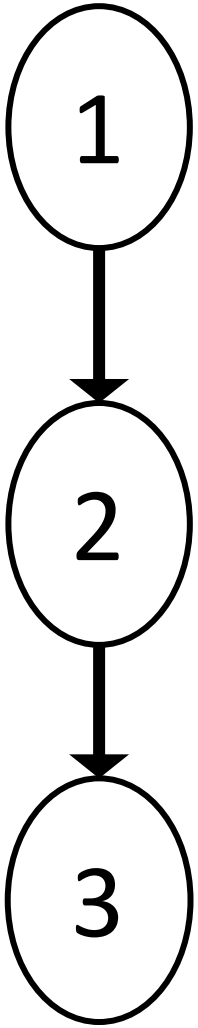

Fig.2 (b)

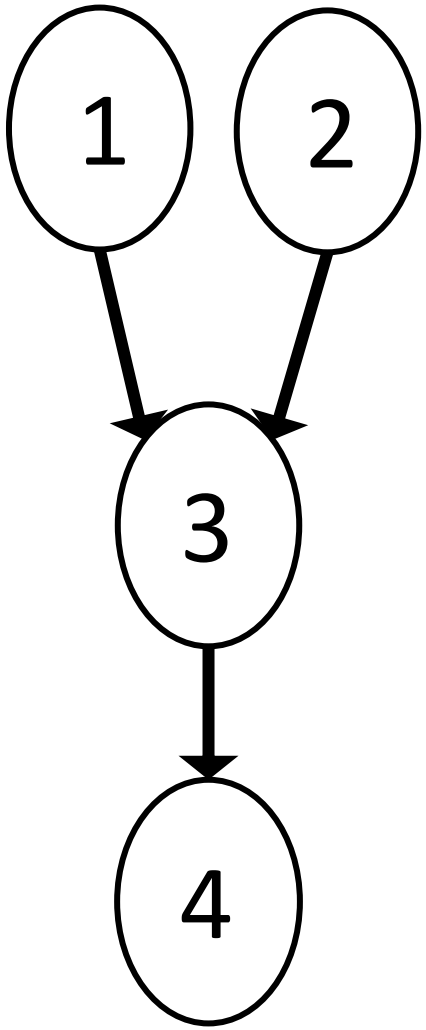

Fig.2 (c)

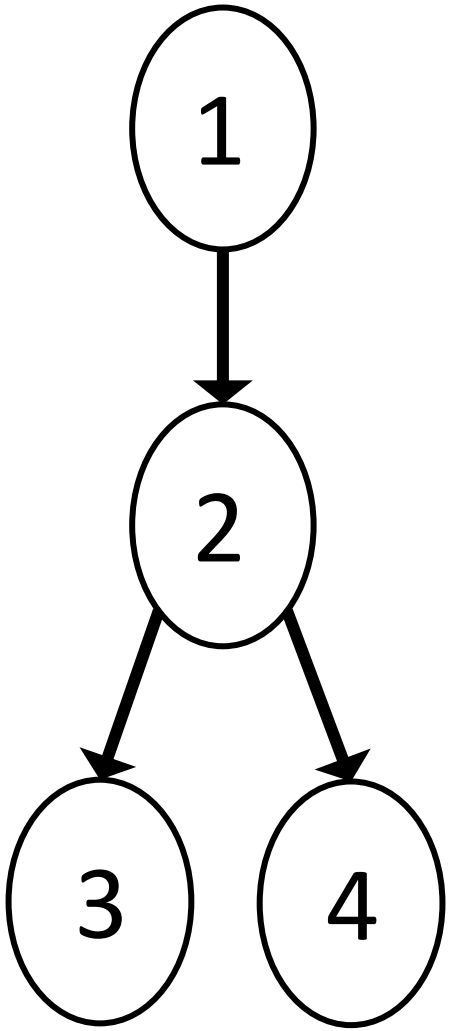

Fig.2 (d)

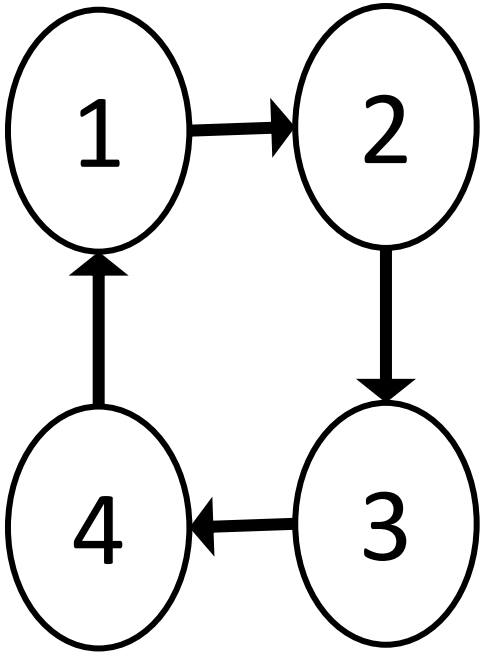

Fig.3

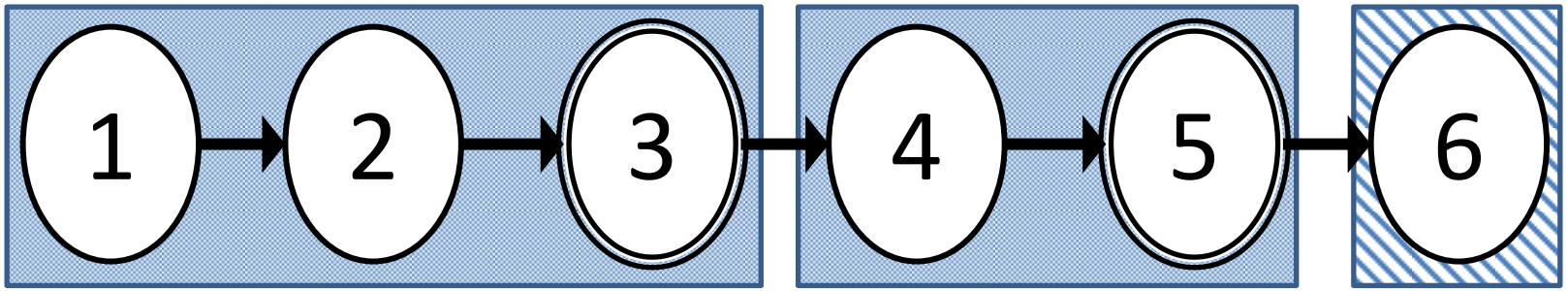

Fig.4 (a)

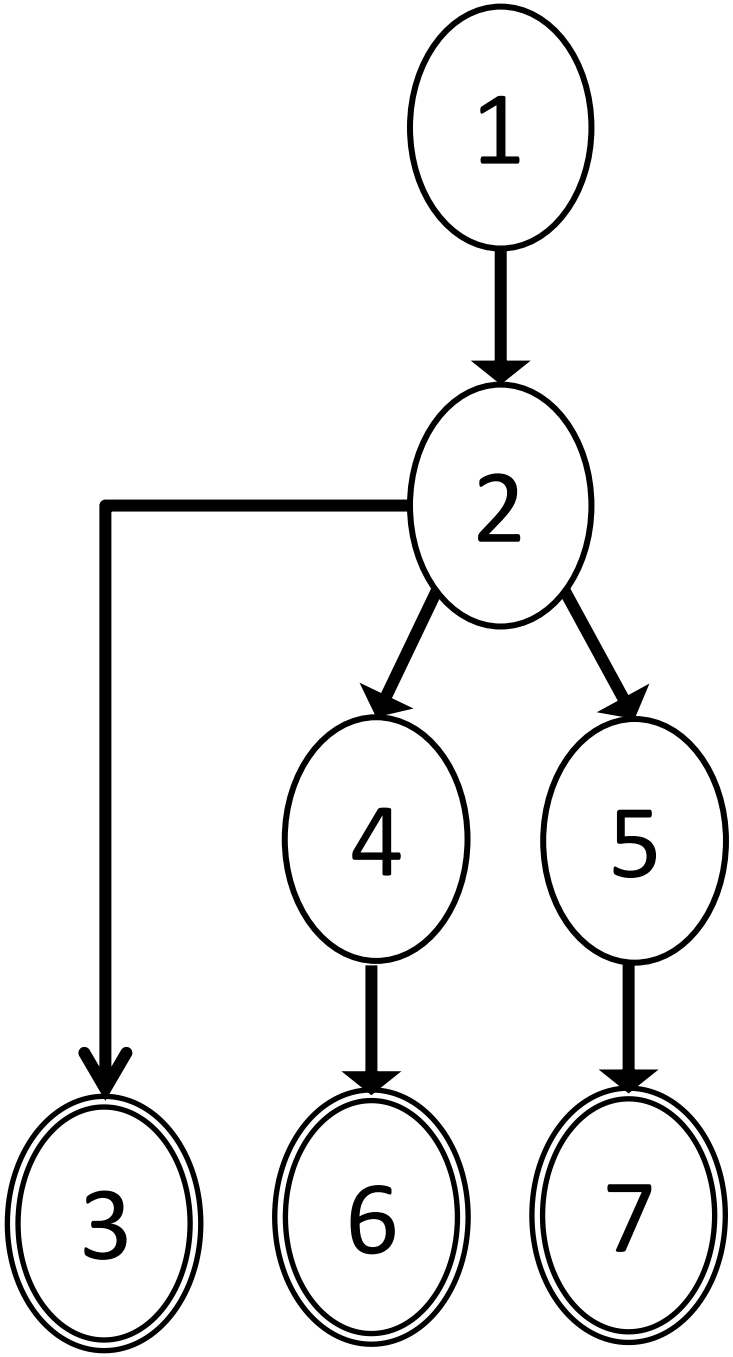

Fig.4 (b)

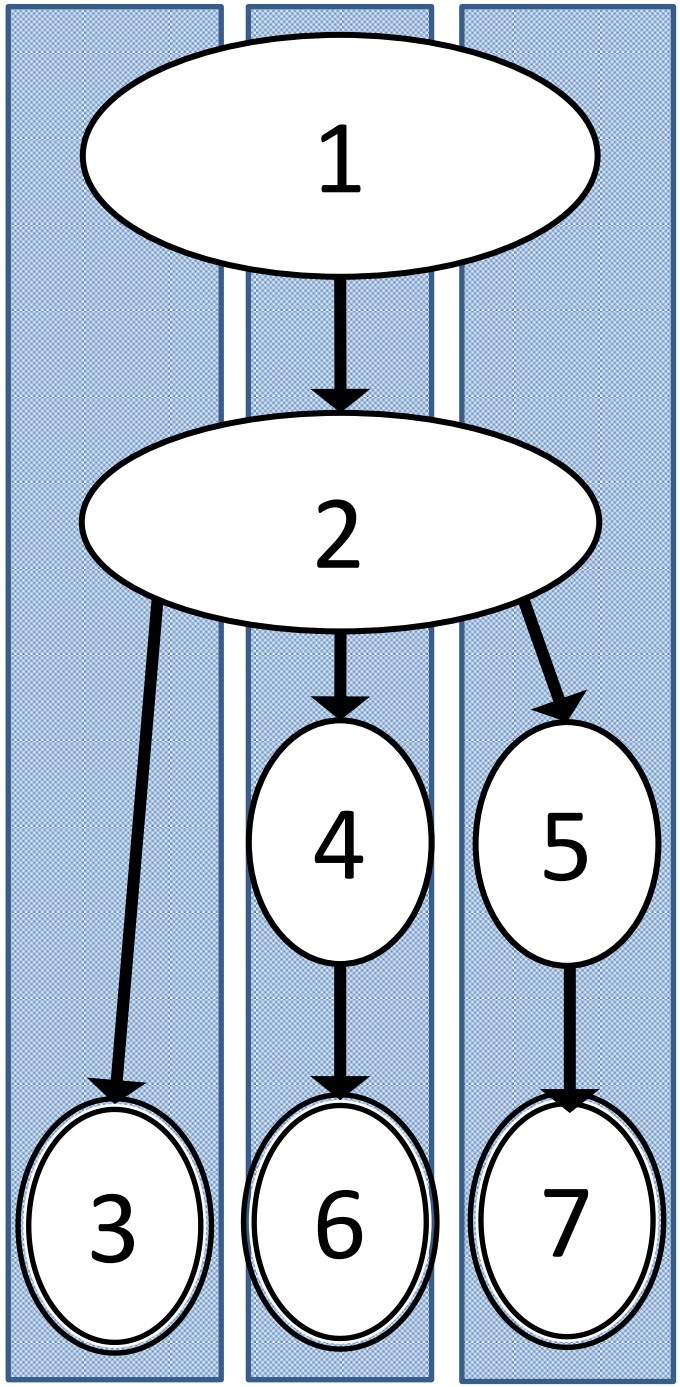

Fig.5 (a)

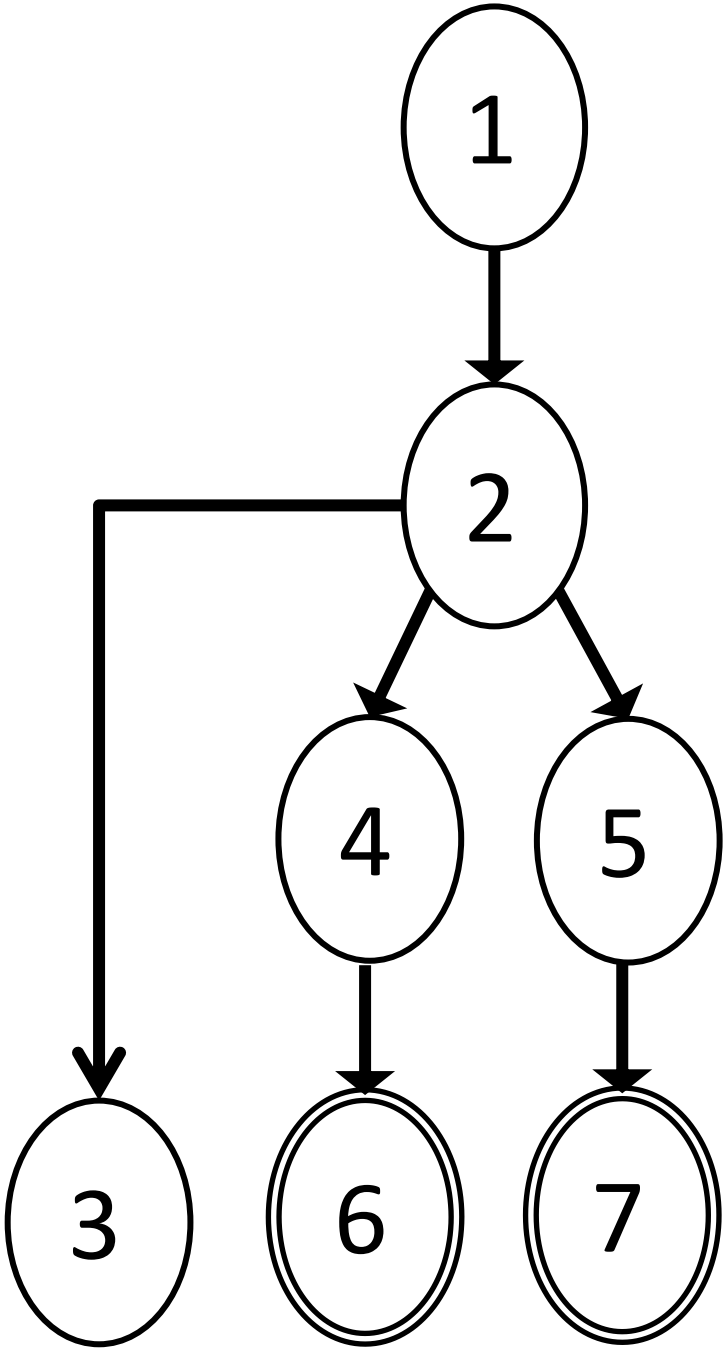

Fig.5 (b)

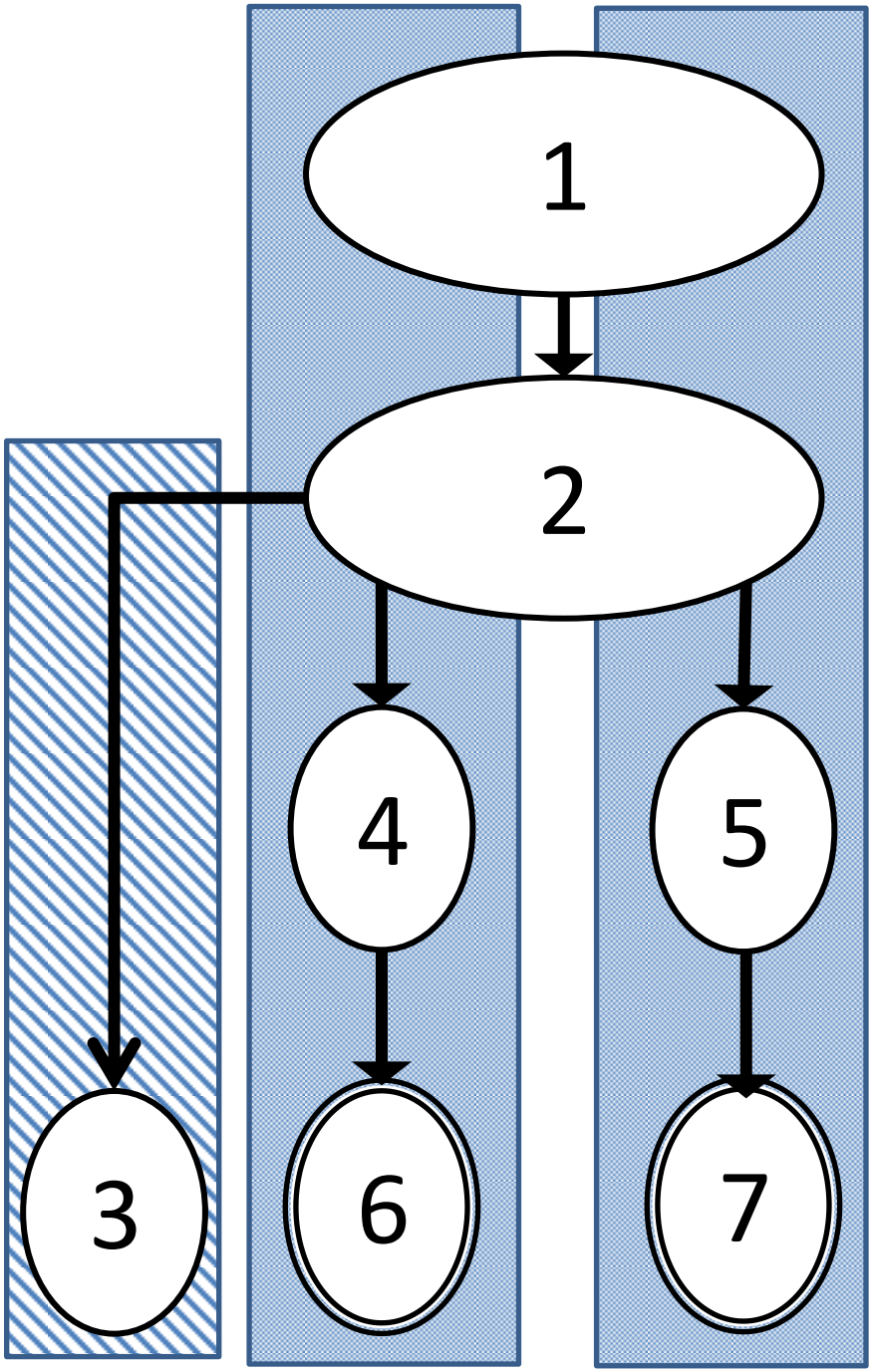

Fig.6 (a)

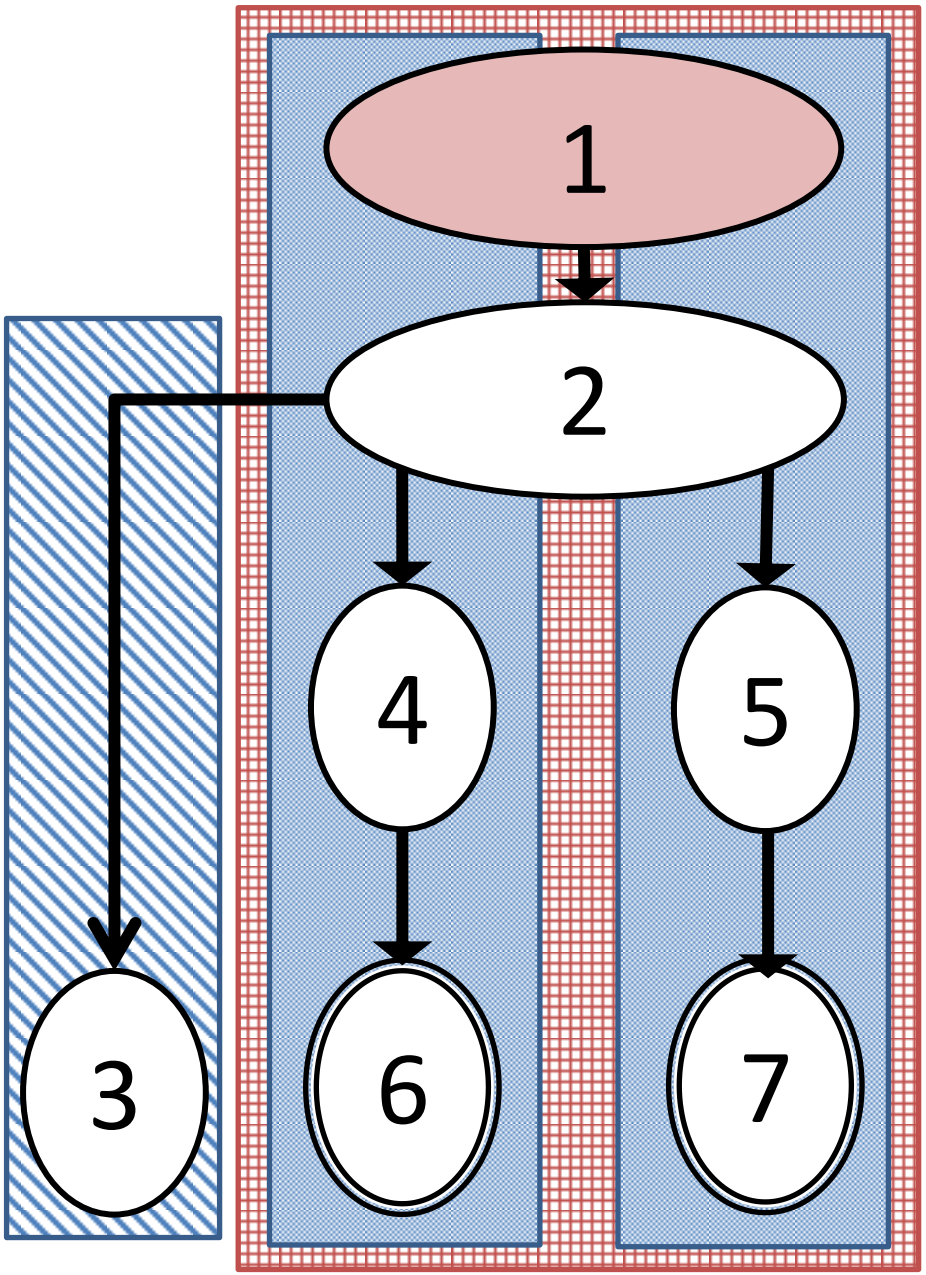

Fig.6 (b)

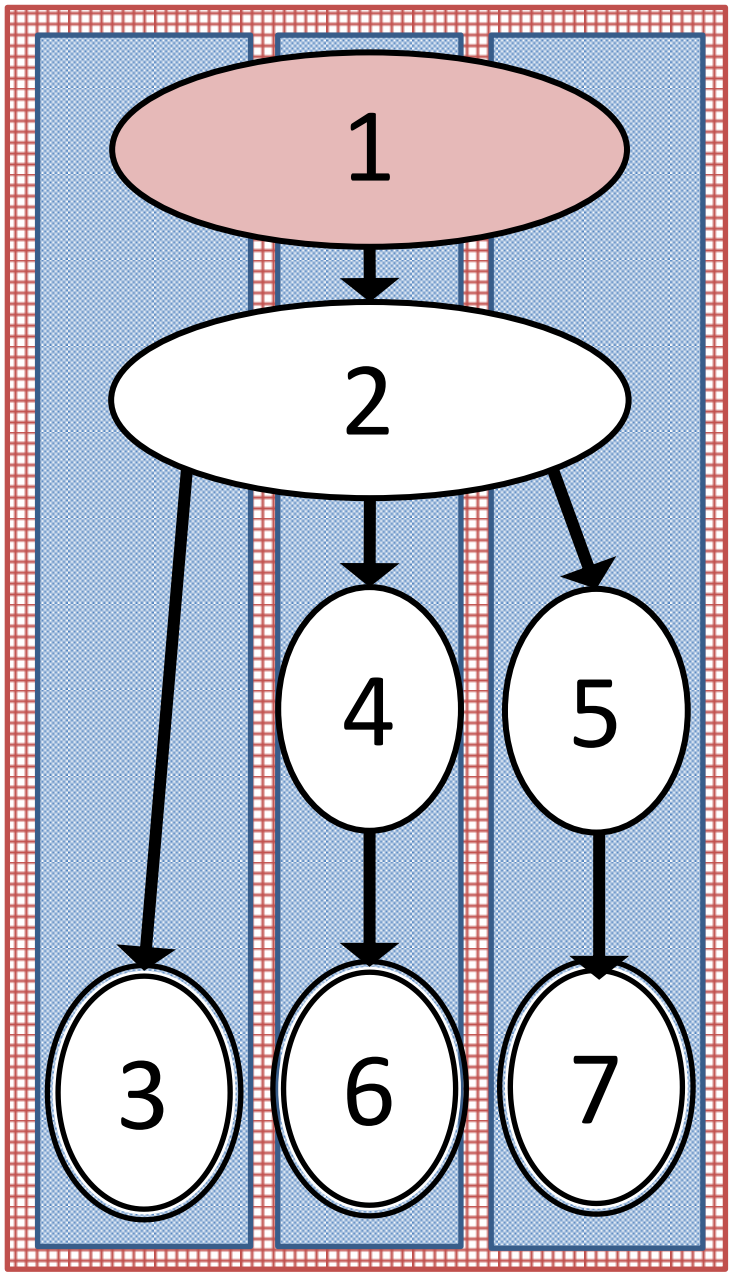

Fig.7 (a)

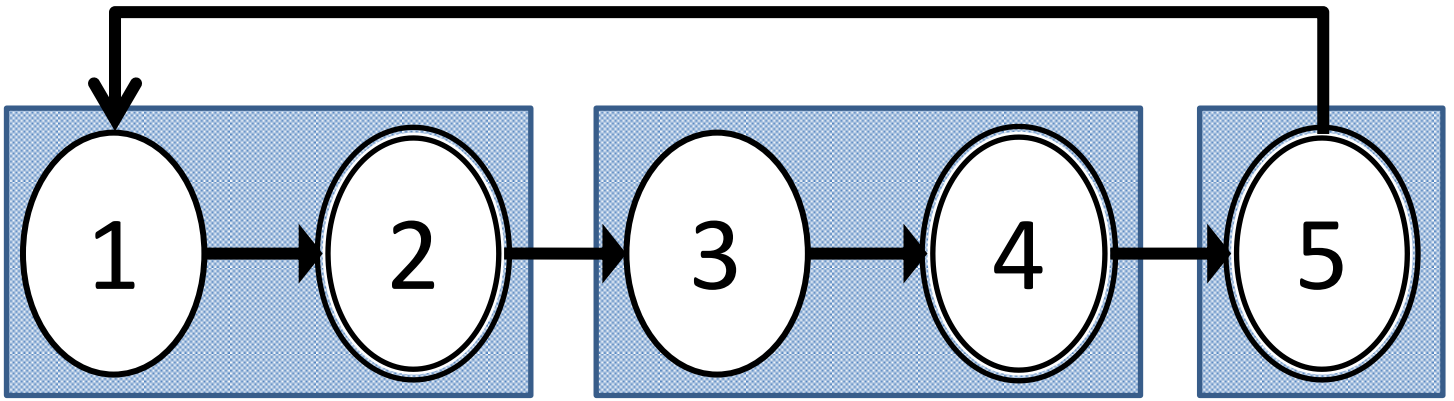

Fig.7 (b)

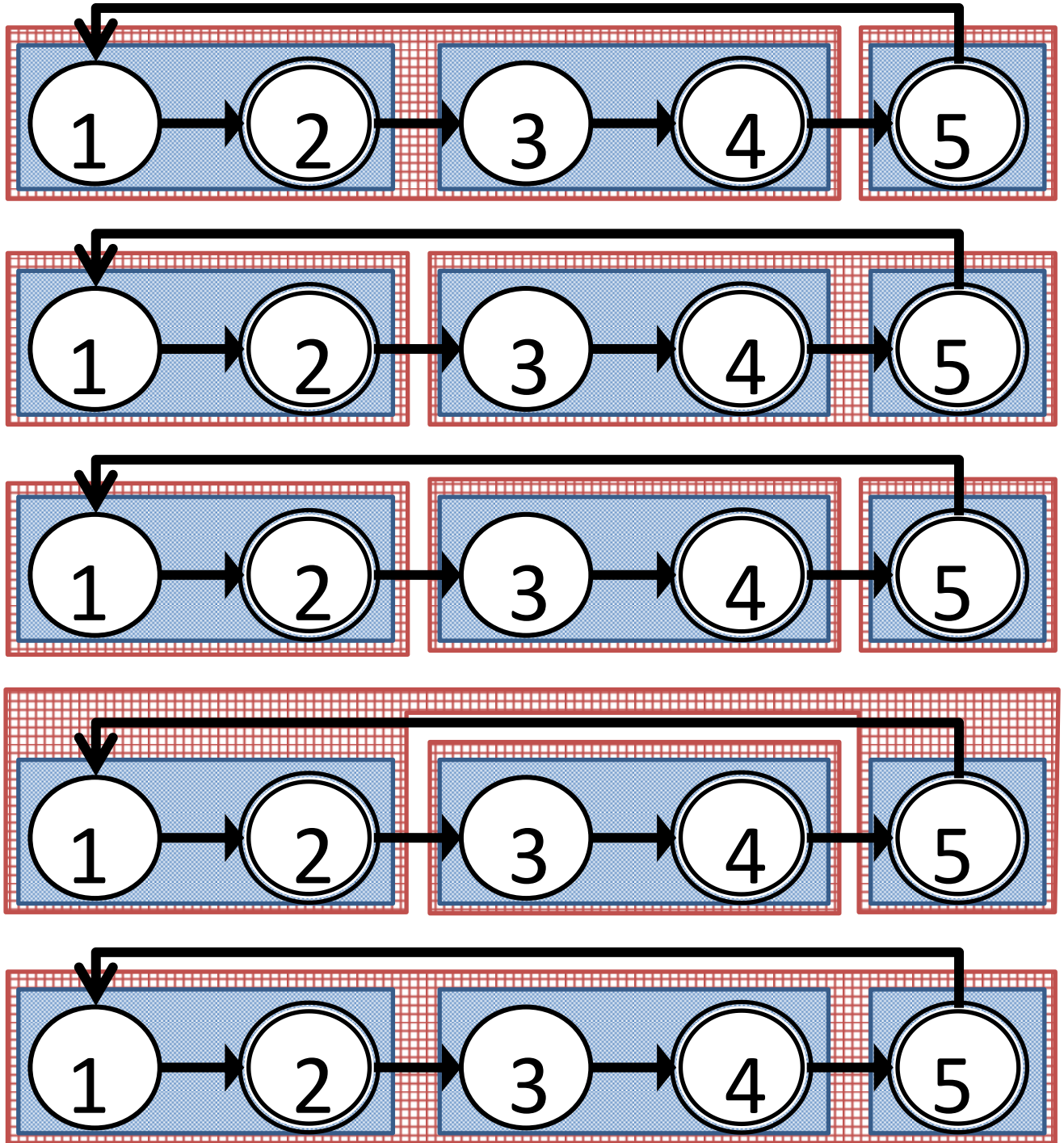

Fig.7 (c)